Note No.__

APPROVE

Deputy Chief Executive Officer of the State Enterprise “DIIA”

_____ Yurii KOZLOV
« 26 » February 2026

RULES AND PROCEDURES

FOR THE OPERATION OF THE QUALIFIED TRUST SERVICE PROVIDER “DIIA”

On 177 sheets

Kyiv 2026

TABLE OF CONTENT

INTRODUCTION

List of abbreviations

USR	Unified State Register of Legal Entities, Natural Persons- Entrepreneurs and Community Groups
USDR	Unified State Demographic Register
ICS	Information and Communication System
CPI	Cryptographic Protection of Information
QESST	Qualified Electronic Signature or Seal Tool
OS	Operating System
SW	Software
RNTRC	Registration number of the taxpayer's registration card
URN	Unique record number in the USDR
DPC	Data Processing Centre
CMP	Certificate Management Protocol
OCSP	Online Certificate Status Protocol
TSP	Time Stamp Protocol
ISMS	Information Security Management System according to the provisions of the standard ISO/IEC 27001:2022
AATL	Adobe's approved trust list of certificate authorities and trust service providers. Acrobat/Reader periodically downloads the trusted roots of these hierarchies so that document-signing certificates and timestamp services from AATL members are trusted automatically in Adobe products
AATL Technical Requirements	Adobe Approved Trust List Technical Requirements v2.0) — normative technical document by Adobe that sets eligibility criteria for participation in the AATL program for certificate authorities and trust service providers

Terms and definitions

In these Rules and Procedures, terms and definitions are applied in the meanings set out in the Civil Code of Ukraine, the Law of Ukraine "On Electronic Identification and Electronic Trust Services", Resolution of the Cabinet of Ministers of Ukraine No. 764 dated June 28, 2024 "Some Issues of Compliance with the Requirements in the Fields of Electronic Identification and Electronic Trust Services", Resolution of the Cabinet of Ministers of Ukraine No. 970 dated September 05, 2023 "Some Issues of Electronic Residents (E-residents) Activities and Maintenance of the "E-resident" Information System", Resolution of the Cabinet of Ministers of Ukraine No. 1137 dated December 04, 2019 "Issues of the Unified State Web Portal of Electronic Services and the Register of Administrative Services", and other legislative and regulatory acts on cryptographic and technical protection of information.

Status of the Rules and Procedures

These Rules and Procedures are a document of the Qualified Trust Service Provider "Diia" (hereinafter referred to as the QTSP "Diia"), which defines the organisational and methodological, technical and technological conditions of the QTSP "Diia" activity during provision of qualified electronic trust services, including the policy of the certificate and regulations on certification practices.

These Rules and Procedures are developed in accordance with:

- The Law of Ukraine "On Electronic Identification and Electronic Trust Services" (hereinafter referred to as the "Law");
- The Law of Ukraine "On Electronic Documents and Electronic Circulation of Documents" (with amendments);
- The Law of Ukraine "On State Registration of Legal Entities, Natural Persons - Entrepreneurs and Community Groups";
- Resolution of the Cabinet of Ministers of Ukraine No. 764 dated June 28, 2024 "Some Issues of Compliance with the Requirements in the Fields of Electronic Identification and Electronic Trust Services";
- Resolution of the Cabinet of Ministers of Ukraine No. 842 dated July 23, 2024 "On Approval of the List of Documents and Electronic Data Received as a Result of Provision of Electronic Trust Services That Are Subject to Continuous Storage and the Rules of Order for Transferring the Maintenance of Users of Electronic Trust Services with Whom a Qualified Trust Service Provider that Terminates the Provision of Qualified Electronic Trust Services Has Entered into Agreements for the Provision of Qualified Electronic Trust Services to Another Qualified Trust Service Provider";
- Resolution of the Cabinet of Ministers of Ukraine dated 10.10.2018 dated 10.12.2024 No. 1408 "Some issues of storage of documented information and its transfer to the central certifying body in the event of termination of the activities of a qualified provider of electronic trust services";
- Resolution of the Cabinet of Ministers of Ukraine No. 1137 dated December 04, 2019 "Issues of the Unified State Web Portal of Electronic Services and the Register of Administrative Services";
- Resolution of the Cabinet of Ministers of Ukraine No. 970 dated September 05, 2023 "Some Issues of Electronic Residents (E-residents) Activities and Maintenance of the "E-resident" Information System";
- other legislative and regulatory acts in the field of electronic trust services provision.

Provisions of these Rules and Procedures shall apply to:

- employees of the Head Office of the QTSP "Diia";

- employees of the separate registration units of the QTSP “Diia”;
- applicants;
- signatories;
- electronic seal creators.

Requirements of these Rules and Procedures are mandatory for employees of the Head Office and separate registration units of the QTSP “Diia”.

Acknowledgement of the requirements of these Rules and Procedures by applicants, signatories and electronic seal creators is a mandatory condition and reason for conducting an Agreement with them on the provision of qualified electronic trust services.

Requirements of these Rules and Procedures are founded on the principles of respect for rights and fulfilment of obligations by the entities of provision and receipt of qualified electronic trust services, which are set out in the Law of Ukraine “On Electronic Identification and Electronic Trust Services”.

Any interested person may familiarise themselves with the provisions of these Rules and Procedures on the official QTSP “Diia” website.

If an international Agreement, the approval of which has been given by the Verkhovna Rada of Ukraine, establishes rules other than those provided for in these Rules and Procedures, the rules of the international Agreement shall apply.

Amendments and additions to the Rules and Procedures

Approval, amendments and additions to these Rules and Procedures are carried out by the QTSP “Diia” in accordance with the Law of Ukraine “On Electronic Identification and Electronic Trust Services”.

QTSP “Diia” shall notify applicants, signatories, electronic seal creators and other interested parties of amendments and additions to these Rules and Procedures by posting the indicated amendments and additions on the official QTSP “Diia” website.

All amendments and additions made by the QTSP “Diia” to these Rules and Procedures, which are not related to changes in legislation, shall come into force 10 (ten) calendar days after the date of posting of the indicated amendments and additions on the official QTSP “Diia” website.

All amendments and additions made by the QTSP “Diia” to these Rules and Procedures due to changes in legislation shall come into force simultaneously with the entry into force of the appropriate legislative and regulatory acts, but not earlier than the moment of publication of amendments to these Rules and Procedures on the official website of the QTSP “Diia”.

1. GENERAL INFORMATION ABOUT THE PROVIDER

Full name of the legal entity QTSP “Diia”: State Enterprise “DIIA”.
Abbreviated names of the legal entity: SE “DIIA”.
Full name of the QTSP “Diia”: Qualified Trust Service Provider “DIIA”.
Abbreviated names of the QTSP “DIIA”: QTSP “DIIA”.
Legal address of the QTSP “Diia”: 24 Dilova Str., Kyiv, 03150
Postal address of the QTSP “Diia” Head Office: 24 Dilova Str., Kyiv, 03150.
Address of the QTSP “Diia” Head Office: 5B Vasylia Tiutiunnyka Str., Kyiv, 04070
Tel: +38 067 107-20-41.

USREOU code: 43395033.

Email addresses of the official QTSP “Diia” websites: ca.diia.gov.ua, ca.informjust.ua.

E-mail addresses of the QTSP “Diia” Head Office: ca@diia.gov.ua, keys@diia.gov.ua, ca@informjust.ua.

State Enterprise "DIIA" is a legal entity responsible for the activities of the QTSP "Diia" and the electronic trust services provided by it, in particular, services related to the issuing of qualified certificates, verification and confirmation of the validity of a qualified electronic signature or seal, including for the services provided by registration authorities.

Head Office of the QTSP “Diia” is represented by a separate department of the State Enterprise “Diia” (hereinafter referred to as SE “Diia”), which carries out the organisation of the provision of qualified electronic trust services by the QTSP “Diia” representative offices and ensures compliance of the qualified trust service providers with the requirements of the legislation.

QTSP “Diia” representative offices are separate registration units represented by separate subdivisions or non-staff units of the SE “Diia”, or legal entities or natural persons who, based on an Agreement with the SE “Diia”, carry out registration of users of electronic identification tools or signatories in compliance with the requirements of the legislation in the fields of electronic identification, electronic trust services and information protection.

Agreements for the provision of qualified electronic trust services shall be conducted on behalf of SE “DIIA” or on behalf of a representative office.

2. LIST OF QUALIFIED ELECTRONIC TRUST SERVICES

QTSP “Diia” provides the following qualified electronic trust services:

- qualified electronic trust service for the creation, verification and confirmation of a qualified electronic signature or seal;
- qualified electronic trust service for the formation, verification and confirmation of the validity of a qualified certificate of electronic signature or seal;
- qualified electronic trust service for the formation, verification and confirmation of the validity of a qualified electronic time stamp.

3. LIST OF POSITIONS AND FUNCTIONS OF THE PROVIDER’S PERSONNEL

QTSP “Diia” personnel, whose position responsibilities are directly related to the provision of qualified electronic trust services at the Head Office of the QTSP “Diia”, are employees who are assigned to the following functional responsibilities:

- Head of the QTSP “Diia”;
- Registration Administrator;
- Certification Administrator;
- Security Administrator;
- System Auditor;
- System Administrator.

Detailed description of the responsibilities of the QTSP “Diia” personnel is defined in the Clause 5.3.1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

Detailed description of the responsibilities of the separate registration unit officials of the QTSP “Diia” is defined in the Clause 5.3.1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

4. POLICY OF THE CERTIFICATE AND REGULATIONS ON CERTIFICATION PRACTICES

4.1. Policy of the Certificate

4.1.1. List of fields where it is allowed to use qualified certificates of public keys formed by the Provider

List of fields where it is allowed to use qualified certificates of public keys is defined in the Clause 1.4.1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

4.1.2. Restrictions on the use of qualified certificates of public keys formed by the Provider

Restrictions on the use of qualified certificates of public keys are defined in the Clause 1.4.2 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

4.1.3. List of information posted by the Provider on the official website

Clause 2.2 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains a list of information access to which is provided by the QTSP “Diia” through the official website.

4.1.4. Time and rules of order for publishing qualified certificates of public keys and lists of revoked certificates

Time and rules of order for publishing qualified certificates of public keys and lists of revoked certificates are defined in the Clause 2.3 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

4.1.5. Mechanism for confirming the applicant’s possession of a private key, the appropriate public key is provided to form a qualified certificate of public key

Mechanism for confirming the applicant’s possession of a private key, the appropriate public key is provided to form a qualified certificate of public key is defined in the Clause 3.2.1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

4.1.6. Terms for establishing the applicant

Terms for establishing the applicant (person/entity authentication) are defined in the Clause 3.2.2 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures), Clause 3.2.2 of the Regulation on Certification Practices of the Qualified Trust Service Provider “Diia” for Qualified Certificates of Electronic Signature and Seal (Annex 2 to

these Rules and Procedures) and the Clause 3.2.2 of the Regulation on Certification Practices of the Qualified Trust Service Provider “Diia” for Qualified Certificates of Remote Qualified Electronic Signature “Diia.Signature” (Annex 3 to these Rules and Procedures).

Terms of powers of the authorised representative of the legal entity are defined in the Clause 3.2.4 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures), Clause 3.2.4 of the Regulation on Certification Practices of the Qualified Trust Service Provider “Diia” for Qualified Certificates of Electronic Signature and Seal (Annex 2 to these Rules and Procedures) and the Clause 3.2.4 of Regulation on Certification Practices of the Qualified Trust Service Provider “Diia” Regarding Qualified Certificates of the Remote Qualified Electronic Signature “Diia.Signature” (Annex 3 to these Rules and Procedures).

4.1.7. **Authentication mechanism for the users who have a valid qualified certificate of public key formed by the Provider**

Authentication mechanism for the users who have a valid qualified certificate of public key formed by the QTSP “Diia” is defined in the Clause 3.3 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) and the Clause 3.3 of the Regulation on Certification Practices of the Qualified Trust Service Provider “Diia” Regarding Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures).

4.1.8. **User authentication mechanisms for blocking, cancelling or renewing a qualified certificate of public key**

User authentication mechanism for blocking, cancelling or renewing a qualified certificate of public key is defined in the Clause 3.4 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) and the Clause 3.4 of the Regulation on Certification Practices of the Qualified Trust Service Provider “Diia” for Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures).

4.1.9. **Physical environment description**

This section of the Rules and Procedures contains confidential information about the QTSP “Diia” in accordance with the Regulation on Confidentiality and Classification of Information at the SE “Diia”, approved by the Order of the SE “Diia” No. 20231220-3 dated December 20, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 2 dated December 19, 2023”.

Procedure for access to the special premises of the QTSP “Diia” is defined in the Clause 5.1.2 of the Policy of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

4.1.10. **Procedural control**

Provisions on procedural control are defined in Clause 5.2 of the Regulation on Certification Practices of the Qualified Trust Service Provider “Diia” regarding Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures).

4.1.11. **Rules of order for maintaining event audit log books**

This section of the regulations is not included in the scope of provisions specified by the provider for users to review.

4.1.12. **Procedure for maintaining the Provider's archives**

This section of the regulations is not included in the scope of provisions specified by the provider for users to review.

4.1.13. **Process, rules of order and terms for generating key pairs of the Provider and users**

This section of the regulations is not included in the scope of provisions specified by the provider for users to review.

4.1.14. **Procedures for receiving a private key by the user as a result of the provision of a qualified electronic trust service by the Provider**

Procedures for receiving a private key by the user as a result of the provision of a qualified electronic trust service are defined in the Clause 6.1.2 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures).

4.1.15. **Mechanism for providing the user's public key to the Provider to form a qualified certificate of public key**

Mechanism for providing the public key of the user of the QTSP "Diia" to form a qualified certificate of public key is defined in the Clause 6.1.3 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures).

4.1.16. **Rules of order for protection and access to the Provider's private key**

This section of the regulations is not included in the scope of provisions specified by the provider for users to review.

4.1.17. **Rules of order and conditions for backup of the Provider's private key, the servers of ICS of Provider, Administrators, storage, access and use of backup copies**

Rules of order and conditions for backup of the private key of the QTSP "Diia", the servers of QTSP "Diia" ICS are defined in the Clause 6.2.4 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures).

Rules of order for backup of the private keys of QTSP "Diia", servers of QTSP "Diia" ICS (OCSP, TSP, CMP) and Administrators is defined in the Rules of Order of Their Generation (Clauses 4.1.13.1 and 4.1.13.2 of these Rules and Procedures).

Facts of backup of the private keys of the QTSP "Diia" and servers of QTSP "Diia" ICS (OCSP, TSP, CMP) shall be recorded in the key data log book.

Facts of renewal of the private keys of QTSP "Diia" and servers of the QTSP "Diia" ICS (OCSP, TSP, CMP) from backup copies or application (transition to use) of backup QESST (network cryptomodules) with private keys shall be recorded in the key data log. Upon the fact of renewal of private keys or use of backup copies of QESST or network cryptomodules, the acts shall be drawn up.

A backup of the QTSP “Diia” private key may be used with the permission of the QTSP “Diia” Head in case of a failure of the network cryptomodule in which the private key was stored and used to recover the key in the repaired or replaced network cryptomodule.

Backup copies of personal keys of servers of QTSP “Diia” ICS (OCSP, TSP, CMP) can be used in case of failure of the QESST with the private keys of the servers or network cryptomodules in which they were stored and used to replace the main QESST or to recover the keys in the repaired or replaced network cryptomodule.

Backup copies of the Administrators’ private keys can be not created. At the same time, backup QESST with pre-generated private keys can be issued to the Administrators. Requests for the formation of the Administrators’ qualified certificates of public keys are stored by the Security Administrator. In case of compromise of the private key or failure of the main QESST, a new qualified certificate is issued to the Administrator, and the Administrator starts using the backup QESST.

4.2. REGULATION ON CERTIFICATION PRACTICES

4.2.1. Process for submitting a request for the formation of a qualified certificate of public key

Rules of order for submitting a request for the formation of a qualified certificate of public key is defined in the Clause 4.1 of the Regulation on Certification Practices of the Qualified Trust Service Provider “Diia” Regarding Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures).

4.2.2. Rules of order for providing the formed qualified certificate of public key to the user

Rules of order for providing the formed qualified certificate of public key to the user is defined in the Clause 4.3 of the Regulations of Certification Practices of the Qualified Trust Service Provider “Diia” Regarding Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures).

Sequence of actions of the user to verify the data contained in the generated qualified certificate of public key is defined in the Clause 4.4 of the Regulation on Certification Practices of the Qualified Trust Service Provider “Diia” Regarding Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures).

4.2.3. Rules of order for publishing the formed user’s qualified certificate of public key on the Provider’s official website

Rules of order for publishing the formed user’s qualified certificate of public key on the QTSP “Diia” official website is defined in the Clause 2.2.1 of the Regulation on Certification Practices of the Qualified Trust Service Provider “Diia” Regarding Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures).

4.2.4. Terms of use of a user’s qualified certificate of public key and user’s private key

Terms of use of electronic trust services by users are defined in the Clause 1.3.3.2 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

Qualified certificates of public key of signatories and electronic seal creators shall be used in the fields and with the restrictions specified in the Clauses 1.4.1 and 1.4.2 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures).

The consequences of improper use of a qualified certificate of the public key and private key may include unreliable authentication of the signatory or an electronic seal creator in information systems, misuse of user access rights to information, forgery of electronic documents, material and reputational losses of the user.

Terms of use of the user's qualified certificate of public key and user's private key, as well as information on the consequences of their incorrect use, shall be specified in the Agreement for the provision of a qualified electronic trust service.

4.2.5. **Procedure for submitting a request for formation of a qualified certificate of public key for users who have a valid qualified certificate of public key formed by the Provider**

Rules of order for submitting a request for formation of a qualified certificate of public key for users who have a valid qualified certificate of public key formed by the QTSP "Diia" is defined in the Clause 4.7 of the Regulation on Certification Practices of the Qualified Trust Service Provider "Diia" Regarding Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures).

4.2.6. **Circumstances of cancellation (blocking, renewal) of a qualified certificate of public key**

List of circumstances for changing the status of a qualified certificate of public key is defined in the Clause 3.4 of the Regulation on Certification Practices of the Qualified Trust Service Provider "Diia" for Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures).

Rules of order for blocking and cancelling a qualified certificate of public key is defined in the Clause 4.9 of the Regulation on Certification Practices of the Qualified Trust Service Provider "Diia" Regarding Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures).

Rules of order for forming lists of revoked certificates, publishing and distributing lists of revoked certificates is defined in the Clause 2.3 of the Regulation on Certification Practices of the Qualified Trust Service Provider "Diia" for Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures).

4.2.7. **Expiration date of a User's qualified certificate of public key**

Validity period of user's qualified certificates of public keys is defined in the Clause 1.4.1.2 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" for Qualified Certificates of the Electronic Signature and Seal (Annex 1 to these Rules and Procedures).

Validity period of user's qualified certificates of public keys is no more than two years.

Date and time of the beginning and end of the validity period of a qualified certificate of public key of user shall be indicated in such certificate with an accuracy of one second.

After the date and time of expiry of the qualified certificate of public key of the user, such qualified certificate of public key shall be deemed invalid.

4.2.8. **Organisational requirements**

These Rules and Procedures, as well as other regulatory documents of the QTSP “Diia”, define the procedure requirements for managing risks, personnel, operational security, incidents, evidence and archives, handling with personal data of users, procedures for identifying the applicant, operation of separate registration units, physical environment description.

5. PROCEDURES AND PROCESSES CARRIED OUT DURING PROVIDING QUALIFIED ELECTRONIC TRUST SERVICES THAT DO NOT PROVIDE FOR THE FORMATION AND MAINTENANCE OF QUALIFIED CERTIFICATES

5.1. Provision of qualified electronic signature or seal tools

In order to provide qualified electronic trust services, QTSP “Diia” uses qualified electronic signature or seal tools that have documentary evidence of compliance with the requirements of the Articles 18 and 19 of the Law, issued based on the results of certification of such tools.

Provision of qualified electronic signature or seal tools in the form of hardware and software and their technical support and maintenance by the QTSP “Diia” is carried out on a contractual basis.

Provision of qualified electronic signature or seal tools by the QTSP “Diia” in the form of separate software applications or software modules (crypto libraries) operating as part of other software applications may be carried out by transferring these tools on information media directly to the signatory or creator of the electronic seal or by providing access through the QTSP “Diia” official website.

Qualified electronic signature or seal tools in the form of SIM cards are provided to users by the QTSP “Diia” or by the mobile operator that serves such tools and that carries out the functions of the QTSP “Diia” representative office (separate registration unit).

Generation of private keys as part of key pairs in qualified electronic signature tools in the form of SIM cards is carried out by the built-in mechanisms of these hardware and software means. Assistance in generating keys in the SIM card is provided by the Administrator of Registration or an employee of the representative office of the QTSP “Diia” (separate registration unit), who is responsible for registering users and who carries out the functions of the Administrator of Registration.

5.2. Provision of a qualified electronic trust service for formation, verification and confirmation of a qualified electronic time stamp

Rules of order for providing a qualified electronic trust service for formation, verification and confirmation of a qualified electronic time stamp is defined in the Clause 6.8 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

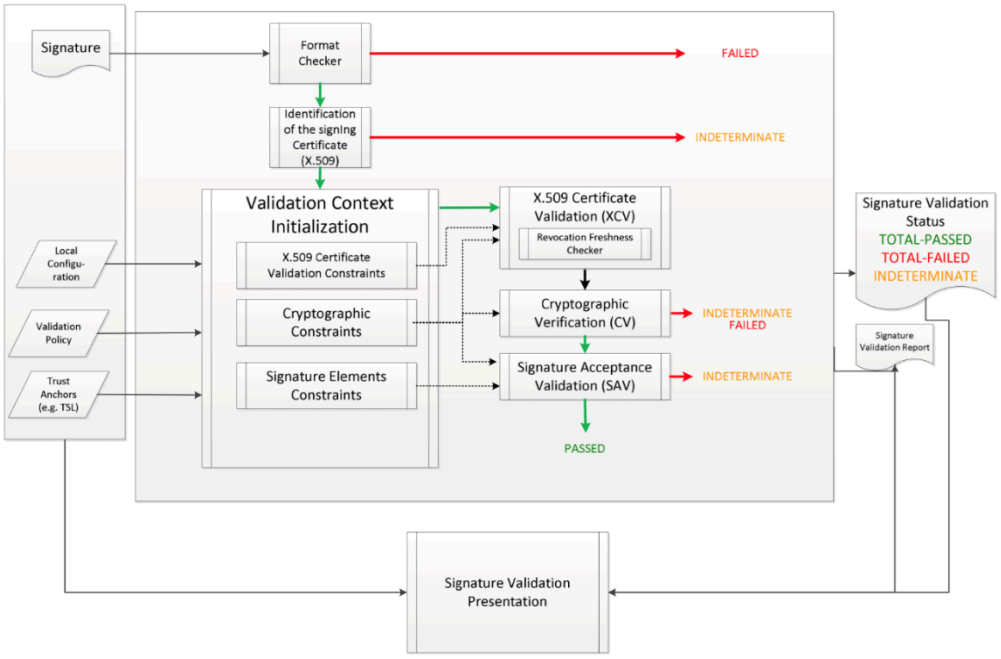
5.3. Design of the signature verification process

Verification and confirmation of an electronic signature or seal affixed to an electronic document (hereinafter referred to as signature verification) is carried out by QTSP "Diia" as part of the provision of a qualified electronic trust service for creation, verification and confirmation of a qualified electronic signature or seal.

All interested users can verify the signature using the Signature Verification Service located at the following links:

on the website of QTSP "Diia" at the link: https://ca.diia.gov.ua/verify;
on the website of the central certification body at the link: https://czo.gov.ua/verify;
on the website of the integrated system of electronic identification at the link: https://id.gov.ua/verify.

The design of the signature verification process using the Signature Verification Service that complies with DSTU ETSI EN 319 102-1:2022 (ETSI EN 319 102-1 V1.3.1 (2021-11), IDT) "Electronic signatures and infrastructures (ESI). Creation procedures and AdES digital signature checks Part 1. Formation and verification" (hereinafter - ETSI EN 319 102-1), shown in Scheme 1.



The signature can also be checked using the PC software "IIT User CSK-1" in accordance with the instructions of the PC operator "IIT User CSK-1", which are posted on the website of QTSP "Diia" at the link: https://ca.diia.gov.ua/download-all.

5.3.1. Requirements for the signature verification process

The signature verification process performed using the Signature Verification Service complies with ETSI EN 319 102-1.

Clauses 5.3.2 - 5.3.4 of this Regulation define separate components of the signature verification process and restrictions. If there are no specific requirements for the signature verification process in this Regulation, the requirements defined in ETSI EN 319 102-1 shall apply.

QTSP "Diia" implements the algorithm defined in ETSI EN 319 102-1, allowing alternative implementations, provided that they produce the same basic status indication when receiving the same set of input information. The specific requirements for the signature verification process set out in this Regulation take precedence over the requirements set out in ETSI EN 319 102-1.

The Signature Verification Service provides a comprehensive verification report, allowing the application software to review the details of the qualifications accepted during the verification and to investigate in detail the reasons reflected in the qualifications provided by the Signature Verification Service.

The signature verification service provides a report in a user-friendly way – a readable HTML page with the possibility of downloading the verification report in the form of a PDF file with the superimposed qualified electronic seal of the QTSP "Diia".

The result of the signature verification process contains the attributes and artifacts provided by ETSI EN 319 102-1, including but not limited to:

- list of verified signatures;
- status indicating the results of the signature verification process;
- errors describing why the signature is invalid (TOTAL-FAILED) or warnings describing why the Signature Verification Service was unable to determine the status of the signature (INDETERMINATE);
- an indication of the policy according to which the signature was verified;
- use of any alias, if applicable.

According to the algorithm defined in ETSI EN 319 102-1, the signature verification status can be:

1. TOTAL-PASSED
2. TOTAL-FAILED
3. INDETERMINATE

The structure of the semantics of the verification report is given in Table 7.

Table 7

Main qualification	**Relevant information in the inspection report**	**Semantics**

TOTAL-PASSED	The verification process must establish a validated certificate chain, including the certificate used in the verification process. In addition, the validation process can provide a validation result for each of the validation constraints. The verification process must ensure that the DA has access to the signed attributes present in the signature, signer identity, and certificate chain	The signature verification process results in TOTAL-PASSED based on the following considerations: • the cryptographic signature checks were successful (including checks on the hashes of individual data objects that were indirectly signed); • any restrictions applicable to the certification of the signer's identity were validated (i.e., the certificate was consequently deemed to be trusted); • the signature was positively verified against the verification constraints and is therefore considered to comply with those constraints
TOTAL-FAILED	The verification process should establish additional information to explain the TOTAL-FAILED indication for each of the verification constraints that were considered and for which a negative result occurred.	The signature verification process results in TOTAL-FAILED because it failed to verify the format, cryptographic signature checks (including hash checks of individual data objects that were signed indirectly), or it was proven that the signature generation occurred after the certificate was revoked
INDETERMINATE	The validation process should establish additional information to explain the INDETERMINATE indication and to help the verifier determine what data is missing to complete the validation process. In particular, it should provide verification result	There is not enough information available to determine whether the signature is TOTAL-PASSED or TOTAL-FAILED.

	indications for those verification constraints that were considered and for which an indeterminate result occurred.	

In addition to the main status, the signature verification report also contains additional information with the semantics defined in Table 8.

Table 8

Main qualification	Secondary qualification	Relevant information in the inspection report	Semantics
TOTAL-FAILED	**FORMAT_FAILURE**	The verification process should provide any available information explaining why signature parsing failed.	The signature does not meet one of the basic standards to the extent that the cryptographic verification building block cannot process it.
	HASH_FAILURE	The process shall establish: The identifier(s) (e.g., URI or OID) that uniquely identifies the element in the signed	The signature verification process results in TOTAL-FAILED because at least one hash of the signed data object(s)

		data object (e.g., signature attributes or SD) that caused the error	that was included in the signing process does not match the corresponding hash value in the signature.
	SIG_CRYPTO_FAILURE	The process must install the certificate used in the verification process	The signature verification process results in TOTAL-FAILED because the signature value in the signature could not be verified using the signer's public key in the certificate
	REVOKED	The process should establish: • The certificate chain used in the verification process. • The time and, if available, the reason for the certificate revocation	The signature verification process results in TOTAL-FAILED because: • the certificate has been revoked; and • there is evidence of signature creation after the certificate was revoked
	EXPIRED	The process must establish a verified certificate chain	The result of the signature verification process is TOTAL-FAILED because there is evidence that the signature was created after the certificate expired (notAfter)
	NOT_YET_VALID		The result of the signature verification process is TOTAL-FAILED because there is evidence that the signature was created before the certificate issuance date (notBefore)

INDETERMINATE	**SIG_CONSTRAINTS_FAILURE**	The process must establish a set of constraints that the signature does not meet.	The result of the signature validation process is INDETERMINATE because one or more signature attributes do not meet the validation constraints.
	CHAIN_CONSTRAINTS_FAILURE	The process should establish: • The certificate chain used in the verification process. • The set of constraints that were not satisfied by the chain	The signature verification process resulted in INDETERMINATE because the certificate chain used in the verification process does not meet the verification constraints associated with the certificate
	CERTIFICATE_CHAIN_GENERAL_FAILURE	The process should establish additional information regarding the cause	The signature verification process resulted in INDETERMINATE because the set of certificates available for chain verification failed for an unspecified reason.
	CRYPTO_CONSTRAINTS_FAILURE	The process shall establish the identity of an entity (signature, certificate) created using an algorithm or key size below the required level of cryptographic security. If known, the time up to which the algorithm or key size was considered secure	The signature verification process results in INDETERMINATE because at least one of the algorithms used in the entity (e.g., signature value, certificate, etc.) involved in the signature verification, or the key size used with such an algorithm, is below the required

			cryptographic level of security, and: this material was created after the time up to which this algorithm/key was considered secure (if such time is known); and the material is not protected by a sufficiently strong timestamp applied to the time up to which this algorithm/key was considered secure (if such time is known)
	POLICY_PROCESSING_ ERROR	The process should provide additional information about the problem	The signature verification process resulted in INDETERMINATE because the specified formal policy file could not be processed for any reason (e.g., unavailable, unable to parse, digest mismatch, etc.)
	SIGNATURE_POLICY_NOT_AVAILABLE	-	The signature verification process results in INDETERMINATE because the electronic document containing the policy details is not available
	TIMESTAMP_ORDER_ FAILURE	The process must establish a list of timestamps that do not meet the ordering constraints.	The result of the signature verification process is INDETERMINATE because some constraints on the order of the signature

			timestamps and/or the signed timestamps of the data object(s) are not respected
	NO_SIGNING_CERTIFICATE_FOUND	-	The signature verification process results in INDETERMINATE because the certificate cannot be identified
	NO_CERTIFICATE_CHAIN_FOUND	-	The result of the signature verification process is INDETERMINATE because no certificate chain was found for the identified certificate.
	NO_CERTIFICATE_CHAIN_FOUND_NO_POE		The signature verification process results in INDETERMINATE because no certificate chain was found for the identified signing certificate because the trust binding is not trusted at the date/time of the verification according to the verification policy in use. However, the signature verification algorithm cannot ensure that the signing time is before or after the time the trust binding was trusted by the verification policy in use.

	REVOKED_NO_POE	The process should establish: • The certificate chain used in the verification process. • The time and reason for certificate revocation	The signature verification process results in INDETERMINATE because the certificate was revoked at the date/time of the verification. However, the signature verification algorithm cannot verify that the signing time is before or after the revocation time.
	REVOKED_CA_NO_POE	The process should establish: • The certificate chain that includes the revoked CA certificate. • The time and reason for the certificate revocation	The signature verification process resulted in INDETERMINATE because at least one certificate chain was found, but the intermediate CA certificate has been revoked.
	OUT_OF_BOUNDS_NOT_REVOKED	-	The signature verification process results in INDETERMINATE because the signing certificate has expired or is not yet valid at the date/time of the verification, and the signature verification algorithm cannot verify that the signing time is within the validity interval of the signing certificate. The certificate is known not to have been revoked
	OUT_OF_BOUNDS_NO_POE	-	The signature verification process

			results in INDETERMINATE because the certificate has expired or is not yet valid at the date/time of the verification, and the signature verification algorithm cannot verify that the signing time is within the certificate validity interval.
	REVOCATION_OUT_OF_BOUNDS_NO_POE	The validation process should provide the following: • The certificate chain used in the validation process. • Revocation data related to the error	The signature verification process results in INDETERMINATE because the revocation data signing certificate containing the revocation status information of the signing certificate has expired or is not yet valid at the date/time of the verification, and the signature verification algorithm cannot verify that the revocation data is confirmed to exist at a time that is within the validity period of the revocation data signing certificate
	CRYPTO_CONSTRAINTS_FAILURE_NO_POE	The process should establish: • The identification of material (signature, certificate) created using an algorithm or key size	The signature verification process results in INDETERMINATE because at least one of the algorithms used in the objects (e.g., signature value,

		below the required level of cryptographic security. • The time until which the algorithm or key size was considered secure, if known	certificate, etc.) involved in the signature verification, or the key size used with such an algorithm, is below the required cryptographic security level, and there is no evidence that this material was created before the time when this algorithm/key was considered secure.
	NO_POE	The process should at least detect signed objects for which POEs are missing. The verification process should provide additional information about the problem	The signature verification process results in INDETERMINATE because there is no proof of existence to confirm that the signed object was created before some compromising event (e.g., a faulty algorithm)
	TRY_LATER	The process should establish the point in time when the required recall information is expected to be available.	The signature verification process results in INDETERMINATE because not all constraints can be satisfied with the available information. However, it is possible to do so with additional revocation information that will be available later.
	SIGNED_DATA_NOT_FOUND	The process must establish the identifier(s) (e.g., URI) of the signed data that caused the error.	The signature verification process results in INDETERMINATE

			because the signed data cannot be retrieved.
	CUSTOM	The process should output information that allows you to identify the cause of the result of a special diagnostic	The signature verification process results in INDETERMINATE for a specific diagnostic not specified in this document
	GENERIC	The process must establish additional information why the verification status was declared INDETERMINATE.	The signature verification process results in INDETERMINATE for any other reason

The Signature Verification Service shall apply an appropriate signature verification policy, such that:

- The Signature Verification Service shall not accept multiple sources of signature verification policies;
- The Signature Verification Policy shall not be overridden and replaced by signature verification roles according to the protocol defined in ETSI EN 319 102-1;
- The verification process shall ensure that the signature verification policy used complies with the policy defined in the Signature Verification Service policy or the terms of use of the Signature Verification Service;
- The policy defined in the Signature Verification Service policy or the terms of use of the Signature Verification Service shall adhere to the following principles:
    - For the same input, including the signature verification policy, the Signature Verification Service shall return the same result;
    - The Signature Verification Service may accept different elements as proof of existence for a signature.

5.3.1.1 Signature verification process

Depending on the electronic signature/seal format used, the Signature Verification Service supports verification processes for basic signature/seal formats and extended formats (with an added electronic timestamp or time verification data) as follows:

- Basic Signature/Seal Verification Process – Basic Level;
- Signature/Seal Verification Process with Base Time - Basic Level + T;
- Signature/Seal Verification Process with Long-Term Verification Data - Basic Level + LT

The process consists of the following steps:
Step 1. The user creates and sends a signature verification request.

Signature verification limitations are defined in ETSI EN 319 102-1, and in accordance with this policy, QTSP "Diia" limits signature verification only to the parameters described therein.
QTSP "Diia" does not support signature verification policies provided by the user.

Step 2. The signature verification service implements the signature verification process in accordance with ETSI EN 319 102-1.
The verification is performed by the Signature Verification Service in accordance with the restrictions set by the service itself.

Step 3. The Signature Verification Service prepares and sends a response for signature verification. QTSP "Diia" may use the protocols described in DSTU ETSI TS 119 442:2021 (ETSI TS 119 442 V1.1.1 (2019-02), IDT) "Electronic Signatures and Infrastructures (ESI). Protocol Profiles for Trust Service Providers Providing AdES Digital Signature Verification Services".

The response to the signature verification confirmation is entered into a verification report containing:

- A report with a qualified electronic seal of QTSP "Diia". Reports for each signature verification restriction:
- if the restriction was processed, with the corresponding result;
- if the restriction was not processed, with an instruction that the restriction was ignored or replaced, if applicable.

Step 4. Presentation of the signature verification report.

5.3.1.2 Verification restrictions for electronically signed documents

The Signature Verification Service is controlled by a set of verification constraints. These constraints are defined during operation when managing the Signature Verification Service. In addition, there may be constraints on the certificates used for the electronic signature/seal. The service supports certain constraints related to the elements of the posted signature/seal, the allowed cryptographic combinations and algorithms used, as well as other constraints. There are constraints on the size of the file with the electronic signature that is accepted for signing.

5.3.1.3 Verification restrictions for electronic signature or seal certificates

The signature verification service supports verification constraints for electronic signature/seal certificates in accordance with DSTU ETSI TS 119 172-1:2016 (ETSI TS 119 172-1:2015, IDT) "Electronic Signatures and Infrastructures (ESI). Signature Policies. Part 1. Components and content of human-readable signature policy documents" (hereinafter - ETSI TS 119 172-1).

5.3.1.4 Cryptographic suite limitations

The signature verification service supports cryptographic constraints associated with the required algorithms and parameters in accordance with DSTU ETSI TS 119 312:2022 (ETSI TS 119 312 V1.4.2 (2022-02), IDT) "Electronic Signatures and Infrastructures (ESI). Cryptographic Packages", and meets the requirements of ETSI TS 119 172-1.

5.3.1.5 Restrictions on signature or seal elements

The signature verification service supports restrictions on qualified verification elements of electronic signatures and seals according to the requirements of ETSI TS 119 172-1.

5.3.2. Signature verification protocol requirements

The signature verification service supports restrictions on qualified verification elements of electronic signatures and seals according to the requirements of ETSI TS 119 172-1.

5.3.3. Interface

The Signature Verification Service interface defines the signature verification interface for a single document that has an electronic signature or seal applied to it.

5.3.3.1 Communication channel

The communication channel between the user and the Signature Verification Service is protected using a securely protected channel using the HTTPS protocol and using a TLS 1.2 or higher security channel. QTSP "Diia" guarantees that it can establish a secure channel with the user and maintain data confidentiality.

The Signature Verification Service does not require the user to authenticate in it using electronic identification means.

5.3.3.2 Provider – other providers of electronic trust services

The status of the signature verification and the signature verification report may be affected by the provisions of practices, policies for the provision of electronic trust services and agreements of other electronic trust service providers, the activities of which are beyond the control of QTSP "Diia".

The signature verification service (QTSP "Diia") may, in order to obtain the necessary information, send requests to other electronic trust service providers that provide the formation of electronic time stamps, signature verification, the formation of certificate revocation lists (CRLs) and certificate status protocols (OCSP).

The issue of the functioning of the communication channel between QTSP "Diia" and other electronic trust service providers is beyond the scope of these Regulations.

5.3.4. Signature Verification Report Requirements

QTSP "Diia" provides three types of verification reports:
- a simple signature verification report, which provides the necessary information about the signer's identity and an indication of the status of each verified signature, including additional indications.

- a detailed signature verification report, which provides information about each signature verification constraint that is processed, including any signature verification constraints implicitly applied by the implementation.

- a machine-readable verification report, which complies with the requirements of ETSI EN 319 102-1 and ETSI TS 119 172-4 and provides a detailed verification report in XML format.

- All signature verification reports provided to QTSP "Diia" must bear the qualified electronic seal of QTSP "Diia".

6. ELECTRONIC IDENTIFICATION SCHEME

Electronic identification schemes were approved by the Resolution of the Cabinet of Ministers of Ukraine No. 1276 dated December 05, 2023 “On Approval of the List of Electronic Identification Schemes” and published on the website of the Integrated Electronic Identification
System in accordance with the Paragraph 15 of the Section 1 of the Article 71 of the Law of Ukraine “On Electronic Identification and Electronic Trust Services”.

ANNEX 1

to the Rules and Procedures for the Operation of the
Qualified Trust Service Provider “Diia”

POLICY OF THE CERTIFICATE
OF THE QUALIFIED TRUST SERVICE PROVIDER “DIIA"

Table on content

1. INTRODUCTION

1.1. Overview

This Policy of the Certificate defines the list of all rules applied by the Qualified Trust Service Provider “Diia” (hereinafter referred to as the QTSP “Diia”) in the process of registering users of electronic trust services, in particular, signatories and electronic seals creators (hereinafter referred to as users) formation and maintenance of qualified certificates of public keys (hereinafter referred to as qualified certificates) of the QTSP “Diia” and users, in particular, management of their status (blocking, renewal and cancellation).

Compliance with the requirements defined in this Policy of the Certificate is mandatory for the Head of the specialised subdivision of the QTSP “Diia” and hired employees of the QTSP “Diia” whose position responsibilities are directly related to the registration of users, formation and maintenance of their qualified certificates (hereinafter referred to as the personnel), as well as natural persons and legal entities that, on the basis of agreements conducted with the QTSP “Diia” (State Enterprise “DIIA”), are directly or indirectly related to the registration of users, the formation and/or maintenance of their qualified certificates, in particular, separate registration units of the QTSP “Diia”.

Acknowledgment by users of the requirements defined in this Policy of the Certificate is a mandatory and basis for conducting an Agreement with them on the provision of electronic trust services.

List of all practical actions and procedures used to implement the QTSP “Diia” of this Policy of the Certificate is determined by:

- Regulations of Certification Practices of QTSP “Diia” on Qualified Certificates of Electronic Signature and Seal;
- Regulations of Certification Practices of the QTSP “Diia” on Qualified Certificates of Remote Qualified Electronic Signature “Diia.Signature”.

This Policy of the Certificate complies with the requirements defined in:

- DSTU ETSI EN 319 411-1: “Electronic signatures and infrastructures (ESI). Policy and security requirements for certificate issuing trust services providers. Part 1: General requirements” (hereinafter referred to as DSTU ETSI EN 319 411-1);
- DSTU ETSI EN 319 411-2: “Electronic signatures and infrastructures (ESI). Policy and security requirements for certificate issuing trust services providers. Part 2. Requirements for trust service providers issuing qualified EU certificates” (hereinafter referred to as DSTU ETSI EN 319 411-2);
- DSTU ETSI EN 319 412-2 (ETSI EN 319 412-2, IDT) “Electronic signatures and infrastructures. (ESI). Certificate profiles. Part 2. Profiles of certificates issued to natural persons” (hereinafter referred to as DSTU ETSI EN 319 412-2);
- DSTU ETSI EN 319 401 (ETSI EN 319 401, IDT) “Electronic signatures and infrastructures (ESI). General policy requirements for trust service providers” (hereinafter referred to as DSTU ETSI EN 319 401).

1.2. Name of the document and its identification

Name of the document and its identification is determined in accordance with the provisions of the Clause 5.3 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2.

Full name of the document: Policy of the Certificate of the Qualified Trust Service Provider

“Diia”.

Short name of the document: Policy of the QTSP “Diia” Certificate.

Version: 1.0.

Object identifier (OID) of this Policy of the Certificate: 1.2.804.2.1.1.1.2.

Object identifier (OID) of this Policy of the Certificate is assigned in accordance with ASN.1 according to the contents of the table below.

Table 1. Structure of the Object Identifier (OID) of the Policy of the Certificate

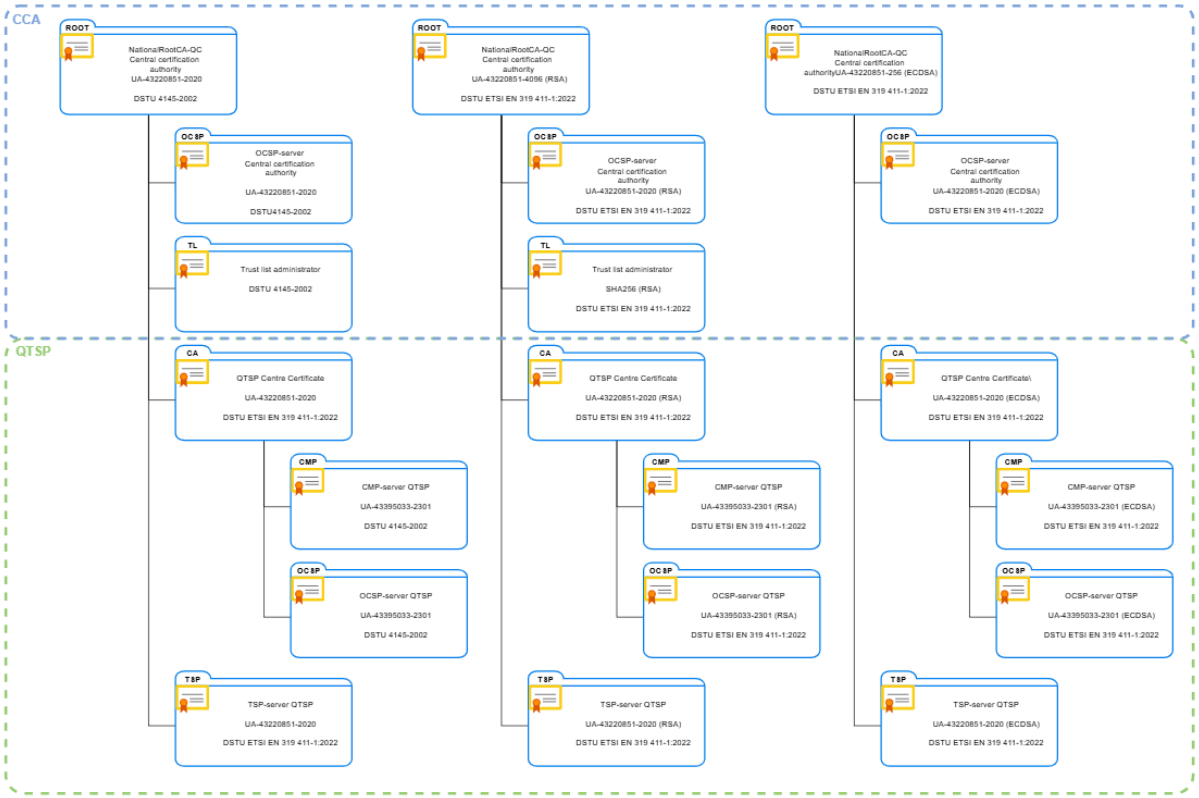
Description	Short name	Indicator (index)
Attribute of the first branch (arc) of the root node of the global object identifiers tree (OID) that is subordinated to the node of the International Organisation for Standardisation (ISO).	iso	1
Attribute of the National Standardisation Authority that is a participant of the International Organisation for Standardisation (ISO)	participant-body	2
Unique numeric code of Ukraine in accordance with DSTU ISO 3166-1:2009 “International Country Names Codes” (ISO 3166-1:2006, IDT), approved by the Order of the State Committee of Ukraine for Technical Regulation and Consumer Policy No. 471 dated December 23, 2009 (hereinafter - ISO 3166-1)	ua	804
Attribute of an infrastructure of public keys	root; security; cryptography; ua-pki	2.1.1.1
Attribute of the Policy of the Certification	cp	2

Qualified certificates formed by the QTSP “Diia” contain the Object Identifier (OID) of this Policy of the Certificate, which is used by entities that trust QTSP “Diia” to define the suitability and reliability of such certificates during user authentication, in particular by verifying and confirming an electronic signature or seal.

1.3. Certificate hierarchy of the Issuer

As shown in Fig. 1, QTSP “Diia” directly trusts the central certification authority.

Figure 1. Certificate hierarchy of the Issuer



1.4. Public key infrastructure participants

Requirements specified in the Clause 5.4 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 apply to the public key infrastructure participants referred to in this Section.

1.4.1. Provider

State Enterprise "DIIA" is a legal entity responsible for the activities of the QTSP "Diia" and the electronic trust services provided by it, in particular, services related to the issuing of qualified certificates, verification and confirmation of the validity of a qualified electronic signature or seal certificate, including for the services provided by registration authorities.

QTSP “Diia” is a Qualified Trust Service Provider that provides qualified electronic trust services in compliance with the requirements of the Law of Ukraine “On Electronic Identification and Electronic Trust Services”, in particular, it registers users, forms and maintains their Qualified Certificates, including managing their status (blocking, renewal and cancellation).

QTSP “Diia” registers users independently and/or through the QTSP “Diia” separate registration units.

Appropriate Regulations of Certification Practices of the Qualified Trust Service Provider "Diia" on the Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures) contain additional information.

1.4.1.1. Rights of the Provider

QTSP "Diia" has the right to:

provide electronic trust services in compliance with the requirements of the legislation in the field of electronic trust services;

receive documents and/or electronic data necessary to identify the person whose identification data will be contained in the qualified certificate;

during the formation and issuance of qualified certificates, verify information about the identities to whom such certificates are issued using information from the information resources of the Unified Information System of the Ministry of Internal Affairs (information contained in the USDR and information on stolen (lost) documents on citizens' appeals), the State Register of Natural Persons-Taxpayers, the State Civil Status Registration Office, USR, as well as information from other public electronic registers in accordance with the Law of Ukraine "On Public Electronic Registers", received in the course of electronic interaction through the integrated electronic identification system (https://id.gov.ua);

receive consultations from the Central Certifying Authority (CCA) and the Control Authority (CA) on issues related to the provision of electronic trust services;

apply to the Conformity Assessment Authority (CAA) to receive documents of conformity;

apply to the CCA with applications for the formation of qualified certificates, their cancellation, blocking or renewal;

independently choose, within each service, which standards they will apply for the provision of qualified electronic trust services from the list of standards determined by the Cabinet of Ministers of Ukraine.

1.4.1.2. Provider's obligations

QTSP "Diia" is obliged to ensure:

protection of users' personal data in accordance with the requirements of the Law of Ukraine "On Personal Data Protection";

functioning of the ICS and the software and hardware complex used to provide electronic trust services, and protection of information processed in them in accordance with the requirements of the legislation in the field of electronic trust services;

creation and functioning of its website;

implementation, maintaining up to date and publication on its website information from the register of valid, blocked and cancelled certificates of public key;

twenty-four-hour access to the register of valid, blocked and cancelled certificates of public key and to information on the status of qualified certificates via public communication networks;

twenty-four-hour acceptance and verification of users' electronic applications for cancellation, blocking and renewal of their qualified certificates;

acceptance and verification of users' paper applications for cancellation, blocking and renewal of their qualified certificates within one business day after receipt of the application and in accordance with the QTSP "Diia" hours of operation;

cancellation, blocking and renewal of qualified certificates in accordance with the requirements of the Law of Ukraine "On Electronic Identification and Electronic Trust Services";

establishing that the public key and the corresponding private key belong to the user during formation of a qualified certificate;

entering user data into the appropriate qualified certificate;

taking organisational and technical measures to manage risks associated with the security of electronic trust services;

informing the CA and, if necessary, the personal data protection authority on violations of confidentiality and/or integrity of information affecting the provision of electronic trust services or relating to users' personal data without unreasonable delay, no later than 24 hours after becoming aware of such a violation;

informing users about violations of confidentiality and/or integrity of information that affect the provision of electronic trust services to them or relate to their personal data without unreasonable delay, but no later than two hours after becoming aware of such a violation;

preventing the use of the user's private key if it has become known that such a private key has been compromised and if the user's private key is stored at the QTSP "Diia" as part of the service of creation, verification and confirmation of an electronic signature or electronic seal;

continuous storage of all issued qualified certificates;

continuous storage of documents and electronic data received in connection with the provision of electronic trust services;

depositing funds to a current account with a special regime of use in a bank (an account with a body that provides treasury services for budgetary funds) to ensure compensation for damage that may be caused to users or third parties as a result of improper performance of the QTSP "Diia" obligations, or civil liability insurance to ensure compensation for such damage in the amount determined by the Law of Ukraine "On Electronic Identification and Electronic Trust Services";

restoration of the amount of the deposit on the current account with a special regime of use in the bank (on the account with the body that provides treasury services for budgetary funds) or the amount of the insurance amount determined by the Law of Ukraine "On Electronic Identification and Electronic Trust Services" within three months in case of changes in the minimum salary or in case of compensation for losses incurred by users or third parties as a result of improper fulfilment of their obligations;

use of exclusively qualified certificates formed by the CCA during the provision of qualified electronic trust services;

hiring employees and, if necessary, carrying out work by subcontractors that have the knowledge, experience and qualifications necessary to provide electronic trust services, and applying administrative and management procedures that comply with the national or international standards;

clear and comprehensive notification to any person who has applied for an electronic trust service of the terms of use of such a service, including any restrictions on its use, before entering into an Agreement for the provision of electronic trust services;

informing the CA and the CCA of the intention to terminate its activity and of changes in the provision of qualified electronic trust services within 48 hours of such changes occurring;

transfer of documented information to the CCA or another provider of documented information in case of termination of activity related to the provision of qualified electronic trust services;

connecting to the software interface of the ICS of the CCA in order to ensure interoperability, research of the current state, prospects for the development of electronic trust services field and perform other powers.

1.4.2. Registration authorities

QTSP "Diia" separate registration units are registration authorities represented by separate subdivisions, non-staff units of the state QTSP "Diia" or legal entities or natural persons who, on the basis of an Agreement with the QTSP "Diia", carry out registration of users.

Employees of the QTSP "Diia" separate registration units, who are responsible for registering users, shall be subject to the same requirements as the Administrators of Registration specified in the Clause 5.3.1.2 of this Policy of the Certificate.

Appropriate Regulations of Certification Practices of the Qualified Trust Service Provider "Diia" on Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures) contain additional information.

1.4.3. Users

Users are signatories and electronic seals creators in respect of whom the QTSP "Diia" carries out their registration (independently or through separate registration units of the QTSP "Diia"), formation and maintenance of their qualified certificates.

According to the Law of Ukraine "On Electronic Identification and Electronic Trust Services":

- signatory – a natural person who creates an electronic signature;
- electronic seal creator – a legal entity or a natural person-entrepreneur who creates an electronic seal.

1.4.3.1. Rights of the users

Users have the right to:

- receive electronic trust services;
- free choice of the provider;
- appeal in court against actions or inactions of the provider and authorities carrying out state regulation in the field of electronic trust services;
- compensation for damage caused to them and protection of their rights and legal interests;
- apply for cancellation, blocking and renewal of their qualified certificate.

1.4.3.2. User's obligations

Users are obliged to:

ensure confidentiality and impossibility of access to the private key by other persons;

immediately notify the provider of any suspicion or fact of compromise of the private key;

provide reliable information necessary to receive electronic trust services;

timely pay for electronic trust services, if such payment is provided for in the Agreement on the provision of qualified electronic trust services concluded with the Provider;

timely provide the Provider with information on changes in the identification data contained in the qualified certificate;

not use the private key in case of its compromise, as well as in case of cancellation or blocking of the qualified certificate.

1.4.4. Entities that trust the Provider

Natural and legal persons, as well as their information and communication systems, are entities that trust the QTSP “Diia” and use user qualified certificates for the purpose of their authentication, in particular by verifying and confirming an electronic signature or seal.

1.4.5. Other participants

Natural and legal persons directly or indirectly related to the formation and/or maintenance of qualified certificates of the QTSP “Diia” and users are other participants.

Other participants include the CCA and the CA, which are the supervisory authorities of the QTSP “Diia”.

CCA, in particular:

- forms QTSP “Diia” qualified certificates using the self-signed certificate of the electronic seal of the CCA;
- approves this Policy of the Certificate and the appropriate Regulations on Certification Practices of the QTSP “Diia”, amendments to them, and sends copies to the CA;
- agrees on the rules of order for synchronising time with the Coordinated Universal Time (UTC) and the QTSP “Diia”;
- approves the Plan for the Termination of the QTSP “Diia” activity.

CA (Administration of the State Service of Special Communications and Information Protection of Ukraine), in particular:

- carries out state control over compliance with the requirements of legislation in the field of electronic trust services;
- cooperates with the CCA and CAA on issues of state control over compliance with the requirements of the legislation;
- cooperates with the personal data protection authorities by promptly informing them of violations of the personal data protection legislation revealed during the CA inspections of the QTSP “Diia”;
- informs public in case of receipt from QTSP “Diia” or based on the results of its verification, information on violations of confidentiality and/or integrity of information that affect the provision of electronic trust services or relate to personal data of users;
- issues prescripts to eliminate violations of the requirements of the legislation in the field of electronic trust services;
- imposes administrative fines for violations of the legislation in the field of electronic trust services;
- analyses conformity documents based on the results of conformity assessment procedures of the QTSP “Diia” within the framework of off-site state supervision (control) measures.

1.5. Use of the certificate

Certificate is used in accordance with the provisions of the Clause 5.5 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2.

In addition, the following special requirements apply:

1.5.1. Permitted use of the certificate

1.5.1.1. Types of qualified certificates

QTSP “Diia” forms qualified certificates of the following types:

- qualified certificate of the electronic signature that links the public key of a qualified electronic signature with a natural person and confirms his or her identification data during authentication, as well as the creation, verification and confirmation of a qualified electronic signature;
- qualified certificate of the remote qualified electronic signature “Diia.Signature”, which links the public key of the remote qualified electronic signature “Diia.Signature” with a natural person and confirms his/her identification data during authentication, as well as the creation, verification and confirmation of a qualified electronic signature;
- qualified certificate of the electronic seal that links the public key of a qualified electronic seal to a legal entity or natural person-entrepreneur and confirms its identification data during authentication, as well as the creation, verification and confirmation of a qualified electronic seal
- qualified certificate of encryption that links the public key of a qualified electronic signature or seal with a natural person, legal entity or natural person-entrepreneur and provides directed encryption during the exchange of information.

Appropriate Regulations of Certification Practices of the Qualified Trust Service Provider “Diia” on Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures) contain additional information.

1.5.1.2. Validity period of qualified certificates

QTSP “Diia” qualified certificates are issued by the CCA with a validity of no more than 5 years.

Validity period of the qualified certificates of the QTSP “Diia” is:

1. CMP – 5 years with parameters that conforms to the following requirements:
   • electronic signature algorithm of DSTU 4145-2002 “Information Technologies. Cryptographic protection of information. Digital signature based on elliptic curves. Formation and verification”, (hereinafter - DSTU 4145-2002), the key size is 256 bits, which conforms to DSTU 4145-2002;
   • ECDSA electronic signature algorithm with a key length of 256 bits, which conforms to DSTU ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);
   • RSA electronic signature algorithm with a key size of 4096 bits, which conforms to the PKCS#1 standard (IETF RFC 3447).
2. QTSP “Diia” private key – 5 years with parameters that conforms to the following requirements:
   • electronic signature algorithm DSTU 4145-2002, key size - 256 bits, which conforms to DSTU 4145-2002;
   • ECDSA electronic signature algorithm with a key length of 256 bits, which conforms to DSTU ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);
   • RSA electronic signature algorithm with a key size of 4096 bits, which conforms to the PKCS#1 standard (IETF RFC 3447).
3. TSP – 5 years;
4. OCSP – 5 years with parameters that conforms to the following requirements:
   • electronic signature algorithm DSTU 4145-2002, key size - 256 bits, which conforms to DSTU 4145-2002;
5. OCSP – 1 year with parameters that conforms to the following requirements:

• ECDSA electronic signature algorithm with a key length of 256 bits, which conforms to DSTU ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);

• RSA electronic signature algorithm with a key size of 4096 bits, which conforms to the PKCS#1 standard (IETF RFC 3447).

Qualified certificates of the user are formed by the QTSP "Diia" with a validity of 1 or 2 years.

Qualified certificates shall contain information on the beginning and end of their validity.

Appropriate Regulations of the Certification Practices of the QTSP "Diia" contain additional information.

1.5.2. Prohibited use of the certificate

Qualified certificate may be used only in accordance with the public key usage ("keyUsage") specified in it.

1.5.3. Use of test certificates

Test certificates are formed by the QTSP "Diia" through integration with the test software and hardware complex created on the CCA official website as part of the field of the electronic trust services monitoring tool (https://czo.gov.ua/tool) in accordance with the Order of the Ministry of Digital Transformation of Ukraine No. 11 dated January 18, 2024 "On Some Issues of Activity and Development in the Fields of Electronic Identification and Electronic Trust Services", registered with the Ministry of Justice of Ukraine under No. 180/41525 on February 05, 2024.

1.6. Management of Policy of the Certificate

1.6.1. Responsibility for the Policy of the Certificate

This Policy of the Certificate is supported by the State Enterprise "DIIA" (hereinafter referred to as SE "DIIA").

SE "DIIA" is a public legal entity registered in accordance with the legislation – a state commercial enterprise based on state ownership and falls within the field of management of the Ministry of Digital Transformation of Ukraine.

QTSP "Diia" Head Office is represented by the functional subdivision of the SE "DIIA", which carries out the organisation of the provision of qualified electronic trust services of the QTSP "Diia" and QTSP "Diia" separate registration units and ensures compliance with the requirements of the legislation to qualified trust service providers (hereinafter referred to as providers).

Agreements for the provision of qualified electronic trust services shall be concluded on behalf of SE "DIIA" or on behalf of a separate registration unit of the SE "DIIA".

Details of SE "DIIA":

- Code according to the Unified State Register of Enterprises and Organisations of Ukraine (USREOU): 43395033.
- Address: 24 Dilova Str., Kyiv, 03150, Ukraine.
- Contact phone number: +38 (067) 258 05 20.
- E-mail address: inbox@diia.gov.ua.

Details of the QTSP "Diia":

- Website addresses: ca.diia.gov.ua.
- Contact phone number: +38 (067) 107 20 41.
- E-mail address: ca@diia.gov.ua; keys@diia.gov.ua; ca@informjust.ua.

This Policy of the Certificate is structured in accordance with RFC 3647 “Internet Public Key Infrastructure X.509 Policy of the Certificate and Certification Practices”, and contains all the necessary information.

This Policy of the Certificate, as well as amendments thereto, shall be signed by the QTSP “Diia” Head of the specialised subdivision, who is responsible for compliance with the rules set forth herein, and approved by the Chief Executive Officer of the SE “DIIA”.

This Policy of the Certificate, as well as amendments thereto, shall be approved by the Ministry of Digital Transformation of Ukraine, which shall send copies thereof to the Administration of the State Service of Special Communications and Information Protection of Ukraine.

1.6.2. Amendments to the Policy of the Certificate

In accordance with the Clause 9.12 of this Policy of the Certificate.

1.7. Definitions of terms and list of abbreviations

1.7.1. Definitions of terms

In this Policy of the Certificate, the terms are used in the meanings set out in the Civil Code of Ukraine, the Laws of Ukraine “On Protection of Information in Information and Communication Systems”, “On Personal Data Protection”, “On the Unified State Demographic Register and Documents Confirming Citizenship of Ukraine, Identifying a Person or His/Her Special Status”, “On Electronic Communications”, “On Electronic Identification and Electronic Trust Services”, Resolution of the Cabinet of Ministers of Ukraine No. 764 dated June 28, 2024 “Some Issues of Compliance with Requirements in the Fields of Electronic Identification and Electronic Trust Services”, other legislative and regulatory acts in the fields of electronic trust services, cryptographic and technical protection of information, electronic communications.

1.7.2. List of abbreviations

SCSR	State Civil Status Register
SRNPT	State Register of Natural Persons - Taxpayers
USDR	Unified State Demographic Register
USR	Unified State Register of Legal Entities, Natural Persons-Entrepreneurs and Community Groups
UIS MIAU	Unified Information System of the Ministry of Internal Affairs of Ukraine
ICS	Information and Communication System
CPI	Cryptographic Protection of Information
CA	Controlling Authority (Protocol of the State Service of Special Communications and Information Protection of Ukraine)
CAA	Conformity Assessment Authority

CCA	Central Certifying Authority (Ministry of Digital Transformation of Ukraine)
CMP	Certificate Management Protocol
OCSP	Online Certificate Status Protocol
TSP	Time Stamp Protocol
ISMS	Information Security Management System in accordance with the provisions of ISO/IEC 27001:2022
TSU	Time-Stamping Unit of QTSP “Diia”, responsible for generating qualified electronic time-stamps.
TST	time-stamp token, electronic data representing a qualified electronic time-stamp.
UTC(UA)	the national realisation of Coordinated Universal Time maintained by the State Primary Standard of Time and Frequency of Ukraine.

2. PUBLICATION AND STORAGE OBLIGATIONS

Requirements specified in the provisions of the Clause 6.1 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures mentioned in this section.

The CP/CPS URLs used in certificates are maintained stable, publicly accessible, and monitored for correctness.

In addition, the following special requirements are applied:

2.1. Repository/website

QTSP “Diia” shall ensure:

creation and functioning of the QTSP “Diia” website;

implementing, maintaining up-to-date and publishing on the QTSP “Diia” website information from the register of valid, blocked and cancelled certificates of public keys;

possibility of twenty-four-hour access to the register of valid, blocked and cancelled certificates of public keys and to information on the status of certificates of public keys via public communication networks.

QTSP “Diia” shall also ensure that users are informed about the conditions for receiving qualified electronic trust services by posting appropriate information on the QTSP “Diia” website.

Through the QTSP “Diia” website (https://ca.diia.gov.ua), the QTSP “Diia” provides free access to:

- information about the QTSP “Diia”;
- data on the inclusion of information about the QTSP “Diia” in the Trust List;
- Policy of the Certificate of the QTSP “Diia”;
- appropriate Regulations of Certification Practices of the QTSP “Diia”;

- General terms and conditions for the provision of qualified electronic trust services to users of the QTSP “Diia”;
- QTSP “Diia” qualified certificates;
- list of qualified electronic trust services provided by the QTSP “Diia”;
- data on the tools of a qualified electronic signature or seal used during the provision of qualified electronic trust services by QTSP “Diia”;
- forms of documents on the basis of which qualified electronic trust services are provided
- information on the QTSP “Diia” separate registration units;
- register of valid, blocked and cancelled certificates of public key;
- information about restrictions during the use of qualified certificates by users;
- data on the rules of order for verifying the validity of a qualified certificate, including the conditions for verifying the status of the certificate;
- list of legislative acts in the field of electronic trust services.

This Policy of the Certificate is available 24 hours a day, 7 days a week in a read-only format on the QTSP “Diia” website.

QTSP “Diia” ensures regular updating of information and publication of qualified certificates, this Policy of the Certificate, appropriate Regulations on Certification Practices, lists of revoked certificates, agreements, legislative acts and other regulatory documents on the QTSP “Diia” website.

Appropriate Regulations of Certification Practices of the Qualified Trust Service Provider “Diia” on the Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures) contain additional information.

2.2. Publication of information

2.2.1. Publication of user certificates

Qualified certificates of users who have consented to their publication shall be published immediately after the formation of such qualified certificates and the fulfilment by users of the terms of the agreement on the provision of qualified electronic trust services.

Consent to the publication of a qualified certificate is provided by the user when submitting an application for the formation of a qualified certificate.

Appropriate Regulations of the Certification Practices of the QTSP “Diia” contain additional information.

2.2.2. Publication of Provider’s certificates

QTSP “Diia” qualified certificates shall be published on the QTSP “Diia” website immediately after they are received from the CCA.

Qualified certificates of the QTSP “Diia” servers are published immediately after they are formed by the QTSP “Diia”.

QTSP “Diia” ensures regular updating of information and publication of qualified certificates, this Policy of the Certificate, appropriate Regulations on Certification Practices of the QTSP “Diia”, CRL, agreements, legislative acts and other regulatory documents on the QTSP “Diia” website: https://ca.diia. gov.ua.

Appropriate Regulations of Certification Practices of the Qualified Trust Service Provider "Diia" on the Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures) contain additional information.

2.2.3. Access to user certificates

User's qualified certificate, after its formation by the QTSP "Diia", shall be available to the user for whom such a certificate was formed.

Access of other persons to user qualified certificates is granted provided that such users agree to their publication.

Appropriate Regulations on Certification Practices of the QTSP "Diia" contain additional information.

2.2.4. Certificate expiry date

User qualified certificates are valid for not more than two years.

Validity of the qualified certificates of the QTSP "Diia" is:

1. CMP – 5 years with parameters that conforms to the following requirements:
   - electronic signature algorithm DSTU 4145-2002, key size - 256 bits, which conforms to DSTU 4145-2002;
   - ECDSA electronic signature algorithm with a key length of 256 bits, which conforms to DSTU ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);
   - RSA electronic signature algorithm with a key size of 4096 bits, which conforms to the PKCS#1 standard (IETF RFC 3447).
2. private key of the QTSP "Diia" – 5 years with parameters that conforms to the following requirements:
   - electronic signature algorithm DSTU 4145-2002, key size - 256 bits, which conforms to DSTU 4145-2002;
   - ECDSA electronic signature algorithm with a key length of 256 bits, which conforms to DSTU ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);
   - RSA electronic signature algorithm with a key size of 4096 bits, which conforms to the PKCS#1 standard (IETF RFC 3447).
3. TSP – 5 years;
4. OCSP – 5 years old with parameters that conforms to the following requirements:
   - electronic signature algorithm DSTU 4145-2002, key size - 256 bits, which complies with DSTU 4145-2002;
5. OCSP 1 year with parameters that comply with the following requirements:
   - ECDSA electronic signature algorithm with a key length of 256 bits, which conforms to DSTU ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);
   - RSA electronic signature algorithm with a key size of 4096 bits, which conforms to the PKCS#1 standard (IETF RFC 3447).

   Appropriate Regulations on Certification Practices of the Qualified Trust Service Provider "Diia" on Qualified Certificates of the Electronic Signature and Seal (Annex 2 to this Rules and Procedures) contain additional information.

2.2.5. Samples for preliminary verification by third-party trust programs

Prior to the official inclusion of QTSP “Diia” in a third-party trust program (e.g., Adobe Approved Trust List, AATL), QTSP “Diia” provides the program operator with sample end-entity certificates (signature/seal) and sample PDF documents signed with Diia certificates to verify compatibility with the program’s requirements. This is a one-time action prior to official listing; thereafter, additional evidence is provided upon the program operator’s request or in connection with changes requiring prior notice under the program rules.

2.3. Time and frequency of publication

Qualified certificates of the QTSP “Diia” servers are published immediately after they are formed by the QTSP “Diia”.

Qualified certificates of the QTSP “Diia” servers are published immediately after they are formed by QTSP “Diia”.

Qualified certificates of users who have given their consent to their publication are published by the QTSP “Diia” immediately after the formation of such certificates.

Appropriate Regulations on Certification Practices of the QTSP “Diia” contain additional information.

2.4. Access control to the repository/website

Repository/website is protected from unauthorised access and changes. QTSP “Diia” provides twenty-four-hour functioning of its own repository/website.

Information Security Service is responsible for the protection of information in the repository/website and database of the QTSP “Diia”, determined in accordance with the decision of the SE “DIIA” Management and documents on the information security management system. Access to the management of the repository/website and database of the QTSP “Diia” is granted to the Administrators of the Information Protection Service of the QTSP “Diia”. Protection of information on the website, in the repository and database of the QTSP “Diia” is carried out in accordance with the Regulations on Confidentiality and Classification of Information at the SE “DIIA”, approved by the Order of the SE “DIIA” No. 20231220-3 dated December 20, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 2 dated December 19, 2023”.

3. IDENTIFICATION AND AUTHENTICATION

Requirements specified in the Clause 6.2 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

3.1. Designations

Qualified certificates shall contain the information specified in the Part two of the Article 23 of the Law of Ukraine “On Electronic Identification and Electronic Trust Services”.

Qualified certificates may contain information on restrictions on the use of a qualified electronic signature or seal.

Qualified certificates may contain other optional additional special attributes defined in the standards for qualified certificates. Following attributes shall not affect the interoperability and recognition of qualified electronic signatures or seals.

Information contained in qualified certificates corresponds to the designations (details, attributes) defined in the standards for certificate profiles in accordance with the Clause 7.1 of this Policy of the Certificate.

Designations used in user qualified certificates are shown in the Table 2.

Table 2: Designations used in user qualified certificates

Names	Designations
Country (C)	Country name in accordance with DSTU ISO 3166-1:2009 "International Country Names Codes" (ISO 3166-1:2006, IDT), approved by the Order of the State Committee of Ukraine on Technical Regulation and Consumer Policy No. 471 dated December 23, 2009
Organization (O)	Name of the legal entity for a qualified certificate of a legal entity or a qualified certificate of a legal entity's representative. This field is not available for qualified certificates of natural persons who do not belong to a legal entity
Organizational Unit (OU)	Name of a subdivision or department in the organisation. This field is not available for qualified certificates of natural persons who do not belong to a legal entity
State or Province (S)	Name of the user's location or place of registration
Locality (L)	Name of the city of residence or place of registration of the user
Common Name (CN)	Full name of the user to whom the qualified certificate belongs
E-Mail Address (E)	E-mail of the user who owns the qualified certificate
Title (T)	Position (for qualified certificates of legal entity representatives, if necessary)
Unique Identifier (UID)	Identifier of the user to whom the qualified certificate belongs: for users who are natural persons, the RNTRC or passport number is used for the UID; for users who are natural persons-entrepreneurs, the RNTRC is used for the UID; for users who are legal entities, the code according to the USREOU is used for UID

Appropriate Regulations of Certification Practices of the Qualified Trust Service Provider “Diia” on Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures) contain additional information.

3.1.1. Types of certificate designations

Types of designations (details, attributes) of a qualified certificate that comply with the information contained in qualified certificates are defined in the standards for certificate profiles in accordance with the Clause 7.1 of this Policy of the Certificate.

3.1.2. Designation (details and attributes) of certificates

Qualified certificate shall have all the necessary designations (details, attributes) defined in the standards for certificate profiles in accordance with the Clause 7.1, Section 7 of this Policy of the Certificate.

3.1.3. Anonymity or use of pseudonyms

Procedure for using pseudonyms is carried out in accordance with the Rules of order for the use of pseudonyms by natural persons who are users of electronic identification services or electronic trust services, approved by the Resolution of the Cabinet of Ministers of Ukraine No. 764 dated June 28, 2024 “Some Issues of Compliance with Requirements in the Fields of Electronic Identification and Electronic Trust Services” and DSTU ETSI EN 319 412-2.

3.1.4. Rules for interpreting different forms of certificate designations

International letters shall be encoded according to UTF-8.

3.1.5. Uniqueness of certificate designations

QTSP “Diia” shall ensure that certificates with the same data specified in the “Common Name” and “SerialNumber” fields are not issued to different users.

3.1.6. Acknowledgment, authentication and the role of trademarks

Not applicable.

3.2. Initial identification verification

Requirements specified in the Clause 6.2.2 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

In addition, the following special requirements apply:

3.2.1. Method of confirming a private key possession

Confirmation of the user’s possession of a private key, the appropriate public key for which is provided to form a qualified certificate, is provided in one of the following ways:

- visual and technical control of recording and transferring to the QTSP “Diia” of a request for the formation of a qualified certificate by the user personally during the generation of a key pair immediately after the user’s identification, provided that the user is present in person;
- technical control of recording and transferring to the QTSP “Diia” a request for the formation of a qualified certificate personally by the user during the generation of a key pair immediately after the identification of the applicant and obtaining identification data using – the identification mechanisms specified in the Subclause 3.2.2 of this Policy of the Certificate, as well as the appropriate Regulations of the Certification Practices of the QTSP “Diia”.

In all cases, using the tools of a qualified electronic signature or the seal of the QTSP "Diia", the advanced electronic signature created using the user's private key in the request for the formation of a qualified certificate is verified using the public key contained in this request.

Confirmation of the user's possession of the private key is carried out without disclosing the private key.

3.2.2. Person identification

Formation and issuance of a qualified certificate without identification of the person/entity whose/which identification data will be contained in the qualified certificate are not allowed.

Identification of a person/entity who/that has applied for the service of formation of a qualified certificate shall be carried out in one of the following ways:

1) in the personal presence of a natural person, a natural person-entrepreneur or an authorised representative of a legal entity - based on the results of verification of information (data) about a person obtained in accordance with the order established by the legislation from the USDR, on the basis of a passport of a citizen of Ukraine or other documents issued in accordance with the legislation on the USDR and on identity documents confirming the citizenship of Ukraine or special status of a person (passport of a citizen of Ukraine, passport of a citizen of Ukraine for travelling abroad, permanent/temporary residence permit);

2) remotely (without the person's personal presence), with the simultaneous use of an electronic identification tool with a high or medium level of trust previously issued to a natural person, a natural person-entrepreneur or authorised representative of a legal entity in person, and multi-factor authentication;

3) according to the identification data of the person/entity contained in the qualified certificate previously formed and issued in accordance with the Subclause 1 or 2 of this Clause, provided that such certificate is valid;

4) using other methods of identification specified by the law, the reliability of which is equivalent to personal presence and confirmed by the CAA.

If foreigners and stateless persons do not have documents issued in accordance with the legislation on the USDR and on identity documents confirming the citizenship of Ukraine or special status of a person, their identification in the manner specified in the Subclause 1 of the Clause 3.2.2 of this Policy of the Certificate is carried out on the basis of a duly legalised passport document of a foreigner or a document certifying a stateless person.

During verification of the civil legal capacity and legal capability of a legal entity or natural person-entrepreneur (for the purpose of formation a qualified certificate of electronic seal), the QTSP "Diia" is liable to use information about the legal entity or natural person-entrepreneur contained in the USR or in a commercial, bank or court register maintained by the country of residence of the foreign legal entity, as well as to make sure that the scope of civil legal capacity and legal capability of the legal entity or natural person-entrepreneur is sufficient to form and issue a qualified certificate.

Verification of the civil legal capacity and legal capability of international organisations, information about which is not entered in the USR or a commercial, bank or court register maintained by a foreign state, at the location of the headquarters of an international organisation is carried out using information from an international agreement or other official document on the basis of which the international organisation was established and/or operates.

In cases of transfer of the service of user qualified certificates and documented information, on the basis of which the mentioned certificates were formed, from the provider, that terminates its

activity, to the QTSP “Diia”, the procedure for identifying these users shall be carried out in one of the ways specified in this Clause and in accordance with the Law of Ukraine “On Electronic Identification and Electronic Trust Services”.

Appropriate Regulations on Certification Practices of the QTSP “Diia” contain additional information.

3.2.3. Unverified user information

Unverified user information is not allowed.

Appropriate Regulations on Certification Practices of the QTSP “Diia” contain additional information.

3.2.4. Confirmation of powers

Authorised representative of a legal entity or natural person-entrepreneur signs the documents required to form and issue a qualified certificate to an employee of a legal entity or natural person-entrepreneur. QTSP “Diia” during the formation and issuance of a qualified certificate to an employee of a legal entity or natural person-entrepreneur carries out an identification of the employee, as well as the identification of the authorised representative of the legal entity or natural person-entrepreneur in accordance with the requirements established in the Subclause 3.2.2 of this Policy of the Certificate and verifies the scope of his/her powers by the document defining the powers of the authorised representative of the legal entity or natural person-entrepreneur, or using the information contained in the USR or in the commercial, bank or court register maintained by the country of residence of the foreign legal entity.

Authorised representative of a legal entity is the Head of the legal entity listed in the USR, or an employee (Head of a separate subdivision (branch) of the legal entity) authorised to enter into transactions with third parties, as specified in the Order, Power of Attorney, etc.

Before forming a qualified certificate of a representative of a legal entity and a self-employed person (attorney, notary, private enforcement officer, insolvency officer, etc.), the user’s powers are also verified by verifying documents certifying his/her powers or affiliation with a legal entity, the right to carry out activity in a certain area (licence, certificate, appointment order, documents of authorisation, etc.) or by verifying information in the relevant state information systems (registers, databases, etc.).

Appropriate Regulations on Certification Practices of the QTSP “Diia” contain additional information.

3.3. Identification and authentication upon application for repeated formation of the qualified certificates of public key

Requirements specified in the Clause 6.2.3 of ETSI EN 319 411-1 and ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

3.3.1. Identification and authentication of the user on the basis of the application for certificate formation, provided that the previous certificate is valid

To form a new qualified certificate of a user who has a valid qualified certificate formed by the QTSP “Diia”, such user shall undergo an authentication procedure based on an application for the formation of a qualified certificate submitted electronically to QTSP “Diia”, provided that the identification data entered in the previous qualified certificate remains unchanged from the moment of formation of the qualified certificate until the qualified electronic signature is created on the application for the formation of the qualified certificate.

Verification of the identification data of the user who applies for the formation of a qualified certificate in electronic form, as well as the legality of such an application, is carried out by authenticating the user and confirming his or her powers based on the results of verification of the qualified electronic signature on the application and the establishment of a validity, at the time of the submission of the application, of the certificate of key, containing the person's identification data.

Appropriate Regulations on Certification Practices of the Qualified Trust Service Provider "Diia" on the Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures) contain additional information.

3.3.2. Identification and authentication of the user to receive repeated formation of a qualified certificate of public key in case of cancellation of the certificate

If the user qualified certificate is cancelled, in order to form a new qualified certificate in the QTSP "Diia", the user shall pass identification and authentication in accordance with the conditions for initial user identification and authentication.

3.4. User identification and authentication based on applications on certificate blocking or revocation

Requirements specified in the Clause 6.2.4 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and activity referred to in this Section.

Verification of the identification data of the user who applies for blocking or cancelling a qualified certificate in electronic form, as well as the legality of such a request, is carried out by authenticating and identifying the user using:

- electronic identification tools belonging to the electronic identification scheme of the QTSP "Diia" "DIIA.PKI" and confirmation of the user's powers based on the results of verification of the qualified electronic signature on the application and the establishment of the validity of the user qualified certificate containing the person's identification data at the time of application submission;
- electronic identification tools belonging to the electronic identification scheme of the QTSP "Diia" "DIIA.PKI.Remote" and confirmation of the user powers based on the results of verification of the qualified electronic signature on the application and the establishment of the validity of the user qualified certificate containing the person's identification data at the time of application submission.

Identification schemes of the QTSP "Diia" were approved by the Resolution of the Cabinet of Ministers of Ukraine No. 1276 dated December 05, 2023. "On Approval of the List of Electronic Identification Schemes" and published on the Integrated Electronic Identification System website in accordance with the Paragraph 15 of the Section 1 of the Article 7^1 of the Law of Ukraine "On Electronic Identification and Electronic Trust Services".

To block or cancel a qualified certificate of a user who has a valid qualified certificate formed by the QTSP "Diia", such user shall undergo an authentication procedure based on an application for blocking or cancelling a qualified certificate submitted electronically to the QTSP "Diia".

Clause 4.9 of this Policy of the Certificate and the appropriate Regulations on Certification Practices of the QTSP "Diia" contains additional information on blocking and cancelling a user's qualified certificate.

4. REQUIREMENTS FOR THE CERTIFICATE LIFECYCLE

Requirements specified in the Clause 6.3 of ETSI EN 319 411-1 and ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

4.1. Request for formation of a certificate

List of entities authorised to submit request for the formation of a qualified certificate includes users who have passed the identification and authentication procedures.

Request for the formation of a qualified certificate is accepted for processing after acceptance and registration of an application for the formation of a qualified certificate, identification and authentication of the user's identity and confirmation of the user's possession of a private key, the corresponding public key of which is provided for the formation of a qualified certificate.

Clause 4.1 of the appropriate Regulations on Certification Practices of the Qualified Trust Service Provider "Diia" on Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures) contain additional information on the user registration process.

4.2. Processing a request for formation of a certificate

Requirements specified in the Clause 6.3.2 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

Processing a request for formation of the qualified certificate is carried out by the software tools of the QTSP "Diia" ICS with the participation of the Registration Administrator, an employee of the QTSP "Diia" separate registration unit who is responsible for user registration and who performs the functions of the Registration Administrator, or automatically, provided the continuity of processes of generating key pairs, forming requests, transmitting them for processing via secure communication channels that ensure the confidentiality and integrity of data. Automatic processing of requests does not exclude the processes of identifying the user's identity and confirming the user's possession of a private key, the corresponding public key of which is provided to generate a qualified certificate.

During the processing of a request for a qualified certificate formation, the uniqueness of the public key in the register of valid, blocked and cancelled certificates of public key is verified by the tools of the QTSP "Diia" ICS and the uniqueness of the serial number of the user's qualified certificate is ensured.

Processing time of a request for a qualified certificate formation submitted together with a registration application is not more than one hour.

4.3. Formation of a certificate

Provision of the formed qualified certificate to the user is carried out in one of the following ways:

- by sending a file with the formed qualified certificate to the e-mail address specified by the user in the application for the formation of a qualified certificate;
- by recording a file with the formed qualified certificate to the information media provided by the user;
- by publishing a qualified certificate on the QTSP "Diia" website.

4.4. Acceptance of a certificate

Requirements specified in the Clause 6.3.4 of ETSI EN 319 411-1 and ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

User qualified certificate is published on the QTSP “Diia” website at https://ca.diia.gov.ua/certificates-search immediately after the certificate request is processed.

User shall verify his/her identification data entered by the QTSP “Diia” into the qualified certificate within one day. QTSP “Diia” shall provide appropriate consultations on how to conduct such verification. User shall use the private key to create a qualified electronic signature only after verification. Use of the private key by the user is the fact of his/her recognition of the qualified certificate corresponding to his/her public key.

User verifies the operability of his/her private key and identification data entered in the qualified certificate by reading the private key on the QTSP “Diia” website in the “Find certificate” section or using specialised software available on the QTSP “Diia” website https://ca.diia.gov.ua/certificates-search.

If the user finds a discrepancy between the identification data entered by the QTSP “Diia” and the qualified certificate within one day, the user shall contact the QTSP “Diia” to cancel the qualified certificate and form a new certificate free of charge. If the user applies after 24 hours, the certificate is formed on a paid basis.

In case of discrepancies between the identification data entered by the QTSP “Diia” in the qualified certificate and found by the QTSP “Diia” before the formed qualified certificate is provided to the user, an official of the QTSP “Diia” shall provide the repeated formation of the qualified certificate using a previously certified public key and in compliance with the requirements for preventing the validity of the private key and the corresponding public key from exceeding two years. The official who has provided repeated formation of the qualified certificate shall draw up an act stating the date and time of cancellation of the qualified certificate, user identification data contained in the qualified certificate and the inconsistent user identification data specified in the application for the qualified certificate formation. The Act shall be signed by an official of the QTSP “Diia” who conducted the repeated formation of the qualified certificate and attached to the documents (duly certified copies of documents) used during the identification and registration of the user.

4.5. Using a key pair and a certificate

Requirements specified in the Clause 6.3.5 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

QTSP "Diia" provides public HTTP access without authentication to the current Certificate Policy and Certification Practice Statements, as well as to archived versions indicating version numbers and effective/retirement dates. Stable links to these documents are maintained in the Repository.”

4.5.1. Use of a private key and a certificate by the user

User is obliged to comply with the following rules when using a private key:

ensure confidentiality and impossibility of access to the private key by other persons;

immediately notify the QTSP “Diia” of any suspicion or fact of compromise of the private key;

not to use the private key in case of its compromise, as well as in case of cancellation or blocking of the appropriate qualified certificate;

be personally responsible for protecting the private key password.

User is obliged to use a qualified certificate in accordance with the public key purpose (“keyUsage”) and restrictions on its use specified therein.

When using a private key and a qualified certificate, the user shall comply with the requirements of the legislation in the field of electronic trust services, as well as the provisions of:

- this Policy of the Certificate;
- appropriate Regulations of Certification Practices of QTSP “Diia”;
- General terms and conditions for the provision of qualified electronic trust services to users of the QTSP “Diia”;
- Agreement concluded with the QTSP “Diia” (SE “DIIA”) on provision of qualified electronic trust services.

4.5.2. Use of a public key and a certificate by entities that trust the Provider

User qualified certificates formed by the QTSP “Diia” can be used by any entities that trust the QTSP “Diia” for the purpose of their authentication, in particular by verifying and confirming an electronic signature or seal.

Before accepting a user qualified electronic signature or seal, the entity that trusts the QTSP “Diia” shall verify the following information:

- status of the user qualified certificate, the scope of use of the user qualified certificate, restrictions on use and information about the user qualified certificate.
- compliance of the private key of a qualified electronic signature or seal with the public key specified in the user qualified certificate.

Entity that trusts the QTSP “Diia” shall perform the following verifications:

- verify the user qualified certificate status at the time of affixing a qualified electronic signature or seal using the OCSP server of the QTSP “Diia” (qualified certificate status verification server), the scope of use (KeyUsage field in the certificate), usage restrictions and information about the qualified certificate to ensure that the user qualified certificate is currently valid;
- verify the QTSP “Diia” qualified certificate status when affixing a qualified electronic signature or seal by the user.

Qualified electronic signature or seal shall be deemed valid when the verification results in the above clauses are successfully completed and are valid simultaneously.

Entity that trusts the QTSP “Diia” is responsible for not following the above verification procedure or performing the verification knowing that the qualified certificate is not valid at the time of verification.

When using a user public key and qualified certificate, entities that trust the QTSP “Diia” shall comply with the requirements of the legislation in the field of electronic trust services, as well as the provisions of:

- this Policy of the Certificate;
- appropriate Regulations of Certification Practices of QTSP “Diia”.

4.6. Renewal of a certificate

Requirements specified in the Clause 6.3.6 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

QTSP “Diia” is obliged to ensure, in particular:

- twenty-four-hour acceptance and verification of user electronic applications for the renewal of their qualified certificates that were blocked by the QTSP “Diia”;
- acceptance and verification of user paper applications for renewal of their qualified certificates that have been blocked by the QTSP “Diia” within one business day after receipt of the application and in accordance with the QTSP “Diia” operating hours;

- renewal of qualified certificates that were blocked by the QTSP “Diia” in accordance with the requirements of the Law of Ukraine “On Electronic Identification and Electronic Trust Services”.

Informing users about the expiration of their qualified certificate is carried out by the QTSP “Diia” 7 days before the expiration of the qualified certificate by sending SMS messages to the user’s phone number specified in the registration application.

Appropriate Regulations of Certification Practices of the Qualified Trust Service Provider “Diia” on the Qualified Certificates of Electronic Signature and Seal (Annex 2 to these Rules and Procedures) contain additional information.

4.7. Repeated formation of the certificate

Requirements specified in the Clause 6.3.7 of ETSI EN 319 411-1 and ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

QTSP “Diia” shall form a user qualified certificate, including on the basis of a valid qualified certificate formed by the QTSP “Diia”, containing the user’s identification data received as a result of his/her identification in one of the following ways:

- in the personal presence of a natural person, a natural person-entrepreneur or an authorised representative of a legal entity - based on the results of verification of information (data) about a person received in accordance with the order established by the USDR legislation, on the basis of a passport of a citizen of Ukraine or other documents issued in accordance with the legislation on the USDR and on identity documents confirming the citizenship of Ukraine or special status of a person;

- remotely (without the person’s personal presence), with the simultaneous use of an electronic identification tool with a high or medium level of trust previously issued to a natural person, a natural person-entrepreneur or an authorised representative of a legal entity in person, and multi-factor authentication.

User can also form a new qualified certificate after the expiration date and in case of urgent need (compromise of the private key or password to it, loss of the private key, change of information contained in the user qualified certificate) by contacting the QTSP “Diia” service point or the QTSP “Diia” separate registration unit.

Appropriate Regulations on Certification Practices of the Qualified Trust Service Provider “Diia” on the Qualified Certificates of Electronic Signature and Seal (Annex 2 to these Rules and Procedures) contain additional information.

4.8. Change of the certificate

Changes to the qualified certificate are not allowed.

Appropriate Regulations on Certification Practices of the Qualified Trust Service Provider “Diia” on the Qualified Certificates of Electronic Signature and Seal (Annex 2 to these Rules and Procedures) contain additional information.

4.9. Cancellation and blocking of the certificate

Requirements specified in the Clause 6.3.9 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

QTSP “Diia” is obliged to ensure, in particular:

- twenty-four-hour acceptance and verification of user electronic applications for cancellation and blocking of their qualified certificates formed by the QTSP “Diia”;

- acceptance and verification of user applications in paper form for cancellation and blocking of their qualified certificates formed by the QTSP “Diia” within one business day after receipt of the application and in accordance with the QTSP “Diia” operating hours;

- cancellation and blocking of qualified certificates formed by the QTSP “Diia” in accordance with the requirements of the Law of Ukraine “On Electronic Identification and Electronic Trust Services”.

User has the right to cancel a qualified certificate at his/her own request by passing electronic identification using electronic identification tools that have a high and medium level of trust in accordance with the Clause 3.4 of this Policy.

User has the right to block the qualified certificate at his/her own request. Blocking of a qualified certificate may be carried out by the QTSP “Diia” upon a paper application for changing the status of a qualified certificate or after identifying the user by the key phrase included in the registration application. Blocking a qualified certificate means the temporary suspension of the validity of a qualified certificate for a period of up to 30 calendar days.

After blocking a qualified certificate, user may renew the qualified certificate within 30 calendar days. A blocked qualified certificate will be automatically cancelled by the QTSP “Diia” if the user does not renew its validity within the specified period.

Qualified certificate expires from the moment its status is changed to “cancelled”.

Cancelled qualified certificate cannot be renewed.

Qualified certificate is considered blocked from the moment its status changes to “blocked”.

Qualified certificate whose status has been changed to “blocked” is invalid and not used during the blocking period.

Qualified certificates of users who have agreed to their publication are published immediately after the formation of such certificates.

QTSP “Diia” forms lists of revoked certificates (CRLs) in the format of full and partial lists that meet the following requirements:

- each list of revoked certificates shall indicate the expiry date of its validity before a new list is issued;
- a new list of revoked certificates may be published before the expiry date of the certificate before the next list is published;
- a qualified electronic signature or seal of the QTSP “Diia” shall be affixed to the list of revoked certificates.

Lists of revoked certificates are published automatically.

Time of status change of qualified certificates is synchronised with the Coordinated Universal Time (UTC) with an accuracy of one second.

Links to lists of revoked certificates are included in the user qualified certificates.

Full list of revoked certificates is formed and published 1 (One) time per week and contains information on all revoked certificates formed by the QTSP “Diia”.

Partial list of revoked certificates is formed and published every 2 (Two) hours and contains information on all revoked qualified certificates whose status has been changed in the interval between the time of issuance of the last full list of revoked certificates and the time of formation of the current partial list of revoked certificates.

Appropriate Regulations of Certification Practices of the QTSP “Diia” contain additional information.

QTSP "Diia" changes the status of a qualified certificate without undue delay and, in any case, no later than two hours in the cases defined by the laws of Ukraine.

Revocation applies, inter alia, where:

(i) a request is submitted by the user;

(ii) the fact of compromise of the subscriber’s private key is established;

(iii) the subscriber’s identification data in the certificate have changed; and other grounds provided by law.

Blocking applies, inter alia, where:

(i) a request is submitted by the user;

(ii) there is a notification of suspected compromise of the subscriber’s private key;

(iii) other grounds provided by law.

A revoked certificate shall not be reinstated; a blocked certificate may be reinstated in the cases set by law. The operational procedure for revocation/blocking/renewal is defined in QTSP "Diia’s" Rules (Regulations).

The Registration Administrator and/or ICS performs revocation/blocking or renewal without undue delay and no later than two hours after the grounds are recorded, in accordance with the Law and this Certificate Policy: records the request/event, verifies the requester’s authorization and identity (where applicable), initiates the operation in the ICS, ensures status publication, creates operational logs (event time, cause, certificate identifier), and ensures immediate availability of the status change to relying parties.

For the "Diia.Signature" service, the registration administrator and/or the ICS ensure status change without undue delay and no later than two hours in the cases defined by the Law and the Certificate Policy, with automatic status publication and event logs with timestamps.

4.10. Certificate status services

QTSP “Diia” ensures the availability of information on the certificate status in real time using the OCSP server and the lists of revoked certificates (CRL) published on the QTSP “Diia” website.

The certificate status services operate so as to ensure immediate availability of status changes (revocation/blocking/renewal) upon the decision in accordance with this Policy and QTSP "Diia’s" Rules.”

QTSP "Diia" provides certificate status information via OCSP and CRL with public HTTP access and no authentication. Access identifiers to the status services are embedded in certificates: Authority Information Access (OCSP) and CRL Distribution Points (CRL). OCSP responses return correct GOOD/REVOKED/UNKNOWN values, are signed by an authorized responder, and include correct timestamps (thisUpdate, nextUpdate/producedAt). For serial numbers not issued by QTSP "Diia", the response is UNKNOWN. Status changes shall be immediately available after revocation/blocking/renewal operations.

AIA (OCSP) and CDP (CRL) references embedded in certificates shall be HTTP-only, publicly accessible and unauthenticated.

4.11. Certificate expiry date

The date and time of the start and end of the user certificate validity period is indicated in the certificate with an accuracy of one second.

After the date and time of expiry of the user certificate specified in it occurs, such certificate shall be deemed cancelled.

4.12. Depositing and returning keys

Not applicable.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROL

Requirements specified in the Clauses 5, 6.3 and 7.3 of DSTU ETSI EN 319 401 are applied to the objects, processes and measures referred to in this Section.

5.1. Physical security control

Physical security control is carried out in accordance with the provisions of the Clause 6.4.2 of DSTU ETSI EN 319 411-1:2022

In addition, the following special requirements are applied:

5.1.1. Requirements for the Provider's premises

QTSP "Diia" premises shall be divided into functional zones according to the security levels of the premises established by the QTSP "Diia".

QTSP "Diia" premises are divided into special and service premises according to security levels. For each security level of premises, the minimum required set of security mechanisms is determined, in particular: access control, intrusion detection, fire alarm and fire extinguishing, alternative and standby power supply, etc.

The specified premises security mechanisms may be changed based on the assessed risks and the selected neutralisation mechanisms corresponding to these risks.

Components critical to the safe operation of the QTSP "Diia" shall be located in a secure and safe environment with physical protection against intrusion, access control through the security perimeter and alarms to detect intrusion.

Access to the premises of the QTSP "Diia" is provided in accordance with the ISMS documents Regulations on Physical Security at the SE "DIIA" DIIA/13 - ISMS - Ph - SOP/1 - Physical and environmental security, approved by the Order of the SE "DIIA" No. 20231220-3 dated December 20, 2023 "On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 2 dated December 19, 2023".

5.1.2. Physical access

Access to the special and service premises of the QTSP "Diia" (safe zone) is provided with the use of organisational and technical control measures (physical and logical control) in accordance with ISMS documents, namely: Regulations on Physical Security at the SE "DIIA" DIIA/13 - ISMS - Ph - SOP/1 - Physical and environmental security, approved by the Order of the SE "DIIA" No. 20231220-3 dated December 20, 2023 "On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 2 dated December 19, 2023".

Right of access to special premises of the data processing centre (DPC) shall be granted only to the Head of the specialised subdivision of the QTSP "Diia" and the QTSP "Diia" personnel in accordance with their official duties, who are included in the appropriate list of authorised QTSP "Diia" employees having access to special premises of the QTSP "Diia".

Access of unauthorised employees to special premises is carried out:

1) in routine situations (scheduled inspections, repair and restoration works, etc.) - by decision of the CEO of the SE "DIIA" or a person acting in his/her capacity, based on consideration of

the memo submitted by the employee who is responsible for the duties of the Head of the Information Security Service of the ICS of the SE “DIIA”, and with further inclusion of such employees in the Application for Access;

2) in emergency situations (fire, flooding, natural disaster, accidents, etc.) - without the permission of the CEO of the SE “DIIA” or a person performing his/her duties, with the obligatory entry of the reasons for emergency access to the facility in the appropriate section of the Form “Registration of Emergency Events and Failures of the QTSP “Diia” ICS”.

At the entrance to the DPC, a security officer identifies authorised employees of the QTSP “Diia” by their identity documents (passport of a citizen of Ukraine, driver’s licence).

Access to a special premises is registered in an electronic or paper access log book located in the DPC.

Server cabinet where the QTSP “Diia” ICS equipment is located is locked and sealed by the responsible employees of the QTSP “Diia”.

Territory of the DPC and the server premises where the QTSP “Diia” ICS equipment is located are equipped with a video surveillance system that operates around the clock, video surveillance logs are stored in the DPC.

Equipment shall be brought in/removed from the special premises on the basis of an equipment bringing in/removing act signed by the responsible employees.

QTSP “Diia” ICS consists of two identical, independent sites (main and reserve) located remotely from each other at a distance of more than 100 km.

5.2. Procedural control

Procedural control is carried out in accordance with the requirements specified in the Clause 6.4.3 of DSTU ETSI EN 319 401.

5.3. Personnel control

Personnel control is carried out in accordance with the requirements specified in the Clause 6.4.4 of DSTU ETSI EN 319 401, as well as in accordance with the internal instruction of the SE “DIIA”, which is part of the ISMS documentation, in particular, the Procedure for conducting a preliminary reputational verification, in particular, verification of the reliability of a candidate for vacant positions of the SE “DIIA” DIIA/13 - ISMS - Ppl - PL/1 - SOP/1 - Screening, approved by the Order of the SE “DIIA” No. 20231220-3 dated December 20, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 2 dated
December 19, 2023”.

5.3.1. Entrusted personnel roles

QTSP “Diia” personnel are:

- Head of the QTSP “Diia” specialised subdivision;
- Registration Administrator;
- Certification Administrator;
- Security Administrator;
- System Auditor;
- System Administrator.

5.3.1.1. Head

Within the scope of his/her duties, the Head of the QTSP “Diia” specialised subdivision is responsible for organising and controlling the processes aimed to ensure functioning, development of the QTSP “Diia” and protection of information in the QTSP “Diia” ICS, in particular:

- control over the implementation of regulatory procedures for the operation and technical maintenance of the QTSP “Diia” ICS;
- control over the implementation and operation of the QTSP “Diia” ICS;
- control over the operability of the system-wide and special software of the QTSP “Diia” ICS;
- ensuring the updating databases created and processed in the QTSP “Diia” ICS;
- review and assessment of technical decisions on the modernisation of QTSP “Diia” ICS;
- development and agreement of technical tasks, design and exploitation documentation of the QTSP “Diia” ICS;
- control over construction, installation and commissioning works;
- conducting preliminary tests, experimental exploitation, and commissioning the QTSP “Diia” ICS.

Head of the QTSP “Diia” specialised subdivision directly participates in and controls the process of generating and backup of QTSP “Diia” keys with the rights and responsibilities of a Certification Administrator.

Head of the QTSP “Diia” specialised subdivision represents the QTSP “Diia” in cases stipulated by the Policy of the Certificate and the Regulations of Certification Practices of the CCA.

5.3.1.2. Registration Administrator

Registration Administrator is responsible for verification of documents provided by users, their applications for formation, blocking, renewal and cancellation of qualified certificates.

The main responsibilities of the Registration Administrator are:

- identification and authentication of users;
- verification of applications for the formation, blocking, renewal and cancellation of qualified certificates;
- establishing that the public key and its corresponding private key belong to the user;
- maintaining records of users.

Additional responsibilities of the Registration Administrator include:

- providing assistance during generation of user key pair;
- processing requests for generation and change of the status of user key certificates;
- providing consultation on the terms and rules of order for obtaining qualified electronic trust services;
- maintaining the QTSP “Diia” archive.

The same requirements as for registration administrators shall apply to employees of the QTSP “Diia” separate registration units who are responsible for registering users.

5.3.1.3. Certification Administrator

Certification Administrator is responsible for formation of qualified certificates, maintaining an electronic register of valid, blocked and cancelled certificates of public key, storing and using private keys of the QTSP “Diia”, as well as creating their backup copies.

The main responsibilities of a Certification Administrator are:

- participation in the generation of key pairs of the QTSP “Diia” and the creation of backup copies of QTSP “Diia” private keys;
- storage of the QTSP “Diia” private keys and their backup copies;
- ensuring the use of QTSP “Diia” private keys during the formation and maintenance of qualified certificates of the QTSP “Diia” and users;
- verification of applications for the formation of qualified certificates of the QTSP “Diia” for compliance with the requirements of this Policy of Certification and the appropriate Regulations of Certification Practices;
- participation in the destruction of the QTSP “Diia” private keys;
- ensuring the maintenance, archiving and renewal of databases of user qualified certificates;
- ensuring publication of user qualified certificates and lists of revoked certificates on the QTSP “Diia” website;
- creating backup copies of user qualified certificates;
- storage of user qualified certificates of public keys, their backup copies, lists of revoked certificates and other important resources of the QTSP “Diia” ICS.

Additional responsibilities of the Certification Administrator are to maintain the Certification Administrator’s log books provided for by the internal documentation of the QTSP “Diia” ICS.

5.3.1.4. Security Administrator

Security Administrator is responsible for the proper functioning of the QTSP “Diia” ICS.

The main responsibilities of the Security Administrator are:

- participation in the generation of the QTSP “Diia” key pairs and the creation of backup copies of the QTSP “Diia” key pairs;
- control over the formation, maintenance, creation and verification of backup copies of the QTSP “Diia” qualified certificates, users and lists of revoked certificates;
- control over the storage of the QTSP “Diia” private keys and their backup copies, private keys of Administrators;
- participation in destruction of QTSP “Diia” private keys, control over the correct and timely destruction of their private keys by Administrators;
- organisation of differentiation of access to the QTSP “Diia” ICS resources;
- ensuring monitoring of the functioning of the QTSP “Diia” ICS (registration of events in the QTSP “Diia” ICS, monitoring of events, etc.);
- ensuring the organisation and implementation of measures for the modernisation, testing, and prompt restoration of the functioning of the QTSP “Diia” ICS after failures, disruptions;
- ensuring access to the premises of the QTSP “Diia”, where the QTSP “Diia” ICS is located;
- maintaining log books of the Security Administrator, as defined by the documentation on the QTSP “Diia” ICS or reporting provided by the ISMS
- conducting audits on compliance with the provisions of the internal organisational and administrative documentation of the QTSP “Diia” and the ISMS;
- control over compliance by the QTSP “Diia” personnel with the provisions of the QTSP “Diia” internal organisational and administrative documentation and ISMS documentation;
- control over the maintenance of the databases of the QTSP “Diia”.

Security Administrator is responsible for conducting audits of compliance by the QTSP “Diia” personnel and the QTSP “Diia” separate registration units with the provisions of the internal organisational and administrative documentation of the QTSP “Diia” and the ISMS documentation approved by the Orders of the SE “DIIA” No. 20231012-2 dated October 12, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 1 dated
October 09, 2023”, No. 20231220-3 dated December 20, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 2 dated October 09, 2023”.

It is prohibited to combine the duties of the Security Administrator with other duties directly related to the provision of qualified electronic trust services.

5.3.1.5. System Administrator

System Administrator is responsible for the functioning of the technical tools of the QTSP “Diia” ICS.

The main responsibilities of a System Administrator are:

- organisation of exploitation and technical maintenance of the QTSP “Diia” ICS and administration of its technical tools;
- ensuring the functioning of the QTSP “Diia” website;
- participation in the implementation and ensuring functioning of the QTSP “Diia” ICS and ISMS;
- maintaining audit log books of events recorded by the technical tools of the QTSP “Diia” ICS;
- installation, configuration and maintenance of the system-wide and special software of the QTSP “Diia” ICS;
- installation and adjustment of the staff subsystem of backup of the QTSP “Diia” database;
- ensuring that the databases created and processed in the QTSP “Diia” ICS are updated in case of failures.

5.3.1.6. System Auditor

System Auditor is responsible for the proper functioning of the QTSP “Diia” ICS.

The main responsibilities of the System Auditor are:

- conducting audits of event audit log books that record the tools and equipment of the software and hardware complex (hereinafter referred to as the technical tools) of the QTSP “Diia” ICS;
- control over the QTSP “Diia” archive.

5.3.2. Requirements for personnel qualifications, experience and competency

QTSP “Diia” personnel shall have the knowledge, experience and qualifications necessary to provide qualified electronic trust services and comply with the provisions and requirements specified in the ISMS Policy of Ensuring Information Security in Issues Related to Personnel at the SE “DIIA” DIIA/13 - ISMS - Ppl - PL/1 - Human_resource_security, approved by the Order of the SE “DIIA” No. 20231012-2 dated October 12, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 1 dated
October 09, 2023”.

Certification Administrator, Security Administrator, System Administrator, System Auditor may be a person who has a higher education in the field of information technology, information protection or cybersecurity, as well as at least three years of professional experience in these fields.

5.3.3. Personnel training requirements and procedures

Head of the QTSP “Diia” specialised subdivision is obliged to ensure the creation of conditions for continuous personal education and continuous professional development of the QTSP “Diia” personnel in the fields of information technology, information security or cybersecurity and personal data protection.

QTSP “Diia” personnel regularly participate in seminars, conferences and meetings on the provision of qualified electronic trust services, information technology, information protection, cybersecurity and personal data protection. Training shall be confirmed by a diploma, certificate, etc.

QTSP “Diia” personnel are also trained and tested in accordance with the section “Training” of the website http://suib.office.diia/is-course.

5.3.4. Sanctions for personnel’s unauthorised actions

Head of the QTSP “Diia” specialised subdivision has established a clear system of disciplinary sanctions for non-compliance by the QTSP “Diia” personnel with their position responsibilities, the requirements of legislative and regulatory acts in the field of electronic trust services and the requirements of the internal organisational and administrative documentation of the QTSP “Diia” and the Policy of Ensuring Information Security in Issues Related to Personnel at the SE “DIIA” DIIA/13 - ISMS - Ppl - PL/1 - Human_resource_security, approved by the Order of the SE “DIIA” No. 20231012-2 dated October 12, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 1 dated October 09, 2023”.

Non-compliance by the QTSP “Diia” personnel with their position responsibilities, requirements of legislative and regulatory acts in the field of electronic trust services, requirements of the internal organisational and administrative documentation of the QTSP “Diia” and the Policy of Ensuring Information Security in Issues Related to Personnel at the SE “DIIA” DIIA/13 - ISMS - Ppl - PL/1 - Human_resource_security, approved by the Order of the SE “DIIA” No. 20231220-3 dated December 20, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 2 dated October 09, 2023” within the organisation, taking into account the mode of operation of the QTSP “Diia”, provides disciplinary sanctions, administrative and criminal liability, provided for by the following documents:

- Collective Agreement of the State Enterprise “DIIA” for 2024-2026;
- Agreement for the representation of the QTSP “Diia” (for QTSP “Diia” separate registration units);
- Code of Ukraine on Administrative Offences;
- Criminal Code of Ukraine.

5.3.5. Control of separate registration units

The same requirements are applied to the employees of the QTSP “Diia” separate registration units, who are responsible for registering users, as to the registration administrators.

Employees of the QTSP “Diia” separate registration units include employees of legal entities and natural persons-entrepreneurs who, on the basis of an agreement with the QTSP “Diia”, register users.

The following functional responsibilities are assigned to the employees of the QTSP “Diia” separate registration units:

- Remote Registration Administrator;
- responsible for information protection at the QTSP “Diia” separate registration unit.

Remote Registration Administrator shall be responsible for performing the functions and bear the responsibilities of the Registration Administrator as defined in this Policy of the Certificate.

The persons responsible for information protection shall be appointed from among the remote Registration Administrators at the QTSP “Diia” separate registration unit.

Within the scope of his/her duties, the person responsible for information protection at the QTSP “Diia” separate registration unit is responsible for the proper exploitation of the complex of security measures of the QTSP “Diia” separate registration unit.

The main responsibilities of the person responsible for information protection at the QTSP “Diia” separate registration unit are:

- organisation of exploitation and maintenance of hardware and software of the QTSP “Diia” separate registration unit;
- participation in the implementation and ensuring the functioning of the ICS of the QTSP “Diia” separate registration unit;
- control over the operation of the software complex of the QTSP “Diia” separate registration unit;
- control over the use of private keys of the personnel of the QTSP “Diia” separate registration unit;
- participation in the creation and launching of the ICS of the QTSP “Diia” separate registration unit.

System Administrator and Security Administrator may carry out the functions of the person responsible for information protection at the QTSP “Diia” separate registration unit to the extent that does not contradict to their similar functions in relation to other components of the QTSP “Diia” ICS.

5.3.6. Documentation provided to personnel

Organisational and legal status of the Head of the specialised subdivision and the personnel of the QTSP “Diia”, their tasks and functions, rights and duties, responsibilities, as well as professional knowledge, experience and qualifications are defined in position instructions.

Position instructions shall contain information security requirements and methods for ensuring it.

Head and personnel of the QTSP “Diia” shall be familiar with the provisions of their position instructions, act in accordance with their position tasks and functions and with the ISMS document Policy of Ensuring Information Security in Issues Related to Personnel at the SE “DIIA” DIIA/13 - ISMS - Ppl - PL/1 - Human_resource_security, approved by the Order of the SE “DIIA” No. 20231012-2 dated October 12, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 1 dated October 09, 2023”.

QTSP “Diia” personnel shall be notified of changes in the organisation of QTSP “Diia” processes that relate to their position responsibilities.

5.4. Maintaining an event audit log book

Event audit log book shall be maintained in accordance with the requirements specified in the Clause 6.4.5 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2.

5.4.1. Types of recorded events

Evidence and archive management procedures shall include the maintaining event audit log books that record the following types of events:

- attempts to create, destroy, set passwords, change access rights in the QTSP “Diia” ICS, etc.;
- replacement of technical tools of the QTSP “Diia” ICS and key pairs;
- formation, blocking, cancellation and renewal of certificates, formation of revoked certificate lists (CRL);
- attempts of unauthorised access to the QTSP “Diia” ICS;
- providing personnel with access to the QTSP “Diia” ICS;
- changes in system configurations and technical maintenance of the QTSP “Diia” ICS;
- malfunctions in the work of the QTSP “Diia” ICS;
- other events necessary for the collection of evidence.

5.4.2. Frequency of processing the event audit log book

Event audit log books are being reserved and reviewed by Security Administrator at least once a week, who verifies for unauthorised modification and examines events.

5.4.3. Event audit log book retention period

QTSP “Diia” keeps event audit log books at the place of their creation for 10 years, after that it ensures their transfer to archival storage.

5.4.4 Event audit log book protection

All records in the electronic event audit log books shall contain the date and time of the event, as well as identify the entity that initiated or participated in it.

Time specified in the event audit log book shall be synchronised with Coordinated Universal Time (UTC) with an accuracy of a second.

Event audit log books shall be protected from unauthorised viewing, modification and destruction.

The event records in the event audit log books shall be subject to a qualified electronic signature of the Security Administrator.

5.4.5. Event audit log book backup procedures

Event audit log book is backed up by the QTSP “Diia” in accordance with the internal documentation on QTSP “Diia” ICS protection and the ISMS document Procedure for Event Logging at the State Enterprise “DIIA” DIIA/13 - ISMS - Tech - GU/2 - SOP/3 -Event logging, approved by the Order of the SE “DIIA” No. 20240212-1 dated February 12, 2024 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 3 dated
February 08, 2024”.

5.4.6. Time synchronisation

Time synchronisation in the technical means of the QTSP “Diia” ICS at the main and backup sites is ensured by a set of time synchronisation tools, taking into account the document Procedure for Time Synchronisation at the State Enterprise “DIIA” DIIA/13 - ISMS - Tech - GU/2 - SOP/6 - Clock synchronisation, approved by the Order of the SE “DIIA” No. 20240325-1 dated March 25, 2024 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 4 dated March 22, 2024”.

Complex of time synchronisation means provides receiving time synchronisation signals from the QTSP “Diia” ICS interaction servers (hereinafter referred to as NTP servers), backup NTP servers synchronised with the state standard of time and frequency units, GPS time synchronisation servers of the QTSP “Diia” and system time synchronisation on the technical tools of the QTSP “Diia” ICS.

GPS time synchronisation servers of the QTSP “Diia” receive time signals from the GPS receiver, as well as reserve time synchronisation sources: external NTP servers of the CCA (czo.gov.ua, time.czo.gov.ua), ntp.metrology.kharkov.ua and kyivtime.org, which are synchronised with the State Standard of Time and Frequency Units and transmit synchronised data to the QTSP “Diia” interaction servers.

The main source of time for the QTSP “Diia” ICS is NTP servers.

All servers, CPI equipment and personal computers of the QTSP “Diia” are connected to the NTP server and synchronise the system clock according to the time value received from it.

5.5. Document archive

Requirements specified in the Clause 6.4.6 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

5.5.1. Types of documents and data subject to archival storage

Archival storage of information is carried out in accordance with the internal organisational and administrative documents of the QTSP “Diia”.

The following are subject to mandatory archiving:

- qualified certificates of the QTSP “Diia” and users;
- revoked certificate lists (CRL);
- event audit log books;
- documented information - documents (applications for the formation, blocking, renewal , cancellation of user certificates), on the basis of which users were provided with electronic trust services.

5.5.2. Archive storage period

Documents in paper and electronic forms shall be stored in accordance with the rules established by the legislation in the field of archives and legislation in the field of electronic trust services.

QTSP “Diia” certificates, QTSP “Diia” server certificates and Administrator certificates, user certificates, and revoked certificate lists (CRLs) are stored permanently.

5.5.3. Archive protection

QTSP “Diia” ensures the archive protection in accordance with internal organisational and administrative documents and legislation in the field of archiving.

A separate storage facility (safe or safe compartment) with two copies of keys and sealing devices is allocated for storing media with backup and archive copies. One copy of the key to the storage is kept by the Security Administrator, and the other is kept in a sealed form in the storage (safe) of the Head of the QTSP “Diia” specialised subdivision.

Archive premises are equipped with technical tools that exclude the possibility of unauthorised access to the information to be archived. The archival documents of the QTSP “Diia” users are stored in a specialised company under an agreement in compliance with all security requirements. The contractual relations between the specialised company and the QTSP “Diia” is carried out in accordance with the ISMS documentation, in particular: Policy on Information Security of the SE “DIIA” with representatives of third-party organisations DIIA/13 - ISMS - Org - PL/3 - IS Supplier relations, approved by the Order No. 20231220-3 dated December 20, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 2 dated December 19, 2023”.

5.5.4. Archive backup procedures

QTSP “Diia” ensures backup of the archive in accordance with the requirements and instructions of the QTSP “Diia” ICS.

Tools included in the central server of the QTSP “Diia” ICS provide automatic data backup. Automatic backup shall be performed at least once a day during the lowest load of the central server of the QTSP “Diia” ICS.

Additionally, it is possible to perform backup of certificates to optical media or other removable storage media manually. After creating a new backup copy, the previous one becomes an archive copy.

Certificates are restored from a backup copy by tools of the central server of the QTSP “Diia” ICS by reading certificates from the last (current) backup copy and recording them to the database of the QTSP “Diia” ICS server.

Removable media are stored in envelopes or packages that are affixed by Security Administrator’s seal. The copy account number is indicated on the packaging. Facts of creating and using copies are recorded in a separate log book.

Database backup copies and event audit log books are stored in the QTSP “Diia” ICS premises for 10 years. System Administrator is responsible for controlling automatic backup and performing manual backup. Security Administrator regularly controls the process of creating, storing and verifying backup copies in accordance with internal instructions and the ISMS, in particular the Plan for Ensuring Continuous Operation of the SE “DIIA” within the scope of the ISMS DIIA/13 - ISMS - Org - PL/2 - GU/2 - SOP/1 - Business Continuity Plan, approved by the Order of the SE “DIIA” No. 20231220-3 dated December 20, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 2 dated December 19, 2023”.

5.5.5. Requirement to affix electronic time stamps to records

QTSP “Diia” may affix electronic time stamps to records related to its activity.

5.5.6. Archive collection system (internal or external)

Archive collection systems are located in the office and special premises of the QTSP “Diia” and in a specialised company under an agreement in compliance with all security requirements.

Requirements for office and special premises are described in the Clause 5.2.1 of this Policy of the Certificate.

5.5.7. Procedures for receiving and verifying archival information

Access to archived data is strictly limited. Only authorised employees have access to this system in accordance with their official duties. QTSP “Diia” releases information from the archive only by the Court Order.

5.6. Change of the key

Change of the QTSP “Diia” key pair and the QTSP “Diia” ICS servers may be:

- scheduled;
- unscheduled.

Scheduled change of the QTSP “Diia” key pair is carried out no later than two years before the expiration of the QTSP “Diia” qualified certificate to ensure the uninterrupted operation of the QTSP “Diia” and user qualified certificates.

Special requirements specified in the Instruction on the rules of order for generating key data and handling key documents are applied during the scheduled change of the QTSP “Diia” keys.

Procedure for scheduled change of the QTSP “Diia” keys is carried out in a special premises with the participation of the Head of the QTSP “Diia” specialised subdivision, the Security Administrator and the Certification Administrator in the following order:

- Security Administrator and the Head of the QTSP “Diia” specialised subdivision generate a new private and public key of the QTSP “Diia”;
- Security Administrator and Certification Administrator form a request for a qualified certificate of public key of the QTSP “Diia”;
- Head of the QTSP “Diia” specialised subdivision initiates the process of certifying the validity of the QTSP “Diia” public key at the Central Certifying Authority in accordance with the Rules and Procedures for Operation of the Central Certifying Authority, approved by the Order of the Ministry of Digital Transformation of Ukraine No. 33 dated February 28, 2024, registered with the Ministry of Justice of Ukraine No. 393/41738 dated March 15, 2024;
- after receiving a QTSP “Diia” qualified certificate of public key from the Central Certifying Authority, the Security Administrator enters the private key of the QTSP “Diia” for use;
- after receiving a QTSP “Diia” qualified certificate of public key from the Central Certifying Authority, a new QTSP “Diia” certificate is published on the official QTSP “Diia” website;
- current key pair of the QTSP “Diia” becomes the previous one, and the newly generated key pair becomes the current one.

Previous QTSP “Diia” private key is used only to create a qualified electronic seal of the QTSP “Diia” on the data on the status of qualified certificates of public keys of signatories and electronic seal creators generated before the scheduled change of QTSP “Diia” keys. Previous QTSP “Diia” private key is used to verify the qualified electronic seal on the qualified certificate of public keys of signatories and electronic seal creators formed before the scheduled change of QTSP “Diia” keys and the qualified electronic seal on the data on the status of these certificates.

Upon expiry of the qualified certificate of the previous QTSP “Diia” public key, the appropriate private key and all its copies are destroyed.

Previous QTSP “Diia” public key is stored in the qualified certificate of public key of the QTSP “Diia” permanently.

Unscheduled change of the key pair is carried out in cases of compromise or suspicion of compromise of private keys of the QTSP “Diia”, the QTSP “Diia” ICS servers (OCSP, TSP, CMP) or in case of failure of the QESST (cryptomodule) with the private key.

After changing private keys, QTSP “Diia” forms user qualified certificates using the new key pair of the QTSP “Diia”.

Access to the current qualified certificate of the QTSP “Diia” is provided on the official CCA website at the following link: https://czo.gov.ua/ca-registry-details?type=0&id=116.

5.7. Compromise and emergency renewal

Requirements specified in the Clause 6.4.8 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

5.7.1. Incident and compromise handling procedures

QTSP “Diia” has an incident response plan and a disaster renewal plan.

Rules of order on actions and response of the QTSP “Diia” personnel to incidents are determined by the ISMS document Information Security Incident Management Policy at the SE “DIIA” DIIA/13 - ISMS - Org - PL/4 - Incident management policy, approved by the Order of the SE “DIIA” No. 20231220-3 dated December 20, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 2 dated December 19, 2023”.

Incident management procedures shall include:

- implementation of measures determined by the Rules of order for coordinating the activity of state authorities, local self-government authorities, military formations, enterprises, institutions and organisations regardless of ownership on prevention, detection and elimination of consequences of unauthorised actions against state information resources in information, electronic communication and information and communication systems, approved by the Order of the Administration of the State Service of Special Communications and Information Protection of Ukraine No. 94 dated June 10, 2008, registered in the Ministry of Justice of Ukraine under
No. 603/15294 dated July 07, 2008;
- informing the CA of violations of the security and information protection requirements specified in the Paragraph twelve of the Part four of the Article 13 of the Law of Ukraine “On Electronic Identification and Electronic Trust Services” within 24 hours after the violation is detected;
- informing the users to whom services are provided about security violations that have a negative impact on them within two hours after the violation is detected.
- QTSP "Diia" shall immediately notify Adobe at AATLNotification@adobe.com (or another address designated by Adobe), unless restricted by competent authorities, of any breach of security or loss of integrity, compromise (or suspected compromise) of QTSP "Diia"’s certification signing key, personal data protection breach, and security issues leading to certificate mis-issuance, on any server, PC, other system or endpoint logically connected to certificate issuance and management systems or reasonable suspicion thereof.
- Within three (3) calendar days of sending the notification to Adobe, QTSP “Diia” shall provide detailed information about the incident and a remediation/action plan.

5.7.2. Renewal procedures if computing resources, software and/or data are damaged

It is determined by the following ISMS documents: Information Security Incident Management Policy at the SE “DIIA” DIIA/13 - ISMS - Org - PL/4 - Incident Management Policy and Business Continuity Plan of the SE “DIIA” within the scope of the ISMS DIIA/13 - ISMS - Org - PL/2 - GU/2 - SOP/1 - Business Continuity Plan, approved by the Order of the SE “DIIA” No. 20231220-3 dated December 20, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 2 dated December 19, 2023”.

5.7.3. Renewal procedures after key compromise

If there is a suspicion of compromise of the private key of the QTSP “Diia” or its servers, the operation of network cryptomodules with these private keys is suspended, and the QTSP “Diia” Information Security Service initiates an internal investigation.

In case of confirmation of the fact of compromise of the QTSP “Diia” private key, the Head of the specialised subdivision of the QTSP “Diia” and the Security Administrator shall take the following measures:

- to stop the operation of network cryptomodules with compromised private keys of the QTSP “Diia” or its servers;
- to notify the CAA about the compromise of the QTSP “Diia” private key;
- to cancel the QTSP “Diia” qualified certificate corresponding to the compromised private key;
- to initiate the destruction of the QTSP “Diia” compromised private key in the network cryptomodule;
- to carry out the generation of a new QTSP “Diia” private key and initiate the formation of the appropriate qualified certificate of the QTSP “Diia” for it;
- to activate the new private key of the QTSP “Diia” by reading it from the network cryptomodule.

Detailed rules of order for renewal after compromise of the QTSP “Diia” private key is defined by the ISMS.

5.7.4. Business continuity capabilities after a disaster

QTSP “Diia” has a backup site similar to the main site to ensure continuity of operations in the event of accidents or disasters in accordance with the ISMS document Business Continuity Plan of the SE “DIIA” within the scope of the ISMS DIIA/13 - ISMS - Org - PL/2 - GU/2 - SOP/1 - Business Continuity Plan, approved by the Order of the SE “DIIA” No. 20231220-3 dated December 20, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 2 dated December 19, 2023”.

In the event of an emergency, accident or a disaster, or failure of the main site, QTSP “Diia” resumes its work from the backup site. Backup copies of private keys, data and information critical for the restoration of the QTSP “Diia” ICS are constantly up to date and reliably protected.

5.7.5. Ensuring Continuity of the Time-Stamping Unit (TSU)

Ensuring continuity of the TSU includes:

- timely rollover of the key pair and certificate dedicated to time-stamp generation before the end of the private key usage period;

- the use of backup mechanisms for technical components supporting qualified time-stamp generation and the ability to promptly restore service functionality;
- secure destruction of outdated private keys;
- immediate suspension of time-stamp generation in case of loss of synchronisation with the national UTC(UA) scale or in case of security incidents;
- resumption of the service after eliminating the cause of suspension and confirming restoration of accurate time synchronisation.

5.8. Termination of the Provider's activity

Requirements specified in the Clause 6.4.9 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 shall apply to the objects, processes and measures specified in this Section. The termination of the QTSP "Diia" activity shall be carried out in accordance with the approved Plan for the Termination of the Provision of Qualified Electronic Trust Services (hereinafter referred to as the Termination Plan), taking into account the requirements of the Law of Ukraine "On Electronic Identification and Electronic Trust Services".

5.8.1. Reasons for termination of the Provider's activity

QTSP "Diia" shall terminate its activity in providing qualified electronic trust services in case of:

1) decision by the CCA to cancel the status of a Qualified Provider;
2) decision of the QTSP "Diia" to terminate the provision of qualified electronic trust services specified in the Trust List;
3) termination of the QTSP "Diia" activity (termination of the legal entity), except in cases of succession as defined in the Clause 5.8.4 of this Policy of the Certificate;
4) entry into force of a court decision on cancellation of the status of a Qualified Provider, recognition of the QTSP "Diia" as a bankrupt.

QTSP "Diia" shall notify users, CCA and CA of the decision to terminate the provision of qualified electronic trust services no later than five business days from the date of such decision.

CCA is obliged to publish information about its decision to terminate the QTSP "Diia" activity in providing qualified electronic trust services, including in connection with the cancellation of the status of a qualified trust service provider, no later than the next business day after such a decision is made by:

- posting information about such a decision on its official website;
- to send a notice of such decision to the QTSP "Diia", indicating the reasons for its decision.

CCA shall announce on its official website about the termination of the provision of qualified electronic trust services of the QTSP "Diia" no later than the next business day after the date of receipt of the notice of the reasons for compulsory termination.

Notification of the CCA on termination of provision of qualified electronic trust services of the QTSP "Diia" shall contain the date of publication.

QTSP "Diia" shall terminate the provision of qualified electronic trust services three months after the date of publication by the CCA on its official website of the notification on the termination of the provision of qualified electronic trust services by the QTSP "Diia".

From the date of publication by the CCA on its official website of the notification on termination of the provision of qualified electronic trust services of the QTSP "Diia" and until the date

of termination of the provision of qualified electronic trust services, the QTSP “Diia” is obliged to provide electronic trust services, except for the formation of new qualified certificates.

Upon termination of the activity of providing qualified electronic trust services, the QTSP “Diia” shall transfer to another service provider the users with whom it has concluded agreements on the provision of qualified electronic trust services.

If the user refuses to continue receiving services under the agreement for the provision of qualified electronic trust services concluded with the QTSP “Diia” (SE “DIIA”) with another provider before the expiration of the appropriate agreement, the QTSP “Diia” is obliged to repay the funds to such user for services that cannot be provided in the future if they were prepaid by the user.

If the user has agreed to continue the provision of services under the agreement for the provision of qualified electronic trust services concluded with the QTSP “Diia” (SE “DIIA”) with another provider before the expiration of the appropriate agreement, the QTSP “Diia” is obliged to pay for the further provision of qualified electronic trust services to such user at the rates set by the appropriate provider.

On the day defined as the date of termination of the provision of qualified electronic trust services of the QTSP “Diia”, the CCA shall make the appropriate changes to the Trust List.

In case of termination of the provision of qualified trust services, QTSP “Diia” is obliged to transfer documented information (documents on the basis of which qualified electronic trust services were provided to users and qualified certificates of public keys were formed, blocked, renewed, cancelled, all formed qualified certificates of public keys, as well as registers of formed qualified certificates of public keys to another provider or CCA).

Documented information would be transmitted by the QTSP “Diia” no later than the date defined by the QTSP “Diia” as the date of termination of the provision of qualified electronic trust services or the date of entry into force of the appropriate court decision.

CCA cancels the qualified certificate issued by it to the QTSP “Diia” on the date determined by the QTSP “Diia” as the date of termination of the activity of providing qualified electronic trust services, or on the date of entry into force of the appropriate court decision.

5.8.2. Notification of termination of the Provider’s activity

QTSP “Diia” shall notify users, CCA and CA of the decision to terminate the provision of qualified electronic trust services no later than five business days from the date of such decision.

CCA is obliged to publish information on the decision of the CCA to terminate the activity of QTSP “Diia” in providing qualified electronic trust services, including in connection with the cancellation of the status of a qualified trust service provider, no later than the next business day after such a decision is made by:

- posting information about such decision on its official website;
- sending a notification of such decision to the QTSP “Diia” indicating the basis for this decision.

CCA is obliged to publish on its official website a notice of termination of the provision of qualified electronic trust services of the QTSP “Diia” no later than the next business day from the date of receipt of the notification of the occurrence of the reasons provided for in the Subclauses 2 - 4 of the Clause 5.8.1 of this Policy of the Certificate.

Notification of the CCA on termination of activity on provision of qualified electronic trust services of the QTSP “Diia” shall contain the date of publication.

In the event of service termination or handover, QTSP “Diia” shall notify Adobe at least one (1) month in advance of the termination/handover date. The notification shall be sent to AATLNotification@adobe.com (or another address designated by Adobe).

5.8.3. Date of termination of the Provider’s activity

QTSP “Diia” shall terminate its activity in the provision of qualified electronic trust services three months after the date of publication on its official website of the notification on the termination of the provision of qualified electronic trust services by the QTSP “Diia”.

From the date of publication on its official website of the notification of termination of the provision of qualified electronic trust services by the QTSP “Diia” and until the date of termination of the provision of qualified electronic trust services, the QTSP “Diia” is obliged to provide electronic trust services, except for the formation of new qualified certificates.

From the date of publication on its official website of the notification of termination of the provision of qualified electronic trust services by the QTSP “Diia” and until the date of termination of the provision of qualified electronic trust services, the QTSP “Diia” is obliged to provide electronic trust services, except for the formation of new qualified certificates.

On the day defined as the date of termination of the activity of the QTSP “Diia” for the provision of qualified electronic trust services, the CCA shall make the appropriate changes to the Trust List.

5.8.4. Legal succession

In order to ensure the continuous provision of qualified electronic trust services to their users, the CCA may decide to amend the Trust List to replace the Qualified Trust Service Provider by replacing the information about the QTSP “Diia” with information about another qualified trust service provider, if the transfer of the appropriate rights and obligations is carried out by mutual consent of such providers, under an agreement or on other reasons for legal succession determined by the legislation.

In case the user refuses to continue the service under the agreement for the provision of qualified electronic trust services concluded with the QTSP “Diia” (SE “DIIA”), which terminates the provision of qualified electronic trust services, with another Qualified Trust Service Provider before the expiration of the appropriate agreement, the QTSP “Diia” is obliged to repay to such user the funds for services that cannot be provided in the future if they were previously paid by the user.

If the user has agreed to continue the service under the agreement for the provision of qualified electronic trust services concluded with the QTSP “Diia” (SE “DIIA”), which terminates the provision of qualified electronic trust services, with another Qualified Trust Service Provider before the expiration of the relevant agreement, the QTSP “Diia” is obliged to pay for the further provision of qualified electronic trust services to such user at the rates set by the appropriate qualified trust service provider.

5.8.5. Transfer of documented information

In case of termination of activity in the provision of qualified electronic trust services, the QTSP “Diia” shall transfer to another Qualified Trust Service Provider that has expressed its intention to continue to serve users until the expiration of the appropriate agreements on the provision of qualified electronic trust services, or to the CCA the documents on the basis of which qualified electronic trust services were provided to users and qualified certificates were formed, blocked,

renewed, cancelled qualified certificates, all formed qualified certificates, as well as registers of formed qualified certificates.

Transfer of documented information is carried out in accordance with:

- Rules of order for the transfer of services to users of electronic trust services with whom a Qualified Trust Service Provider that terminates to provide qualified electronic trust services has entered into agreements for the provision of qualified electronic trust services to another qualified trust service provider, approved by the Resolution of the Cabinet of Ministers of Ukraine No. 842 dated July 23, 2024;
- Rules of order for storage of documented information and its transfer to the Central Certifying Authority in case of termination of a qualified electronic trust services provider, approved by the Resolution of the Cabinet of Ministers of Ukraine No.1408 dated 10.12.2024;
- subclauses 6.3.4-10A and 6.3.4-11A of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2.

5.8.6. Activity Termination Plan

QTSP “Diia” has an approved Activity Termination Plan.

Activity Termination Plan defines the conditions to be complied with by QTSP “Diia” in order to prevent negative consequences in case of termination of its activity in providing qualified electronic trust services, as well as to ensure the stability and durability of qualified electronic trust services.

QTSP “Diia” approves the Activity Termination Plan and, if necessary, amends it to update the information contained therein.

CCA approves the Activity Termination Plan and amendments to it in accordance with the order established by the legislation.

Activity Termination Plan shall define:

- rules of order for notifying users, the Central Certifying Authority, QTSP “Diia” personnel, separate registration units, entities that trust QTSP “Diia” and counterparties of the termination of activity in providing qualified electronic trust services;

- arrangements and agreements with third parties to continue carrying out obligations in the case of termination of the activity of providing qualified electronic trust services by the QTSP “Diia” (transfer of user services to another qualified provider).

Activity Termination Plan is confidential and verified by the CAA.

6. TECHNICAL SAFETY MEASURES

Requirements specified in the Clause 6.5 of DSTU ETSI EN 319 411-1, DSTU ETSI EN 319 411-2 and ISMS document Regulation on the use of cryptographic information protection means at the SE “DIIA” DIIA/13 - ISMS - Tech - SOP/2 - Use of cryptography, approved by the Order No. 20231220-3 dated December 20, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 2 dated December 19, 2023”.

Furthermore, the following special requirements apply:

6.1. Generating and installing a key pair

6.1.1. Generating a key pair

6.1.1.1. Generating a Provider key pair

Generation of the private key of the QTSP “Diia” is performed in the cryptographic module (hereinafter referred to as the cryptomodule) on the central server of QTSP “Diia” ICS, which is located in a special room, by two persons – the Head of the specialised subdivision of the QTSP “Diia”, the Certification Administrator under the supervision of the Security Administrator.

Before the process of generating the private key of the QTSP “Diia”, the Security Administrator is authenticated in the cryptomodule. The authentication data in the cryptomodule is created in accordance with the exploitation documentation for the cryptomodule before the generation process begins.

Generation of private keys and their corresponding public keys of the QTSP “Diia” is carried out in accordance with the exploitation documentation for the appropriate QESST of QTSP “Diia” ICS, on which the generation is carried out.

Generation of the QTSP “Diia” key pair and storage of QTSP “Diia” private keys takes place in the HSM used for key issuance and storage, which provides protection against external compromise and operates in a physically secure environment.

Generation of the key pair of the QTSP “Diia” servers (OCSP, TSP, CMP) is performed on the central server of the QTSP “Diia” complex in the service premises by two persons – the – Security Administrator and the Certification Administrator.

Information on the procedure of generating private keys of the QTSP “Diia” and servers of QTSP “Diia” ICS (OCSP, TSP, CMP) is set out separately in the Instruction on the rules of order of key data generation and handling key documents, which is an integral part of the ISMS and is classified as confidential information that is not subject to disclosure.

Facts of generation of private keys of the QTSP “Diia” and servers of the QTSP “Diia” ICS (OCSP, TSP, CMP) are recorded in the electronic key data log book.

6.1.1.2. Generating a user key pair

During the provision of a qualified electronic trust service for the creation, verification and confirmation of qualified electronic signatures or seals, the QTSP “Diia” shall provide:

- usage by the user exclusively of a qualified electronic signature or seal and a qualified certificate;
- protection of the exchange of information between the user and the QTSP “Diia” by means of public electronic communication networks;
- creation of conditions for generating a user key pair;
- assistance during the generation of the user’s key pair in a manner that does not violate the confidentiality and integrity of the private key, as well as familiarisation with the value of the private key parameters and their copying;
- uniqueness of the user’s key pair;
- storage of the user’s private key;
- protection against unauthorised access to the user’s private key parameters when using a qualified electronic signature or seal.

A private key as part of a user key pair can be generated:

- at the user’s stationary workplace or on their own portable computing device;

- at the key generation workstation in the QTSP “Diia” offices and QTSP “Diia” separate registration units;

- via the mobile application of the Unified State Web Portal of Electronic Services (“Diia”);

- via a mobile application that is part of the “E-Resident” Information System.

In case the key pair was generated by the user outside the QTSP “Diia” premises and/or in the absence of the appropriate personnel, the identification of such a user, verification of the sufficiency of the scope of his/her civil legal capacity and legal capability, formation and issuance of a qualified certificate to him/her shall be carried out by the QTSP “Diia” after verification of the fact that the user possesses a private key that corresponds to the public key provided for the formation of a qualified certificate.

Generation and/or management of a key pair on behalf of the user may be carried out exclusively by the QTSP “Diia”. To generate private keys, qualified electronic signature or seal tools are used in the form of hardware and software tools (secure private key carriers, tokens, SIM cards, network cryptomodules), which can function under the control or using separate software applications or software modules (crypto libraries) that function as part of other software applications and are owned by users or provided by the QTSP “Diia”.

Generated user’s private key is protected by means of attributes to prevent unauthorised persons from accessing the private key parameters (password, PIN, biometric data of the private key holder).

In order to provide qualified electronic trust services, QTSP “Diia” uses qualified electronic signature or seal tools that have documentary evidence of compliance with the requirements of the Articles 18 and 19 of the Law, issued based on the results of certification of such tools.

Provision of qualified electronic signature or seal tools in the form of hardware and software tools and their technical support and maintenance by the QTSP “Diia” is carried out on a contractual basis.

Provision of qualified electronic signature or seal tools by QTSP “Diia” in the form of separate software applications or software modules (crypto libraries) functioning as part of other software applications may be carried out by transferring these tools on information media directly to the user or by providing access through the QTSP “Diia” website.

For certificate profiles submitted to AATL, the private key of an end-entity certificate is generated directly in a qualified signature/seal creation device (QSCD), at the time of qualified e-signature creation it is confirmed that the private key resides in the QSCD. Generation and/or management of a subscriber’s key pair may only be performed by the QTSP. Private-key export is not permitted.

6.1.2. Delivery of a private key to the user

User receives a private key in possession as a result of the provision of a qualified electronic trust service by the QTSP “Diia” under the following conditions:

- receiving and using a private key on the basis of full possession of a qualified electronic signature or seal, including the media of the private key;
- receiving and using a private key on the rights of full possession or access on a contractual basis to a part of the resource of a qualified electronic signature or seal, which implements the storage of a set of private keys of a qualified electronic signature or seal (for example, a network cryptomodule).

Actual receipt of the private key by the user occurs at the time of generation of the private key personally or at the time of changing the attributes of protection against unauthorised access to the parameters of the private key (password, PIN, biometric data of the private key holder) in case the key pairs were previously created by the QTSP “Diia”. It is not allowed for the QTSP “Diia” to form qualified certificates until the user actually receives the private key.

Appropriate Regulations on Certification Practices of the Qualified Trust Service Provider “Diia” on the Qualified Certificates of the Electronic Signature and Seal (Annex 2 to these Rules and Procedures) contain additional information.

6.1.3. Delivery of the public key to the user

Public key is provided for formation of a qualified certificate as part of a request for formation of a qualified certificate, which is a PKCS#10 file containing the user’s public key and additional information for formation of a qualified certificate.

A PKCS#10 request is formed during the generation of private and public keys by tools of a qualified electronic signature or seal. Formation of the request involves creation of an advanced electronic signature using a private key from the same pair with the public key.

6.1.4. Delivery of the Provider’s public key to entities that trust the Provider

Qualified certificates of the QTSP “Diia” and the Central Certifying Authority are published on the website of the QTSP “Diia”.

Certificate chain container, available for download by entities that trust the QTSP “Diia”, is available on the QTSP “Diia” website at the following link: https://ca.diia.gov.ua/download-all.

Access to the current qualified certificate of the QTSP “Diia” is provided on the official website of the CCA at the link: https://czo.gov.ua/ca-registry-details?type=0&id=116.

6.1.5. Key sizes (parameters)

Private and appropriate public keys with parameters that comply with the following requirements are used in the QTSP “Diia” ICS:

- electronic signature algorithm DSTU 4145-2002, key size - 256 bits, which conforms to the DSTU 4145-2002;
- ECDSA electronic signature algorithm with a key length of 256 bits, which conforms to the DSTU ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);
- RSA electronic signature algorithm with a key size of 4096 bits, which conforms to the PKCS#1 standard (IETF RFC 3447).
- For profiles submitted to AATL, the minimum levels apply: RSA 2048+, ECDSA 256+, and a hash algorithm no weaker than SHA-256.

6.1.6. Generating public key parameters

During the public key generation, a hardware random number generator (RNG) is used to generate keys, including statistical verification of the generator output. Statistical verification of random bit sequences from the hardware RNG is performed in accordance with the Instruction on the Rules of Order of the Key Data Generation and Handling Key Documents. Keys are generated and stored in the hardware network cryptomodule “Hriada-301”.

6.1.7. Main purposes of using a private key by the Provider

QTSP “Diia” private keys ensure the functioning of the QTSP “Diia” ICS

QTSP “Diia” defines the practice of using QTSP “Diia” keys to sign user certificates, OCSP server certificates, QTSP “Diia” CMP, and the revoked certificate list (CRL).

6.2. Private key protection and engineering control of the cryptographic module

6.2.1. Standards and controls for the cryptographic module

To store the user private keys, QTSP “Diia” uses QESST that have documentary evidence of compliance with the requirements of the Articles 18 and 19 of the Law, issued as a result of certification of such tools and also on flash media in the form of files in *.dat and *.pfx formats.

For storing private keys of the QTSP “Diia” and servers of the QTSP “Diia” ICS, network cryptomodules are used, which are made in the form of separate hardware devices. The cryptomodules shall have documentary evidence of compliance with the requirements of the Articles 18 and 19 of the Law, issued based on the results of certification of such tools.

Qualified signature/seal creation devices (QSCD) used to store and/or operate on end-entity private keys are certified to FIPS 140-2 Level 2 or Common Criteria (incl. EN 419 241 for remote solutions), or recognized as QSCD under applicable law; QSCD conformity is evidenced by conformity assessment documents.

6.2.2. Private key (n with m) for control over several persons

Only QTSP “Diia” authorised representatives have access to the private key:

- Head of a specialised subdivision;
- Security Administrator;
- Certification Administrator.

Access attributes (login and password) to the QTSP “Diia” private keys are stored in an envelope sealed with the personal seal of the responsible person, which is stored in a secure storage (safe) located in the DPC special premises of the QTSP “Diia”, the keys and access to which are exclusively available to the responsible persons listed above.

Management of the private keys of the QTSP “Diia” is carried out by responsible persons after their authentication on the QTSP “Diia” central server by their personal access attributes.

6.2.3. Management of the signatory’s private key

QTSP “Diia” ensures the storage and protection of user private keys generated in the network cryptomodules of the Hriada-301 (high-performance device), which have documentary evidence of compliance with the requirements of the Articles 18 and 19 of the Law, issued on the basis of the results of certification of such tools, which are located in DPC special premises, access to which is available only to QTSP “Diia” responsible persons.

QTSP “Diia” ensures storage and protection of private keys of users generated in network cryptomodules that have documentary evidence of compliance with the requirements of the Articles 18 and 19 of the Law, issued as a result of certification of such tools, at remote registration units under an agreement concluded with them, which register users, access to which is available only to responsible persons at the appropriate registration unit.

6.2.4. Backup of the private key

Backing up your private key is only possible to ensure continuity of service, provided that the security level of the backup matches that of the original private key.

Backup of the private keys of the QTSP “Diia” and its servers is carried out by the Certification Administrator under the control of the Security Administrator.

During backup of the private keys of the QTSP “Diia”, at least two backup copies of the private key from the cryptomodule are created. Each backup copy of the private key of the QTSP “Diia” is recorded (if necessary, with the distribution of secrecy) on an external tool of a qualified electronic signature or seal, which is a hardware and software or hardware device in a secure form that ensures their integrity and confidentiality.

During backup of the private keys of the servers of the QTSP “Diia” ICS (OCSP, TSP, CMP), at least two backup copies of each private key are created. Each backup copy of the private key shall be recorded (if necessary, with the distribution of secrecy) on the QESST. If the private keys of the servers are not stored in cryptomodules, their backup copies are created by copying them from the main QESST to the backup ones.

Facts of backup of private keys of the QTSP “Diia” and servers of QTSP “Diia” ICS (OCSP, TSP, CMP) are recorded in the electronic key data log book.

6.2.5. Archiving of the private key

Private keys of QTSP “Diia” and users are archived in accordance with the Instruction on the Rules of Order for Generating Key Data and Handling Key Documents to the QTSP “Diia” ICS and the “Regulation on Data Backup at the SE “DIIA” DIIA/13-ISMS-Tech-GU/2 - SOP/1 - Information backup, approved by the Order No. 20231220-3 dated December 20, 2023 “On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 2 dated December 19, 2023”.

After cancellation or expiration of user qualified certificates, the user’s private key stored in the network cryptomodule of the Hriada-301 (high-performance device) of the QTSP “Diia” is automatically destroyed.

QTSP “Diia” private keys and its servers shall be destroyed by the QTSP “Diia” responsible persons upon expiry of the appropriate qualified certificates. Facts of destruction of the private keys of the QTSP “Diia” and its servers shall be recorded in the electronic key data log book.

6.2.6. Renewal of a private key

Renewal of a private keys of the QTSP “Diia” and servers (CMP, TSP, OCSP) is carried out from backup copies.

Facts of renewal of private keys of the QTSP “Diia” and servers (CMP, TSP, OCSP) of the QTSP “Diia” from backup copies are recorded in the electronic key data log book.

6.2.7. Storage of the private key in the cryptographic module

Private keys of the QTSP “Diia” and servers of the QTSP “Diia” ICS (CMP, TSP, OCSP) are stored and protected from unauthorised access in network cryptomodules that have documentary evidence of compliance with the requirements of the Articles 18 and 19 of the Law, issued on the basis of the certification of such tools.

6.2.8. Activation of the private keys

Activation of the private key of the QTSP “Diia” and servers (OCSP, CMP, TSP) is performed on the central server of the QTSP “Diia” ICS in the Provider’s service premises by the Security Administrator.

During the activation of the private key by connecting the cryptomodule to the central servers of the QTSP “Diia”, the Security Administrator is authenticated in the cryptomodule. In the process of

entering the private key of the QTSP “Diia” and servers (OCSP, CMP, TSP), the qualified certificate of the QTSP “Diia” containing the public key is read from the continuous permanent drive of the central server.

6.2.9. Deactivation of private keys

Procedure for deactivation of private keys of the QTSP “Diia” by destroying them is defined in the Clause 6.2.10 of this Policy of the Certificate.

6.2.10. Destruction of private keys

Upon expiration of the validity period of the QTSP “Diia” qualified certificate and the servers of the QTSP “Diia” ICS (OCSP, TSP, CMP), the appropriate private key and all its backup copies are destroyed.

Destruction of private keys of the QTSP “Diia” and servers of the QTSP “Diia” ICS (OCSP, TSP, CMP) shall be carried out in accordance with the exploitation documentation for the appropriate qualified electronic signature or seal tools, QESST or network cryptomodules in which they were stored and used. Procedures for destroying private keys shall ensure that the keys cannot be recovered after destruction.

Facts of destruction of private keys of the QTSP “Diia” and servers of the QTSP “Diia” ICS (OCSP, TSP, CMP), as well as their backup copies, are recorded in the key data log book.

6.2.11. Capabilities of the network cryptographic module

Network cryptomodule supports procedures that cover the secure operation of the QTSP “Diia” (generation, backup, storage, destruction).

All network cryptographic modules containing copies of the private key of the QTSP “Diia” and its servers (OCSP, CMP, TSP) are physically protected from unauthorised access.

All signing operations using the QTSP “Diia” private key are performed in the QTSP “Diia” network cryptomodule.

6.2.12. Requirements for the environment and processes for the QTSP ‘Diia’ certificate private key.

The QTSP ‘Diia’ certificate private key(s) shall be generated, stored and used in a medium that prohibits exportation and duplication that could allow unauthorized use; such a medium includes a Hardware Security Module (HSM) with a security level not lower than FIPS 140-2 Level 3 or an equivalent level of conformity.

All cryptographic operations with the QTSP ‘Diia’ certificate private key (including certificate/CRL signing) shall be performed within the HSM only; exportation of the private key and its duplication in forms enabling unauthorized use are prohibited.

Backup/recovery of the QTSP ‘Diia’ certificate private key is permitted only by HSM means and/or within the trusted HSM environment so that the private key never leaves the HSM in plaintext and no opportunities for unauthorized use are created; the security of any backup copy shall be at least equal to that of the original.

Generation, initialization and activation of the QTSP ‘Diia’ certificate private key shall follow approved procedures for generation, initialization and activation of the QTSP ‘Diia’ key, defining roles

and privileges, HSM access control, multi-factor authentication requirements, logging and log retention.

The QTSP 'Diia' shall retain documentary evidence of the HSM conformity with this clause (certificates/test reports) and provide it upon request to the auditor and/or Adobe within the AATL programme.

6.3. Other aspects of key pair management

6.3.1. Archiving of the public key

Public keys, on the basis of which qualified certificates are formed, are permanently stored in the QTSP "Diia" database.

6.3.2. Validity periods of the certificate and the usage period of the key pair

Validity periods of the QTSP "Diia" private keys comply with the validity periods of the qualified certificates of the appropriate public keys and are:

- for private keys of the QTSP "Diia" and its servers (OCSP, CMP, TSP) - not more than 5 years;
- for private keys of Administrators and users - no more than 2 years.

6.4. Activation data

6.4.1. Creation and installation of activation data

In accordance with the Clause 3.2 of this Policy of the Certificate.

6.4.2. Protection of the activation data

Private keys stored in the QESST shall be protected by passwords consisting of at least 8 characters containing uppercase and lowercase Latin letters, numbers and symbols.

6.4.3. Other aspects of activation data

No conditions.

6.5. Computer security control

6.5.1. Special technical requirements for computer security

QTSP "Diia" ensures the protection of information resources from external threats, attacks and unauthorised information leakage by creating and maintaining secure information technologies (application of multi-factor authentication), within which access to information of various categories is organised in such a way that only authorised users or processes are given the opportunity to work with specific information, access to which is restricted and integrity is guaranteed during its electronic processing, in the form of a printed document or a set of data contained on removable media, taking into account the ISMS document Regulation on Acceptable Use of SE "DIIA" Assets DIIA/13 - ISMS - Org - PL/2 - GU/4 - SOP/1 - Acceptable use, approved by the Order of SE "DIIA" No. 20231220-3 dated December 20, 2023 "On Approval of Documents in Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 3 dated December 19, 2023".

QTSP "Diia" ensures:

– confidentiality and integrity of information stored and processed in the components of the QTSP "Diia", as well as transferred between them;

– confidentiality of private keys used in the QTSP "Diia" and by its users;

– confidentiality of technological information that ensures the functioning of the QTSP "Diia" ICS;

– access to the information and resources of the QTSP "Diia" ICS to users in accordance with the rules established by the security policy of the QTSP "Diia";

– observation of users' actions by implementing mechanisms and procedures for control, registration and audit of registered events.

6.5.2. Computer security rating

QTSP "Diia" ICS are verified, inspected by the acknowledged CAA and properly controlled in accordance with [EN 319 401] and requirements of the applicable legislation.

After passing the certification procedure for conformity to the requirements of ISO/IEC 27002:2013(E) "Information security, cybersecurity and privacy protection - Information security management systems – Requirements", the ISMS of the SE "DIIA" receives a Certificate of Conformity. In case of inspections by CA, the QTSP "Diia" receives an appropriate audit report drawn up by the Commission with the appropriate conclusions on the results of the audit.

6.6. Lifecycle safety control

6.6.1. Control of system development

During the development and implementation of the QTSP "Diia" ICS, the existing trends in the development of secure information technologies, known developments of the appropriate information security tools, requirements of the regulatory framework for technical information security shall be taken into account.

In order to protect information at all stages of the lifecycle, the QTSP "Diia" ICS shall provide for the application of the following measures and means of information protection:

- organisational and legal measures implemented outside the QTSP "Diia" ICS;

- engineering and technical measures implemented outside the QTSP "Diia" ICS;

– apparatus, hardware and software and hardware protection against unauthorised access to information processed and stored in the QTSP "Diia".

Information security software development and updates of its components are obtained directly from the developer. Downloading from the developer's official websites is allowed.

QTSP "Diia" receives the hardware of the security complex directly from the developer or from organisations that have appropriate licences to implement the complex of security tools of a complex of technical solutions.

6.6.2. Security management tools

Control over compliance with the security requirements in the QTSP "Diia" ICS is carried out by the Information Security Service of the QTSP "Diia", which is responsible for ensuring the protection of information in the ICS.

Support for the functioning and maintenance of the system is carried out by Administrators in accordance with their position responsibilities and the provisions of the ISMS document Regulation on the Applicability of Security Measures to the Information Security Management System of the SE "DIIA" DIIA/13 - ISMS - Org - SoA - Statement of Applicability (Version 1.1.), approved by the Order of the SE "DIIA" No. 20240605-1 dated June 05, 2024 "On Approval of Documents in

Accordance with the Minutes of the Commission on Implementation, Maintenance and Continuous Improvement of the Information Security Management System No. 5 dated May 02, 2024".

Monitoring of information on the state of functioning of the QTSP "Diia" ICS, such as data on the use of hardware resources, failures, malfunctions and problems in the operation of software and services, is carried out automatically. Administrators of the QTSP "Diia" receive notifications from the monitoring system in case of an emergency situation occurrence/elimination.

6.6.3. Lifecycle security control

QTSP "Diia" ensures that the equipment and workstations of the QTSP "Diia" ICS Administrators are timely upgraded and have the latest security updates.

6.7. Network security control

This section of the regulations is not included in the scope of provisions specified by the provider for users to review.

6.8. Electronic time stamps

6.8.1. Scope and Conformance

QTSP "Diia" provides a qualified electronic time-stamping service used to evidence the existence of electronic data at a specific moment in time. The service relies on the use of time synchronized with the national UTC(UA) time scale and implements the requirements of RFC 3161 (as updated by RFC 5816), ETSI EN 319 421 and ETSI EN 319 422.

6.8.2. Properties of a Qualified Electronic Time-Stamp

A qualified electronic time-stamp:

1. includes at least the following:

- a unique serial number;

- the date and time of generation together with the declared accuracy;

- the identifier of the time-stamp policy applied;

- a cryptographic hash of the electronic data to which the time-stamp relates;

- identifying information of QTSP "Diia", as contained in the certificate of the qualified electronic seal applied to the time-stamp, together with data allowing unambiguous identification of that certificate;

2. is generated using a private key dedicated exclusively to time-stamp generation;

3. ensures that any modification of the referenced electronic data without detection is highly improbable;

4. benefits from the presumption of the accuracy of the date and time indicated and the integrity of the associated electronic data.

6.8.3. Time Source and UTC Synchronisation

Time used for generating qualified time-stamps is synchronized exclusively using precise time signals provided by the Central Certification Authority, traceable to the national UTC(UA) time scale and synchronized with the State time and frequency standard.

The procedures for obtaining time signals, monitoring synchronisation, acceptable deviation limits and actions in case of deviations are defined in the UTC(UA) Synchronisation Procedure, approved by QTSP “Diia” and agreed with the Central Certification Authority.

6.8.4. Time-Stamp Issuance Process

The qualified electronic time-stamp is generated through the following steps:

- the user computes a cryptographic hash of the electronic data;

- the user submits a time-stamp request;

- QTSP “Diia” verifies the correctness of the request and the availability of the precise time source;

- QTSP “Diia” creates a structured time-stamp object linked to the hash value, the date and time of generation, and the applicable policy;

- the time-stamp is sealed using the qualified electronic seal dedicated for time-stamp generation;

- the resulting time-stamp or a reasoned refusal is returned to the user.

6.8.5. Relying Party Time-Stamp Validation

When validating a qualified time-stamp, the relying party performs at least:

- extraction of information on QTSP “Diia” and the certificate of the qualified electronic seal applied to the time-stamp;

- verification of the qualified electronic signature and construction of a valid certification path to a trusted root;

- confirmation that the certificate was valid and intended for “time-stamp generation” at the indicated generation time;

- verification that the hash of the electronic data matches the hash contained in the time-stamp;

- consideration of the time-stamp policy.

6.8.6. Invalidity Conditions

A time-stamp is considered invalid if:

- the certificate of the qualified electronic seal was expired, revoked, or compromised;

- the integrity of the time-stamp or its electronic seal has been compromised;

- the referenced electronic data have been altered, resulting in a hash mismatch.

6.8.7. TSU Keys, Certificates and Service Continuity

The private key dedicated to time-stamp generation is stored and used within a secure cryptographic device. Its certificate is designated for “time-stamp generation” and is valid for a period defined by the security policy.

QTSP “Diia”:

- ensures timely key and certificate rollover before the end of the key usage period;

- securely destroys outdated private keys;

- implements backup and recovery measures for the continuity of the time-stamping service;

6.8.8. Event Logging and Retention

QTSP “Diia” maintains logs of the time-stamping service containing at least:

- request/response processing data;

- information on incidents (equipment failures, key compromise, service suspension and restoration).

Log entries record time using the UTC(UA) scale.

7. PROFILES OF CERTIFICATES, LISTS OF REVOKED CERTIFICATES (CRL) AND ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

Requirements specified in the Clause 6.6 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

Certificate profiles declared for AATL use shall include Authority Information Access with a reference to QTSP "Diia’s" OCSP responder and CRL Distribution Points with a reference to QTSP "Diia’s" current CRL, both publicly accessible over HTTP.

Certificates declared for AATL use shall include the Certificate Policies extension with a QTSP "Diia" policy OID matching the relevant certificate profile/purpose. The extension shall include a CPS Pointer (cps) qualifier with a public HTTP link to the current CP/CPS.

For certificate profiles declared for AATL use, only RSA with SHA-256 or stronger and ECDSA with SHA-256 or stronger signature algorithms are permitted. SHA-1, DSTU 4145-2002 and GOST 34.311-95 shall not be used in certificate signatures or status service responses.

7.1. Certificate profiles

All user certificates generated by QTSP "Diia" are X.509 version 3 certificates, profiled in accordance with RFC 5280.

End-entity certificates for signers/seal creators contain a KeyUsage and ExtendedKeyUsage combination, as defined by RFC 5280, compatible with Adobe Acrobat/Reader. Specifically:

— keyUsage includes digitalSignature and, where applicable, nonRepudiation (contentCommitment);

— extendedKeyUsage includes object identifier 1.2.804.2.1.1.1.3.9, which indicates that the certificate is intended for electronic seals. In cases provided for by the requirements for separately defined information and telecommunications systems, in addition to the fact that the private key was

generated using a secure private key carrier (id-etsi-qcs 4), to identify the type of secure personal key carrier, when generating a qualified public key certificate, the provider sets an additional extension ‘Specified public key usage’ ‘extendedKeyUsage’ and a conditional designation of the type of such a carrier with its unique serial number in the additional data of the signatory.

The set of supported combinations is maintained per Adobe’s public guidance without altering any other provisions of this Certificate Policy.

Qualified certificates formed by QTSP “Diia” shall conform to the requirements of the following standards:

- DSTU ISO/IEC 9594-8:2021 (ISO/IEC 9594-8:2020, IDT) “Information technology. Interconnection of open systems. Part 8: Catalogue. Structure of certificates of public keys and attributes” (hereinafter referred to as ISO/IEC 9594-8:2020).
- DSTU ETSI EN 319 412-1 (ETSI EN 319 412-1 V1.4.4, IDT) “Electronic signatures and infrastructures (ESI). Certificate profiles. Part 1: Overview and typical data structures” (hereinafter referred to as ETSI EN 319 412-1).
- DSTU ETSI EN 319 412-2 (ETSI EN 319 412-2, IDT) “Electronic signatures and infrastructures. Certificate profiles. Part 2. Profiles of certificates issued to natural persons” (hereinafter - ETSI EN 319 412-2).
- DSTU ETSI EN 319 412-3 (ETSI EN 319 412-3, IDT) “Electronic signatures and infrastructures (ESI). Certificate profiles. Part 3. Profiles of certificates issued to legal entities”.
- DSTU ETSI EN 319 412-5 (ETSI EN 319 412-5, IDT) “Electronic signatures and infrastructures. Certificate profiles. Part 5. Qualified certificates”.
- DSTU ETSI TS 119 312 (ETSI TS 119 312, IDT) “Electronic signatures and infrastructures (ESI). Cryptographic sets”.
- DSTU 4145-2002 “Information technologies. Cryptographic protection of information. Digital signature based on elliptic curves. Formation and verification” (hereinafter - DSTU 4145-2002). With the function of hashing according to GOST 34.311-95 “Information technology. Cryptographic protection of information. Hashing function” or according to DSTU 7564-2014 “Information technology. Cryptographic protection of information. Hashing function”.

For preliminary checks during inclusion in third-party trust programs (including AATL), sample certificates and signed documents are provided by QTSP "Diia" to the operator of such trust program.

Fields and format of information contained in a qualified certificate:

Name	**Meaning**
Version	Version 3 (version 3) X.509 standard
Serial Number	Certificate number Value of this field is unique

Name	Meaning
Signature algorithm	Cryptographic algorithm Defines the algorithm used to sign a qualified certificate
Office of issue	Name of the provider forming the qualified certificate
Valid from	Validity date of the qualified certificate (in accordance with standard RFC 5280)
Valid until	Expiration date of the qualified certificate (in accordance with standard RFC 5280)
Topic	Information about the recipient of the qualified certificate (in accordance with standard RFC 5280) For more details, see the Clause 3.1.1
Public key	Public key that corresponds to the private key of the qualified certificate (in accordance with standard RFC 5280)
Signature	Qualified electronic signature of the QTSP “Diia”, which provides the service of creating, verifying and confirming a qualified electronic signature or seal Generated and encoded in accordance with standard RFC 5280.

All user certificates generated by QTSP "Diia" are X.509 version 3 certificates, profiled in accordance with RFC 5280.

7.2. Profiles of lists of the revoked certificates (CRL)

Lists of the revoked certificates (CRLs) formed by the QTSP “Diia” shall conform to the following standards:

- DSTU ISO/IEC 9594-8:2021 (ISO/IEC 9594-8:2020, IDT) “Information technology. Interconnection of open systems. Part 8: Catalogue. Structure of certificates of public keys and attributes” (hereinafter referred to as ISO/IEC 9594-8:2020).
- RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

Information format in the CRL published by QTSP “Diia” conforms to the standard ITU-T X.509 and RFC 5280. CRL shall have at least the following fields:

Name	Meaning
Version	Version CRL (version 2).

Name	Meaning
Office of issue	Name of the Provider forming the CRL
Effective date	Current date of issue (update) of the CRL
Next update	Date of the next CRL update
Cancelled certificates	This field contains information about cancelled qualified certificates, in particular: - serial number (serial number of the cancelled qualified certificate); - cancellation date (time when the qualified certificate was cancelled); - cancellation record (extended information of the cancelled qualified certificate (optional field)
Signature algorithm	Algorithm used to sign CRL
Hashing signature algorithm	Hashing algorithm
Signature	Value of the digital signature from the provider
CRL extension	Other extended information (optional field)

7.3. Online certificate status protocol (OCSP) profiles

Information dissemination on the status of user qualified certificates is carried out by creating the possibility of verifying the status of a user qualified certificate in real time through public electronic communication networks using the OCSP protocol.

Links to the service for verifying the status of a user qualified certificate in real time are included in user's qualified certificates.

Procedure for interactive definition of the certificate status and data formats shall conform to the requirements of the following standards:

- ISO/IEC 8825-1:2002 "Information technology - ASN.1 Encoding Rules - Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).
- RFC 2560 "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP".

7.4. Certificate Policy and OID for AATL

Qualified certificates intended for AATL shall include OID AATL-EE in the certificatePolicies extension. The use of OID AATL-EE in certificates that do not meet AATL end-entity requirements is prohibited. The QTSP ‘Diia’ does not issue certificates to other certification authorities (CAs); AATL ICA1(b) is not applicable.

7.5. Profile of the Issuing Certification Authority (ICA) certificate of the QTSP ‘Diia’

7.5.1. General requirements

The ICA certificate of the QTSP ‘Diia’ shall be an X.509 version 3 certificate profiled in accordance with RFC 5280; the encoding shall be DER; the serial number shall be unique within the issuer’s namespace.

7.5.2. Subject and Issuer names

Names shall follow ITU-T X.500/X.520 and RFC 5280; the organization identification attributes shall reflect Ukrainian law requirements and the QTSP ‘Diia’ internal identifiers.

7.5.3. Mandatory X.509 v3 extensions for the ICA certificate

a) basicConstraints — CA=TRUE (critical); pathLenConstraint=0 (the QTSP ‘Diia’ does not issue certificates to other CAs).
b) keyUsage — (critical) at least keyCertSign, cRLSign.
c) subjectKeyIdentifier (SKI) — (non-critical).
d) authorityKeyIdentifier (AKI) — (non-critical).
e) authorityInfoAccess (AIA) — (non-critical) including at least id-ad-ocsp (OCSP URL) and, where applicable, id-ad-caIssuers (issuer’s certificate URL).
f) crlDistributionPoints (CDP) — (non-critical) with the CRL distribution URL for the ICA.
g) certificatePolicies — (optional) including the OID of the QTSP ‘Diia’ Certificate Policy 1.2.804.2.1.1.1.2.4 and, where applicable, a CPS/Policy URI (link to the published document).

7.5.4. Algorithms and hash functions

Signature and hash parameters shall comply with RFC 5280 and the QTSP ‘Diia’ crypto policies; the use of SHA-1 for new ICA certificates is not permitted.

7.5.5. Status checking and revocation

The ICA certificate shall include references to OCSP and CRL services operating in accordance with RFC 5280 and this Policy (see paras. 7.2 and 7.3).

7.5.6. Subject name attributes for the ICA certificate

The ICA certificate Subject shall include the organizationName attribute (per ITU-T X.520) containing the full registered name of the QTSP “Diia” (exactly as notified to Adobe).

Where an official registration number exists, the organizationIdentifier (X.520) shall be added to the Subject with that number; the value format shall follow ETSI EN 319 412-1 (schemes NTR/VAT/LEI/… with the two-letter country code UA for Ukraine; e.g., NTRUA-<EDRPOU>).

Scheme guidance: use NTR for the national trade/business register (EDRPOU), LEI if a Legal Entity Identifier exists; other schemes defined by ETSI EN 319 412-1 are permitted.

The values of organizationName and, where present, organizationIdentifier shall be consistent with QTSP “Diia” public documentation and identical to the data notified to Adobe for AATL participation.

7.5.7. Environment and operations for the QTSP ‘Diia’ certificate private key

The environment for generation, storage and use of the QTSP ‘Diia’ certificate private key, and the performance of cryptographic operations, shall be as defined in para. 6.2.12 of this Policy; a

Hardware Security Module (HSM) at least FIPS 140-2 Level 3 or equivalent shall be used, and export/duplication of the private key that could lead to unauthorized use is prohibited.

Certificate/CRL signing shall be performed within the HSM and in accordance with the procedures for generation, initialization and activation of the QTSP ‘Diia’ key.

Backup/recovery of the QTSP ‘Diia’ certificate private key is only allowed as specified in para. 6.2.12 of this Policy.

8. CONFORMITY AUDITS AND OTHER ASSESSMENTS

Requirements specified in the Clause 6.7 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

8.1. Frequency or circumstances of the assessment

It is not allowed to provide qualified electronic trust services without valid documents specified by the legislation confirming the conformity of the QTSP “Diia” ICS and the information security tools in its composition to the requirements of legislative and regulatory acts in the field of technical and cryptographic information protection, or documents of conformity, based on the results of the conformity assessment procedure, in the field of electronic trust services.

QTSP “Diia” is supervised by the CA, the functions of which are carried out by the Administration of the State Service of Special Communications and Information Protection of Ukraine.

In cases defined by the law, the CA may:

1) conduct an unscheduled inspection of the provider’s conformity to the requirements of the legislation in the field of electronic trust services:

- according to its statement;
- in case of detection and confirmation of inaccurate information in the documents submitted by it;
- upon receipt of information or notification of a violation of the requirements of the legislation in the field of electronic trust services from the CCA, court, users or third parties;
- by a reasonable decision of the CA.

CA does not carry out scheduled control measures.

2) submit a request to the CAA to provide an audit report on the provider’s conformity assessment procedure at the expense of the provider to confirm that it and the electronic trust services it provides conform to the requirements in the field of electronic trust services.

Provider shall notify the CA of the results of the conformity assessment by providing a copy of the conformity document no later than three working days from the date of its receipt.

QTSP "Diia" undergoes an independent conformity assessment (audit) at least once every 24 months under a recognized scheme ETSI EN 319 411-1 and/or ETSI EN 319 411-2 (or an equivalent scheme such as WebTrust for CA or ISO 21188:2006), performed by a Conformity Assessment Body accredited to ISO/IEC 17065 and ETSI EN 319 403.

Upon request, a valid certificate/report of the assessment is provided.

The latest conformity assessment of QTSP ‘Diia’ against ETSI EN 319 411-1/-2 was successfully passed on 05.03.2025 by the accredited CAB TAYLLORCOX s.r.o. (TAYLLORCOX PCEB, CAB No. 3239); Certificate ID: PCEB 25/03/05, valid until 04.03.2027.

Conformity assessment is carried out by the CAA as specified in the Section 8.2 of this Policy of the Certificate.

QTSP “Diia” undergoes conformity assessment in accordance with the requirements:

- DSTU ETSI EN 319 401;
- DSTU ETSI EN 319 411-1;
- DSTU ETSI EN 319 411-2.

Certificate of conformity of the QTSP “Diia” ICS to the requirements of ISO/IEC 27001:2022 “Information security, cybersecurity and privacy protection - Information security management systems – Requirements”, received as a result of the certification procedure, and is valid for the period specified in the Certificate.

8.2. Appraiser’s identity/qualifications

8.2.1. Qualification requirements for the Controlling Authority (CA)

Functions of the CA are performed by the State Service of Special Communications and Information Protection of Ukraine.

Off-site unscheduled state supervision (control) over compliance with the requirements of the legislation in the field of electronic trust services (hereinafter referred to as the inspection) is carried out by the officials of the CA in accordance with their functional responsibilities at the location of the QTSP “Diia”.

Audit is carried out in accordance with the decision of the CA.

Decision to conduct an audit shall include:

1) name of the Administration of the State Service of Special Communications and Information Protection of Ukraine;
2) name of the provide,
3) location of the provider;
4) reasons for the audit;
5) subject of audit;
6) dates of the start and end of the audit;
7) official and personal composition of the audit commission.

8.2.2. Qualification requirements for a Conformity Assessment Authority (CAA)

CAA is an enterprise, institution, organisation or its structural subdivision that carries out conformity assessment activity in the field of electronic trust services and is accredited by a national accreditation authority or a foreign accreditation authority that is a signatory to a multilateral recognition agreement of the International Accreditation Forum and/or the European Cooperation for Accreditation (EA MLA).

The conformity assessment of QTSP "Diia" against the ETSI EN 319 411 series shall be performed by a CAA that is independent from QTSP ‘Diia’ and accredited to ISO/IEC 17065 and ETSI EN 319 403 to conduct audits under the relevant scheme (ETSI EN 319 411-1 / ETSI EN 319 411-2).

CAA shall comply with the provisions defined in DSTU ETSI EN 319 403-1 (ETSI EN 319 403-1, IDT) “Electronic Signatures and Infrastructures (ESI). Conformity assessment of trust service providers. Part 1: Requirements for conformity assessment authorities that assess trust service

providers", approved by the Order of the State Enterprise "Ukrainian Research and Training Centre for Standardisation, Certification and Quality Problems" No. 512 dated December 16, 2021.

8.3. Relations between the expert and the object of assessment

8.3.1. Relations between officials of the Controlling Authority (CA) and the object of assessment

In accordance with the Part six of the Article 4 of the Law of Ukraine "On Basic Principles of State Supervision (Control) in the Field of Business Activity", an official of a state supervision (control) authority is prohibited from exercising state supervision (control) over business entities with which (or whose officials) the official has a family tie or in case of the conflict of interest in accordance with the legislation on preventing and combating corruption.

Participants of the Audit Commission are obliged to:

- conduct the audit objectively and impartially;
- comply with the requirements of the legislation in the fields of electronic identification, electronic trust services, information security and personal data protection;
- perform their official duties and the instructions of the Head of the Audit Commission in good faith, in a timely and high-quality manner;
- follow business ethics in relations with the Head and personnel of the QTSP "Diia";
- familiarise the QTSP "Diia" Head or his/her authorised representative with the results of the audit;
- provide advisory assistance to the QTSP "Diia" on the issues of the audit;
- not to disclose restricted information that they have become aware of in connection with the performance of their official duties.

8.3.2. Relations of experts (auditors) conducting conformity assessment with the object of assessment

The assessment is performed by an independent CAA and engaged auditors acting within the CAA's scope of accreditation. The CAA and the auditors shall not have employment, corporate, contractual or other relationships that create a conflict of interest with QTSP "Diia" (State Enterprise "DIIA"), its personnel, or related parties/contractors. Audit activities are carried out solely on behalf of, and under the responsibility of, the CAA.

8.4. Topics covered by the assessment

8.4.1. Issues subject to audit during state control

Object of the audit carried out by the CA is the state of conformity to the requirements of the legislation in the field of electronic trust services, including this Policy of the Certificate and the relevant Certification Practices on the following issues:

- general requirements;
- ensuring the security of information resources;
- human resources;
- exploitation of tools of qualified electronic signature or seal;
- requirements for the provision of electronic trust services;

- Policy of the Certificate;

- provisions of Certification Practices;

- provision of a qualified electronic trust service for the creation, verification and confirmation of qualified electronic signatures or seals;

- ensuring the security of physical access to the premises.

The minimum audit scope covers:

– overall CA operations (network, physical security, HR, and other general functions);

– registration services (RA);

– revocation management;

– dissemination/publication services;

– certificate status information services;

– subject device provisioning;

– certificate generation services.

8.4.2. Issues subject to verification during the conformity assessment

Object of conformity assessment conducted by the CAA is the state of conformity to the requirements of DSTU ETSI EN 319 401.

8.5. Actions taken as a result of the violation

8.5.1. Actions taken as a result of a violation detected by the state control results

When carrying out measures of state supervision (control) over compliance with the requirements of the legislation in the field of electronic trust services, the officials of the CA have the right to:

- carry out on-site and off-site measures of state supervision (control) over compliance with the requirements of the legislation in the fields of electronic identification and electronic trust services;
- in case of violations of the requirements of the legislation in the fields of electronic identification and electronic trust services, issue binding prescripts to eliminate violations and define the timeframe for eliminating the identified violations;
- impose administrative penalties on perpetrators for violations of the Law of Ukraine “On Electronic Identification and Electronic Trust Services” and other regulatory and legislative acts adopted in accordance with this Law;
- apply to the court for the use of response measures;
- carry out other powers defined by the law.

Based on the results of the audits, the CA takes the following response measures:

1) demands that the QTSP “Diia” eliminate violations of the requirements of the legislation in the field of electronic trust services within the time limit established by the prescript;

2) makes a decision to block the qualified certificate of the QTSP “Diia” if during the verification there is a suspicion of compromising the private key;

3) makes a decision to cancel the qualified certificate of the QTSP “Diia” if the fact of compromise of the private key is revealed during the verification.

Decision to block or cancel the qualified certificate of the QTSP “Diia” shall be sent by the CA to the CCA on the day of its decision;

4) sends a request to the CCA to revoke the status of a Qualified Trust Service Provider or a service provided by the QTSP “Diia” in the Trust List in case of:

- provision of qualified electronic trust services by the provider without valid documents required by the legislation confirming conformity to the requirements of ISO standards in the field of ISMS and information security tools within it with the requirements of legislative and regulatory acts in the field of technical and cryptographic information protection, or documents of compliance based on the results of the conformity assessment procedure in the field of electronic trust services;
- provision of qualified electronic trust services in the absence of a current account of QTSP “Diia” with a special regime of use in a bank (account with the authority that provides treasury services for budgetary funds) with the required amount of funds or a valid civil liability insurance agreement with the required amount of insurance established by the Law of Ukraine “On Electronic Identification and Electronic Trust Services” to ensure compensation for losses that may be caused to users of electronic trust services or to third parties as a result of improper fulfilment of the obligations by the Provider;
- violation of the requirements for the exploitation of the ISMS of the QTSP “Diia” ICS;
- provision of qualified electronic trust services by the QTSP “Diia” without valid documents specified by the legislation confirming its ownership and/or the right to use the tools of a qualified electronic signature or seal used to provide qualified electronic trust services;
- establishing the fact of providing false information provided in the documents submitted by the QTSP “Diia” for entering information about it into the Trust List;
- failure to eliminate the violations identified during the inspection within the time limit established by the prescript;
- blocking or cancellation of the QTSP “Diia” qualified certificate.

8.5.2. Actions taken as a result of a violation identified in the course of a conformity assessment

Based on the results of the conformity assessment procedure in the field of electronic trust services, the CAA shall make one of the following decisions:

- on conformity of the object of conformity assessment to the requirements in the field of electronic trust services in full;
- non-conformity of the object of conformity assessment to the requirements in the field of electronic trust services.

In case of a decision on non-conformity of the object of conformity assessment to the requirements in the field of electronic trust services, the CAA shall issue an audit report to the customer of the conformity assessment procedure with conclusions on non-conformity and a list of deficiencies.

Results of the conformity assessment in the fields of electronic identification and electronic trust services are analysed by the CA. In case of negative results of the conformity assessment and/or recommendations provided by the conformity assessment authority, the controlling authority may, by its decision, appoint an additional conformity assessment after eliminating all the deficiencies indicated in the audit report.

CA shall send a request to the CCA to revoke the status of a provider or a service provided by a provider in the Trust List in case of:

- provision of qualified electronic trust services by the provider without valid documents required by legislation confirming conformity to the requirements of ISO standards in the field of ISMS and information security tools as part of it with the requirements of legislative and regulatory acts in the field of technical and cryptographic information protection, or documents of conformity based on the results of the conformity assessment procedure in the field of electronic trust services.

8.6. Reporting the results

8.6.1. Presentation of state control results

Results of the provider's audit shall be presented by the Audit Commission by drawing up an audit report, the form of which shall be approved by the CA.

The audit report shall contain the following information:

- name of the CA;
- Personal and official composition of the Audit Commission;
- surname and initials of the Head of the Provider;
- details of the license for the audit conduction;
- dates of the start and end of the audit;
- address of the Provider's premises where the audit was carried out;
- results of the previous audit;
- information on the results of the last conformity assessment in the field of electronic trust services preceding the audit;
- title and summary of the documents provided during the audit;
- qualitative and quantitative indicators established during the audit that characterise the activity of the Provider related to the provision of electronic trust services;
- violations and deficiencies identified during the audit (if any) and the Provider's explanation of the reasons for non-conduction of the requirements established by the legislation (if any);
- conclusions based on the audit results;
- facts of prevention to the audit conduction (if any);
- recommendations for eliminating the identified violations (if any);
- date of drawing up the audit report;
- signatures of the Chairperson and participants of the Audit Commission;
- signature of the Provider's Head or authorised representative confirming the fact of familiarisation with the audit report.

Audit report shall be drawn up in two copies and signed no later than the last day of the audit by the Chairperson and all participants of the Audit Commission and the head of the provider or his/her authorised representative.

Participant of the Audit Commission who does not agree with the conclusions of the Audit Commission stated in the audit report shall sign it and state his/her dissenting opinion in writing, which shall be attached to the audit report. In this case, before signing the audit report, it shall be indicated "With dissenting opinion attached".

If the Head of the Provider or his/her authorised representative has any comments on the facts and conclusions set out in the inspection report, the following words shall be written before the signature: “With the attached comments”.

Comments to the audit report shall be drawn up as a separate document and signed by the Head of the Provider or authorised representative.

Comments on the audit report and the dissenting opinion of a participant of the Audit Commission shall be integral parts of the audit report.

If the Head of the Provider or his/her authorised representative refuses to read the inspection report or sign it after reading it, the Chairperson of the Audit Commission shall make a corresponding note in front of the place for signature of the Head of the Provider or his/her authorised representative, which shall be certified by the signatures of the Head and one of the participants of the Audit Commission.

8.6.2. Prescript on eliminating violations identified during state control

When carrying out the measures of state supervision (control) over conformity to the requirements of the legislation in the field of electronic trust services, the officials of the CA have the right to issue binding prescripts to eliminate violations and determine the time limit for eliminating the identified violations in case of identification of violations of the legislation in the field of electronic trust services.

Prescript on eliminating violations shall be drawn up by the Audit Commission in two copies within five business days after the completion of the audit. One copy of the prescript shall be provided to the Provider no later than five business days after the date of the audit report, and the second copy signed by the Head of the Provider or authorised representative regarding the agreed terms for eliminating violations of the requirements of the legislation in the field of electronic trust services shall remain with the CA.

Form of the prescript on eliminating violations is approved by the CA.

Prescript on eliminating violations is signed by the Chairperson and Participants of the Audit Commission who conducted them.

In case the Head of the Provider or his/her authorised representative refused to receive the prescript on eliminating violations, such a prescript shall be sent by registered mail, and the copy of the prescript that remains with the CA shall bear the relevant outgoing number and date of sending.

Head of the Provider shall take measures to eliminate the deficiencies and violations specified in the prescript on eliminating violations within the period specified in the prescript.

Provider is obliged to submit in writing to the CA information on the elimination of violations together with supporting documents within the period specified in the prescript on eliminating violations.

8.6.3. Presentation of the results of conformity assessment

Conformity document shall contain the following information:

- name of the CAA;
- information on CAA accreditation (date and number of the Accreditation Certificate);
- Surname, name, patronymic (if any) of the persons who conducted the conformity assessment procedure;
- period of the conformity assessment procedure;
- Provider’s details (name, identification data and contact information);

- scope of conformity assessment;
- a list of qualified electronic trust services to be provided by the QTSP “Diia”;
- name of the ICS;
- name of the qualified electronic signature tools used in the provision of qualified electronic trust services;
- a list of requirements in the field of electronic trust services, national standards and/or technical specifications for conformity to which the conformity assessment procedure was carried out;
- conclusion on conformity to the requirements in the field of electronic trust services;
- validity of the conformity document.

Results of the scheduled and repeated (unscheduled) conformity assessment procedure in the field of electronic trust services shall be reported by the providers to the CA by providing copies of conformity documents (if any) and audit reports no later than three business days from the date of their receipt. The assessment results shall explicitly state conformance to ETSI EN 319 411-1/-2 and include the date/period evidencing the 24-month window.

CAA provides public access to current information on the results of conformity assessment in the field of electronic trust services.

8.7. Self-checks

During the period of certificate formation, QTSP “Diia” controls compliance with this Policy of the Certificate and the appropriate Certification Practices, strictly controlling the quality of its services, performing self-checks from time to time, issuing certificates.

QTSP “Diia” conducts regular internal audits to assess compliance with requirements of the legislations, internal policy and requirements of this Policy of the Certificate and the appropriate Regulation on Certification Practices at least once a year.

9. OTHER COMMERCIAL AND LEGAL ISSUES

Requirements specified in the Clause 6.8 of ETSI EN 319 411-1 and ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

9.1. Charges

9.1.1. Fee for issuing or renewing a certificate

Fee for the issuance of a qualified certificate shall be made, the cost of which shall be defined in accordance with the tariff plans for the provision of qualified electronic trust services of the QTSP “Diia” published on the QTSP “Diia” website at the following link: https://ca.diia.gov.ua.

In the case of provision of qualified electronic trust services through separate registration units of the QTSP “Diia”, an additional fee may be charged for the provision of qualified electronic trust services.

Renewal of blocked qualified certificates is free of charge.

Appropriate Regulations on Certification Practices of the Qualified Trust Service Provider “Diia” on the Qualified Certificates of Electronic Signature and Seal (Annex 2 to these Rules and Regulation) contain additional information.

9.1.2. Certificate access fee

There is no fee for access to a qualified certificate.

9.1.3. Fee for blocking/cancellation or access to certificate status information

There is no fee for blocking/cancelling a qualified certificate or access to information on the status of a qualified certificate.

9.1.4. Fee for other services

QTSP “Diia” may provide users with additional services for a fee, including:

- providing tools of qualified electronic signature or seal to users;
- off-site generation of a user key pair;
- storage of private keys in the cloud storage of QTSP “Diia”.

9.1.5. Refund Policy

QTSP “Diia” does not refund paid invoices for services rendered.

9.2. Financial responsibility

Activity of the QTSP “Diia” complies with the requirements of Part five of the Article 16 of the Law of Ukraine “On Electronic Identification and Electronic Trust Services” regarding the provision of qualified electronic trust services, subject to the deposit of funds to a current account with a special regime of use in a bank (an account with an authority that provides treasury services for budgetary funds) or civil liability insurance to ensure compensation for damage that may be caused to users of such services or third parties. Amount of the contribution on the current account with a special regime of use in the bank (account with an authority that provides treasury services for budgetary funds) or the sum insured may not be less than 1 thousand minimum salaries.

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

In the process of providing services, QTSP “Diia” processes confidential information that is not made public. Protection of confidential information is carried out in accordance with the current legislation.

9.3.2. Information that is not confidential

Information and documentation that is available for public awareness is published on the QTSP “Diia” website and is not considered confidential.

9.3.3. Responsibility for the protection of confidential information

QTSP “Diia” protects confidential information and is responsible in accordance with the requirements of the current legislation.

9.4. Confidentiality of personal data

9.4.1. Personal data protection concept

In the process of providing qualified electronic trust services, QTSP “Diia” carries out the following:

protection of users’ personal data in accordance with the requirements of the Law of Ukraine “On Personal Data Protection”;

informing the CA and, if necessary, the personal data protection authority of violations of confidentiality and/or integrity of information affecting the provision of qualified electronic trust services or relating to users’ personal data without unreasonable delay, no later than 24 hours after becoming aware of such a violation;

informing users about violations of confidentiality and/or integrity of information that affect the provision of electronic trust services to them or relate to their personal data without unreasonable delay, but no later than two hours from the moment they become aware of such a violation.

9.4.2. Definition of personal data

The term “personal data” shall be understood in the meaning given in the Article 2 of the Law of Ukraine “On Personal Data Protection”.

9.4.3. Personal data that is not considered confidential

Personal data may be classified as open information in cases defined by the current legislation.

9.4.4. Responsibility for the protection of personal data

QTSP “Diia” guarantees compliance with the requirements of the legislation on personal data protection and is responsible in accordance with the requirements of the current legislation.

Head of the specialised subdivision of the QTSP “Diia” ensures the creation of conditions for continuous personal education and continuous professional development of the QTSP “Diia” personnel in the fields of information technology, information and personal data protection.

9.4.5. Information and consent to the use of personal data

In accordance with the Law of Ukraine “On Personal Data Protection”, the QTSP “Diia” provides qualified trust services in accordance with the agreement concluded with the user and processes the user’s personal data within the framework of the agreement or for the implementation of measures preceding the conclusion of the agreement at the request of the user.

9.4.6. Personal data disclosure

QTSP “Diia” provides access to personal data of users only in cases stipulated by the Law of Ukraine “On Personal Data Protection”.

Head of the specialised subdivision of the QTSP “Diia” and QTSP “Diia” personnel comply with the requirements of the legislation of Ukraine in the field of personal data protection and sign a confidentiality and non-disclosure agreement.

9.5. Intellectual property rights

Issues related to intellectual property rights of the QTSP “Diia” are regulated in accordance with the requirements of the current legislation of Ukraine.

9.6. Obligations and guarantees

9.6.1. Obligations and guarantees of the Provider

QTSP “Diia” provides qualified electronic trust services in compliance with the requirements of the legislation in the field of electronic trust services, this Policy of the Certificate and the appropriate Regulations on Certification Practices.

9.6.2. Obligations and guarantees of separate registration units

On the basis of an agreement concluded with the QTSP “Diia” (SE “DIIA”), users are registered by separate registration units of the QTSP “Diia”, which perform their functions in accordance with this Policy of the Certificate and the appropriate Regulations of Certification Practices.

The same requirements are applied to the employees of the separate registration units of the QTSP “Diia”, who are responsible for registering users, as to the Registration Administrators of the QTSP “Diia”.

9.6.3. Obligations and guarantees of users

QTSP “Diia” provides users with the ability to sign and verify signed files using signature and signature verification widgets and specialised software available on the website https://ca.diia.gov.ua.

Users are obliged to:

- ensure confidentiality and impossibility of access to the private key by other persons;
- immediately notify the QTSP “Diia” of any suspicion or fact of compromise of the private key;
- provide reliable information necessary to receive electronic trust services;
- timely pay for electronic trust services, if such payment is provided for in the agreement between QTSP “Diia” and the user;
- timely provide QTSP “Diia” with information on changes in the identification data contained in the qualified certificate;
- not to use a private key in case of its compromise, as well as in case of cancellation or blocking of a qualified certificate.

User guarantees that:

- for signing, uses a private key that corresponds to the public key in a qualified certificate;
- at the time of signing, the qualified certificate is valid (not in the status of blocked or cancelled);
- the private key and its password are not compromised and are not used by other persons;
- all information specified in the qualified certificate is correct;
- qualified certificate is used for its intended purpose, in accordance with the provisions of this Policy of the Certificate;
- additional terms and conditions may be included in the agreement for the provision of electronic trust services. The content of the agreement for the provision of electronic trust services is published on the QTSP “Diia” website ca.diia.gov.ua.

9.6.4. Obligations and guarantees of entities that trust the Provider

Entity that trusts the QTSP “Diia” shall verify the validity of the qualified certificate formed by the QTSP “Diia” using the services of verification and confirmation of electronic signature or seal before using the qualified certificate.

9.6.5. Obligations and guarantees of other parties

Before making a decision to include the QTSP “Diia” in the Trust List and grant it qualified status, the CCA made sure that the QTSP “Diia” has:

- document confirming the compliance of the information security system of the QTSP “Diia” with the requirements of the Article 8 of the Law of Ukraine “On Information Protection in Information and Communication Systems”;
- documents confirming the right of ownership and the right to use non-residential premises used by the QTSP “Diia” to place all components of the software and hardware complex that ensure the provision of qualified electronic trust services;
- proper personnel of the QTSP “Diia”;

- documents confirming the educational qualification level and three years of work experience in the speciality of the personnel of the QTSP “Diia”;
- documents confirming the right of ownership or the right to use the tools of a qualified electronic signature or seal used by the QTSP “Diia” to provide qualified electronic trust services;
- documents confirming the deposit of funds to the current account of the QTSP “Diia” with a special regime of use in a bank (an account with the authority that provides treasury services for budgetary funds) to ensure compensation for losses that may be caused to users as a result of improper performance of the QTSP “Diia” of its obligations;
- this Policy of the Certificate and the appropriate Regulations on Certification Practices;
- data on separate registration units and their employees whose obligations will be directly related to the provision of qualified electronic trust services.

9.7. Waiver of guarantees

QTSP “Diia” does not provide any guarantees regarding the services provided by it, except for those clearly defined in the Clause 9.7.1 of this Policy of the Certificate.

9.8. Limitation of liability

In case the QTSP “Diia” duly notifies users in advance of restrictions on the use of electronic trust services provided by it, provided that such restrictions are clear to users, it shall not be liable for damage caused by the use of electronic trust services in violation of such restrictions.

9.9. Compensation for losses

Compensation for losses that may be caused to users of electronic trust services or third parties as a result of improper fulfilment of the obligations by the QTSP “Diia” is carried out in accordance with the requirements of the current legislation of Ukraine.

9.10. Validity and termination

This Policy of the Certificate applies from the moment of its publication and is valid until the expiration of the last certificate issued in accordance with this Policy of the Certificate or until the termination of the activity of the QTSP “Diia”.

9.11. Individual notifications and communications with public key infrastructure participants

QTSP “Diia” communicates with participants of the public key infrastructure by:
- posting notifications and announcements on the QTSP “Diia” website;
- informing the CCA, CA and the personal data protection authority by sending notifications in paper and electronic forms;
- sending emails to the user’s email address;
- making phone calls and SMS notifications to the user’s phone number.

9.12. Amendments

Amendments to this Policy of the Certificate shall be made by the QTSP “Diia” in case of:
- amendments to the requirements, processes and procedures described in this Policy of the Certificate;
- amendments to the legislation;
- amendments to the requirements for service providers;
- amendments to the AATL Technical requirements.

New versions of this Policy of the Certificate shall be published on the website of the QTSP "Diia" after amendments are made to it.

Any amendments not mentioned in the history of this Policy of the Certificate are grammatical and spelling changes that do not affect the essence and do not relate to the processes and procedures described in this Policy of the Certificate.

9.13. Dispute resolution provisions

In case of any disputes or disagreements, the QTSP "Diia" (SE "DIIA") shall resolve them through negotiations and consultations with the participants of the public key infrastructure.

If the participants of the public key infrastructure fail to reach an agreement, disputes (disagreements) shall be resolved in court in accordance with the current legislation of Ukraine.

9.14. Applicable law

Relations governed by this Policy of the Certificate are subject to the current legislation of Ukraine.

9.15. Compliance with the current legislation

When providing electronic trust services, QTSP "Diia" shall comply with the following requirements:

- Law of Ukraine "On Electronic Identification and Electronic Trust Services";
- Law of Ukraine "On Protection of Information in Information and Communication Systems";
- Law of Ukraine "On Personal Data Protection";
- Resolution of the Cabinet of Ministers of Ukraine No. 55 dated January 27, 2010 "On Streamlining the Transliteration of the Ukrainian Alphabet into Latin";
- Resolution of the Cabinet of Ministers of Ukraine No. 798 dated August 01, 2023 "On Approval of the Procedure for the Use of Electronic Trust Services in State Authorities, Local Self-Government Authorities, Enterprises, Institutions and Organisations of State Ownership";
- Resolution of the Cabinet of Ministers of Ukraine No. 1137 dated December 04, 2019 "Issues of the Unified State Web Portal of Electronic Services and the Register of Administrative Services";
- Resolution of the Cabinet of Ministers of Ukraine dated 10.12.2024 No. 1408 "Some issues of storing documented information and its transfer to the central certification body in the event of termination of the activities of a qualified provider of electronic trust services";
- Resolution of the Cabinet of Ministers of Ukraine No. 764 dated June 28, 2024 "Some Issues of Compliance with Requirements in the Fields of Electronic Identification and Electronic Trust Services";
- Resolution of the Cabinet of Ministers of Ukraine No. 1215 dated December 18, 2018 "On Approval of the Procedure for Conducting a Conformity Assessment Procedure in the Field of Electronic Trust Services";
- Resolution of the Board of the National Bank of Ukraine No. 32 dated March 17, 2020 "On Approval of the Regulation on the BankID System of the National Bank of Ukraine";
- Order of the Ministry of Justice of Ukraine, the Administration of the State Service of Special Communications and Information Protection of Ukraine No. 316/5/57 dated February 01, 2019

"On Marking a Qualified Certificate of Public Key", registered with the Ministry of Justice of Ukraine under No. 123/33094 on February 05, 2019;

- Order of the Ministry of Digital Transformation of Ukraine No. 149 dated November 17, 2023 "On Approval of the Procedure for Maintaining the Register of Valid, Blocked and Cancelled Public Key Certificates Formed by the Central Certifying Authority", registered with the Ministry of Justice of Ukraine under No. 2110/41166 on December 05, 2023;
- Order of the Ministry of Digital Transformation of Ukraine No. 125 dated August 25, 2020 "On the Requirements for the Format of Registers of Formed Qualified Certificates of Public Keys, as well as Information Media and the Procedure for Recording Documents in Electronic Form", registered with the Ministry of Justice of Ukraine under No. 1086/35369 on November 06, 2020;
- Order of the Ministry of Digital Transformation of Ukraine No. 54 dated April 06, 2024 "On Approval of the Form of the Plan for Termination of Activity for the Provision of Qualified Electronic Trust Services", registered with the Ministry of Justice of Ukraine under No. 588/41933 on April 23, 2024;
- Order of the Ministry of Digital Transformation of Ukraine No. 33 dated February 28, 2024 "On Approval of the Rules and Procedures of the Central Certifying Authority", registered with the Ministry of Justice of Ukraine under No. 393/41738 on March 15, 2024;
- Order of the Ministry of Digital Transformation of Ukraine No. H191 dated December 28, 2023 "Some Issues of Implementation of Standards Requirements, Including Interoperability".

9.16. Other provisions

9.16.1. AATL membership and conformance obligations.

QTSP "Diia", in the context of the AATL Technical Requirements, operates as an Issuing Certification Authority (Issuing CA; (I)CA). Within the scope of this Policy, an upper-level/root CA (RCA/upper CA) is not used; therefore, the AATL Technical Requirements G12 and RCA1–RCA9 do not apply to QTSP "Diia".

The obligations regarding conformance to the AATL Technical Requirements take effect from the effective date of the AATL Membership Agreement.

QTSP "Diia" ensures continuous conformance with the current edition of the AATL Technical Requirements for the entire term of the AATL Membership Agreement.

QTSP "Diia" provides Adobe with this Certificate Policy and the Certification Practice Statements as part of participation in the AATL (upon request / during the initiation of membership / for attestations).

QTSP "Diia" maintains a self-assessment of conformity with the AATL Technical Requirements together with supporting evidence (kept up to date as needed and prior to submissions to Adobe).

Under AATL obligations, QTSP "Diia" shall provide the audit report to Adobe no later than three (3) months after the end of the audit period; if the delay exceeds three months, an explanatory letter signed by the qualified auditor shall be provided.

Adobe notification in case of incidents and subsequent reporting shall be performed in accordance with clause 5.7.1 of this Certificate Policy and clause 7.6 of the Incident Management Policy (DIIA/13 – ISMS – Org – PL/4).

Detailed information and the remediation/action plan shall be provided to Adobe within the time and in the manner set out in clause 5.7.1 of this Certificate Policy and clause 7.6 of the Incident Management Policy (DIIA/13 – ISMS – Org – PL/4).

QTSP “Diia” shall notify Adobe at least one (1) month in advance of changes concerning:

a) the PKI hierarchy of QTSP “Diia”;

b) the Certificate Policies (CP) and the Certification Practice Statements (CPS);

c) certificate issuance procedures (including registration, provisioning/use of devices where the end-entity private key resides, and revocation procedures), as well as termination or handover of services.

The notification shall be sent to AATLNotification@adobe.com (or another address designated by Adobe).

QTSP “Diia” acknowledges Adobe’s right to not accept or to remove QTSP “Diia’s” from the AATL as provided in the AATL Technical Requirements. Upon receipt of Adobe’s notice specifying the reasons, including:

(a) an audit with material non-conformities lacking an acceptable remediation/mitigation plan;

(b) failure to provide prior notice of a change required under AATL requirements;

(c) failure to report a security incident;

(d) failure to remediate a security incident;

(e) failure to cure any AATL non-compliance within an Adobe-set timeframe.

If Adobe sets deadlines for remediation, QTSP "Diia" shall ensure completion within the specified timeframe.

QTSP "Diia" shall ensure timely alignment with the current version of the AATL Technical requirements and maintain conformance of all services and processes declared for AATL participation to those requirements. When Adobe publishes updates to the AATL Technical requirements, QTSP "Diia" implements the necessary changes in its documents and processes and, where required by AATL Technical requirements, provides advance notice to Adobe of such changes and meets any Adobe-set deadlines.

QTSP “Diia” complies with the AATL EE3 requirements regarding the use of electronic time-stamps. Custom OIDs for AATL purposes are not mandatory. If needed, QTSP “Diia” may implement Adobe-specific OIDs to enable automatic time-stamping and/or inclusion of revocation information for Long-Term Validation (LTV) in Adobe products, in line with Adobe public guidelines. Where QTSP “Diia” requires or recommends the use of a specific Time-Stamping Authority (TSA), such TSA shall meet the state-of-the-art and comply with applicable legislation of Ukraine.

All provisions describing the policy and practice for the generation of qualified electronic time-stamps required for AATL EE3 compliance are defined in section 6.8 of this Certificate Policy and form an integral part of this section.

9.16.2. AATL certificate policy (OID AATL-EE)

For qualified public key certificates intended for use under the Adobe Approved Trust List (AATL) programme, the QTSP ‘Diia’ applies a dedicated certificate policy OID (OID AATL-EE), which is assigned within the QTSP ‘Diia’ OID tree and is notified to Adobe as part of the AATL inclusion/update package.

OID AATL-EE is additional to the OID of this Certificate Policy 1.2.804.2.1.1.1.2.4 and shall be used exclusively for the AATL profile of qualified certificates.

ANNEX 2

to the Rules and Procedures for Operation of the Qualified Trust Service Provider “Diia”

REGULATIONS ON CERTIFICATION PRACTICES OF THE QUALIFIED TRUST SERVICE PROVIDER “DIIA” FOR QUALIFIED CERTIFICATES OF ELECTRONIC SIGNATURE AND SEAL

Table of Content

1. INTRODUCTION

1.1. Overview

These Regulations on Certification Practices define the list of practical actions and procedures for qualified certificates of electronic signature and seal (hereinafter referred to as the "qualified certificates") of users of electronic trust services, in particular, signatories and electronic seals creators (hereinafter referred to as the "users"), which are used by the QTSP "Diia" to implement the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures).

Compliance with the practical actions and procedures defined in these Regulations on Certification Practices is mandatory for the Head of the specialised subdivision of the QTSP "Diia" and hired employees of the QTSP "Diia", whose position responsibilities are directly related to the registration of users, formation and maintenance of their qualified certificates of the electronic signature and seal (hereinafter referred to as the personnel), as well as natural and legal persons who, on the basis of agreements concluded with the QTSP "Diia" (State Enterprise "DIIA"), are directly or indirectly related to the registration of users, the formation and/or maintenance of their qualified certificates of electronic signature and seal, in particular, separate registration units of the QTSP "Diia".

Acknowledgment by users of the requirements defined in these Regulations on Certification Practices is a mandatory condition and basis for concluding an agreement with them on the provision of electronic trust services.

List of all rules applied by the QTSP "Diia" in the process of user registration, formation and maintenance of qualified certificates of public keys of the QTSP "Diia" and users, including management of their status (blocking, renewal and cancellation) are determined by the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures).

List of all practical actions and procedures for the qualified certificate of remote qualified electronic signature "Diia.Signature" ("Diia ID"), which are used to implement the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures), is determined by the Regulations on Certification Practices of the Qualified Trust Service Provider "Diia" for qualified certificates of remote qualified electronic signature "Diia.Signature" (Annex 3 to these Rules and Procedures).

These Regulations on Certification Practices conform to the requirements defined in:

- DSTU ETSI EN 319 411-1 (ETSI EN 319 411-1 V1.3.1, IDT) "Electronic signatures and infrastructures (ESI). Requirements for policy and security for trust service providers issuing certificates. Part 1: General requirements" (hereinafter referred to as DSTU ETSI EN 319 411-1);
- DSTU ETSI EN 319 411-2 (ETSI EN 319 411-2 V2.4.1, IDT) "Electronic signatures and infrastructures (ESI). Requirements for policy and security for trust service providers issuing certificates. Part 2. Requirements for trust service providers issuing qualified EU certificates" (hereinafter referred to as ETSI EN 319 411-2).

1.2. Name of the document and its identification

In accordance with the provisions of the Clause 5.3 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2.

Name of the document: Regulations on Certification Practices of the QTSP "Diia" on the

Qualified Certificates of Electronic Signature and Seal.

Full name	Provisions of the certification practices of the qualified electronic trust service provider “Diia” regarding qualified certificates of remote qualified electronic signature “Diia.Signature”
Short name	Provisions of the certification practices of QTSP “Diia” regarding qualified certificates “Dія.Signature”
Version	1.0
OID	1.2.804.2.1.1.1.2.2
Identificator	NCP+ (пункт 5.3 (b) ETSI EN 319 411-1): Normalized Certificate Policy requiring a secure cryptographic device itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)

1.3. Public key infrastructure participants

Participants of the public key infrastructure are specified in the Clause 5.4 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2.

1.3.1. Provider

QTSP “Diia” is a Qualified Electronic Trust Services Provider, which provides qualified electronic trust services in compliance with the requirements of the Law of Ukraine “On Electronic Identification and Electronic Trust Services”, in particular, it registers users, forms and maintains their qualified certificates, including managing their status (blocking, renewal and cancellation).

QTSP “Diia” registers users independently and/or through separate registration units of QTSP “Diia”.

Clause 1.3.1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains additional information.

1.3.2. Registration authorities

Separate registration units of QTSP “Diia” are registration authorities represented by separate subdivisions, non-staff units of the state QTSP “Diia”, or legal entities or natural persons who register users on the basis of an agreement with the QTSP “Diia”.

Direct registration of a user at a separate registration unit of the QTSP “Diia” is carried out by an employee of the QTSP “Diia” separate registration unit who is entrusted with the appropriate user registration responsibilities (hereinafter referred to as the Remote Registration Administrator).

Employees of the separate registration units of the QTSP “Diia”, who are responsible for registering users, shall be subject to the same requirements as Registration Administrators, as defined in the Clause 5.3.1.2 of the Policy of the Certificate of a Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

1.3.3. Users

Users are the signatories and electronic seals creators in respect of which QTSP “Diia” carries out their registration (independently or through separate registration units of QTSP “Diia”), the formation and maintenance of their qualified certificates, in particular:

1) signatories:
- natural persons - residents;
- natural persons - non-residents;
- self-employed persons (notaries, attorneys, insolvency officers, private executors, etc.);
- officials (hired employees, contractors, etc.) of a legal entity, representative office of a non-resident legal entity, officials of a non-resident legal entity, natural person-entrepreneur, self-employed persons;

2) creators of electronic seals:
- legal entities - residents;
- representative offices of legal entities - non-residents;
- natural persons - entrepreneurs.

Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains additional information.

1.3.4. Entities that trust

Natural and legal persons, as well as their Information and Communication Systems, are entities that trust the QTSP “Diia” and use the user qualified certificates for the purpose of their authentication, in particular by verifying and confirming an electronic signature or seal.

1.3.5. Other participants

Natural and legal persons directly or indirectly related to the formation and/or maintenance of qualified certificates of the QTSP “Diia” and users are other participants.

Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains additional information.

1.4. Use of the certificate

Use of Certificates conforms to the provisions of the Clause 5.5 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2.

1.4.1. Allowed use of the certificate

Qualified certificates formed by the QTSP “Diia” are allowed to be used for:

- authentication;
- creation, verification and confirmation of a qualified electronic signature;
- creation, verification and confirmation of a qualified electronic seal;
- encryption key approval.

All qualified certificates formed by the QTSP “Diia” contain the following values in the “qualified certificate statement” extension:

1.2.804.2.1.1.1.2.1 - to ensure electronic document management and authentication of persons within the country;

1.2.804.2.1.1.1.2.2 - for software keys;

1.2.804.2.1.1.1.2.4 - for personal keys or seals that meet international standards.

In order to determine the scope of use of a user qualified certificate, QTSP “Diia” shall, during its formation, set the certificate extensions “Public key usage” (“keyUsage”) specified in the Table 1.

Table 1. Certificate extensions included in a qualified certificate to determine its scope of use

Scope of use of the qualified certificate	**Certificate extension “Public key usage” (“keyUsage”)**
Authentication	digitalSignature + nonRepudiation or keyAgreement
Creation, verification and confirmation of a qualified electronic signature	digitalSignature + nonRepudiation
Creation, verification and confirmation of a qualified electronic seal	digitalSignature + nonRepudiation
Encryption key agreement	keyAgreement

QTSP “Diia” forms qualified certificates with “digitalSignature + nonRepudiation” or “keyAgreement” certificate extensions, provided that such public keys belong to different key pairs.

To determine the scope of use of a user qualified certificate as a qualified electronic seal certificate during its formation, the QTSP “Diia” installs an additional extension “Extended public key usage” (“extendedKeyUsage”) with an object identifier (OID): 1.2.804.2.1.1.1.3.9.

In cases where the requirements for certain Information and Communication Systems stipulate that authentication in them can only be carried out using a qualified certificate whose private key was generated using an QESST (id-etsi-qcs 4),during formation of the appropriate qualified certificate, the QTSP “Diia” shall install an additional extension “Extended Public Key Usage” (“extendedKeyUsage”) and a conventional designation of the type of such media with its unique serial number in the additional user data to identify the type of such QESST. This extension is applied only to qualified certificates whose private keys are generated in accordance with DSTU 4145-2002 “Information Technologies. Cryptographic protection of information. Digital signature based on elliptic curves. Formation and verification”, approved by the Order of the State Committee for Technical Regulation and Consumer Policy No. 31 dated December 28, 2002.

1.4.1.1. Types of certificates

In accordance with these Regulations on Certification Practices, the QTSP “Diia” creates qualified certificates of the following types:

- qualified certificate of the electronic signature that links the public key of a qualified electronic signature to a natural person and confirms his or her identification data during authentication, as well as the creation, verification and confirmation of a qualified electronic signature;
- qualified certificate of the electronic seal that links the public key of a qualified electronic seal to a legal entity or a natural person - entrepreneur and confirms its identification data during authentication, as well as the creation, verification and confirmation of a qualified electronic seal;
- qualified certificate of encryption that links the public key of a qualified electronic signature or seal with a natural person, legal entity or natural person - entrepreneur and provides directed encryption during the exchange of information.

1.4.1.2. Validity of certificates

User qualified certificates are issued by QTSP “Diia” with a validity period of 1 or 2 years.

1.4.2. Prohibited use of the certificate

It is not allowed to use a qualified certificate formed by the QTSP “Diia” in fields that do not correspond to the public key usage (“keyUsage”) specified in the qualified certificate.

1.5. Management of the Regulations on Certification Practices

1.5.1. Responsibility for the Regulations on Certification Practices

These Regulations on Certification Practices are maintained by the State Enterprise “DIIA” (hereinafter referred to as SE “DIIA”).

SE “DIIA” is a legal entity of public law registered in accordance with the legislation - a state-owned commercial enterprise based on state property and belonging to the field of management of the Ministry of Digital Transformation of Ukraine.

Head office of the QTSP “Diia” is represented by the functional subdivision of the SE “DIIA”, which organises the provision of qualified electronic trust services by separate registration units of the QTSP “Diia” and ensures compliance with the requirements of the legislation to qualified trust service providers.

Agreements for the provision of qualified electronic trust services are concluded on behalf of the SE “DIIA” or on behalf of a separate registration unit of the QTSP “Diia”.

Details of the SE “DIIA”:

- Code according to the Unified State Register of Enterprises and Organisations of Ukraine (USREOU): 43395033.
- Address: 24 Dilova Str., Kyiv, 03150, Ukraine.
- Contact phone number: +38 (067) 258 05 20.
- E-mail address: inbox@diia.gov.ua.

Details of the QTSP “Diia”:

- Website address: ca.diia.gov.ua.
- Contact phone number: +38 (067) 107 20 41.
- E-mail address: ca@diia.gov.ua; keys@diia.gov.ua; ca@informjust.ua.

These Regulations on Certification Practices are structured in accordance with RFC 3647, “Internet Public Key Infrastructure X.509 Policy of the Certificates and Certification Practices”, and contains all the necessary information.

These Regulations on Certification Practices, as well as amendments thereto, shall be signed by the Head of the specialised subdivision of the QTSP “Diia”, who is responsible for compliance with the practical actions and procedures defined in them, and approved by the Chief Executive Officer of the SE “DIIA”.

These Regulations on Certification Practices, as well as amendments as amendments thereto, shall be approved by the Ministry of Digital Transformation of Ukraine, which sends copies to the Administration of the State Service of Special Communications and Information Protection of Ukraine.

1.5.2. Amendments to the Regulations on Certification Practices

In accordance with the Clause 9.12 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

1.6. Definitions of terms and list of abbreviations

1.6.1. Definition of terms

In these Regulations on Certification Practices, the terms are used in the meanings given in the Civil Code of Ukraine, the Laws of Ukraine “On Protection of Information in Information and Communication Systems”, “On Protection of Personal Data”, “On the Unified State Demographic Register and Documents Confirming Citizenship of Ukraine, Identifying a Person or His/Her Special Status”, “On Electronic Communications”, “On Electronic Identification and Electronic Trust Services”, Resolution of the Cabinet of Ministers of Ukraine No. 764 dated June 28, 2024, “Some issues of compliance with requirements in the fields of electronic identification and electronic trust services”, other legislative and regulatory acts in the fields of electronic trust services, cryptographic and technical protection of information, electronic communications.

1.6.2. List of abbreviations

USDR	Unified State Demographic Register
USR	Unified State Register of Legal Entities, Natural Persons-Entrepreneurs and Community Groups
USREOU	Unified State Register of Enterprises and Organisations of Ukraine
ICS	Information and Communication System
CPI	Cryptographic Protection of Information
RNTRC	Registration number of the taxpayer’s registration card
URN	Unique Record Number in the Unified State Register
CMP	Certificate Management Protocol
OCSP	Online Certificate Status Protocol
TSP	Time Stamp Protocol

2. PUBLICATION AND STORAGE OBLIGATIONS

Requirements specified in the Clause 6.1 of ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

2.1. Repository/website

Through its website (https://ca.diia.gov.ua), the QTSP “Diia” provides free access to:

- information about the QTSP “Diia”;
- data on the inclusion of information about the QTSP “Diia” in the Trust List;
- Policy of the Certificate of the QTSP “Diia”;
- appropriate Regulations on Certification Practices of the QTSP “Diia”;
- general terms and conditions for the provision of qualified electronic trust services to users of the QTSP “Diia”;
- QTSP “Diia” qualified certificates;
- list of qualified electronic trust services provided by QTSP “Diia”;
- data on the tools of a qualified electronic signature or seal used in the provision of qualified electronic trust services by QTSP “Diia”;
- forms of documents on the basis of which qualified electronic trust services are provided
- information on the separate registration units of the QTSP “Diia” and on-site registration administrators;
- register of valid, blocked and cancelled public key certificates;
- information about restrictions on the use of qualified certificates by users;
- data on the rules of order for verifying the validity of a qualified certificates, including the conditions for verifying the status of the certificate;
- list of legislative acts in the field of electronic trust services.

These Regulations on Certification Practices are available 24 hours a day, 7 days a week in a read-only format on the QTSP “Diia” website (https://ca.diia.gov.ua).

2.2. Publishing information

2.2.1. Publication of user certificates

The Certification Administrator of the QTSP “Diia” ensures the publication of user qualified certificates, the consent to the publication of which was provided by such users, and revoked certificate lists (CRL) on the QTSP “Diia” website.

QTSP “Diia” provides free access to the register of valid, blocked and cancelled public key certificates through its website (https://ca.diia.gov.ua/certificates-search).

2.2.2. Publication of Provider’s certificates

QTSP “Diia” provides free access to information on qualified certificates of the QTSP “Diia” through its website (https://ca.diia.gov.ua/).

Information about the qualified certificates of the QTSP “Diia” formed using the self-signed electronic seal certificate of the Central Certifying Authority, the status and restrictions on the use of such certificates, as well as revoked certificate list (CRL) are contained in the register of valid, blocked and cancelled public key certificates maintained by the Central Certifying Authority (https://czo.gov.ua/).

2.2.3. Access to user certificates

QTSP “Diia” provides users with twenty-four-hour access to their own qualified certificates.

Access of other persons to the user qualified certificates is granted provided that such users agree to the publication of their qualified certificates.

2.2.4. Certificate expiration date

Date and time of commencement and expiration of the qualified certificate shall be indicated in such qualified certificate with an accuracy of one second.

Qualified certificate shall be deemed cancelled upon the date and time of expiry of the qualified certificate.

2.3. Time and frequency of publication

QTSP “Diia” forms revoked certificate list in the form of full and partial lists that comply with the following requirements:

- each revoked certificates list shall indicate the expiry date of its validity before a new list is issued;
- a new revoked certificates list may be published before the expiry date of its validity until the next list is published;
- qualified electronic signature or seal of the QTSP “Diia” shall be affixed to the revoked certificate list.

Revoked certificate lists are published automatically.

The time of change in the status of qualified certificates is synchronised with the Coordinated Universal Time (UTC) with an accuracy of one second.

Links to revoked certificates lists are included in user qualified certificates.

A complete revoked certificates list is formed and published 1 (once) a week and contains information on all revoked qualified certificates formed by the QTSP “Diia”.

Partial revoked certificates list is formed and published every 2 (two) hours and contains information on all revoked qualified certificates whose status has been changed in the interval between the time of issuance of the last full revoked certificates list and the time of formation of the current partial revoked certificates list.

2.4. Control to the repository/website access

Qualified certificates of the QTSP “Diia” and users, revoked certificates lists, appropriate Regulations on Certification Practices and Policy of the Certificate are available in the repository/website 24 hours a day, 7 days a week.

Read-only access is unlimited. Changes to the repository/website are made exclusively by the QTSP “Diia”.

User can find information about his/her qualified certificate by searching for it on the website of the QTSP “Diia” in the “Certificate Search” section by filling in the appropriate tabs with information about the RNTRC (in case of absence, the series (if any) and passport number) or the serial number of the qualified certificate.

3. IDENTIFICATION AND AUTHENTICATION

Requirements specified in the Clause 6.2 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

3.1. Designation

Qualified certificates issued by the QTSP “Diia” shall contain the information specified in the Part two of the Article 23 of the Law of Ukraine “On Electronic Identification and Electronic Trust Services”, in particular:

1) a designation (in a form suitable for automated processing) that the certificate is issued as a qualified certificate;

2) a mark that the certificate was issued in Ukraine;

3) identification data that clearly defines the QTSP “Diia”, including the name and code according to the USREOU;

4) identification data that uniquely identifies the user, including, without limitation:

- surname, name, patronymic (if any) of the signatory and the URN or RNTRC, or series (if any) and passport number of a citizen of Ukraine (for natural persons who, due to their religious beliefs, refuse to accept the RNTRC and have officially notified the relevant tax authority and have a mark or information in the passport of a citizen of Ukraine on the right to make any payments by series and/or passport number), or passport number of a foreigner or stateless person;
- name or surname, name, patronymic (if any) of the electronic seal creator and code according to the USREOU (code/number from the commercial, bank or court register maintained by the country of residence of the foreign legal entity, code/number from the registration license of the local authority of the foreign state on registration of the legal entity), except for international organisations, information about which is not entered in the USR or commercial, bank or court register, maintained by a foreign state, at the location of the headquarters of the international organisation, or a unique record number in the USDR, or the RNTRC, or the series (if any) and number of the passport of a citizen of Ukraine (for natural persons who, due to their religious beliefs, refuse to accept the RNTRC and have officially notified the relevant tax authority and have a mark or information in the passport of a citizen of Ukraine on the right to make any payments by series and/or passport number);

5) the value of the public key that corresponds to the private key;

6) information on the beginning and end of the validity period of the qualified certificate;

7) serial number of the qualified certificate, unique for the QTSP “Diia”;

8) a qualified electronic signature or a qualified electronic seal created by the QTSP “Diia”;

9) information on the place of placement in free access of the qualified certificate, which is used to verify the advanced electronic signature or seal provided for in the Subclause 8 of this Clause;

10) information on the location of the service for verifying the status of the appropriate qualified certificate;

11) an indication that the private key linked with the public key is stored in a qualified electronic signature or seal - in a form suitable for automated processing.

Qualified certificates may contain information on restrictions on the use of a qualified electronic signature or seal.

Qualified certificates may contain other optional additional special attributes as defined in the standards for qualified certificates. Such attributes shall not affect the interoperability and recognition of qualified electronic signatures or seals.

The information contained in qualified certificates corresponds to the designations (details, attributes) defined in the standards for certificate profiles in accordance with the Clause 7.1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

The designations used in the user qualified certificates are shown in Table 2.

Table 2: Designations used in user qualified certificates

Name	Designation
Country (C)	Country name in accordance with DSTU ISO 3166-1:2009 “International Country Names Codes” (ISO 3166-1:2006, IDT), approved by the Order of the State Committee of Ukraine for Technical Regulation and Consumer Policy No. 471 dated December 23, 2009
Organization (O)	Name of the legal entity for a qualified certificate of a legal entity or a qualified certificate of a legal entity’s representative. This field is not available for qualified certificates of natural persons who do not belong to a legal entity
Organizational Unit (OU)	Name of a subdivision or department in the organisation. This field is not available for qualified certificates of natural persons who do not belong to a legal entity
State or Province (S)	Name of the user’s location or place of registration
Locality (L)	Name of the city of residence or place of registration of the user
Common Name (CN)	Full name of the user to whom the qualified certificate belongs
E-Mail Address (E)	E-mail of the user who owns the qualified certificate
Title (T)	Title (for qualified certificates of legal entity representatives, if necessary)

Unique Identifier (UID)	Identifier of the user to whom the qualified certificate belongs: - for users who are natural persons, the RNTRC or passport number is used as the UID; - for users who are natural persons-entrepreneurs, the RNTRC is used as UID; - for users who are legal entities, the code according to the USREOU is used as the UID

3.1.1. Types of certificate designations

The types of designations (details, attributes) of a qualified certificate that comply with the information contained in qualified certificates are defined in the standards for certificate profiles in accordance with the Clause 7.1 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures).

3.1.2. Designation (details and attributes) of certificates

Qualified certificate shall have all the necessary designations (details, attributes) defined in the standards for certificate profiles in accordance with the Clause 7.1 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures).

3.1.3. Anonymity or use of pseudonyms

Pseudonyms shall be used in accordance with the Clause 3.1.3 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures).

3.1.4. Rules for interpreting different forms of certificate designations

International letters shall be encoded according to UTF-8.

3.1.5. Uniqueness of certificate designations

QTSP "Diia" shall ensure that certificates with the same data specified in the "Common Name" and "Serial Number" fields are not issued to different users.

3.1.6. Acknowledgment, authentication and the role of trademarks

Not applicable.

3.2. Initial identification verification

3.2.1. Method of confirming possession of a private key

Clause 3.2.1 of the QTSP "Diia" Policy of the Certificate contains information on the methods of confirming the user's possession of a private key.

3.2.2. Identity authentication

To identify a user who has applied to the QTSP "Diia" for qualified electronic trust services, the QTSP "Diia" shall require, along with the application, and the user shall provide identification data that shall be entered into a qualified certificate.

The list of identification data to be included in the qualified certificate and the mechanisms for their confirmation are defined in the Tables 3 and 4.

Table 3. Identification data and their confirmation mechanisms during the identification of natural persons who first applied for the service of forming a qualified certificate

Identification data	**Mandatory provision of identification data**	**Identification data verification mechanisms**
Surname, name, patronymic (if any)	Mandatory	Documentary or electronic (passport, continuous (temporary) residence permit)
RNTRC	If any	Documentary or electronic (taxpayer registration card, passport)
Series (if any), passport number	Mandatory	Documentary or electronic (passport)
URN	If any	Documentary or electronic (passport)
Phone number	Mandatory	Technical (reproduction of the text of the SMS message sent by the QTSP “Diia”)
E-mail address	Mandatory	Technical (response to an email sent by the QTSP “Diia”)
Authority or position held	At the user’s request for their inclusion in a qualified certificate	Documentary (a document certifying the right to carry out activity in a certain field: a license, a certificate, an appointment order, a document of authorisation, etc.) or technical (information from appropriate state information systems (registers, databases, etc.)

Table 4. Identification data and their confirmation mechanisms during the identification of legal entities whose authorised employees have applied for the first time for the service of forming a qualified certificate.

Identification data	**Mandatory provision of identification data**	**Identification data verification mechanisms**
Name of the legal entity	Mandatory	Documentary or technical (obtaining information in electronic form from the USR)
Code according to USREOU	Mandatory	Documentary or technical (obtaining information in electronic form from the USR)
Location	Mandatory	Documentary or technical (obtaining information in electronic form from the USR)

Lists, forms of documents on the basis of which qualified electronic trust services are provided, and explanations on their execution are published on the website of the QTSP “Diia”.

In order to conclude agreements on the provision of qualified electronic trust services, QTSP “Diia” may receive other documents from users as provided by the legislation.

To confirm that the user identification procedure was carried out properly, QTSP “Diia” ensures the storage of applications for the formation or change of the status of qualified certificates and copies of documents provided by users during their identification. Copies of such documents shall be kept in paper form in the archival premises of the QTSP “Diia” or separate registration units of the QTSP “Diia”, as well as in electronic form with automatic backup by tools of the QTSP “Diia” ICS and manual archival copying to separate media.

Statements and copies of documents used to identify the user shall be certified according to the rules set out in Table 5.

Table 5. Rules for certifying documents used for user identification.

Form of the document	**Certification by the user**		**Certification by the QTSP “Diia” (Registration Administrator)**	
	Type of signature	**Certification queue**	**Type of signature**	**Certification queue**

Paper	Handwritten signature	First	Stamp of the Registration Administrator on paper documents. Qualified electronic signature of the Registration Administrator in the user account creation subsystem	Second
Electronic	Qualified electronic signature or electronic signature obtained by means of handwritten signature reproduction using interactive touchscreen displays	First	Qualified electronic signature of the Registration Administrator or a off-site Registration Administrator on an electronic document. Qualified electronic signature of the Registration Administrator in the user account creation subsystem	Second

Certification of applications and copies of documents by the QTSP “Diia” (Registration Administrator) without completing the user identification and without proper certification of documents is not allowed.

During user identification, QTSP “Diia” may use tools of photographic recording of the fact of presentation of identity documents by the user. Photo documents are stored in the QTSP “Diia” ICS after their certification by creating a qualified electronic signature of the Registration Administrator.

Verification of information (data) about a person on the basis of a passport of a citizen of Ukraine or other documents issued in accordance with the legislation on the USDR and on documents that identify a person, confirm the citizenship of Ukraine or a special status of a person is carried out in one of the following ways:

- without the use of additional devices by visually comparing the same information (value “URN”, “document No.”, “date of birth”, “validity period”) printed in the visual inspection zone and the machine-readable zone;
- by tools of the Unified State Web Portal of Electronic Services (Diia Portal) by transferring, at the request of the person, an electronic copy of the displaying information in electronic form contained in his/her passport of a citizen of Ukraine in the form of a card and/or an electronic copy

of the displaying information in electronic form contained in his/her passport of a citizen of Ukraine for travelling abroad to the QTSP “Diia” ICS;

- by automated reading of information using hardware and software tools (readers) that have an interface published on the official website of the State Enterprise “Printing Plant “Ukraine”.

When identifying a user with a passport of a citizen of Ukraine or other documents issued in accordance with the legislation on the USDR and on documents that identify a person, confirm Ukrainian citizenship or special status of a person, the validity of such documents is verified using the database on stolen (lost) documents upon requests of citizens of the unified information system of the Ministry of Internal Affairs from the Unified State Demographic Register by tools of the unified information system of the Ministry of Internal Affairs.

3.2.3. Unverified user information

Identification of a person/entity is carried out by the QTSP “Diia” (QTSP “Diia” separate registration unit) by verifying and confirming that the person’s/entity’s identification data received by the QTSP “Diia” (QTSP “Diia” separate registration unit) belongs to the natural person or legal entity that applied for the service of forming a qualified certificate.

3.2.4. Confirmation of powers

During the identification of an authorised representative of a legal entity or a natural person - entrepreneur, the QTSP “Diia” authenticates such a user in accordance with the Clause 3.2.2 of these Regulations on Certification Practices, verifies the scope of authority according to the document defining the powers of the authorised representative of the legal entity or natural person - entrepreneur, or using information contained in the USR or in the commercial, banking or court register maintained by the country of residence of the foreign legal entity.

If a collegial authority acts on behalf of a legal entity, a document defining the powers of the appropriate authority and the distribution of responsibilities among its participants is submitted to the QTSP “Diia”.

3.3. Identification and authentication for requests of change of keys

During the repeated formation of a user qualified certificate, the QTSP “Diia” shall verify the relevance of the information provided for the previous formation of the qualified certificate.

In case of changes in the information contained in the qualified certificate, the user shall notify the QTSP “Diia” within three days from the date of such changes and provide documents confirming the appropriate changes.

On the basis of documents provided by the user confirming changes in the information contained in the qualified certificate, the QTSP “Diia” provides the repeated formation of such a certificate and publishes it if the user consents.

Authentication of users who have a valid qualified certificate formed by the QTSP “Diia” is carried out in the case of submission in electronic form of applications for the formation, blocking and cancellation of qualified certificates, in the case of unchanged identification data entered in the previous qualified certificate from the moment of certificate formation until the creation of a qualified electronic signature on the application.

Verification of the identification data of the user who submits an application in electronic form, as well as the legality of such application, is carried out by authenticating the user and his/her powers based on the results of verification of the qualified electronic signature on the application and the

establishment of validity of a qualified certificate containing the person's identification data at the time of submission of the application.

Repeated formation of a user qualified certificate does not extend its validity period.

3.4. User identification and authentication based on certificate blocking or revocation requests

List and description of user authentication mechanisms for blocking, revoking or renewing a qualified certificate is given in Table 6.

Table 6. List and description of user authentication mechanisms for the issues of blocking, cancelling or renewing a qualified certificate.

Type of operation (reason for submitting applications)	Form of submitting applications	Mechanisms for confirming identification data
Blocking of a qualified certificate	Oral	According to the voice authentication key phrase, which is initially exchanged between the user and the QTSP "Diia" during the submission of application for the formation of a qualified certificate
	Written paper	Mechanisms similar to the confirmation of the identification data of users who first applied for the service of formation of a qualified certificate
	Written electronic	Mechanisms are similar to the confirmation of the identification data of users who have a valid qualified certificate formed by the QTSP "Diia"
Cancellation of a qualified certificate	Written paper	Mechanisms similar to the confirmation of the identification data of users who first applied for the service of formation of a qualified certificate
	Written electronic	Mechanisms are similar to the confirmation of the identification data of users who have a valid qualified certificate formed by the QTSP "Diia"
Renewal of the qualified certificate	Written paper	Mechanisms similar to the confirmation of the identification data of users who first applied for the service of formation of a qualified certificate

3.5. Authentication in case of loss of an authentication tool

QTSP "Diia" does not use the user's phone number or email address as a tool of user authentication for submitting applications for blocking or cancelling a qualified certificate.

User authentication is carried out with the participation of the QTSP "Diia" consulting switch by answering a secret question or using another form of authentication.

4. REQUIREMENTS FOR THE CERTIFICATE LIFECYCLE

Requirements specified in the Clause 6.3 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

4.1. Request to form a certificate

List of entities authorised to submit a request for the formation of a qualified certificate includes users who have passed the identification and authentication procedures.

A request for formation of a qualified certificate shall be accepted for processing after acceptance and registration of an application for formation of a qualified certificate, identification and authentication of the user's identity and confirmation of the user's possession of a private key, the appropriate public key for which is provided for the formation of a qualified certificate.

The user registration process includes the following steps:

1. User shall execute the request for the obtaining the qualified electronic trust services at the QTSP "Diia" or a QTSP "Diia" separate registration unit in the form established by QTSP "Diia" on the QTSP "Diia" website https://ca.diia.gov.ua.
2. When receiving qualified electronic trust services, natural persons, legal entities, representatives of legal entities shall undergo initial identification of the person subject to personal presence at the QTSP "Diia" or a QTSP "Diia" separate registration unit, and provide the necessary documents for registration, the list of which is sent to the user by e-mail after the registration application is submitted and is available on the QTSP "Diia" website.
3. After identification, the user generates a private key using the tools provided by the QTSP "Diia" or submits requests (public key in PKCS#10 format) for the formation of a qualified certificate generated by the user outside the premises of the QTSP "Diia" or a QTSP "Diia" separate registration unit for the further formation of the user qualified certificates.
4. Registration Administrator of the QTSP "Diia" or a Remote Registration Administrator using specialised software forms a user qualified certificates in accordance with the information specified in the registration application.

List of documents to be provided by the user:

1) Natural person:
- application for registration;
- original passport document (for familiarization);
- a copy of the passport document;
- original taxpayer's registration card (if any, for familiarization);
- a copy of the taxpayer's registration card (if any);

2) Legal entity, authorised representative of a legal entity:
- application for registration;
- original passport document (for familiarization);
- a copy of the passport document;
- original taxpayer's registration card (if any, for familiarization);
- a copy of the taxpayer's registration card (if any);

- a copy of the Order on appointment to a position in a legal entity (if necessary, entering information about the position of an authorised representative of a legal entity in the qualified certificate);
- description (if any) or original constituent document/its certified copy (for familiarisation);
- a copy of the Order, Power of Attorney, other document executed in the name of the authorised representative of the legal entity confirming his/her powers to enter into transactions with third parties (in case of absence of appropriate information about the authorised representative of the legal entity in the USR);

3) Self-employed person (notary, lawyer, insolvency officer, private executive, etc.)
- application for registration;
- original passport document (for familiarisation);
- a copy of the passport document;
- original taxpayer's registration card (if available, for familiarisation);
- a copy of the taxpayer's registration card (if any);

4) Natural person - non-resident:
- application for registration;
- the original of the permanent (temporary) residence permit, passport document of a citizen of another country (refugee certificate) (for familiarisation) with a notarised translation into Ukrainian;
- a copy of a permanent (temporary) residence permit, passport document of a citizen of another country (refugee certificate) with a notarised translation into Ukrainian;
- original taxpayer's registration card (if any, for familiarisation);
- a copy of the taxpayer's registration card (if any);

5) Representative office of a legal entity - non-resident, authorised representative of a legal entity - non-resident:
- application for registration;
- original passport document (for familiarisation);
- a copy of the passport document;
- original of the taxpayer's registration card (if any, for familiarisation);
- a copy of the taxpayer's registration card (if any);
- copy of the order on appointment to a position in a legal entity - non-resident (if necessary, entering information about the position of an authorised representative of a legal entity - non-resident in the qualified certificate);
- original registration certificate (for familiarisation) and its certified copy issued by the Ministry of Economy of Ukraine or the Ministry of Finance of Ukraine;
- a copy of the certificate from the Chief Directorate of Statistics on the information from the USREOU;
- certified copy of the Power of Attorney, agreement with the Head (Manager) of the representative office of a legal entity - non-resident;

6) Legal entity - non-resident, authorised representative of a legal entity - non-resident:
- application for registration;
- original passport document (for familiarisation);
- a copy of the passport document;
- original taxpayer's registration card (if any, for familiarisation);

- a copy of the taxpayer's registration card (if any);
- a copy of the document on appointment to a position in a legal entity - non-resident (if necessary, entering information about the position of an authorised representative of a legal entity - non-resident in the qualified certificate);
- a copy of the registration document (code/number from the commercial, banking or court register maintained by the country of residence of the foreign legal entity, code/number from the registration certificate of the local authority of the foreign state on the registration of the legal entity), except for international organisations, information about which is not entered in the USR or the commercial, banking or court register maintained by a foreign state, at the location of the Headquarters of the international organisation.

4.2. Processing of a request for certificate formation

Processing of a request for a qualified certificate formation is carried out by the software tools of the QTSP "Diia" ICS with the participation of the Registration Administrator or Remote Registration Administrator, or automatically, provided the continuity of the processes of generating key pairs, forming requests, transferring them for processing via secure communication channels that ensure the confidentiality and integrity of data. Automatic processing of requests for the formation of a qualified certificate includes the processes of identifying the user's identity and confirming the user's possession of a private key, the corresponding public key of which is provided for the formation of a qualified certificate.

During the processing of a request for a qualified certificate formation, the uniqueness of the public key in the register of valid, blocked and cancelled public key certificates is verified with tools of the QTSP "Diia" ICS and the uniqueness of the serial number of the user qualified certificate is ensured.

The processing time for a request for a qualified certificate formation submitted together with a registration application is no more than one hour.

4.3. Formation of a certificate

Provision of the formed qualified certificate to the user is carried out in one of the following ways:

- by sending a file with the formed qualified certificate to the email address specified by the user in the application for the formation of a qualified certificate;
- by recording a file with the formed qualified certificate to the information medium provided by the user;
- by publishing a formed qualified certificate on the QTSP "Diia" website.

4.4. Acceptance of a certificate

User shall verify his/her identification data entered by the QTSP "Diia" into the qualified certificate within one day. QTSP "Diia" shall provide appropriate consultations on how to conduct such verification. User shall use the private key to create a qualified electronic signature only after verification. The use of the private key by the user is the fact of his/her recognition of the qualified certificate corresponding to his/her public key.

If the user found a discrepancy between the identification data entered by the QTSP "Diia" to the qualified certificate within a day, the user shall contact the QTSP "Diia" to cancel the qualified certificate and form a new certificate free of charge. If the user applies after 24 hours, the qualified certificate is formed on a paid basis.

In case of discrepancy of the identification data entered by the QTSP “Diia” in the qualified certificate and found by the QTSP “Diia” before the generated qualified certificate is provided to the user, an official of the QTSP “Diia” shall provide repeated formation of the qualified certificate using a previously certified public key and in compliance with the requirements for preventing the validity of the private key and its corresponding public key from exceeding two years. Official who has provided the repeated formation of the qualified certificate shall draw up an act stating the date and time of cancellation of the qualified certificate, user identification data contained in the qualified certificate and the inconsistent user identification data specified in the application for the qualified certificate formation. The act shall be signed by an official of the QTSP “Diia”, who has provided repeated formation the qualified certificate, and shall be attached to the documents (duly certified copies of documents) used to establish the identity and registration of the user.

4.5. Key pair and certificate purpose

4.5.1. Use of a private key and certificate by the user

User shall use a private key and a qualified certificate as required by the legislation and in accordance with:

- Policy of the Certificate of the QTSP “Diia”;
- these Regulations on Certification Practices;
- General terms and conditions for the provision of qualified electronic trust services to users of the QTSP “Diia”;
- Agreement for the provision of qualified electronic trust services concluded with the QTSP “Diia” (SE “DIIA”).

To receive a qualified certificate, the user shall:

- place an order for the service on the QTSP “Diia” website (https://ca.diia.gov.ua) in the “Get a service” section;
- make a payment for the ordered service;
- prepare the documents necessary to receive the service (the list of required documents and the registration application is sent to the user to e-mail specified when ordering the service);
- visit a QTSP “Diia” separate registration unit, which was selected when ordering the service;
- pass the initial identification procedure and provide the documents required for registration;
- generate a private key on a key information medium (hardware or software device or flash media) and provide a public key in PKCS#10 format to form a qualified certificate.

To verify and use a private key, the user shall have:

- a personal computer with Microsoft Windows XP/2003 Server/Vista/2008 Server/2012 Server/2016 Server/7/8/8.1/10/11 or Apple macOS 10.0.4 or later version installed;
- installed software “IIT User Key Certification Centre-1” version not lower than 1.3.1.51 or higher or a web browser such as Google Chrome, Mozilla Firefox, Opera.

Detailed information for the user is available on the QTSP “Diia” website (https://ca.diia.gov.ua) in the “Questions and Answers” section.

Clause 4.5.1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains additional information on the use of a private key and a qualified certificate by the user.

4.5.2. Use of the public key and a certificate by entities that trust the Provider

During the use of the public key and the user's qualified certificate, entities that trust the QTSP "Diia" shall comply with the requirements of the legislation in the field of electronic trust services, as well as the provisions of:

- these Regulations on Certification Practices;
- Policy of the Certificate of the QTSP "Diia".

Clause 4.5.2 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains additional information on the use of the public key and qualified certificate by entities that trust the QTSP "Diia".

4.6. Renewal of the certificate

Within two hours, the blocked qualified certificate shall be renewed by the QTSP "Diia", in case of:

- submission by the user of an application for the renewal of his/her blocked qualified certificate in any way that ensures confirmation of the user's identity (if the blocking was carried out on the basis of an application for blocking a qualified certificate);
- submission of an application for renewal of a qualified certificate of an employee of a legal entity or a natural person - entrepreneur signed by an authorised person of the appropriate legal entity or natural person - entrepreneur;
- notification of the establishment of unreliability of information on the fact of compromise of the private key by the user or the supervisory authority that previously reported such a suspicion;
- receipt by QTSP "Diia" of a notice of a court decision on the renewal of a qualified certificate that has entered into force.

Qualified certificate that has been blocked shall become valid from the moment of its renewal .

Qualified certificate shall be deemed renewed from the moment when the status of the qualified certificate is changed to "renewed" by the QTSP "Diia".

4.7. Repeated formation of the certificate

A request for the formation of a new qualified certificate for users who have a valid qualified certificate formed by the QTSP "Diia" shall be submitted together with an application for the formation of a new qualified certificate.

The software tools of the QTSP "Diia" ICS with integrated tools of a qualified electronic signature or seal, published on the QTSP "Diia" website, provide:

- verification of the validity of the previous user qualified certificate;
- automatic formation of an application for the formation of a new qualified certificate using the identification data entered in the previous user qualified certificate;
- creating a qualified electronic signature or seal to this application using the previous private key;
- creating a request for the formation of a qualified certificate in PKCS#10 format for the generated new key pair;
- transferring the request for the formation of a new qualified certificate together with the application for the formation of a new qualified certificate for processing to the QTSP "Diia" ICS.

Creation of an application for the formation of a new qualified certificate, a request for the formation of a new qualified certificate and their transfer for processing to the QTSP "Diia" ICS is

carried out with the ensuring integrity and confidentiality of information with tools of a qualified electronic signature or seal, and CPI tools that have documentary evidence of compliance with the requirements of the Articles 18 and 19 of the Law, issued based on the results of certification of such tools.

4.8. Change of the certificate

Change of the identification data entered in the user qualified certificate is a reason for cancellation of the qualified certificate.

4.9. Blocking and cancellation of the certificate

QTSP "Diia" cancels the qualified certificate formed by it within two hours in case of:

1) submission by the user of an application for cancellation of the qualified certificate issued to him/her in any way that ensures confirmation of the user's identity;

2) submission of an application for cancellation of a qualified certificate of an employee of a legal entity or a natural person - entrepreneur signed by an authorised person of the appropriate legal entity or natural person - entrepreneur;

3) receipt of information by the QTSP "Diia" confirming:

- death of a natural person - user;
- state registration of termination of a legal entity or termination of entrepreneurial activity of a natural person - entrepreneur who is a user;
- change of user identification data contained in a qualified certificate;
- providing false identification data by the user during the formation of his/her qualified certificate;
- the fact of compromise of the user's private key, found by the user independently or by the controlling authority in the course of conduction of measures of state control over compliance with the requirements of the legislation in the field of electronic trust services;
- entry into force of a court decision on cancellation of a qualified certificate, declaration of a natural person or natural person-entrepreneur who is a user as deceased, recognition of him/her as missing, incapacitated, restriction of his/her civil capacity, declaration of the user as bankrupt.

QTSP "Diia" blocks the qualified certificate formed by it no later than within two hours, in case of:

- submission by the user of an application for blocking the qualified certificate issued to him/her in any way that ensures confirmation of the user's identity;
- submission of an application for blocking a qualified certificate of employee of a legal entity or natural person-entrepreneur signed by an authorised person of the appropriate legal entity or natural person-entrepreneur;
- notification by the user or the controlling authority of suspicion of compromise of the user's private key;
- entry into force of a court decision to block a qualified certificate;
- violation by the user of the essential terms of the agreement on the provision of qualified electronic trust services.

List of entities authorised to submit a request for cancellation (blocking and renewal) of a qualified certificate, formation of a qualified certificate includes natural and legal persons who submit applications to the Provider or provide information confirming the reasons for changing the status of the certificate provided for in the Article 25 of the Law of Ukraine "On Electronic Identification and Electronic Trust Services".

List of reasons for changing the status of a qualified certificate to “blocked” and “cancelled” with indication of the subjects of submission of requests for status change and forms of confirmation of the reasons is given in the Table 7.

Table 7. List of reasons for changing the status of a qualified certificate to “blocked” and “cancelled”

Reasons for changing the certificate status	**Cancelling**	**Blocking**	**Confirmation of the reasons**
Submission of an application by the user	+	+	User’s application
Death of a natural person - user	+		Documentary confirmation
Termination of the user’s activity (legal entity or natural person - entrepreneur)	+		Documentary or technical (receiving information electronically from the USR) confirmation
Changes to user identification data	+		Documentary or technical (receiving information electronically from the USR) confirmation
User provides false identification data	+		Documentary confirmation
Fact of compromise of the user’s private key, found independently by the user or the controlling authority in the course of conduction of measures of state supervision (control) over compliance with the requirements of the legislation in the field of electronic trust services	+		Documentary confirmation
Notification by the user or controlling authority of suspicion of compromise of the private key of the user of electronic trust services		+	User application or documentary confirmation
Entry into force of a court decision	+	+	Documentary confirmation
Violation by the user of the essential terms of the agreement on the provision of qualified electronic trust services		+	Documentary confirmation

User has the right to block a qualified certificate at his/her own discretion. Blocking a qualified certificate tools the temporary suspension of the validity of a qualified certificate for a period of up to 30 calendar days.

After blocking a qualified certificate, the user may renew the validity of the qualified certificate within 30 calendar days. A blocked qualified certificate will be automatically cancelled by the QTSP "Diia" if the user does not renew it within the specified period.

Application for cancellation, blocking qualified certificate shall be submitted to the QTSP "Diia" in a manner that ensures confirmation of the user's identity.

List and description of user authentication mechanisms for blocking or cancellation of a qualified certificate is provided in the Table 6 of these Regulations on Certification Practices.

QTSP "Diia" carries out twenty-four-hour acceptance and verification of users' applications for cancellation and blocking of their qualified certificates, including through information channels, information about which is available on the QTSP "Diia" website.

Qualified certificates shall be cancelled and blocked by the QTSP "Diia" within two hours of receipt of confirmation of the reasons for changing the status of the qualified certificate and the appropriate verification of the authenticity of documentary messages and user authentication.

4.10. Service for verifying the certificate status

QTSP "Diia" ensures the availability of information on the certificate status in real time using the OCSP server and revoked certificate lists (CRL) published on the QTSP "Diia" website.

The OCSP responder and CRL publication service operate with high availability, under continuous monitoring for availability and data correctness. The ICS ensures:

a) immediate publication of status changes;

b) correct generation of CRLs and OCSP responses (GOOD/REVOKED/UNKNOWN with timestamps);

c) logging of publication events with timestamps;

d) periodic validation of the OCSP responder's certificate and trust chain.

The ICS performs periodic checks of the CP/CPS URLs embedded in certificates (CPS Pointer) and records the results in the monitoring log.

When issuing AATL-declared profiles, the ICS sets HTTPS-only AIA/CDP URLs; SHA-1 and DSTU/GOST are not used. Periodic monitoring of CPS URLs (CPS Pointer) and AIA/CDP URLs is performed with results logged.

4.11. Certificate expiry date

The date and time of the commencement and expiry of the user certificate validity period are indicated in the certificate with an accuracy of one second.

After the date and time of expiry of the user certificate specified in it, such certificate shall be considered cancelled.

User may apply to the QTSP "Diia" with an application for cancellation of the qualified certificate issued to him/her in case of necessity of early termination of its service according to the procedure specified in the Clause 4.9 of these Regulations on Certification Practices.

4.12. Depositing and returning keys

Not applicable.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROL

Requirements specified in the Clause 6.4 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

5.1. Physical security control

Clause 5.1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the requirements for the premises of the QTSP “Diia” and ensuring the physical access to them.

5.2. Procedural control

Clause 5.4 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the trusted roles of the personnel of the QTSP “Diia” (Head, Registration Administrator, Certification Administrator, Security Administrator, System Administrator, System Auditor) and their functional responsibilities, the number of persons required to perform tasks, as well as the trusted roles of the personnel of the QTSP “Diia” that require the distribution of responsibilities.

5.3. Personnel control

Clause 5.3 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the requirements for qualification, experience and competency of the personnel of the QTSP “Diia”, training requirements and procedures, sanctions for unauthorised actions, control of separate registration units of the QTSP “Diia”, documentation provided to the QTSP “Diia” personnel.

5.4. Maintaining an event audit log book

Clause 5.4 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the types of recorded events, frequency of event audit log book processing, event audit log book retention periods, event audit log book protection, event audit log book backup procedures and time synchronisation issues.

5.5. Archive of documents

Clause 5.5 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the types of documents and data subject to archival storage, archive storage periods, archive protection, archive backup procedures, requirements for affixing the electronic time stamps on records, archive collection systems, procedures for obtaining and verifying archival information.

5.6. Change of key

Clause 5.6 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the reasons and frequency of key pair change of the QTSP “Diia”, the procedure for using and accessing the current public key of the QTSP “Diia”.

5.7. Compromise and disaster renewal

Clause 5.7 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on incident and compromise handling procedures, renewal procedures if computing resources, software and/or data are damaged, renewal procedures after compromise of a private key, business continuity capabilities after a disaster.

5.8. Termination of the Provider’s activity

Clause 5.8 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the reasons for termination of the

activity of the QTSP “Diia”, the procedure for providing notification of termination of activity, determining the date of termination of activity, succession and transfer of documented information issues, as well as the Plan for termination of activity for the provision of qualified electronic trust services by the QTSP “Diia”.

6. TECHNICAL SAFETY MEASURES

Requirements defined in the Clause 6.5 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes, and measures mentioned in this Section.

6.1. Key pair generation and installation

Clause 6. 1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the generation of a key pair of the QTSP “Diia” and users, delivery of private and public keys to users, delivery of the public key of the QTSP “Diia” to entities that trust the QTSP “Diia”, on key sizes, generation of the public key parameters of the QTSP “Diia” and quality control, main purposes of using the QTSP “Diia” private keys.

6.2. Private key protection and engineering control of the cryptographic module

Clause 6.2 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on standards and controls of the cryptographic module, backup of the private key, archiving of the private key, renewal of the private key, storage of the private key in the cryptographic module, activation of the private keys, deactivation of the private keys, destruction of the private keys, capabilities of the network cryptographic module.

6.3. Other aspects of key pair management

Clause 6.3 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on archiving of the public key of the QTSP “Diia”, the certificate validity period and the period of use of the QTSP “Diia” key pair.

6.4. Activation data

Clause 6.4 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the protection of private key activation data.

6.5. Computer security control

Clause 6.5 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on special technical requirements for computer security, computer security rating.

6.6. Lifecycle security control

Clause 6.6 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on control of the development of the QTSP “Diia” ICS, security controls in the QTSP “Diia” ICS, security control during the lifecycle.

6.7. Network security control

Clause 6.7 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on network security controls.

6.8. Electronic time stamps

Clause 6.8 of the Policy of the Certificate of the Qualified Trust Service Provider ‘Diia’ (Annex 1 to these Rules and Procedures) contains information on the formation and verification of a qualified electronic time stamp, the consequences of invalidity of a qualified electronic time stamp and the procedure for receiving a qualified electronic time stamp by the QTSP “Diia”.

7. PROFILES OF CERTIFICATES, REVOKED CERTIFICATE LISTS (CRL) AND ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

Requirements specified in the Clause 6.6 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section. During certificate issuance, the ICS populates AIA (ocsp) and cRLDistributionPoints as configured by the profile. Non-public or inaccessible URLs are not permitted for certificates declared for AATL use.

During issuance, the ICS sets:

a) the Certificate Policies extension with the policy OID per profile;

b) the CPS Pointer (cps) qualifier with an HTTP-URL to the current CP/CPS in the Repository. These URLs shall be public and require no authentication.

7.1. Certificate profiles

Clause 7.1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the information to be contained in qualified certificates.

7.2. Revoked certificate list profiles

Clause 7.2 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the information to be contained in the revoked certificate lists.

7.3. Online certificate status protocol profiles

Clause 7.3 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the possibility of verifying the status of a user qualified certificate in real time via public electronic communication networks using the OCSP protocol.

8. CONFORMITY AUDITS AND OTHER ASSESSMENTS

Requirements specified in the Clause 6.7 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

8.1. Frequency or circumstances of assessment

Clause 8.1 of the Policy of the Certificate of Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the frequency and circumstances of assessment of the QTSP “Diia”.

8.2. Appraiser's identity/qualifications

Clause 8.2 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the qualification requirements for officials of the Controlling Authority (CA) and the Conformity Assessment Authority (CAA).

8.3. Relations between the expert and the object of assessment

Clause 8.3 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the relations between officials of the Controlling Authority (CA) and experts (auditors) of the Conformity Assessment Authority (CAA) and the object of assessment (QTSP "Diia").

8.4. Topics covered by the assessment

Clause 8.4 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the issues to be verified during state control and conformity assessment.

8.5. Actions taken as a result of the violation

Clause 8.5 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on actions taken as a result of a violation found by the results of the state control or results of conformity assessment.

8.6. Reporting results

Clause 8.6 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the presentation of the results of state control or conformity assessment, issuance of a prescript to eliminate violations identified during state control.

8.7. Self-checks

Clause 8.7 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on regular internal audits of conformity with the established requirements by the QTSP "Diia".

9. OTHER COMMERCIAL AND LEGAL ISSUES

Requirements specified in the Clause 6.8 of DSTU ETSI EN 319 411-1 and DSTU ETSI EN 319 411-2 are applied to the objects, processes and measures referred to in this Section.

9.1. Prices and tariffs

9.1.1. Fee for issuing or renewing a certificate

A fee is paid for the formation of a qualified certificate, the cost of which is determined in accordance with the tariff plans for the provision of qualified electronic trust services of the QTSP "Diia" published on the QTSP "Diia" website at the following link: https://ca.diia.gov.ua.

In case of provision of qualified electronic trust services through QTSP "Diia" separate registration units, an additional fee may be charged for the provision of qualified electronic trust services.

Renewal of blocked qualified certificates is free of charge.

9.1.2. Certificate access fee

There is no fee for access to a user qualified certificate.

9.1.3. Fee for blocking/cancellation or access to certificate status information

There is no fee for blocking and cancelling a user qualified certificate or access to information about the status of a user qualified certificate.

9.1.4. Fee for other services

QTSP "Diia" may provide users with additional services for a fee, including:

- providing tools of qualified electronic signature or seal to users;
- off-site generation of a user key pair;
- storage of private keys in the cloud storage of QTSP "Diia".

9.1.5. Refund policy

QTSP "Diia" does not refund paid invoices for services rendered.

9.2. Financial liability

Clause 9.2 of the Policy of the Certificate of Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the financial responsibility of the QTSP "Diia".

9.3. Business data confidentiality

Clause 9.3 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the content and scope of confidential information held by the QTSP "Diia", as well as responsibility for the protection of confidential information.

9.4. Personal data protection

Clause 9.4 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the concept of personal data protection in the QTSP "Diia", the definition of personal data and personal data that are not considered confidential, responsibility for personal data protection, consent to the use of personal data and circumstances of personal data disclosure.

9.5. Intellectual property rights

Issues of intellectual property rights of the QTSP "Diia" are regulated in accordance with the requirements of the current legislation of Ukraine.

9.6. Statements and guarantees

Clause 9.6 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the obligations and guarantees of the QTSP "Diia", separate registration units of the QTSP "Diia", users, relying parties, and other participants.

9.7. Waiver of liability

Clause 9.7 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the waiver of guarantees of the QTSP "Diia".

9.8. Limitations of liability

Clause 9.8 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the circumstances for limiting the liability of the QTSP "Diia".

9.9. Damages

Compensation for damages that may be caused to users of electronic trust services or third parties as a result of improper fulfilment of the liabilities by the QTSP "Diia" is carried out in accordance with the requirements of the current legislation of Ukraine.

9.10. Validity and termination

These Regulations on Certification Practices are applied from the moment of their publication and are valid until the expiration of the last certificate issued in accordance with these Regulations on Certification Practices or until the termination of the activity of the QTSP "Diia".

9.11. Individual communications and deeds with public key infrastructure subjects

QTSP "Diia" communicates with participants of the public key infrastructure by:

- posting notifications and announcements on the QTSP "Diia" website;
- informing the CCA, CA and the personal data protection authority by sending notifications in paper and electronic forms;
- sending emails to the user's email address;
- making phone calls and SMS messaging to the user's phone number.

9.12. Amendments

Amendments and additions to these Regulations on Certification Practices shall be made by the QTSP "Diia" in case of:

- changes in the requirements, processes and procedures described in these Regulations on Certification Practices;
- changes in the legislation;

changes in the requirements for service providers.

New versions of these Regulations on Certification Practices, after amendments have been made, are published on the QTSP "Diia" website.

Any amendments not defined in the history of these Regulations on Certification Practices are grammatical and spelling changes that do not affect the substance and do not relate to the processes and procedures described in these Regulations on Certification Practices.

9.13. Regulation on dispute resolution

In case of any disputes or disagreements, the QTSP "Diia" (SE "DIIA") shall resolve them through negotiations and consultations with the participants of the public key infrastructure.

If the participants of the public key infrastructure fail to reach an agreement, disputes (disagreements) shall be resolved in court in accordance with the current legislation of Ukraine.

9.14. Applicable law

Relations governed by these Regulations on Certification Practices are subject to the current legislation of Ukraine.

9.15. Compliance with the current legislation

Clause 9.15 of the Policy of the Certificate of the QTSP “Diia” contains information on the legislative and regulatory acts that establish requirements for the provision of Qualified Electronic Trust Services by the QTSP “Diia”.

ANNEX 3

to the Rules and Procedures for Operation of the Qualified Trust Service Provider “Diia”

REGULATIONS ON CERTIFICATION PRACTICES OF THE QUALIFIED TRUST SERVICE PROVIDER “DIIA” FOR QUALIFIED CERTIFICATES OF REMOTE QUALIFIED ELECTRONIC SIGNATURE “DIIA.SIGNATURE”

Table of content

1. INTRODUCTION

1.1. Overview

These Regulations on Certification Practices define a list of practical actions and procedures for qualified certificates of remote qualified electronic signature “Diia.Signature” (hereinafter referred to as qualified certificates “Diia.Signature”) of users of electronic trust services, in particular, signatories (hereinafter referred to as users), which are used by the Qualified Trust Service Provider “Diia” to implement the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

Compliance with the practical actions and procedures defined in these Regulations on Certification Practices is mandatory for the Head of the specialised subdivision of the QTSP “Diia” and hired employees of the QTSP “Diia”, whose position responsibilities are directly related to the registration of users, formation and maintenance of their qualified certificates “Diia.Signature” (hereinafter referred to as the personnel), as well as natural and legal persons who, on the basis of agreements concluded with the QTSP “Diia” (State Enterprise “DIIA”), are directly or indirectly related to the registration of users, the formation and/or maintenance of their qualified certificates “Diia.Signature”.

Recognition by users of the requirements defined in these Regulations on Certification Practices is a mandatory condition and basis for concluding with them an agreement on the provision of qualified electronic trust services related to the use of the “Diia.Signature” remote qualified electronic signature (hereinafter referred to as the Agreement on the Provision of Qualified Electronic Trust Services).

List of all rules applied by the QTSP “Diia” in the process of user registration, formation and maintenance of qualified certificates of QTSP “Diia” public keys and qualified certificates of “Diia.Signature” of users, including management of their status (blocking, renewal and cancellation) is determined by the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

List of all practical actions and procedures for qualified certificates of electronic signature and seal used to implement the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) is determined by the Regulations on Certification Practices of the Qualified Trust Service Provider “Diia” on Qualified Certificates of Electronic Signature and Seal (Annex 2 to these Rules and Procedures).

These Regulations on Certification Practices conform to the requirements defined in:

- DSTU ETSI EN 319 401 (ETSI EN 319 401, IDT) “Electronic signatures and infrastructures (ESI). General policy requirements for trust service providers” (hereinafter - ETSI EN 319 401);
- DSTU ETSI EN 319 411-1 (ETSI EN 319 411-1), IDT) “Electronic signatures and infrastructures (ESI). Policy and security requirements for trust services providers issuing certificate. Part 1: General requirements” (hereinafter - ETSI EN 319 411-1);
- DSTU ETSI EN 319 411-2 (ETSI EN 319 411-2, IDT) “Electronic signatures and infrastructures (ESI). Policy and security requirements for trust services providers issuing certificate. Part 2.

Requirements for trust service providers issuing qualified EU certificates" (hereinafter - ETSI EN 319 411-2). Creation of the remote qualified electronic signature "Diia.Signature" is performed using a remote qualified signature creation device (QSCD); the private key is used under the signer's control with multi-factor authentication."

1.2. Name of the document and its identification

In accordance with the provisions of the Clause 5.3 of ETSI EN 319 411-1 and the Clause 5.3 of ETSI EN 319 411-2.

Full name	Regulations on Certification Practices of the Qualified Trust Service Provider "Diia" on the Qualified Certificates of Remote Qualified Electronic Signature "Diia.Signature"
Short name	Regulations on Certification Practices of the QTSP "Diia" on the Qualified Certificates "Diia.Signature"
Version	1.0
OID	1.2.804.2.1.1.1.2.2
Identifier	NCP+ (Clause 5.3 (b) ETSI EN 319 411-1): Normalized Policy of the Certificate requiring a secure cryptographic device itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)

1.3. Public key infrastructure participants

According to the provisions of the Clause 5.4 of ETSI EN 319 411-1 and the Clause 5.4 of ETSI EN 319 411-2.

1.3.1. Provider

QTSP "Diia" is a Qualified Trust Services Provider, which provides qualified electronic trust services in compliance with the requirements of the Law of Ukraine "On Electronic Identification and Electronic Trust Services", in particular, it registers users, forms and maintains their qualified certificates "Diia.Signature", including managing their status (blocking, renewal and cancellation).

QTSP "Diia" is obliged to:

- provide users with all the necessary information regarding the receipt and use of "Diia.Signature";
- receive applications for receiving "Diia.Signature" from users in electronic form using the mobile application of the Diia Portal (Diia) and the mobile application of the "E-Resident" Information System;

- receive electronic copies of documents and photographs of users who submitted request for obtaining “Diia.Signature” via the mobile application of the Diia Portal (Diia) and the E-Resident information system mobile application;
- on the basis of information and certified documents received from the mobile application “Diia Portal” (Diia) and the mobile application of the “E-Resident” Information System, form qualified certificates “Diia.Signature” of users.

Clause 1.3.1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains additional information.

1.3.2. Registration authorities

In accordance with these Regulations on Certification Practices, users are registered by the QTSP “Diia” remotely, without their personal presence at the QTSP “Diia” premises or at a the QTSP “Diia” separate registration unit.

1.3.3. Users

Users are signatories for whom the QTSP “Diia” carries out their registration, formation and maintenance of their qualified certificates “Diia.Signature”.

Users can be

- users of the mobile application of the Diia Portal (Diia), in particular, natural persons who have been issued a passport of a citizen of Ukraine or a passport of a citizen of Ukraine for travelling abroad, or a permanent residence permit or a temporary residence permit issued using the tools of the Unified State Demographic Register, provided that the appropriate passport or the appropriate permit is valid;
- users of the mobile application «Diia Portal” (“Diia”), in particular, representatives of legal entities who have been issued a passport of a citizen of Ukraine or a passport of a citizen of Ukraine for travelling abroad, or a permanent residence permit or a temporary residence permit issued using the tools of the Unified State Demographic Register, provided that the appropriate passport or the appropriate permit is valid and the confirmation of the legal entity’s representative’s affiliation with the legal entity;
- users of the mobile application of the “E-Resident” Information System, in particular, foreign natural persons who acquire the status of E-resident and are identified by a foreigner’s passport in accordance with the Resolution of the Cabinet of Ministers of Ukraine No. 970 dated
September 05, 2023 “Some Issues of Electronic Residents (E-residents) Activities and Maintenance of the “E-Resident” Information System”.

Clause 1.3.1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains additional information.

1.3.4. Entities that trust the Provider

Natural and legal persons, as well as their Information and Communication Systems, are subjects that trust the QTSP “Diia” and use user qualified certificates “Diia.Signature” for the purpose of their authentication, in particular by verifying and confirming the remote qualified electronic signature “Diia.Signature”.

1.3.5. Other participants

Natural and legal persons directly or indirectly related to the formation and/or maintenance of user qualified certificates of the QTSP “Diia” and qualified certificates “Diia.Signature” of users are other participants.

Clause 1.3.5 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains additional information.

1.4. Use of the certificate

In accordance with the provisions of the Clause 5.5 of ETSI EN 319 411-1 and the Clause 5.5 of ETSI EN 319 411-2.

1.4.1. Permitted use of the certificate

Qualified certificates “Diia.Signature” can be used in Information and Communication Systems for the provision of electronic services, in which, in accordance with the legislation, a qualified electronic signature shall be used.

Qualified certificates “Diia.Signature” formed by the QTSP “Diia” are allowed to be used for:

- authentication;
- creation, verification and confirmation of a qualified electronic signature “Diia.Signature”.

All qualified certificates “Diia.Signature” formed by the QTSP “Diia” contain the value “1.2.804.2.1.1.1.2.2” in the “qualified certificate statement” extension.

1.4.1.1. Types of certificates

In accordance with these Regulations on Certification Practices, the QTSP “Diia” forms a qualified certificate “Diia.Signature”, which links the public key of the remote qualified electronic signature “Diia.Signature” to an natural person and confirms his/her identification data during authentication, as well as the creation, verification and confirmation of the qualified electronic signature “Diia.Signature”.

1.4.1.2. Validity of certificates

User qualified certificates “Diia.Signature” are formed by the QTSP “Diia” with a validity period of 1 year.

1.4.2. Prohibited use of the certificate

It is not allowed to use qualified certificate “Diia.Signature” in fields that do not correspond to the purpose of the public key (“keyUsage”) specified in the qualified certificate “Diia.Signature”.

1.5. Policy management

1.5.1. Responsibility for the document

These Regulations on Certification Practices are maintained by the State Enterprise “DIIA” (hereinafter referred to as SE “DIIA”).

SE “DIIA” is a legal entity of public law registered in accordance with the legislation - a state-owned commercial enterprise based on state property and belonging to the field of management of the Ministry of Digital Transformation of Ukraine.

Headquarters of the QTSP “Diia” is represented by the functional subdivision of the SE “DIIA”.

Details of the SE “DIIA”:

- Code according to the Unified State Register of Enterprises and Organisations of Ukraine (USREOU): 43395033.
- Address: 24 Dilova Str., Kyiv, 03150, Ukraine.
- Contact phone number: +38 (067) 258 05 20.

- E-mail address: inbox@diia.gov.ua.
  Details of the QTSP “Diia”:
- Website addresses: ca.diia.gov.ua; ca.informjust.ua.
- Contact phone number: +38 (067) 107 20 41.
- E-mail address: ca@diia.gov.ua.
- These Regulations on Certification Practices are structured in accordance with RFC 3647, “Internet Public Key Infrastructure X.509 Policy of the Certificates and Certification Practices”, and contain all the necessary information.

  These Regulations on Certification Practices, as well as amendments thereto, shall be signed by the Head of the specialised subdivision of the QTSP “Diia”, who is responsible for compliance with the practical actions and procedures defined in them, and approved by the Chief Executive Officer of the SE “DIIA”.

  These Regulations on Certification Practices, as well as amendments to them, are approved by the Ministry of Digital Transformation of Ukraine, which sends copies to the Administration of the State Service of Special Communications and Information Protection of Ukraine.

1.5.2. Amendments to the Regulations on Certification Practices

In accordance with the Clause 9.12 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

1.6. Definitions of terms and list of abbreviations

1.6.1. Definition of terms

In these Regulations on Certification Practices, the terms are used in the meanings given in the Civil Code of Ukraine, the Laws of Ukraine “On Information Protection in Information and Communication Systems”, “On Personal Data Protection”, “On the Unified State Demographic Register and Documents Confirming Ukrainian Citizenship, Identity or Special Status”, and “On Electronic Communications”, “On Electronic Identification and Electronic Trust Services”, Resolutions of the Cabinet of Ministers of Ukraine No. 764 dated August 28, 2024 “Some Issues of Compliance with Requirements in the Fields of Electronic Identification and Electronic Trust Services”, No. 1137 dated December 04, 2019 “Issues of the Unified State Web Portal of Electronic Services and the Register of Administrative Services”, No. 970 dated September 05, 2023 “Some Issues of Electronic Residents (E-residents) Activities and Maintenance of the “E-Resident” Information System” (hereinafter - the Resolution on E-residents), other legislative and regulatory acts in the fields of electronic trust services, cryptographic and technical protection of information, electronic communications.

1.6.2. List of abbreviations

Diia. Signature	Remote qualified electronic signature “Diia.Signature” (“Diia.ID”) created using the mobile application of the Diia Portal (Diia) or the mobile application of the “E-Resident” Information System
USDR	Unified State Demographic Register
USR	Unified State Register of Legal Entities, Natural Persons-Entrepreneurs and Community Groups
USREOU	Unified State Register of Enterprises and Organisations of Ukraine

ICS	Information and Communication System
Diia Portal	Unified State Web Portal of Electronic Services
RNTRC	Registration number of the taxpayer's registration card
URN	Unique Record Number in the USDR
CRL	Certificate Revocation List
OCSP	Online certificate status Protocol

2. PUBLICATION AND STORAGE OBLIGATIONS

In accordance with the provisions of the Clause 6.1 of ETSI EN 319 411-1 and the Clause 6.1 of ETSI EN 319 411-2.

2.1. Repository

Through its website (https://ca.diia.gov.ua), the QTSP "Diia" provides free access to:

- information about the QTSP "Diia";
- data on entering of information about the QTSP "Diia" in the Trust List;
- Policy of the Certificate;
- appropriate Regulations on Certification Practices;
- General terms and conditions for the provision of qualified electronic trust services to users of the QTSP "Diia";
- qualified certificates of the QTSP "Diia";
- a list of qualified electronic trust services provided by the QTSP "Diia";
- data on the tools of a qualified electronic signature or seal (QSCD) used in the provision of qualified electronic trust services by the QTSP "Diia";
- forms of documents on the basis of which qualified electronic trust services are provided;
- information on the separate registration units of the QTSP "Diia" and off-site Registration Administrators;
- register of valid, blocked and cancelled public key certificates;
- information about restrictions on the use of qualified certificates by users;
- data on the rules of order for verifying the validity of a qualified certificate, including the conditions for verifying the status of a qualified certificate;
- list of legislative acts in the field of electronic trust services.

These Regulations on Certification Practices are available 24 hours a day, 7 days a week in a read-only format on the QTSP "Diia" website (https://ca.diia.gov.ua).

2.2. Publication of information

2.2.1. Publication of user certificates

Certification Administrator of the QTSP "Diia" ensures the publication of qualified certificates "Diia.Signature" of users, the consent to the publication of which has been granted by such users, and revoked certificate lists (CRL) on the QTSP "Diia" website.

QTSP “Diia” provides free access to the register of valid, blocked and cancelled public key certificates through its website (https://ca.diia.gov.ua/).

2.2.2. Publication of Provider’s certificates

QTSP “Diia” provides free access to information on qualified certificates of the QTSP “Diia” through its website (https://ca.diia.gov.ua/).

Information about the qualified certificates of the QTSP “Diia” formed using the self-signed electronic seal certificate of the Central Certifying Authority, the status and restrictions on the use of such certificates, as well as revoked certificate lists (CRL) are contained in the register of valid, blocked and cancelled public key certificates maintained by the Central Certifying Authority (https://czo.gov.ua/).

2.2.3. Access to user certificates

QTSP “Diia” provides users with twenty-four-hour access to their own qualified certificates “Diia.Signature”.

Access of other persons to the user qualified certificates “Diia.Signature” is provided on condition that such users give their consent to the publication of their qualified certificates “Diia.Signature”.

2.2.4. Certificate expiration date

Date and time of the commencement and expiry of the validity period of the qualified certificate “Diia.Signature” shall be indicated in such qualified certificate with an accuracy of one second.

Qualified certificate “Diia.Signature” is considered cancelled after the date and time of expiration of such qualified certificate.

Validity of the qualified certificate “Diia.Signature” is one year.

2.3. Time and frequency of publication

QTSP “Diia” forms revoked certificate lists in the form of full and partial lists that comply with the following requirements:

- each revoked certificate list shall indicate the expiry date of its validity before a new list is published;
- a new revoked certificate list may be published before the expiry date of the certificate before the next list is published;
- a qualified electronic signature or seal of the QTSP “Diia” shall be affixed to the revoked certificate list

Revoked certificate lists are published automatically.

Time of change of status of qualified certificates is synchronised with the Coordinated Universal Time (UTC) with an accuracy of one second.

Links to revoked certificate lists are included in user qualified certificates.

A complete list of revoked certificates is formed and published 1 (once) a week and contains information on all revoked qualified certificates formed by the QTSP “Diia”.

Partial revoked certificate list is formed and published every 2 (Two) hours and contains information on all revoked qualified certificates whose status has been changed in the interval between the time of publishing of the last full revoked certificate list and the time of formation of the current partial revoked certificate list.

2.4. Control of access to the repository

Qualified certificates of the QTSP “Diia” and users, revoked certificate lists, appropriate Regulations on Certification Practices and QTSP “Diia” Policy of the Certificate are available in the repository 24 hours a day, 7 days a week.

Read-only access is unlimited. Changes to the repository and website are made exclusively by the QTSP “Diia”

The user can find information about his/her qualified certificate “Diia.Signature” by searching for it on the QTSP “Diia” website in the “Certificate Search” section, filling in the appropriate tabs with information about the RNTRC (if not available, the series (if any) and passport number) or the serial number of the qualified certificate.

3. IDENTIFICATION AND AUTHENTICATION

In accordance with the provisions of the Clause 6.2 of ETSI EN 319 411-1 and the Clause 6.2 of ETSI EN 319 411-2.

3.1. Designations

Qualified certificates issued by the QTSP “Diia” shall contain the information specified in the Part two of the Article 23 of the Law of Ukraine “On Electronic Identification and Electronic Trust Services”, in particular:

1) a mark (in a form suitable for automated processing) that the certificate is issued as a qualified certificate;

2) a mark that the certificate was issued in Ukraine;

3) identification data that clearly defines the QTSP “Diia”, including the name and code according to the USREOU;

4) identification data that clearly defines the user:

- surname, first name, patronymic (if any) of the person;
- URN;
- RNTRC (if any) or series (if any) and passport number of a citizen of Ukraine (for natural persons who, due to their religious beliefs, refuse to accept RNTRC and have officially notified the appropriate supervisory authority and have a note in their passport), if the appropriate information is available in the USDR;
- code according to USREOU (for a representative of a legal entity);
- name of the legal entity (for a representative of a legal entity);

5) value of the public key that corresponds to the private key;

6) information on the commencement and expiry of the validity period of the qualified certificate;

7) the serial number of the qualified certificate, unique to the QTSP “Diia”;

8) qualified electronic signature created by QTSP “Diia”;

9) information on the place of location in free-of-charge access of the qualified certificate, which is used to verify the advanced electronic signature or seal provided for in the Subclause 8 of this Clause;

10) information on the place of the service for verifying the status of the appropriate qualified certificate;

11) an indication that the private key linked to the public key is stored in a qualified electronic signature or seal tool - in a form suitable for automated processing.

Qualified certificates may contain information on restrictions on the use of a qualified electronic signature or seal.

Qualified certificates may contain other optional additional special attributes as defined in the standards for qualified certificates. Such attributes shall not affect the interoperability and recognition of qualified electronic signatures or seals.

Information contained in qualified certificates complies with the designations (details, attributes) defined in the standards for certificate profiles in accordance with the Clause 7.1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures).

Designations used in user qualified certificates are shown in the Table 2.

Table. 2. Designations used in user qualified certificates

Name	Value
Country (C)	Country name in accordance with DSTU ISO 3166-1:2009 “International Country Names Codes” (ISO 3166-1:2006, IDT), approved by the Order of the State Committee of Ukraine for Technical Regulation and Consumer Policy No. 471 dated December 23, 2009
Organization (O)	Name of the legal entity for a qualified certificate of a legal entity’s representative. This field is not available for qualified certificates of natural persons and e-residents who do not belong to a legal entity
Organizational Unit (OU)	Name of a subdivision or department in the organisation. This field is not available for qualified certificates of natural persons and e-residents who do not belong to a legal entity
State or Province (S)	Name of the user’s region of place of location or place of registration Name the legal entity’s region of place of registration for a qualified certificate of a representative of legal entity
Locality (L)	Name of the city of the place of location or place of registration of the user Name of the legal entity’s city of registration for the qualified certificate of the representative of legal entity
Common Name (CN)	Full name of the user who owns the qualified certificate
E-Mail Address (E)	E-mail of the user who owns the qualified certificate
Title (T)	Title (for qualified certificates of representatives of legal entity, if necessary)

Unique Identifier (UID)	Identifier of the user owns the qualified certificate: - for users who are natural persons, the RNTRC or series (if available) and passport number are used as the UID; - for users that are legal entities, the code according to the USREOU is used as the UID;

3.1.1. Types of certificate designations

The types of designations (details, attributes) of a qualified certificate that correspond to the information contained in qualified certificates are defined in the standards for certificate profiles in accordance with the Clause 7.1 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures).

3.1.2. Designation (details and attributes) of certificates

A qualified certificate shall have all the necessary designations (details, attributes) defined in the standards for certificate profiles in accordance with clause 7.1 of the QTSP "Diia" Policy of the Certificate.

3.1.3. Anonymity or use of pseudonyms

Not applicable.

3.1.4. Rules for interpreting different forms of certificate designations

International letters should be encoded according to UTF-8.

3.1.5. Uniqueness of certificate designations

QTSP "Diia" ensures that certificates with the same data specified in the "Common Name" and "Serial Number" fields are not issued to different users.

3.1.6. Acknowledgment, authentication and the role of trademarks

Not applicable.

3.2. Initial identification verification

3.2.1. Method of confirming possession of a private key

Private key of the qualified electronic signature "Diia.Signature" consists of two parts.

One part is stored in the user's smartphone, and the other part is stored in the qualified electronic signature tool, which is a hardware and software device located in a separate, specially designed premises of the QTSP "Diia".

To confirm possession of the private key of the qualified electronic signature "Diia.Signature", it is necessary to confirm the identity by authorization in the mobile application of the Diia Portal (Diia) or the mobile application of the "E-resident" Information System and performing face recognition and entering the PIN code to the private key of the qualified electronic signature "Diia.Signature".

Activation and use of the signer's private key in the remote qualified signature creation device (QSCD) require at least two-factor authentication of the signer.

3.2.2. Identity authentication

3.2.2.1. Identification of natural persons and representatives of legal entities

Persons who have been issued a passport of a citizen of Ukraine or a passport of a citizen of Ukraine for travelling abroad, or a permanent residence permit or a temporary residence permit issued using the tools of the USDR may, at their own request, use the mobile application of the Diia Portal (Diia), and representatives of a legal entity, after receiving confirmation of belonging to a legal entity in the mobile application of the Diia Portal (Diia), apply for the specified service for the formation of a qualified certificate "Diia.Signature", provided that the appropriate passport or residence permit is valid. Identification of such persons is carried out remotely without their personal presence at the premises of the QTSP "Diia" or at QTSP "Diia" separate registration unit by performing a set of the following procedures:

1. identification of a person using information from the USDR on the basis of a request from the mobile application of the Diia Portal (Diia) transmitted by the unified information system tools of the Ministry of Internal Affairs containing information that allows clearly identify a person. The request is formed on the basis of the person's identification data transferred to the mobile application of the Diia Portal (Diia) using the BankID System of the National Bank or read by the person using the mobile application of the Diia Portal (Diia) from a contactless electronic medium implanted in the person's passport of a citizen of Ukraine or passport of a citizen of Ukraine for travelling abroad, or permanent residence permit or temporary residence permit issued by the USDR;
2. verification of the validity of a passport of a citizen of Ukraine or a passport of a citizen of Ukraine for travelling abroad, or a permanent residence permit or a temporary residence permit issued to a person using the USDR tools, using the information of the USDR and the database of stolen (lost) documents at the applications of citizens of the Unified Information System of the Ministry of Internal Affairs on the basis of a request transmitted by the Unified Information System of the Ministry of Internal Affairs from the mobile application of the Diia Portal (Diia) containing information that allows for unambiguous identification of the person;
3. facial recognition by comparing a photo image of a person created by the person using the mobile application of the Diia Portal (Diia) with the digitised image of the person's face, transferred from the USDR with tools of the Unified Information System of the Ministry of Internal Affairs to the mobile application of the Diia Portal (Diia) (provided that the person has given unambiguous consent for the processing of his/her personal data in terms of transferring a digitised facial image to the State Migration Service) or read by the person using the mobile application of the Diia Portal (Diia) from a contactless electronic medium, implanted in a passport of a citizen of Ukraine or a passport of a citizen of Ukraine for travelling abroad, or a permanent residence permit or a temporary residence permit issued to a person with the use of the USDR tools. Face recognition is carried out using the mobile application of the Diia Portal (Diia) tools, provided that the verification of the absence of signs of an attack on the biometric presentation and third-party influence on the person is successful;
4. application of additional mechanisms for identity verification.

Data and documents on the basis of which the services are provided are stored in the archive of the QTSP "Diia".

Clause 5.5 of the QTSP "Diia" Policy of the Certificate contains information on the types of documents and data subject to archival storage, archive retention periods, archive protection, archive

backup procedures, requirements for affixing the electronic time stamps on records, archive collection systems, procedures for obtaining and verifying archival information.

3.2.2.2. Identification of E-residents

A person, a foreigner who has applied for e-resident status acquisition and has undergone the verification procedures provided for by the Resolution on E-Residents and, in case of successful identification by documents displayed in the "E-resident" Information System, may independently apply for the service of formation of a qualified certificate "Diia.Signature" using the mobile application of the E-Resident information system, provided that the documents in the "E-resident" Information System are valid.

Identification of foreigners for formation of a qualified certificate "Diia.Signature" is carried out remotely without their personal presence at the premises of the QTSP "Diia" or at separate registration unit of the QTSP "Diia" by performing a set of the following procedures:

1) verification of the person using the "E-resident" Information System on the basis of a transmitted request from the mobile application of the "E-resident" Information System containing information that allows to unequivocally identify the person. Request is formed on the basis of the person's identification data transmitted to the mobile application of the "E-Resident" Information System using the "E-resident" Information System;

2) facial recognition by comparing a photo of a person created by him/her using the mobile application of the "E-resident" Information System with the digitised image of the person's face uploaded to the "E-resident" Information System by an official of a foreign diplomatic mission of Ukraine. Face recognition is carried out with tools of the mobile application of the "E-resident" Information System.

Until the appropriate amendments to these Regulations on Certification Practices are made, the QTSP "Diia" may use identification procedures other than those specified in this Clause, which have been assessed and, in accordance with the requirements of the legislation, ensure proper identification, according to the preliminary description of such identification procedures on the QTSP "Diia" website.

Data and documents on the basis of which the services are provided are stored in the archive of the QTSP "Diia".

Clause 5.5 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the types of documents and data subject to archival storage, archive storage periods, archive protection, archive backup procedures, requirements for affixing the electronic time stamps on records, archive collection systems, procedures for obtaining and verifying archival information.

3.2.3. Unverified user information

3.2.3.1 Unverified information about the user (natural person and representative of a legal entity)

Identification of a person is carried out by QTSP "Diia" by verifying and confirming the identification data of a person received by QTSP "Diia" from the USDR, and for representatives of a legal entity, additionally receiving confirmation of the affiliation of such a person to a legal entity from the Head of the legal entity or an authorised representative of the legal entity that applied for the service of formation of a qualified certificate "Diia.Signature".

In order to verify the validity of a passport of a citizen of Ukraine or a passport of a citizen of Ukraine for travelling abroad or a permanent residence permit or a temporary residence permit issued to

a person using the USDR tools, using the database of stolen (lost) documents, upon requests of citizens of the Unified Information System of the Ministry of Internal Affairs from the USDR, the information on the number of the appropriate passport or the appropriate residence permit is transferred to the mobile application of the Diia Portal (Diia) with tools of the Unified Information System of the Ministry of Internal Affairs.

3.2.3.2. Unverified user information (e-resident)

Identification of a foreigner who has applied for e-resident status is carried out by the QTSP "Diia" by verifying and confirming the identification data of the person received by QTSP "Diia" from the "E-resident" Information System, who has applied for the service of formation of a qualified certificate "Diia.Signature".

Verification of the validity of a passport document of a foreigner who has applied for e-resident status is carried out in accordance with the Resolution on E-residents.

Formation of a qualified certificate "Diia.Signature" of a foreigner who has obtained the status of an e-resident after the expiration of the period of confirmed identification data use (1 year), provided that his/her data contained in the Information System "E-resident" is unchanged, and in the case when the passport expires no earlier than in three months, is carried out subject to the identification of the appropriate natural person in accordance with the requirements of the Clause 3.2.2.2 of these Regulations on Certification Practices.

If a passport document expires in less than three months, a foreigner who has been granted e-resident status shall change the passport document, update the data in his/her e-resident account and be identified by an official of a foreign diplomatic mission of Ukraine.

After receiving a new passport document, in which his/her personal data has not changed, the foreigner shall upload a copy of the new passport document to the e-resident electronic cabinet and undergo the identification procedure in accordance with the Resolution on E-residents, followed by receiving a qualified electronic trust service for the formation of a qualified certificate "Diia.Signature" provided by the QTSP "Diia" on the basis of a new passport document with the simultaneous cancellation of the previous certificate valid at the moment.

In case of receiving a new passport document with changed personal data, a foreigner shall undergo again the identification procedure in accordance with the Resolution on E-residents with the subsequent receipt of a qualified electronic trust service for the formation of a qualified certificate "Diia.Signature" provided by the QTSP "Diia" on the basis of a new passport document with the simultaneous cancellation of the previous certificate valid at the moment.

3.2.4. Confirmation of powers

QTSP "Diia" provides formation of qualified certificates "Diia.Signature" for representatives of legal entities.

Powers of the Head and authorised person of a legal entity are confirmed by a record in the USREOU or a Power of Attorney issued by the Head of this legal entity.

Authentication and verification of representatives of legal entities are carried out in accordance with the Clauses 3.2.2.1 and 3.2.3.1 of these Regulations on Certification Practices.

3.3. Identification and authentication for requests of change of keys

3.3.1. Identification and authentication of the user on the basis of the application for certificate formation, provided that the previous certificate is valid

3.3.1.1. For natural persons and representatives of legal entities

Formation of the qualified certificate “Diia.Signature” instead of the valid previous qualified certificate “Diia.Signature” is carried out subject to the identification of the appropriate natural person and representative of the legal entity in accordance with the requirements of the Clauses 3.2.2.1 and 3.2.3.1 of these Regulations on Certification Practices. In this case, the previous qualified certificate “Diia.Signature” is cancelled.

3.3.1.2. For E-residents

Formation of the qualified certificate “Diia.Signature” instead of the previous qualified certificate “Diia.Signature” is carried out subject to the identification of the e-resident in accordance with the requirements of the Clauses 3.2.2.2 and 3.2.3.2 of these Regulations on Certification Practices. In this case, the previous qualified certificate “Diia.Signature” is cancelled.

3.3.2. Identification and authentication of the user to receive a second key in case of certificate cancellation

Formation of the qualified certificate “Diia.Signature” after the expiration of the period of confirmed identification data use (1 year) is carried out subject to the identification of the appropriate natural person, representative of the legal entity and e-resident in accordance with the requirements of the Clauses 3.2.2 and 3.2.3 of these Regulations on Certification Practices.

3.4. User identification and authentication based on applications on certificate blocking or cancellation

Identification and authentication of the user, when cancelling the “Diia.Signature” certificate, is carried out with tools of the mobile application of the Diia Portal (Diia) for natural persons and representatives of legal entities and the mobile application of the “E-resident” Information System for e-residents by authorising the user in the mobile application with a password or Face ID, which are set during the initial authentication of the user in the mobile application of the Diia Portal (Diia) and the mobile application of the “E-Resident” Information System in accordance with the Clause 3.2.2 of these Regulations on Certificate Practices.

Qualified certificate “Diia.Signature” is cancelled in accordance with the requirements of Clause 4.9 of these Regulations on Certification Practices.

Formation of a qualified certificate “Diia.Signature” after the expiration of the confirmed identification data (1 year) is carried out subject to the identification of the appropriate natural person in accordance with the requirements of the Clauses 3.2.2 and 3.2.3 of these Regulations on Certification Practices.

4. REQUIREMENTS FOR THE CERTIFICATE LIFECYCLE

According to the provisions of the Clause 6.3 of ETSI EN 319 411-1 and the Clause 6.3 of ETSI EN 319 411-2.

4.1. Certificate formation request

Qualified certificate formation request may be submitted only by users specified in the Clause 1.3.3 of these Regulations on Certification Practices, who have passed the identification and authentication procedures in accordance with the Clauses 3.2.2 and 3.2.3 of these Regulations on Certification Practices.

4.1.1. For a natural person

User registration process includes the following steps:

1) user authorisation in the mobile application of the Diia Portal (Diia), which involves identification and authentication of the user with tools of the mobile application of the Diia Portal (Diia);
2) preparation of a package of documents on behalf of the user, including an application for accession to the Agreement on the Provision of Qualified Electronic Trust Services, which provides for:

- sending the formed package of documents to the QTSP “Diia” by tools of the mobile application of the Diia Portal (Diia);
- verification of the correctness of the formed documents by the QTSP “Diia”;

3) generating a key pair “Diia.Signature” of the user using the mobile application of the Diia Portal (Diia), for which it is required:

- to click on “Create Diia.Signature” in the menu of the mobile application of the Diia Portal (Diia);
- to confirm the identity by photo verification and by verifying the identification data obtained from the passport of a citizen of Ukraine in the form of an ID card or passport of a citizen of Ukraine for travelling abroad, or a permanent residence permit, or a temporary residence permit using NFC technology;
- to create a 6-digit access code to the private key “Diia.Signature”;
- to form a qualified certificate “Diia.Signature” by the QTSP “Diia” to the user on the basis of the user’s identification data.

4.1.2. For representatives of legal entities

4.1.2.1. For the Head of a legal entity

In accordance with the USREOU data, in the mobile application of the Diia Portal (Diia), the Head of the legal entity has access to the section “For legal entities”, in which it is possible to create “Diia.Signature” for the representative of the legal entity.

User (Head) registration process includes the following steps:

1) user authorisation in the mobile application of the Diia Portal (Diia), which provides for identification and authentication of the user with tools of the mobile application of the Diia Portal (Diia);
2) creating a package of documents on behalf of the user, including an application for accession to the Agreement on the Provision of Qualified Electronic Trust Services and signing it, which provides for:

- sending the formed package of documents to the QTSP “Diia” with tools of the mobile application of the Diia Portal (Diia);
- verification of the correctness of the documents by the QTSP “Diia”;

3) generating a pair of keys “Diia.Signature” of the user using the mobile application of the Diia Portal (Diia), for which it is required:

- to click on “Create Diia.Signature” in the section “For legal entities” in the menu of the mobile application of the Diia Portal (Diia);

- to confirm the identity by photo verification and by verifying the identification data obtained from the passport of a citizen of Ukraine in the form of an ID card or passport of a citizen of Ukraine for travelling abroad, or a permanent residence permit, or a temporary residence permit using NFC technology;
- to create a 6-digit access code to the private key “Diia.Signature” of the representative of the legal entity;
- to form a qualified certificate “Diia.Signature” of the Head of a legal entity based on the user’s identification data by the QTSP “Diia”.

4.1.2.2 For a representative of a legal entity

Process of registering a user (representative of a legal entity) includes the following steps:

1) user authorisation in the mobile application of the Diia Portal (Diia), which involves identification and authentication of the user with tools of the mobile application of the Diia Portal (Diia);
2) to receive confirmation of affiliation to a legal entity by receiving a Push-notification about the possibility of creating a “Diia.Signature” of a representative of a legal entity in the mobile application of the Diia Portal (Diia);
3) creation of a package of documents on behalf of the user, in particular, receipt of an application for accession to the Agreement on the Provision of Qualified Electronic Trust Services signed by the Head or authorised person of the legal entity and its signing, which provides for:
- sending the formed package of documents to the QTSP “Diia” with tools of the mobile application of the Diia Portal (Diia);
- verification of the correctness of the documents by the QTSP “Diia”;
4) generation of a pair of keys “Diia.Signature” of the user using the mobile application of the Diia Portal (Diia), for which it is required:
- to click “Create Diia.Signature” in the mobile application of the Diia Portal (Diia);
- to confirm the identity by photo verification and by verifying the identification data obtained from the passport of a citizen of Ukraine in the form of an ID card or passport of a citizen of Ukraine for travelling abroad, or a permanent residence permit, or a temporary residence permit using NFC technology;
- to create a 6-digit access code to the private key “Diia.Signature” of the representative of the legal entity;
- to form a qualified certificate “Diia.Signature” of a representative of a legal entity based on the user’s identification data by the QTSP “Diia”.

4.1.3. For e-residents

Process of user registration (e-resident) includes the following steps:

1) to go through authorisation in the mobile application of the “E-resident” Information System using a one-time QR code created by the “E-resident” Information System, by scanning which the user is authenticated in the mobile application of the “E-resident” Information System;
2) creating a package of documents on behalf of the e-resident, including an application for accession to the Agreement on the Provision of Qualified Electronic Trust Services and signing it, which provides for:
- sending the formed package of documents to the QTSP “Diia” with tools of the mobile application of the “E-Resident” Information System;
- verification of the correctness of the documents by the QTSP “Diia”;

3) generation of key pair “Diia.Signature” of users using the mobile application of the Diia Portal (Diia), for which it is required:
- to click “Create Diia.Signature” in the menu of the mobile application of the “E-resident” Information System;
- to confirm the identity by photo verification;
- to create a 6-digit access code to the user’s private key “Diia.Signature”;
- formation of a qualified certificate “Diia.Signature” of an e-resident by the QTSP “Diia” based on the user’s identification data received from the mobile application of the “E-resident” Information System.

4.2. Processing a certificate formation request

Processing of a qualified certificate “Diia.Signature” formation request for is carried out automatically with the software tools of the QTSP “Diia” ICS, provided that the processes of generating key pairs, forming requests, and transmitting them for processing via secure communication channels that ensure confidentiality and integrity of data are continuous. The automatic processing of requests is carried out after the user’s identity is identified and the user confirms that he or she owns a private key, the corresponding public key of which is provided to form a qualified certificate “Diia.Signature”.

When processing a qualified certificate “Diia.Signature” formation request, the uniqueness of the public key in the register of valid, blocked and cancelled public key certificates is verified by the tools of the QTSP “Diia” ICS and the uniqueness of the serial number of the user’s qualified certificate “Diia.Signature” is ensured.

Processing time for a qualified certificate “Diia.Signature” formation request submitted together with the application for registration is no more than one hour.

If the user has a valid qualified certificate “Diia.Signature”, it will be cancelled after processing the request for a formation of a new qualified certificate “Diia.Signature”.

4.3. Formation of a certificate

Provision of the formed qualified certificate to the user is carried out by publishing the formed qualified certificate on the QTSP “Diia” website.

4.4. Certificate acceptance

User shall verify his/her identification data entered by QTSP “Diia” into the qualified certificate within one day. QTSP “Diia” shall provide appropriate consultations on how to conduct such verification. User shall use the private key to create a qualified electronic signature only after verification. Use of the private key by the user is a fact of recognition of the qualified certificate corresponding to his/her public key.

In case the user found a discrepancy between the identification data entered by the QTSP “Diia” in the qualified certificate, the user shall contact the QTSP “Diia” to cancel the qualified certificate and form a new certificate in accordance with the procedure established by this Policy of the Certificate and the appropriate Regulations on Certification Practices.

In case of discrepancies between the identification data entered by the QTSP “Diia” into the qualified certificate and found by the QTSP “Diia” prior to the provision of the formed qualified certificate to the user, QTSP “Diia” shall provide repeated formation of the qualified certificate in compliance with the requirements for preventing the validity of the private key and its corresponding public key from exceeding one year.

User has the opportunity to familiarise with the terms of service, which are posted on the QTSP “Diia” website and are specified in:

- Agreement on the Provision of Qualified Electronic Trust Services;
- General terms and conditions for the provision of qualified electronic trust services to users of the Qualified Trust Service Provider "Diia'.

4.5. Key pair and certificate purpose

4.5.1. Use of a private key and certificate by the user

User shall use a private key and a qualified certificate in accordance with the requirements of the legislation and in accordance with:

- Policy of the QTSP "Diia" certificate;
- these Regulations on Certification Practices;
- General terms and conditions for the provision of qualified electronic trust services to users of the QTSP "Diia";
- Agreement for the Provision of Qualified Electronic Trust Services concluded with the QTSP "Diia" (SE "DIIA").

4.5.1.1. Receiving a qualified certificate "Diia.Signature" of a natural person

To receive a qualified certificate "Diia.Signature", the user shall:

- install the mobile application of the Diia Portal (Diia) on an electronic medium whose criteria support the use of this mobile application (iOS 11.2 operational system or later or Android 4.4 or later);
- have a passport of a citizen of Ukraine in the form of an ID-card or a passport of a citizen of Ukraine for travelling abroad, or a permanent residence permit or a temporary residence permit issued using the tools of the USDR;
- log in to the mobile application of the Diia Portal (Diia) using BankID or NFC technology;
- select "Diia.Signature" in the "Menu" section of the mobile application of the Diia Portal (Diia), read the application for accession to the Agreement on the Provision of Qualified Electronic Trust Services, which is signed in the process of creating "Diia.Signature", click "Activate Diia.Signature" and confirm your identity with a photo and by verifying the identification data obtained from the passport of a citizen of Ukraine in the form of an ID card or passport of a citizen of Ukraine for travelling abroad, or a permanent residence permit, or a temporary residence permit using NFC technology, enter a 6-digit digital code for "Diia.Signature".

Clause 4.5.1 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) and the section "Issues regarding Diia.Signature" on the QTSP "Diia" website contain additional information on the use of a private key and qualified certificate by the user.

4.5.1.2 Receiving a qualified certificate "Diia.Signature" by a representative of a legal entity

To receive a qualified certificate "Diia.Signature" of a representative of a legal entity (Head), the user shall:

- install the mobile application of the Diia Portal (Diia) on an electronic medium whose criteria support the use of this mobile application (iOS 11.2 operational system or later or Android 4.4 or later);
- have a passport of a citizen of Ukraine in the form of an ID-card or a passport of a citizen of Ukraine for travelling abroad, or a permanent residence permit or a temporary residence permit issued using the tools of the USDR;
- log in to the mobile application of the Diia Portal (Diia) using BankID or NFC technology;

- have activated “Diia.Signature”;
- in the “Menu” section in the mobile application of the Diia Portal (Diia), select “For legal entities” section, which is created in accordance with the data from the USREOU, and select “Diia.Signature”, read the application for accession to the Agreement on the Provision of Qualified Electronic Trust Services, which is signed in the process of creating “Diia. Signature” of the representative of the legal entity, click “Activate “Diia.Signature” and confirm his/her identity with a photo and by verifying the identification data obtained from the passport of a citizen of Ukraine in the form of an ID card or passport of a citizen of Ukraine for travelling abroad, or a permanent residence permit, or a temporary residence permit using NFC technology, enter a 6-digit digital code for “Diia.Signature”.

To receive a qualified “Diia.Signature” certificate of a representative of a legal entity, the user shall:

- install the mobile application of the Diia Portal (Diia) on an electronic medium whose criteria support the use of this mobile application (iOS 11.2 operational system or later or Android 4.4 or later);
- have a passport of a citizen of Ukraine in the form of an ID-card or a passport of a citizen of Ukraine for travelling abroad, or a permanent residence permit or a temporary residence permit issued using the tools of the USDR;
- log in to the mobile application of the Diia Portal (Diia) using BankID or NFC technology;
- have activated “Diia.Signature”;
- receive confirmation of affiliation to a legal entity by receiving a Push notification about the possibility of forming a “Diia.Signature” of a representative of a legal entity;
- read and sign an application for accession to the Agreement, which is signed in the process of creating a “Diia.Signature” of a representative of a legal entity, click “Activate “Diia.Signature” and confirm his/her identity with a photo and by verifying the identification data obtained from the passport of a citizen of Ukraine in the form of an ID card or passport of a citizen of Ukraine for travelling abroad, or a permanent residence permit, or a temporary residence permit using NFC technology, enter a 6-digit digital code for “Diia.Signature”.

Clause 4.5.1 of the QTSP “Diia” Policy of the Certificate and the section “Issues regarding Diia.Signature” on the QTSP “Diia” website contain additional information on the use of a private key and a qualified certificate by the user.

4.5.1.3. Receiving an e-resident qualified certificate “Diia.Signature”

To receive a qualified certificate “Diia.Signature”, the user shall:

- install the mobile application of the “E-resident” Information System on an electronic medium whose criteria support the use of this mobile application (iOS 11.2 operational system or later or Android 4.4 or later);
- have a passport document of a foreigner entered into the “E-resident” Information System in accordance with the Resolution on E-residents;
- log in to the in the mobile application of the “E-resident” Information System using a one-time QR code created by the “E-resident” Information System, by scanning which the user is authenticated in the mobile application of the “E-resident” Information System;
- select “Diia.Signature” in the “Menu” section of the mobile application of the “E-resident” Information System, read the application for accession to the Agreement on the Provision of Qualified Electronic Trust Services, which is signed in the process of creating “Diia.Signature”, click “Activate “Diia.Signature” and confirm his/her identity with a photo and by verifying the identification data obtained from the passport of a citizen of Ukraine in the form of an ID card or passport of a citizen of

Ukraine for travelling abroad, or a permanent residence permit, or a temporary residence permit using NFC technology, enter a 6-digit digital code for “Diia.Signature”.

Clause 4.5.1 of the QTSP “Diia” Policy of the Certificate and the section “Issues regarding Diia.Signature” on the QTSP “Diia” website contain additional information on the use of a private key and a qualified certificate by the user.

4.5.2. Use of a public key and certificate by entities that trust the Provider

When using a public key and a qualified user certificate, entities that trust the QTSP “Diia” shall comply with the requirements of the legislation in the field of electronic trust services, as well as the provisions of:

- these Regulations on Certification Practices;
- Policy of the Certificate QTSP “Diia”.

Clause 4.5.2 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains additional information on the use of the public key and qualified certificate by entities that trust the QTSP “Diia”.

4.6. Certificate renewal

Not applicable.

Upon expiry of the qualified certificate “Diia.Signature”, such certificate is automatically cancelled, and with the aim to receive a new certificate “Diia.Signature”, the user shall go through the procedure provided for in the Clause 3.2.2 again.

4.7. Repeated formation of the certificate

Formation of the qualified certificate “Diia.Signature” after the expiration of the period of use of the confirmed identification data (1 year) is carried out subject to the identification of the appropriate natural person in accordance with the requirements of the Clause 3.2.2 of these Regulations on Certification Practices.

Repeated (guaranteed) formation of the qualified certificate “Diia.Signature” for representatives of legal entities is possible within the validity of the previously formed qualified certificate, taking into account the terms of the tariff plan and subject to the identification of representatives of legal entities in accordance with the requirements of the Clause 3.2.2.1 of these Regulations on Certification Practices and the invariability of the data specified in the previously formed qualified certificate.

4.8. Change of the certificate

Changing the identification data entered in the qualified user certificate is a reason for cancelling the qualified certificate.

4.9. Blocking and cancelling a certificate

Not later than within two hours, the QTSP “Diia” shall early terminate the use of verified identification data for the provision of the service for the formation of a qualified certificate “Diia.Signature” with the simultaneous cancellation of such a certificate, valid at that time, in case of:

1) user submitting an application for early termination of the use of verified identification data belonging to him/her for the provision of the service for the formation of a qualified certificate “Diia.Signature” in any way that ensures the confirmation of the user’s identity;

2) notification by the user or the Administration of the State Service of Special Communications and Information Protection of Ukraine of suspicion of compromise of a private key belonging to the user;

3) receipt by the QTSP “Diia” of a document confirming that:

change of confirmed identification data;

unreliability of the confirmed identification data;

death of a natural person - user;

the entry into force of a court decision on the early termination of the use of the user’s verified identification data for the provision of the service for formation of a qualified certificate “Diia.Signature”, the declaration of a natural person - user deceased, recognition of him/her as missing, incapacitated, limitation of his/her civil capacity, recognition of his/her bankruptcy;

4) violation by the user of the essential terms of the agreement on the provision of qualified electronic trust services;

5) termination of the Agreement for the Provision of Qualified Electronic Trust Services;

6) termination of the use by the user of the mobile application of the Diia Portal (Diia) or the mobile application of the “E-resident” Information System.

In accordance with the application for accession to the Agreement for the Provision of Qualified Electronic Trust Services, the user agrees to the automatic cancellation of the valid qualified certificate “Diia.Signature” in the case of:

independently deactivating “Diia.Signature” in the mobile application of the Diia Portal (Diia) or the mobile application of the “E-resident” Information System;

deactivation of “Diia.Signature” of the representative of the legal entity in the mobile application of the Diia Portal (Diia) by the Head of the legal entity or an authorised representative of the legal entity;

when forming a new qualified certificate “Diia.Signature” in the mobile application of the Diia Portal (Diia) or in the mobile application of the “E-Resident” Information System;

logging out of the mobile application of the Diia Portal (Diia) or the mobile application of the “E-resident” Information System.

Cancelled qualified certificates “Diia.Signature” are included in the revoked certificate lists published on the QTSP “Diia” website. Partial revoked certificate list is updated every 2 hours, complete revoked certificate list is updated once every 7 days.

4.10. Certificate status verification service

QTSP “Diia” ensures the availability of information on the certificate status in real time using the OCSP server and revoked certificate lists (CRL) published on the QTSP “Diia” website.

QTSP “Diia” ensures the availability of information on the certificate status 24 hours a day, 7 days a week.

For the ‘Diia.Signature’ service, the ICS guarantees immediate reflectivity of status after revocation/blocking operations and produces correct OCSP/CRL responses. Availability targets, monitoring and logging shall comply with this CPS and the Certificate Policy requirements for OCSP/CRL services.

The ICS performs periodic checks of the CP/CPS URLs embedded in certificates (CPS Pointer) and records the results in the monitoring log.

4.11. Certificate expiry date

Date and time of the commencement and expiry of the user certificate validity period are indicated in the certificate with an accuracy of one second.

After the date and time of expiry of the user certificate specified in it, such certificate shall be deemed cancelled.

If it is necessary to terminate the service of the qualified certificate "Diia.Signature" early, the user may apply to the QTSP "Diia" with an application for cancellation of such a certificate according to the procedure specified in the Clause 4.9 of these Regulations on Certification Practices or independently initiate automatic cancellation of the valid qualified certificate "Diia.Signature" in the following cases:

- independently deactivating the "Diia.Signature" in the mobile application of the Diia Portal (Diia) or in the mobile application of the "E-resident" Information System;
- deactivation of "Diia.Signature" of the representative of the legal entity in the mobile application of the Diia Portal (Diia) by the Head of the legal entity, the authorised representative of the legal entity or the Registration Administrator upon request;
- during the formation of a new qualified certificate "Diia.Signature" in the mobile application of the Diia Portal (Diia) or in the mobile application of the "E-resident" Information System;
- logging out of the mobile application of the Diia Portal (Diia) or the mobile application of the "E-resident" Information System.

4.12. Depositing and returning keys

Not applicable.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROL

In accordance with the provisions of the Clause 6.4 of ETSI EN 319 411-1 and the Clause 6.4 of ETSI EN 319 411-2.

5.1. Physical security control

Clause 5.1 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the requirements for the premises of the QTSP "Diia" and physical access to them.

5.2. Procedural control

Clause 5.2 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the trusted roles of the QTSP "Diia" personnel (Head, Registration Administrator, Certification Administrator, Security Administrator, System Administrator, System Auditor) and their functional responsibilities, on the number of persons required to carry out the tasks, as well as on the trusted roles of the QTSP "Diia" personnel requiring the distribution of responsibilities.

5.3. Personnel control

Clause 5.3 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the requirements for qualification, experience and competency of the QTSP "Diia" personnel, training requirements and procedures,

sanctions for unauthorised actions, control of the QTSP “Diia” separate registration units, documentation provided to the QTSP “Diia” personnel.

5.4. Maintaining an event audit log book

Clause 5.4 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the types of recorded events, frequency of event audit log book processing, event audit log retention periods, event audit log protection, event audit log backup procedures and time synchronisation issues.

5.5. Document archive

Clause 5.5 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the types of documents and data subject to archival storage, archive storage periods, archive protection, archive backup procedures, requirements for affixing the electronic time stamps on records, archive collection systems, procedures for obtaining and verifying archival information.

5.6. Change of the key

Clause 5.6 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the reasons and frequency of changing the key pair of the QTSP “Diia”, the procedure for using and accessing the current public key of the QTSP “Diia”.

5.7. Compromise and disaster renewal

Clause 5.7 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on incident and compromise handling procedures, renewal procedures if computing resources, software and/or data are damaged, renewal procedures after compromise of a private key, business continuity capabilities after a disaster.

5.8. Termination of the Provider’s activity

Clause 5.8 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the reasons for termination of the QTSP “Diia” activity, the procedure for providing notification of termination, determining the date of termination, succession and transfer of documented information, as well as the Plan for termination of the activity of providing qualified electronic trust services of the QTSP “Diia”.

6. TECHNICAL SAFETY MEASURES

In accordance with the provisions of the Clause 6.5 of ETSI EN 319 411-1 and the Clause 6.5 of ETSI EN 319 411-2.

6.1. Generating and installing a key pair

A private key as part of a user’s key pair can be generated using the mobile application of the Diia Portal (Diia).

During the generation of a private key, the following procedures are carried out:

- identification of the user with tools of the mobile application of the Diia Portal (Diia) or in the mobile application of the "E-resident" Information System;
- generation of a package of documents and an application for accession to the Agreement on the Provision of Qualified Electronic Trust Services;
- sending the formed documents to the QTSP "Diia" with tools of the ICS of the mobile application of the Diia Portal (Diia) or the mobile application of the "E-resident" Information System;
- verification of the correctness of the formed QTSP "Diia" documents;
- generation of a user key pair;
- formation of a user qualified certificate.

As a result of this procedure, a user's private key is formed, which is stored in the QTSP "Diia" cloud service (network cryptomodules), and a qualified certificate "Diia. Signature" certificate is also created.

In the QTSP "Diia" ICS, private and their corresponding public keys are used using electronic signature algorithms defined by the standards DSTU ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI). Cryptographic Sets" or DSTU 4145-2002 "Information Technologies. Cryptographic protection of information. Digital signature based on elliptic curves. Generation and verification". Generation of the private key of the QTSP "Diia" is described in detail in the Clause 6.1.1.1 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures).

The signer's key pair is generated directly in a qualified signature creation device (QSCD); the private key is stored only in such device. At the time of qualified e-signature creation it is confirmed that the private key resides in the qualified signature creation device (QSCD).

Devices conform to at least FIPS 140-2 Level 2 or Common Criteria (incl. EN 419 241 for remote solutions), or are recognized as a qualified signature creation device (QSCD) under applicable law.

Minimum cryptographic levels for profiles submitted to AATL: RSA 2048+, ECDSA 256+, SHA-256+.

6.2. Private key protection and engineering control of the cryptographic module

Clause 6.2 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on standards and controls of the cryptographic module, backup of the private key, archiving of the private key, renewal of the private key, storage of the private key in the cryptographic module, activation of the private key, deactivation of the private key, destruction of the private key, capabilities of the network cryptographic module.

6.3. Other aspects of key pair management

Clause 6.3 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on archiving of the public key of the QTSP "Diia", certificate validity period and terms of use of the QTSP "Diia" key pair.

6.4. Activation data

Clause 6.4 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the protection of personal key activation data.

6.5. Computer security control

Clause 6.5 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on special technical requirements for computer security, computer security rating.

6.6. Lifecycle safety control

Clause 6.6 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on control of the development of the QTSP “Diia” ICS, security controls in the QTSP “Diia” ICS, security control during the lifecycle.

6.7. Network security control

Clause 6.7 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on network security controls.

6.8. Electronic time stamps

Clause 6.8 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the formation and verification of a qualified electronic time stamp, the consequences of invalidity of a qualified electronic time stamp and the procedure for receiving a qualified electronic time stamp by the QTSP “Diia”.

7. PROFILES OF CERTIFICATES, REVOKED CERTIFICATE LISTS (CRL) AND ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

In accordance with the provisions of the Clause 6.6 of ETSI EN 319 411-1 and the Clause 6.6 of ETSI EN 319 411-2. During certificate issuance, the ICS populates AIA (ocsp) and cRLDistributionPoints as configured by the profile. Non-public or inaccessible URLs are not permitted for certificates declared for AATL use.

For the "Diia.Signature" service, the ICS sets the Certificate Policies with the policy OID per profile and the CPS Pointer (cps) qualifier with an HTTP URL to the current CP/CPS in the Repository. URLs shall be public and accessible without authentication.

7.1. Certificate profiles

Clause 7.1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the information to be contained in qualified certificates.

7.2. Profiles of the revoked certificate list

Clause 7.2 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the data to be contained in the revoked certificate lists.

7.3. Online certificate status protocol profiles

Clause 7.3 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the possibility of verifying the status of a qualified user certificate in real time via public electronic communication networks using the OCSP protocol.

8. CONFORMITY AUDIT AND OTHER ASSESSMENTS

In accordance with the provisions of the Clause 6.7 of ETSI EN 319 411-1 and the Clause 6.7 of ETSI EN 319 411-2.

8.1. Frequency or circumstances of assessment

Clause 8.1 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the frequency and circumstances of assessment of the QTSP “Diia”.

8.2. Appraiser’s identity/qualifications

Clause 8.2 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the qualification requirements for officials of the Controlling Authority (CA) and the Conformity Assessment Authority (CAA).

8.3. Relations between the expert and the object of assessment

Clause 8.3 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the relations between officials of the Controlling Authority (CA) and experts (auditors) of the Conformity Assessment Authority and the object of assessment (QTSP “Diia”).

8.4. Topics covered by the assessment

Clause 8.4 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the issues to be verified during state control and conformity assessment.

8.5. Actions taken as a result of the violation

Clause 8.5 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on actions taken as a result of a violation detected by the results of state control or conformity assessment.

8.6. Reporting results

Clause 8.6 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the registration of the results of state control or conformity assessment, issuance of an order to eliminate violations identified during state control.

8.7. Self-checks

Clause 8.6 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on regular internal audits of conformity with the established requirements by the QTSP “Diia”.

9. OTHER COMMERCIAL AND LEGAL ISSUES

According to the provisions of the Clause 6.8 of ETSI EN 319 411-1 and the Clause 6.8 of ETSI EN 319 411-2.

9.1. Charges

9.1.1. Fee for issuing or renewing a certificate

In accordance with the Resolution of the Cabinet of Ministers of Ukraine No. 1137 dated December 04, 2019 “Issues of the Unified State Web Portal of Electronic Services and the Register of Administrative Services”, the QTSP “Diia” provides a service for the formation of a qualified certificate “Diia.Signature”:

- for natural persons - free of charge,
- for representatives of legal entities - on a paid basis in accordance with the approved tariffs of the QTSP “Diia”, which are posted on the QTSP “Diia” website.
- for e-residents - free of charge.

9.1.2. Fee for access to the certificate

There is no fee for access to the qualified certificate “Diia.Signature”.

9.1.3. Fee for blocking/cancellation or access to certificate status information

There is no fee for cancellation of the qualified certificate “Diia.Signature” or access to information on the status of the qualified certificate “Diia.Signature”.

9.1.4. Fee for other services

Formation of a qualified certificate “Diia.Signature” does not provide for the provision of additional services by the QTSP “Diia”.

9.1.5. Refund policy

QTSP “Diia” does not refund paid invoices for provided services.

9.2. Financial responsibility

Clause 9.2 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the financial responsibility of the QTSP “Diia”.

9.3. Confidentiality of business data

Clause 9.3 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the content and scope of confidential information held by the QTSP “Diia”, as well as responsibility for the protection of confidential information.

9.4. Protection of personal data

Clause 9.4 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the concept of personal data protection in the QTSP “Diia”, the definition of personal data and personal data that are not considered confidential, responsibility for personal data protection, consent to the use of personal data and circumstances of personal data disclosure.

9.5. Intellectual property rights

Issues related to intellectual property rights of the QTSP “Diia” are regulated in accordance with the requirements of the current legislation of Ukraine.

9.6. Statements and guarantees

Clause 9.6 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the obligations and guarantees of the QTSP "Diia", QTSP "Diia" separate registration units, users, relying parties and other participants.

9.7. Waiver of liability

Clause 9.7 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the waiver of guarantees of the QTSP "Diia".

9.8. Limitation of liability

Clause 9.8 of the Policy of the Certificate of the Qualified Trust Service Provider "Diia" (Annex 1 to these Rules and Procedures) contains information on the circumstances for limiting the liability of the QTSP "Diia".

9.9. Damages

Compensation for damages that may be caused to users of electronic trust services or third parties as a result of improper fulfilment of the obligations by the QTSP "Diia" shall be made in accordance with the requirements of the current legislation of Ukraine.

9.10. Validity and termination

These Regulations on Certification Practices are applied from the moment of their publication and are valid until the expiration of the last certificate issued in accordance with these Regulations on Certification Practices or until the termination of the activity of the QTSP "Diia".

9.11. Individual communications and agreements with public key infrastructure entities

QTSP "Diia" communicates with participants of the public key infrastructure by:

- posting notifications and announcements on the QTSP "Diia" website;
- informing the CCA, CA and the personal data protection authority by sending notifications in paper and electronic forms.

9.12. Amendments

Amendments and additions to these Regulations on Certification Practices shall be made by the QTSP "Diia" in case of:

- changes to the requirements, processes and procedures described in these Regulations on Certification Practices;
- changes in the legislation;
- changes in the requirements for service providers.

New versions of these Regulations on Certification Practices, after amendments to them, are published on the QTSP "Diia" website.

Any changes not noted in the history of these Regulations on Certification Practices are grammatical and spelling changes that do not affect the meaning and do not affect the processes and procedures described in these Regulations on Certification Practices.

9.13. Provisions for dispute resolution

In case of any disputes or disagreements, the QTSP "Diia" (SE "DIIA") shall resolve them through negotiations and consultations with the participants of the public key infrastructure.

If the participants of the public key infrastructure fail to reach an agreement, disputes (disagreements) shall be resolved in court in accordance with the current legislation of Ukraine.

9.14. Applicable law

Relations governed by these Regulations on Certification Practices are subject to the current legislation of Ukraine.

9.15. Compliance with current legislation

Clause 9.15 of the Policy of the Certificate of the Qualified Trust Service Provider “Diia” (Annex 1 to these Rules and Procedures) contains information on the legislative and regulatory acts that establish requirements for the provision of qualified electronic trust services by the QTSP “Diia”.