Certificates practice statement (Chapter V of the Regulations of the CCA)

1. Submission of the request for the creation of the qualified public key certificate

1. Administrator of the information and telecommunication system of the Central Certification Authority (Administrator of ITS of CCA) generates qualified public key certificates of legal entities or natural persons - entrepreneurs who intend to provide qualified electronic trust services - providers who meet the requirements of parts one, two and three of Article 23 of the Law of Ukraine on electronic trust services (the Law), and provides round-the-clock access to information about the date and time of change of the status of qualified public key certificates.

2. Creation of a qualified public key certificate of a qualified trust services provider (trust services provider/provider) is carried out on basis of applications for qualified electronic trust service of creation, verification and validation of a qualified electronic signature or seal to the provider specified in Annex 2 (for the provider - legal entity) and Annex 3 (natural person - entrepreneur) to the Regulations of the CCA, submitted to the Administrator of ITS CCA).

3. An application for the creation of a qualified public key certificate shall be submitted to the Administrator of ITS CCA in paper or electronic form.

An application in electronic form, which is accompanied by a qualified electronic signature of the head of the legal entity or his authorized person or individual entrepreneur, is sent to the e-mail of the Administrator of ITS CCA: support.its@czo.gov.ua.

In paper form, an application is submitted in person by a representative of a legal entity or a natural person - entrepreneur who intends to provide qualified electronic trust services, or by the provider, signed by him or his authorized person and sealed.

During the acceptance of an application for the creation of a public key certificate, the identification and verification of the civil capacity and legal capacity of the representative of the legal entity or natural person - entrepreneur (or his authorized person) is carried out by verifying the identification data of the person from the documents submitted by the applicant and the information obtained from the information systems of state authorities.

4. Together with the application for the provision of a qualified electronic trust service of creation, verification and validation of a qualified electronic signature or seal certificate the following documents shall be submitted in person by a representative of a legal entity or individual entrepreneur (or his authorized person) or sent by e-mail to the Administrator of ITS CCA signed by the head of the legal entity or his authorized person:

- The request for certificate creation;
- an agreement on the provision of a qualified electronic trust service for the creation, verification and confirmation of the validity of a qualified electronic signature or seal certificate.

Two copies of the agreement on the provision of a qualified electronic trust service for the formation, verification and validation of a qualified electronic signature or seal certificate, signed by the provider and sealed (if any) (head of the legal entity that is the provider, or his authorized person or individual person - an entrepreneur who is a provider).

5. Requirements for the request:

- the request is submitted in a format according to the certification request syntax specification (PKCS # 10) defined by RFC 2986 "PKCS # 10: CertificationRequestSyntaxSpecification";
- the request shall contain the public key information of the provider making the request. This information is defined by the attribute "Information on the public key of the provider"

(subjectPublicKeyInfo), the format of which shall meet the technical requirements for technical means and processes of their use in electronic trust services, cryptographic information protection, their creation and operation as part of information and telecommunications systems , which are established by the main body in the system of central executive bodies, which ensures the formation and implementation of state policy in the field of electronic trust services and specially authorized central executive body for special communication and information protection, in accordance with the Resolution of the KMU on December 16, 2015 No. 1057 “On defining the spheres of activity in which the central bodies of executive power and the Security Service of Ukraine perform technical regulation functions” (the Resolution).

The request, in addition to the mandatory details of the provider in the request for a key certificate, as defined in Table 1 of Annex 1 to the Regulations of the CCA, and the provider's services, may contain other identification data of individuals or legal entities, optional additional special attributes defined in the standards for qualified public key certificates. These attributes should not affect the interoperability and recognition of qualified electronic signatures.

These optional additional special attributes are defined by the "Extended Request" attribute, which looks like this:

extensionRequest ATTRIBUTE:: = {

WITH SYNTAX ExtensionRequest

SINGLE VALUE TRUE

ID pkcs-9-at-extensionRequest

}

ExtensionRequest:: = Extensions.

6. Consideration of an application for the provision of a qualified electronic trust service for the creation, verification and confirmation of the validity of a qualified electronic signature or seal certificate to a provider shall not exceed two working days from the date of acceptance of the application.

During the consideration of an application for the provision of a qualified electronic trust service for the creation, verification and confirmation of the validity of a qualified electronic signature or seal certificate to a provider, the verification shall be carried out:

- compliance of the data entered in the application with the provider's documents received from the Ministry of digital transformation in accordance with the established procedure for maintaining the Trusted List;

- uniqueness of the public key of the service according to the register of valid, blocked and revoked public key certificates;

- belonging to the provider of the relevant personal key of the service by checking the advanced electronic signature or seal in the request;

- compliance of the request with the requirements specified in paragraph 6 of this chapter.

7. In case of successful verification, the Administrator of ITS CCA generates a qualified public key certificate of the provider. In case of failure to pass the verification, the provider shall be submitted with a motivated refusal to generate a key certificate and the application for providing a qualified electronic trust service for creation, verification and validation a qualified electronic signature or seal certificate shall be returned to the provider together with its appendices.

8. Creation of qualified certificates of public keys of providers is carried out by the certification administrator under the control of the administrator of security and audit.

9. While creating a qualified public key certificate, additional extensions that may be contained in the request are installed in the qualified public key certificate of the provider, in case that they are defined as not critical, and object identifiers of such extensions are registered in the prescribed manner.

2. Providing the generated qualified public key certificate to a trust services provider

1. After the creation of a qualified provider's public key certificate, the Administrator of ITS CCA sends to the provider's e-mail specified in the Trust List and in the electronic register of valid, blocked and revoked public key certificates, documents in electronic form with a qualified electronic signature of the authorized person of the Administrator of ITS CCA, namely:

created/qualified /certificate/certificates of the provider;

an act of provided services (for each of the certificates) on the formation of a qualified certificate;

an agreement on the provision of a qualified electronic trust service for the creation, verification and validation of a qualified electronic signature or seal certificate to a provider.

2. Based on the results of the creation and transfer of the provider's qualified public key certificate, the Administrator of ITS CCA, in case of receiving signed agreements from the provider in paper form, submits the provider's authorized person with one signed copy of the agreement on providing qualified electronic trust service of electronic signature or seal to a provider in paper form.

In case of receiving a signed agreement from the provider in electronic form, the Administrator of ITS CCA based on the results of creation and submitting a qualified certificate of the provider's public key shall submit the authorized person of the provider with a signed copy of the agreement on providing qualified electronic trust service of electronic signature or seal to a provider in electronic form.

3. Terms of use of qualified public key certificates and private keys of trust services providers

1. Providers use key pairs (private and public) for their intended purpose (scope of usage) in accordance with the requirements for technical means, processes of their creation, use and operation as part of information and telecommunications systems when providing qualified electronic trust services established by the main body in the system of central executive bodies that ensures the formation and implementation of state policy in the field of electronic trust services and the specially authorized central executive body on establishing of special communications and information protection, in accordance with the Resolution.

2. When providing services, providers shall use key pairs (private and public) with the following parameters:

- with the degree of expansion of the main field of the elliptic curve not less than 257 according to DSTU 4145-2002;

- with the degree of expansion of the main field of the elliptic curve not less than 256 for the ECDSA algorithm according to DSTU ETSI EN 119 312: 2015;

- with a key length of at least 4096 bits for the RSA algorithm in accordance with DSTU ETSI EN 119 312: 2015.

3. Algorithms for calculating the value of the hash function are defined in the technical requirements to technical means and processes of their use in the field of electronic trust services, means of cryptographic protection of information, processes of their creation and functioning as a

part of information and telecommunication systems, that are established by the main body in the system of central executive bodies that ensures the formation and implementation of state policy in the field of electronic trust services and the specially authorized central executive body on establishing of special communications and information protection, in accordance with the Resolution.

4. Providers shall use private keys only for their intended purpose (scope of usage) during the period of validity of the relevant qualified public key certificates generated in accordance with this Certificates Practice Statement, and on condition that this certificate has not been ceased or revoked.

5. Providers shall ensure the use of qualified public key certificates and private keys only for the purpose (scope of usage) specified in paragraph 2 of Chapter 1 of Section IV of the Regulations of the CCA.

6. When providing qualified electronic trust services, providers shall ensure the verification of the validity term and status of public key certificates created by the Administrator of ITS CCA.

7. Before using any public key certificate, the following validation must be carried out:

- validity of the qualified public key certificate of the provider at the time of imposition of the qualified electronic signature or creation of the electronic seal or the qualified electronic signature or seal on the document;

- validity of the qualified electronic seal of the CCA, which was added to the qualified certificate of the public key of the provider by means of the self-signed certificate of the CCA key, valid at the time of creation of the qualified certificate of the public key of the provider;

- status of the qualified provider's public key certificate in real time, if the verification is carried out at the time of validity of this key certificate or by the Certificate Revocation List (CRL).

8. During the verification of the status of the qualified public key certificate of the provider by CRL, the authenticity, integrity and validity of CRL shall be verified.

4. Circumstances and procedure for changing the status (revocation, cessation, renewal) of a qualified public key certificate

1. Revocation of the qualified provider's public key certificate:

1) revocation of qualified certificates of public keys of providers is carried out in the cases specified in parts one, two and three of Article 25 of the Law, on the basis of an application for revocation of the qualified certificate of public key of the provider;

2) the forms of applications for revocation of the qualified provider's public key certificates submitted to the Administrator of ITS CCA are defined in Annex 4 (for the provider - legal entity) and Annex 5 (for the provider - individual - entrepreneur) to the Regulations of the CCA.

3) an application for revocation of a qualified public key certificate is submitted by a provider to the Administrator of ITS CCA in electronic form, which has a qualified electronic signature of the head of the legal entity or its authorized person or in any other way that insures confirmation of the provider in accordance with legislation;

4) while accepting an application for revocation of a qualified public key certificate, the identity of the head of the legal entity - provider (natural person - entrepreneur who is the provider) or his authorized person is carried out as well as the adequacy of civil capacity is verified by checking the person's identification data from documents, submitted by the applicant and the data obtained from the information systems of state authorities;

5) applications and documents that are damaged and do not allow unambiguous interpretation of the content, corrections or additions and also in case a qualified electronic signature has not been validated while submitting the application in electronic form, shall not be accepted for consideration;

6) processing of the application for revocation of the qualified public key certificate and informing by the Administrator of ITS of CCA of the provider about the revocation of the key certificate of its services shall be carried out within two hours from the moment of receipt of the application by Administrator of ITS CCA;

7) revocation of the qualified public key certificate of the provider is carried out by the certification administrator under the control of the administrator of security and audit;

8) revocation of the qualified public key certificate of the provider comes into force from the date and time of this operation;

9) serial number of the revoked qualified public key certificate of the provider shall be entered into the CRL indicating the date and time of this operation.

2. Cessation of the qualified public key certificate of a trust services provider:

1) Cessation of qualified public key certificates of providers is carried out in the cases specified in parts six and seven of Article 25 of the Law.

In case of cessation a qualified provider's public key certificate on the basis of its application, such applications shall be submitted to the Administrator of ITS CCA in the forms specified in Annex 6 (for the provider - legal entity) and Annex 7 (for the provider - individual entrepreneur) to this Certificates Practice Statement;

2) an application for cessation a qualified public key certificate is submitted by a provider to the Administrator of ITS CCA in electronic form with a qualified electronic signature of the head of the legal entity or its authorized person or in any other way that insures confirmation of the provider in accordance with legislation;

3) during the acceptance of the application for cessation of a qualified public key certificate, the identity of the head of the legal entity - provider (natural person - entrepreneur who is the provider) or his authorized person is carried out and the adequacy of civil capacity is verified by checking the identity of the person from documents, submitted by the applicant and the data obtained from the information systems of public authorities;

4) applications and documents that are damaged and do not allow unambiguous interpretation of the content, corrections or additions and also in the case the qualified electronic signature has not been verified while submitting the application in electronic form shall not be accepted for concideration;

5) a qualified public key certificate of the provider shall be ceased by the Administrator of the ITS CCA not later than within two hours from the moment of receipt of the application for cessation of a qualified public key certificate

6) cessation of a qualified public key certificate of the provider is carried out by the certification administrator under the control of the administrator of security and audit;

7) cessation of a qualified public key certificate of the provider comes into force from the date and time of this operation;

8) serial number of the ceased qualified public key certificate of the provider shall be entered into the CRL indicating the date and time of this operation.

3. Renewal of the qualified public key certificate of a trust services provider:

1) renewal of qualified public key certificates of providers is carried out in the cases specified in parts ten, eleven of Article 25 of the Law, on the basis of applications for renewal of qualified public

key certificate in the forms specified in Annex 8 (for the provider - legal entity) and Annex 9 (for the provider - natural person - entrepreneur) to the Regulations of the CCA, submitted to the Administrator of ITS CCA;

2) an application for renewal of a qualified public key certificate is submitted to the Administrator of ITS CCA in electronic form with a qualified electronic signature of the head of the legal entity or his authorized person or in any other way that insures confirmation of the provider in accordance with legislation;

3) while accepting an application for renewal of a qualified public key certificate, the identity of the head of the legal entity - provider (natural person - entrepreneur who is the provider) or his authorized person is established and the adequacy of civil capacity is verified by checking the person's identification data from documents, provided by the applicant and the data obtained from the information systems of state authorities;

4) applications and documents that are damaged and do not allow unambiguous interpretation of the content, corrections or additions and also in the case the qualified electronic signature has not been verified while submitting the application in electronic form shall not be accepted for consideration;

5) the ceased qualified public key certificate of the provider shall be renewed no later than within two hours from the moment of receipt of the application for renewal of the qualified public key certificate by the Administrator of the ITS CCA;

6) renewal of the qualified provider's public key certificate is carried out by the certification administrator under the control of the security and audit administrator;

7) renewal of the qualified public key certificate of the provider comes into force from the date and time of this operation;

8) information on the renewal of the qualified public key certificate of the provider shall be entered into the CRL indicating the date and time of this operation.

4. Dissemination of information on status changes of qualified certificates of public keys of trust services providers:

1) dissemination of information on the status of qualified public key certificates of providers is carried out by publishing full and partial CRL on the official website of the CCA and providing the ability to verify the status of the key certificate in real time through public telecommunications networks;

2) publication of the next CRL is carried out with the frequency specified in paragraphs 1-3 of Chapter 2 of Section IV of the Regulations of the CCA;

3) in the process of formation of CRL the Administrator of the ITS CCA insures the following:

each CRL indicates the deadline of its validity until the publication of the next list;

a new CRL can be published before its deadline for the publication of the next list;

the electronic seal of the CCA must be imposed on the CRL;

4) information on the status of the qualified public key certificate of a provider in real time is distributed according to the protocol of determining the status of the certificate in accordance with the technical requirements for technical means and processes of their use in electronic trust services, cryptographic information protection, their creation and operation as part of information and telecommunications systems , which are established by the main body in the system of central executive bodies, which ensures the formation and implementation of state policy in the field of electronic trust services and specially authorized central executive body for special communication and information protection, in accordance with the Resolution.

5. Termination of the qualified public key certificate of a trust services provider

1. The validity of the qualified public key certificate of a provider shall not exceed five years.

2. The beginning of the validity period of the qualified public key certificate of a provider is calculated from the date and time of creation of the certificate by the CCA, which is shown in the certificate.

3. Not later than by half of the validity term of the qualified public key certificate of a provider, the provider shall receive a new qualified public key certificate in the manner specified in paragraphs 1-8 of Chapter 1 of this Certificate Practice Statement.

Положення сертифікаційних практик (Глава V Регламенту роботи ЦЗО)

1. Подання запиту на формування кваліфікованого сертифіката відкритого ключа

1. Адміністратор ІТС ЦЗО формує кваліфіковані сертифікати відкритих ключів юридичних осіб або фізичних осіб - підприємців, що мають намір надавати кваліфіковані електронні довірчі послуги, надавачам, які відповідають вимогам, встановленим частинами першою, другою та третьою статті 23 Закону “Про електронні довірчі послуги” (Закон), та забезпечує цілодобовий доступ до інформації про дату та час зміни статусу кваліфікованих сертифікатів відкритих ключів.

2. Формування кваліфікованого сертифіката відкритого ключа надавача здійснюється на підставі заяв про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки кваліфікованому надавачу довірчих послуг (надавач), визначених у додатку 2 (для надавача - юридичної особи) та додатку 3 (для надавача - фізичної особи - підприємця) до Регламенту ЦЗО, що подаються до Адміністратора ІТС ЦЗО.

3. Заява про формування кваліфікованого сертифіката відкритого ключа подається до Адміністратора ІТС ЦЗО в паперовій чи електронній формі.

Заява в електронній формі, на яку накладається кваліфікований електронний підпис керівника юридичної особи чи його уповноваженої особи або фізичної особи - підприємця, надсилається на електронну пошту Адміністратора ІТС ЦЗО: support.its@czo.gov.ua.

У паперовій формі зазначена заява подається особисто представником юридичної особи або фізичною особою - підприємцем, що має намір надавати кваліфіковані електронні довірчі послуги, або надавачем, підписується ним або його уповноваженою особою та скріплюється печаткою.

Під час приймання заяви про формування сертифіката відкритого ключа здійснюються ідентифікація, перевірка обсягу цивільної правоздатності та дієздатності представника юридичної особи або фізичної особи - підприємця (або його уповноваженої особи) шляхом перевірки ідентифікаційних даних особи з документів, що надаються заявником, та даних, одержаних з інформаційних систем органів державної влади.

4. Разом із заявою про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки подаються особисто представником юридичної особи або фізичної особи - підприємця (або його уповноваженою особою) або надсилаються на електронну пошту Адміністратора ІТС ЦЗО підписані кваліфікованим електронним підписом керівника юридичної особи чи його уповноваженою особою такі документи:

- запит на формування сертифіката;
- договір про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки.

У паперовій формі подаються два примірники договору про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки, підписані надавачем та скріплені печаткою (за наявності) (керівником юридичної особи, що є надавачем, чи його уповноваженою особою або фізичною особою - підприємцем, що є надавачем).

5. Вимоги до запиту:

- запит подається у форматі згідно зі специфікацією синтаксису запиту на сертифікацію (PKCS#10), що визначена RFC 2986 «PKCS #10: CertificationRequestSyntaxSpecification»;

- запит має містити інформацію про відкритий ключ надавача, що подає такий запит. Зазначена інформація визначається атрибутом «Інформація про відкритий ключ надавача» (subjectPublicKeyInfo), формат якого має відповідати технічним вимогам до технічних засобів та процесів їх використання у сфері електронних довірчих послуг, засобів криптографічного захисту інформації, процесів їх створення та функціонування у складі інформаційно-телекомунікаційних систем, які встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг та спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації, відповідно до Постанови.

Запит, крім обов'язкових реквізитів надавача в запиті на формування сертифіката ключа, що визначені таблицею 1 додатка 1 до цього Регламенту, та послуг надавача, може містити інші ідентифікаційні дані фізичних або юридичних осіб, необов'язкові додаткові спеціальні атрибути, визначені у стандартах для кваліфікованих сертифікатів відкритих ключів. Ці атрибути не мають впливати на інтероперабельність і визнання кваліфікованих електронних підписів.

Зазначені необов'язкові додаткові спеціальні атрибути визначаються атрибутом «Розширений запит» (extensionRequest), який має такий вигляд:

extensionRequest ATTRIBUTE:: = {

WITH SYNTAX ExtensionRequest

SINGLE VALUE TRUE

ID pkcs-9-at-extensionRequest

}

ExtensionRequest:: = Extensions.

6. Розгляд заяви про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу становить не більше двох робочих днів від дати прийняття заяви.

Під час розгляду заяви про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу здійснюється перевірка:

відповідності даних, внесених до заяви, документам надавача, отриманим від Мінцифри відповідно до встановленого порядку ведення Довірчого списку;

унікальності відкритого ключа послуги за відомостями реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

належності надавачу відповідного особистого ключа послуги шляхом перевірки удосконаленого електронного підпису чи печатки в запиті;

відповідності запиту вимогам, зазначеним у пункті 6 цієї глави.

7. У разі успішної перевірки Адміністратор ІТС ЦЗО формує кваліфікований сертифікат відкритого ключа надавача. У разі непроходження перевірки надавачу надається вмотивована

відмова у формуванні сертифіката ключа та повертається заява про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу разом із додатками до неї.

8. Формування кваліфікованих сертифікатів відкритих ключів надавачів здійснюється адміністратором сертифікації під контролем адміністратора безпеки та аудиту.

9. Під час формування кваліфікованого сертифіката відкритого ключа додаткові розширення, що можуть міститись у запиті, встановлюються у кваліфікованому сертифікаті відкритого ключа надавача за умови, що вони були визначені як не критичні, а об'єктні ідентифікатори таких розширень зареєстровані у встановленому порядку.

2. Надання сформованого кваліфікованого сертифіката відкритого ключа надавачу

1. Після формування кваліфікованого сертифіката відкритого ключа надавача Адміністратор ІТС ЦЗО надсилає на електронну пошту надавача, зазначену в Довірчому списку та в електронному реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів, документи в електронній формі, на які накладено кваліфікований електронний підпис уповноваженої особи Адміністратора ІТС ЦЗО, а саме:

- сформований/ні кваліфікований/ні сертифікат/сертифікати надавача;

- акт наданих послуг (для кожного з сертифікатів) про формування кваліфікованого сертифіката;

- договір про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу.

2. За результатами проведеного формування та передавання кваліфікованого сертифіката відкритого ключа надавача Адміністратор ІТС ЦЗО, в разі отримання від надавача підписаних договорів в паперовій формі, надає уповноваженій особі надавача один підписаний примірник договору про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу в паперовій формі.

В разі отримання від надавача підписаного договору в електронній формі Адміністратор ІТС ЦЗО за результатами проведеного формування та передавання кваліфікованого сертифіката відкритого ключа надавача, надає уповноваженій особі надавача підписаний примірник договору про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу в електронній формі.

3. Умови використання кваліфікованих сертифікатів відкритих ключів та особистих ключів надавачів

1. Надавачі використовують пари ключів (особистих та відкритих) за призначенням (сферою використання) згідно з вимогами до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг, які встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг та спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації, відповідно до Постанови.

2. Під час надання послуг надавачі повинні використовувати пари ключів (особистих та відкритих) із такими параметрами:

- зі ступенем розширення основного поля еліптичної кривої не менше 257 за ДСТУ 4145-2002;

- зі ступенем розширення основного поля еліптичної кривої не менше 256 для алгоритму ECDSA за ДСТУ ETSI EN 119 312:2015;

- з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI EN 119 312:2015.

3. Для обчислення значення геш-функції використовуються алгоритми, визначені до технічних вимог до технічних засобів та процесів їх використання у сфері електронних довірчих послуг, засобів криптографічного захисту інформації, процесів їх створення та функціонування у складі інформаційно-телекомунікаційних систем, які встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг та спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації, відповідно до постанови КМУ від 16 грудня 2015 № 1057" Про визначення сфер діяльності, в яких центральні органи виконавчої влади та Служба безпеки України здійснюють функції технічного регулювання" Постанова.

4. Надавачі використовують особисті ключі тільки за призначенням (сферою використання) в період чинності відповідних кваліфікованих сертифікатів відкритих ключів, сформованих відповідно до цього Положення сертифікаційних практикАре, та за умови, що цей сертифікат не був заблокований або скасований.

5. Надавачі забезпечують використання кваліфікованих сертифікатів відкритих ключів та особистих ключів тільки за призначенням (сферою використання), зазначених у пункті 2 глави 1 розділу IV Регламенту ЦЗО

6. Під час надання кваліфікованих електронних довірчих послуг надавачі забезпечують обов'язковість перевірки строку чинності та статусу сформованих Адміністратором ЦЗО сертифікатів відкритих ключів.

7. Перед використанням будь-якого сертифіката відкритого ключа має забезпечуватись перевірка:

- чинності кваліфікованого сертифіката відкритого ключа надавача на момент накладення кваліфікованого електронного підпису чи створення електронної печатки на документ або кваліфікованого електронного підпису чи печатки на документі;

- чинності кваліфікованої електронної печатки ЦЗО, що була додана до кваліфікованого сертифіката відкритого ключа надавача за допомогою самопідписаного сертифіката ключа ЦЗО, чинного на момент формування кваліфікованого сертифіката відкритого ключа надавача;

- статусу кваліфікованого сертифіката відкритого ключа надавача в режимі реального часу, якщо перевірка здійснюється на момент чинності цього сертифіката ключа або за СВС.

8. Під час перевірки статусу кваліфікованого сертифіката відкритого ключа надавача за СВС здійснюється перевірка автентичності, цілісності та терміну дії СВС.

4. Обставини та порядок зміни статусу (скасування, блокування, поновлення) кваліфікованого сертифіката відкритого ключа

1. Скасування кваліфікованого сертифіката відкритого ключа надавача:

1) скасування кваліфікованих сертифікатів відкритих ключів надавачів здійснюється у випадках, передбачених частинами першою, другою та третьою статті 25 Закону, на підставі заяви про скасування кваліфікованого сертифіката відкритого ключа надавача;

2) форми заяв про скасування кваліфікованого сертифіката відкритого ключа надавача, що подаються до Адміністратора ІТС ЦЗО, визначені в додатку 4 (для надавача - юридичної особи) та додатку 5 (для надавача - фізичної особи - підприємця) до цього Регламенту;

3) заява про скасування кваліфікованого сертифіката відкритого ключа подається надавачем до Адміністратора ІТС ЦЗО в електронній формі, на яку накладено кваліфікований електронний підпис керівника юридичної особи чи його уповноваженої особи або в будь-який інший спосіб, що забезпечує підтвердження особи - надавача відповідно до вимог законодавства;

4) під час приймання заяви про скасування кваліфікованого сертифіката відкритого ключа здійснюється встановлення особи керівника юридичної особи - надавача (фізичної особи - підприємця, що є надавачем) або його уповноваженої особи та перевіряється достатність обсягу цивільної правоздатності та дієздатності шляхом перевірки ідентифікаційних даних особи з документів, що надаються заявником, та даних, одержаних з інформаційних систем органів державної влади;

5) не приймаються до розгляду заяви та документи, які мають пошкодження, що не дають змогу однозначно тлумачити зміст, виправлення або дописки та якщо кваліфікований електронний підпис не пройшов перевірку у разі подання заяви в електронній формі;

6) опрацювання заяви на скасування кваліфікованого сертифіката відкритого ключа та інформування Адміністратором ІТС ЦЗО надавача про скасування сертифіката ключа його послуги здійснюються протягом двох годин від моменту отримання заяви Адміністратором ІТС ЦЗО;

7) скасування кваліфікованого сертифіката відкритого ключа надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки та аудиту;

8) скасування кваліфікованого сертифіката відкритого ключа надавача набирає чинності з дати та часу здійснення цієї операції;

9) серійний номер скасованого кваліфікованого сертифіката відкритого ключа надавача вноситься до СВС із зазначенням дати та часу здійснення цієї операції.

2. Блокування кваліфікованого сертифіката відкритого ключа надавача:

1) блокування кваліфікованих сертифікатів відкритих ключів надавачів здійснюється у випадках, передбачених частинами шостою та сьомою статті 25 Закону.

У разі блокування кваліфікованого сертифіката відкритого ключа надавача на підставі його заяви такі заяви подаються до Адміністратора ІТС ЦЗО за формами, визначеними у додатку 6 (для надавача - юридичної особи) та у додатку 7 (для надавача - фізичної особи - підприємця) до цього Регламенту;

2) заява про блокування кваліфікованого сертифіката відкритого ключа подається надавачем до Адміністратора ІТС ЦЗО в електронній формі з накладенням кваліфікованого електронного підпису керівника юридичної особи чи його уповноваженої особи або в будь-який інший спосіб, що забезпечує підтвердження особи - надавача відповідно до вимог законодавства;

3) під час приймання заяви про блокування кваліфікованого сертифіката відкритого ключа здійснюється встановлення особи керівника юридичної особи - надавача (фізичної особи - підприємця, що є надавачем) або його уповноваженої особи та перевіряється достатність обсягу цивільної правоздатності та дієздатності шляхом перевірки ідентифікаційних даних

особи з документів, що надаються заявником, та даних, одержаних з інформаційних систем органів державної влади;

4) не приймаються до розгляду заяви та документи, які мають пошкодження, що не дають змогу однозначно тлумачити зміст, виправлення або дописки та якщо кваліфікований електронний підпис не пройшов перевірку у разі подання заяви в електронній формі;

5) кваліфікований сертифікат відкритого ключа надавача блокується не пізніше ніж протягом двох годин від моменту отримання заяви про блокування кваліфікованого сертифіката відкритого ключа Адміністратором ІТС ЦЗО;

6) блокування кваліфікованого сертифіката відкритого ключа надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки та аудиту;

7) блокування кваліфікованого сертифіката відкритого ключа надавача набирає чинності з дати та часу здійснення цієї операції;

8) серійний номер заблокованого кваліфікованого сертифіката відкритого ключа надавача вноситься до СВС із зазначенням дати та часу здійснення цієї операції.

3. Поновлення кваліфікованого сертифіката відкритого ключа надавача:

1) поновлення кваліфікованих сертифікатів відкритих ключів надавачів здійснюється у випадках, передбачених частинами десятою, одинадцятою статті 25 Закону, на підставі заяв про поновлення кваліфікованого сертифіката відкритого ключа за формами, визначеними в додатку 8 (для надавача - юридичної особи) та додатку 9 (для надавача - фізичної особи - підприємця) до Регламенту, що подаються до Адміністратора ІТС ЦЗО;

2) заява про поновлення кваліфікованого сертифіката відкритого ключа подається до Адміністратора ІТС ЦЗО в електронній формі з накладенням кваліфікованого електронного підпису керівника юридичної особи чи його уповноваженої особи або в будь-який інший спосіб, що забезпечує підтвердження особи - надавача відповідно до вимог законодавства;

3) під час приймання заяви про поновлення кваліфікованого сертифіката відкритого ключа здійснюється встановлення особи керівника юридичної особи - надавача (фізичної особи - підприємця, що є надавачем) або його уповноваженої особи та перевіряється достатність обсягу цивільної правоздатності та дієздатності шляхом перевірки ідентифікаційних даних особи з документів, що надаються заявником, та даних, одержаних з інформаційних систем органів державної влади;

4) не приймаються до розгляду заяви та документи, які мають пошкодження, що не дають змогу однозначно тлумачити зміст, виправлення або дописки та якщо кваліфікований електронний підпис не пройшов перевірку у разі подання заяви в електронній формі;

5) заблокований кваліфікований сертифікат відкритого ключа надавача поновлюється не пізніше ніж протягом двох годин від моменту отримання заяви про поновлення кваліфікованого сертифіката відкритого ключа Адміністратором ІТС ЦЗО;

6) поновлення кваліфікованого сертифіката відкритого ключа надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки та аудиту;

7) поновлення кваліфікованого сертифіката відкритого ключа надавача набирає чинності з дати та часу здійснення цієї операції;

8) відомості щодо поновлення кваліфікованого сертифіката відкритого ключа надавача вносяться до СВС із зазначенням дати та часу здійснення цієї операції.

4. Розповсюдження інформації про зміну статусу кваліфікованих сертифікатів відкритих ключів надавачів:

1) розповсюдження інформації про статус кваліфікованих сертифікатів відкритих ключів надавачів здійснюється за допомогою публікації повного та часткового СВС на офіційному вебсайті ЦЗО та забезпечення можливості перевірки статусу сертифіката ключа в режимі реального часу через телекомунікаційні мережі загального користування;

2) публікація наступного СВС здійснюється з періодичністю, зазначеною у пунктах 1-3 глави 2 розділу IV цього Документу;

3) Адміністратор ІТС ЦЗО під час формування СВС забезпечує такі умови:

- у кожному СВС зазначається граничний термін його дії до видання наступного списку;
- новий СВС може бути опублікований до настання граничного терміну його дії для видання наступного списку;
- на СВС має бути накладена електронна печатка ЦЗО;

4) інформація про статус кваліфікованого сертифіката відкритого ключа надавача в режимі реального часу розповсюджується за протоколом визначення статусу сертифіката відповідно до технічних вимог до технічних засобів та процесів їх використання у сфері електронних довірчих послуг, засобів криптографічного захисту інформації, процесів їх створення та функціонування у складі інформаційно-телекомунікаційних систем, які встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг та спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв’язку та захисту інформації, відповідно до Постанови.

5. Закінчення строку чинності кваліфікованого сертифіката відкритого ключа надавача

1. Строк чинності кваліфікованого сертифіката відкритого ключа надавача становить не більше ніж п’ять років.

2. Початок строку чинності кваліфікованого сертифіката відкритого ключа надавача обчислюється з дати та часу формування сертифіката у ЦЗО, що відображається в сертифікаті.

3. Не пізніше закінчення половини строку чинності кваліфікованого сертифіката відкритого ключа надавача останній отримує новий кваліфікований сертифікат відкритого ключа в порядку, визначеному у пунктах 1-8 глави 1 розділу Положення сертифікаційних практик.