Правила и постапки

за издавање на квалификувани сертификати за електронски потписи и електронски печати

KIBSTrust Verba

Верзија 2.0

Датум на стапување во сила: 15.11.2024

111.01

OID 1.3.6.1.4.1.16305.1.1.5.

КИБС АД Скопје

https://www.kibstrust.com/

Правила и постапки за издавање квалификувани сертификати за електронски потписи и електронски печати

Белешки за трговската марка

КИБС и KIBSTrust се регистрирани марки на КИБС АД Скопје. Други имиња може да бидат трговски марки на нивните сопственици.

Историја на документот

верзија	датум	автор	цел на промената
2.0	15.11.2024	Кристина Радомировиќ Исидора Мартиновска	Промени согласно воведување на нови издавачки сертификати од генерација G3 и соодветни промени во корисничките профили на сертификатите. Промени во главите: 1.3.1, 7.1, 7.3
1.0	01.04.2021	Тело за управување со правилата и постапките на ДДУ	Правила и постапки за издавање на квалификувани сертификати на електронски потписи и електронски печати во хиерархија на **KIBSTrust Root CA G2** според барањата на МК-eIDAS и eIDAS.

Содржина

1. ВОВЕД

Овој документ ги претставува Правилата и постапките за издавање на квалификувани сертификати (CP/CPS) на КИБС. Во него е наведена праксата која ја користи КИБС како Давател на доверливи услуги (TSP) при обезбедување услуги за издавање на квалификувани сертификати за електронски потписи и квалификувани сертификати за електронски печати во согласност, без ограничување на членовите 24, 29, 38, 39, 40, 55 од МК-eIDAS[1] и членовите 19, 24,26, 27, 28, 36, 37, 38 и 45 од Регулативата (ЕУ) бр. 910/2014 (eIDAS)[2].

Квалификувани сертификати за електронски потписи може да се издадат на локално средство за креирање квалификуван потпис (локален QSCD) или далечински QSCD. Квалификуваните сертификати за електронски печати може да се издадат на локален QSCD или далечинки QSCD.

Овој документ ги утврдува деловните, правните и техничките барања за одобрување, издавање, управување, користење, поништување и обновување сертификати и обезбедување на придружни доверливи услуги. Овие барања се однесуваат на сите Издавачи на сертификати (ИС), Регистрациони канцеларии (РК), претплатници, засегнати страни и други PKI субјекти кои остваруваат интероперабилност со инфраструктурата на јавни клучеви (PKI) на КИБС.

Овој документ ја опишува праксата што ја применува КИБС за:

- Сигурно управување со соодветната инфраструктура која го поддржува PKI на КИБС, и
- Издавање, одржување, управување, поништување и обновување (управување со животниот циклус) на квалификуваните сертификати како што е дефинирано во МК-eIDAS и eIDAS.

Овие CP/CPS се усогласени со RFC 3647 на Техничкиот стручен тим за интернет (Internet Engineering Task Force - IETF) за изготвување на Правилата и постапките за издавање на квалификувани сертификати.

1.1. Преглед

Овие CP/CPS ја опишуваат праксата и процедурите што се користат за решавање на сите барања утврдени со МК-eIDAS и eIDAS за издавање, одржување и управување со животниот циклус на квалификуваните сертификати за електронски потписи и квалификувани сертификати за електронски печати.

Оваа пракса и процедури се во согласност со:

- ETSI EN 319 411-2 Политики:
  - QCP-n / QCP-n-qscd за квалификувани сертификати за електронски потписи; и
  - QCP-l / QCP-l-qscd за квалификувани сертификати за електронски печати.

КИБС има безбеден капацитет за складирање, меѓу другото, и на системи за издавање сертификати, вклучувајќи ги криптографските модули со приватни клучеви што се користат за издавање сертификати. КИБС делува како ИС под покровителство на регистрираната трговска марка KIBSTrust. KIBSTrust ги извршува сите услуги за животниот циклус на сертификатите во однос на издавање, управување, поништување и обновување на квалификувани сертификати.

Овие CP/CPS се посебно применливи за издавачките сертификати на КИБС, кои издаваат квалификувани сертификати за електронски потписи и електронски печати.

Приватните издавачки сертификати и другите хиерархии со кои управува КИБС или услугите што ги обезбедува КИБС на други организации се, исто така, во рамките на овие CP/CPS. Практиките во врска со услугите обезбедени од други организации се надвор од обемот на овие CP/CPS.

КИБС ги објавува овие CP/CPS за да се усогласи со специфичните барања за правилата на важечкото законодавство или другите индустриски стандарди и барања.

[1] Закон за електронски документи, електронска идентификација и доверливи услуги (Службен весник на Република Северна Македонија 101/19, 215/19))

[2] Регулатива (ЕУ) бр. 910/2014 на Европскиот парламент и на Советот од 23 јули 2014 г. за електронска идентификација и доверливи услуги за електронски трансакции на внатрешниот пазар и укинување на Директивата 1999/93/ЕЗ

CP/CPS се само еден дел од пакетот документи релевантни за доверливите услуги на KIBSTrust. Овие други документи вклучуваат:

– Дополнителни доверливи, безбедносни и оперативни документи кои ги надополнуваат CP/CPS со обезбедување подетални барања, како што се:

  - Референтен водич за церемонијата на генерирање клучеви, кој детално ги презентира оперативните барања за управување со клучеви,
  - Политика за управување со криптографски клучеви на КИБС, која ги претставува деталните оперативни барања за управување со клучеви,
  - Политика за физичка безбедност на КИБС, која ги поставува безбедносните принципи според кои се регулира инфраструктурата на КИБС,
  - Политика за сигурност на информатичкиот систем на КИБС, каде се наведени барањата за инфраструктурата на информатичкиот систем со цел да функционира безбедно и според поврзаните закони и договорни барања.

  (Иако овие документи не се јавно достапни, нивните спецификации се вклучени во Извештајот за проценка на сообразноста на КИБС и може да бидат достапни според посебен договор.)

  - Правила и услови на КИБС за употреба на квалификувани доверливи услуги. Овие Правила и услови ги обврзуваат клиентите, претплатниците и засегнатите страни со широк спектар на комерцијални и други посебни услови или доверливи услуги на КИБС.

Во многу случаи, CP/CPS се однесуваат на овие дополнителни документи за посебна, детална пракса за спроведување на правилата на КИБС, каде што вклучувањето на специфичностите во CP/CPS може да ја загрозат безбедноста на ИС на КИБС.

КИБС, исто така, нуди сертификати за веб-страници (безбедна серверска идентификација).

Овие сертификати за веб-страници се нудат врз основа на посебна соработка со трето лице како давател на доверливи услуги, а не во рамките на КИБС ИС. За оваа деловна активност КИБС ги применува правилата и условите на давателите на доверливи услуги на тоа трето лице.

1.2. Име и идентификација на документ

Овој документ ги претставува Правилата и постапките за издавање на квалификувани сертификати на КИБС. КИБС им ја додели следнава вредност на предметен идентификатор (OID) на овие CP/CPS.

1.3.6.1.4.1.16305.1.1.5

1.3.6.1.4.1.16305	Идентификациски број (OID) на КИБС, регистриран во IANA
1.3.6.1.4.1.16305.1	Давател на доверливи услуги
1.3.6.1.4.1.16305.1.1	Политики за квалификувани сертификати
1.3.6.1.4.1.16305.1.1.5	Применлива и тековна верзија на CP/CPS

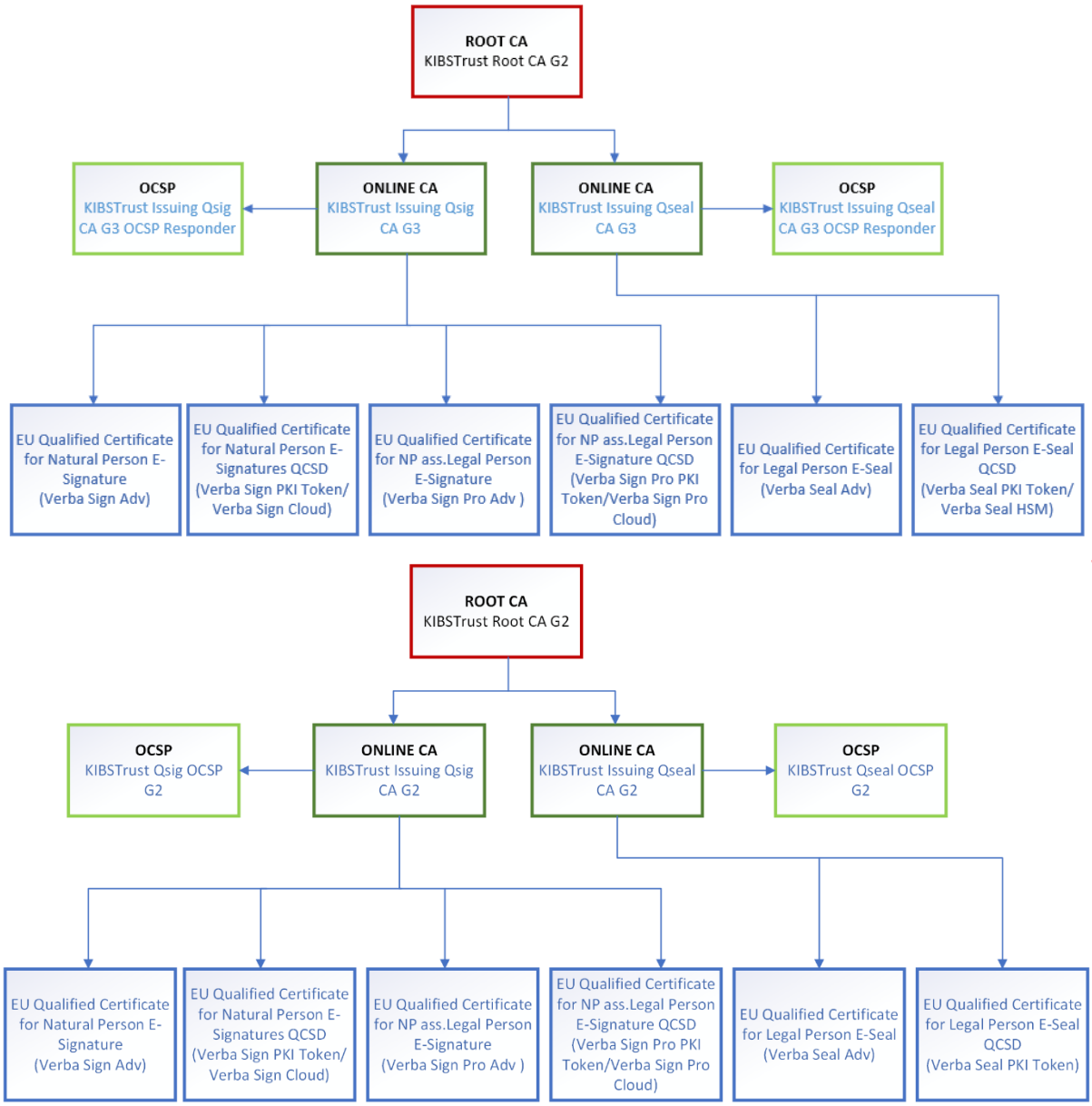
Применливиот и тековен CP/CPS (OID) се вметнува со упатување во секоја Политика за сертификати управувана од CP/CPS на КИБС.

1.3. PKI учесници

1.3.1. Издавачи на сертификати

Авторитетот во кој имаат доверба корисниците на услугите за сертификати (односно претплатници, како и засегнати страни) за креирање и доделување сертификати, се нарекува Издавач на сертификати (ИС). ИС има целосна одговорност за обезбедување услуги за сертификати.

КИБС тековно ја користи следнава хиерархија за сертификати:



Слика 1 Хиерархија на сертификати

Оваа ИС хиерархија е составена од следниве субјекти:

Листа на Коренски ИС

#	Карактеристично име на субјект	SHA-256 Fingerprint (Единствен идентификатор на) на сертификат
1	**CN** = KIBSTrust Root CA G2 **O** = KIBS AD Skopje **2.5.4.97** = NTRMK-5529581 **OU** = KIBSTrust Services **C** = MK	9E0D33A6B826F84030A8110 11E92217731C40CD28DBC23 37931286D8A4951235

Листа на Издавачки ИС

#	Карактеристично име на субјект	Сертификат SHA-256 Fingerprint (Единствен идентификатор) на сертификат
1	**CN** = KIBSTrust Issuing Qsig CA G3 **2.5.4.97** = NTRMK-5529581 **OU** = KIBSTrust Services **O** = KIBS AD Skopje **C** = MK	410CF3BEFD8B711C1AE06AB81778CC3F85B7DBE9BEC4F19F9EB38E97554DB1E2
2	**CN =** KIBSTrust Issuing Qseal CA G3 **2.5.4.97 =** NTRMK-5529581 **OU =** KIBSTrust Services **O =** KIBS AD Skopje **C =** MK	B3EADB5037E5C6785DE190D3061F296848C617AECAB006BA6A057E5F1DB0FC0C
3	**CN** = KIBSTrust Issuing Qsig CA G2 **2.5.4.97** = NTRMK-5529581 **OU** = KIBSTrust Services **O** = KIBS AD Skopje **C** = MK	C2F8EAF1ECF1646778223B45D1DEFDF67932A8352CC8303176DF5F4B627D2B41
4	**CN =** KIBSTrust Issuing Qseal CA G2 **2.5.4.97 =** NTRMK-5529581 **OU =** KIBSTrust Services **O =** KIBS AD Skopje **C =** MK	086ABDC02F43244865436EF125141DA731F7B3EABCABEBA8531FF2FA7AAECF65

1.3.2. Регистрациони канцеларии

Регистрационата канцеларија (РК) е ентитет кој врши идентификација и валидација на претплатници за издавање сертификати, иницира или проследува барања за поништување на сертификати и одобрува барања за сертификати со обновување на парот клучеви во име на ИС. КИБС делува како РК за квалификуваните сертификати што ги издава.

КИБС може да склучи договори со едно или повеќе трети лица, за извршување на дел или сите обврски (аутсорсинг) на РК. Во овој случај, третото лице претставува Регистрациона канцеларија (РК) и таа ги извршува своите обврски во целосна усогласеност со овие CP/CPS, соодветните планови за потврдување (валидација) и условите од договорот на РК, потпишан помеѓу РК и КИБС.

Потврдување на адресата за е-пошта не може да се делегира на трето лице и се потврдува само од РК на Издавачот на сертификати.

Пред да започне со операциите поврзани со РК, КИБС обучува овластени вработени во РК за процесот на потврдување и процедурите за сигурност и потоа спроведува повторна годишна обука.

КИБС врши годишни ревизии на функционирањето и процедурите на РК со цел да обезбеди усогласеност со овие CP/CPS, плановите за валидација и со договорот со РК (ако РК е надворешна компанија).

1.3.3. Локални регистрациони канцеларии

Локална регистрациона канцеларија (или ЛРК) е ентитет кој врши идентификација и валидација на претплатници и субјекти и првична проверка на нивните соодветни документи за издавање, обновување пар клучеви и поништување сертификати.

КИБС може да склучи договор со едно или повеќе трети лица, за извршување на дел од одговорностите (аутсорсинг) на РК, особено во врска со валидацијата на претплатникот. Во овој случај, третото лице претставува ЛРК. ЛРК ги извршува своите одговорности во целосна согласност со овие CP/CPS, соодветните планови за валидација и условите на ЛРК согласно договорот потпишан помеѓу ЛРК и КИБС.

Односот помеѓу КИБС, ЛРК и РК е опишан во договорот на ЛРК и вклучува, но не се ограничува на следново:

- Целосни детали за овластените вработени во ЛРК, кои ќе ги извршуваат обврските и активностите на ЛРК;
- Обврска на ЛРК да добива годишна обука на овластените вработени во ЛРК од КИБС, во врска со обврските и активностите на ЛРК и да прифати годишни ревизии од страна на КИБС во врска со работењето и процедурите на ЛРК;
- Обврска на овластениот вработен во ЛРК да користи документи издадени од КИБС РК за да обезбеди сигурна комуникација меѓу двете страни;
- Обврска на ЛРК да ги обработува барањата на претплатникот исклучиво преку овластените вработени во ЛРК.

Локалната регистрациона канцеларија е одговорна за доставување на средство за креирање квалификуван потпис (QSCD) или автентикација на документи во случај на далечински квалификуван сертификат на претплатникот или субјектот.

ЛРК ги доставува до Регистрационата канцеларија сите барања на претплатникот, придружени со поврзаните документи за одобрување или одбивање за издавање, обновување со нов пар клучеви или поништување сертификати.

КИБС ги обучува овластените вработени во ЛРК за процесот на валидација и безбедносните процедури, пред да започне со операциите поврзани со ЛРК и потоа спроведува повторна годишна обука.

КИБС прави годишни ревизии на работењето и процедурите на ЛРК за да се обезбеди усогласеност со овие CP/CPS, плановите за валидација и договорот за ЛРК.

1.3.4. Претплатници

Во овие CP/CPS се користат два различни термини за да се направи разлика помеѓу следните две улоги:

- **„Претплатник“** е ентитетот кој склучува договор со КИБС за издавање на сертификат; и
- **„Субјект“** е лицето кое е поврзано со сертификатот.

Претплатникот ја има крајната одговорност за користењето на сертификатот, но субјектот е лице кое се автентицира кога ќе се презентира сертификатот.

Претплатник подразбира физичко или правно лице на кое КИБС им ги обезбедува доверливите услугите во согласност со овие CP/CPS.

Субјект значи:
- физичко лице,
- физичко лице кое е идентификувано дека е поврзано со правно лице,
- правно лице.

Претплатникот може или не мора да биде субјект на сертификат. Врската помеѓу претплатникот и субјектот е едно од следниве:

- За да се побара сертификат за физичко лице, претплатникот е:
  - а) самото физичко лице;
  - б) физичко лице со овластување да го застапува субјектот; или
  - в) секој ентитет со кој е поврзано физичкото лице.
- За да се побара сертификат за правно лице, претплатникот е:
  - а) секој ентитет како што е дозволено според релевантниот правен систем да го претставува правното лице; или

b) правен застапник на правно лице кое се претплатува за своите подружници или единици или оддели.

1.3.5. Засегнати страни

Засегната страна е лице или ентитет чие делување се заснова на доверба во сертификат и/или дигитален потпис издаден од ИС. Засегнатата страна може или не мора да биде претплатник. Засегнатите страни мора да го проверат соодветниот CRL или OCSP одговор, пред да се потпрат на информациите дадени во сертификатот. Локацијата на точката на дистрибуција на CRL детално е дадена во рамките на сертификатот.

1.3.6. Други учесници

Другите учесници вклучуваат:

- Тело за управување со правилата и постапките на ДДУ (PMA - Policy Management Authority) на КИБС, кое е одговорно за измените и дополнувањата на овие CP/CPS.
- Компанија „ADACOM S.A.“ врз основа на договор со КИБС. Основа на договорот е фактот дека ADACOM е QTSP кој е соодветно ревидиран според eIDAS и е во согласност со барањата од член 20 од eIDAS. Според овој договор, КИБС прави аутсорсинг на потребата за средства, доверливи системи и процедури за генерирање, безбедно чување и обезбедување на други делови од животниот циклус на коренските и издавачките сертификати на КИБС (КИБС ИС) во ADACOM.

  Со овој договор, КИБС прифаќа дека во рамките на овие CP/CPS, капацитетите, системите и процедурите на ADACOM ги наведува како свои.

1.4. Користење на сертификатите

Дигитален сертификат претставува форматирани податоци кои криптографски ги врзува идентификуваниот претплатник со јавен клуч. Дигиталниот сертификат му овозможува на ентитетот кој учествува во електронска трансакција да го докаже својот идентитет на другите учесници во таквата трансакција.

1.4.1. Дозволена употреба на сертификати

1.4.1.1. Сертификати издадени за електронски потпис

Квалификуваните сертификати за електронски потписи обично се користат од страна на поединци за потпишување електронски документи, е-пораки и за автентикација, под услов употребата на друг начин да не е забранета со закон, со овие CP/CPS, Правилата и условите и други договори со претплатниците.

Сертификати се усогласени со QCP-n и QCP-n-qscd.

Сертификатите издадени според овие барања имаат за цел да поддржат квалификувани електронски потписи со употреба на средство за креирање квалификуван потпис (QSCD), како што е дефинирано во член 3 (29) од MK-eIDAS и член 3 (12) од eIDAS и напредни електронски потписи без употреба на средство за креирање квалификуван потпис (QSCD), како што е дефинирано во член 3 (28) од MK-eIDAS и член 3 (11) од eIDAS.

1.4.1.2. Сертификати издадени за електронски печати

Квалификуваните сертификати за електронски печат обично се користат за да се обезбеди интегритет и потекло на тие податоци со кои се поврзани или за други цели, под услов употребата на друг начин да не е забранета со закон, со овие CP/CPS, Правилата и условите и сите други договори со претплатници.

Сертификатите се усогласени со QCP-l и QCP-l-qscd.

Сертификатите издадени според овие барања имаат за цел да поддржат квалификувани електронски печати со употреба на средство за креирање квалификуван потпис (QSCD) како што е дефинирано во член 3 (33) од MK-eIDAS и член 3 (27) од eIDAS и напредни електронски печати без употреба на QSCD како што е дефинирано во член 3 (32) од MK-eIDAS и член 3 (26) од eIDAS.

1.4.2. Забранета употреба на сертификати

Сертификатите ќе се користат само до таа мера до која користењето е во согласност со важечки закон, а особено се користат само до таа мера до која е дозволено со важечките закони за извоз или увоз.

Издавачките сертификатите не смеат да се користат за какви било функции освен за функциите за издавање на претплатнички сертификати. Покрај тоа, претплатничките сертификати нема да се користат како издавачки сертификати. Забрането е користење сертификати, освен за поддршка на апликации идентификувани во дел 1.4.1 од овие CP/CPS.

Засегнатите страни ќе го користат OID на политиката за издавање на сертификати на КИБС, идентификувани во сертификатот за соодветно прифаќање или одбивање на користењето на сертификатот.

1.5. Администрирање на правилата

1.5.1. Организација која го администрира документот

Овие CP/CPS и релевантните документи што се наведени овде ги одржува Тело за управување со правилата и постапките на ДДУ (PMA - Policy Management Authority) на КИБС, со кое може да се контактира на:

КИБС АД Скопје
Кузман Јосифовски Питу 1
1000, Скопје, Република Северна Македонија
тел. +389 2 5513401, +389 2 3297401
е-пошта: pma@kibstrust.com

1.5.2. Лице за контакт

Менаџер за PKI политика
КИБС АД Скопје
Кузман Јосифовски Питу 1,
1000, Скопје, Република Северна Македонија
тел. +389 2 5513401, +389 2 3297401
е-пошта: pma@kibstrust.com

1.5.2.1. Лице за контакт за поништување

За барање за поништување сертификат, види дел 4.9.3.

1.5.3. Лице кое ја определува соодветноста на овие правила

Телото за управување со правилата и постапките на ДДУ на КИБС (PMA) ја утврдува соодветноста и применливоста на овие CP/CPS врз основа на резултатите и препораките од ревизиите за сообразност.

1.5.4. Процедура за одобрување на правилата

Одобрување на овие CP/CPS и последователните измени се прават од страна на PMA. Измените се како документ што содржи изменета форма на CP/CPS или како забелешка за ревидиран текст. Изменетите верзии или ажурираните одредби се поврзани со делот за Ажурирања и известувања за практики на складиштето на КИБС што се наоѓа на:

https://www.kibstrust.com/repository/cps.

Ажурирањата ги заменуваат сите назначени или спротивставени одредби на референтната верзија на CP/CPS. PMA утврдува дали промените во CP/CPS бараат промена во предметните идентификатори на политиката за сертификати, во рамките на Политиките за сертификати.

Дури и ако нема задолжителна причина за промена на овие CP/CPS, PMA спроведува процес на преглед најмалку еднаш годишно во обид за подобрување.

1.6. Дефиниции и кратенки

Види Додаток А за табела на кратенки и дефиниции.

2. ОДГОВОРНОСТ ПОВРЗАНА СО ОБЈАВУВАЊЕ И СМЕСТУВАЊЕ

2.1. Складишта

КИБС е одговорен за функциите на складиштето за своите сопствени издавачки сертификати. КИБС ги објавува претплатничките сертификати за крајните корисници во складиштето, во согласност со дел 2.2.

По поништување на претплатнички сертификат, КИБС го објавува поништувањето во складиштето и издава нова верзија на Регистар на поништени сертификати (CRL) и овозможува OCSP услуги во согласност со одредбите од овие CP/CPS.

КИБС обезбеди неговото складиште да биде достапно 24 часа на ден, 7 дена неделно, со минимална достапност од 99,00% годишно и со предвидено време на прекин што не надминува 0,4% на годишно ниво.

При нефункционирање на системот, услугата или другите фактори кои не се под контрола на КИБС, КИБС треба да вложи максимални напори за да спречи недостапноста на оваа информативна услуга да не го надмине горенаведеното време.

2.2. Објавување на информации за сертификатот

КИБС одржува веб-базирано складиште во јавната мрежа за комуникација на податоци (https://pki.kibstrust.com/repository) кое им овозможува на засегнатите страни да побараат онлајн информации за поништен или некој друг статус на сертификат. КИБС им дава на засегнатите страни информации за тоа како да го пронајдат складиштето за да го проверат статусот на некој сертификат и како да го најдат вистинскиот OSCP респондер.

КИБС во своето складиште за јавни информации ги објавува во најмала мера следниве информации:

- Преглед на хиерархијата за сертификати,
- Правила за издавање сертификати,
- Резултати од ревизија,
- Политики на осигурување,
- Политики за сертификати,
- Сертификати, вклучувајќи коренски и издавачки сертификати,
- Профили на сертификати,
- Правила и услови за користење на квалификувани доверливи услуги,
- Регистар на поништени сертификати,
- Пребарување на сертификат,
- Политика на приватност.

2.2.1. Политики на објавување и известување

Овие CP/CPS на КИБС се објавени во КИБС складиштето за јавно информирање на:

https://www.kibstrust.com/repository/CPS

CP/CPS на КИБС се објавуваат заедно со датумите на применување не порано од 10 дена пред нивно стапување во сила.

2.2.2. Делови кои не се објавуваат во Правилата за издавање сертификати

Види дел 9.3.1 од овој CP/CPS.

2.3. Време и периодичност на објавување

Информации за статусот на сертификатот се објавуваат во согласност со одредбите на овие CP/CPS.

Види дел 2.2.1 од тековните CP/CPS за ажурирања на овие CP/CPS. Ажурираните одредби и услови се објавуваат според потреба. Сертификатите се објавуваат веднаш по издавање.

2.4. Контрола на пристап во складиштата

Информациите објавени во делот на складиштето на веб страницата на КИБС се јавно достапни информации. Пристап до таквата информација со опција само за преглед не е ограничена. КИБС бара лицата да се согласат со Правилата и условите како услов за пристап до сертификатите, до информациите за статусот на сертификатите или до CRL. КИБС применува мерки на логичка и физичка сигурност за да се спречи неовластени лица да додаваат, бришат или менуваат содржини во складиштето, во согласност со политиките за сигурност на КИБС. КИБС го прави своето складиште јавно достапно само на начин за да може да се прочитаат информациите, посебно на линкот https://pki.kibstrust.com/repository.

3. ИДЕНТИФИКАЦИЈА И АВТЕНТИКАЦИЈА

3.1. Именување

Именувањата во сертификатите се наведени во препораката ITU-T X.509 или IETF RFC 5280 и соодветниот дел од ETSI EN 319 412.

3.1.1. Типови на имиња

Типовите на имиња доделени на ИС и на претплатникот се опишани во соодветната документација за профилот на сертификатот објавена во складиштето на КИБС.

Сертификатите на КИБС ИС и на претплатникот содржат карактеристични имиња (Distinguished Names) во полињата за Издавач (Issuer) и Субјект (Subject) согласно X.501.

3.1.2. Потреба имињата да имаат значење

Претплатничките сертификати содржат имиња со вообичаено разбирлива семантика која дозволува определување на идентитетот на лицето кое е субјект на сертификатот.

КИБС ИС сертификатите содржат имиња со вообичаено разбирлива семантика која дозволува определување на идентитетот на ИС кој е субјект на сертификатот.

3.1.3. Анонимност или псевдоними на претплатниците

Не е дозволена анонимност или употреба на псевдоними .

3.1.4. Правила за интерпретирање различни именски форми

Полињата содржани во дигиталните сертификати се во согласност со овие CP/CPS и профилите на дигиталните сертификати, детално наведени во дел 7. Општо, правилата за толкување на формите на имиња може да се најдат во Стандардите за меѓународни телекомуникации (ITU) и Техничкиот стручен тим за интернет (IETF), како што се серијата стандарди ITU-T X.500 и применливите IETF RFC.

RFC-822 имињата може да се користат како алтернативни имиња на субјекти со назначување на адреса за е-пошта на субјектот на сертификатот.

3.1.5. Единственост на имињата

КИБС потврдува дека карактеристичните имиња на субјектот (Distinguished Names of Subject (DN)) на претплатникот се единствени во доменот за определен ИС преку автоматизирани компоненти на процесот на запишување на претплатникот. Возможно е еден претплатник да има два или повеќе сертификати со слични карактеристични имиња на субјектот.

Единствеността на карактеристичното име за електронски потписи и автентикација е обезбедена со вредноста на атрибутот Сериски број во полето Субјект на сертификатот. За електронските печати тоа е обезбедено со вредноста на атрибутот Организациски идентификатор во полето Субјект на сертификатот.

3.1.6. Признавање, проверка и улога на трговските марки

На подносителите на барања за сертификат им е забрането во своите барања за сертификати да користат имиња што ги прекршуваат правата на интелектуална сопственост на други. Сепак, КИБС не проверува дали подносителот на барањето за сертификат има права на интелектуална сопственост на името што се појавува во барањето за сертификат, ниту пак арбитрира, посредува или на кој било друг начин

разрешува спорови во врска со кое било име на домен, трговско име, трговска марка или сервисна марка. КИБС има право, без да понесе одговорност кон кој било подносител на барање за сертификат, да одбие или суспендира барање за сертификат заради таков спор.

3.2. Првична потврда на идентитетот

КИБС може да користи методи опишани во овој дел за да го утврди идентитетот на претплатникот. КИБС може да одбие да издаде сертификат според свој избор, доколку проверката на идентитетот не е успешна.

Проверувањето на идентитетот е дел од процесот на барањето за сертификат, издавање сертификат и обезбедување уред/средство.

3.2.1. Метод за докажување сопственост врз приватниот клуч

Процесот на генерирање клучеви е обезбеден со овие CP / CSP во согласност со техничките стандарди ETSI EN 319 401, ETSI EN 319 411-1 и ETSI EN 319 411-2.

Подносителот на барањето за сертификат мора да покаже дека тој / таа со право го има приватниот клуч што одговара на јавниот клуч што треба да се наведе во сертификатот. Методот за докажување поседување на приватен клуч е PKCS # 10, друга еквивалентна криптографска демонстрација или друг одобрен метод од КИБС. Ова барање не се применува кога парот клучеви се генерира од КИБС во име на претплатникот, на пример, кога клучевите кои претходно се генерирани се постават на QSCD.

За квалификувани сертификати поврзани со приватни клучеви во средство за креирање квалификуван потпис / печат (QSCD):

- Во случај на локално QSCD, приватните клучеви се генерираат и складираат на локалното QSCD. Генерирање приватни клучеви може да биде во присуство на носителот на сертификатот (во случај на лице-в-лице препознавање) или без присуство на носителот на сертификатот (во случај на далечинско препознавање). Носителот на сертификатот е одговорен за обезбедување на локалното QSCD со доделен личен идентификациски број (PIN) надвор од опсегот, за пристап до QSCD.
- Во случај на далечинско QSCD, приватните клучеви се генерираат и складираат под контрола на носителот на сертификатот на хардверски безбедносен модул кој се наоѓа во центарот за податоци на КИБС. Пристапот од страна на носителот на сертификатот до клучевите е заштитен со помош на повеќефакторска автентикација со цел да се постигне истото ниво на сигурност на единствена контрола како што е постигната со локалното QSCD.

3.2.2. Автентикација на идентитетот на организацијата (правно лице)

3.2.2.1. Верификација на идентитетот на правното лице

Идентитетот на правното лице кое е претплатник на квалификуван сертификат се верификува во согласност со сегашното законодавство, и се изведува на еден од следниве начини:

За издавање сертификат, потребно е да се идентификува претплатникот - правното лице и правниот застапник (точки 1 и 2):

1) Потврдата на идентитетот на **претплатникот** (правно лице) се врши на еден од следниве начини:
   - За правно лице регистрирано во Македонија, внесените податоци за правното лице во образецот за порачка и договор се проверуваат со податоците за тоа правно лице, зачувани во регистарот на правни лица и други субјекти во Централниот регистар на Република Северна Македонија, вклучително и името на правниот застапник.
   - За правно лице регистрирано надвор од Македонија, потребно е да се приложи доказ од трговскиот регистар или сличен орган кој има право да потврди дека претплатникот е регистриран како правно лице во домицилната земја, вклучувајќи го името на правникот застапник. Сертификатот се доставува во оригинал, а документот преведен од овластен судски преведувач на македонски или англиски јазик.
2) Потврда за идентитетот на **застапникот на правното лице**

- кој своерачно го потпишува образецот „Порачка и договор“, се врши на следниов начин:
  - За правно лице регистрирано во Македонија, се приложува нотарски заверен примерок од заверен образец за потпис (ЗП образец), каде е заведен своерачниот потпис на правниот застапник, или
  - За правно лице регистрирано надвор од Македонија: со доставување соодветен образец, каде поврзувањето на банкарската сметка со своерачниот потпис на правниот застапник е заверена, или
  - Правниот застапник го потпишува овој образец за порачка и договор пред нотар. Нотарот ќе го завери образецот.
  - Правниот застапник приложува документ за лична идентификација и го потпишува овој образец за порачка и договор пред службеникот на ЛРК / РК.
- кој **дигитално го потпишува** образецот ,,Порачка и договор” со квалификуван сертификат за електронски потпис или електронски печат, издаден од давател на квалификувана услуга, којшто го потврдува идентитетот на правниот застапник.

Во случај кога трето лице ќе се поднесе барање за издавање на квалификуван сертификат, треба да се приложи примерок од полномошно од правниот застапник на тоа трето лице или кој било друг еквивалентен документ кој докажува дека третото лице може да се потпише во име на правниот застапник.

3.2.3. Автентикација на идентитетот на лице (физичко лице)

3.2.3.1. Верификација на идентитетот на физичко лице

Идентитетот на физичкото лице кој е претплатник и субјектот на квалификуван сертификат се верификува согласно сегашното законодавство, и се изведува на еден од следниве начини:

- Со физичко присуство на претплатникот во ЛРК / РК на КИБС ИС, на адресата објавена на https://www.kibstrust.com/en-GB/Home/Contact/ , каде што:
  - приложува документ за лична идентификација (лична карта или пасош)
  - го потпишува образецот ,,Порачка и договор” пред службеникот на ЛРК / РК.
- Доколку претплатникот не е во можност лично да дојде во ЛРК / РК на KIBS ИС, тој / таа лично мора да оди кај нотар и пред нотарот да го потпише образецот ,,Порачка и договор” за кој нотарот ќе направи нотарска заверка,
- Далечински, со користење на квалификуван сертификат за електронски потпис издаден од давател на квалификувана доверлива услуга, или преку далечинска верификација на идентитетот еквивалентна на физичко присуство со која физичкото лице се идентификува преку сесија на препознавање, управувано автоматски или од овластен вработен во ЛРК/РК.
- Физичкото лице треба да обезбеди прифатливи документи за идентификација: лична карта за жител на Република Северна Македонија, привремена лична карта за странски државјани со привремен престој во Република Северна Македонија, лична карта за странски државјани за државјани од земји што Владата на Република Северна Македонија ја прифаќа како легална патна исправа и пасош за сите граѓани. Документот за идентификација вклучува единствен број што му е доделен на подносителот од споменатата земја што го издава личниот документ.

3.2.3.2. Верификација на идентитетот на физичко лице поврзано со правно лице

Во случај на физичко лице кое е субјект на квалификуван сертификат поврзан со правно лице кое е претплатник:

1. со физичко присуство на физичкото лице поврзано со правното лице (Субјект) и застапникот на правното лице во ЛРК/РК на КИБС ИС, на адресата објавена на https://www.kibstrust.com/en-GB/Home/Contact/ кои ги доставуваат на РК или на ЛРК на КИБС или овластениот вработен на ЛРК следниве документи:
   - Доказ за идентитетот на субјектот и на застапникот на правното лице [полно име, датум и место на раѓање], врз основа на лична карта за жител на Република Северна Македонија, привремена

лична карта за странски државјани со привремен престој во Република Северна Македонија, лична карта за странски државјани за државјани од земји што Владата на Република Северна Македонија ја прифаќа како легална патна исправа и пасош за сите граѓани, со оглед на тоа што документот вклучува единствен број што му е доделен на подносителот на барањето од горенаведената земја што го издава личниот документ;

- Писмено и прописно потпишан образец ,,Порачка и договор" од застапникот на правното лице и физичкото лице дека атрибутите на субјектот, исто така, ја идентификуваат таа организација.

2. Доколку субјектот и застапникот на правното лице не се во можност да дојдат лично во ЛРК/ РК на КИБС ИС, тие мора лично да одат кај нотар и пред нотарот да го потпишат образецот ,,Порачка и договор" за кој нотарот ќе направи нотарска заверка. Документите се доставуваат до РК на КИБС со физичко присуство на соодветно овластен претставник на претплатникот, доколку претставникот е прописно овластен од претплатникот да го застапува.

3. Далечински, со квалификуван сертификат за електронски потпис или електронски печат издаден од квалификуван давател на доверлива услуга, со кој се потврдува идентитетот на правниот застапник, и со испраќање на сите документи наведени во став 1 погоре, преку е-порака до РК/ЛРК на КИБС.

4. Со далечинска проверка на лична карта, еквивалентно на физичко присуство на физичкото лице поврзано со правно лице (Субјект) и застапникот на правното лице. Далечинска проверка на лична карта се заснова на лична карта за жител на Република Северна Македонија, привремена лична карта за странски државјани со привремен престој во Република Северна Македонија, лична карта за странски државјани за државјани од земји што Владата на Република Северна Македонија ја прифаќа како легална патна исправа. Образецот ,,Порачка и договор" креиран онлајн мора да биде прифатен од физичкото лице и застапникот на правното лице.

3.2.3.3. Потврдување на доменот електронска пошта

КИБС го потврдува правото на претплатникот да користи или контролира адреса за е-пошта што треба да биде содржана во сертификат со испраќање на е-порака за одобрување на адресата за е-пошта што треба да се вклучи во сертификатот.

3.2.4. Информација за претплатникот што не се проверува

Информациите за претплатници што не се проверуваат вклучуваат:

- Атрибути на Организациската единица (ОЕ),
- Сите други информации означени како непотврдени во сертификатот (како на пр. „Назив" за упатување на работната позиција).

3.2.5. Потврдување на овластување

Секогаш кога во сертификатот името на физичкото лице е поврзано со име на правно лице на таков начин за да покаже поврзаност на лицето или негово овластување да делува во име на правното лице.

КИБС РК:

- потврдува дека организацијата постои преку користење на најмалку една услуга за докажување на идентитетот или база на податоци на трето лице, или алтернативно, со документација на организацијата издадена од или доставена до соодветна надлежна институција која го потврдува постоењето на таа организација, и

- користи информации што се содржани во деловната документација или базата на податоци за деловни информации (директориуми на вработени и клиенти) на некоја РК која одобрува сертификати на лица поврзани со неа или потврдува преку телефон, поштенска пратка со потврда или во слична процедура на организацијата, кога тоа е соодветно, дека лицето има овластување да делува во име на организацијата.

3.2.6. Критериуми на интероперабилност

Не се применува.

3.3. Идентификација и автентикација на барања за обновување на пар клучеви

Пред истекот на постоечки претплатнички сертификат, неопходно е претплатникот да добие нов сертификат за да го одржи континуитетот на користење на сертификатот. КИБС обично бара на претплатникот да му се генерира нов пар клучеви за да се замени парот на кој му истекува важноста (технички дефинирано како ,,обнова на пар клучеви“ (re-key).

Видете го делот 3.2.2 и 3.2.3 од овие CP/CPS.

Покрај тоа, сите потребни документи можат да бидат испратени електронски, дигитално потпишани од постоечки квалификуван сертификат за електронски потписи.

3.3.1. Идентификација и автентикација за рутинско обновување на пар клучеви

Не се применува.

3.3.2. Идентификација и автентикација при обновување на пар клучеви после поништување

Претплатникот мора да го помине почетниот процес на регистрација според деловите 3.2.2 и 3.2.3 на овие CP/CPS.

3.4. Идентификација и автентикација на барање за поништување

РК ги автентицира сите барања за поништување.

Пред да поништи сертификат, РК проверува дали поништувањето е побарано од претплатникот на сертификатот или ентитетот кој го одобрил барањето за сертификат.

Прифатливите процедури за автентикација на барање за поништување од претплатникот вклучуваат една или повеќе од следниве постапки:

- Да се побара од претплатникот да ја внесе фразата за автентикација, по што автоматски се поништува сертификатот ако фразата за автентикација се совпаѓа со онаа што е веќе евидентирана;
- Претплатникот потпишува образец за поништување сертификат во хартиена форма од барањето за поништување;
- Претплатникот доставува електронски образец за поништување преку веб порталот на КИБС автентициран како регистриран корисник со дополнително сигурносно ниво, обезбедено со двофакторска автентикација;
- Добивање порака од претплатникот кој бара поништување, а која содржи дигитален потпис којшто може да се верификува со сертификатот што треба да се поништи;
- Комуникација со претплатникот што ќе обезбеди разумни уверувања кои потврдуваат со сигурност дека лицето или организацијата која бара поништување е навистина претплатникот или има прописно овластување да го побара тоа. Таквата комуникација, во зависност од околностите, може да вклучи едно или повеќе од следново: телефон, факс, електронска пошта, стандардна пошта или курирска служба.

Администраторите на РК на КИБС се овластени да побараат поништување сертификати во рамките на доменот на КИБС. КИБС, пред да му дозволи на администраторот да ја изведе функцијата на поништување, ќе изврши автентикација на идентитетот на администраторот преку контрола на пристапот со употреба на SSL и автентикација на клиентот.

4. ОПЕРАТИВЕН ЖИВОТНИОТ ЦИКЛУС НА СЕРТИФИКАТОТ

4.1. Барање за сертификат

4.1.1. Кој може да поднесе барање за сертификат

Барање за квалификуван сертификат може да поднесе физичко лице или правно лице кое е претплатник на сертификатот, доколку е законски квалификувано. Подносителите на барање се одговорни за сите податоци што барателот или секое друго лице, овластено од барателот, ќе ги достави до КИБС.

4.1.2. Процес на регистрирање и одговорности

Сите претплатници на сертификат се согласуваат со Правилата и условите, кои содржат изјави и гаранции опишани во делот 9.6.3 и поминуваат низ процесот на регистрација кој се состои од:

- Прифаќање на Правилата и условите во врска со користењето на сертификатот;
- Пополнување и потпишување образец ,,Порачка и договор" и давање точни и вистинити информации во согласност со барањата од оваа Политика;
- Обезбедување релевантни документи за валидација;
- Генерирање или организирање за да се генерира пар клучеви;
- Добивање на неговиот/нејзиниот сертификат, директно или преку РК/ЛРК;
- Докажување дека поседуваат и/или имаат ексклузивна контрола на приватниот клуч кој соодветствува на јавниот клуч;
- Плаќање на сите применливи давачки, доколку е потребно.

4.2. Обработка на барањето за сертификат

4.2.1. Извршување на функциите на идентификација и автентикација

КИБС врши идентификација и автентикација на сите потребни информации за претплатникот:

а) со физичко присуство,
б) на оддалеченост со квалификуван сертификат, или
в) со употреба на метод еквивалентен на физичко присуство, во согласност со дел 3.2.

Ако ЛРК/РК помага во верификацијата, тогаш ЛРК/РК мора да креира и да одржува евиденција доволна за да утврди дека ги извршила своите потребни задачи за верификација и му го соопштува на КИБС завршувањето на таквите задачи. Откако ќе заврши верификацијата, КИБС ги оценува информациите и одлучува дали да го издаде сертификатот.

Како дел од оваа евалуација, КИБС РК може да го провери сертификатот во однос на внатрешната база на податоци на претходно поништени сертификати и одбиени барања за сертификат за да ги идентификува сомнителните барања за сертификати.

4.2.2. Одобрување или одбивање на барањата за сертификат

КИБС одобрува барање за сертификат само доколку се задоволени следниве критериуми:

- Успешна идентификација и автентикација на сите потребни информации за претплатникот, во согласност со дел 3.2;
- Уплатен надоместок.

КИБС ќе го одбие барањето за сертификат ако:

- Не може целосно да се изврши идентификацијата и автентикацијата на сите потребни информации за претплатникот во смисла на дел 3.2, или
- Претплатникот не ги доставил потребните документи за барање,
- Претплатникот не одговорил на забелешките во рокот определен за тоа;
- Не е уплатен надоместокот за сертификатот, или
- КИБС оценил дека издавањето на сертификатот на претплатникот може да и донесе лоша репутација на КИБС.

Во случај КИБС да одбие сертификат за барање поврзано со далечинското QSCD, релевантната претплатничка сметка не се креира и не се потребни други активности од претплатникот.

4.2.3. Време на обработка на барањата за сертификат

КИБС започнува со обработка на барањата за сертификат во разумен временски рок по приемот на целосната документација. Барањето за сертификат останува активно сè додека не се одбие, издаде или автоматски не истече во рок од 30 дена. Истечените обрасци ,,Порачка и договор" за сертификат автоматски се бришат од корисничката база на податоци на КИБС.

4.3. Издавање сертификат

4.3.1. Активности на ИС за време на издавање на сертификатот

Сертификатот се креира и издава по одобрување на барањето за сертификат (образец ,,Порачка и договор") од страна на КИБС, врз база на информации што се содржани во образецот ,,Порачка и договор".

Базите на податоци и процесите на ИС што се одвиваат при издавање на сертификат се заштитени од неовластена модификација. По завршувањето на издавањето, сертификатот се чува во базата на податоци и се испраќа до претплатникот.

4.3.2. Известување на претплатникот од страна на КИБС ИС за издавање на сертификатот

КИБС ги известува претплатниците дека сертификатите се креирани и им овозможува на претплатниците пристап до сертификатите известувајќи ги дека истите им се достапни. Сертификатите им се стават на располагање на претплатниците, со нивно информирање преку електронска порака или директно во просториите на РК/ЛРК. Известувањето содржи информации за тоа како претплатникот може да го подигне сертификатот.

4.4. Прифаќање сертификат

4.4.1. Однесување кое означува прифаќање на сертификатот

Следниве постапки престставуваат прифаќање на сертификатот:

- Преземањето на сертификат претставува прифаќање на сертификатот од претплатникот,
- Претплатникот нема да достави приговор за сертификатот или неговата содржина во рок од 5 дена претставува прифаќање на сертификатот.

4.4.2. Објавување на сертификатот од страна на ИС

КИБС објавува информации за сертификатите што ги издава во јавно достапно складиште. Претплатникот има право да избере дали информациите за сертификат и самиот сертификат, ќе бидат објавени во Јавниот именик за сертификати за издадените сертификати на КИБС ИС.

4.4.3. Известување за издавање на сертификатот од страна на КИБС ИС кон други ентитети

РК и ЛРК може да добијат известување за издавање на сертификати кои тие ги одобриле.

4.5. Користење на парот клучеви и на сертификатот

4.5.1. Користење на претплатничкиот приватен клуч и сертификатот

Користењето на приватниот клуч што кореспондира со јавниот клуч во сертификатот е дозволено само откако претплатникот ќе се согласи со Правилата и условите и ќе го прифати сертификатот. Сертификатот треба да се користи во согласност со Правилата и условите на КИБС ИС, и овие CP/CPS. Користењето на сертификатот мора да биде конзистентно со полето за користење на клучот (KeyUsage) вклучено во сертификатот. Употребата на клучот за сертификат е од типот Б како што е наведено во клаузулата 4.3.2 од ETSI EN 319 412-2.

Претплатниците треба да ги одржуваат своите приватни клучеви под нивна единствена контрола, да ги заштитат нивните приватни клучеви од неовластено користење и да престанат да го користат приватниот клуч по истекот или поништувањето на сертификатот. Другите страни кои не се претплатник не треба да го архивираат приватниот клуч на претплатникот.

4.5.2. Користење на јавниот клуч и сертификатот од страна на засегната страна

Засегнатите страни треба да се согласат со условите од Правилата и условите на КИБС, како услов за да се потпрат на сертификатот.

Довербата во сертификатот мора да биде соодветна на дадените околности. Ако околностите наложат потреба за дополнителни уверувања, засегнатите страни мора да ги добијат таквите уверувања за да може да имаат доверба во сертификатот.

Засегнатите страни, пред да се потпрат на податоците од сертификатот, самостојно треба да проценат:

- соодветност на употребата на сертификатот за која било дадена намена и треба да утврдат дека сертификатот, всушност, ќе се користи за соодветна намена што не е забранета или на друг начин ограничена со овие CP/CPS. КИБС не е одговорен за проценката на соодветноста за користењето на сертификатот;
- дека сертификатот се користи во согласност со екстензиите наведени во полето за употреба на клучот (KeyUsage), вклучени во сертификатот;
- статусот на сертификатот и на останатите сертификати во синџирот на сертификати. Ако некој од сертификатите во синџирот е поништен, единствено засегнатата страна е одговорна да истражува дали довербата во дигиталниот потпис, спроведен од претплатникот - краен корисник на сертификатот пред поништувањето на сертификатот во синџирот на сертификати е законски. Ризикот од укажување доверба е исклучиво на засегнатата страна.

Под претпоставка дека користењето на сертификатот е соодветно, засегнатите страни треба да применат соодветен софтвер и/или хардвер за да извршат проверка на дигиталниот потпис или други криптографски операции што сакаат да ги изведат, како услов за потпирање на сертификатите во однос на секоја таква операција. Овие операции вклучуваат и идентификување на синџирот на сертификати и проверување на дигиталните потписи за сите сертификати во синџирот на сертификати.

4.6. Обновување сертификат

Не се применува.

4.7. Обновен сертификат со нов пар клучеви (Certificate Re-Key)

Обновување сертификат со нов пар клучеви е барање за издавање нов сертификат со кој се сертифицира новиот јавен клуч.

4.7.1. Околности за обновување сертификат со нов пар клучеви

За да го одржи континуитетот на користење на сертификатот, неопходно е претплатникот да изврши обновување на сертификатот со нов пар клучеви најмалку 30 дена пред истекот на важноста на постојниот сертификат на претплатникот. Исто така, сертификат може да се обнови со нов пар клучеви по истекувањето.

4.7.2. Кој може да побара сертифицирање на нов јавен клуч

Само претплатникот може да побара обновување на сертификатот со нов пар клучеви.

4.7.3. Обработка на барања за обновување сертификат со нов пар клучеви

Процедурата на обновување сертификат со нов пар клучеви со сигурност утврдува дека лицето кое бара да се обнови сертификатот за претплатникот - краен корисник навистина е претплатникот (или овластен од претплатникот) на сертификатот.

Претплатникот поднесува барање за нов пар клучеви до КИБС РК/ЛРК дигитално потпишано (со својот постоечки и важечки сертификат).

КИБС РК/ЛРК повторно го потврдува идентитетот на претплатникот, согласно со условите за идентификација и автентикација опишани во дел 3.3.1.

Освен оваа постапка или друга постапка одобрена од КИБС, барањата за автентикација на оригиналната апликација за сертификат ќе се искористат за обновување клучеви на сертификат за претплатник - краен корисник.

4.7.4. Известување за издавање на нов сертификат до претплатникот

Известувањето на претплатникот за издавањето на сертификатот со обновен пар клучеви е во согласност со дел 4.3.2.

4.7.5. Однесување кое означува прифаќање на обновениот сертификат

Однесувањето кое означува прифаќање на обновениот сертификат со нов пар клучеви е во согласност со дел 4.4.1.

4.7.6. Објавување на обновен сертификат со нов пар клучеви од страна на ИС

Објавувањето на обновениот сертификат со нов пар клучеви се врши во јавно достапното складиште на КИБС.

4.7.7. Известување на други ентитети за издавање на сертификатот од страна на ИС

РК и ЛРК може да добие известување за издавањето на сертификати кои тие ги одобриле.

4.8. Изменување на сертификат

4.8.1. Околности за изменување на сертификат

Изменувањето на сертификат се однесува на барањето за издавање нов сертификат заради промена на податоците во постојниот сертификат (различни од јавниот клуч на претплатникот).

Изменувањето на сертификат се смета како барање за сертификат во смисла на дел 4.1.

4.8.2. Кој може да побара измени во сертификатот

Види дел 4.1.1.

4.8.3. Обработка на барања за измени во сертификат

КИБС врши идентификација и автентикација на сите потребни информации на претплатникот во согласност со дел 3.2.

4.8.4. Известување на претплатникот за издавање на нов сертификат

Види дел 4.3.2.

4.8.5. Однесување кое означува прифаќање на изменетиот сертификат

Види дел 4.4.1.

4.8.6. Објавување на изменетиот сертификат од страна на ИС

Види дел 4.4.2.

4.8.7. Известување на други ентитети за издавање сертификат од страна на ИС

Види дел 4.4.3.

4.9. Поништување и суспендирање на сертификат

Со поништувањето на сертификат трајно завршува оперативниот период на сертификатот пред сертификатот да го достигне крајот на наведениот период на важење. Пред поништување на сертификат, сите барања за поништување се автентицираат според дел 3.4.

Поништување на сертификати се врши според деловите кои следат.

За сертификатите кои вклучуваат адреса за е-пошта, поништувањето и суспендирањето на сертификатот е во согласност со барањата на CA/B Форумот.

4.9.1. Околности за поништување

Правилата и условите на КИБС обезбедуваат обврска и/или право на претплатникот да бара поништување на сертификат. Само во околностите наведени подолу, претплатничкиот сертификат ќе биде поништен од КИБС ИС (или од претплатникот) и објавен во CRL.

Сертификатот за претплатник се поништува ако:

- КИБС ИС или претплатникот имаат причина да веруваат или да се сомневаат дека се случило компромитирање на приватниот клуч на претплатникот. Доколку трето лице пријави компромитација, КИБС ИС бара соодветна потврда од претплатникот;
- КИБС ИС има причина да верува дека претплатникот прекршил материјална обврска, изјава или гаранција од применливите Правила и услови за користење на квалификувани доверливи услуги;
- КИБС ИС има причина да верува дека сертификатот е издаден спротивно на процедурите од овие CP/CPS, издаден е на лице различно од она што е наведено како субјект во сертификатот, или сертификатот е издаден без овластување на лицето наведено како субјект во сертификатот;
- КИБС е свесен за измените кои влијаат врз валидноста на сертификатот;
- Користената криптографија повеќе не обезбедува поврзување на субјектот и јавниот клуч;
- КИБС има причина да верува дека некој од материјалните факти во барањето за сертификат е погрешен;
- КИБС утврдил дека материјалниот предуслов за издавање на сертификатот ниту е задоволен ниту одречен;
- Претплатникот ја губи правната квалификуваност, прогласен е за отсутен или починат, имајќи предвид дека сертификатот во секој случај е непреносliв;
- Претплатникот ја губи можноста да го користи локалното QSCD или мобилниот уред потребен за пристап до далечинското QSCD;
- Во случај кога субјектот на сертификатот е физичко лице поврзано со претплатник - правно лице и претплатникот бара поништување;
- Во случај на судска одлука без право на жалба која наложува поништување на сертификатот;
- Приватниот клуч на ИС е компромитиран;
- Надзорното тело бара поништување според законот;
- Идентитетот на претплатникот не е успешно повторно верификуван;
- Претплатникот не извршил плаќање кое доспеало;
- Продолжување со употребата на тој сертификат е штетен за КИБС ИС;

Кога се разгледува дали користењето на сертификат е штетно за КИБС ИС, КИБС ИС го разгледува, меѓу другото, и следново:

- Природата и бројот на примените рекламации;
- Идентитетот на оној кој ги направил рекламациите;
- Релевантните прописи што се во сила;
- Одговорите на наводното штетно користење од страна на претплатникот.

КИБС ИС може, исто така, да поништи администраторски сертификат ако овластувањето на администраторот да делува како администратор е прекинато или на друг начин завршило.

Според Правилата и условите на КИБС, претплатникот – краен корисник е должен веднаш да го извести КИБС ИС за сознанието или претпоставката дека неговиот приватен клуч е компромитиран.

По одобрување на барањето за поништување од страна на ИС, поништениот сертификат не може повторно да се стави во сила.

4.9.2. Кој може да побара поништување

Барање за поништување на квалификуван сертификат може да поднесе:

- РК или ЛРК;
- физичко или правно лице, или нивни правни застапници, кој е претплатник на сертификатот, или наследник кој сака да побара поништување во случај на починат претплатник (физичко лице), под услов тој да е законски квалификувано;
- надлежен суд или орган;
- Надзорно тело.

Барање за поништување на ИС сертификат може да поднесе:

- правно лице, кое е претплатник на сертификатот, под услов да е законски квалификуван;
- надлежен суд или орган;
- Надзорно тело.

4.9.3. Процедура за барање за поништување

Претплатникот кој бара поништување треба да упати барање до КИБС ИС за поништување на еден од следниве начини: преку онлајн услуга за поништување, по електронска пошта на revoke@kibstrust.com или образец во хартиена форма за поништување на сертификат кој се доставува до РК по што веднаш ќе биде иницирано поништување на сертификатот.

Доставувањето на ваквото барање за поништување мора да биде во согласност со дел 3.4.

4.9.4. Грејс период за барање за поништување

Барањата за поништување се поднесуваат во што е можно пократок временски период, во рамките на комерцијално разумно време.

4.9.5. Време за кое КИБС ИС мора да го обработи барањето за поништување

КИБС ИС презема комерцијално разумни чекори за да ги обработи барањата за поништување, без одлагање и во секој случај максималното одложување од моментот кога КИБС ИС ќе добие барање за поништување, во согласност со дел 4.9.3, до одлуката да ги промени информациите за статусот кои им се достапни на сите засегнати страни е најмногу 24 часа. Ако барањето за поништување не може да се потврди во рок од 24 часа, тогаш статусот не треба да се менува.

Веднаш по одобрувањето на барањето за поништување, ИС за овој настан го известува претплатникот и субјектот на сертификатот за поништувањето преку е-порака.

4.9.6. Барања за проверка на поништувањето на засегнатите страни

Засегнатите страни треба да го проверат статусот на сертификатот на кој сакаат да се потпрат. Еден од начините на кој засегнатите страни може да го проверат статусот на некој сертификат е да го консултираат најновиот CRL на ИС што го издал сертификатот на кој засегнатите страни сакаат да се потпрат. Како друга можност, засегнатите страни може да го проверат статусот на сертификатот со користење на веб-базираното складиште на КИБС ИС или со користење на OCSP. КИБС ИС ќе им обезбеди на засегнатите страни информација како да го пронајдат соодветниот CRL, веб-базираното складиште или OCSP респондерот за да го проверат статусот на поништување. Поради бројните и различните локации за CRL складиштата, засегнатите страни ќе бидат известени да пристапат до CRL со помош на URL поставени во екстензијата за CRL точките на дистрибуција на сертификатот.

Соодветниот OCSP респондер за даден сертификат е поставен во неговата екстензијата за пристап до информациите за Издавачот.

Информациите за статусот на поништување се стават на располагање по периодот на важење на сертификатот.

4.9.7. Интервали на издавање на CRL

CRL за сертификатите за претплатници- крајни корисници се издаваат најмалку еднаш дневно. CRL за ИС сертификатите се издаваат барем еднаш годишно, но, исто така, и секогаш кога ИС сертификат ќе биде поништен. Ако на сертификат што е наведен во CRL му истече важноста, тој може да биде отстранет во следно издадениот CRL, по истекот на важноста на сертификатот.

4.9.8. Максимално доцнење на CRL

CRL се поставува во складиштето во разумно комерцијално време откако ќе биде генериран. Ова главно се прави автоматски неколку минути по генерирањето.

4.9.9. Достапност за онлајн проверка на статусот во врска со поништување

Информации во врска со онлајн поништување, како и други информации за статусот на сертификатот се достапни преку веб-базираното складиште и OCSP. Покрај објавувањето на CRL, КИБС обезбедува

информации за статусот на сертификат и преку функциите за пребарување во складиштето на КИБС. Информации за статусот на сертификатот за квалификувани сертификати се достапни во складиштето на КИБС на: https://pki.kibstrust.com/repository.

OCSP одговорите се обезбедуваат во комерцијално разумен рок по приемот на барањето, и тоа подлежи на доцнење при преносот преку интернет. OCSP одговорите се во согласност со RFC 5019 и / или RFC 6960. OCSP одговорите:

1. Се потпишани од ИС што ги издал сертификатите чиј статус на поништување се проверува, или
2. Се потпишани од OCSP респондер чиј сертификат е потпишан од ИС што го издал сертификатот, чиј статус на поништување се проверува.

Во вториот случај, сертификатот со OCSP потпишување содржи екстензија од типот id-pkix-ocspnocheck, како што е дефинирано од RFC 6960.

Максималното доцнење помеѓу потврдата за поништување на сертификатот за да стане ефективна и вистинската промена на информациите за статусот на овој сертификат што им се стават на располагање на засегнатите страни е најмногу 60 минути. Ако сепак, барањето за поништување бара поништување однапред (на пр., планиран прекин на должностите на субјектот на одреден датум), тогаш планираниот датум може да се смета како време на потврда.

4.9.10. Барања за онлајн проверка на поништување

Засегнатата страна мора да го провери статусот на сертификатот на кој сака да се потпре. Доколку засегната страна не го провери статусот на сертификатот на кој засегнатата страна сака да се потпре преку консултација со најновиот релевантен CRL, засегнатата страна ќе го провери статусот на сертификатот со консултација на КИБС складиштето или со барање за статус на сертификат користејќи го применливиот OCSP респондер.

4.9.11. Други достапни форми на огласување за поништување

Не се применува.

4.9.12. Посебни барања во врска со компромитирање на клуч

КИБС вложува комерцијално разумни напори да ги извести потенцијалните засегнати страни ако открие, или има причини да верува, дека приватниот клуч на некој од неговите сопствени ИС е компромитиран .

4.9.13. Околности за суспендирање

Не се применува.

4.9.14. Кој може да побара суспендирање?

Не се применува.

4.9.15. Процедура за барање за суспендирање

Не се применува.

4.9.16. Ограничувања на периодот на суспензија

Не се применува.

4.10. Услуги во врска со статусот на сертификатите

4.10.1. Оперативни карактеристики

Информациите за статусот на сертификатот се достапни преку CRL и OCSP респондер. Серискиот број на поништениот сертификат останува во CRL, сè додека не се објави уште еден дополнителен CRL по завршувањето на периодот на важење на сертификатот. OCSP информациите за претплатнички сертификати се ажурираат според дел 4.9.9.

4.10.2. Достапност на услуги

КИБС обезбедува достапност на услугите за статус на сертификат 24 часа дневно, 7 дена во неделата со минимум 99% достапност вкупно во годината со предвиден прекин кој не надминува 0,4% годишно.

4.10.3. Опционални карактеристики

Не се применува.

4.11. Крај на претплатата

Претплатникот може да ја прекине претплатата за квалификуван сертификат на КИБС:

- со тоа што ќе дозволи неговиот/нејзиниот квалификуван сертификат да истече без обновување на клучеви за тој сертификат;
- со поништување на квалификуваниот сертификат пред истекувањето на неговата важност, без да се изврши замена.

4.12. Давање на чување клучеви кај трето лице и повторно преземање

Не се применува.

4.12.1. Политика и пракса за давање на чување клучеви кај трето лице и повторно преземање

Не се применува.

4.12.2. Политика и пракса за енкапсулирање на сесиски клуч и повторно преземање

Не се применува.

5. ОБЈЕКТ, УПРАВУВАЊЕ И ОПЕРАТИВНИ КОНТРОЛИ

5.1. Физички контроли

КИБС има имплементирано множество од безбедносни правила, кои ги поддржуваат барањата од овие CP/CPS за сигурност. Придржувањето кон овие правила е вклучено во условите за ревизија на КИБС опишани во дел 8. Безбедносните правила на КИБС содржат чувствителни сигурносни податоци и се стават на располагање само по потпишување на договор со КИБС. Краток преглед на овие услови е даден подолу.

5.1.1. Локација на објект и негова конструкција

Операциите на КИБС ИС и РК се изведуваат во рамките на физички заштитена средина која одбива, спречува и регистрира неовластено користење, пристап или откривање на чувствителни информации, било да е тоа прикриено или неприкриено.

КИБС, исто така, одржува објект за опоравување по откажување на системот за своите операции на издавање на сертификати. Објектот за опоравување по откажување на системот на КИБС се заштитени со повеќе нивоа на физичка сигурност споредено со тие на примарната локација на КИБС.

5.1.2. Физички пристап

Системите на КИБС се заштитени со пет (5) нивоа на физичка заштита, при што е потребно да се има пристап до пониското ниво пред да се добие дозвола за пристап во повисокото ниво.

Прогресивно ограничувачките привилегии за физички пристап го контролираат пристапот до секое ниво. Чувствителните оперативни активности на ИС, сите активности поврзани со животниот циклус во процесот на сертификација, како што се автентикација, верификација и издавање, се случуваат во рамките на многу рестриктивни физички нивоа. За влез во секое ниво потребна е безконтактна картичка за пристап на вработениот. Физичкиот пристап автоматски се регистрира и се снима на видео. На непридружуван персонал, вклучувајќи вработени без овластување за пристап или посетители не им е дозволен влез во таквите обезбедени простори.

Системот за физичка безбедност вклучува нивоа за безбедност на управувањето со клучеви што служи за заштита на онлајн и офлајн складирање на единицата за криптографско потпишување (CSU) и материјалот

со клучеви. Во деловите што се користат за креирање и зачувување на криптографски материјал се спроведува двојна контрола, секоја преку истовремена употреба на картички за близина и биометрика. Онлајн CSU се заштитени со употреба на заклучени ормани. Офлајн CSU се заштитени со употреба на заклучени сефови, ормани и контејнери. Пристапот до CSU и материјалите за клучеви е ограничен во согласност со барањата за одделување на должностите на KIBS. Отворањето и затворањето на ормaните или контејнерите во овие нивоа се евидентираат за ревизорски цели.

Операциите на КИБС РК се заштитени со употреба на физички контроли за пристап што ги прави достапни само за соодветно овластени лица. Пристапот до безбедни делови на објектите бара употреба на картичка за ,,пристап" или ,,пропусница". Користењето картичка за пристап се евидентира од безбедносниот систем на објектот.

Дневниците за картичките за пристап и видео записите се прегледуваат редовно. КИБС безбедно ги складира сите отстранливи медиуми и хартија што содржат чувствителни информации со обичен текст, поврзани со неговите РК операции, во безбедни контејнери.

КИБС безбедно ги чува единиците за криптографско потпишување (CSU) што се користат за генерирање и зачувување на приватните клучеви на претплатниците за далечински потпис. Пристапот до просториите што се користат за складирање клучеви и активности за генерирање клучеви е контролиран и евидентиран од системот за картички за пристап. Дневниците за картичките за пристап и видео записите редовно се прегледуваат.

5.1.3. Електрична енергија и климатизација

Безбедните простории на КИБС се опремени со примарни и резервни:

- системи за електрична енергија кои обезбедуваат континуирано и непрекинато напојување со електрична енергија и
- системи за греење/ вентилација/ климатизација, со кои се контролира температурата и релативната влажност.

5.1.4. Изложеност на вода

КИБС има преземено разумни мерки на претпазливост со цел да се минимизира негативното влијание од изложување на своите системи на вода.

5.1.5. Превенција од пожар и противпожарна заштита

КИБС ги има преземено сите разумни мерки за спречување и гасење пожар или други штетни изложувања на оган или чад. Превентивните и заштитните мерки се дизајнирани за да бидат во согласност со локалните регулативи за сигурност од пожар.

5.1.6. Складирање на медиумите

Сите медиуми кои содржат продукциски софтвери и податоци од ревизија, архивски информации или резервни копии на податоци се складирани во рамките на просториите на КИБС и во безбедни објекти надвор од деловните простории со соодветни контроли за физички и логички пристап, дизајнирани на начин да го ограничат пристапот само на овластениот персонал и да ги заштитат тие медиуми од евентуални штети (пр. вода, оган).

5.1.7. Отстранување отпад

Чувствителните документи и материјали се уништуваат со сечкање пред да се исфрлат. Медиумите што се користат за чување или пренос на чувствителни податоци се прават нечитливи пред да се исфрлат. Криптографските уреди физички се уништуваат или онеспособуваат во согласност со инструкциите на производителот пред да се исфрлат. Останатиот отпад се исфрла во согласност со нормалните барања на КИБС за исфрлање отпад.

5.1.8. Резервни копии (бекап) надвор од деловните простории

КИБС врши рутински креирање на резервни копии (бекап) на клучните системски податоци, податоците од ревизорски траги и другите чувствителни информации. Медиумите со резервни копии што се чуваат

надвор од деловните простории се складираат на физички безбеден начин користејќи капацитет за опоравување по кризни ситуации надвор од деловните простории, во согласност со ,,План за непрекинатост на работењето" на КИБС.

5.2. Процедурални контроли

5.2.1. Доверливи улоги

Доверливи лица се сите вработени кои имаат пристап до или ја контролираат автентикацијата или криптографските операции кои можат материјално да влијаат на:

- потврдувањето на информациите во барањата за сертификати,
- прифаќањето, одбивањето или друг вид на обработка на барањата за сертификати, барањата за поништување, барањата за обновување, или информациите за регистрација,
- издавањето или поништувањето на сертификати, вклучително и персоналот кој има пристап до ограничените делови од складиштето,
- постапувањето со информациите или барањата на претплатниците.

Како доверливи лица се сметаат, но не е ограничено на:

- персонал кои дава услуги на клиентите,
- РК/ЛРК персонал,
- персонал кој работи на криптографски деловни операции,
- персонал кој е задолжен за сигурност,
- интерни ревизори,
- персонал задолжен за администрација на системот,
- назначен технички персонал, и
- извршни раководни лица кои се назначени да управуваат со доверливоста на инфраструктурата.

КИБС ги смета категориите на вработени лица наведени во овој дел за доверливи лица кои имаат доверливи позиции. Вработените кои сакаат да станат доверливи лица со добивање на доверливи позиции мораат успешно да ги исполнат барањата за скрининг наведени во овие CP/CPS.

Функциите и должностите што ги вршат лицата со доверливи улоги се распоредени така што едно лице не може да ги избегне безбедносните мерки или да ја наруши сигурноста и доверливоста на PKI операциите. Високиот менаџмент ги назначува доверливите улоги. Списокот на персонал назначен за доверливи улоги се одржува и разгледува на годишно ниво.

Лицата под договор и консултантите кои имаат пристап или ја контролираат автентикацијата и криптографските операции, може да ги извршуваат овие операции само во придружба и со директен надзор од доверливи лица во текот на целото време.

5.2.2. Број на лица потребни за една работна задача

КИБС воспостави, одржува и применува ригорозни контролни процедури за да обезбеди издвојување на должностите врз основа на работните одговорности и согласно потребите за да обезбеди повеќе доверливи лица да ги извршуваат чувствителните задачи.

Политиката и контролните процедури треба да обезбедат одвојување на должностите врз основа на работните одговорности. Најчувствителните задачи, како пристап до и управување со криптографскиот хардвер (криптографска единица за потпишување или CSU) на ИС и поврзаниот материјал со клучеви бараат ангажирање на повеќе доверливи лица.

Овие внатрешни контролни процедури се дизајнирани за да обезбедат дека потребни се минимум две доверливи лица за физички или логички пристап до уредот. Пристапот до криптографскиот хардвер на ИС строго се спроведува од повеќе доверливи лица во текот на целиот негов животен циклус, почнувајќи од приемот и проверката до неговото финално логичко и/или физичко уништување. Откако модулот ќе се активира со оперативните клучеви, се спроведуваат понатамошните контроли за да се одржи поделена контрола на логички и физички пристап до уредот. Лицата со физички пристап до модулите не поседуваат „тајни удели" и обратно.

Проверката и издавањето на квалификувани сертификати наложува потреба од најмалку 2 доверливи лица, или комбинација од барем едно доверливо лице и процес за автоматска проверка и издавање.

5.2.3. Идентификација и автентикација за секоја улога

За сите вработените лица кои треба да станат доверливи лица, се врши проверка на идентитетот со нивно лично (физичко) присуство пред доверливите лица на КИБС, кои работат во одделот за човечки ресурси или ги вршат безбедносните функции и проверка на признаени форми на идентификација (на пример, пасош или лична карта). Идентитетот потоа се потврдува преку процедурите на проверка на биографијата, на начин уреден во делот 5.3.2.

КИБС потврдува дека персоналот го добил доверливиот статус и на тој персонал се дава одобрување од одделот пред да им бидат:

- издадени уреди за влез со дозволен пристап во потребните простории, и
- издадени електронски овластувања за пристап и за изведување специфични функции во КИБС, РК или други системи на информатичка технологија.

КИБС воведе систем за контрола на пристап, кој ги идентификува овластувањата и ги регистрира сите корисници на информатичкиот систем на КИБС на доверлив начин.

Корисничките сметки се креираат за персонал со специфични улоги за кои е потребен пристап до предметниот систем. Сите корисници мора да се најават со соодветната сметка, а административните команди се достапни само со експлицитно одобрение и ревизија на извршувањето. Дозволи за системот со датотеки и други карактеристики достапни во моделот на безбедносниот оперативен систем се користат за да се спречи секоја друга употреба.

- Корисничките сметки се заклучуваат веднаш штом промената на улогата ќе го наложи тоа. Правилата за пристап се ревидираат годишно.

5.2.4. Работни улоги за кои е потребно одвојување на должностите

Работни позиции, за кои е потребно одвојување на должностите, вклучуваат, но не се ограничени на тоа извршување/спроведување:

- валидација на информациите во барањата за сертификати,
- прифаќање, одбивање или друг вид на обработка на барањата за сертификати, барањата за поништување, или за обновување, или информации за регистрација;
- издавање или поништување на сертификати, вклучувајќи ги и лицата кои имаат пристап до ограничените делови од просторот за складирање;
- генерирање, издавање и уништување на ИС сертификати;
- вчитување на ИС во производствената средина;.
- пристап до далечинското QSCD;
- функции за бекап, снимање и водење евиденција;
- функции за ревизија, преглед, надзор или усогласување;
- за да се постигне ова одвојување на должностите, КИБС назначува поединци за доверливи улоги, ограничувајќи го вработениот да презема повеќе улоги и со тоа да спречи вработен да има повеќе од еден идентитет.

5.3. Контроли на персоналот

Вработените лица кои бараат да станат доверливи лица мораат да презентираат доказ за биографските податоци, квалификациите и искуството кои се потребни за извршување на нивните идни работни задачи компетентно и на задоволителен начин како и доказ за какви било владини дозволи, доколку ги има, неопходни за извршување услуги за сертификација според договори на Владата. Проверки на биографските податоци за лицата на доверливи работни позиции, се вршат најмалку на 5 години.

5.3.1. Барања за квалификации, искуство и дозволи

КИБС бара од вработените кои сакаат да станат доверливи лица да презентираат доказ за неопходните биографски податоци, квалификациите и искуството што им се потребни за целосно и задоволително да

ги извршуваат своите идни работни обврски како што е наведено во договорот за вработување, описот на работното место и документите за улоги и одговорности, како и доказ за какви било владини дозволи, доколку ги има, потребни за извршување на услуги за сертификација според договори на Владата, пред тие да извршат какви било оперативни или безбедносни функции.

Договорите за вработување потпишани од вработените во КИБС ги предвидуваат следниве обврски:

- Да ја чуваат тајноста на доверливите информации што ќе им станат познати за време на нивното работење,
- Да се спречи поседување на деловни интереси во некоја компанија, што може да влијае на нивната проценка при обезбедување на услугата и да се осигура дека тие не биле казнети за намерно сторено кривично дело.

Целиот персонал со доверливи улоги да нема било какви интереси што можат да влијаат на нивната непристрасност во врска со операциите на КИБС.

5.3.2. Процедури за проверка на биографијата

КИБС, пред да вработи лице на доверлива позиција, спроведува проверка на биографијата, која вклучува:

- Верификација на идентитет,
- Проверка на претходните вработувања и професионални референци, (доколку постојат),
- Потврда на највисокиот или најрелевантниот степен на образование што е стекнат,
- Потврда за неосудуваност,
- Проверка на финансиската евиденција.

Онаму каде што некои од овие предуслови наведени во овој дел не можат да бидат задоволени заради забрани или ограничувања од локалниот закон или поради други околности, КИБС ќе примени алтернативни техники дозволени со закон, кои ќе обезбедат суштествено слични информации.

Фактите од проверката на биографијата што можат да се сметаат како основа за одбивање на кандидатите за доверливи позиции или за преземање дејствија против веќе вработено доверливо лице главно вклучуваат, (но не се ограничени) на следново:

- Погрешно претставување од страна на кандидатот или доверливото лице,
- Крајно неповолни професионални референци,
- Одредени кривични пресуди,
- Индикации за отсуство на финансиска одговорност.

Извештаите кои содржат такви информации се разгледуваат од страна на одделот за човечки ресурси и сигурност, кои ги определуваат понатамошните насоки на делување земајќи ги превид видот, големината и зачестеноста на однесувањето што се констатирани со проверката на биографијата. Тие дејствија може да вклучат мерки до откажување на понудата за вработување на кандидати за доверливи позиции или до прекин на работниот однос на постојното доверливо лице.

Користењето на информациите утврдени со проверката на биографијата за преземање на одредени активности подлежи на важечките закони.

5.3.3. Неопходна обука

КИБС обезбедува обука на вработените што е им е потребна за да ги извршуваат своите работни обврски компетентно и на задоволителен начин веднаш по вработувањето или обуката ја врши на самото работно место. КИБС води евиденција за таквите обуки. На одредени временски периоди, КИБС ги ревидира и надградува своите програми за обука според потребите.

Програмите на КИБС за обука се изработуваат според индивидуалните работни одговорности и како релевантно го вклучуваат следново:

- Основни PKI концепти,
- Работни одговорности,
- Безбедносни и оперативни политики и процедури на КИБС,

- Користење и оперирање со хардверот и софтверот што е дистрибуиран,
- Пријавување и справување со инциденти и компромитирања,
- Процедури на опоравување од кризни состојби и континуитет на деловното работење.

5.3.4. Услови и период на повторна обука

КИБС обезбедува обновена и осовременета обука за својот персонал до онаа мера и со онаа периодичност што е потребна за да го одржи потребното ниво на стручност за извршување на работните задачи компетентно и на задоволителен начин.

5.3.5. Период и редослед на ротирање на работните места

Не се спроведува ротирање.

5.3.6. Санкции за неовластени дејствија

За вработени и агенти кои не се придржуваат кон овие CP/CPS, вршат неовластени дејствија и други прекршувања на политиките и процедурите на КИБС се преземаат соодветни дисциплински мерки. Дисциплинските активности може да опфатат различни мерки сè до прекин на работниот однос и соодветствуваат на зачестеноста и сериозноста на неовластените дејствија.

5.3.7. Предуслови за независни лица по договор

Само во одредени околности може да се користат самостојни лица по договор или консултанти за да се пополнат доверливи позиции. Таквите лица по договор или консултанти подлежат на истите функционални и безбедносни критериуми коишто важат за вработените на КИБС на слична позиција.

На независните лица по договор и на консултантите кои не ги завршиле или поминале процедурите на проверка на биографски податоци наведени во делот 5.3.2, пристапот до безбедните простори на КИБС им е дозволен само доколку се придружувани и постојано директно се надгледувани од страна на доверливо лице.

5.3.8. Документација што му се обезбедува на персоналот

КИБС на својот персонал ја обезбедува потребната обука, како и документацијата што им е потребна за да ги извршуваат своите работни обврски компетентно и на задоволителен начин, вклучувајќи примерок од овие CP / CPS и друга техничка и оперативна документација, потребна за одржување на интегритетот на работењето на КИБС ИС. На вработените им се дава пристап и до информации за внатрешни системи и документација за безбедност, процедури за верификација на идентитет и други релевантни информации.

5.4. Процедури за ревизорска трага (Audit logging Procedures)

5.4.1. Видови настани што се евидентираат

КИБС обезбедува сите релевантни информации во врска со работењето со доверливите услуги да се евидентираат заради обезбедување докази наменети за правни постапки. Овие информации ги вклучуваат архивските записи што се потребни за докажување на валидноста на работењето со доверливата услуга.
КИБС ги евидентира, мануелно или автоматски, следниве значајни настани:

- Настани од управувањето со животниот циклус на сертификатите и клучевите на ИС, вклучувајќи:
  - Генерирање клучеви, резервна копија, складирање, обновување, архивирање и уништување,
  - Измени на ИС деталите или клучевите,
  - Настани поврзани со управување на животниот циклус на криптографските уреди.
- Настани од управувањето со животниот циклус на претплатничките сертификати и клучевите, кои вклучуваат:
  - Барања за издавање сертификати, издавање, обновување нов пар клучеви и поништување,
  - Генерирање клуч, правење резервна копија (бекап), складирање, опоравување, архивирање и уништување,

- Успешна или неуспешна обработка на барањата,
- Промени во политиките за креирање сертификати,
- Генерирање и издавање сертификати и CRL.

– Настани за доверливи вработени, вклучително:

- Обиди за најавување и одјавување,
- Обиди за креирање, отстранување, поставување лозинки или промена на системските привилегии на сите привилегирани корисници,
- Промени во персоналот.

– Сите важни настани поврзани со сигурноста, кои вклучуваат:

- Успешни или неуспешни обиди за пристап до PKI системот,
- Стартување и исклучување на системи и апликации,
- Поседување на активациски податоци за операциите на приватен клуч на ИС,
- PKI и безбедносни системски активности спроведени од страна на персоналот на КИБС,
- Безбедносно чувствителни документи или евиденција што се прочитани, напишани или избришани,
- Промени на правилата во Политиката за безбедност,
- Испади на системот, откажување на хардверот и други аномалии,
- Активности поврзани со огнени зидови (firewall) и мрежниот насочувач (рутер),
- Влез/излез на посетители во просториите на ИС,
- Влез/излез за пристап до далечинското QSCD.

Записите во дневникот за евиденција ги вклучуваат следниве елементи:

– Датум и време на внесување,
– Серија или редоследен број на записи,
– Идентитет на ентитетот кој запишува во дневникот,
– Вид на запис.

Информации за барањето за сертификат од дневникот на КИБС РК и ЛРК, вклучително:

– Вид на документ (и) за идентификација презентиран од барателот на сертификат;
– Евиденција на единствени податоци за идентификација, броеви или нивна комбинација (на пример, број лична карта на барателот на сертификат) на документи за идентификација, доколку е применливо. Локација на складирање на копии од барањата, и документи за идентификација за квалификувани сертификати,
– Сите посебни избори во барањето за сертификат,
– Идентитет на субјектот кој го прифаќа барањето и во случај на квалификувани е-печати, идентитет на физичкото лице кое го застапува правното лица на кого му се дава квалификуваниот сертификат за електронски печат,
– Метод што се користи за потврдување (валидација) на документи за идентификација, доколку ги има,
– Име на ИС која прима или РК или ЛРК која доставува, доколку е применливо.

5.4.2. Интервал на преглед на ревизорски траги

Системите на КИБС постојано се следат за да обезбедат сигнали во реално време за значајни безбедносни и оперативни настани за преглед од страна на назначениот персонал за безбедност на системот. Месечните прегледи на ревизорските траги вклучуваат проверка дека евиденцијата не била менувана и темелно истражување на сите предупредувања или неправилности откриени во евиденцијата. Активностите преземени врз основа на прегледите на ревизорските траги , исто така, се документираат.

5.4.3. Период на зачувување на ревизорските траги

Евиденцијата од ревизија се задржува најмалку два (2) месеци по обработката и потоа се архивира во согласност со дел 5.5.

Физичката или дигиталната архивска евиденција за барањата за сертификати, информациите за регистрација и барањата или барањата за поништување се чуваат десет (10) години откако ќе престана да важи кој било сертификат заснован на оваа евиденција.

Во случај на прекинување на ИС, ревизорските траги и архивската евиденција на КИБС се чуваат и се достапни до гореспоменатиот рок за чување, во согласност со дел 5.8.

Лицата кои ги отстрануваат ревизорските траги од системите на КИБС ИС се различни од лицата кои ги контролираат клучевите за потпис.

5.4.4. Заштита на ревизорските траги

Ревизорските траги се заштитуваат со електронски систем за ревизорски траги, кој вклучува механизми за заштита на евиденцијата од неовластено прегледување, изменување, бришење или друго интервенирање.

5.4.5. Процедури за правење резерви копии (бекап) на ревизорските траги

Инкрементална резервна копија (на промените) на ревизорските траги се прави секојдневно, а целосна резервна копија на ревизорските траги се прави неделно.

5.4.6. Систем за зачувување на ревизорска трага (интерен наспроти екстерен)

Автоматизираните ревизорски податоци се генерираат и се зачувуваат на ниво на апликација, мрежа и оперативен систем. Рачно генерираните податоци за ревизија ги бележи персоналот на КИБС со доверливи улоги.

5.4.7. Известување до субјектот што го предизвикал настанот

Кога некој настан се евидентира од страна на системот за ревизорска евиденција, не е потребно известување на лицето, организацијата, уредот или апликацијата што го предизвикала тој настан, освен доколку таквото известување е задолжително според законот.

Доколку евиденцијата во врска со функционирањето на услугите е потребна заради обезбедување докази за правилно функционирање на услугите и за целите на правните постапки, таа се става на располагање на правните органи и/или лицата кои имаат законско право на пристап.

5.4.8. Проценка за ранливост

Настаните во процесот на ревизија се евидентираат делумно и заради надгледување на ранливоста на системот. Проценките на ранливост се извршуваат и прегледуваат на годишно ниво за да се идентификува и да се проценат разумно предвидливи интерни и екстерни закани што може да резултираат со неовластен пристап.

КИБС, исто така, рутински проценува дали политиките, процедурите, информатичките системи, технологијата и другите постапки што ги има воспоставено се доволни за контрола на ваквите ризици. Проценката на ранливост и проценката на ризик се влезни информации во годишната ревизија за проценка на сообразност на КИБС.

5.5. Архивирање на записите

5.5.1. Видови записи кои се архивираат

КИБС ИС ги архивира:

- Сите податоци од ревизијата прибрани во согласност со условите од дел 5.4.,
- Информациите за барањата за сертификати,
- Документацијата приложена кон барањата за сертификати,
- Информациите за животниот циклус на сертификатот,
- Одобрувањето и одбивањето на барањето за поништување,
- CP и CP/CPS верзии,
- Извештаите од ревизија на проценката за усогласеност,
- КИБС сертифицирање,

- Назначувањето поединец за доверлива улога.

5.5.2. Период на чување во архивата

Периодот на чување во архивата е опишан во дел 5.4.3.

5.5.3. Заштита на архивата

КИБС ја заштитува архивата на тој начин, што само овластени доверливи лица имаат можност да добијат пристап до неа. Архивата е заштитена од неовластено прегледување, изменување, бришење или друг вид на интервенција во рамките на доверливиот систем. Медиумот на кој се чуваат архивските податоци и барањата што се потребни за обработка на архивските податоци се одржува со цел да се обезбеди пристап до архивските податоци во временскиот период наведен во овие CP/CPS.

5.5.4. Процедури на правење резервни копии (бекап) на архивата

КИБС прави резервни копии на промените во електронските архиви на дневна основа, а целосни резервни копии на неделна основа. Електронските копии од документацијата во хартиена форма се чуваат во безбедни простории надвор од деловните простории на КИБС.

5.5.5. Барања за временски печат на документацијата

Сертификатите, CRL и другите записи за поништување содржат информации за времето и датумот. Овие информации за времето не се криптографски базирани.

5.5.6. Систем за архивирање

КИБС користи архивирање во интерниот архивски систем.

5.5.7. Процедури за добивање и верификување на архивските податоци

Само овластени доверливи лица можат да добијат пристап до архивата. Интегритетот на информациите се верификува кога ќе се обноват.

Доколку евиденцијата во врска со функционирањето на услугите е потребна заради обезбедување докази за правилно функционирање на услугите и за целите на правните постапки, тие се стават на располагање на правните органи и / или лицата кои имаат законско право на пристап.

5.6. Промена на клучеви

Парот клучеви на КИБС ИС се повлекува од употреба на крајот од нивниот максимален животен циклус, согласно овие CP/CPS. Сертификатите на КИБС ИС можат да се обноват, доколку кумулативниот животен циклус на ИС парот клучеви, не го надмине максималниот животен циклус на ИС парот клучеви. Доколку е неопходно, се генерира нов пар ИС клучеви, на пример, за да се заменат ИС паровите клучеви што се повлекуваат, за да се надополнат постојните, активни парови на клучеви и за да се поддржат нови услуги.

Кон крајот на животниот циклус на приватниот клуч на ИС, КИБС престанува да го користи ИС приватниот клуч што истекува и го користи стариот приватен клуч само за да потпише CRL и OCSP респондер сертификати. Во функција се става нов ИС пар клучеви за потпишување и сите последователно издадени сертификати и CRL се потпишуваат со новиот приватен клуч за потпишување. И старите и новите пар клучеви може да бидат истовремено активни. Овој процес на менување клучеви помага да се минимизираат сите негативни ефекти од истекот на ИС сертификатот. Соодветниот нов сертификат за јавен клуч на ИС им се обезбедува на претплатниците и на засегнатите страни преку методите за испорака, детално наведени во дел 6.1.4.

Онаму каде КИБС вкрстено сертифицирал друг ИС кој е во процес на обновување клучеви, КИБС добива нов ИС јавен клуч (PKCS # 10) или нов ИС сертификат од другиот ИС и дистрибуира нов ИС вкрстен сертификат следејќи ги постапките опишани погоре.

5.7. Опоравување од компромитирање и од кризни ситуации

5.7.1. Процедури за справување со инциденти и компромитирање

Резервните копии на следниве ИС информации се чуваат во простории надвор од локацијата на деловните простории и се расположливи во случај на компромитирање и кризни ситуации и тоа: податоци од барањата за сертификати, податоци од ревизијата, евиденција од базата на податоци за сите издадени сертификати. Резервната копија на ИС приватните клучеви се генерира и се одржува во согласност со овие CP/CPS.

5.7.2. Компромитирани компјутерски ресурси, софтвер и/или податоци

Во случај на корумпирање на компјутерските ресурси, софтверот и/или податоците, таквиот настан се пријавува во одделот за сигурност на КИБС или на ADACOM и се активираат процедурите за справување со инциденти. Таквите процедури претпоставуваат соодветна ескалација, истражување на инцидентот и одговор на инцидентот. Доколку е неопходно, ќе се применат процедурите за справување со компромитиран клуч или кризна ситуација.

5.7.3. Процедури при компромитирање на приватниот клуч на ентитетот

По претпоставено или познато компромитирање на КИБС ИС, КИБС го следи планот на активности како што е опишано во постапката за управување со безбедносни инциденти.

Доколку е потребно поништување на ИС сертификат, се изведуваат следниве процедури:

- За статусот на поништениот сертификат се информираат засегнатите страни преку КИБС складиштето, во согласност со дел 4.9.9 ,
- Се вложуваат комерцијално разумни напори за да се достави дополнително известување за поништувањето до сите засегнати учесници, и
- ИС генерира нов пар клучеви во согласност со дел 5.6 , освен кога се укинува ИС во согласност со дел 5.8.
- Овој став е применлив и во случај кога PKI алгоритмите или придружните параметри ќе станат недоволни за неговата преостаната наменета употреба.

5.7.4. Способност за продолжување на деловните активности по кризна ситуација

КИБС одржува План за деловен континуитет (ПДК) за воспоставување процедури за враќање на критичните деловни функции на КИБС по кризната ситуација.

За овој план утврдени се следниве цели:

- Да се зголеми ефикасноста на операциите во вонредни состојби преку утврден план кој се состои од следниве фази:
    - Фаза на известување / активирање за откривање и проценка на штетата и активирање на планот.
    - Фаза на закрепнување за враќање на привремените ИТ-операции и оправување по штетата направена на оригиналниот систем.
- Идентификација на активностите, ресурсите и процедурите потребни за извршување на функциите на КИБС ИС и сертификатот за време на подолги прекинувања на нормалното работење.
- Доделување одговорности на назначениот персонал на КИБС и давање насоки за враќање на постапките на КИБС за време на подолги периоди на прекин на нормалното работење.
- Обезбедување координација со другите вработени во КИБС кои ќе учествуваат во стратегиите за планирање на непредвидени ситуации. Обезбедување координација со надворешните точки на контакт и снабдувачите кои ќе учествуваат во стратегиите за вонредно планирање.

КИБС има можност да ги врати или обнови основните операции во рок од дваесет и четири (24) часа по кризна ситуација, во најмала мера со поддршка на следниве функции:

- Издавање сертификат,
- Поништување сертификат,
- Објавување на информации за поништување.

ADACOM одржува дуплиран хардвер и резервни копии од софтверот за својот ИС и инфраструктурниот системски софтвер во својот објект за закрепнување по кризни ситуации. Покрај тоа, се прави резервна копија од ИС приватните клучеви и тие се одржуваат заради опоравување, во согласност со Дел 6.2.4.

5.8. Прекин на дејноста на ИС или РК

Прекин на дејноста на ИС се врши:

- со одлука на Бордот на директори на КИБС,
- со одлука на органот кој врши надзор на снабдувањето услуга,
- со судска одлука,
- по ликвидација или прекинување со работењето на КИБС.

КИБС гарантира дека потенцијалните дисконтинуитети за претплатниците и засегнатите страни како резултат на прекинот на услугите на КИБС се минимизирани, а особено, тој обезбедува континуирано одржување на информациите, потребни за да се верификува исправноста на доверливите услуги.

Доколку е потребно КИБС ИС да ја прекине работата, КИБС ќе вложи економско разумни напори однапред да ги извести претплатниците, засегнатите страни и другите засегнати субјекти за ваквиот прекин на активноста пред престанокот на ИС. Тогаш кога е потребен престанок на ИС и кога е применливо, КИБС ќе ги пренесе своите обврски на друг TSP и ќе го активира документираниот „План за престанок на КИБС“ за да се минимизира дисконтинуитет за клиентите, претплатниците и засегнатите страни. Овој план за престанок се однесува на следново, како што е применливо:

- Доставување известување до страните погодени од престанокот, како што се претплатници, засегнати страни и клиенти, информирајќи ги за статусот на ИС,
- Поднесување на трошоците за такво известување,
- Поништување на сертификатот издаден на ИС од КИБС,
- Чување на архивите и документацијата на ИС во периодот предвиден со овие CP/CPS,
- Продолжување на услугите за поддршка на претплатници и клиенти,
- Продолжување на услугите на поништување, како што се издавање на CRL или одржување на услуги за онлајн проверка на статусот,
- Поништување на неистечените непоништени сертификати на претплатници - крајни корисници и издавачки ИС, доколку е потребно,
- Рефундирање (доколку е потребно) на претплатници чиишто неистечени непоништени сертификати се поништуваат според планот за престанок или одредба, или алтернативно, издавање сертификати како замена од страна на ИС што ќе ја наследи дејноста,
- Дислокација на приватниот клуч на ИС, вклучувајќи ја резервната копија од приватниот клуч и хардверските токени што го содржат таквиот приватен клуч,
- Одредби потребни за пренесување на услугите на ИС на ИС наследник, кога е можно,
- Известување до релевантните органи, како што се надзорни тела,
- Пренесување на обврските на сигурна страна за одржување на сите информации потребни за да се обезбедат докази за функционирањето на доверливите услуги за разумен временски период, освен ако може да се докаже дека КИБС не поседува такви информации,
- Доставување на архивите и евиденцијата на КИБС ИС на друг договорен давател на услуги за сертифицирање на квалификувани сертификати, за временските периоди што се бараат според законот.

По престанокот на работењето на КИБС ИС, или престанокот на услугите на РК, поради некоја причина, сите договори што доделуваат дел од TSP одговорностите на трети лица, односно одговорностите за валидација на претплатникот, доделени со аутсорсинг на Регистрационата канцеларија, автоматски истекуваат. За таа цел, трети лица ќе обезбедат пренесување на евиденцијата и документите поврзани со доделените одговорности, во согласност со важечкиот закон..

6. КОНТРОЛИ НА ТЕХНИЧКАТА СИГУРНОСТ

6.1. Генерирање и инсталирање на пар клучеви

6.1.1. Генерирање на пар клучеви

Генерирањето на ИС пар клучеви се изведува од повеќе однапред избрани, обучени и доверливи лица со употреба на сигурни системи и процеси кои обезбедуваат безбедност и потребна криптографска јачина за генерираните клучеви. Криптографските модули што се користат за генерирање клучеви ги исполнуваат барањата на FIPS 140-2 ниво 3.

Сите ИС парови клучеви се генерираат со претходно планирана церемонија на генерирање клучеви, во согласност со условите на Референтниот водич за церемонија на генерирање клучеви и Корисничкиот водич за алатки за управување со ИС клучеви. Активностите што се изведуваат при секоја церемонија на генерирање клучеви се документираат, датираат и потпишуваат од сите лицата кои се вклучени. Оваа документација се чува со цел за ревизија и пребарување во временски период што се смета за соодветен од страна на Управата на КИБС.

Генерирање на пар клучеви на претплатници - крајни корисници главно го врши операторот на КИБС, со помош на софтверот за управување со картички, во присуство на претплатникот, на QSCD сертифициран криптографски модул, усогласен со барањата на регулативата eIDAS.

За далечински квалификувани сертификати, генерирањето клучеви, нивното складирање и последователна употреба се извршува од КИБС користејќи исклучиво уреди сертифицирани специјално во согласност со важечките барања од член 30.3 од eIDAS и, на тој начин се вклучени во списокот на квалификувани средства одржувани од Европската комисија, во согласност со членовите 30, 31 и 39 од eIDAS. Горенаведените средства чија цел е да бидат управувани во име на потписникот од страна на QTSP, може да бидат уредно управувани од трет QTSP, во согласност со регулативата eIDAS (ЕУ) 910/2014.

6.1.2. Доставување на приватниот клуч на претплатникот

Кога парот клучеви за претплатникот - краен корисник се генерира на QSCD од страна на претплатникот, не се применува доставување на приватниот клуч на претплатникот.

Кога паровите клучеви на претплатникот претходно се генерирани од КИБС на QSCD, таквиот уред се доставува до претплатникот со користење на комерцијална услуга за испорака преку регистрирана пошта. Податоците потребни за активирање на уредот се доставуваат до претплатникот со испорака преку алтернативни канали. Дистрибуцијата на ваквите уреди ја следи КИБС.

Кога претплатничкиот пар клучеви се генерира на далечинско QSCD од страна на претплатникот, доставувањето на приватниот клуч до претплатникот се врши во далечинското QSCD.

6.1.3. Доставување на јавниот клуч на Издавачот на сертификати

Претплатниците го доставуваат својот јавен клуч до КИБС за да биде електронски сертифициран со користење на PKCS#10 Барање за потпишување сертификат (Certificate Signing Request - CSR) или друг дигитално потпишан пакет во сесија обезбедена со протоколот Secure Sockets Layer (SSL). Ова барање не се применува кога парот клучеви на претплатникот претходно се генерирани од КИБС.

6.1.4. Доставување на ИС јавниот клуч на засегнатите страни

КИБС ги става ИС коренските и издавачките сертификати на располагање на претплатниците и засегнатите страни преку своето складиште. По издавањето на сертификатот, КИБС вообичаено им обезбедува целосен синџир на сертификати (вклучувајќи издавачки ИС и сите ИС во синџирот) на своите претплатници.

Претплатниците, за време на процесот на подигнување на сертификатот, автоматски го преземаат и го инсталираат на својот компјутер јавниот клуч на издавачкиот ИС. Во секој случај, доколку корисникот има потреба да го верификува и/или преземе јавниот клуч на ИС, тој може да го стори тоа пристапувајќи до веб-базираното складиште на КИБС: https://pki.kibstrust.com/repository.

6.1.5. Големина на клучевите

Парот клучеви треба да биде со должина доволна да ги спречи другите да го откријат приватниот клуч од парот клучеви со користење на криптоанализа за време на периодот кога се очекува да се користи тој пар

клучеви. Стандард на КИБС за минимална големина на клуч е користењето на пар клучеви еквивалентен според јачината на 4096 бита RSA за ИС и 2048 бита RSA за РК клучеви и сертификати на претплатникот.

Парот клучеви се генерираат со употреба на безбедни алгоритми и параметри засновани на тековните истражувања и индустриски стандарди следејќи ги препораките на ETSI TS 119 312, за потпишување сертификати, CRL и одговори на серверот за статус на сертификат.

Сите ИС сертификати и сертификати на претплатникот користат SHA-256 за дигитално потпишување хаш (hash) алгоритам.

6.1.6. Параметри за генерирање јавен клуч и проверка на квалитетот

Квалитетот на јавните клучеви е загарантиран со генерирање случајно избран безбеден број и вградено генерирање јавни клучеви. Паровите клучеви се генерираат со употреба на безбедни алгоритми и параметри засновани на тековните истражувања и индустриски стандарди следејќи ги препораките на ETSI TS 119 312.

6.1.7. Намени за употребата на клуч (според X.509 v3 Key Usage полето)

Види дел 7.

6.2. Заштита на приватниот клуч и инженерски контроли на криптографскиот модул

КИБС има имплементирано комбинација од физички, логички и процедурални контроли за да ја обезбеди сигурноста на приватните клучеви на КИБС ИС. Од претплатниците договорно се бара тие да ги преземат сите неопходни мерки на претпазливост за да спречат губење, откривање, измена или неовластена употреба на приватните клучеви.

6.2.1. Стандарди на криптографски модули и контроли

За генерирање на ИС пар клучеви и за складирање ИС приватен клуч, КИБС користи криптографски модули кои се сертифицирани за или ги задоволуваат барањата од FIPS 140-2 Ниво 3.

Приватните клучеви на претплатниците се генерираат на QSCD, во согласност со барањата за Регулативата eIDAS.

КИБС го следи статусот на сертификат на QSCD до крајот на периодот на важење на сертификатот поврзан со соодветното QSCD. Во случај на измена на статусот на сертификат на QSCD, КИБС ќе престане да издава сертификати на овие уреди.

6.2.2. Контрола на приватен клуч од повеќе лица (м од н)

КИБС користи сигурни услуги на ADACOM кои опфаќаат технички и процедурални механизми за кои е потребно учество на повеќе доверливи лица да ги изведуваат чувствителните ИС криптографски операции. ADACOM користи „Споделување на тајни удели" за да ги раздели податоците за активирање што се потребни за да се користи ИС приватниот клуч на одвоени делови наречени „Тајни удели", кои се чуваат од страна на обучени и доверливи лица наречени „Чувари на удели". За да се активира ИС приватниот клуч, складиран во модулот, потребен е минимален број на Тајни удели (м) од вкупниот број на Тајни удели креирани и дистрибуирани за конкретен криптографски модул (н).

Минималниот број удели што се потребни за да се потпише ИС сертификат е три (3). Тајните удели се заштитени во согласност со овие CP/CPS.

6.2.3. Давање на чување на приватниот клуч

Приватните клучеви на КИБС ИС и на крајните корисници не се даваат на чување кај трето лице.

6.2.4. Резервни копии (бекап) на приватен клуч

ADACOM прави резервни копии на приватните клучеви на КИБС ИС заради рутинско обновување и со цел за оправување по откажување на системот. Таквите клучеви се складираат во шифрирана форма во рамките на хардверски криптографски модули и слични уреди за складирање клучеви. Криптографските

модули што се користат за складирање на приватните клучеви на ИС ги задоволуваат критериумите на овие CP/CPS. Приватните клучеви на ИС се копираат на хардверски криптографски модули за резервни копии, во согласност со овие CP/CPS.

Модули што содржат резервни копии на приватни клучеви на ИС на главната локација подлежат на условите на овие CP/CPS. Модули што содржат копии за оporавување по откажување на системот за ИС приватните клучеви се предмет на условите на овие CP/CPS.

ADACOM не складира копии од приватните клучеви на РК. За складирање на приватните клучеви на претплатниците - крајни корисници, види дел 6.2.3 и дел 4.1.2.

6.2.5. Архивирање приватен клуч

По истекот на периодот на важност на КИБС ИС сертификатот, парот клучеви што е поврзан со сертификатот безбедно се зачувува одреден временски период од најмалку 5 години со користење на хардверски криптографски модули кои ги задоволуваат барањата на овие CP/CPS и CP/CPS на ADACOM. Овие ИС парови на клучеви не се користат за потпишување по истекување на нивната важност, освен ако ИС сертификатот не се обнови согласно овие CP/CPS.

КИБС не архивира копии од приватните клучеви на Претплатници.

6.2.6. Пренос на приватен клуч во или од криптографскиот модул

ADACOM генерира парови на клучеви за КИБС ИС на хардверските криптографски модули во кои клучевите ќе се користат. Покрај тоа, ADACOM прави копии на тие ИС парови на клучеви заради рутинско обновување и со цел за оporавување по откажување на системот. Во случаи кога ИС паровите клучеви се резервно складирани во друг хардверски криптографски модул, таквите парови на клучеви се пренесуваат помеѓу модулите во шифрирана форма.

6.2.7. Складирање на приватниот клуч на криптографски модул

Приватните клучеви кои се поставени на хардверски криптографски модули се складираат во шифрирана форма.

6.2.8. Метод на активирање на приватниот клуч

Сите КИБС претплатници ги заштитуваат податоците за активирање за нивните приватни клучеви од губење, кражба, изменување, неовластено откривање или неовластена употреба.

Приватните клучеви на претплатниците на локалното QSCD се заштитени со ПИН кодови. Следниве правила се применуваат:

- Претплатникот треба да го внесе ПИН-кодот на QSCD за секоја трансакција,
- Претплатникот е должен да го смени ПИН-кодот пред почетниот процес на регистрација,
- Во случај претплатникот да внесе погрешен ПИН-код 5 пати по ред, QSCD се блокира,
- ПИН може да се деблокира со користење на администраторскиот ПИН-код само во РК,
- Користењето на администраторскиот ПИН код ќе биде блокирано по 3 последователни неточни обиди,
- Корисникот може да ги смени ПИН-кодот.

Приватните клучеви на претплатникот на далечинското QSCD се заштитени со корисничко име, лозинка и OTP кодови. Следниве правила се применуваат:

- Претплатникот треба да ги внесе корисничкото име, лозинката и OTP-кодот на QSCD за секоја трансакција,
- Во случај претплатникот да внесе погрешно корисничко име, лозинка и OTP код 5 пати по ред, далечинската сметка на QSCD се заклучува,
- Далечинската сметка на QSCD не може да се ресетира со лозинка,
- Корисникот може да ја смени лозинката.

ИС приватниот клуч се активира онлајн со ограничен број Чувари на удели, како што е дефинирано во дел 6.2.2, доставувајќи ги нивните податоци за активирање (зачувани на безбедни медиуми). Откако

еднаш ќе се активира приватниот клуч, тој може да биде активен на неопределено време додека не се деактивира кога ИС ќе се исклучи од мрежата (офлајн). Слично на тоа, од минималниот број Чувари на удели ќе се бара да ги достават своите податоци за активирање со цел да го активираат ИС приватниот клуч кој е исклучен од мрежата (офлајн). Откако ќе се активира приватниот клуч, тој ќе биде активен само во еден наврат.

6.2.9. Метод на деактивирање на приватниот клуч

КИБС ИС приватните клучеви се деактивираат со исклучување на криптографскиот модул.

Приватните клучеви на претплатниците можат да се деактивираат после секоја операција, по одјавување од системот или со отстранување на локалното QSCD од системот или по одјавување на далечинското QSCD. Во секој случај, претплатниците имаат обврска на соодветен начин да го заштитуваат својот приватен клуч(клучеви) во согласност со овие CP/CPS.

6.2.10. Метод на уништување на приватниот клуч

Онаму каде што е потребно, КИБС ги уништува ИС приватните клучеви и приватните клучеви на претплатникот на начин кој обезбедува разумни уверувања дека нема остатоци од клучот кои би можеле да доведат до реконструкција на клучот. КИБС ја користи функцијата на анулирање на своите хардверски криптографски модули и други соодветни средства за да обезбеди со сигурност целосно уништување на ИС приватните клучеви. За време на уништување се прави евиденција од активностите.

Приватните клучеви на претплатниците на локално QSCD може да бидат уништени со физичко уништување или оштетување на QSCD.

6.2.11. Рангирање на криптографскиот модул

Види дел 6.2.1

6.3. Други аспекти на управување со пар клучеви

6.3.1. Архивирање на јавен клуч

Од КИБС ИС сертификатите се прават резервни копии и се архивираат според договорот со ADACOM за неговите доверливи услуги.

Од сертификатите на КИБС ИС, РК и на претплатниците - крајни корисници се прават резервни копии кои се архивираат како дел од рутинските процедури на резервно складирање на КИБС.

6.3.2. Оперативни периоди на сертификатите и периоди на користење на парот клучеви

Оперативниот период на сертификатот завршува по истекот на неговата важност или по неговото поништување. Оперативниот период за паровите клучеви е еднаков како и оперативниот период на сертификатите поврзани со нив, само што тие можат да продолжат да се користат за дешифрирање и верификување на потписот. Максималните оперативни периоди на сертификатите на КИБС, за сертификати издадени на или по датумот на стапување во сила на овие CP/CPS, се наведени во Табелата „Оперативни периоди на сертификати" подолу.

Сертификат издаден од:	Употреба на приватен клуч	Период на важност
Коренски ИС	Не е пропишано со одредба	Нормално до 20 години
Издавачки ИС	Не е пропишано со одредба	Нормално до 10 години
Сертификат со долготрајна важност	Не е пропишано со одредба	Нормално 1-3 години

Табела : Оперативен период на сертификатите

Покрај тоа, КИБС ИС престануваат да издаваат нови сертификати на соодветен датум (60 дена плус максималниот рок на важење на издадени сертификати) пред истекот на ИС сертификатот, така што ниту

еден сертификат, издаден од подреден ИС не истекува по истекот на сите надредени ИС сертификати. Времетраењето на сертификатите на претплатникот нема да го надмине животниот век на сертификатот за потпишување на ИС.

Претплатниците престануваат да ги користат сите парови клучеви откако ќе истечат периодите на употреба.

Ако алгоритамот или соодветната должина на клучот не понудат доволна сигурност за време на периодот на важење на сертификатот, засегнатиот сертификат ќе биде поништен и ќе биде иницирано барање за нов сертификат. Применливоста на криптографските алгоритми и параметри постојано се надгледува од страна на менаџментот на КИБС.

6.4. Податоци за активирање

6.4.1. Генерирање и инсталирање податоци за активирање

Податоците за активирање (Тајни удели) што се користат за заштита на HSM кој го содржи приватниот клуч на КИБС ИС се генерираат во согласност со условите од дел 6.2.2 и Референтниот водич за церемонија на генерирање клучеви. Креирањето и дистрибуирањето на Тајните удели се евидентира.

Користените податоци за активирање (ПИН) за заштита на локалното QSCD што ги содржи приватните клучеви на субјектот, се генерираат во согласност со упатството за употреба на QSCD.

- Кога паровите на клучеви на претплатникот претходно се генерирани од КИБС, податоците за активирање се доставуваат до претплатникот користејќи услуга за комерцијално регистрирана поштенска испорака.
- Кога паровите клучеви се генерираат од претплатникот, претходно дефинираните податоци за активирање мора да бидат изменети непосредно пред генерирањето на клучот. Користените податоци за активирање (корисничко име, лозинка и OTP-код) за заштита на далечинското QSCD, кои содржат приватни клучеви на субјектот, се генерираат во согласност со барањата за усогласеност на QSCD.

Користените податоци за активација (корисничко име, лозинка и код на OTP) за заштита на далечинското QSCD што содржи приватни клучеви на субјектот се генерираат во согласност со барањата за усогласеност на QSCD.

КИБС ќе пренесува податоци за активирање само преку соодветно заштитен канал и во време и место што се разликува од испораката на придружниот криптографски модул.

6.4.2. Заштита на податоците за активирање

КИБС ги штити податоците, користени за отклучување на приватните клучеви, од откривање со употреба на комбинација на контролни механизми. Од Чуварите на удели на КИБС се бара да ги чуваат своите тајни удели и тајните удели на далечинското QSCD и да потпишат договор со кој ќе ги прифатат одговорностите на Чувари на удели.

Персоналот и претплатниците на КИБС имаат упатства да користат силни лозинки и да ги штитат ПИН-от и лозинките. На претплатниците, исто така, им е наложено да ги запаметат своите податоци за активирање (ПИН, ПУК, корисничко име, лозинка, ОТП) и да не ги споделуваат со друг.

КИБС спроведува повеќефакторска автентикација за сите сметки што можат да причинат издавање сертификат или извршување функции на Регистрациона канцеларија, или функции на делегирано трето лице или имплементирање на технички контроли управувани од ИС за да се ограничи издавањето на сертификатот преку сметката на ограничена група однапред одобрени домени или адреси за е-пошта.

6.4.3. Други аспекти на податоците за активирање

6.4.3.1. Пренос на податоци за активирање

Кога се пренесуваат податоците за активирање на приватните клучеви, учесниците ќе го заштитат преносот користејќи методи кои штитат од загуба, кражба, модификација, неовластено откривање или неовластено користење на таквите приватни клучеви.

6.4.3.2. Уништување на податоци за активирање

Податоците за активирање на приватните клучеви на ИС се повлекуваат од употреба со применување на методи кои обезбедуваат заштита од губење, кражба, изменување, неовластено откривање или неовластена употреба на приватните клучеви заштитени со таквите податоци за активирање. Откако ќе помине периодот за чување на документација согласно дел 5.5.2, КИБС ги уништува податоците за активирање со бришење и преснимување преку нив или со физичко уништување.

6.5. Контроли за сигурност на компјутерите

КИБС ги изведува функциите на ИС и РК со користење на доверливи системи кои ги задоволуваат условите на Системот за управување со информатичка сигурност (ISMS).

6.5.1. Посебни технички услови за компјутерска сигурност

КИБС обезбедува системите кои го одржуваат ИС софтверот и податоците да бидат доверливи системи заштитени од неовластен пристап. Покрај тоа, КИБС го ограничува пристапот до продукцискиот сервер само на оние лица кои имаат оправдана деловна причина за таков пристап. Обичните корисници на апликации немаат пристап до продукциските сервери.

Продукцискатa мрежа на КИБС е логички одвоена од другите делови. Ова одвојување спречува пристап во мрежата, освен преку определени апликациски процеси. КИБС користи мрежни бариери (firewalls) за да ја заштити продукцискатa мрежа од интерни и екстерни упади и да ги ограничи видот и изворот на мрежни активности кои можат да влезат во продукциските системи.

Сите критични компоненти на софтверот се инсталираат и ажурираат само од доверливи извори. Исто така, постојат внатрешни процедури за заштита на интегритетот на компонентите на услуги за сертификација од вируси, малициозен и неовластен софтвер.

Персоналот на КИБС се автентицира пред да користи критични апликации поврзани со услугите. Корисничките сметки се креирани за персоналот со специфични улоги на кои им е потребен пристап до системот за кој станува збор. Дозволите за системот со датотеки и другите карактеристики достапни во моделот за сигурност на оперативниот систем се користат за да се спречи каква било друга употреба. Корисничките сметки се отстрануваат што е можно поскоро кога диктира промената на улогата. Правилата за пристап се ревидираат на годишно ниво.

КИБС бара употреба на лозинки кои имаат минимална должина на карактери и комбинација на алфанумерички и специјални знаци. КИБС бара лозинките да се менуваат на периодична основа.

Директниот пристап до базите на податоци на КИБС, кои ги поддржуваат операциите на КИБС ИС, е ограничен на доверливи лица во групата за производство на КИБС, кои имаат валидна деловна причина за ваквиот пристап.

Со компонентите на системот за услуги на сертификација на КИБС се управува во согласност со дефинирани процедури за управување со промените. Овие процедури вклучуваат тестирање на системот во изолирана околина за тестирање и услов дека промената мора да биде одобрена од службеникот за безбедност. Одобрението е документирано за понатамошно упатување.

Сите медиуми што содржат софтвер за производство и податоци, ревизија, архива или резервни копии од информации се чуваат во КИБС со соодветни физички и логички контроли за пристап. Медиумите што содржат чувствителни информации безбедно се сместуваат кога повеќе не се потребни.

Процедурите за управување со одговор на инциденти и ранливост се документирани во интерен документ. Системот за набљудување открива и алармира за абнормални активности на системот кои укажуваат на потенцијално нарушување на сигурноста, вклучително и упад во мрежата.

Документите во хартиена форма и материјалите со чувствителни информации се уништуваат пред отстранување. Медиумите што се користат за прибирање или пренесување на чувствителни информации се прават нечитливи пред да се отстранат.

РК мора да обезбедат дека системите што одржуваат софтвер и датотеки со податоци се сигурни системи, обезбедени од неовластен пристап и логично одделени од другите компоненти. РК мора да користат

заштитни (огнени) зидови (firewall) за да ја заштитат мрежата од внатрешен и надворешен упад и да ја ограничат природата и изворот на активности со кои може да се пристапи до ваквите системи и информации.

6.5.2. Рангирање на сигурноста на компјутерите

Не се применува.

6.6. Технички контроли на животниот циклус

6.6.1. Контроли на развојот на системот

Софтверот на КИБС поминува низ процедури за развој на безбедноста пред да биде објавен во производствената средина.

Развиени се и имплементирани се нови верзии на софтвер, во согласност со промената на постапката за управување.

6.6.2. Контроли за управување со сигурноста

КИБС има утврдено механизми и/или политики за контролирање и надгледување на конфигурацијата на своите ИС системи.

КИБС ги следи мрежните безбедносни упатства од дел 7.8 од ETSI EN 319 401. КИБС ги следи и безбедносните упатства на „Барања за безбедност на системот на мрежа и сертификати“ на CA/Browser Форумот.

По инсталирањето и подоцна на определени интервали, КИБС го проверува интегритетот на своите ИС системи. Во информатичкиот систем се користи само софтверот директно користен за извршување на задачите.

6.6.3. Безбедносни контроли на животниот циклус

Политиките и средствата на КИБС се разгледуваат во планирани интервали или кога се случуваат значителни промени за да се обезбеди нивна постојана соодветност, адекватност и ефективност.

Конфигурациите на системите на КИБС се проверуваат најмалку на годишно ниво за промени што ги кршат безбедносните политики на КИБС. Промените што имаат влијание врз нивото на обезбедена сигурност, ги разгледува службеникот за сигурност и ги одобрува менаџментот.

КИБС има процедури за обезбедување безбедносни софтверски делови за подобрување и отстранување грешки (закрпа/ patch) кои се применуваат на системот за сертификација во разумен временски период откако ќе станат достапни, но не подоцна од шест месеци по достапноста на безбедносните софтверски делови за подобрување и отстранување грешки (закрпа/patch). Причините за неприменување на безбедносни софтверски делови за подобрување и отстранување грешки ќе бидат документирани.

КИБС управува со регистрација на информатички средства и ги класифицира сите средства за информации во класи на сигурност според резултатите од редовната анализа на сигурноста во согласност со проценката на ризикот.

6.7. Контроли за сигурност на мрежата

КИБС ги изведува сите свои ИС и РК функции со користење на мрежи обезбедени во согласност со ISMS на КИБС со цел да спречи неовластен пристап и други злонамерни активности. КИБС го заштитува пренесувањето на чувствителни информации со користење на шифрирање и дигитални потписи.

Безбедносното ниво на внатрешната мрежа и надворешните врски постојано се следи за да се спречи целосно пристап до протоколите и услугите што не се потребни за функционирање на доверливите услуги.

КИБС периодично врши проценка на ранливост на јавните и приватните IP адреси во смисла на тестови за непробојност на системите за сертификација.

6.8. Временски жиг

Сертификатите, CRL и другите записи за поништување во базата на податоци содржат информации за времето и датумот.

Времето на системот на компјутерите на КИБС се ажурира со помош на Протоколот за мрежно време (NTP) кој ги синхронизира системските часовници најмалку еднаш на секој еден час.

7. ПРОФИЛИ НА СЕРТИФИКАТИ, РЕГИСТАР НА ПОНИШТЕНИ СЕРТИФИКАТИ (CRL) И НА ПРОТОКОЛ ЗА МОМЕНТАЛЕН СТАТУС НА СЕРТИФИКАТ (OCSP)

7.1. Профили на сертификати

Профилот на сертификатот е во согласност со X.509 v.3, IETF RFC 5280 и клаузулата 6.6.1 од ETSI EN 319 411-1.

7.1.1. Нумерирање верзии

Сите сертификати се X.509 верзија 3.

7.1.2. Екстензии на сертификати

Сите издадени сертификати вклучуваат екстензии кога се дефинираат за X.509v3 сертификатите.

Технички ограничените издавачки ИС сертификати опфаќаат екстензија за проширена употреба на клуч (EKU-Extended Key Usage) со наведување на сите проширени употреби на клучот за кој Издавачкиот ИС сертификат е овластен да издаде сертификати. **anyExtendedKeyUsage KeyPurposeId** не се појавува во EKU екстензијата на доверливите сертификати на КИБС.

Подолу е листата со екстензии користени од КИБС за секој тип на сертификат.

7.1.2.1. За коренски сертификати

Коренскиот сертификат е со име KIBSTrust Root CA G2 и тој е ист за издавачките сертификати од G2 и G3 генерација

Standard Extension	Field	Value
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**None**
Certificate Policies	Cert Policy ID	**1.3.6.1.4.1.15976.1.1**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.kibstrust.com/repository/cps**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Subject Key Identifier	Key Identifier	D4E9C6758EDBFEA63227A1C4DA9A0435AE4CBC58 *(This field contains the ID of the Certificate Holder's key.)*

7.1.2.2. За издавачки сертификати за електронски потписи

Имињата на ИС за електронски потписи се: KIBSTrust Issuing Qsig CA G2 и KIBSTrust Issuing Qsig CA G3

Standard Extension	Field	Value
Authority Key Identifier	Key Identifier	D4E9C6758EDBFEA63227A1C4DA9A0435AE4CBC58 *(This field contains the Subject Key Identifier of the issuer's Certificate.)*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	Cert Policy ID	**1.3.6.1.4.1.16305.1.1.5**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.kibstrust.com/repository/cps**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.kibstrust.com/rootg2.crl**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://pki.kibstrust.com/repository/certs/rootg2.crt**
Subject Key Identifier	Key Identifier	1FF18B5F563D2C9002089867B03B46259146C869 *(за G3)* 8A7748F3F4E03221EA9ED52BC9633D25A8CE24B5 *(за G2)* *(This field contains the ID of the Certificate Holder's key.)*
Subject Alternative Name	Directory Address	N/A *(за G3)* CN=PRIVATE-4096-11 *(за G2)* *(This field contains the Key identification)*

7.1.2.3. За издавачки сертификати за електронски печати

Имињата на ИС за електронски печати се: KIBSTrust Issuing Qseal CA G2 и KIBSTrust Issuing Qseal CA G3

Standard Extension	Field	Value
Authority Key Identifier	Key Identifier	D4E9C6758EDBFEA63227A1C4DA9A0435AE4CBC58 *(This field contains the Subject Key Identifier of the issuer's Certificate.)*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	Cert Policy ID	**1.3.6.1.4.1.16503.1.1.5**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.kibstrust.com/repository/cps**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.kibstrust.com/rootg2.crl**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**

	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://pki.kibstrust.com/repository/certs/rootg2.crt**
Subject Key Identifier	Key Identifier	E0B0E64BB05E5F53CF95DBFF17B747C4227432A9 *(за G3)* 264AABD306A8E9D270DA7104B631504785A9094D *(за G2)* *(This field contains the ID of the Certificate Holder's key.)*
Subject Alternative Name	Directory Address	N/A *(за G3)* CN=PRIVATE-4096-12 *(за G2)* *(This field contains the Key identification)*

7.1.2.4. За електронски потпис на физичко лице

Standard Extension	Field	Value
Authority Key Identifier	Key Identifier	1FF18B5F563D2C9002089867B03B46259146C869 *(за G3)* 8A7748F3F4E03221EA9ED52BC9633D25A8CE24B5 *(за G2)* *(This field contains the Subject Key Identifier of the issuer's Certificate.)*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.16305.1.1.5**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://www.kibstrust.com/repository/cps**
	Cert Policy ID	**0.4.0.194112.1.0** (QCP-n), или **0.4.0.194112.1.2** (QCP-n-qscd)
	Cert Policy ID	***За G3:*** **1.3.6.1.4.1.16305.1.2.5.4.2** (QCP-n), или **1.3.6.1.4.1.16305.1.2.5.4.3** (Local QSCD), или **1.3.6.1.4.1.16305.1.2.5.4.4** (Remote QSCD) ***За G2:*** **1.3.6.1.4.1.16305.1.2.5.1.2** (QCP-n), или **1.3.6.1.4.1.16305.1.2.5.1.3** (Local QSCD), или **1.3.6.1.4.1.16305.1.2.5.1.4** (Remote QSCD)
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl3.kibstrust.com/KIBSTrustIssuingQsigCAG3.crl** *(за G3)* **http://crl.kibstrust.com/qSigG2.crl** *(за G2)*
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate	**etsiQcsCompliance**	**0.4.0.1862.1.1**

Statements	**etsiQcsQcSSCD** (N/A for QCP-n)	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location (EN)	**https://www.kibstrust.com/repository/docs/PDSG3-EN.pdf** *(за G3)* **https://www.kibstrust.com/repository/docs/PDSG2-EN.pdf** *(за G2)*
	PDS Location (MK)	**https://www.kibstrust.com/repository/docs/PDSG3-MK.pdf** *(за G3)* **https://www.kibstrust.com/repository/docs/PDSG2-MK.pdf** *(за G2)*
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEsign	**0.4.0.1862.1.6.1**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	**http://ocsp3.kibstrust.com/** *(за G3)* **http://ocsp2.kibstrust.com/** *(за G2)*
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://cacerts.kibstrust.com/KIBSTrustIssuingQsigCAG3.crt** *(за G3)* **https://www.kibstrust.com/repository/certs/CA-qSig-G2.crt** *(за G2)*
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Enhanced Key Usage	Secure Email	**1.3.6.1.5.5.7.3.4**
	Client Authentication	**1.3.6.1.5.5.7.3.2**
Subject Alternative Name	RFC822 Name	*Email address of Subject*

7.1.2.5. За електронски потпис за физичко лице поврзано со правно лице

Standard Extension	Field	Value
Authority Key Identifier	Key Identifier	1FF18B5F563D2C9002089867B03B46259146C869 *(за G3)* 8A7748F3F4E03221EA9ED52BC9633D25A8CE24B *(за G2)* *(This field contains the Subject Key Identifier of the issuer's Certificate.)*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.16305.1.1.5**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://www.kibstrust.com/repository/cps**
	Cert Policy ID	**0.4.0.194112.1.0** (QCP-n), или **0.4.0.194112.1.2** (QCP-n-qscd)

	Cert Policy ID (N/A for QCP-n)	***За G3:*** **1.3.6.1.4.1.16305.1.2.5.4.2** (QCP-n), или **1.3.6.1.4.1.16305.1.2.5.4.3** (Local QSCD), или **1.3.6.1.4.1.16305.1.2.5.4.4** (Remote QSCD) ***За G2:*** **1.3.6.1.4.1.136305.1.2.5.1.2** (QCP-n), или **1.3.6.1.4.1.16305.1.2.5.1.3** (Local QSCD), или **1.3.6.1.4.1.16305.1.2.5.1.4** (Remote QSCD)
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl3.kibstrust.com/KIBSTrustIssuingQsigCAG3.crl** *(за G3)* **http://crl.kibstrust.com/qSigG2.crl** *(за G2)*
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD (N/A for QCP-n)	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location (EN)	**https://www.kibstrust.com/repository/docs/PDSG3-EN.pdf** *(за G3)* **https://www.kibstrust.com/repository/docs/PDSG2-EN.pdf** *(за G2)*
	PDS Location (MK)	**https://www.kibstrust.com/repository/docs/PDSG3-MK.pdf** *(за G3)* **https://www.kibstrust.com/repository/docs/PDSG2-MK.pdf** *(за G2)*
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEsign	**0.4.0.1862.1.6.1**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	**http://ocsp3.kibstrust.com/** *(за G3)* **http://ocsp2.kibstrust.com/** *(за G2)*
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://cacerts.kibstrust.com/KIBSTrustIssuingQsigCAG3.crt** *(за G3)* **https://www.kibstrust.com/repository/certs/CA-qSig-G2.crt** *(за G2)*
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder'skey.*
Enhanced Key Usage	Secure Email	**1.3.6.1.5.5.7.3.4**
	Client Authentication	**1.3.6.1.5.5.7.3.2**
Subject Alternative Name	RFC822 Name	*Email address of Subject*

7.1.2.6. За електронски печат за правно лице

Standard Extension	Field	Value
Authority Key Identifier	Key Identifier	E0B0E64BB05E5F53CF95DBFF17B747C4227432A9 *(за G3)* 264AABD306A8E9D270DA7104B631504785A9094D *(за G2)* *(This field contains the Subject Key Identifier of the issuer's Certificate.)*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.16305.1.1.5**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://www.kibstrust.com/repository/cps**
	Cert Policy ID	**0.4.0.194112.1.1** (QCP-l), или **0.4.0.194112.1.3** (QCP-l-qscd)
	Cert Policy ID	***За G3:*** **1.3.6.1.4.1.16305.1.2.5.5.2** (QCP-l), или **1.3.6.1.4.1.16305.1.2.5.5.3** (Local QSCD), или **1.3.6.1.4.1.16305.1.2.5.5.4** (Remote QSCD) ***За G2:*** **1.3.6.1.4.1.16305.1.2.5.2.2** (QCP-l), или **1.3.6.1.4.1.16305.1.2.5.2.3** (Local QSCD), или **1.3.6.1.4.1.16305.1.2.5.2.4** (Remote QSCD)
CRL Distribution Point	Distribution Point	Full Name
	Uniform Resource ID	**http://crl3.kibstrust.com/KIBSTrustIssuingQsealCAG3.crl** *(за G3)* **http://crl.kibstrust.com/qSealG2.crl** *(за G2)*
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD (N/A for QCP-l)	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location (en)	**https://www.kibstrust.com/repository/docs/PDSG3-EN.pdf** *(за G3)* **https://www.kibstrust.com/repository/docs/PDSG2-EN.pdf** *(за G2)*
	PDS Location (MK)	**https://www.kibstrust.com/repository/docs/PDSG3-MK.pdf** *(за G3)* **https://www.kibstrust.com/repository/docs/PDSG2-MK.pdf** *(за G2)*
	etsiQcType	**0.4.0.1862.1.6**

	etsiQcTypeEseal	**0.4.0.1862.1.6.2**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	**http://ocsp3.kibstrust.com/** *(за G3)* **http://ocsp2.kibstrust.com/** *(за G2)*
	Access Method	
	Access Location	**http://cacerts.kibstrust.com/KIBSTrustIssuingQsealCAG3.crt** *(за G3)* **https://www.kibstrust.com/repository/certs/CA-qSeal-G2.crt** *(за G2)*
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder'skey.*
Enhanced Key Usage	Secure Email	**1.3.6.1.5.5.7.3.4**
	Client Authentication	**1.3.6.1.5.5.7.3.2**
Subject Alternative Name	RFC822 Name	*Email address of Subject*

7.1.3. Предметни идентификатори на алгоритми

Алгоритмите за потпис ги следат спецификациите опишани во деловите 6.1.5 и 6.1.6. Сите алгоритами што се користат за ИС и претплатникот ги следат тековните стандарди за истражување и индустриски стандарди за да обезбедат разумна безбедност за предвидените цели за што се користат.

7.1.4. Форми на имиња

Секој сертификат вклучува единствен сериски број кој никогаш повторно не се користи.

Содржината на полето за карактеристично име на Издавачот на сертификат се совпаѓа со Subject DN на издавачот ИС за да се поддржи поврзаноста на имињата во синџир, како како што е наведено во RFC 5280, дел 4.1.2.4.

7.1.4.1. За коренски и издавачки сертификати

Field	Value	
Issuer	**CN = KIBSTrust Root CA G2** **2.5.4.97 = NTRMK-5529581** **OU = KIBSTrust Services** **O = KIBS AD Skopje** **C = MK** *(For Root CA it is the same as SubjectDN; For Issuing CAs it is the SubjectDN of the Root CA)*	
Subject DN	Common Name	**KIBSTrust Issuing Qsig CA G3** *(за G3 Issuing CA for e-Signature)* **KIBSTrust Issuing Qseal CA G3** *(за G3 Issuing CA for e-Seal)* **KIBSTrust Issuing Qsig CA G2** *(за G2 Issuing CA for e-Signature)* **KIBSTrust Issuing Qseal CA G2** *(за G2 Issuing CA for e-Seal)* *(Is used for user-friendly representation of the CA name to represent itself. This name does not need to be exact match of the fully registered organization name)*
	Organization	**KIBS AD Skopje** *(for Root CA and Issuing CAs)*
	OrganizationIdentifier (2.5.4.97)	***NTRMK-5529581***
	Organization Unit	*For Root and Issuing CA it is "*KIBSTrust Services*"*
	Country	**MK**

Version	**3**
Serial number	*Unique serial number of the certificate*
Key Size	**4096**
Validity Start	*First date of certificate validity*
Validity End	*Last date of certificate validity*
Signature Algorithm	**Sha256withRSAEncryption**

7.1.4.2. За електронски потпис за физичко лице

Field	Value	
Issuer	**CN = KIBSTrust Issuing Qsig CA G3** *(за G3)* **CN = KIBSTrust Issuing Qsig CA G2** *(за G2)* **2.5.4.97 = NTRMK-5529581** **OU = KIBSTrust Services** **O = KIBS AD Skopje** **C = MK** *(For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.)*	
Subject DN	Common Name	*Space separated Person Given name and Surname.*
	givenName	*Person given name in UTF8 format according to RFC5280*
	surName	*Person surname in UTF8 format according to RFC5280*
	serialNumber	*Unique Identification Number according registration number in CA database with the following semantics:"123456789"*
		Random code as specified in clause 5.1.3 of ETSI EN 319 412-1
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.3. За електронски потписи за физичко лице поврзано со правно лице

Field	Value	
Issuer	**CN = KIBSTrust Issuing Qsig CA G3** *(за G3)* **CN = KIBSTrust Issuing Qsig CA G2** *(за G2)* **2.5.4.97 = NTRMK-5529581** **OU = KIBSTrust Services** **O = KIBS AD Skopje** **C = MK** *(For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.)*	
Subject DN	Common Name	*Space separated Person Given name and Surname.*
	givenName	*Person given name in UTF8 format according to RFC5280*
	surName	*Person surename in UTF8 format according to RFC5280*
	Title	*Natural person position in Legal Person*
	serialNumber	*Unique Identification Number according to registration number in CA database with the following semantics:*

		"123456789"
		Random code as specified in clause 5.1.3 of ETSI EN 319 412-1
	Organization	*Issuer organization name who made subscriber identification.*
	Organizational Unit	*Issuer organization unit name (optional)*
	Organizational Unit	*VAT- <VATNumber> (optional)*
	OrganizationIdentifier (2.5.4.97)	**NTR***<Country code>-NTRnumber Identification of the Subscriber organization different from the organization name* *Legal Entity's Identification Number from a national trade register with the following semantics:* *"**NTR**MK-1234567".*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.4. За електронски печат за правно лице

Field	Value	
Issuer	**CN = KIBSTrust Issuing Qseal CA G3** *(за G3)* **CN = KIBSTrust Issuing Qseal CA G2** *(за G2)* **2.5.4.97 = NTRMK-5529581** **OU = KIBSTrust Services** **O = KIBS AD Skopje** **C = MK** *(For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.)*	
Subject DN	Common Name	*Legal Person's name*
	Organization	*Issuer organization name who made subscriber identification.*
	Organizational Unit	*Issuer organization unit name (optional)*
	Organizational Unit	*VAT- <VATNumber> (optional)*
	OrganizationIdentifier (2.5.4.97)	*Legal Entity's Identification Number from a national trade register with the following semantics:* *"**NTR**MK-1234567".*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.5. Ограничувања на имињата

KIBS може да вклучи ограничувања на имињата во полето nameConstrains, кога е соодветно.
Ако сертификатот на издавачкиот ИС вклучува проширена употреба на клучот „id-kp-emailProtection“, тој се третира како технички ограничен и ревидиран како што е опишано во дел 8.

7.1.6. Предметен идентификатор на Политиката за сертификати

Според секој тип на сертификат, следниве признати OID може да се додадат во екстензијата certificatePolicies:

- **QCP-n**: 0.4.0.194112.1.0 како што е опишано во ETSI EN 319 411-2
- **QCP-l**: 0.4.0.194112.1.1 како што е опишано во ETSI EN 319 411-2
- **QCP-n-qscd**: 0.4.0.194112.1.2 како што е опишано во ETSI EN 319 411-2
- **QCP-l-qscd**: 0.4.0.194112.1.3 како што е опишано во ETSI EN 319 411-2

КИБС, исто така, ги додава следниве OID во наставката за Политики за сертификати, за да идентификува кога приватниот клуч за квалификуван сертификат се наоѓа на локално QSCD средство чие управување за креирање на овој приватен клуч го има претплатникот / субјектот и кога приватниот клуч на квалификуваниот сертификат се наоѓа на далечинско QSCD средство чие управување за креирање на овој приватен клуч го има QTSP во име на претплатникот:

- Квалификувани електронски потписи
  - **1.3.6.1.4.1.16305.1.2.5.4.3** Приватниот клуч е на локално QSCD за G3
  - **1.3.6.1.4.1.16305.1.2.5.1.3** Приватниот клуч е на локално QSCD за G2
  - **1.3.6.1.4.1.16305.1.2.5.4.4** Приватниот клуч е на далечинско QSCD G3
  - **1.3.6.1.4.1.16305.1.2.5.1.4** Приватниот клуч е на далечинско QSCD за G2.
- Квалификувани електронски печати
  - **1.3.6.1.1.4.1.15976.1.5.5.3** Приватниот клуч е на локално QSCD за G3
  - **1.3.6.1.1.4.1.15976.1.5.2.3** Приватниот клуч е на локално QSCD за G2
  - **1.3.6.1.4.1.16305.1.2.5.5.4** Приватниот клуч е на далечинско QSCD за G3
  - **1.3.6.1.4.1.16305.1.2.5.2.4** Приватниот клуч е на далечинско QSCD за G2.

7.1.7. Користење екстензија за ограничување на Политиката

Не се применува.

7.1.8. Синтакса и семантика за квалификаторите на Политиката

Квалификатор за политиката е URI што укажува на објавениот КИБС CP/CPS.

7.1.9. Процесирачка семантика за критичните екстензии на сертификациските политики

Не се применува.

7.2. CRL профил

CRL профилот е во согласност со X.509 верзија 2 и IETF RFC 5280.

7.2.1. Нумерирање верзии

KIBS издава CRL верзија 2 што ги содржи следниве полиња:

Поле	Вредност
Issuer Signature Algorithm (Алгоритам за потпис на Издавачот)	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer Distinguished Name (Карактеристично име на Издавачот)	Карактеристично име (SubjectDN) на издавачкиот ИС на КИБС
thisUpdate (сегашно ажурирање)	датум на издавање на CRL во UTC формат

nextUpdate (следно ажурирање)	датум кога следниот CRL ќе се објави во UTC формат
Revoked Certificates List (Регистар на поништени сертификати)	Регистар на поништени сертификати, вклучувајќи сериски број и датум на поништување
Signature (Потпис)	Алгоритамот за потпис МОРА да ги следи барањата опишани во дел 6.1.5. и 6.1.6.

7.2.2. CRL и екстензии на записот во CRL

CRL ги има следниве екстензии:

Екстензија	**Вредност**
CRL број	Никогаш не се повторува, монотоно зголемување на цел број
Идентификатор на клучот на Издавачот	Исто како и идентификаторот на клучот на Издавачот наведен во сертификатот
Датум на невалидност	Опционален датум во формат UTC
Шифра за причина	Опционална причина за поништување

7.3. OCSP профил

7.3.1. Нумерирање на верзии

OCSP профилот на КИБС е во согласност со IETF RFC 6960.

7.3.2. OCSP екстензии

Ектензии за KIBSTrust Issuing Qsig CA G2 and KIBSTrust Issuing Qseal CA G2 OCSP Responder:

Standard Extension	Field	Value
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.16305.1.1.5**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.kibstrust.com/repository/cps**
Key Usage	Digital Signature	**Set**
OCSP No Revocation Checking	ocsp-nocheck	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**https://www.kibstrust.com/repository/certs/CA-qSig-G2.crt**, или **https://www.kibstrust.com/repository/certs/CA-qSeal-G2.crt**
Enhanced Key Usage	OCSP Signing	**Set**
Subject Key Identifier	RFC822 Name	*This field contains the ID of the Certificate Holder's key.*

Ектензии за KIBSTrust Issuing Qsig G3 OCSP Responder and KIBSTrust Issuing Qseal CA G3 OCSP Responder:

Standard Extension	Field	Value
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Key Usage	Digital Signature	**Set**
OCSP No Revocation Checking	ocsp-nocheck	**Set**
Enhanced Key Usage	OCSP Signing	**Set**
Subject Key Identifier	RFC822 Name	*This field contains the ID of the Certificate Holder's key.*

8. НАДЗОР ВО ВРСКА СО УСОГЛАСЕНОСТА И ДРУГИ ПРОЦЕНКИ

Сообразноста на информатичкиот систем, политиките и практиките, објектите, персоналот и средствата на КИБС се проценува од тело за проценка на сообразност, согласно законот МК-eIDAS и eIDAS регулативата, соодветните закони и стандарди или секогаш кога е направена голема промена во работата на доверлива услуга, врз база на ETSI стандардите наведени во дел 9.15.

Покрај ревизиите за усогласеност, КИБС има право да изврши други прегледи и истражувања за да се обезбеди доверливост на услугите за сертификација на КИБС. КИБС има право да го делегира извршувањето на овие ревизии, прегледи и истраги на ревизорска фирма на трета страна.

КИБС има право да изврши надворешни ревизии на договарачи кои се поврзани со КИБС за да работат како Локална регистрациона канцеларија (ЛРК).

8.1. Интервали и околности на проценките

Ревизијата за сообразност на КИБС ИС се изведува најмалку еднаш годишно. Ревизиите се вршат во непрекинати низи на ревизорски периоди, и секој период е со траење не подолго од една година.

8.2. Идентитет и квалификации на проценителот

Ревизијата за сообразност на КИБС ИС се изведува од страна на:

- Интерни ревизори,
- Тело за проценка на усогласеност кое е акредитирано во согласност со Регулативата ЕЗ бр. 765/2008, ETSI стандардите (т.е. ETSI EN 319 403),
- Надзорно тело.

8.3. Однос на проценителот со проценуваниот субјект

Ревизорот на телото за проценка на сообразноста е независен од КИБС и од системите на КИБС кои се проценуваат. Внатрешниот ревизор не врши ревизија на сопствените области на одговорност.

8.4. Прашања опфатени со проценката

Проценката на сообразност опфаќа усогласеност на информатичкиот систем, политиките и практиките, објектите, персоналот и средствата на КИБС со МК-eIDAS и eIDAS регулативите, соодветните закони и стандарди. Телото за проценка на сообразноста врши ревизија на деловите на информатичкиот систем користен за давање доверливи услуги.

Областите на активност, предмет на внатрешна ревизија се следниве:

- Квалитет на услугата;
- Сигурност на услугата;

- Сигурност на работењето и процедурите;
- Заштита на податоците на претплатниците и безбедносната политика, извршување на работните процедури и договорните обврски, како и усогласеност со CP и изјавите за политики и практики засновани врз услуги.

Телото за проценка на сообразноста и внатрешниот ревизор, исто така, ги ревидираат овие делови од информатичкиот систем, политиките и практиките, објектите, персоналот и средствата на поддоговарачите кои се поврзани со обезбедување доверливи услуги на КИБС (на пр., вклучувајќи ја ЛРК).

8.5. Дејствија што се преземаат како резултат на пропусти

Во однос на ревизиите за усогласеност на работењето на КИБС, значајните исклучоци или недостатоци утврдени за време на ревизијата за усогласеност ќе резултираат со утврдување на активности што треба да се преземат. Оваа определба ја утврдува менаџментот на КИБС со внесување податоци од ревизорот. Менаџментот на КИБС е одговорен за развој и спроведување на корективен акциски план. Ако КИБС утврди дека ваквите исклучоци или недостатоци претставуваат непосредна закана за сигурноста или интегритетот на доверливите услуги, корективниот акциски план ќе се развие во рок од 30 дена и ќе се спроведе во разумен временски период. За помалку сериозни исклучоци или недостатоци, менаџментот на КИБС ќе го процени значењето на ваквите проблеми и ќе го одреди соодветниот тек на дејствување.

Дополнително, во случај на резултат на проценка од телото за проценка на сообразноста, кој покажува дека има недостаток, Надзорниот орган бара КИБС да отстрани какво било неисполнување на барањата во временски рок (доколку е применливо) утврден од Надзорниот орган. КИБС прави напори да остане во согласност и навреме да ги исполни сите барања за недостаток. Менаџментот на КИБС е одговорен за спроведување на корективниот акциски план. КИБС го проценува значењето на недостатоците и дава приоритет на соодветните активности што треба да се преземат барем во временскиот рок што е определен од Надзорното тело или во разумен временски период.

Кога се чини дека се повредени правилата за заштита на личните податоци, Надзорниот орган го известува органот за заштита на податоците за резултатите од ревизијата за усогласеност.

8.6. Соопштување на резултатите

Заклучоците од ревизијата или сертификатот (-ите) за доверливи услуги, кои се засноваат на резултатите од ревизијата на телото за проценка на сообразност, спроведено во согласност со МК- eIDAS законот и eIDAS регулативата, соодветните закони и стандарди, може да бидат објавени на веб-страницата на КИБС https://www.kibstrust.com/repository.

Покрај тоа, КИБС го доставува добиениот извештај за проценка на сообразноста до Надзорното тело во рок од три (3) работни дена од приемот на истиот. КИБС ги доставува заклучоците од ревизијата или сертификатот (ите) за доверливи услуги на одржувачите на програмите за Root Browsers во кои учествуваат КИБС и други заинтересирани страни.

Резултатите од ревизијата на усогласеност на работењето на КИБС ИС може да бидат објавени според дискреционото право на менаџментот на КИБС.

8.7. Самопроценки

КИБС врши редовни внатрешни ревизии за да утврди усогласеност согласно дел 8.4.

9. ОСТАНАТИ ДЕЛОВНИ И ПРАВНИ РАБОТИ

9.1. Надоместоци

9.1.1. Надоместоци за издавање и обновување сертификати

КИБС наплатува на претплатниците - крајни корисници надоместок за издавање, управување и обновување сертификатите со нови парови на клучеви.

9.1.2. Надоместоци за пристап до сертификатите

КИБС не наплатува надоместок како услов за да ги стави на располагање сертификатите во складиште или на друг начин да ги направи сертификатите достапни на засегнатите страни.

9.1.3. Надоместоци за пристап до информациите за поништување или за статусот на сертификатот

КИБС не наплатува надоместок како услов на OCSP и ги прави CRL, потребни со оваа CP, достапни во складиштето или на друг начин достапни на засегнатите страни. КИБС не дозволува пристап до информациите за поништување, информациите за статусот на сертификатите или информациите за статусот на сертификатите во своите складишта на трети лица кои обезбедуваат производи или услуги кои користат вакви информации за статусот на сертификатите, без претходно јасно изразена писмена согласност од страна на КИБС.

9.1.4. Надоместоци за други услуги

КИБС не наплатува надоместоци за пристап до овие Правила. Секое друго користење, освен едноставно разгледување на документот, како репродуцирање, редистрибуирање, изменување или креирање на текстови што ќе произлезат од нив се предмет на договор за лиценца со КИБС.

9.1.5. Политика на рефундирање (повраток на средства)

9.1.5.1. Продажба од далечина

Во случај продажбата на сертификатот да се изврши преку интернет или телефонски повик, претплатникот има право, согласно Законот за заштита на потрошувачите[3], член 89, како што е дополнет и изменет, да се повлече од договорот за продажба без да ги наведе причините во временски рок од четиринаесет (14) календарски денови од датумот на купување. Остварувањето на ова право ќе се изврши во писмена форма со испраќање на е-порака на helpdesk@kibstrust.com од страна на претплатникот до КИБС.

Потоа, и после комуникацијата, КИБС е должен да ги врати средствата што соодветствуваат на вредноста на договорот за продажба на претплатникот. Плаќањето за рефундација се извршува со ист метод како и првичното плаќање, а претплатникот нема право да го користи сертификатот доколку е издаден. По тој период, правото на повлекување истекува и КИБС нема дополнителна обврска за горенаведената клаузула.

Претплатникот има право да се повлече од онлајн подготвениот образец ,,Порачка и договор" пред активирање на сертификатот. Доколку претплатникот не покаже или не достави соодветна документација во рок од триесет (30) дена од неговиот / нејзиниот образец ,,Порачка и договор" за квалификуван сертификат за електронски потпис или печат во / до РК / ЛРК на давателот на доверливи услуги, образецот за ,,Порачка и договор" автоматски ќе се отфрли од системот. Во овој случај, доколку претплатникот веќе го платил сертификатот за електронски потпис или печат, КИБС нема да го рефундира плаќањето, туку ќе го поврзе плаќањето со нова постапка за набавка на сертификат во текот на тековната фискална година.

Доколку е издаден сертификат, претплатникот, во рок од пет (5) дена од денот на активирање на сертификатот може да го рекламира истиот или локалното QSCD во случај на неисправност, едноставно поради фабричка грешка, поради што сертификатот или локалното QSCD не одговара на описот, предвидената намена и употреба што се декларирани и објавени од КИБС.

Во тој случај претплатникот, единствено има право да бара да му биде извршена замена на купениот сертификат со нов и исправен сертификат. Во секој случај, претплатникот нема право на раскинување на договорот за купопродажба и враќање на платените средства.

По навремено направената рекламација, КИБС се обврзува да направи неопходна проверка на сертификатот со цел утврдување на неговата функционална исправност.

КИБС во секој случај нема да прифати никакви рекламации направени по истекот на утврдениот рок од 5 дена од активирањето на сертификатот.

[3] Закон за заштита на потрошувачите (Службен весник на Република Северна Македонија 38/04...140/18)

КИБС не прифаќа какви било рекламации за недостатоци и оштетувања на сертификатот настанати по вина или активности преземени од претплатникот.

9.1.5.2. Други случаи

Според дел 9.1.5.1, КИБС се справува со наплата од случај до случај.

За да се побара рефундирање, претплатникот треба да испрати писмено барање до КИБС. Оваа политика на рефундирање не е ексклузивен лек и не ги ограничува другите лекови кои можат да им бидат достапни на претплатниците за да се справат со рефундирањето, случај по случај. Во ретки случаи, КИБС може да направи рефундација на претплатникот. Остварувањето на ова право ќе се изврши во писмена форма од претплатникот со испраќање на е-порака до helpdesk@kibstrust.com до КИБС.

9.2. Финансиска одговорност

9.2.1. Покритие на осигурување

КИБС одржува комерцијално разумно ниво на покритие со осигурување од професионална одговорност за грешки и пропусти преку програма за осигурување од грешки и пропусти кај Друштво за осигурување. Потврда за полиса за осигурување е достапна во јавното складиште КИБС на http://www.kibstrust.com/repository.

Правилата за обештетување во согласност со осигурувањето од професионална одговорност на давателот на доверливи услуги КИБС (во натамошниот текст: Правила) го следат законот МК-eIDAS[4]. Следејќи го подзаконскиот акт[5] на МК-eIDAS, TSP КИБС е целосно прилагоден на утврдените барања за износот на покривање на ризик од одговорност за штета. За секоја доверлива услуга, КИБС јавно издава „Правила и услови“ за користење на услугата. Овие правила и услови вклучуваат соодветни информации за осигурување од професионална одговорност на давателот на доверливи услуги.

9.2.2. Други средства

КИБС има доволно финансиски средства да ги одржува своите операции и да ги извршува своите должности, како и разумна можност да го понесе ризикот од одговорност кон претплатниците и засегнатите страни. Доказите за финансиските средства не се јавно достапни.

9.2.3. Осигурување или гарантно покритие за крајните субјекти

Види дел 9.2.1. од овие CP/CPS.

9.3. Доверливост на деловните информации

9.3.1. Опсег на доверливи информации

Сите информации што се откриени при обезбедување услуги, а кои не се наменети за објавување (на пр. информации што биле познати на КИБС заради функционирање и обезбедување на доверливи услуги) се доверливи. Претплатникот има право да добие информации од КИБС за себе, според важечките закони.

9.3.2. Информации што не се во доменот на доверливи информации

Секоја информација која не е наведена како доверлива или наменета за внатрешна употреба е јавна информација. Информациите што се сметаат за јавни во КИБС се наведени во делот 2.2 од овие CP/CPS.

Покрај тоа, статистички податоци за услугите на КИБС кои не се персонализирани се сметаат за јавни информации. КИБС може да објави статистички податоци за своите услуги кои не се персонализирани.

[4] Закон за електронски документи, електронски информации и доверливи услуги (МК-eIDAS)

[5] Правилник за определување на најнискиот износ на осигурување за можна штета предизвикана од издавачот и минималниот износ или тип на покривање со осигурување од ризик од одговорност за штети предизвикани од давателот на квалификувани доверливи услуги.

9.3.3. Одговорност за заштитата на доверливите информации

КИБС ги заштитува доверливите информации и информациите наменети за внатрешна употреба од компромитирање и откривање на трети страни со спроведување на различни безбедносни контроли.

Откривањето или доставувањето доверливи информации на трета страна е дозволено само со писмена согласност од правниот сопственик на информацијата, врз основа на судски налог или во други случаи предвидени со закон.

9.4. Приватност на личните информации

9.4.1. План за лични податоци

КИБС применува Политика за заштита на личните податоци, која е поставена на: http://pki.kibstrust.mk/repository во согласност со важечките закони.

9.4.2. Информации што се третираат како приватни

Каков било податок за претплатник кој не е јавно достапен преку содржината на издадениот сертификат, директориумот на сертификати и онлајн CRL се третира како приватен.

9.4.3. Информации што не се сметаат за приватни

Во зависност од важечките закони, сите информации објавени во сертификатот не се сметаат како приватни.

9.4.4. Одговорност за заштита на приватните податоци

КИБС ќе ги обезбеди личните податоци од компромитирање и од откривање на трети лица и ќе се придржува кон важечките закони за заштита на личните податоци.

9.4.5. Известување и согласност за користење на личните податоци

Согласно важечкиот законот за заштита на личните податоци, освен ако поинаку не е наведено во овие CP/CPS, применливата Политиката за заштита на личните податоци и со договор, приватните податоци не се користат без согласност на страната на која се однесува информацијата.

9.4.6. Откривање што произлегува од судски или административен процес

КИБС има право да открие доверливи информации ако, со добра намера, верува дека:

- откривањето е неопходно како одговор на судска покана и налог за претрес;
- откривањето е неопходно како одговор на судски, административни и други правни процедури за време на истражни процеси во граѓански или административни дејствија, како на пример судска покана, распит, барање за прифаќање и барање за продуцирање на документи.

Овој дел подлежи на применливите закони за приватност.

9.4.7. Откривање по барање на сопственикот

Правилата и принципите за заштита на личните податоци на КИБС содржат одредби поврзани со откривање на лични податоци на лицето кое му ги доставило тие податоци на КИБС. Овој дел подлежи на важечките закони за приватност.

9.4.8. Други околности на откривање информации

Не се применува.

9.5. Права на интелектуална сопственост

Распределбата на правата на интелектуална сопственост помеѓу учесниците на КИБС, освен претплатниците и засегнатите страни, е регулирана со важечките договори, склучени помеѓу тие учесници на поддоменот на КИБС. Следниве потточки се однесуваат на правата на интелектуална сопственост поврзани со претплатниците и засегнатите страни.

9.5.1. Права на сопственост во сертификатите и информациите за поништување

ИС ги задржува сите права на интелектуална сопственост во и на сертификатите и на информациите за поништување што ги издава. КИБС дава дозвола за репродуцирање и дистрибуирање на сертификатите на неексклузивна основа без плаќање на авторски права, под услов тие да бидат репродуцирани во целост и користењето на сертификатите да биде регулирано со Правилата и условите наведени во сертификатот. КИБС дава дозвола за користење на информациите за поништување заради извршување на функциите на засегнатите страни, што е регулирано во соодветните Правила и услови или некои други важечки договори.

9.5.2. Права на сопственост во Правилата

Претплатниците прифаќаат дека КИБС ги задржува сите права на интелектуална сопственост во и на овие CP/CPS.

9.5.3. Права на сопственост на имиња

Подносителот на барањето за сертификат ги задржува сите права што ги има (доколку ги има) на трговската марка, сервисната марка или трговското име содржани во барањето за сертификат и карактеристичното име во сертификатот, издаден на таквиот барател на сертификат.

9.5.4. Права на сопственост на клучевите и материјалот со клучеви

Паровите клучеви што соодветствуваат со сертификатите на ИС и на претплатниците - крајни корисници се сопственост на ИС и на претплатниците - крајни корисници кои се субјекти на тие сертификати, без оглед на физичкиот медиум во кој тие се складираат и заштитуваат, и тие лица ги задржуваат сите права на интелектуална сопственост во и на овие парови клучеви. Без да се ограничува воопштеноста на претходното, коренските јавни клучеви на КИБС и коренските сертификати кои ги содржат нив, вклучително и PRCA јавните клучеви и самопотпишаните сертификати, се сопственост на КИБС. Конечно, Тајните удели на приватните клучеви на ИС се сопственост на ИС и ИС ги задржува сите права на интелектуална сопственост на тие Тајни удели, иако не може да стекне физичка сопственост врз тие удели или ИС од КИБС.

9.5.5. Прекршување на правата на сопственост

КИБС свесно не ги крши правата на интелектуална сопственост на која било трета страна.

9.6. Изјави и гаранции

9.6.1. Изјави и гаранции на ИС

КИБС ИС гарантира дека:

- ги обезбедува своите услуги во согласност со барањата и процедурите дефинирани во овие CP/CPS и поврзаните документи;
- е во согласност со MK-eIDAS и eIDAS регулативата и поврзаните правни акти утврдени во овие CP/CPS и поврзаните документи;
- ги објавува своите CP/CPS и поврзаните документи и ја гарантира нивната достапност во мрежата за комуникација со јавни податоци;
- ги објавува и исполнува барањата на правилата и условите за претплатници и гарантира нивна достапност и пристап во мрежата за комуникација со јавни податоци;
- ја одржува доверливоста на информациите што ги добива во текот на снабдувањето со услугата и што не подлежат на објавување;
- води сметка за токените за доверливите услуги, издадени од него и нивната валидност, и обезбедува можност за проверка на важноста на сертификатите;
- обезбедува пристап до приватните клучеви на далечинското QSCD на овластениот претплатник на клучевите;
- обезбедува правилно управување и усогласеност на далечинското QSCD;
- го известува Надзорното тело за какви било промени во јавниот клуч што се користи за давање доверливи услуги;

- без непотребно одложување, но во секој случај во рок од 24 часа откако ќе дознае за какво било нарушување на сигурноста или загубата на интегритетот што има значајно влијание врз пружената доверлива услуга или врз личните податоци што се содржат во неа, ќе го извести Надзорниот орган и, кога е соодветно, другите релевантни тела како националниот CERT или Инспекторатот за податоци.
- кога постои можност прекршувањето на сигурноста или загубата на интегритетот да влијае негативно на физичко или правно лице на кое му е обезбедена доверлива услуга, без одложување ќе го извести физичкото или правното лице за повредата на сигурноста или за губењето на интегритетот;
- ја чува целата документација, евиденција и записи поврзани со доверливите услуги според точките 5.4 и 5.5;
- обезбедува проценка на усогласеноста според барањата и го презентира заклучокот на телото за проценка на усогласеноста на Надзорното тело за да обезбеди континуиран статус на доверливите услуги во доверливиот список;
- има финансиска стабилност и ресурси потребни за да работи во согласност со овие CP/CPS;
- ги објавува условите на политиката за задолжително осигурување и заклучокот на телото за проценка на усогласеноста во мрежата за комуникација со јавни податоци;
- овозможува пристап до своите услуги за лица со посебни потреби, доколку тоа е можно;
- нема материјално погрешно претставување на факт во сертификатот, познат или што потекнува од субјекти кои го одобруваат барањето за сертификат или издаваат сертификат,
- нема грешки во информациите во сертификатот што се воведени од субјектите кои го одобруваат барањето за сертификат или издавањето на сертификат како резултат на неуспехот да се употреби разумна грижа во управувањето со барањето за сертификат или да се креира сертификат;
- услугите за поништување и употреба на складиште се усогласени со важечките CP/CPS во сите материјални аспекти.

Правилата и условите за користење на квалификувани доверливи услуги на КИБС може да вклучат дополнителни изјави и гаранции.

9.6.2. Изјави и гаранции на РК

КИБС РК гарантира дека:

- Го верификувале идентитетот на претплатникот преку постапки одобрени од КИБС,
- Нема материјално погрешно претставување на факт во сертификатот што е познат или што потекнува од субјекти кои го одобруваат барањето за сертификат или издаваат сертификат,
- Нема грешки во информациите во сертификатот што се воведени од субјектите кои го одобруваат барањето за сертификат како резултат на непостоење разумна грижа при управувањето со барањето за сертификат,
- Нивните сертификати ги исполнуваат сите материјални барања на овие CP/CPS, и
- Услугите за поништување (кога е применливо) и употребата на складиштето се усогласени со применливите CP/CPS во однос на сите материјални аспекти.

Правилата и условите на КИБС може да вклучат дополнителни изјави и гаранции.

9.6.3. Изјави и гаранции на претплатникот

Претплатниците гарантираат дека:

- Секој е-потпис или е-печат креиран со употреба на приватниот клуч кој одговара на јавниот клуч, наведен во квалификуваниот сертификат е квалификуван е-потпис или е-печат на претплатникот и квалификуваниот сертификат е прифатен и оперативен (не е истечен или поништен) во моментот кога се креира квалификуван е-потпис или е-печат,
- Податоците (ПИН, корисничко име, лозинка, OTP) со кои се пристапува до приватниот клуч се заштитени и дека ниту едно неовластено лице досега немало пристап до нив,
- Квалификуваното е-потпис се креира само на QSCD, додека пак квалификуван е-печат може да се креира на QSCD или без него,

- Сите изјави направени од претплатникот во барањето за сертификат кој го поднесува претплатникот се вистинити, а претплатникот е свесен за тоа дека КИБС може да одбие да ја обезбеди услугата ако претплатникот намерно претставил лажни, неточни или нецелосни информации во барањето за услуга;
- Претплатникот ги почитува барањата дадени од КИБС во овие CP/CPS и поврзаните документи;
- Сите информации доставени од претплатникот и содржани во сертификатот се вистинити и во случај на промена на доставените податоци, претплатникот треба да ги извести точните податоци во согласност со правилата утврдени со овие CP/CPS и поврзаните документи;
- Сертификатот се користи исклучиво за овластени и правни цели, во согласност со овие CP/CPS;
- Претплатникот не е ИС, и не го користи приватниот клуч што одговара на јавен клуч наведен во сертификатот за целите на дигитално потпишување на кој било сертификат (или кој било друг формат на овластен јавен клуч) или CRL, како ИС или поинаку;
- Претплатникот без одложување ќе го извести КИБС, доколку приватниот клуч на субјектот е украден или потенцијално компромитиран, или пак контролата врз него е изгубена.

Правилата и условите на КИБС за користење на квалификувани доверливи услуги може да вклучат дополнителни изјави и гаранции.

9.6.4. Изјави и гаранции на засегнатата страна

Според Правилата и условите на КИБС за користење на квалификувани доверливи услуги се предвидува засегнатата страна да потврди дека поседува доволно информации за да донесе информирана одлука за обемот до кој таа ќе одбере да се потпре на информациите во сертификатот, дека единствено таа е одговорна за одлуката дали ќе се потпре или не на таквата информација, и дека таа ќе ги поднесе законските последици од нејзиното неуспевање да ги изврши обврските на засегната страна согласно овие CP/CPS.

Правилата и условите на КИБС за користење на квалификувани доверливи услуги може да вклучат дополнителни изјави и гаранции на засегнатите страни.

9.6.5. Изјави и гаранции на други учесници

Не се применува.

9.7. Одрекување на гаранциите

До онаа мера која е дозволена со важечкиот закон, Правилата и условите за користење на квалификувани сертификати ги одрекуваат можните гаранции на КИБС, вклучително и каква било гаранција за пласирање на пазарот или соодветност за одредена намена.

КИБС не е одговорен за:

- Тајноста на податоците (ПИН, корисничко име, лозинка, OTP) со кои се има пристап до приватните клучеви на претплатниците, можната злоупотреба на сертификати или несоодветните проверки на сертификати или за погрешни одлуки на засегнатата страна, или какви било последици поради грешки или пропусти во проверките за валидација на доверлива услуга;
- Неизвршување на своите обврски, доколку таквото неизвршување се должи на грешки или безбедносни проблеми на Надзорното тело, органот за супервизија на заштитата на податоци, доверливиот список или кој било друг јавен орган;
- Неизвршување на обврските што произлегуваат од овие CP/CPS и поврзаните документи, доколку таквото неизвршување е предизвикано од Виша сила.

9.8. Ограничувања на одговорност

Правилата и условите на КИБС за користење на квалификувани доверливи услуги ја ограничуваат одговорноста на КИБС. Ограничувањата на одговорноста вклучуваат изземање на индиректни, посебни, случајни и последователни штети. Тие, исто така, вклучуваат и ограничување на одговорноста во износ на петстотини евра (500,00 €) изразено во денарска противвредност според средниот курс на НБРСМ, со што се ограничуваат штетите на КИБС во врска со квалификуван сертификат.

Одговорноста (и/или нејзиното ограничување) на претплатниците и засегнатите страни е наведена во релевантните Претплатнички договори за користење на квалификувани доверливи услуги.

9.9. Обесштетувања

9.9.1. Обесштетување од страна на претплатниците

До мера до која е пропишано со применливиот закон, од претплатниците се очекува да го обесштетат КИБС за:

- Фалсификување или погрешно интерпретирање на факти од страна на претплатникот во
- барањето за сертификат,
- Неприкажување на материјален факт во барањето за сертификат, од страна на претплатникот, ако погрешната интерпретација или пропустот се направени од небрежност или со намера да се измами некоја од страните,
- Неуспехот на претплатникот да го заштити претплатничкиот приватен клуч, да го користи доверливиот систем или неуспевањето на друг начин да спречи компромитирање, губење, откривање, изменување или неовластено користење на претплатничкиот приватен клуч, или
- Користењето на име (вклучително и без ограничувања во рамките на општото име, името на доменот, или електронската адреса) од страна на претплатникот кое ги прекршува правата на интелектуална сопственост на трето лице.

Претплатничкиот договор може да вклучи дополнителни обврски за обесштетувања.

9.9.2. Обесштетување од страна на засегнатите страни

До мера до која е пропишано со применливиот закон, Правилата и условите на КИБС за користење на квалификувани доверливи услуги бараат засегнатата страна да го обесштети КИБС во случај кога:

- Засегнатата страна не ги исполнила обврските на засегната страна,
- Засегнатата страна се потпира на сертификат за кој во дадени околности, тоа не е разумно, или
- Засегнатата страна не го проверила статусот на сертификатот за да утврди дали сертификатот е истечен или поништен.

Правилата и условите за користење на квалификуваните доверливи услуги може да вклучат дополнителни обврски за обесштетување.

9.10. Период и прекин на важност

9.10.1. Период на важност

Овие CP/CPS стапуваат во сила по објавувањето во складиштето на КИБС. Измените и дополнувањата на овие CP/CPS стапуваат во сила по објавувањето во складиштето на КИБС.

9.10.2. Прекин на важност

Овие CP/CPS со промените кои се прават одвреме навреме остануваат во сила сè додека не се заменат со нова верзија.

9.10.3. Ефекти од прекинот на важност и продолжување

Без оглед на прекинувањето на важноста на овие CP/CPS, КИБС PKI учесниците , се обврзани со сите услови за сите издадени сертификати до крајот на периодот на важност на таквите сертификати.

9.11. Индивидуални известувања и комуникација со учесниците

Доколку не е специфицирано поинаку со договор помеѓу страните, КИБС PKI учесниците ќе користат комерцијално разумни методи за да комуницираат помеѓу себе, имајќи ги предвид критичноста и темата на комуникацијата.

Делот 1.5.1 ги дава сите достапни средства за комуникација.

9.12. Измени и дополнувања

9.12.1. Процедура на измени и дополнувања

Измените и дополнувањата на овие CP/CPS ги прави Телото за управување со политика (PMA) на КИБС. Измените и дополнувањата се во форма на документ кој содржи изменета и дополнета форма на CP / CPS или ажурирање. Верзиите со измените и дополнувањата или ажурирањата поврзани со складиштето на КИБС се објавени на https://www.kibstrust.com/repository/cps.

Ажурирањата ги заменуваат сите наведени или спротивставени одредби на наведената верзија на CP/CPS. PMA утврдува дали промените во CP/CPS бараат промена во предметните идентификатори на Политиката за сертификати, според Политиките за сертификати.

9.12.2. Механизам и период на известување

Телото за управување со политика (PMA) на КИБС го задржува правото да ги измени и дополни CP/CPS без известување за измените и дополнувањата што не се материјални, вклучително и без ограничување корекција на типографски грешки, измени во URL адреси и промени во информации за контакт. Одлуката на PMA да ги означи измените како материјални или нематеријални е според дискреционото право на PMA.

Предложените измени и дополнувања на CP/CPS се поврзани со складиштето КИБС лоцирано на: https://www.kibstrust.com/repository/cps.

Без оглед на сè спротивно во CP/CPS, доколку PMA верува дека материјалните измени и дополнувања во CP/CPS се неопходни веднаш да се запре или да се спречи нарушување на сигурноста на давателот на доверливи услуги (TSP) или на кој било дел од тоа, КИБС и PMA имаат право да ги направат ваквите измени и дополнувања преку објавување во складиштето на КИБС. Ваквите измени и дополнувања ќе стапат во сила веднаш по објавувањето. Во разумно време по објавувањето, КИБС ќе ги извести учесниците на КИБС PKI за ваквите измени и дополнувања.

KIBS и PMA, ќе ги ажурираат овие CP/CPS минимум на годишно ниво, во согласност со упатствата на Форумот CA / Browser.

Измените и дополнувањата што не го менуваат значењето на овие CP/CPS, како што се правописни корекции, превод и ажурирања за деталите за контакт, се документирани во делот историја на верзии на овој документ. Во овој случај, избраниот дел од бројот на верзијата на документот е зголемен.

Во случај на значителни промени, новата верзија на CP/CPS јасно се разликува од претходните и серискиот број е зголемен за еден.

9.12.3. Околности под кои мора да се промени предметниот идентификатор (OID)

Ако PMA одреди дека е неопходна промена во некој предметен идентификатор што соодветствува на Политиката за сертификати, измените и дополнувањата ќе содржат нов предметен идентификатор за Политиките за сертификати. Инаку, измените и дополнувањата не бараат промена во предметниот идентификатор на Политиката за сертификати.

9.13. Одредби за решавање на спорови

9.13.1. Спорови помеѓу КИБС, ЛРК, претставништва и клиенти

Споровите меѓу учесниците во КИБС PKI се решаваат во согласност со одредбите на важечките договори меѓу страните.

9.13.2. Спорови со претплатници - крајни корисници или засегнати страни

Правилата и условите на КИБС содржат клаузула за решавање на спорови. За споровите во кои е инволвиран КИБС, предвиден е почетен период на преговори од шеесет (60) дена, после кој ќе следи судски спор во надлежниот судот во Скопје.

9.14. Меродавно право

Законите на Република Северна Македонија ќе бидат надлежни за извршувањето, составувањето, интерпретирањето и важноста на овие CP/CPS, без оглед на договорот или изборот на други законски одредби и без барање да се воспостави комерцијална врска во земјата. Овој избор на закон е направен за да се обезбедат униформни процедури и толкување за сите учесници на КИБС PKI, без оглед каде се наоѓаат.

Одредбата за меродавно право важи само за овие CP/CPS. Договорите кои ги вклучуваат овие CP/CPS само како референца може да имаат свои сопствени одредби за меродавно право, под услов делот 9.14 да го регулира извршувањето, составувањето, интерпретирањето и важноста на условите од овие CP/CPS, одделно и раздвоено од останатите одредби на кој било таков договор, предмет на какви било ограничувања што се појавуваат во применливиот закон.

9.15. Усогласеност со меродавното право

КИБС обезбедува усогласеност со законските услови за исполнување на сите применливи законски барања за заштита на евиденцијата од губење, уништување и фалсификување и барањата на следново:

- MK-eIDAS - Закон за електронски документи, електронска идентификација и доверливи услуги (Службен весник на Република Северна Македонија 101/19...215/19);
- eIDAS - Регулатива (ЕУ) бр. 910/2014 на Европскиот парламент и на Советот од 23 јули 2014 година за електронски услуги за идентификација и доверливи услуги за електронски трансакции на внатрешниот пазар и укинување на Директивата 1999/93 / ЕЗ;
- Закони за лични податоци донесени во Република Северна Македонија и поврзаната ЕУ регулатива;
- Поврзани европски стандарди:
  - а) ETSI EN 319 401 Електронски потписи и инфраструктури (ESI); Општи барања за политика за даватели на доверливи услуги ;
  - б) ETSI EN 319 411-1 Електронски потписи и инфраструктури (ESI); Барања за политика и сигурност за давателите на доверливи услуги кои издаваат сертификати; Дел 1: Општи барања;
  - в) ETSI EN 319 411-2 Електронски потписи и инфраструктури (ESI); Барања за политика и сигурност за давателите на доверливи услуги кои издаваат сертификати; Дел 2: Барања за органи за сертификација за издавање квалификувани сертификати;
- Основни барања на CA / Browser Форумот,

Овие CP/CPS подлежат на македонските закони.

9.16. Останати одредби

9.16.1. Целосност на договорот

Не се применува.

9.16.2. Доделување

Сите субјекти кои работат според овие CP/CPS не можат да ги доделат своите права или обврски без претходна писмена согласност од КИБС. Освен ако не е поинаку определено во договор со страна, КИБС не дава известување за доделување.

9.16.3. Одвоивост на одредби

Во случај ако некој член или клаузула од овие CP/CPS се прогласат за неспроведливи од соодветен суд или од друг надлежен авторитет, останатиот дел од овие CP/CPS ќе остане во сила.

9.16.4. Спроведување (надоместок за адвокат и откажување од правата)

КИБС може да бара надомест на штета и адвокатски такси од страната за штети, загуби и трошоци поврзани со однесувањето на таа страна. Неуспехот на КИБС да спроведе одредба од овие CP/CPS не го одрекува правото на КИБС да ја спроведе истата одредба подоцна или правото да спроведе друга

одредба од овие CP/CPS. За да бидат во сила, одрекувањата мора да бидат во писмена форма и потпишани од КИБС.

9.16.5. Виша сила

Неисполнувањето на обврските што произлегуваат од CP/CPS и / или поврзаните документи не се смета за прекршување, доколку таквото неисполнување е предизвикано од Виша сила. Ниту една од страните нема да бара оштета или друг надомест од другите страни за доцнење или неисполнување на овие CP/CPS и / или поврзаните документи, предизвикани од Виша сила.

9.17. Други одредби

Не се применува.

Додаток А. Табела на кратенки и дефиниции

Табела на кратенки

Термин	Дефиниција
CA (ИС)	Издавач на сертификати
CP	Политика за сертификати
CP/CPS	Правила и постапки за издавање на квалификувани сертификати
CRL (РПС)	Регистар на поништени сертификати
CSR	Барање за потпишување сертификат
EBA	Европски банкарски орган
FIPS	Федерални стандарди за обработка на информации на САД
LRA (ЛРК)	Локана регистрациона канцеларија
NCA	Национален надлежен орган
NCP	Нормализирана политика за сертификати
NCP+	Проширена нормализирана политика за сертификати
OCSP	Протокол за електронско добивање на статусот на сертификат
OID	Предметен идентификатор, единствен код на предметен идентификатор
PDS	PKI Декларација
PIN	Личен идентификациски број
PKCS	Стандард за криптографски јавен клуч
PKI	Инфраструктура на јавен клуч
PMA	Тело за управување со политиката
PRCA	Примарен Издавач на коренски сертификати
QSCD	Средство за креирање квалификуван електронски потпис/печат
RA (РК)	Регистрациона канцеларија
RFC	Барање за забелешка
SSL	Протокол Secure Socket Layer
TSP	Давател на доверлива услуга

Дефиниции

Термин	Дефиниција
Администратор	Доверливо лице во организацијата на процесирачки центар, услужен центар или управуваниот PKI клиент, кое врши валидација и други ИС или РК функции.
Администраторски сертификат	Сертификат што му се издава на администраторот и кој може да се користи само за извршување на ИС или РК функции.
Напреден електронски печат	Електронски печат што ги исполнува следниве услови: • тој е единствено поврзан со креаторот на печатот; • тој е способен да го идентификува креаторот на печатот; • се креира со користење податоци за креирање на електронски печат што креаторот на печатот може, со високо ниво на доверба под своја контрола, да ги користи за креирање електронски печат; и тој е поврзан со податоците на кои се однесува, на таков начин што може да се детектира секоја последователна промена во податоците.
Напреден електронски потпис	Електронски потпис што ги исполнува следниве услови: • тој е единствено поврзан со потписникот; • тој е способен да го идентификува потписникот; • се креира со употреба на податоци за креирање електронски потпис така што потписникот може, со високо ниво на доверба, да ги користи под своја единствена контрола; и тој е поврзан со податоците потпишани со него, на таков начин што може да се детектира секоја последователна промена во податоците.

Термин	Дефиниција
Сертификат	Јавен клуч на корисник, заедно со некои други информации, кој е шифриран со приватниот клуч на телото за сертификација кое го издало, за да не може да се фалсификува.
Подносител на барање за сертификат/Барател на сертификат	Лице или организација што бара издавање на сертификат од ИС.
Барање за сертификат	Барање поднесено до ИС за издавање сертификат.
Синџир на сертификати	Подредена листа на сертификати која го содржи сертификатот на претплатникот - краен корисник и ИС сертификатите, а завршува со коренски сертификат.
Политика за сертификати (CP)	Именуван пакет правила што укажува на применливост на сертификат за одредена заедница и / или класа на примена со заеднички безбедносни барања.
Регистар на поништени сертификати (CRL)	Потпишан список што означува збир на сертификати што се поништени од Издавачот на сертификати.
Барање за потпишување сертификат (CSR)	Порака која го пренесува барањето за издавање сертификат.
Издавач на сертификати (ИС)	Орган овластен да креира и доделува сертификати.
Правила за издавање сертификати (CPS)	Правила за практиките што ги користи органот за сертификација при издавање, управување, поништување и обновување или сертификати со обновување на клучеви.
Фраза за проверка	Тајна фраза избрана од подносителот на барањето за сертификат за време на регистрирањето за сертификатот. Кога сертификатот ќе му биде издаден, подносителот на барањето за сертификат станува претплатник, и ИС или РК може да ја користи оваа фраза за да го автентицира претплатникот кога тој сака да го поништи или обнови претплатничкиот сертификат.
Ревизија за усогласеност	Периодична ревизија на која подлежи Центарот за обработка, Центарот за услуги или Управуваниот PKI клиент, за да се определи нивната усогласеност со PKI стандардите кои важат за нив.
Компромитирање	Прекршување (или претпоставено прекршување) на безбедносната политика, при кое може да се случи неовластено откривање или губење на контролата врз чувствителни информации. Во однос на приватните клучеви, компромитирање претставува губење, кражба, откривање, изменување, неовластено користење или друг вид на компромитирање на сигурноста на тој приватен клуч.
eIDAS	Регулатива на ЕУ бр. 910/2014 на Европскиот парламент и на Советот од 23 јули 2014 година за услуги за електронска идентификација и доверливи услуги за електронски трансакции на внатрешниот пазар и укинување на Директивата 1999/93 / ЕЗ.
Електронски потпис	Податоци во електронска форма кои се приложени или логички се поврзани со други електронски податоци, и кој потписникот го користи за потпишување.
Електронски печат	Податоци во електронска форма, кои се приложени или логично се поврзани со други податоци во електронска форма за да се обезбеди нивното потекло и интегритет.
Инцидентна ревизија/испитување	Ревизија или испитување од страна на КИБС кога КИБС има причина да верува дека некој ентитет не се придржува кон барањата на CP/CPS, инцидент или компромитирање поврзани со ентитетот, или дека настанала реална или потенцијална опасност за сигурноста на PKI од страна на ентитетот.
Општи правила и услови за користење квалификувани доверливи услуги	Обврзувачки документ во кој се наведени правилата и условите според кои физичко или правно лице дејствува како претплатник или како засегната страна, а КИБС ги обезбедува соодветните доверливи услуги.
Права на интелектуална сопственост	Права кои потпаѓаат под некое од следново: авторски права, патент, трговска тајна, заштитена марка и кои било други права на интелектуална сопственост.
Церемонија на генерирање клуч	Постапка со која се генерира пар клучеви на ИС или РК, неговиот приватен клуч се пренесува во криптографски модул, направена е резервна копија од неговиот приватен клуч и / или неговиот јавен клуч е сертифициран.
Складиште на КИБС	База на податоци на КИБС со сертификати и други релевантни информации на КИБС, достапни онлајн.

Термин	Дефиниција
Управуван PKI	Целосно интегрирана управувана PKI услуга на KIBSTrust која им овозможува на компаниите, клиенти на KIBSTrust да дистрибуираат сертификати на физички лица, како на пример, членови на персоналот, партнери, добавувачи и клиенти. Управуваниот PKI им овозможува на компаниите да ги обезбедат своите пораки или апликациите во електронската трговија.
Локално QSCD	USB PKI токен или PKI смарт картичка на QSCD.
Сертификат со долготрајна важност	Квалификуван сертификат кој е валиден 1 до 3 години.
Рачна автентикација	Процедура при која барањата за сертификати се разгледуваат и одобруваат рачно една по една, од страна на администраторот со користење на веб-базирана апликација.
MK-eIDAS	Закон за електронски документи, електронска идентификација и доверливи услуги. (Службен весник на Република Северна Македонија 101/19… 275/19).
Неверификувана претплатничка информација	Информација поднесена од барателот на сертификат до ИС или РК и вклучена во сертификат, а која не била потврдена од ИС или РК и за која релевантните ИС и РК не обезбедуваат други гаранции, освен дека информацијата била поднесена од подносителот на барањето за сертификат.
Неодрекување	Атрибут на комуникацијата кој обезбедува заштита на страна од : комуникација за која лажно се одрекува нејзиното потекло, се одрекува дека таа била поднесена или се одрекува нејзиното доставување. Одрекување на потеклото вклучува негирање дека комуникацијата потекнува од истиот извор како редослед од една или повеќе претходни пораки, дури и кога идентитетот поврзан со испраќачот е непознат. Забелешка: само судска одлука, арбитража или некој друг трибунал може во крајна мерка да спречат одрекување. На пример, дигитален потпис верификуван во врска со квалификуван сертификат може да обезбеди доказ во прилог на определувањето на неодрекувањето од страна на трибунал, но тоа само по себе не претставува неодрекување.
Исклучени (Офлајн) ИС	PRCA издавачки коренски ИС и други назначени ИС, кои се одржуваат исклучени (офлајн) од безбедносни причини, со цел да бидат заштитени од можни напади од натрапници преку мрежата. Овие ИС директно не потпишуваат сертификати на претплатници - крајни корисници.
Вклучени (Онлајн) ИС	ИС кои потпишуваат сертификати на претплатници - крајни корисници и се одржувани онлајн за да овозможат континуирани услуги на потпишување.
Протокол за онлајн статус на сертификат (OCSP)	Протокол со кој им се обезбедува на засегнатите страни информација за статусот на сертификатот во реално време.
OTP	Еднократна лозинка.
Оперативен период	Период што започнува на датумот и во времето на издавање на сертификатот (или на подоцнежен датум и време ако е така наведено во сертификатот), а завршува на датумот и во времето кога сертификатот истекува или е претходно поништен.
Учесник	Лице или организација што е КИБС, клиент, Издавач на сертификат, Регистрациона канцеларија, претплатник или засегната страна.
PKCS #10	Криптографски стандард на јавен клуч # 10, развиен од RSA Security Inc., кој дефинира структура за барање за потпишување сертификат.
PKCS #12	Криптографски стандард за јавен клуч # 12 развиен од RSA Security Inc., кој дефинира безбеден начин за трансфер на приватни клучеви.
Тело за управување со правилата и постапките на давателот на доверливи услуги (PMA)	Тело/група во рамките на КИБС одговорна за објавување на оваа политика.
Правила за практики	Правила за практиките што ги користи TSP при обезбедување на доверлива услуга.
Примарен коренски Издавач на сертификати (PRCA)	ИС што делува како коренски ИС и им издава сертификати на ИС кои му се потчинети.

Термин	Дефиниција
Приватен клуч	Клучот од парот клучеви што се чува во тајност од страна на носителот на клучот, и тој се користи за креирање квалификуван сертификат или за дешифрирање на електронски записи или датотеки што биле шифрирани со соодветниот јавен клуч.
Центар за обработка	Локацијата на КИБС што претставува безбеден објект за складирање, меѓу другото, и криптографските модули што се користат за издавање сертификати.
Јавен клуч	Клучот од парот на клучеви што може да биде јавно обелоденет од носителот на соодветниот приватен клуч и кој се користи од страна на засегнатата страна за да потврди квалификуван сертификат, креиран со соодветниот приватен клуч на носителот.
Инфраструктура на јавен клуч (PKI)	Архитектура, организација, техники, практики и процедури кои заеднички ги поддржуваат имплементацијата и функционирањето на криптографскиот систем на јавни клучеви базирани на сертификат. КИБС PKI се состои од системи кои соработуваат за обезбедување и имплементирање на криптиграфски систем за јавен клуч врз основа на сертификат.
Квалификуван електронски печат	Напреден електронски печат што е креиран од квалификуван уред за креирање електронски печати и се заснова на квалификуван сертификат за електронски печати.
Квалификуван електронски потпис	Напреден електронски потпис што е креиран од квалификуван уред за креирање електронски потпис и се заснова на квалификуван сертификат за електронски потпис.
Квалификуван сертификат	Квалификуван сертификат е сертификат издаден од ИС, кој е акредитиран и надгледуван од органи назначени од земја-членка на ЕУ.
Квалификуван сертификат за електронски потпис	Сертификат за електронски потписи, издаден од квалификуван давател на доверливи услуги кој ги исполнува условите утврдени во Анекс I на eIDAS.
Квалификуван сертификат за електронски печат	Сертификат за електронски печат, издаден од квалификуван давател на доверливи услуги кој и ги исполнува условите утврдени во Анекс III на eIDAS.
Средство за креирање квалификуван потпис/печат (QSCD)	Уред кој е одговорен за квалификување на дигитални потписи со употреба на специфичен хардвер и софтвер со што се гарантира дека единствено потписникот има контрола врз неговиот приватен клуч.
Давател на квалификувани доверливи услуги	Давател на доверливи услуги кој обезбедува една или повеќе квалификувани доверливи услуги и на кој му е доделен квалификуван статус од страна на надзорно тело.
Регистрациона канцеларија (РК)	Ентитет одобрен од ИС за да им помогне на барателите на сертификати при поднесување на барањата за сертификати и да ги одобри или одбие барањата за сертификати, да ги поништи сертификатите или да ги обнови сертификатите.
Засегната страна	Поединец или организација која делува потпирајќи се на сертификат и / или дигитален потпис.
Далечинско QSCD	Серверски базиран HSM што се користи за централно генерирање и употреба на претплатнички приватни клучеви.
Далечинска верификација на идентитет	Методот / процесот со кој претплатникот се идентификува преку сесија за видео повик и е еквивалентен на валидација со физичко присуство.
Коренски ИС	Орган за сертификација кој е на највисоко ниво во доменот на TSP и кој се користи за потпишување подредени ИС.
RSA	Криптографски систем за јавен клуч дизајниран од Ривест, Шамир и Аделман.
Таен удел	Дел од приватен клуч на ИС или дел од податоци за активирање што се потребни за да функционира приватниот клуч на ИС во рамките на аранжманот на тајни удели.
Поделба на тајни делови	Практика на разделување на приватниот клуч на издавачот на сертификати или податоци за активирање што се потребни за да функционира приватниот клуч на издавачот на сертификати со цел да се воспостави контрола од повеќе лица врз операциите на приватниот клуч на издавачот на сертификати, согласно овие CP/CPS дел 6.2.2.

Термин	Дефиниција
Secure Sockets Layer (SSL)	Метод на индустриски стандарди за заштита на веб комуникации развиен од Netscape Communications Corporation. SSL безбедносниот протокол обезбедува шифрирање на податоци, серверска автентикација, интегритет на пораките и опционално, автентикација на клиент за конекција на Протоколот за контрола на трансмисија/Интернет протоколот.
Подреден ИС (Sub CA)	Орган за сертификација чијшто сертификат е потпишан од Root ИС или друг.
Субјект	Предметот може да биде: - физичко лице; - физичко лице идентификувано дека е поврзано со правно лице; - правно лице (тоа може да биде организација или единица или оддел идентификуван дека е поврзана со организација);
Претплатник	Субјект што се претплатува кај давателот на доверливи услуги и кој е законски обврзан на сите обврски на претплатник.
Правила и услови	Договор кој се користи од ИС или РК за поставување на правилата и условите под кои физичкото лице или организацијата делуваат како претплатник или засегната страна.
Надзорно тело	Органот што е назначен од страна на земја-членка за извршување на надзорни активности на доверливите услуги и давателите на услуги според eIDAS
Доверлива услуга	Електронска услуга за: - креирање, верификација и валидација на дигитални потписи и сродни сертификати. - креирање, верификација и валидација на временски жигови и сродни сертификати. - регистрирана испорака и сродни сертификати. - креирање, верификација и валидација на сертификати за автентикација на веб-страници; или - зачувување на дигитални потписи или сертификати поврзани со тие услуги.
Давател на доверлива услуга	Ентитет кој обезбедува една или повеќе доверливи услуги.
Доверливо лице	Вработен, соработник под договор или консултант на ентитет во рамките на DigiCert PKI одговорен за управување со инфраструктурната сигурност на ентитетот, неговите производи, услуги, неговите простории и/или практики како што е поконкретно дефинирано во CP дел 5.2.1 .
Доверлива позиција	Позиции во DigiCert PKI ентитетот на кои мора да бидат поставени доверливи лица.
Сигурен и безбеден систем	Компјутерски хардвер, софтвер и процедури кои се логично безбедни од упади и погрешна употреба, обезбедуваат разумно ниво на достапност, доверливост и коректно функционирање, во разумна мерка се адекватни за извршување на наменетите функции и ја применуваат потребната безбедносна политика. Сигурен систем нужно не е доверлив систем, во смисла на класифицираната владина номенклатура.
Валиден сертификат	Сертификат што ја поминува постапката за валидација наведена во RFC 5280.
Период на валидност	Временскиот период измерен од датумот на издавање на сертификатот до датумот на истекување.

Крај на документот