Правила
за издавање на квалификувани сертификати

KIBSTrust Verba

Верзија 1.0

Датум на стапување во сила: 01.09.2020

11.48

КИБС АД Скопје

http://www.kibstrust.com

Правила за издавање квалификувани сертификати

Белешки за трговската марка

КИБС е регистрирана марка на КИБС АД Скопје. ADACOM е регистрирана марка на ADACOM SA. DigiCert, логото DigiCert и логото Checkmark се регистрирани трговски марки на DigiCert корпорацијата или нејзините филијали во САД и други земји. Други имиња може да бидат трговски марки на нивните сопственици.

Без ограничување на погоре заштитените права, освен онаму каде што е дозволено подолу, ниеден дел од оваа публикација не смее да се репродуцира, складира или воведе во систем од кој може да биде преземена, или да се пренесува, во која било форма или на кој било начин (електронски, механички, со фотокопирање, снимање или на друг начин), без претходна писмена дозвола од КИБС АД Скопје.

Без оглед на погоре наведеното, одбрена е репродукција и дистрибуција на Правилата за издавање квалификувани сертификати на неексклузивна основа и без надоместок за авторски права, под услов (i) горенаведеното известување за авторски права и почетните параграфи да бидат видливо прикажани на почетокот на секој примерок, и (ii) овој документ да биде точно репродуциран во целост, дополнет со измените на КИБС.

Барања за каква било друга дозвола за репродуцирање на овие Правила на КИБС за издавање квалификувани сертификати (како и барања за примероци од КИБС АД) мора да се адресираат на КИБС АД, Кузман Јосифовски Питу 1, 1000, Скопје, Република Северна Македонија, тел: +389 2 5513401, +389 2 3297401, e-mail: pma@kibstrust.com.

Историја на документот

верзија	датум	автор	цел на промената
1.0	01.09.2020	Лиле Гаговска Кристина Радомировиќ Кочовска	Правила за издавање сертификати според барањата на МК-eIDAS и eIDAS.

Содржина

1. ВОВЕД

Овој документ ги претставува Правилата за издавање квалификувани сертификати на КИБС (во понтамошниот текст како: Правила). Во него се наведени практиките што ги користи КИБС како давател на доверливи услуги (TSP) при обезбедување сертификациски услуги за квалификувани сертификати за електронски потписи и квалификувани сертификати за електронски печати во согласност со членовите 24, 29, 40, 55 од МК-eIDAS[1] и членовите 19, 24, 28, 38 и 45 од регулативата (ЕУ) бр. 910/2014 [eIDAS] и со посебните барања на Политиката за издавање сертификати (CP) на DigiCert.

CP на DigiCert е основен документ за политиката што ја уредува Инфраструктурата на јавни клучеви (во понатамошниот текст како: PKI) на DigiCert. Овој документ ги утврдува деловните, правните и техничките предуслови за одобрување, издавање, управување, користење, поништување и обновување на дигиталните сертификати во рамките на PKI на DigiCert и обезбедува поврзани доверливи услуги. Овие предуслови, наречени „PKI стандарди на DigiCert“, обезбедуваат заштита на сигурноста и интегритетот на DigiCert PKI и се однесуваат на сите учесници во DigiCert PKI и според тоа обезбедуваат потврда за подеднаква доверба низ целата DigiCert PKI. Повеќе информации поврзани со DigiCert PKI и стандардите на DigiCert PKI се достапни во CP[2].

КИБС има овластување над дел од DigiCert PKI наречен „Поддомен“ на DigiCert PKI. Поддоменот на КИБС вклучува ентитети кои се зависни од него, како што се неговите клиенти, претплатници и засегнати страни.

Во овие Правила се опишува како КИБС ги исполнува барањата во согласност со Регулативата (ЕУ) бр. 910/2014. Поконкретно, овие Правила ги опишуваат практиките што ги применува КИБС за:

- Сигурно управување со поврзаната инфраструктура која ја поддржува PKI на DigiCert, и
- Издавање, управување, поништување и обновување квалификувани сертификати како што е дефинирано во МК-eIDAS и Регулативата (ЕУ) бр. 910/2014.

Овие Правила се усогласени со RFC 3647 на Инженерскиот стручен тим за Интернет (Internet Engineering Task Force - IETF) за изготвување Политики за сертификати и Сертификациски практики.

1.1. Преглед

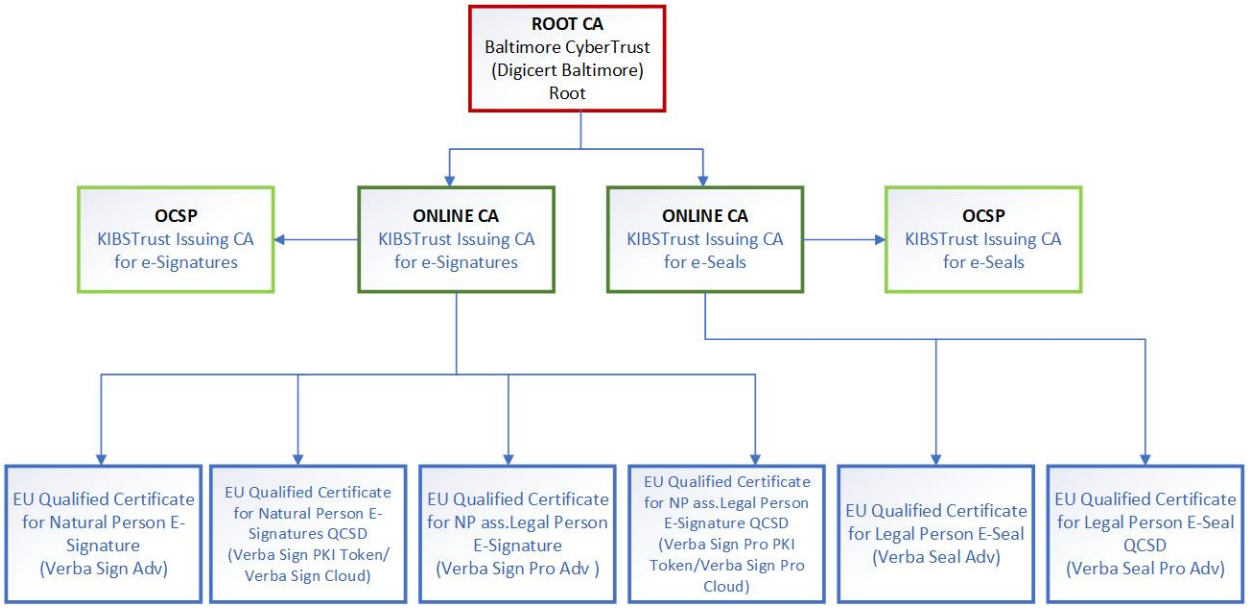
Овие Правила ги опишуваат практиките и процедурите што се користат за решавање на сите барања утврдени со МК-eIDAS и Регулативата (ЕУ) бр. 910/2014 за издавање, одржување и управување со животниот циклус на квалификувани сертификати за електронски потписи и квалификувани сертификати за електронски печати.

Овие практики 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.
- ETSI EN 319 411-1 Политики:
  - Политика за нормализиран сертификат (Normalized Certificate Policy (NCP))
  - Политика за нормализиран сертификат за употреба кога е неопходен безбеден уред за корисникот (extended Normalized Certificate Policy (NCP+))

КИБС тековно го користи следниот синџир на сертификати:

[1] Закон за електронски документи, електронска идентификација и доверливи услуги (Службен весник на РНМ 101/19, 215/19))
[2] Тековната верзија на DigiCert CP може да се најде на https://www.kibstrust.com/repository/cps



КИБС определи безбедни простории за сместување, меѓу другото на системи на ИС, вклучувајќи ги и криптографските модули кои ги чуваат приватните клучеви што се користат за издавање сертификати. КИБС делува како ИС во рамките на PKI на DigiCert и ги извршува сите услуги за животниот циклус на сертификатите за издавање, управување, поништување и обновување на квалификувани сертификати.

Овие Правила се особено применливи за:

- Издавачкиот ИС на КИБС кој издава квалификувани сертификати за електронски потписи и електронски печати.

Приватните ИС и другите хиерархии со кои управува КИБС, кои не се споменати во овој документ, се надвор од опсегот на овие Правила. Практиките кои се однесуваат на услугите обезбедени од други организации или услуги обезбедени од КИБС на други организации се надвор од опсегот на овие Правила.

ИС управувани од други организации, исто така, се надвор од опсегот на овие Правила.

КИБС ги објавува Правилата за издавање сертификати со цел да се придржува кон специфичните барања на политиката на важечкото законодавство или другите стандарди и барања во индустријата.

Општо, Правилата, исто така, ја регулираат употребата на PKI услугите на DigiCert кои се однесуваат на квалификувани сертификати во рамките на поддоменот на КИБС во рамките на PKI на DigiCert од страна на сите поединци и субјекти во рамките на поддоменот на КИБС (заеднички, учесници во поддоменот на КИБС).

КИБС нуди квалификувани сертификати во рамките на својот поддомен на PKI на DigiCert. Овие Правила опишуваат како КИБС ги исполнува барањата на CP и на Европската директива (European Directive Policies (EDP)) за квалификувани сертификати што ги издава во рамките на својот поддомен. На тој начин, Правилата, како единствен документ, ги опфаќаат практиките и процедурите во врска со издавање и управување со квалификуван сертификат обезбеден од КИБС.

КИБС може да објави Правила за издавање квалификувани сертификати кои се дополнителни на овие Правила, со цел да се исполнат специфичните барања на политика во однос на законодавство или други стандарди и барања во индустријата. Овие дополнителни практики за сертификати ќе им бидат ставени на располагање на претплатниците на сертификати издадени во рамките на дополнителните политики, како и на нивните засегнати страни.

Правилата се само една збирка од документи што се релевантни за поддоменот КИБС на DigiCert PKI. Овие останати документи вклучуваат:

- Дополнителни доверливи безбедносни и оперативни документи[3] што ги надополнуваат Политиката за сертификати и Правилата со обезбедување подетални барања, како што се:
    - Референтен прирачник за церемонијата на клучеви, кој детално ги презентира оперативните барања за управување со клучеви,
    - Политиката за физичка и просторна сигурност на КИБС, која ги поставува безбедносните принципи според кои се раководи инфраструктурата на КИБС,
    - Политика за сигурност на информатичкиот систем на КИБС, каде се наведени барањата за инфраструктура на информатичкиот систем со цел да функционира безбедно и според поврзаните законски и договорни барања,
    - Политика за управување со криптографски клучеви на КИБС, која ги претставува деталните оперативните барања за управување со клучеви.
- Одредби и услови на КИБС за употреба на квалификувани доверливи услуги. Овие општи Одредби и услови ги обврзуваат клиентите, претплатниците и засегнатите страни на КИБС. Меѓу другото, Одредбите и условите опфаќаат широк спектар на комерцијални услови или посебни услови за доверливи услуги на KIBS.

Правилата се однесуваат на овие дополнителни документи за посебни, детални практики за имплементирање на политиките на КИБС, ADACOM и DigiCert, каде што вклучувајќи ги спецификите во Правилата може да се компромитира сигурноста на подредениот ИС на КИБС, подредениот ИС на ADACOM на DigiCert PKI.

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

КИБС нуди сертификати за веб-страници (безбедни серверски идентификации и глобални серверски идентификации) во посебна соработка со DigiCert, а не во рамките на КИБС ИС. За оваа деловна активност се применуваат Правилата на DigiCert, објавени на https://www.digicert.com/legal-repository/.

1.2. Име и идентификација на документ

Овој документ ги претставува Правилата за издавање квалификувани сертификати. DigiCert PKI сертификатите содржат вредности на предметен идентификатор (OID) кои соодветствуваат на соодветна DigiCert PKI класа на сертификати. Поради тоа, КИБС на овие Правила нема доделено вредност на предметен идентификатор.

Предметните идентификатори на квалификуваните сертификати се користат во согласност со делот 7.1.6.

1.3. PKI учесници

1.3.1. Издавачи на сертификати

Терминот Издавач на сертификати (во понатамошниот текст како: ИС) се однесува на сите ентитети овластени да издаваат сертификати за јавен клуч во рамките на DigiCert PKI. Терминот ИС ја опфаќа и поткатегоријата на издавачи наречени Примарни издавачи на сертификати (во понатамошниот текст како: PCA, (Primary Certification Authority - PCA). PCA делуваат како корени на домени. Секој PCA е ентитет на DigiCert. Подредени на PCA се Издавачите на сертификати кои издаваат сертификати на претплатници како крајни корисници или на други ИС. КИБС е издавачки ИС кој управува со квалификувани сертификати.

DigiCert ги поседува и управува со GTE Cybertrust Global Root, Baltimore Cybertrust Root, Cybertrust Global Root CA и Verizon Global Root CA. Во ограничени околности, овие коренски ИС се користат за издавање на вкрстени сертификати на надворешни трети страни кои работат со свои PKI.

КИБС ги применува овие Правила врз основа на своите внатрешни барања, кои се во согласност со сите барања на DigiCert PKI CP и ADACOM Правилата.

[3] Иако овие документи не се јавно достапни, нивните спецификации се вклучени во годишниот WebTrust извештај на DigiCert за Издавачи на сертификати и можат да се стават на располагање во согласност со посебен Договор.

Еден DigiCert PKI ИС кој технички е надвор од трите хиерархии под секој од PCA е Издавачот на сертификати за безбеден сервер (Secure Server Certification Authority). Овој ИС нема надреден ИС, како корен или PCA. Издавачот на сертификати за безбеден сервер делува како свој сопствен корен и си има издадено на себе само-потпишан коренски сертификат. Тој, исто така, издава сертификати и на клиентите - крајни корисници. На тој начин, хиерархијата на безбеден сервер се состои само од ИС за безбеден сервер.

Во овие Правила, упатувањата на ИС се однесуваат на ИС кои го опфаќаат синџирот на сертификати на квалификуваните сертификати на КИБС. Поконкретно, овие се:

Коренски ИС

c = IE
o = Baltimore
ou = CyberTrust
cn= Baltimore CyberTrust Root
Serial Number: 020000b9
Subject Key Identifier: e59d5930824758ccacfa085436867b3ab5044df0
Thumbprint: d4de20d05e66fc53fe1a50882c78db2852cae474

Издавачки ИС за е-потписи

c = MK
o = KIBS AD Skopje
ou = Class 2 DigiCert PKI Platform Individual Subscriber CA
Organizational Unit = KIBS AD Trust Services
organizationIdentifier = NTRMK-5529581
cn = KIBSTrust Issuing CA for e-Signatures
Serial Number: 0f5f12d3fc361edeb611c5ad2f2dd0b2
Subject Key Identifier: 548aca06bbb185e3f03400f9277f12c6f8d75c51
Thumbprint: 826c4721c72b97a72bdaa74ad13aedb152b4fbe5

Издавачки ИС за е-печати

c = MK
o = KIBS AD Skopje
ou = Class 2 DigiCert PKI Platform Individual Subscriber CA
ou = KIBS AD Trust Services
organizationIdentifier = NTRMK-5529581
cn = KIBSTrust Issuing CA for e-Seals
Serial Number: 0e99c387276568e05f4be5ca9d1b7adb
Subject Key Identifier: 2d122df5f15b7d1cb7dd43e898bfcd8b0fe72907
Thumbprint: b5a5e3d7e4320c266f0e3347fb232b603f97795c

КИБС ИС сертификатите се издаваат во согласност со следниве политики за сертификати:

- Digicert OID 2.16.840.1.114412.5.2 (non-smime-class2)
- OID 0.4.0.194112.1.0 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural(0)
- OID 0.4.0.194112.1.1 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal(1)
- OID 0.4.0.194112.1.2 Itu-t(0) identified-organization(4) etsi(0) qualified-certificatepolicies(194112) policy-identifiers(1) qcp-natural-qscd (2)
- OID 0.4.0.194112.1.3 itu-t(0) identified-organization(4) etsi(0) qualified-certificatepolicies(194112) policy-identifiers(1) qcp-legal-qscd (3)
- OID 0.4.0.2042.1.1 itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp(1)
- OID 0.4.0.2042.1.2 itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus(2)

1.3.2. Регистрациски канцеларии

Регистрациска канцеларија (во понатаммошниот текст како: РК) е ентитет кој врши идентификација и автентикација на подносителите на барања за сертификат за сертификати за крајните корисници, иницира или проследува барања за поништување на сертификати за сертификати за крајните корисници и одобрува барања за обновување на сертификати или повторно издавање клучеви, во име на КИБС ИС. КИБС делува како РК за квалификуваните сертификати што ги издава.

КИБС може да склучи договорни односи со една или повеќе трети страни, со цел да изврши дел од обврските на РК, особено во врска со потврдување на претплатникот. Во овој случај, третата страна претставува Локална регистрациска канцеларија (ЛРК). ЛРК ги извршува своите обврски во целосна согласност со овие Правила, соодветните планови за потврдување и условите од Договорот на ЛРК, потпишан помеѓу ЛРК и КИБС.

КИБС, исто така, може да склучи договорен однос со една или повеќе трети страни, со цел да ги извршат сите обврски на РК. Во овој случај, третата страна станува РК и ги извршува своите обврски во целосна согласност со овие Правила, соодветните планови за потврдување и условите од Договорот на РК, потпишан помеѓу РК и КИБС.

Потврдување на дел од доменот на адресата за е-пошта не може да се делегира на трета страна и се потврдува само од РК на Издавачот на сертификати.

Пред да започне со операциите поврзани со ЛРК, КИБС обучува овластени вработени во ЛРК за процесот на потврдување и процедурите за сигурност. Потоа, КИБС годишно врши повторна обука на овластени вработени во ЛРК.

КИБС врши годишни ревизии на операциите и процедурите на РК / ЛРК со цел да обезбеди усогласеност со овие Правила, плановите за потврдување и со Договорот со РК / ЛРК.

1.3.3. Локални регистрациски канцеларии

Локална регистрациска канцеларија е ентитет кој врши идентификација и потврдување на претплатници и субјекти и првична проверка на нивните соодветни документи за издавање, обновување пар клучеви и поништување сертификати. Односот помеѓу ЛРК и РК е опишан во договорот на ЛРК и вклучува, но не е ограничен на следново:

- Целосни детали за овластените вработени во ЛРК, кои ќе ги извршуваат обврските и активностите на ЛРК;
- Обврска на ЛРК да добие годишна обука на овластените вработени во ЛРК од ADACOM 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 работник на ЛРК да користи документи издадени од КИБС РК за да обезбеди безбедна комуникација меѓу двете страни;
- Обврска на ЛРК да ги обработува барањата на претплатникот исклучиво преку овластените вработени во ЛРК.

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

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

1.3.4. Претплатници

Претплатници во рамките на DigiCert PKI се сите крајни корисници (вклучувајќи ентитети) на сертификати издадени од DigiCert PKI ИС. Претплатник е ентитет што е именуван како претплатник-краен корисник на сертификат. Претплатници-крајни корисници може да бидат лица или организации. Во однос на квалификуваните сертификати, во согласност со македонскиот закон, претплатници-крајни корисници можат да бидат само правно квалификувани лица или ентитети.

Во некои случаи, сертификатите се издаваат директно на лицата или на ентитетите за нивна сопствена употреба. Меѓутоа, често се јавуваат и случаи во кои страната која бара сертификат е различна од субјектот за кој се однесуваат документите. На пример, некоја организација може да бара сертификати за своите вработени за да им овозможи тие да ја застапуваат организацијата во електронските трансакции/деловното работење. Во такви случаи, ентитетот што се претплатува за издавање на сертификатите (т.е. плаќа за нив, или се претплатува за специфична услуга) е различен од ентитетот кој е субјект на сертификатот (вообичаено, носител/имател на акредитив (збир на информации што вклучува идентификација и доказ за идентификација што се користи за да се добие пристап до одредени ресурси)).

Во овие Правила се користат два различни термини за да се направи разлика помеѓу овие две улоги:

- **„Претплатник“** е ентитет 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 чија автентичност се потврдува кога ќе се презентира сертификатот.

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

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:
  a) самото физичко лице;
  b) физичко лице со овластување да го застапува субјектот; или
  c) секој ентитет со кој е поврзано физичкото лице.
- За да се побара сертификат за правно лице, претплатникот е:
  a) 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 сертификат. Локацијата на точката на дистрибуција на CRL детално е дадена во рамките на сертификатот.

1.3.6. Други учесници

Не е пропишано со одредба.

1.4. Користење на сертификатите

Дигитален сертификат е форматиран податок кој криптографски го 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.

Квалификуваните сертификати за електронски потпис обично ги користат поединците за да потпишат и шифрираат е-пошта и за целите на автентикација, под услов употребата поинаку да не е забранета со закон, од овие Правила или за други намени, под услов употребата поинаку да не е забранета со закон, според овие Правила, Одредбите и условите и сите договори со претплатниците.

Квалификувани сертификати на КИБС за електронски печати се издаваат на организации по автентикација дека организацијата легално постои и дека другите атрибути на организацијата вклучени во сертификатот

се автентицирани. Квалификуван сертификат за електронски печат обично се користи за да го обезбеди интегритетот и потеклото на податоците со кои се поврзува, или за други намени, под услов употребата поинаку да не е забранета со закон, со овие Правила, Правилата и условите и какви било договори со претплатници.

1.4.1. Дозволена употреба на сертификати

1.4.1.1. Сертификати издадени за електронски потпис

Сертификатите се усогласени со NCP и QCP-n. Сертификатите издадени според овие барања имаат за цел да поддржат квалификувани електронски потписи без употреба на уред за креирање квалификуван потпис (QSCD), како што е дефинирано во член 3 (28) од МК-eIDAS и член 3 (11) од Регулативата (ЕУ) бр. 910/2014.

Сертификати се усогласени со NCP + и QCP-n-qscd. Сертификатите издадени според овие барања имаат за цел да поддржат квалификувани електронски потписи со употреба на уред за креирање квалификуван потпис (QSCD) како што е дефинирано во член 3 (29) од МК-eIDAS и член 3 (12) од Регулативата (ЕУ) бр. 910/2014.

1.4.1.2. Сертификати издадени за електронски печати

Сертификатите се усогласени со NCP и QCP-l. Сертификатите издадени според овие барања имаат за цел да поддржат квалификувани електронски печати без употреба на уред за креирање квалификуван потпис (QSCD) како што е дефинирано во член 3 (32) од МК-eIDAS и член 3 (26) од Регулативата (ЕУ) бр. 910/2014.

Сертификатите се усогласени со NCP + и QCP-n-qscd. Сертификатите издадени според овие барања имаат за цел да поддржат квалификувани електронски печати со употреба на уред за креирање квалификуван потпис (QSCD) како што е дефинирано во член 3 (33) од МК-eIDAS и член 3 (27) од Регулативата (ЕУ) бр. 910/2014.

1.4.2. Забранета употреба на сертификати

Сертификатите на КИБС не се дизајнирани, наменети или одобрени за користење или за препродажба како контролна опрема во ризични околности или за користење во услови кои бараат неопходна безбедносна работа, како што е функционирањето на нуклеарни постројки, навигациски или комуникациски системи за воздушна пловидба, системи за контрола на воздушниот сообраќај или системи за контрола на оружје, каде што пропустот може да доведе директно до смрт, лична повреда или сериозна штета во однос на заштита на околината.

Квалификуваните сертификати се наменети за користење од страна на клиентите и нема да се користат како сертификати за сервери, ниту пак како ИС сертификати.

ИС сертификатите не смеат да се користат за никакви функции, освен за функциите на ИС.

DigiCert и КИБС периодично ги обновуваат своите Посредничките сертификати (Intermediate CAs) со нов пар клучеви (rekey). Апликациите подготвени од трети страни или платформи кои имаат инкорпорирано Посреднички ИС како коренски сертификат може да не функционираат како што е предвидено со дизајнот откако Посредничкиот ИС ќе бидат обновен со нов пар клучеви. Поради ова, КИБС не го прпорачува користењето на Посреднички сертификати како коренски сертификати и препорачува Посредничките сертификати да не се поставуваат во апликациите и/или платформите како коренски сертификати. КИБС препорачува користење на РСА корени како коренски сертификати.

1.5. Администрирање на Правилата

1.5.1. Организација која го администрира документот

Овие Правила и релевантните документи што се наведени овде ги одржува Одбор за управување со политики на КИБС како давател на доверливи услуги (PMA - Policy Management Authority), со кој 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

Претседател на Одбор за управување со политики на КИБС ДДУ
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 барања за поништување сертификат, види параграф 4.9.3.

1.5.3. Лице кое ја определува соодветноста на овие Правила со СР

Организацијата идентификувана во дел 1.5.1 е одговорна за утврдување на соодветноста и применливоста на овие Правила врз основа на резултатите и препораките од ревизиите за усогласеност.

1.5.4. Процедури за одобрување на Правилата

Одобрување на овие Правила и последователните измени се прават од страна на КИБС РМА и Авторитетот за управување со политики на ADACOM. Измените се во форма на документ што содржи изменета форма на Правилата 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 наведени или спротивставени одредби на референтната верзија на Правилата.

1.6. Дефиниции и кратенки

Види Додаток А за табела на кратенки и дефиниции.

1.7. Референци

Име на политика/ прирачник/барање/стандард	**Локација на изворниот документ**
Политика на сертифицирање на DigiCert	https://pki.adacom.com/repository
Верзија на DigiCert Правила за издавање сертификати	https://www.digicert.com/legal-repository/
Основни барања за Издавачот на сертификати/ Browser Forum (CAB Форум) за издавање и управување со јавно доверливи сертификати	https://cabforum.org/baseline-requirements-document/
Mozilla Root Store Policy v.2.7	https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
MK-eIDAS – Закон за електронски документи, електронска идентификација и доверливи услуги.	https://mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/zakon_za_elektronski_dokumenti_eid_i_doverlivi_uslugi.pdf

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 интернет пазарот и укинување на Директивата 1999/93/EC (eIDAS Regulation)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
ETSI стандарди: ETSI EN 319 401 Електронски потписи и инфраструктури (ESI); Општи барања на политика за даватели на доверливи услуги. ETSI EN 319 411-1 Електронски потписи и инфраструктури (ESI); Барања за политика и сигурност на давателите на доверливи услуги кои издаваат сертификати; Дел 1: Општи барања. ETSI EN 319 411-2 Електронски потписи и инфраструктури (ESI); Барања за политика и сигурност на давателите на доверливи услуги кои издаваат сертификати; Дел 2: Барања за политика за издавачи на сертификати кои издаваат квалификувани сертификати.	https://www.etsi.org/

2. ОДГОВОРНОСТИ ПОВРЗАНИ СО ОБЈАВУВАЊЕ И СМЕСТУВАЊЕ

2.1. Складишта

КИБС е одговорен за функциите на складиштето за своите сопствени ИС сертификати. КИБС ги објавува претплатничките сертификати за крајните корисници во складиштето во согласност со дел 2.2 од овие Правила.

По поништување на претплатнички сертификат за крајниот корисник, КИБС го објавува поништувањето во складиштето и издава Регистар на поништени сертификати (во понатамошниот текст како: РПС) и овозможува OCSP услуги во согласност со одредбите од Правилата.

КИБС треба да обезбеди неговото складиште да биде достапно 24 часа на ден, 7 дена неделно, со минимум достапност од 99,00% годишно, со предвидено време на престанок што не надминува 0,3% 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 информатичка услуга да трае подолго од горенаведеното време.

2.2. Објавување на информации за сертификатот

КИБС одржува веб-базирано складиште кое им овозможува на засегнатите страни онлајн да побараат 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.

КИБС постојано ќе ја објавува на својата веб страница, во делот складиште, најновата верзија од:

- DigiCert PKI CP,
- Овие правила,
- Одредби и услови за употреба на квалификувани сертификати,

- Резултати од ревизија,
- Политики на осигурување,
- Профили на сертификати,
- Сертификати, вклучувајќи коренски и издавачки ИС,
- Регистар на поништени сертификати,
- Пребарување на сертификат,
- Политика на приватност.

2.2.1. Политики на објавување и известување

Овие Правила на КИБС се објавени во КИБС складиштето за јавно информирање на:

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

Правилата на КИБС се објавуваат заедно со датумите на спроведување не помалку од 30 дена пред да стапат во сила.

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

Види дел 9.3.1 од овие Правила.

2.3. Време и периодичност на објавување

Информации за статусот на сертификатот се објавуваат во согласност со одредбите на овие Правила.

Види дел 2.2.1 од тековните Правила за ажурирања на овие Правила. 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 од веб страницата на КИБС се јавно достапни информации. Пристап до такавата информација со опција само за преглед не е ограничена. КИБС бара лицата да се согласат со Одредбите и условите како услов за пристап до сертификатите, до информациите за статусот на сертификатите или до РПС. 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.

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

Сертификатите на КИБС ИС содржат X.501 карактеристични имиња (Distinguished Names) во полињата за Издавач (Issuer) и Субјект (Subject). Типовите на имиња доделени на ИС и на претплатникот се опишани во соодветната документација за профиот на сертификатот објавени во КИБС складиштето.

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 употреба на псевдоними.

3.1.4. Правила за интерпретирање различни именски форми

Не е пропишано со одредба.

3.1.5. Единственост на имињата

КИБС потврдува дека карактеристичните имиња на субјектот 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 на Серискиот број во полето Субјект на сертификатот. За електронските печати тоа е обезбедено со вредноста на атрибутот на Организацискиот 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 субјектот и / или претплатникот. КИБС може да одбие да издаде сертификат по 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.

3.2.1. Метод за докажување сопственост врз приватниот клуч

Подносителот на барање за сертификат мора да покаже дека со право го поседува приватниот клуч кој кореспондира со јавниот клуч што ќе биде наведен во сертификатот.

Начинот на докажување на сопственоста врз приватен клуч е PKCS#10, друга криптографска еквивалентна демонстрација или друг одобрен метод од КИБС и DigiCert. Ова барање не се применува кога парот клучеви се генерира од КИБС ИС во име на претплатникот, на пример, кога клучевите кои претходно се генерирани се постават на 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 кој е субјект и / или 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 менаџерот (точки 1 и 2):

- 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 овој налог за набавка се проверуваат со податоците за тоа правно лице зачувани во Централниот регистар, вклучително и името на менаџерот.
    - За правно лице регистрирано надвор од Македонија, потребно е да се донесе сертификат од трговскиот регистар или слично тело кое има право да потврди дека претплатникот е регистриран како правно лице во домицилната земја. Сертификатот се доставува во

оригинал, а документот преведен од овластен судски преведувач на македонски или англиски јазик.

- Потврда за идентитетот на **менаџерот на правното лице**, кој го потпишува овој налог за набавка, се врши на следниов начин:
    - За правно лице регистрирано во Македонија, се приложува нотарски заверен примерок од сертифициран образец за потпис, каде е заведен своерачниот потпис на менаџерот, или
    - За правно лице регистрирано надвор од Македонија: со доставување соодветен образец, каде поврзувањето на банкарската сметка со своерачниот потпис на менаџерлот е заверена, или
    - Менаџерот го потпишува овој налог пред нотар, за што ќе биде приложен нотарски сертификат, или
    - Менаџерот приложува документ за лична идентификација и го потпишува овој налог пред службеникот за ЛРК / РК.

или

- 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 параграф (1) погоре, преку е-пошта до ЛРК на КИБС, дигитално потпишана со квалификуван сертификат, издаден од квалификуван давател на доверливи услуги, во согласност со Регулативата eIDAS.

Во случај кога трето лице ќе се поднесе барање за издавање на квалификуван сертификат, треба да се приложи примерок од полномошно од законскиот застапник за тоа трето лице или кој било друг еквивалентен документ, кој демонстрира дека третото лице може да се потпише во име на законскиот 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/ или субјектот на квалификуван сертификат се верификува согласно сегашното законодавство, и се изведува на еден од следниве начини:

- Со физичко присуство на крајниот корисник на сертификатот во ЛРК / РК на KIBS ИС, на адресата објавена на https://www.kibstrust.mk/mk-MK/Home/Contact, каде што:
    - покажува документ за лична идентификација (лична карта или пасош),
    - го потпишува налогот за набавка 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 овој налог за набавка за кој нотарот ќе направи нотарска заверка, а потоа
    - треба да ја испрати целата документација по пошта на адресата на РК на КИБС ИС објавена на https://www.kibstrust.mk/en-GB/Home/Contact/, или
    - да овласти друго лице кое ќе ја достави целата документација потпишана од претплатникот и носителот на сертификатот (и кој ќе може да го подигне PKI токенот (ако има писмо за овластување за тип на сертификат со **PKI-токен**)). Писмото за овластување како образец е подготвено од КИБС ИС и може да се преземе од линкот:

      https://www.kibstrust.mk/Storage/Dokumenti/PolnomosnoEN.pdf.
- со еквивалент на физичко присуство преку далечинска верификација на идентитетот со кој физичкото лице се идентификува преку видео сесија во живо од овластен вработен во ЛРК. Физичкото лице треба да обезбеди доказ за неговата/нејзината лична карта или пасош издаден од која било друга земја, со оглед на тоа што документот 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 претплатник кој е правно лице:

1. со физичко присуство на физичкото лице поврзано со правното лице кое им ги доставува на РК на КИБС или овластениот работник на ЛРК следниве документи:

- Доказ за идентитетот на претплатникот [полно име, датум и место на раѓање] врз основа на личната карта или пасош издаден од која било друга земја, 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. Потврдата за личната карта или пасошот мора да биде на македонски и англиски јазик. Во случај на лична карта или пасош издаден на јазик различен од горенаведените јазици, потврдата мора да биде придружена со официјален превод на еден од горенаведените јазици;
- Доказ за поврзаноста на физичкото лице со правното лице во согласност со националните или други применливи практики за идентификација;
- Писмено и прописно потпишано одобрување од правното и физичкото лице дека атрибутите на субјектот, исто така, ја идентификуваат таквата организација.

2. со испраќање на гореспоменатите документи со прописно сертифицирани или нотарски заверени примероци преку курир или поштенска услуга до канцеларијата на РК на КИБС. Сертификација или нотарско заверување на примероците од документи се обезбедува од нотар, правен советник или друг службеник со исто ниво на овластување во рамките на јурисдикцијата на претплатникот / субјектот.

3. со физичко присуство на соодветно овластен претставник на претплатникот, доколку претставникот е прописно овластен од претплатникот да го застапува.

4. 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 параграф 1 погоре, преку е-пошта до ЛРК на КИБС, дигитално потпишан со квалификуван сертификат издаден од квалификуван давател на доверлива услуга, во согласност со Регулативата за eIDAS.

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 (OE)
- Која било друга информација означена како непотврдена во сертификатот (како на пр. „Наслов“ за упатување на работната позиција).

3.2.5. Потврдување на овластување

Секогаш кога во сертификатот името на некое лице е поврзано со име на организација на таков начин за да покаже поврзаност на лицето или негово овластување да делува во име на организацијата , КИБС РК:

- потврдува дека организацијата постои преку користење на најмалку еден сервис за протврдување 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 им одобрува сертификати на лица поврзани со неа или потврдува преку телефон, поштенска пратка со потврда

или во слична процедура на организацијата, дека лицето има овластување да делува во име на организацијата.

3.2.6. Критериуми на интероперабилност

Не е пропишано со одредба.

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 парот клучеви" (re-key).

Општо земено, со „Обнова на пар клучеви" и "Обновување" обично се опишуваат како "Обновување на сертификат", фокусирајќи се на фактот дека стариот сертификат е заменет со нов сертификат, а не се потенцира дали се генерира нов пар на клучеви или не. За квалификуваните сертификати оваа дистинкција не е значајна, бидејќи секогаш се генерира нов пар клучеви како дел од процесот на КИБС за замена на сертификат на краен корисник претплатник.

3.3.1. Идентификација и автентикација за рутинско обновување на пар клучеви

Не е пропишано со одредба.

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 Правила.

3.4. Идентификација и автентикација на барање за поништување

Пред да поништи сертификат, КИБС проверува дали поништувањето е побарано од претплатникот на сертификатот.

Прифатливите процедури за автентицирање 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 е точна.
- 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 безбедносно 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, по пошта или по курир.

Администраторите на КИБС се овластени побараат поништување сертификати на претплатници - крајни корисници во рамките на поддоменот на КИБС. КИБС пред да му дозволи на администраторот да ја изведе функцијата на поништување или друга процедура одобрена од DigiCert PKI, го утврдува идентитетот на администраторот преку контрола на пристапот со користење на SSL автентикација и автентикација на клиентот.

4. ОПЕРИРАЊЕ СО 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 кое е субјект на сертификатот, доколку е полнолетно и од правен аспект има основа за тоа според македонскиот закон.

4.1.2. Процес на регистрирање и одговорности

Претплатници на сертификати за крајни корисници

Претплатниците на сертификат за краен корисник се согласуваат со Одредбите 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 Одредбите и условите во врска со користењето на сертификатот;
- Пополнување и потпишување на барање за сертификат 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;
- Докажување дека поседуваат и/или имаат ексклузивна контрола на приватниот клуч кој соодветствува со јавниот клуч.

Записите кои се чуваат согласно дел 5.4.1 од овие Правила, вклучуваат информации користени за потврдување на автентичноста на идентитетот на подносителот на барањето за на сертификат (вклучувајќи го и референтниот број на документот употребен за автентикација) како и запис за прифатени Одредби и услови во електронска форма, каде Претплатникот се согласува, помеѓу другото, ИС да чува евиденција за информациите кои се користени при регистрацијата и ги дава сите согласности што се потребни според Документот за политиката на ETSI.

Во случај на барање за обнова на пар клучеви:

- Се доставуваат сите промени во условите во Одредбите и условите што ќе следат по претходната или повторната регистрација, и
- Документацијата што се задржува согласно дел 5.5.1 од Правилата, исто така, ја вклучува согласноста на Претплатникот за која било од тие промени.

4.1.2.1. ИС и РК Сертификати

ADACOM, како филијала на DigiCert, може да издава дополнителни РК сертификати за издавање на квалифиувани сертификати.

4.2. Обработка на барањето за сертификат

4.2.1. Извршување на функциите на идентификација и автентикација

КИБС РК врши идентификација и автентикација на сите потребни информации за претплатникот а) со физичко присуство, или б) на оддалеченост со квалификуван сертификат, или в) со употреба на метод еквивалентен на физичко присуство, во согласност со Дел 3.2.

Ако ЛРК помага во верификацијата, тогаш ЛРК мора да креира и да одржува досиеја доволни за да утврди дека ги извршила своите потребни задачи за верификација и му го соопштува на ADACOM завршувањето на таквите задачи. Откако ќе заврши верификацијата, службеникот за ЛРК / РК го означува налогот за набавка како потврден.

4.2.2. Одобрување или одбивање на барањата за сертификат

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

- Успешна е идентификацијата и автентикацијата на сите потребни информации за претплатникот, во согласност со дел 3.2 од овие Правила.
- Уплатен е надоместокот за сертификатот.

КИБС РК 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 од овие Правила, или
- Претплатникот не ги доставил потребните документи на барање,
- Претплатникот не одговорил на забелешките во рокот определен за тоа, или
- Не е уплатен надоместокот за сертификатот, или
- РК оцени дека издавањето на сертификатот на претплатникот може да и донесе лоша репутација на DigiCert PKI.

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 се додека не се одбие, издаде или автоматски не истече во рок од 30 дена. Истечените налози за набавка на сертификат автоматски се бришат од базата на податоци на корисници 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 (налог за набавка) од страна на КИБС или по приемот на барањето на РК да го издаде сертификатот. КИБС го креира и го издава сертификатот на подносителот на барањето за сертификат врз основа на податоците во барањето, по одобрување на таквото барање за сертификат.

Квалификуваните сертификати генерирани и издадени во согласност со 4.2.1 од СР се издаваат од страна на системи кои користат заштита против фалсификување, која е детално опишана во делот 6 од СР и обезбедува со сигурност сертификатот да биде издаден на барателот на сертификат, или на барателот за обновување или креирање нов пар клучеви, кој го поседува приватниот клуч што кореспондира со јавниот клуч во сертификатот кој што треба да се издаде.

Издавањето на сертификат согласно дел 3.3 од овие Правила, во техничка смисла, значи обновување на парот клучеви, а не ресертификација на претходно сертифициран јавен клуч.

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

КИБС, директно, или преку РК или со електронска порака, го известува претплатникот дека му го одобрил барањето за сертификат. Известувањето содржи информација од каде претплатникот може да го преземе сертификатот.

4.4. Прифаќање сертификат

4.4.1. Однесување кое означува прифаќање на сертификатот

Сертификатот се смета за прифатен кога:

- Генерирањето на сертификатот 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 директориумот за сертификати за издадените сертификати на КИБС ИС.

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

Не е пропишано со одредба.

4.5. Користење на парот клучеви и 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 ќе се користи во согласност со Правилата и условите на КИБС ИС, со условите на DigiCert PKI CP и овие Правила. Користењето на сертификатот мора да биде конзистентно со полето за користење на клучот (KeyUsage) вклучено во сертификатот.

Претплатниците треба да ги заштитат своите приватни клучеви од неовластена употреба и да престанат да ги употребуваат своите приватни клучеви по истекот на важноста или поништувањето на сертификатот.

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

Засегнатите страни треба да се согласни со условите во Одредбите 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:

- дека користењето на сертификат е соодветно за одредена цел, а истовремено не е забранета или на друг начин ограничена со овие Правила. КИБС не е одговорен за проценката на соодветноста за користењето на сертификатот.
- дека сертификатот се користи согласно наведеното во полето за употреба на клучот (KeyUsage) од сертификатот
- статусот на сертификатот и на останатите сертификати во синџирот на сертификати. Ако некој од сертификатите во синџирот бил поништен, единствено засегнатата страна е одговорна да истражува дали довербата во дигиталниот потпис изведен од сертификатот на претплатникот - краен корисник, пред поништувањето на сертификат во Синџирот на сертификати е разумен. Ризикот од укажување доверба е исклучиво на засегнатата страна.

Под претпоставка дека користењето на сертификатот е соодветно, засегнатите страни ќе применуваат соодветен софтвер и/или хардвер за да извршат проверка на дигиталниот потпис или други криптографски операции што сакаат да ги изведат, како услов за доверба во сертификатите поврзани со 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 е пропишано со одредба.

4.6.1. Околности за обновување на сертификатот

Не е пропишано со одредба.

4.6.2. Кој може да побара обновување

Не е пропишано со одредба.

4.6.3. Обработка на барањата за обновување сертификат

Не е пропишано со одредба.

4.6.4. Известување на претплатникот за издавање на нов сертификат

Не е пропишано со одредба.

4.6.5. Однесување кое означува прифаќање на обновен сертификат

Не е пропишано со одредба.

4.6.6. Објавување на обновување сертификат од страна на ИС

Не е пропишано со одредба.

4.6.7. Известување до други ентитети за издавање сертификат од страна на ИС

Не е пропишано со одредба.

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

Обновен сертификат со нов пар клучеви е барањето 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 обнова на сертификатот со нов пар клучеви најмалку 30 дена пред истекот на важноста на постојниот сертификат на претплатникот.

4.7.2. Кој може да побара сертифицирање на нов јавен клуч

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

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

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

Во однос на одредбите од дел 3.3.1, по обновување на сертификат со нов пар клучеви на ваков начин, и за барем алтернативни случаи на следни обновување клучеви потоа, идентитетот на претплатникот повторно ќе се потврди во согласност со барањата утврдени во овие Правилата за проверка на првичното барање за сертификат.

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

Не е пропишано со одредба.

4.8. Изменување на сертификат

4.8.1. Околности за изменување на сертификат

Изменувањето на сертификат се однесува на барање 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 РК 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 изменетот 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 сертификати

4.9.1. Околности за поништување

Претплатничкиот договор на КИБС им дава обврска или/и право на страните да бараат поништување на сертификат. Само во подолу наведените околности сертификатот за претплатник - краен корисник ќе биде поништен од страна на КИБС (или од претплатникот) и објавен во РПС.

Сертификатот за претплатник - краен корисник се поништува ако:

- КИБС или претплатникот имаат причина да веруваат или да се сомневаат дека се случило компромитирање на приватниот клуч на претплатникот,
- КИБС има причина да верува дека претплатникот прекршил материјална обврска, изјава или гаранција од применливите Обврски и услови,
- Претплатничкиот договор со претплатникот е истечен,
- КИБС има причина да верува дека сертификатот е издаден спротивно на процедурите од овие Правила, сертификатот е издаден 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 има причина да верува дека некој од материјалните факти во барањето за сертификат е погрешен,
- КИБС утврди дека материјалниот предуслов за издавање на сертификатот не е задоволен ниту поништен,
- Во случај претплатникот да ја изгуби правната квалификуваност, да биде прогласен за исчезнат или мртов, имајќи предвид дека сертификатот е во секој случај непреносliв,
- Во случај на судска одлука без право на жалба која наложува поништување или откажување на сертификатот,
- Во случај кога приватниот клуч на ИС е компромитиран,

- Информациите во сертификатот, освен не-верификуваните информации за претплатникот, се неточни или се промениле, или околностите во кои сертификатот е издаден се промениле (т.е. во случај кога вработен добил сертификат, но не е веќе вработен во таа компанија),
- Идентитетот на претплатникот не е повторно успешно верификуван во согласност со дел 6.3.2 од овие Правила,
- Претплатникот не ги извршил обврските за плаќање во определените временски рамки, или
- Понатамошното користење на тој сертификат е штетно за КИБС или за DigiCert PKI.

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

- Природата и бројот на примените поплаки;
- Идентитетот на оној што ги искажал поплаките;
- 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.

Согласно претплатничкиот договор, претплатникот – краен корисник е должен веднаш да го извести КИБС 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 тоа 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

4.9.3.1. Процедура за барање за поништување на сертификат за претплатник - краен корисник

Претплатникот – краен корисник кој бара поништување треба да упати барање до КИБС за поништување на еден од следните начини: преку онлајн услуга за поништување, по електронска пошта на helpdesk@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.

Комуникацијата за вакво барање за поништување мора да биде во согласност со 3.4 од овие Правила.

4.9.3.2. Процедура за барање за поништување на ИС или РК сертификат

КИБС може да иницира поништување на ИС или РК сертификат.

4.9.4. Грејс период за барање за поништување

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

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

КИБС презема комерцијално разумни чекори за да ги обработи барањата за поништување без одлагање и во секој случај максималното одложување од моментот кога КИБС ќе добие барање за поништување во согласност со дел 4.9.3.1, и 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-пошта.

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 можат да го проверат статусот на сертификатот со користење на веб-базираното складиште на КИБС. ИС ќе им обезбеди на засегнатите страни информација како да го пронајдат соодветниот РПС, веб-базираното складиште 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 овластување.

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

4.9.7. Интервали на издавање на РПС

CRL за сертификатите за претплатници- крајни корисници се издаваат на секои 15 минути. 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 запишан во CRL му истече важноста, тој може да биде отстранет во следно издадениот РПС, по истекот на важноста на сертификатот.

4.9.8. Максимално доцнење на РПС

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. Покрај објавувањето на РПС, КИБС обезбедува информации за статусот на сертификат и преку функциите за пребарување во складиштето на КИБС. Информации за статусот на сертификатот се достапни на: https://e-shop.kibstrust.mk/raforms/VerbaSearchCert.aspx

Онлајн поништување на сертификати не е достапно.

Максималното одложување помеѓу потврдата за поништување сертификат да стане важечка и вистинската промена на информациите за статусот на овој сертификат што им се става на располагање на засегнатите страни е најмногу 60 минути, но практично е 15 минути. Ако барањето за поништување бара однапред поништување (на пр. Планиран престанок на субјектот од неговите / нејзините должности на одреден датум), тогаш закажаниот 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 повика. Ако засегнатата страна не го провери статусот на сертификатот преку консултирање на OCSP или најновиот релевантен РПС, тогаш засегнатата страна ќе го провери статусот на сертификатот консултирајќи го складиштето на КИБС.

4.9.11. Други достапни форми на огласување за поништување

Не е пропишано со одредба.

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 бил компромитиран.

4.9.13. Околности за суспендирање

КИБС не обезбедува услуги на суспендирање за сертификатите што ги издава.

4.9.14. Кој може да побара суспендирање?

Не е пропишано со одредба.

4.9.15. Процедура за барање за суспендирање

Не е пропишано со одредба.

4.9.16. Ограничувања на периодот на суспензија

Не е пропишано со одредба.

4.10. Услуги во врска со статусот на сертификатите

4.10.1. Оперативни карактеристики

Статусот на јавните сертификати е достапен преку CRL и од OCSP респондерот.

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 година со предвиден прекин кој не надминува 0,4% годишно.

4.10.3. Опционални карактеристики

Не е пропишано со одредба.

4.11. Крај на претплатата

Претплатникот може да ја прекине претплатата за сертификат на КИБС:

- со истекувањето на важноста на сертификатот;
- со поништување на сертификатот пред истекувањето на неговата важност, без да се изврши замена на сертификатот.

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

Не е пропишано со одредба. ИС Приватните клучеви и приватните клучеви на претплатниците- крајни корисници не се даваат на чување кај трето лице.

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

Не е пропишано со одредба.

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

Не е пропишано со одредба.

5. КОНТРОЛИ НА ОБЈЕКТИ, УПРАВУВАЊЕ И ОПЕРАТИВНИ КОНТРОЛИ

5.1. Физички контроли

КИБС има имплементирано множество од безбедносни политики, кои ги поддржуваат барањата за сигурност од овие Правила. Придржувањето кон овие политики е вклучено во условите за надзор на КИБС опишани во дел 8. Безбедносните политики на КИБС содржат чувствителни податоци за сигурноста и се стават на располагање само по потпишување на договор со КИБС. Преглед на овие услови е даден подолу.

5.1.1. Локација и конструкција

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

ИС операциите ги извршува ADACOM SA. ADACOM како партнер DigiCert за пружање услуги одржува локации за складирање за оправување по откажување на системот за своите ИС операции. Локацијата за оправување по откажување на системот на ADACOM е во согласност со безбедносните барања за складирање надвор од деловните простории, кои се наведени во „План за привремено надворешно складиште за криптографски материјали за оправување по откажување на системот на ADACOM“ и „План за оправување по откажување на системот на ADACOM“.

5.1.2. Физички пристап

КИБС РК системите се заштитени со пет 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.

КИБС ги користи системите на ADACOM ИС кои се заштитени со седум нивоа на физичка заштита, при што потребно е да се има пристап најнапред до пониското ниво за да се добие дозвола за пристап до повисокото ниво.

Прогресивно ограничувачките привилегии за физички пристап го контролираат пристапот до секое ниво. Чувствителните оперативни активности на ИС, каква било активност поврзана со животниот циклус во сертификацискиот процес, како што се автентикација, верификација и издавање, се случуваат во рамките на многу рестриктивни физички нивоа. За влез во секое ниво потребна е бец картичка за пристап на вработениот. Физичкиот пристап автоматски се запишува и се снима на видео. Некои нивоа применуваат индивидуална контрола на пристапот со истовремено користење и на картичка и на биометрика (два фактори на идентификација). На непридружуван персонал, вклучувајќи вработени без овластување за пристап или посетители не им е дозволен влез во таквите обезбедени простори.

5.1.3. Електрична енергија и климатизација

Безбедните простории на КИБС се опремени со примарни и резервни:

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

5.1.4. Изложеност на вода

КИБС има преземено разумни мерки на претпазливост со цел да го минимизираат негативното влијание од изложување на системите 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 за надзор, архивски информации или резервни копии на податоци се складирани во рамките на просториите на КИБС и во безбедни згради 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 и електромагнетни бранови).

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 нормалните барања на КИБС за исфрлање отпад.

5.1.8. Резервни копии (бекап) надвор од деловните простории

КИБС врши рутински (бекап) - резервни копии на клучните системски податоци, податоците од ревизорски траги и другите чувствителни информации. Медиумите со резервни копии се чуваат надвор од просториите на физички безбеден начин.

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,
- персонал кој работи на криптографски деловни операции,
- персонал кој е задолжен за сигурност,
- персонал задолжен за администрација на системот,
- назначен инженерскиот 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 Правила.

На лицата со договор и консултантите кои имаат пристап или ја контролираат автентикацијата и криптографските операции, дозволено им е да ги извршуваат овие операции само во придружба и директно надгледување од доверливи луѓе 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 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 бараат ангажирање на повеќе доверливи лица.

Овие внатрешни контролни процедури се дизајнирани за да обезбедат дека се потребни минимум две доверливи лица за физички или логички пристап до уредот. Пристапот до криптографскиот хардвер на издавачот е строго спроведен 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 е активиран со оперативните клучеви, се спроведуваат понатамошните контроли за да се одржи поделен 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 бараат 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 5.3.1. од овие Правила.

КИБС, откако ќе утврди дека лицата стекнале доверлив статус, им дава одобрување за работа во соодветниот оддел, 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.

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):

- потврдување 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 на просторот за складирање;
- постапување со информациите и барањата на претплатниците;
- генерирање, издавање или поништување на ИС сертификат.

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 во целост и на задоволителен начин. Проверки на биографските податоци за доверливите лица, се вршат најмалку на 5 години.

5.3.1. Квалификации и искуство

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 да ги извршуваат своите идни работни обврски целосно и на задоволителен начин.

5.3.2. Процедури за проверка на биографијата

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

- проверка на претходните вработувања и професионални референци, доколку постојат,
- потврда на највисокиот или најрелевантниот степен на образование што е стекнат,
- потврда за неосудуваност.

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:

- 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 во зависност од видот, големината и зачестеноста на однесувањето до кое е дојдено 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 веднаш по вработувањето или обуката ја врши на самото работно место што е им е потребна за да ги извршуваат своите работни обврски целосно и на задоволителен начин. 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.

5.3.4. Услови и период на повторна обука

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

5.3.5. Период и редослед на ротирање на работните места

Не е пропишано со одредба

5.3.6. Санкции за неовластени дејствија

За неовластени дејствија и други прекршувања на политиките и процедурите на КИБС се преземаат соодветни дисциплински мерки. Дисциплинските дејствија 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 кои што 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 од овие Правила, 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 целосно и на задоволителен начин.

5.4. Процедури за ревизорска трага (Audit logging Procedures)

5.4.1. Видови настани што се евидентираат

ADACOM ги евидентира, мануелно или автоматски, следниве значајни настани:

- Настани од управувањето со животниот циклус на клучевите на ИС, вклучувајќи :
    - Генерирање клучеви, резервна копија, складирање, обновување, архивирање и уништување,
    - Настани поврзани со управување на животниот циклус на криптографските уреди.
- Настани од управувањето со животниот циклус на ИС сертификатите и претплатничките сертификати, кои вклучуваат:
    - Барања за издавање сертификати, обновување и поништување,
    - Успешна или неуспешна обработка на барањата,
    - Генерирање и издавање сертификати и РПС.
- Настани поврзани со сигурноста, кои вклучуваат:
    - Успешни или неуспешни обиди за пристап до PKI системот,
    - PKI и безбедносни системски дејствија спроведени од страна на персоналот на ADACOM,
    - Безбедносно чувствителни документи или записи што се прочитани, напишани или избришани,
    - Промени на безбедносниот профил,
    - Испади на системот, откажување на хардверот и други аномалии,
    - Активности поврзани со мрежната бариера (firewall) и мрежниот насочувач (рутер),
    - Влез/излез на посетители во просториите на ИС.

КИБС рачно или автоматски, ги евидентира следните значајни настани:

- Евиденција за информациите од барањата за сертификати во РК, вклучувајќи ги:
    - Видот на документот/ите за идентификација презентирани од подносителто на барањето за сертификат,
    - Записот од единствените идентификациски податоци, бројки или комбинација од двете во документот (на пример, број од лична карта на барателот на сертификат) или документи за идентификација, доколку е применливо,
    - Идентитетот на субјектот што го прифаќа барањето,
    - Методот што е применет за потврдување на валидноста на документите за идентификација, доколку има,
    - Име на ИС кој го прима или РК која го поднесува брањето.
- Настани од животниот циклус на претплатникот на сертификат, вклучувајќи:
    - Барање за издавање на сертификат, негова обнова, обнова на нов пар клучеви и поништување,
    - Успешна или неуспешна обработка на барањата,
    - Генерирање и издавање на сертификати.
- Настани поврзани со сигурност, вклучувајќи:
    - Успешни или неуспешни обиди за пристап до системот,
    - Безбедносни системски активности извршени од персоналот на КИБС,
    - Читање, запишување или бришење на чувствителни фајлови или записи од аспект на сигурност,
    - Безбедносни промени на профили,

- Системски испади, нефункционирање на хардверот и други аномалии,
- Активност на мрежна бариера (firewall) и мрежен насочувач (рутер),
- Влез/излез на посетители во просториите на РК.

Записите во евиденцијата ги вклучува следниве елементи:

- Датум и време на влез,
- Сериски или редоследен број на внесување, за автоматски запис,
- Идентитет на ентитетот што прави внесување,
- Вид на внесување.

5.4.2. Интервал на преглед на ревизорски траги

Ревизорската трага се прави најмалку еднаш неделно во однос на значајните безбедносни или оперативни настани. Покрај тоа, КИБС ги прегледува своите ревизорски траги на сомнителните или невообичаени активности, како одговор на тревоги што се појавуваат заради неправилности или инциденти во рамки на системите на КИБС и РК.

Обработката на ревизорската трага се состои од прегледување на ревизорските траги и документацијата на сите значајни настани во прегледот на ревизорската трага. Прегледите на ревизорската трага опфаќаат верификација дека во евиденцијата не е интервенирано неовластено, како и увид во сите записи во евиденцијата и испитување на какви било тревоги или неправилности во записите. Покрај тоа, се документираат и сите дејствија што се преземаат врз основа на прегледите на ревизорските траги.

5.4.3. Период на зачувување на ревизорските траги

Ревизорските траги се зачувуваат на локацијата најмалку триесет (30) дена по обработката, а потоа се архивираат во согласност со дел 5.5.2.

5.4.4. Заштита на ревизорските траги

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

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

Резервна копија на промените во 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)

Автоматизирани ревизорски податоци се генерираат и се зачувуваат на ниво на апликација, мрежа и оперативен систем.

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 физичкото лице, организацијата, уредот или апликацијата што го предизвикала тој настан.

5.4.8. Проценка за ранливост

Настаните во процесот на контролата се евидентираат делумно и заради надгледување на ранливоста на системот. Логичката проценка за ранливост во сигурноста (во понатамошниот текст како: ЛПРБ) се извршува, прегледува и проверува преку испитување на овие следени настани. Овие ЛПРБ се базираат на автоматско евидентирање на податоците во реално време и се изведуваат на дневна, месечна и годишна основа. Податоците од годишната ЛПРБ претставуваат влезни податоци за годишната контрола на сообразност на ентитетот.

5.5. Архивирање на записите

5.5.1. Видови записи кои се архивираат

КИБС ИС ги архивира:

- Сите податоци од контролата 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 како на пример, информации за барања за поништување, креирање нов пар клучеви и обновување.

КИБС ја чува следнава документација што се однесува на идентитетот на претплатниците, а во врска со барањата за квалификувани сертификати:

- Видовите на документи поднесени од подносителите на барања за сертификати, во врска со нивните барања за сертификати.
- Записот за единствени идентификациски податоци, броеви (пр. број на пасош, број на лична карта на подносителот на барањето за сертификат) на документите за идентификација, ако е применливо,
- Идентитетот на ентитетот што го прима и прифаќа барањето за сертификат,
- Планот за валидација во кој се прикажани методите што се користат за валидација на документите за идентификација.

Покрај тоа, КИБС задржува евиденција за локацијата на складирање на барањата за сертификати и од документите за идентификација.

5.5.2. Период на чување во архивата

Документацијата поврзана со квалификуван сертификат се чува најмалку десет (10) години по датумот на поништување или истекот на важноста на конкретниот квалификуван сертификат.

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 разгледување, 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 Правила.

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

КИБС прави целосни резервни електронски архиви на своите издадени сертификати дневно и неделно. Копии од документацијата во хартиена форма се чуваат со користење на безбедни простории во деловните простории и надвор од нив.

5.5.5. Барања за временски печат на документацијата

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

5.5.6. Систем за архивирање

Системите за архивирање на КИБС се интерни.

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 повторно ќе се постават.

5.6. Промена на клучеви

Парот на клучеви на КИБС ИС се повлекува од употреба на крајот на нивниот максимален животен циклус, согласно овие Правила. 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.

Пред истекот на сертификатот на ИС сертификат за надреден ИС, се активираат процедури за промена на клучеви со цел да се овозможи полесен премин за субјектите во рамките на хиерархијата на надредениот ИС од стариот ИС пар клучеви кон нов(и) ИС пар(ови) клучеви. Процесот на промена на КИБС ИС клучевите бара:

- Надредениот ИС да престане да издава нови подредени ИС сертификати најдоцна 60 дена пред даден момент („Датум за престанок на издавање"), при што остатокот од животниот циклус на надредениот ИС пар клучеви е еднаков на периодот на важност на одобрениот сертификат за специфичен(и) тип(ови) на сертификати што се издаваат од страна на подредени ИС во хиерархијата на надредените ИС.
- По успешната валидација на барањата на подредениот ИС (или претплатник- краен корисник) сертификат, барањата што се примени после „Датумот за престанок на издавање" ќе бидат потпишани со новиот ИС пар на клучеви.

Надредениот ИС продолжува да издава CRL потпишани со оригиналниот приватен клуч на Надредениот ИС сè до истекот на датумот на последниот сертификат што е издаден со користење на оригиналниот пар клучеви.

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 деловната зграда и се расположливи во случај на компромитирање и кризни ситуации и тоа: податоци од барањата за сертификати, податоци од контролата, евиденција од базата на податоци за сите издадени сертификати. Сигурносна копија на ИС приватните клучеви се генерира и се одржува во согласност со дел 6.2.4 СР. ADACOM одржува сигурносни копии од гореспомнатите ИС информации за своите сопствени ИС.

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 ADACOM ИС, инфраструктурата на ADACOM или приватниот клуч на КИБС ИС, се применуваат процедурите за Реакција на компромитирање на клуч од страна на Тимот за справување со безбедносен инцидент (во понатамошниот текст како: ASIRT) на ADACOM. Овој тим, во кој се вклучени вработени лица од сигурноста, криптографските деловни операции, персоналот од производните услуги и други претставници на менаџментот на ADACOM, ја проценува ситуацијата, прави акциски план и го спроведува акцискиот план со одобрение од страна на извршниот менаџмент на ADACOM.

Ако 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 4.4.9 од овие Правила,
- Се вложуваат комерцијално разумни напори за да се достави дополнителна информација за поништувањето на сите засегнати DigiCert PKI учесници, и

- ИС генерира нов пар клучеви во согласност со дел 4.7 од овие Правила, освен кога се укинува ИС во согласност со дел 4.9 од овие Правила.

5.7.4. Способност за продолжување на деловните активности по кризна ситуација

5.7.4.1. DigiCert

DigiCert има имплементирано локација за оporавување по откажување на системот поставена на оддалеченост поголема од 1600 км од главните безбедни простории на DigiCert. DigiCert има развиено, применето и тестирано план за оporавување по откажување на системот за да ги ублажи ефектите од какви било природни катастрофи или катастрофи предизвикани од човечки фактор. Овој план редовно се тестира, верификува и надградува за да биде оперативен во случај на откажување на системот.

Деталните планови за оporавувањето од откажување на системот имаат за цел да се насочат кон повторно ставање во функција на услугите на информатичките системи и клучните деловни активности. На локацијата на DigiCert за оporавување по откажување на системот има поставено заштита за физичка сигурност и оперативни контроли потребни според Водичот за барањата за сигурност и надзор на DigiCert за да обезбеди безбедна и здрава оперативна поставеност на сигурносните копии.

Во случај на природна катастрофа или катастрофа предизвикана од човечки фактор заради која е потребен прекин на операциите од DigiCert примарните постројки, се активира процесот за оporавување по откажување на системот од страна на Тимот за делување во итни ситуации (во понатамошниот текст како: SERT) на DigiCert.

DigiCert има капацитет повторно да ги воспостави или да ги поврати неопходните операции во рок од дваесет и четири (24) часа по откажување на системот со поддршка барем на следниве функции:

- Издавање сертификати,
- Поништување сертификати,
- Објавување на информации за поништување, и
- Обезбедување на информации за повторно добивање клучеви за Клиентите - Претпријатија кои користат MPKI менаџер за клучеви.

Базата на податоци за оporавување по откажување на системот на DigiCert редовно се синхронизира со базата на податоци од производството, со временски рокови наведени во Водичот за предуслови за сигурност и надзор. Опремата за оporавување по откажување на системот на DigiCert е обезбедена со заштити за физичка сигурност која можат да се спореди со нивоата за физичка сигурност наведени во дел 5.1.2 од овие Правила.

Планот за оporавување по откажување на системот на DigiCert е дизајниран на начин за да обезбеди потполно оporавување во рок од една седмица од откажувањето на системот што настанало во примарните простории на DigiCert. DigiCert ја тестира својата опрема во своите примарни простории за да ги поддржи ИС/РК функциите што би следеле по сите кризни ситуации, освен голема катастрофа која што би ги ставила надвор од функција сите постројки на таа локација. Резултатите од таквите тестови се прегледуваат и се чуваат за цели на надзор и планирање. До колку е тоа возможно, операциите што е можно поскоро се обновуваат на примарната локација на DigiCert после поголема катастрофа.

DigiCert одржува резервен хардвер и сигурносни копии на своите ИС и на инфраструктурните системски софтвери во своите постројки за оporавување по откажување на системот. Покрај тоа, ИС приватните клучеви резервно се чуваат и одржуваат за цели на оporавување по откажување на системот во согласност со дел 6.2.4. од овие Правила.

DigiCert одржува сигурносна копија од значајните ИС информации за DigiCert ИС, како и за ИС на сервисните центри и клиентите - претпријатија, во рамките на поддоментот на DigiCert. Таквите информации вклучуваат, но не се и ограничени на: податоците од барањата за сертификати, податоците од надзорот (дел 5.4) и документацијата од базата на податоци за сите сертификати што се издадени.

5.7.4.2. ADACOM

ADACOM има развиено, имплементирано и тестирано план за оporавување по откажување на системот со цел да ги ублажи последиците од какви било природни катастрофи или катастрофи предизвикани од

човечки фактор. Овој план редовно се тестира, верификува и надградува за да биде оперативен во случај на откажување на системот.

Деталните планови за оporавување по откажување на системот имаат за цел да се насочат кон повторно ставање во функција на информатичките системи и клучните деловни активности.

Во случај на природна катастрофа или катастрофа предизвикана од човечки фактор заради која е потребен привремен или траен прекин на операциите од примарната локација на ADACOM, се активира процесот за оporавување по откажување на системот од страна на одговорниот тим на ADACOM.

ADACOM има капацитет повторно да ги воспостави или да ги поврати операциите со врвен приоритет, поддршката на функциите за поништување на сертификати и објавување на информации за поништување. ADACOM има опрема за оporавување по откажување на системот која е заштитена со физичка сигурносна заштита соодветна со нивоата на физичка заштита дефинирани во делот 5.1.1 на Правилата.

Планот за надминување на катастрофи на ADACOM е креиран за да обезбеди целосно оporавување по откажување на системот која настанала на примарната локација на ADACOM. ADACOM ја тестира својата опрема на примарната локација способна за да даде поддршка за извршување на ИС/РК функциите непосредно после кое било откажувањето на системот, освен катастрофа од големи размери по која целиот објект останал неоперабилен. Кога е тоа возможно, се продолжува со операциите на примарната локација на ADACOM во најбрз можен рок после голема катастрофа.

ADACOM чува резервни копии на своите ИС системи и инфраструктурните системски софтвери на безбедна локација оддалечена од главните простории.

Дополнително на тоа, за приватните ИС клучеви направена е резервна копија која е одржувана за потребите на оporавување по откажување на системот во согласност со делот 6.2.4 од Правилата. Поконкретно, резервното складирање е извршено во согласност со „Планот за оporавување по откажување на системот на ADACOM за привремено складирање на криптографски материјали на безбедна локација надвор од главните простории", кој ќе обезбеди продолжување на работните процеси на некој подоцнежен датум.

ADACOM, исто така, одржува резервно складирање на друга локација на важни ИС информации за ADACOM ИС. Овие информации вклучуваат, но не се ограничени на: податоци за барање на сертификат, податоци од контрола (согласно делот 4.5 од Правилата), и евиденција од базата на податоци за сите издадени сертификати.

5.7.4.3. КИБС

КИБС има развиено, имплементирано и тестирано план за оporавување по откажување на системот за да ги ублажи ефектите од кој било вид природна или катастрофа предизвикана од човечки фактор. Овој план редовно се тестира, верификува и ажурира за да биде во функција во случај на катастрофа.

Детални планови за надминување на откажувањето на системот се воспоставени за да се изврши обновување на услугите на информатичките системи и клучните деловни функции.

Во случај на природна или катастрофа предизвикана од човечки фактор која бара привремено или трајно прекинување на работењето од примарната локација на КИБС, процесот за оporавување по откажување на системот на КИБС е иницран од одговорниот тим на КИБС.

КИБС има капацитет за обновување или закрепнување на операциите, со највисок приоритет, поддршка за функциите на поништување на сертификати и објавување на информации за поништување. Опремата за оporавување од нарушено функционирање на КИБС е заштитена со заштити со физичко обезбедување, споредлива со нивоата за физичка сигурност, наведени во делот 1 5.1.1 од Правилата.

Планот за оporавување по откажување на системот на КИБС е дизајниран да обезбеди целосно оporавување по откажување на системот што се случила на примарната локација на КИБС. КИБС ја тестира својата опрема на својата примарна локација за да ги поддржи функциите на ИС / РК по сите, освен голема катастрофа што ќе го направи целиот објект нефункционален. Онаму каде е можно, операциите се продолжуваат на примарната локација на КИБС што е можно поскоро по големата катастрофа.

КИБС одржува резервни копии од својот ИС и софтверот на инфраструктурниот систем на безбедна локација надвор од деловните простории.

Поктај тоа, ИС приватните клучеви резервно се чуваат и одржуваат за цели на опоравување по откажување на системот во согласност со дел 6.2.4. од овие Правила. Поточно, се прават резервни копии од нив, во согласност со документот на КИБС „Управување со резервна копија“, кој ќе овозможи продолжување на деловната активност подоцна.

КИБС, исто така, одржува резервни копии од важни ИС информации за КИБС ИС. Ваквите информации вклучуваат, но не се ограничени на: податоци за барањата за сертификати, податоци за контролата (според делот 4.5 од Правилата) и евиденција за базата на податоци за сите издадени сертификати.

5.8. Прекин на дејноста на ИС или РК

Во случај кога е неопходно КИБС ИС да ги прекине активностите, КИБС ќе направи разумни комерцијални напори однапред да ги извести претплатниците, засегнатите страни и другите засегнати ентитети за таквиот прекин на ИС. Доколку е потребно ИС да престане да ја извршува дејноста, КИБС ќе го активира документираниот „План за прекинување на активностите на давателот на доверливи услуги” за да го минимизира дисконтинуитетот кај клиентите, претплатниците и засегнатите страни. Овој план за прекинување на активностите се однесува на следново:

- Доставување известување до страните засегнати со прекинувањето, како што се претплатници, засегнати страни и клиенти информирајќи ги за статусот на ИС,
- Поднесување на трошоците за таквото известување,
- Поништување на сертификатот издаден на ИС,
- Чување на архивите и документацијата на ИС во периодот што е предвиден во овие Правила,
- Продолжување на услугите на поддршка на претплатниците и клиентите,
- Продолжување на услугите на поништување, како што е издавање на CRL или одржување на услугата за онлајн проверка на статусот,
- Поништување на неистечени непоништени сертификати на претплатниците - крајни корисници и подредени ИС, доколку е неопходно,
- Рефундирање (доколку е потребно) на претплатниците чии неистечени непоништени сертификати се поништуваат во рамките на планот за прекинување или обезбедување, или друга алтернатива, на издавање на сертификат како замена, од страна на ИС што ќе ја наследи дејноста,
- Дислокација на приватниот клуч на ИС и хардверските токени што го содржат тој приватен клуч,
- Одредбите што се потребни за пренесување на ИС услугите на ИС што ги продолжува активностите, и
- Доставување на известување до Македонската надлежна институција.

Во случај кога е неопходно КИБС ИС да ги прекине сите активностите, КИБС дополнително ќе ги направи сите неопходни чекори согласно соодветниот Македонски закон. Ова вклучува, но не се ограничува на предавање на архивите и документацијата на КИБС ИС на друг давател на сертификациски услуги за квалификувани сертификати, во временски период предвиден со закон.

6. КОНТРОЛИ НА ТЕХНИЧКАТА СИГУРНОСТ

6.1. Генерирање и инсталирање на пар клучеви

6.1.1. Генерирање на пар клучеви

За КИБС ИС, генерирањето на парот клучеви, нивното складирање и потоа употребата се изведува од страна на ADACOM S.A., со употреба на криптографски модули кои ги задоволуваат барањата на FIPS 140-2 ниво 3. Генерирањето на ИС пар клучеви се изведува од страна на повеќе претходно избрани, обучени и доверливи лица користејќи доверливи системи и процеси кои обезбедуваат сигурност и потребна криптографска јачина за генерираните клучеви.

Сите парови на клучеви на ИС се генерираат со претходно планирана церемонија на генерирање клучеви, во согласност со условите на Референтниот водич за церемонија на генерирање клучеви, Корисничкиот водич за алатки за управување со ИС клучеви и Водичот за услови за сигурност и надзор на DigiCert. 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 надзор и пребарување во временски период што се смета за соодветен од страна на менаџментот на ADACOM.

Генерирањето на парови клучеви на КИБС РК генерално се изведува од страна на КИБС со користење на сертифициран криптографски модул CC EAL 4+ и FIPS 140-2 ниво 3. Генерирањето на РК пар клучеви се изведува од повеќе претходно избрани, обучени и доверливи лица користејќи доверливи системи и процеси кои обезбедуваат сигурност и потребна криптографска јачина за генерираните клучеви.

Генерирањето на парот клучеви за претплатникот - краен корисник се изведува од страна на претплатникот.

6.1.2. Доставување на приватниот клуч на претплатникот

Парот клучеви за претплатникот - краен корисник се генерира од страна на претплатникот - краен корисник, така што доставувањето на приватниот клуч на претплатникот не се применува.

6.1.3. Доставување на јавниот клуч на Издавачот на сертификати

Претплатниците - крајни корисници и РК 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).

6.1.4. Доставување на ИС јавниот клуч на засегнатите страни

КИБС ги става ИС Сертификатите за DigiCert PCA и за своите коренски ИС на располагање на претплатниците и засегнатите страни преку нивно вклучување во софтверот за веб прелистување. Кога новите PCA и коренски ИС сертификати ќе бидат генерирани, DigiCert им ги доставува тие нови сертификати на производителите на прелистувачи за да ги вклучат во новите изданија и ажурирања.

КИБС вообичаено им обезбедува целосен синџир на сертификати (вклучувајќи издавачки ИС и сите ИС во синџирот) на своите претплатници - крајни корисници по издавањето на сертификатот.

Корисниците за време на процесот на подигнување на сертификатот автоматски го преземаат и го инсталираат на својот компјутер јавниот клуч на посредничкиот ИС и на издавачкиот ИС. Овој процес е контролиран од страна на PKI апликацијата. 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://www.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 клучеви 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.

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

6.1.6. Параметри за генерирање јавен клуч и проверка на квалитетот

Не е пропишано со одредба.

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

ADACOM 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 хардверски криптографски модули кои се управувани и обезбедени од ADACOM SA, 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 сертификација на QSCD до крајот на периодот на важење на сертификатот поврзан со соодветниот QSCD. Во случај на измена на статусот на сертификација 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 применува технички и процедурални механизми имплементирани од ADACOM кои бараат 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 (м) на Тајни удели од вкупниот број Тајни удели (н) креирани и дистрибуирани за конкретниот криптографски модул.

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

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 оporавување 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 Правила. Приватните клучеви на ИС се копираат на резервни хардверски криптографски модули во согласност со овие Правила.

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

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 критериумите на овие Правила и на Правилата на ADACOM . Овие ИС парови на клучеви не треба да се користат за потпишување по истекување на нивната важност, освен ако ИС сертификатот не се обнови согласно овие Правила.

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 од кои клучевите ќе се користат. Покрај тоа, ADACOM прави копии на тие ИС парови на клучеви заради рутинско

обновување и со цел за оправување по откажување на системот. Во случаи кога ИС паровите на 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

ИС и РК 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 ќе ги заштитуваат податоците за активирање за нивните приватни клучеви од губење, кражба, изменување, неовластено откривање или неовластена употреба.

Приватните клучеви на претплатниците на локалните 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 блокиран по 3 последователни неточни обиди,
- Корисникот може да ги смени ПИН-кодовите.

Приватните клучеви на претплатникот на далечинскиот 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 со минималниот број на 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 локалниот QSCD од системот или по одјавување на далечинскиот QSCD. Во секој случај, претплатниците имаат обврска на соодветен начин да го заштитуваат својот приватен клуч(клучеви) во согласност со овие Правила.

6.2.10. Метод на уништување на приватниот клуч

По завршувањето на оперативниот животен циклус на сертификатот на КИБС, една или повеќе копии од ИС приватниот клуч се архивира во согласност со дел 6.2.5 од овие Правила. Преостанатите копии од ИС приватните клучеви безбедно се уништуваат. Покрај тоа, архивираните ИС приватни клучеви безбедно се уништуваат на крајот на периодот за архивирање. Активностите за уништување на ИС клучевите предвидуваат учество на повеќе доверливи лица.

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 локален 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 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 поврзаните сертификати со нив, само што тие можат да продолжат да се користат за дешифрирање и верификување на потписот. Максималниот оперативен период за сертификатите на КИБС за сертификати издадени на или по датумот на стапување во сила на овие Правила се наведени во Табелата ,,Оперативни периоди на сертификати" подолу.

Издаден сертификат од:	Период на важност
РСА Само-потпишан (2048 бити)	25 години
КИБС изадавачки ИС	6 години
Краен корисник индивидуален претплатник	Нормално до 3 години

Табела 5: 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 сертификатот 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 ИС сертификатот за потпишување.

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

Ако алгоритмот 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 (Тајните 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 од Правилата и Референтниот водич за церемонија на генерирање клучеви. Креирањето и дистрибуирањето на Тајните удели се евидентира.

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

- Кога парови 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 на претплатникот се генерираат, 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 далечинскиот QSCD, кои содржат приватни клучеви на субјектот, се генерираат во согласност со барањата за усогласеност на QSCD.

6.4.2. Заштита на податоците за активирање

Потребно е чуварите на удели на КИБС ИС да ги чуваат своите тајни удели и тајните удели на уредот за далечинско потпишување QSCD и да потпишат договор во кој ќе бидат јасно изразени нивните одговорности.

Претплатникот ги меморира податоците за активирање (ПИН, корисничко име, лозинка, OTP) и не ги споделува со никој друг.

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 на DigiCert PKI ќе го заштитат преносот користејќи методи кои штитат од загуба, кражба, модификација, неовластено откривање или неовластена употреба 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 враќа податоците за активирање со бришење и преснимување преку нив или со физичко уништување.

6.5. Контроли за сигурност на компјутерите

ADACOM и КИБС ги изведуваат функциите на ИС и РК со користење на доверливи системи кои ги задоволуваат условите на Водичот за предуслови за сигурност и надзор на DigiCert.

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 спречат 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 за 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 сигурност. 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

6.5.2. Рангирање на сигурноста на компјутерите

Не е пропишано со одредба.

6.6. Технички контроли на животниот циклус

6.6.1. Контроли на развојот на системот

Апликациите се развиваат и имплементираат од КИБС во согласност со стандардите на КИБС за управување со развојот и промените на системите.

Новиот и ажуриран софтвер, кога за првпат ќе биде поставен за користење, обезбедува метод за верификување дека софтверот во системот е дизајниран од доверлив извор, дека не бил модификуван пред инсталирањето и дека е тоа верзијата која е наменета за користење.

6.6.2. Контроли за управување со сигурноста

КИБС има механизми и/или политики за контролирање и надгледување на конфигурацијата на своите ИС системи. DigiCert креира хаш од сите софтверски пакети и од надградувањата на DigiCert софтверите. Хашот се користи за да се верификува интегритетот на таквиот софтвер мануелно. По инсталирањето и подоцна на определени интервали, КИБС го проверува интегритетот на своите ИС системи.

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 Водичот за услови за сигурност и надзор на DigiCert 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 работа на доверливите услугит.

КИБС периодично врши проценка на ранливост на јавни и приватни IP адреси што се однесува на тестови за непробојност на системите за сертификација.

6.8. Временски печат

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

7. ПРОФИЛИ НА СЕРТИФИКАТИ, РЕГИСТАР НА ПОНИШТЕНИ СЕРТИФИКАТИ (РПС) И НА ПРОТОКОЛ ЗА ОНЛАЈН 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.

Профилите на сертификати се објавуваат во јавното складиште КИБС на линкот:

http://www.kibstrust.com/repository.

7.2. CRL профил

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

CRL профилите се објавуваат во јавното складиште на КИБС на http://crl.kibstrust.com/(http://crl.kibstrust.com/eSign.crl и http://crl.kibstrust.com/eSeal.crl).

7.3. OCSP профил

OCSP профилот е во согласност со IETF RFC 6960.

Профилите на OCSP се објавуваат во јавното складиште КИБС на http://ocsp1.kibstrust.com.

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 MK-eIDAS и eIDAS регулативата, соодветните закони и стандарди или кога и да е направена голема промена во работата на доверлива услуга.

Покрај ревизиите за усогласеност, КИБС има право да изврши други прегледи и истраги 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 ревизии на втора страна на договарачи кои се поврзани со КИБС за да работат како Локална регистрациска канцеларија (ЛРК).

8.1. Интервали и околности на проценките

Ревизија за усогласеност 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.

Надзорот за усогласеност на КИБС ИС се изведува од страна на:

- Интерни ревизори,
- Тело за проценка на сообразност кое е акредитирано во согласност со Регулативата ЕЗ бр. 765/2008, ETSI стандардите (т.е. ETSI EN 319 403) и Основните барања на CA / B форумот (дел 8.2),
- Надзорно тело.

8.2. Односот на проценителот со проценуваниот субјект

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

8.3. Прашања на кои се однесува проценката

Проценката на сообразност опфаќа сообразност 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 СР и изјавите за политиките и практиките 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 ги ЛРК).

8.4. 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 DigiCert PKI, 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.

8.5. 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 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 учествува КИБС и други заинтересирани страни.

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

8.6. 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 РПС, потребни со оваа СР, 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)

9.1.4.1. 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, член 89, како што дополнет и изменет, да се повлече од договорот за продажба без да ги наведе причините во избран 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-пошта на helpdesk@kibstrust.com од претплатникот до КИБС. Потоа, и после

комуникацијата, КИБС е должна да ги врати парите 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 налог за набавка пред активирање на сертификатот. Доколку претплатникот не покаже или не достави соодветна документација во рок од триесет (30) дена од неговата / нејзината нарачка за квалификуван сертификат за електронски потпис или печат во / до РК / ЛРК на давателот на доверливи услуги, налогот за набавка 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 локалниот QSCD во случаи на неисправност, едноставно поради фабричка грешка, поради што сертификатот или локалниот 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.

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

9.1.4.2. Други случаи

КИБС се справува со рефундирање од случај до случај. Во ретки случаи, КИБС може да направи рефундација на претплатникот. Остварувањето на ова право ќе се изврши во писмена форма од претплатникот до КИБС со испраќање на е-порака до helpdesk@kibstrust.com.

9.2. Финансиска одговорност

9.2.1. Покритие на осигурување

КИБС одржува ниво на осигурително покривање според МК-eIDAS и комерцијално разумно ниво на осигурително покривање за грешки и пропусти согласно Правилникот за осигурување јавно објавен на http://www.kibstrust.com/repository.

Политиката за осигурување на КИБС е достапна во неговото јавно складиште.

9.2.2. Други средства

КИБС има доволно финансиски средства да ги одржува своите операции и да ги извршува своите должности, како и разумна моќ 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 Правила.

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 работење и обезбедување на доверливи услуги) се доверливи. Претплатникот има право да добие информации од КИБС за него, 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 Правила.

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

9.3.3. Одговорност за заштитата на доверливите информации

КИБС заштитува доверливи информации и информации 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://www.kibstrust.com/repository во согласност со важечките закони.

9.4.2. Информации што се третираат како приватни

Каков било податок за претплатникот 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 за приватни.

Сите информации објавени во сертификат не се сметаат за 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 законски 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 Правила, 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, КИБС 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 признавање и барање за продуцирање на документи.

Овој дел е предмет 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 е предмет на важечките закони за приватност.

9.4.8. Други околности на откривање информации

Не е пропишано со одредба.

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

КИБС 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 Одредбите 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 Одредби и услови или некои други важечки договори.

9.5.2. Права на сопственост во Правилата

Претплатниците и засегнатите страни на КИБС прифаќаат дека КИБС ги задржува сите права на интелектуална сопственост во и на овие Правила.

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 на 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 DigiCert и коренските сертификати кои ги содржат нив, вклучително и PCA јавните клучеви и самопотпишаните сертификати, се сопственост на DigiCert. DigiCert дава лиценци на производителите на хардвер и софтвер да ги репродуцираат ваквите коренски сертификати за да ги постават во безбедна хардверска опрема или во софтвер. 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 DigiCert, ADACOM или KIBS.

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 Правила и поврзаните документи;
- е во согласност со MK-eIDAS и eIDAS регулативата и поврзаните правни акти утврдени во овие Правила и поврзаните документи;
- ги објавува своите Правила и поврзаните документи и ја гарантира нивната достапност во мрежата за комуникација со јавни податоци;
- ги објавува и исполнува барањата во смисла и одредби и услови за претплатници и гарантира нивна достапност и пристап во мрежа 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 далечинскиот QSCD на овластениот претплатник на клучевите;
- обезбедува правилно управување и усогласеност на далечинскиот 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 се дознае за какво било нарушување на сигурноста или губење на интегритетот што има значајно влијание врз пружената доверлива услуга или врз личните податоци што се чуваат кај нив, 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 губењето на интегритетот;
- ја чува целата документација, евиденција и записи поврзани со доверливите услуги според точките 5.4 и 5.5;
- обезбедува проценка на усоглсеноста 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 Правила;
- ги објавува условите на политиката за задолжително осигурување и заклучокот на телото за проценка на усоглсеноста 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 никакви грешки во информациите во сертификатот што се воведени од субјектите кои го одобруваат барањето за сертификат или издавањето на сертификатот како резултат на неуспехот да се употреби разумна грижа во управувањето со барањето на сертификат или да се креира сертификат;
- услугите за поништување и употреба на складиште се усогласени со важечите Правила во сите материјални аспекти.

Одредбите и условите за употреба на ЕУ квалификувани сертификати на КИБС може да вклучуваат дополнителни изјави и гаранции.

9.6.2. Изјави и гаранции на РК

КИБС РК гарантира дека:

- 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 никакви 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 Правила,
- услугите за поништување (кога е применливо) и употребата на складиште во согласност со важечките Правила во сите материјални аспекти, и
- ги исполнува барањата од Правилата.

Одредбите и условите на КИБС може да вклучуваат дополнителни изјави и гаранции.

9.6.3. Изјави и гаранции на претплатникот

Претплатниците гарантираат дека:

- секој квалификуван 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, ОТР) со кои се пристапува до приватниот клуч се заштитени и дека ниту една неовластено лице досега немало пристап до нив,
- квалификуванот е-Потпис или е-Печат на ЕУ се креирани само со уред QSCD,
- 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 Правила 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 Правила и поврзаните документи;
- сертификатот се користи исклучиво за овластени и правни цели, во согласност со овие Правила;
- претплатникот не е ИС, и не го користи приватниот клуч што одговара на кој било јавен клуч наведен во сертификатот за целите на дигитално потпишување на кој било сертификат (или кој било друг формат на овластен јавен клуч) или РПС, како ИС или поинаку;
- претплатникот ќе го извести КИБС без разумно одложување, доколку приватниот клуч на субјектот или контролата врз него е изгубен, украден, потенцијално компромитиран.

Одредбите и условите на КИБС за употреба на квалификувани сертификати може да вклучуваат дополнителни изјави и гаранции.

9.6.4. Изјави и гаранции на засегнатата страна

Според Одредбите и условите на КИБС за употреба на квалификувани сертификати 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 нејзинот неуспех да ги изврши обврските на засегната страна согласно овие Правила.

Одредбите и условите на КИБС за употреба на квалификуван сертификат може да вклучат дополнителни изјави и гаранции на засегнатите страни.

9.6.5. Изјави и гаранции на други учесници

Не е пропишано со одредба.

9.7. Одрекување на гаранциите

До степенот дозволен со важечкиот закон, Одредбите и условите за употреба 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, можна злоупотреба на сертификати или несоодветни 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;
- Неисполнување 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;
- Неисполнување на обврските што произлегуваат од овие Правила и поврзаните документи, доколку таквото неисполнување е предизвикано од Виша сила.

9.8. Ограничувања на одговорност

Одредбите и условите на КИБС за употреба на квалификуван сертификат помеѓу другите кавлификувани доверливи услуги ја ограничуваат одговорноста на КИБС. Ограничувањата на одговорноста вклучуваат изземање на индиректни, посебни, случани и последователни штети. Тие, исто така, вклучуваат и ограничување на одговорноста во износ на петстотини евра (500,00 €) изразено во денари според средниот курс на НБРСМ, со што се ограничуваат штетите на КИБС во врска со квалификуван сертификат.

Одговорноста (и/или ограничување на неа) на претплатниците и засегнатите страни е наведена во релевантните Претплатнички договори за употреба на квалификувани доверливи услуги објавени во складиштето на КИБС.

9.9. Обесштетувања

9.9.1. Обесштетување од страна на претплатниците

Од претплатниците се очекува да платат обесштетување на 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 кој било начин да се заштити од компромитирање, губење, откривање, изменување или неовластено користење на претплатничкиот приватен клуч, или
- Користењето на име (вклучително и без ограничувања во рамките на вообичаеното 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 вклучува дополнителни обврски за обесштетувања.

9.9.2. Обесштетување од страна на засегнатите страни

Одредбите и условите на КИБС бараат засегнатата страна да го обесштети КИБС ако:

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

Одредбите и условите на КИБС може да вклучат и други обврски за обесштетување.

9.10. Период и прекин на важност

9.10.1. Период на важност

Овие Правила стапуваат на сила по објавувањето на веб страната на КИБС. Измените и дополнувањата на овие Правила стапуваат на сила по објавувањето во складиштето на КИБС.

9.10.2. Прекин на важност

Овие Правила со промените кои се прават одвреме навреме остануваат на 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 Правила, учесниците во КИБС поддоменот, 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, учесниците во КИБС поддоменот ќе користат комерцијално разумни методи кога ќе комуницираат помеѓу себе, имајќи ги предвид критичноста и темата на комуникацијата.

КИБС ќе го извести ADACOM според барањата за нотификација на Форум CA / B, во случај на:

- Промени во процедурите за издавање сертификати во врска со сертификати кои содржат адреса за е-пошта;
- Прекини или пренесување на сопственост на КИБС АД;
- Сопственост или контрола на измените на ИС сертификати;
- Постоење материјална промена во работењето на КИБС (т.е. кога криптографскиот хардвер е преместен од една сигурна локација на друга)

9.12. Измени и дополнувања

9.12.1. Процедура на измени и дополнувања

Измените и дополнувањата на овие Правила ги прави Групата за развој на практики на КИБС (KPDG). Измените и дополнувањата се вклучуваат во новата верзија на Правилата што се објавува на https://www.kibstrust.com/repository/cps. Новата верзија на Правилата ги заменува кои било специфицирани или спротивставени одредби од претходната верзија на овие Правила.

Ажурирањата ги заменуваат сите наведени или спротивставени одредби на наведената верзија на Правилата. KPDG утврдува дали промените во Правилата бараат промена во предметните идентификатори на Политиката за сертификати на Политиките за сертификати.

9.12.2. Механизам и период на известување

Органот за управување со политика (PMA) на КИБС го задржува правото да ги измени Правилата без известување за измените и дополнуавњата што не се материјални, вклучително и без ограничување на корекција на типографски грешки, измени во URL адреси и промени во информации за контакт. Одлуката на PMA да ги назначи измените како материјални или нематеријални, ќе биде според дискреционото право на PMA. Предложените измени и дополнувања на Правилата се поврзани со складиштето АДАКОМ лоцирано на: https://www.kibstrust.com/repository/cps.

Без оглед на сè спротивно во Правилата, доколку PMA верува дека материјалните измени во Правилата 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 со објавување во складиштето на ADACOM. Ваквите измени ќе стапат на сила веднаш по објавувањето. Во разумно време по објавувањето, КИБС ќе ги извести учесниците на КИБС поддоменот за ваквите измени.

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

Измените што не го менуваат значењето на овие Правила, како што се правописни корекции, активности за превод и ажурирања за детали за контакт, се документирани во делот Верзии и измени на овој документ. Во овој случај, избраниот дел од бројот на верзијата на документот е зголемен. Во случај на значителни промени, новата верзија на Правилата 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 KPDG во соработка ADACOM, одреди дека е неопходна промена во некој предметен идентификатор што соодветствува на Политиката за сертификати, измените ќе содржат нов предметен идентификатор во Политиката за сертификати соодветно за секоја класа на сертификати. Инаку, измените не бараат промена во предметниот идентификатор на Политиката за сертификати.

9.13. Одредби за решавање на спорови

9.13.1. Спорови помеѓу DigiCert, филијали и клиенти

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

9.13.2. Спорови со претплатници - крајни корисници или засегнати страни

Одредбите 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

Македонските закони ќе бидат надлежни за извршувањето, составувањето, интерпретирањето и важноста на овие Правила, без оглед на договор или изборот на друг закон.

Меродавното право важи само за овие Правила. Договорите кои ги вклучуваат овие Правила само како референца може да имаат свои сопствени одредби за меродавно право, под услов делот 9.14 да го регулира извршувањето, сочинувањето, интерпретирањето и важноста на условите од овие Правила 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 услови за заштита на евиденцијата од губење, уништување и фалсификување и барањата на следново:

- MK-eIDAS - Закон за електронски документи, електронска идентификација и доверливи услуги.
- eIDAS - Регулатива (ЕУ) бр. 910/2014 на Европскиот парламент и на Советот од 23 јули 2014 година за електронски услуги за идентификација и доверба за електронски трансакции на внатрешниот пазар и укинување на Директивата 1999/93 / ЕЗ;
- Закони за лични податоци донесени во Македонија и во ЕУ;
- Поврзани европски стандарди:
  a) ETSI EN 319 401 Електронски потписи и инфраструктури (ESI); Општи барања на политика за даватели на услуги од доверба;
  b) ETSI EN 319 411-1 Електронски потписи и инфраструктури (ESI); Барања на политика и сигурност за давателите на доверливи услуги кои издаваат сертификати; Дел 1: Општи барања;
  c) ETSI EN 319 411-2 Електронски потписи и инфраструктури (ESI); Барања на политика и сигурност за давателите на доверливи услуги кои издаваат сертификати; Дел 2: Барања за органи за сертификација за издавање квалификувани сертификати;
- Форум CA / Browser, Основни барања на Политика за сертификати за издавање и управување со јавно доверливи сертификати .

Овие Правила подлежат на македонски закони.

9.16. Останати одредби

9.16.1. Целосност на договорот

Не е пропишано со одредба.

9.16.2. Доделување

Сите субјекти кои работат според овие Правила 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 Правила се прогласат за неспроведливи од соодветен суд или од друг надлежен авторитет, остатокот од овие Правила 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 Правила не го одрекува правото на КИБС да ја спроведе истата одредба подоцна или правото да спроведе друга одредба од овие Правила. 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 Правилата 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 Правила и / или поврзаните документи, предизвикани од Виша сила.

9.17. Други одредби

Не е пропишано со одредба.

Додаток А. Табела на кратенки и дефиниции

Табела на кратенки

Термин	Дефиниција
ИС	Издавач на сертификати
CP	Политика за сертификати
CPS	Правила за издавање сертификати
CRL	Регистар на поништени сертификати
EAL	Ниво на гаранција за проценката (согласно општите критериуми)
FIPS	Федерални стандарди за обработка на информации на САД
KPDG	Група за развој на практики на КИБС
LSVA	Проценка за ранливост на логичката сигурност
OCSP	Протокол за електронско добивање на статусот на сертификат
PCA	Примарен сертификациски авторитет
PIN	Личен идентификациски број
PKCS	Криптографски стандард за јавен клуч
PKI	Инфраструктура на јавен клуч
PMA	Авторитет за управување на политиката
QSCD	Уред за креирање квалификуван потпис
RA	Регистрациска канцеларија
RFC	Барање за коментар
S/MIME	Протокол за безбедно пренесување на интернет пошта
SSL	Протокол Secure Socket Layer
DigiCert PKI	DigiCert Инфраструктура на јавен клуч

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 изведување на ИС или РК функции.
Филијала	Водечка доверлива трета страна, на пример, во технологијата, телекомуникациите или индустријата на финансиските услуги, која склучува договор со DigiCert за да биде DigiCert PKI канал за дистрибуција и услуги во рамките на определена територија.
Сертификат	Порака која како минимум наведува име или идентификува ИС или претплатник, го содржи јавниот клуч на претплатникот, го определува оперативниот период на сертификатот, го содржи серискиот број на сертификатот и е дигитално потпишан од ИС.
Подносител на барање за сертификат	Лице или организација што бара издавање на сертификат од ИС.
Барање за сертификат	Барање од подносителот на барање за сертификат (или овластен застапник на подносителот на барање за сертификат) до ИС за издавање на сертификат.
Синџир на сертификати	Подредена листа на сертификати која го содржи сертификатот на претплатникот - краен корисник и сертификатите на ИС, а завршува со коренски сертификат.
Политика за сертификати (CP)	Документ кој се нарекува Политика за сертификати на DigiCert мрежата на доверба и претставува главна изјава за политиката според која делува DigiCert PKI.

Термин	Дефиниција
Регистар на поништени сертификати (РПС)	Периодично (или инцидентно) издаван регистар, дигитално потпишан од ИС, на определени сертификати кои биле поништени пред датумот на истекување на нивната важност. Листата обично го наведува името на издавачот на РПС, датумот на издавање, датумот на следното закажано издавање на РПС, серискиот број на поништениот сертификат, како и точното време и причините за поништување.
Барање за потпишување сертификат	Порака која го пренесува барањето за издавање на сертификат.
Издавач на сертификати (ИС)	Ентитет овластен да издава, управува, поништува, обновува сертификати во DigiCert PKI.
Правила за издавање сертификати (Правила)	Овој документ кој ги наведува Правилата што КИБС ги применува при одобрување или одбивање на барањата за сертификати; и издавање, управување и поништување на сертификати и бара од неговите корисници и да ги применуваат.
Фраза за проверка	Тајна фраза избрана од подносителот на барањето за сертификат за време на запишувањето на сертификат. 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 својот сертификат.
Класа	Одредено ниво на гаранции, како што е дефинирано во CP. Види го делот 1.1.1 од CP.
Центар за услуги на клиенти	Сервисен центар односно ADACOM обезбедува сертификати за клиент или претпријатие.
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 DigiCert PKI стандардите кои важат за нив.
Компромитирање	Прекршување (или претпоставено прекршување) на безбедносната политика, при кое можело да се случи неовластено откривање или губење на контролата врз чувствителни информации. Во врска со приватните клучеви, компромитирање претставува губење, кражба, откривање, изменување, неовластено користење или друг вид на компромитирање на сигурноста на тој приватен клуч.
Доверлива/лична информација	Информација која треба да се чува како доверлива и лична во согласност со дел 2.8.1 од CP.
Договор за користење на CRL	Договор кој ги поставува одредбите и условите под кои може да се користи CRL или информациите во него.
Претпријатие, како кај Центар за услуги на претпријатија	Деловно работење во кое ADACOM кое обезбедува Управувани PKI услуги за Управувани PKI Клиенти.
Инцидентна ревизија/испитување	Ревизија или испитување од страна на Управуван PKI клиент или ADACOM кога ADACOM има причина да верува дека настанало непридржување на некој ентитет кон DigiCert PKI Стандардите, инцидент или компромитирање поврзан со ентитет, или дека постои реална или потенцијална опасност за сигурноста на DigiCert PKI од страна на ентитет.
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.
Посреднички издавач на сертификат(Посреднички ИС)	Издавач на сертификати чиј сертификат е лоциран во синџирот на сертификати помеѓу сертификатот на коренскиот ИС и сертификатот на Идавачот на сертификати кој го издал сертификатот на претплатникот - краен корисник.
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.
Група за развој на практики на КИБС	Оваа група во рамките на КИБС е одговорна за донесување на оваа политика.

Термин	Дефиниција
КИБС складиште	База на податоци за сертификати на КИБС и други релевантни информации за КИБС ИС, достапна онлајн.
Управуван PKI	Целосно интегрирана управувана PKI услуга на ADACOM која им овозможува на фирмите клиенти на ADACOM да дистрибуираат сертификати на физички лица, како на пример, членови на персоналот, партнери, добавувачи и клиенти. Управуваниот PKI им овозможува на претпријатијата да ги обезбедат своите пораки или апликациите во електронската трговија.
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.
МК-eIDAS	Закон за електронски документи, електронска идентификација и доверливи услуги.
Неверификувана претплатничка информација	Информација поднесена од подносителот на барање за 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.
Не-одрекување	Атрибут на комуникацијата кој обезбедува заштита 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 можат во крајна мерка да спречат одрекување. На пример, дигитален потпис верификуван во врска со DigiCert PKI Сертификат може да обезбеди доказ во прилог на определувањето на Неодрекување од страна на трибунал, но тоа само по себе не претставува Неодрекување.
Исклучени (Офлајн) ИС	DigiCert PCA кои издаваат коренски ИС сертификати и други посреднички ИС, кои се одржуваат исклучени (офлајн) од безбедносни причини, со цел да бидат заштитени од можни напади од натрапници преку мрежата. Овие ИС не потпишуваат директно 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.
Оперативен период	Период што започнува на датумот и во времето на издавање на сертификатот (или на подоцнежна датум и време ако е така наведено во Сертификатот), а завршува на датумот и во времето кога сертификатот истекува или е поништен порано.
PKCS #10	Криптографски стандард # 10 на јавен клуч, развиен од RSA Security Inc., кој дефинира безбедна структура за барање за потпишување сертификат.
PKCS #12	Криптографски стандард # 12 за јавен клуч развиен од RSA Security Inc., кој дефинира безбеден начин за трансфер на приватни клучеви.
Авторитет за управување со Политиката (PMA)	Организација во рамките на DigiCert одговорна за објавување на оваа политика низ целата DigiCert PKI.
Примарен Издавач на Сертификати (PCA)	ИС што делува како коренски ИС за специфична класа на сертификати и им издава сертификати на ИС кои му се потчинети.
Центар за обработка	Локација на ADACOM со безбедни простории за сместување, меѓу другото, и на криптографските модули што се користат за издавање на сертификати. За клиентот и веб страницата, Центрите за обработка делуваат како ИС во рамките на DigiCert PKI и ги извршуваат сите услуги на животниот циклус на сертификатот, како издавање, управување, поништување и обновување на сертификати. Во однос на претпријатија, Центарите за обработка обезбедуваат услуги поврзани со животниот циклус на сертификатите, во име на Управуваните PKI клиенти или Управуваните PKI клиенти на Сервисните центари подредени на нив.

Термин	Дефиниција
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. DigiCert PKI се состои од системи кои соработуваат за обезбедување и имплементирање на DigiCert PKI.
Уред за креирање квалификуван потпис	Уред кој е одговорен за квалификација на дигитални потписи со употреба на специфичен хардвер и софтвер кои гарантираат дека само потписникот има контрола на нивниот приватен клуч. Квалификувани уреди за електронско потпишување или за печат ги исполнуваат барањата на Регулативата (ЕУ) бр. 910/2014 (eIDAS)
Регистрациска канцеларија (РК)	Ентитет одобрен од ИС за да им помогне на барателите на сертификати при поденсување 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.
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.
Споделување на тајна	Практика на разделување на ИС приватен клуч или на податоците за активирање што се потребни за да функционира ИС приватниот клуч со цел да се воспостави контрола од повеќе лица врз операциите на ИС приватниот клуч согласно CP § 6.2.2
ИД на Безбеден сервер	Организациски Сертификат Класа 3 кој се користи за поддржување на SSL сесии помеѓу веб-пребарувачите и веб серверите.
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, по избор, автентикација на клиент за конекција на Протоколот за контрола на трансмисија/Интернет протоколот.
Водич за услови на сигурност и ревизија	DigiCert документ кој поставува барања за сигурност и ревизија за Центрите за обработка и Центрите за услуги.
Сервисен Центар	Работа на ADACOM која не вклучува единици за потпишување сертификати со цел на издавање сертификати од конкретна класа или тип, туку повеќе, се потпира на центарот за обработка за да извршува издавање, управување, поништување и обновување на такви сертификати.
Поддомен	Дел од DigiCert PKI под контрола на кој било ентитет и сите ентитети што му се потчинети нему во рамките на DigiCert PKI хиерархијата.
Субјект	Сопственик на приватен клуч што кореспондира со јавен клуч. Терминот ,,субјект" може, во случај на сертификат за организации, да се однесува на опрема или уред кој е носител на приватниот клуч. На субјектот му се дава недвосмислено име, кое е поврзано со јавниот клуч што се содржи во сертификатот на субјектот.
Претплатник	Во случај на сертификат за физички лица, претплатник е лицето кое што е субјект на сертификатот и на кое му е издаден сертификатот. Во случај сертификат за организации, претплатник е организацијата што ја поседува опремата или направата која е субјект на сертификатот и на која ѝ е издаден сертификатот. Претплатникот може да го користи и има овластување да го користи приватниот клуч што кореспондира со јавниот клуч запишан во сертификатот.
Одредби и услови	Договор кој се користи од ИС и РК за поставување на одредбите и условите под кои физичкото лице или организацијата делуваат како претплатник.
Надреден ентитет	Ентитет надреден над некој друг ентитет во рамките на DigiCert PKI хиерархијата (Класа 1 или 3 хиерархија).

Термин	Дефиниција
Доверливо лице	Вработен, соработник под договор или консултант на ентитет во рамките на DigiCert PKI одговорен за инфраструктурната сигурност и сигурност на ентитетот, неговите производи, услуги, неговите простории и/или практики како што е поконкретно дефинирано во CP § 5.2.1
Доверлива позиција	Позиции во DigiCert PKI ентитет на кои мора да бидат поставени доверливи лица.
Сигурен и безбеден систем	Компјутерски хардвер, софтвер и процедури кои се разумно 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 владејачка номенклатура.
DigiCert	Значи, во врска со секој релевантен дел од овие Правила, DigiCert, Inc., и/или која било подружница во целосна сопственост на DigiCert која е одговорна за специфични операции во издавањето.
DigiCert Доверлива мрежа (DigiCert PKI)	Инфраструктура на јавен клуч базирана на сертификати, која е водена од Политиките за сертификати на DigiCert доверливата мрежа и овозможува распространување и користење на сертификати низ целиот свет од страна на DigiCert и филијалите поврзани со него, како и од нивните клиенти, претплатници и засегнати страни.
DigiCert PKI Учесник	Еден или повеќе. поединец или организација во рамките на DigiCert PKI како: DigiCert, ADACOM, Клиент, Универзален сервисен центар, препродавач, претплатник или засегната страна
DigiCert PKI Стандарди	Деловните, правните и техничките услови за издавање, управување, поништување, обновување и користење на сертификати во рамките на DigiCert PKI.

Крај на документот