Практика

за давање на услуга за електронска идентификација

KIBSTrust OneID

Верзија: 1.0

Датум на стапување во сила: 24.09.2021

Ознака: 111.02

OID: 1.3.6.1.4.1.16305.1.1.6

КИБС АД Скопје
© 2021 КИБС АД Скопје, сите права задржани
https://www.kibstrust.com/

Белешка за трговската марка

КИБС, KIBSTrust и OneID се регистрирани марки на КИБС АД Скопје. Другите имиња кои се спомнуваат во документот, може да бидат трговски марки на други сопственици. Давателот на доверливи услуги организациски претставува дел од КИБС, но настапува под брендот со име **KIBSTrust**, па терминот „Давател на доверливи услуги КИБС“ се поистоветува со „KIBSTrust“.

Репродукција и дистрибуција на овој документ е одобрена на неекслузивна основа и без надоместок за авторски права, под услов (i) горенаведеното известување за авторски права и почетните ставови да бидат видливо прикажани на почетокот на секој примерок, и (ii) овој документ да биде точно репродуциран во целост, дополнет со измените внесени од страна на KIBSTrust.

Барања за било каква друга дозвола за репродуцирање на овој документ, треба да се адресираат на KIBSTrust (КИБС АД Скопје), Кузман Јосифовски Питу 1, 1000, Скопје, Република Северна Македонија, за: Одбор за управување со политики на KIBSTrust, тел: +38925513401, +38923297401, е-пошта: pma@kibstrust.com.

Историја на документот

верзија	датум	Автор	цел на промената
1.0	24.09.2021	Одбор за управување со политики на KIBSTrust	Давање на услуга за електронска идентификација и создавање на шема за електронска идентификација со име **OneID** согласно законот МК-eIDAS.

Содржина

1. ВОВЕД

Овој документ ги содржи практиките применети од страна на KIBSTrust за далечинска проверка и потврда на постоење на физичко лице, веродостојност на приложените документи за лична идентификација на физичкото лице, за издавање на средства за електронска идентификација согласно регистрирана шема за електронска идентификација со високо ниво на сигурност.

Во него се наведени општите барања и сигурносните мерки кои ги користи KIBSTrust при обезбедување услуги за електронска идентификација и издавање на квалификуван сертификат за електронски потпис како една од компонентите на средството за електронска идентификација. Сето ова е во согласност со МК-eIDAS[1], членови 11 до 20 (поврзани со електронска идентификација), членови 24, 29, 38, 39, 40, 55 (поврзани со квалификуваните доверливи услуги), соодветните подзаконски акти и членовите 19, 24, 26, 27, 28, 36, 37, 38 и 45 од Регулативата (ЕУ) бр. 910/2014 (eIDAS)[2]. Дополнително, во однос на заштита на личните податоци, овој документ е усогласен со МК-GDPR[3] и GDPR[4].

Како потврда за усогласеноста со МК-eIDAS и eIDAS, KIBSTrust подлежи на проверка за проценка на сообразноста од страна на независна организација, акредитирано тело за проценка на сообразност, прифатено од македонскиот национален регулатор Министерството за информатичко општество и администрација (МИОа). Врз основа на оваа потврда за сообразност КИБС како квалификуван давател на доверливи услуги и услуги за електронска идентификација е запишан во Регистар на даватели на доверливи услуги и на шеми за електронска идентификација.

Овој документ е јавно објавен со цел субјектите, засегнатите страни, проверувачи и регулаторни тела да се информираат за деловните, правните, техничките и организациските мерки при барање, издавање, управување, користење, обновување, замена, суспендирање, отповикување и повторно активирање на средствата за електронска идентификација на субјектот.

1.1. Преглед

KIBSTrust применува процедури и стандарди, согласно регулаторните барања, за издавање и управување со животниот циклус на средството за електронска идентификација кое се состои од мобилен уред, апликативно решение инсталирано на мобилниот уред, податоци за идентификација на физичкото лице и квалификуван сертификат за електронски потпис како средство за електронско потпишување.

Политиките и постапките за издавање на квалификуван сертификат како дел од средството за електронска идентификација се во согласност со стандардот ETSI EN 319 411-2 и профилот QCP-n-qscd за квалификувани сертификати за електронски потписи издадени на средство за креирање на квалификуван потпис (QSCD) и се објавени во јавното складиште на документи под име „Правила и постапки за издавање на квалификувани сертификати за електронски потписи и електронски печати“ (со интерна ознака 111.01). Овој документ во понатамошниот текст ќе биде референциран како: CP/CPS.

Средствата за креирање на квалификуван потпис (QSCD) коишто ги користи KIBSTrust се запишани на листа на средства за создавање на квалификуван електронски потпис и електронски печат што ја води МИОа согласно МК-eIDAS.

KIBSTrust има безбеден капацитет за складирање, меѓу другото, и на системи за издавање сертификати, вклучувајќи ги криптографските модули со приватни клучеви што се користат за издавање сертификати. KIBSTrust како давател на доверлива услуга за издавање на сертификати ги извршува сите услуги за

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

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

[3] Закон за заштита на лични податоци (Службен весник на Република Северна Македонија (МК-GDPR)

[4] Регулатива (ЕУ) 2016/679 на Европскиот парламент и на Советот од 27 април 2016 за заштита на физички лица во однос на обработката на личните податоци и за слободно движење на тие податоци и укинување на Директивата 95/46/ЕЗ (GDPR)

животниот циклус на сертификатите во однос на издавање, управување, поништување и обновување на квалификувани сертификати.

CP/CPS е посебно применлив за издавачките сертификати на KIBSTrust, кои издаваат квалификувани сертификати за електронски потписи електронски печати. KIBSTrust ги објавува CP/CPS за да се усогласи со специфичните барања за правилата на важечкото законодавство или другите индустриски стандарди и барања.

Секаде во овој документ каде се насловени барања кои се изведуваат согласно тие наведени во CP/CPS истите ќе бидат референцирани кон соодветната точка од CP/CPS .

1.2. Име и идентификација на документ

На овој документ именуван како „Практики за давање услуга за електронска идентификација“ KIBSTrust му ја додели следнава вредност на предметен идентификатор (OID): **1.3.6.1.4.1.16305.1.1.6**

1.3.6.1.4.1.16305	Идентификациски број (OID) на КИБС, регистриран во IANA
1.3.6.1.4.1.16305.1	Давател на доверливи услуги
1.3.6.1.4.1.16305.1.1	Политика и пракса (CP/CPS)
1.3.6.1.4.1.16305.1.1.6	Практики за давање на услуга за електронска идентификација

1.3. Учесници

1.3.1. Издавач на средства за електронска идентификација

Издавач на средства за електронска идентификација е правно лице кое ги исполнува условите утврдени во МК-eIDAS и соодветен подзаконски акт[5] (Правилник) и има целосна одговорност за обезбедување услугите за кои е регистриран.

KIBSTrust е регистриран издавач средства за електронска идентификација и ги исполнува стандардите и техничките мерки за сигурност на својата шема за електронска идентификација на високо ниво кои се однесуваат на карактеристиките и дизајнот на средствата за електронска идентификација на високо ниво.

KIBSTrust е сопственик на шемата за електронска идентификација и применува стандардни протоколи за авторизација (OpenID connect, SAML 2, WS federation) и иницирање на креирање на потпис и креирање на средства за електронска идентификација, со што се обезбедува лесна интероперабилност со било кој систем или апликација.

КИБС е исто така регистриран давател на квалификувани доверливи услуги, во рамките на кои издава квалификувани сертификати за електронски потпис.

Профилот на квалификуваниот сертификат издаден на далечински QSCD, како дел од средството за електронска идентификација е опишан во CP/CPS (точка 7.0).

1.3.2. Регистрациона канцеларија

Регистрационата канцеларија (РК) е ентитет кој врши проверка на идентификациските податоци на субјектот пред издавање на сертификат и средство за електронска идентификација, иницира или проследува барања за поништување на сертификати/отповикување на средства за електронска идентификација и одобрува барања за обновување на парот клучеви. KIBSTrust делува како РК за квалификуваните сертификати и средства за електронска идентификација што ги издава.

КИБС може да склучи договори со едно или повеќе трети лица, за извршување на дел или сите обврски (outsourcing) на РК. Во овој случај, третото лице претставува Регистрациона канцеларија (РК) и таа ги

[5] Правилник за процедурите и стандардите за исполнетост на техничките, физичките и организациските мерки за сигурност на шеми за електронска идентификација (Службен весник на РСМ 53/20).

извршува своите обврски во целосна усогласеност со овие Практики и CP/CPS, соодветните процедури за проверка и верификација на идентитет и условите од договорот на РК, потпишан помеѓу РК и КИБС.

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

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

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

1.3.3. Субјект на електронска идентификација

Субјект на електронска идентификација (Субјект) подразбира физичко лице на кое KIBSTrust му обезбедува услуги во согласност со овие Практики, односно му издава средство на електронска идентификација врз основа на негово барање.

1.3.4. Засегнати страни

Засегната страна е правно лице кое со цел да обезбеди електронски услуги за своите клиенти се потпира на довербата во средствата за електронска идентификација, издадени од KIBSTrust. Засегнатите страни имаат склучено договор за интеграција на своите услуги со услугата KIBSTrust OneID со цел да преземат множество на податоци – атрибути за Субјектот и/или да се потпрат на тие податоци содржани во средствата за електронска идентификација на своите клиенти.

Преземањето на атрибутите од средството за електронската идентификација од страна на засегнатата страна е единствено со изречна согласност на Субјектот.

Засегнатата страна објавува политика за приватност со која се обврзуваат дека со личните податоци на субјектите за електронска идентификација ќе се однесуваат согласно барањата на Законот за заштита на лични податоци. Со давањето на својата согласност за пренос на атрибутите од неговото средство за електронска идентификација Субјектот ја прифаќа и политиката на приватност на засегнатата страна.

Засегнатите страни, пред да се потпрат на информациите од средството за електронска идентификација на клиентот, што се содржани во него, мора да ја проверуваат валидноста на сертификатот преку соодветни услуги за валидација на сертификати обезбедени од KIBSTrust.

1.3.5. Други учесници

Другите учесници вклучуваат:

- Доверлив извор на податоци, како што е Централниот регистар на население (ЦРН).
- Надворешни компании со кои, врз основа на договор, KIBSTrust остварува деловни и технички релации како што се автоматизирани услуги за верификација на документи за лична идентификација; outsourcing на потребата за средства, доверливи системи и процедури за генерирање, безбедно чување и обезбедување на други делови од животниот циклус на коренските и издавачките сертификати на KIBSTrust.

1.4. Примена на електронска идентификација

При издавање на средство за електронска идентификација се применува далечинска проверка и потврда на лични и други податоци на физички лица, кои ќе бидат вклучени во издадениот квалификуван сертификат од страна на KIBSTrust.

Средството за електронска идентификација му овозможува на субјектот којшто учествува во електронска трансакција да го докаже својот идентитет на другите учесници во таквата трансакција.

Засегнатите страни, даватели на електронска услуга кон своите клиенти, применуваат електронска идентификација за проверка на идентитетот на својот клиент, односно се потпираат на податоците од средството за електронска идентификација за да овозможат автентикација и авторизација на своите клиенти.

1.4.1. Дозволена употреба на услугата за електронска идентификација

1.4.1.1. Субјект на електронска идентификација

Субјектот се согласува со условите и правилата за користење на услугата за електронска идентификација. Личните податоци преземени во процесот на електронска идентификација се користат во процесот на онлајн потпишување согласност за издавање на сертификат за квалификуван потпис. Потпишувањето на согласноста се прави со еднократен сертификат издаден само еднаш врз основа на точната идентификација на корисникот во процесот на регистрација и креирање на електронскиот идентитет. Регистриран корисник може да го искористи електронскиот идентитет повеќекратно се до истекот на важноста на квалификуваниот сертификат.

Средството за електронска идентификација се користи од страна на субјектот за автентикација а може да се користи и за потпишување електронски документи, под услов употребата на друг начин да не е забранета со закон, со овие Практики, Правилата и условите за користење и други договори со корисниците.

1.4.1.2. Засегнати страни

Засегнатите страни ќе ги користат податоците на субјектот од средството за електронска идентификација откако субјектот ќе даде согласност. Согласно договорните одредби помеѓу KIBSTrust и засегнатата страна, а со дадена согласност од субјектот, засегнатата страна може со сигурност да се потпре на точноста на атрибутите од средството за електронска идентификација, преземајќи минимално или дополнително множество на податоци за идентификација на лицето кои на единствен начин претставуваат конкретно физичко лице.

Минималното и дополнителното множество на податоци за идентификација на лицето се во согласност со барањата на Правилникот произлезен од законот МК-eIDAS, Законот за спречување перење пари и финансирање тероризам.

За минимално множество на атрибути за идентификација на лица кои употребуваат средства за електронска идентификација, се утврдува: име, презиме, дата на раѓање, единствен матичен број или број за идентификација. Дополнително множество на атрибути може да бидат: име и презиме при раѓање, место на раѓање, тековна адреса, пол, број на документот за идентификација или сериски број на средството за електронска идентификација, органот кој го издал документот и дата на важење, односно назив на издавачот на средството за електронска идентификација и периодот на важност на средството за електронската идентификација.

Засегнатите страни кои овозможуваат електронско потпишување со средството за електронска идентификација треба да ја проверат валидноста на сертификатот така што ќе го потврдат статусот на сертификатот и електронскиот потпис на издавачот што го издал сертификатот. KIBSTrust не сноси одговорност доколку засегнатата страната не направи такви проверки, ако нема право да ги обработува личните податоци на корисникот или ако ги обработува прекршувајќи го важечкото законодавство.

Засегнатите страни може да го користат OID на CP на KIBSTrust, идентификуван во сертификатот за соодветно прифаќање или одбивање на користењето на сертификатот.

1.4.2. Забранета употреба

Услугата за електронска идентификација ќе се користи само до таа мера до која користењето е во согласност со важечки закони, а особено согласно на барањата за заштита од перење пари (AML) и барањата за запознавање на својот корисник на услуги (KYC).

Услугата за електронска идентификација не треба да се користи на начин што може да доведе до нарушување на доверливоста, интегритетот и безбедноста на податоците.

1.5. Администрирање на овој документ

1.5.1. Организација која го администрира документот

Овие Практики, CP/CPS на ИС и релевантните документи што се наведени овде ги одржува Одбор за управување со политиките (ОУП) на KIBSTrust - Policy Management Authority (PMA), којшто може да се контактира на:

КИБС АД Скопје
Кузман Јосифовски Питу 1
1000, Скопје, Република Северна Македонија

1.5.2. Информации за контакт

Менаџер за PKI политики на KIBSTrust
е-пошта: pma@kibstrust.com
тел. +389 2 5513401, +389 2 3297401

1.5.3. Лице кое ја определува соодветноста на овие правила

Координатор на Одборот за управување со политиките на KIBSTrust ја утврдува соодветноста и применливоста на овие Практики врз основа на резултатите и препораките од ревизиите за сообразност.

1.5.4. Процедура за одобрување на правилата

Одобрување на овие Практики и последователните измени се прават од страна на ОУП. Измените се документ што содржи изменета форма на Практики или како забелешка за ревидиран текст. Изменетите верзии или ажурираните одредби се поврзани со делот за ажурирања и известувања за практики на складиштето на KIBSTrust што се наоѓа на: https://pki.kibstrust.com/repository. Дури и ако нема задолжителна причина за промена на овие Практики, ОУП спроведува процес на преглед најмалку еднаш годишно во обид за подобрување.

1.6. Дефиниции и кратенки

Види Додаток А за табела на кратенки и дефиниции.

2. ОДГОВОРНОСТ ПОВРЗАНА СО ОБЈАВУВАЊЕ И СМЕСТУВАЊЕ

2.1. Складиште за јавно информирање

KIBSTrust во своето складиште за јавни информации ги објавува во најмала мера следниве информации кои се однесуваат на издавањето средства за електронска идентификација:

- Практики за давање услуга за електронска идентификација
- CP/CPS за издавање сертификати,
- Политики за сертификати,
- Преглед на хиерархијата за сертификати,
- Резултати од ревизија,
- Политика на осигурување,
- Сертификати, вклучувајќи коренски и издавачки сертификати,
- Профили на сертификати,
- Правила и услови за користење на квалификувани доверливи услуги,
- Политика на приватност,
- Регистар на поништени сертификати,
- Пребарување на сертификат за кој субјектот дал согласност за објавување.

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

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

2.2. Објавување на информации

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

2.2.1. Политики на објавување и известување

Овие Практики и референцираните CP/CPS на KIBSTrust се објавени во складиштето за јавно информирање на: https://pki.kibstrust.com/repository. Документите на KIBSTrust се објавуваат заедно со датумите на применување не порано од 10 дена пред нивно стапување во сила.

2.2.2. Делови кои не се објавуваат

Види дел 9.3.1 од овој документ.

2.3. Време и периодичност на објавување

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

Ажурираните одредби и услови се објавуваат според потреба. Сертификатите се објавуваат веднаш по издавање, доколку субјектот дал согласност за објавување на сертификатот во јавниот именик на издадени сертификати.

2.4. Контрола на пристап во складиштата

Информациите објавени во делот на складиштето на веб страницата на KIBSTrust се јавно достапни информации. Пристап до таквата информација со опција само за преглед не е ограничена. KIBSTrust бара лицата да се согласат со Правилата и условите како услов за пристап до сертификатите, до информациите за статусот на сертификатите или до CRL. KIBSTrust 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. KIBSTrust го прави своето складиште јавно достапно само на начин за да може да се прочитаат информациите, посебно на линкот https://pki.kibstrust.com/repository.

3. ИДЕНТИФИКАЦИЈА И АВТЕНТИКАЦИЈА

Согласно позитивно спроведена проверка од надворешно сертификационо тело за оценка на сообразноста, KIBSTrust применува шема за електронска идентификација со високо ниво на сигурност во фазата на пријавување и регистрација на субјект на електронска идентификација и во фазата на проверка на идентитет и верификација на физички лица.

Шемата за електронска идентификација предвидува:

- проверката на идентитетот на физичкото лице да биде спроведена со користење на биометриски податоци или физички карактеристики кои на единствен начин го поврзуваат лицето со документот за лична идентификација за што има и потврда од доверлив извор или
- проверката на физичкото лице за кое веќе е издадено еквивалентно валидно средство, односно квалификуван електронски потпис кој е издаден од страна на регистриран или признаен давател на квалификувани доверливи услуги.

Личните податоци на Субјектите се обработуваат на начин што гарантира високо ниво на безбедност, вклучително и заштита од неовластена или незаконска обработка и од случајно губење, уништување или оштетување, со примена на соодветни технички и организациски мерки.

Содржината на дел од точките во оваа глава, што се однесува на квалификуваниот сертификат којшто се издава како дел од средството за електронска идентификација се посочува кон соодветната точка од погоре наведените CP/CPS.

3.1. Именување

Види точка 3.1 од CP/CPS.

3.2. Првична потврда на идентитетот

KIBSTrust користи методи опишани во овој дел за да го утврди идентитетот на субјектот на електронска идентификација. KIBSTrust може да одбие да издаде средство за електронска идентификација според свој избор, доколку проверката на идентитетот не е успешна.

KIBSTrust применува далечинско докажување и автоматска верификација на идентитетот на лицето кое бара издавање на средство за електронска идентификација. Во случај на неуспешна автоматска верификација може да се активира агент на РК на KIBSTrust.

Втор начин на потврда на идентитетот е со квалификуван електронски потпис, доколку субјектот на електронска идентификација претходно поседува валиден квалификуван сертификат за електронски потпис издаден од регистриран давател на квалификувани доверливи услуги.

И во двата случаи процесот започнува со регистрација и внес на податоци за креирање на корисничка сметка, било да е иницирана преку форма за внес во инсталирана мобилна апликација или преку веб форма на портал на засегната страна (компанија) чијшто систем за регистрација на корисници е интегриран со услугата за електронска идентификација KIBSTrust OneID.

3.2.1. Пријавување и регистрација на барателот

Во процесот на регистрација на корисник на мобилната апликација:

1. се внесува име, презиме, e-mail адреса (корисничко име), лозинка и потврда на лозинката,
2. се прифаќаат Условите и правилата за користење и Политика за приватност за услугата.
3. на внесената e-mail адреса ќе добие OTP-код. OTP-кодот е 6-цифрен број со важност од 60 минути. Корисникот може да побара нов OTP-код.
4. го внесува добиениот OTP код. Корисникот има 3 обиди да ја заврши потврдата на пријавената електронска адреса. По третиот неуспешен обид, сите внесени податоци за новиот корисник ќе бидат уништени и процесот на регистрирање започнува од почеток.

Корисничката сметка е креирана и може да се користи. Доколку иницијално процесот е започнат преку веб страница на засегната страна, на регистрираниот корисник му се прикажува QR код. Корисникот го фотографира QR кодот со камерата од својот мобилен телефон. Линкот го води корисникот до некое од складиштата за дистрибуција на мобилни апликации за оперативните системи (како iOS, Android, HarmonyOS). Од овие складишта се презема и инсталира мобилната апликација KIBSTrust OneID Mobile.

Следи активација на мобилен уред:

1. Корисникот на OneID Mobile се најавува на мобилната апликација со своите акредитиви (корисничко име и лозинка).
2. По успешна автентикација внесува нов ПИН код којшто ќе се користи за автентикација кон мобилната апликација.
3. Корисникот добива предлог да користи највисок степен на автентикација која е поддржан од оперативниот систем на мобилниот уред. Опционално корисникот може да овозможи биометриска автентикација т.н. FaceID или TouchID која ќе му послужи за да ја активира мобилната апликација.
4. Се креира безбедносен софтверски токен и се сместува на безбедна локација во мобилниот уред, со што уредот се означува како активиран.

Забелешка: Дозволено е корисникот да има само еден активен мобилен уред при користење на услугата OneID. Ако корисникот претходно активирал друг мобилен уред, треба да го оневозможи тој уред преку безбедносни поставки на веб-апликацијата OneID.com.

3.2.2. Далечинска потврда на идентитетот

Регистриран корисник може да побара креирање на средство за електронска идентификација и издавање на сертификат на далечински QSCD, за што ќе треба да презентира валиден документ за лична идентификација (лична карта или пасош).

Процесот на барањето за креирање на средство за електронска идентификација и далечински сертификат за електронски потпис се состои од следните чекори:

1. Автентициран корисник на мобилната апликација избира опција за OneID електронски идентитет.
2. Ги прифаќа Правилата и условите за користење и Политика за приватност за услугата KBSTrust OneID.
3. Внесува име и презиме како што се наведени во документот за лична идентификација, единствен матичен број на граѓанин (ЕМБГ) и број на документ за лична идентификација (лична карта или пасош).
4. Внесените податоци се споредуваат со податоците од доверлив извор на податоци – Централен регистар на население (ЦРН).
5. По позитивна проверка започнува процесот на верификација на документот за лична идентификација:
    a. корисникот скенира соодветни страници кои зависат од типот на документот за лична идентификација (лична карта или пасош).
    b. со регистрираниот мобилен уред прави фотографирање на своето лице (selfie).
    c. врз основа на случајно генерирани налози за придвижување добиени од мобилната апликација прави видео кое служи за потврда на неговата живост.
6. Системот во позадина прави проверка дали документот за лична идентификација е оригинален и издаден од орган на државата Република Северна Македонија, прави биометриска споредба на фотографијата од документот и фотографијата на лицето направена со камерата на регистрираниот мобилен уред, прави споредба на извлечените податоци од документот за лична идентификација со податоците од ЦРН.
7. Во случај на проблем со проверката на идентитет, се известува агент во РК на КИБС, којшто може да го провери и потврди идентитетот во процесот на електронска идентификација.
8. По позитивна верификација започнува автоматизиран процес на барање за издавање сертификат, потврдување и издавање на сертификат за електронски потпис.
9. Барањето за издавање на сертификат се потпишува со сертификат за еднократна употреба што се креира со податоците на корисникот и се одобрува издавање на квалификуван сертификат.
10. Со издавање на сертификатот завршен е процесот на издавање средство за електронска идентификација.

Сите лични податоци извлечени од документ и резултатот на верификацијата на идентитетот се чуваат од KIBSTrust како доказ за далечинската трансакција за електронска идентификација.

3.2.3. Потврда на идентитетот со издадено еквивалентно валидно средство

Регистриран корисник може да побара креирање на средство за електронска идентификација и издавање на сертификат на далечински QSCD, така што ќе презентира дека поседува валиден квалификуван сертификат за електронски потпис (за чие издавање претходно била направена потврда на идентитетот).

Процесот на барањето и креирање на средство за електронска идентификација и далечински сертификат за електронски потпис се состои од следните чекори:

1. Корисникот од мобилната апликација одбира опција за креирање OneID електронска идентификација.
2. Следи форма во која се пополнети податоци за барањето на сертификат со име и презиме (од веќе регистрираната корисничка сметка) и корисникот внесува единствен матичен број на граѓанин (ЕМБГ) и број на документ за лична идентификација (број на лична карта/пасош),
3. ги прифаќа Правилата и условите за користење на услугата.
4. Од понудените две методи ја одбира опцијата за поседување на квалификуван сертификат издаден од KIBSTrust со што се испраќа email порака до претходно регистрираната email адреса на корисникот.

5. Email пораката содржи единствена привремена врска до веб апликацијата www.OneID.mk. Врската истекува за 24 часа.
6. Се прави првична проверка на видот на уредот што се користи за отворање на врската. Потребно е врската да се отвори од десктоп компјутер, бидејќи ќе се понуди да се потпише барањето со квалификуван сертификат издаден на локално QSCD. Се креира XML документ што ги содржи податоците што треба да се верификуваат.
7. Корисникот го потпишува XML документот со валиден квалификуван сертификат издаден од KIBSTrust. Се верификува квалификуваниот сертификат со кој е потпишан XML документот и се проверува врската меѓу сертификатот и Единствениот матичен број на граѓанин што се содржи во податоците за верификација на XML.
8. Ако проверката е во ред, барањето за издавање средство за електронска идентификација се одобрува и се издава нов сертификат во далечинско QSCD. Корисникот е известен дека податоците за издадениот сертификат се запишани во неговата мобилна апликација KIBSTrust OneID Mobile.
9. Издадениот сертификат е запишан во мобилната апликација.

3.3. Идентификација и автентикација на барања за обновување или замена

Пред истекот на постоечки сертификат, неопходно е субјектот да добие нов сертификат за да го одржи континуитетот на користење на сертификатот во рамките на средството за електронска идентификација. Процесот на обновување на електронскиот идентитет на субјектот значи да му се генерира нов пар клучеви за да се замени парот на кој му истекува важноста (технички дефинирано како ,,обнова на пар клучеви“ (re-key)).

Корисникот може да побара обновување 30 дена пред истекот на важноста на сертификатот. Автентикација на барањето за обнова се прави со електронски потпис со сеуште важечкиот сертификат.

Корисникот може да направи обнова само еднаш без повторна идентификација. При следно барање за обнова мора да се помине постапката на идентификација како и при првична потврда на идентитетот.

Процесот на обнова може да биде иницира од субјектот и во случаите на замена на мобилниот уред.

Ако корисник кој има активен OneID сертификат сака да продолжи да го користи на нов мобилен уред или во случај на бришење на апликацијата OneID Mobile од постоечки уред, треба да се проследат следните чекори:

1. Инсталирање на мобилната апликација OneID Mobile,
2. Автентикација со корисничко име за коешто има активен сертификат. Мобилната апликација известува дека постои активен сертификат со податоци за активирање на друг уред и дека за да се направи замена, мора да се потврди поништувањето на стариот сертификат.
3. Потврдување на барањето за поништувањето на стариот сертификат:
   (1) со одобрување од мобилен уред каде што е регистриран стариот сертификат (ако тој сеуште го има во владение стариот уред со активна апликација), или
   (2) користејќи OTP код што се испраќа до мобилниот број што бил верификуван при издавање на сертификатот што треба да се поништи.
4. Иницирање на барање за издавање на нов сертификат коешто се потпишува со сертификат за еднократна употреба што се креира со податоците на корисникот проверени во ЦРН.

Со издавање на нов квалификуван сертификатот завршен е процесот на замена на средство за електронска идентификација.

3.4. Идентификација и автентикација на барање за отповикување

Сите барања за отповикување на средствата за електронска идентификација и поништување на квалификуваниот сертификат мора да бидат автентицирани.

Пред да биде поништен сертификат, се проверува дали поништувањето е побарано од субјектот на сертификатот или ентитетот кој го одобрил барањето за сертификат.

Прифатливите процедури за автентикација на барање за отповикување/поништување од субјектот вклучуваат една или повеќе од следниве постапки:

- Субјектот доставува електронски образец за поништување преку веб порталот на KIBSTrust автентициран како регистриран корисник со дополнително сигурносно ниво, обезбедено со двофакторска автентикација;
- Добивање порака по електронска пошта од email адресата на субјектот кој бара поништување, а која содржи електронски потпис којшто може да се верификува со квалификуваниот сертификатот што треба да се поништи;
- Комуникација со субјектот што ќе обезбеди разумни уверувања кои потврдуваат со сигурност дека лицето кое бара поништување е навистина субјектот или има прописно овластување да го побара тоа. Таквата комуникација, во зависност од околностите, може да вклучи едно или повеќе од следново: телефон или лично присуство на субјектот, или со достава на прописното овластување преку стандардна пошта или курирска служба.

Администраторите на РК на KIBSTrust се овластени да побараат поништување сертификати во рамките на доменот на KIBSTrust. Пред да се даде дозвола на администраторот да ја изведе функцијата на поништување, ќе се изврши автентикација на идентитетот на администраторот преку контрола на пристапот со употреба на SSL и клиентска автентикација.

Отповикување на средството за електронска идентификација може да се направи на повеќе начини во зависност од потребата на корисникот, како на пример: изгубен или оштетен мобилен уред на корисникот или корисникот сака да ја откаже услугата од други причини.

Доколку корисничкиот уред е функционален, корисникот може да го отповика средството за електронска идентификација преку мобилната апликација OneID Mobile од менито за кориснички профил, каде има опција за затворање на сметката. Оваа опција ќе ги избрише сите податоци на уредот, ќе го деактивира уредот, ќе го поништи сертификатот и ќе ги избрише сите податоци за активација на средството.

доколку корисникот не го поседува својот уред (изгубен или украден), може да се користи постапката за откажување преку алтернативни канали (центар за повици за поддршка, веб портал за корисници на OneID услуга).

Корисникот може да се автентицира на веб порталот за услугата OneID и да одбере опција за отповикување на средство за електронска идентификација, што ќе значи бришење на податоците од мобилниот уред и поништување на квалификуваниот сертификат за електронски потпис.

Доколку корисникот се јавува на број на центар за поддршка, за автентикација на барањето за отповикување на средство за електронска идентификација/поништување на сертификатот, покрај личните податоци, корисникот мора да има пристап до адреса за е-пошта преку која се прави верификација на барањето. Агентот од центарот за поддршка ги проверува податоците и ја верификува адресата за е-пошта така што активира генерирање и испраќање на OTP код на е-пошта на корисникот. Корисникот го чита OTP кодот и го претставува на телефонски повик до центарот за повици.

Откако корисникот е идентификуван, серискиот број на активниот OneID сертификат може недвосмислено да се најде во OneID Backoffice системот. Забелешка: за една e-mail адреса (корисничко име) има само еден активен сертификат.

Во рамките на PKI системот, врз основа на утврдениот сериски број, сертификатот се поништува и се бришат активациските податоци за средството за електронска идентификација.

Откако ќе се поништи сертификатот и издаденото средство за електронска идентификација, корисникот треба да ја следи истата постапка за издавање ново средство за електронска идентификацијасо што ќе поднесе ново барање и одново ќе го помине процесот на верификација на идентитетот (точка 3.2.2).

3.5. Идентификација и автентикација на барање од засегната страна

Кога засегната страна за својата електронска услуга, којашто е интегрирана со KIBSTrust OneID, има потреба да преземе податоци за електронска идентификација на својот клиент - субјект на средството за електронска идентификација, бара од корисникот да се автентицира со својата корисничка сметка. По успешна основна автентикација, позадинскиот систем OneID Backend испраќа т.н. Push нотификација до

мобилната апликација за второстепена автентикација (2FA). Веб апликацијата на засегнатата страна е во состојба на чекање за потврден статус на автентикацијата. Субјектот добива Push нотификација на својата OneID Mobile апликација и го внесува својот ПИН или користи биометриски податоци (FaceID/TouchID) за го отвори известувањето. На корисникот му се прикажуваат детали за барањето согласност (име на засегнатата страна и множеството на податоци кои се бараат) и му се нудат опции да прифати или откаже согласност. Доколку даде согласност за преземањето, се креира софтверски токен за пристап, со што далечински го активира приватниот клуч од квалификуваниот сертификат што се чува на далечински QSCD во KIBSTrust системот, за да се создавање квалификуван електронски потпис на согласноста за преземање на личните идентификациски податоци. Системот на засегнатата страна ги добива податоците за електронска идентификација на корисникот.

4. ОПЕРАТИВЕН ЖИВОТЕН ЦИКЛУС НА СЕРТИФИКАТОТ ОД СРЕДСТВОТО ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

4.1. Барање за сертификат како дел од средство за електронска идентификација

4.1.1. Кој може да поднесе барање за сертификат

Барање за квалификуван сертификат може да поднесе субјектот на електронска идентификација во рамките на процесот на создавање на средство за електронска идентификација кое е и субјект на сертификатот, доколку е законски квалификувано.

Издавање на средство за електронска идентификација може да побараат сите физички лица над 15 години кои имаат валиден документ за лична идентификација издаден од државен орган на Република Северна Македонија.

4.1.2. Процес на регистрирање и одговорности

Субјектот на електронска идентификација се согласува со Правилата и условите за издавање на сертификати, кои содржат изјави и гаранции опишани во делот 9.6.3 и поминуваат низ процесот на регистрација кој се состои од:

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

4.2. Обработка на барањето за сертификат

4.2.1. Извршување на функциите на идентификација и автентикација

KIBSTrust врши идентификација и автентикација на сите потребни информации за барателот:

(1) на оддалеченост со квалификуван сертификат, или
(2) со употреба на метод еквивалентен на физичко присуство, во согласност со дел 3.2.

Ако РК помага во верификацијата, тогаш РК мора да креира и да одржува евиденција доволна за да утврди дека ги извршила своите потребни задачи за верификација и му го соопштува на KIBSTrust завршувањето на таквите задачи.

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

4.2.2. Одобрување или одбивање на барањата за сертификат

По успешна далечинска проверката на идентитетот на лицето и автоматска валидација на податоците, барањето за издавање на сертификатот во рамките на средството за електронска идентификација автоматски се одобрува.

4.2.3. Време на обработка на барањата за сертификат

КИБС започнува со обработка на барањата за сертификат веднаш по успешна електронска верификација на идентитетот на барателот. Барањето за сертификат останува активно сè додека не се одбие, издаде или автоматски не истече во рок од 30 дена.

4.3. Издавање сертификат

4.3.1. Активности за време на издавање на сертификатот

Сертификатот се креира и издава по успешна верификација на идентитетот на барателот, регистриран корисник на мобилната апликација како дел од средството за електронска идентификација.

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

4.3.2. Известување на субјектот за издавање на сертификатот

KIBSTrust ги известува субјектите дека сертификатите се креирани и им овозможува на субјектите пристап до сертификатите известувајќи ги дека истите им се достапни. Сертификатите им се стават на располагање на субјектите, преку мобилната апликација за управување со електронскиот идентитет.

4.4. Прифаќање сертификат

4.4.1. Однесување кое означува прифаќање на сертификатот

Следниве постапки престставуваат прифаќање на сертификатот:

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

4.4.2. Објавување на сертификатот

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

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

РК може да добие известување за издавањето на сертификатот кој е последица на позитивно завршена далечинска електронска идентификација.

4.5. Користење на парот клучеви и на сертификатот

4.5.1. Користење на претплатничкиот приватен клуч и сертификатот

Погледнете точка 4.5.1 од документот CP/CPS.

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

Погледнете точка 4.5.2 од документот CP/CPS.

4.6. Обновување сертификат

Не се применува обновување на сертификат со истиот пар на клучеви.

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

Погледнете точка 4.7 од документот CP/CPS.

4.8. Изменување на сертификат

4.8.1. Околности за изменување на сертификат

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

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

KIBSTrust врши идентификација и автентикација на сите потребни информации на субјектот во согласност со дел 3.2.

4.8.4. Известување на субјектот за издавање на нов сертификат

Види дел 4.3.2.

4.8.5. Однесување кое означува прифаќање на изменетиот сертификат

Види дел 4.4.1.

4.8.6. Објавување на изменетиот сертификат од страна на ИС

Види дел 4.4.2.

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

Види дел 4.4.3.

4.9. Поништување и суспендирање на сертификат

Со поништувањето на сертификат трајно завршува оперативниот период на сертификатот пред сертификатот да го достигне крајот на наведениот период на важење. Со поништување на сертификатот се поништува и електронскиот идентитет на корисникот.

Барањето за поништување се автентицира според дел 3.4, пред да се изврши поништување на сертификатот.

Поништување на сертификати се врши според наведеното во следните точки.

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

4.9.1. Околности за поништување

Правилата и условите на KIBSTrust обезбедуваат обврска и/или право на субјектот да бара поништување на сертификат. Само во околностите наведени подолу, сертификатот поврзан со средството за електронска идентификација ќе биде поништен од страна на KIBSTrust или од субјектот и објавен во CRL.

Сертификатот за субјект се поништува ако:

- KIBSTrust или субјектот имаат причина да веруваат или да се сомневаат дека се случило компромитирање на приватниот клуч на субјектот. Доколку трето лице пријави компромитација, KIBSTrust бара соодветна потврда од субјектот;
- KIBSTrust има причина да верува дека субјектот прекршил материјална обврска, изјава или гаранција од применливите Правила и услови за користење на квалификувани доверливи услуги;
- KIBSTrust има причина да верува дека сертификатот е издаден спротивно на процедурите од CP/CPS, издаден е на лице различно од она што е наведено како субјект во сертификатот, или сертификатот е издаден без овластување на лицето наведено како субјект во сертификатот;

- KIBSTrust е свесен за измените кои влијаат врз валидноста на сертификатот;
- Користената криптографија повеќе не обезбедува поврзување на субјектот и јавниот клуч;
- KIBSTrust има причина да верува дека некој од материјалните факти во барањето за сертификат е погрешен;
- KIBSTrust утврдил дека материјалниот предуслов за издавање на сертификатот ниту е задоволен ниту одречен;
- Субјектот ја губи правната квалификуваност, прогласен е за отсутен или починат, имајќи предвид дека сертификатот во секој случај е непреносliв;
- Субјектот ја губи можноста да го користи локалното QSCD или мобилниот уред потребен за пристап до далечинското QSCD;
- Во случај кога субјектот на сертификатот е физичко лице поврзано со субјект - правно лице и субјектот бара поништување;
- Во случај на судска одлука без право на жалба која наложува поништување на сертификатот;
- Приватниот клуч на KIBSTrust е компромитиран;
- Надзорното тело бара поништување според законот;
- Идентитетот на субјектот не е успешно повторно верификуван;
- Субјектот не извршил плаќање кое доспеало;
- Продолжување со употребата на тој сертификат е штетен за KIBSTrust;
- Настанале промени во стандардите и техничките барања усвоени од страна на CA/B форумот и/или регулативата и законите на ЕУ и Република Северна Македонија.

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

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

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

Според Правилата и условите на KIBSTrust , субјектот на електронската идентификација е должен веднаш да го извести KIBSTrust за сознанието или претпоставката дека неговиот приватен клуч е компромитиран.

По одобрување на барањето за поништување од страна на KIBSTrust, 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;
- субјектот на електронската идентификација, или негов правен застапник, или наследник кој сака да побара поништување во случај на починат субјект (физичко лице) под услов тоа да е законски квалификувано;
- надлежен суд или орган;
- Надзорно тело.

Барање за поништување на ИС сертификат (коренски или издавачки) може да поднесе:

- КИБС, кој е субјект на сертификатот, законски квалификуван;
- надлежен суд или орган;
- Надзорно тело.

4.9.3. Процедура на барање за поништување

Субјектот кој бара поништување треба да упати барање до KIBSTrust за поништување на еден од следниве начини: преку онлајн услуга за поништување, по електронска пошта на revoke@kibstrust.com или образец

во хартиена форма за поништување на сертификат кој се доставува лично до РК по што веднаш ќе биде иницирано поништување на сертификатот.

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

4.9.4. Грејс период за барање за поништување

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

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

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

Веднаш по одобрувањето на барањето за поништување, KIBSTrust го известува субјектот за реализирање на поништувањето преку е-порака.

4.9.6. Барања за проверка на поништувањето од 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 KIBSTrust што го издал сертификатот на кој засегнатите страни сакаат да се потпрат. Како друга можност, засегнатите страни може да го проверат статусот на сертификатот со користење на веб-базираното складиште на KIBSTrust или со користење на технологија обезбедена со OCSP респондер. KIBSTrust ќе им обезбеди на засегнатите страни информација како да го пронајдат соодветниот CRL, веб-базираното складиште или OCSP респондерот за да го проверат статусот на поништување. Поради бројните и различните локации за CRL складиштата, засегнатите страни ќе бидат известени да пристапат до CRL со помош на URL поставени во екстензијата за CRL точките на дистрибуција на сертификатот.

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

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

4.9.7. Интервали на издавање на CRL

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

4.9.8. Максимално доцнење на CRL

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

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

Информации во врска со онлајн поништување, како и други информации за статусот на сертификатот се достапни преку веб-базираното складиште и OCSP. Покрај објавувањето на CRL, KIBSTrust обезбедува информации за статусот на сертификат и преку функциите за пребарување во складиштето на KIBSTrust. Информации за статусот на сертификатот за квалификувани сертификати се достапни во складиштето на KIBSTrust на: https://pki.kibstrust.com/repository.

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

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

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

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

4.9.10. Барања за онлајн проверка на поништување

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

4.9.11. Други достапни форми на огласување за поништување

Не се применува.

4.9.12. Посебни барања во врска со компромитирање на клуч

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

4.9.13. Околности за суспендирање

Не се применува.

4.9.14. Кој може да побара суспендирање?

Не се применува.

4.9.15. Процедура за барање за суспендирање

Не се применува.

4.9.16. Ограничувања на периодот на суспензија

Не се применува.

4.10. Услуги во врска со статусот на сертификатите

4.10.1. Оперативни карактеристики

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

4.10.2. Достапност на услуги

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

4.10.3. Опционални карактеристики

Не се применува.

4.11. Крај на претплатата

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

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

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

Не се применува.

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

Не се применува.

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

Не се применува.

5. ОБЈЕКТ, УПРАВУВАЊЕ И ОПЕРАТИВНИ КОНТРОЛИ

5.1. Физички контроли

Погледнете точка 5.1. од документот CP/CPS.

5.1.1. Локација на објект и негова конструкција

Погледнете точка 5.1.1 од документот CP/CPS.

5.1.2. Физички пристап

Погледнете точка 5.1.2 од документот CP/CPS.

5.1.3. Електрична енергија и климатизација

Погледнете точка 5.1.3 од документот CP/CPS.

5.1.4. Изложеност на вода

Погледнете точка 5.1.4 од документот CP/CPS.

5.1.5. Превенција од пожар и противпожарна заштита

Погледнете точка 5.1.5 од документот CP/CPS.

5.1.6. Складирање на медиумите

Погледнете точка 5.1.6 од документот CP/CPS.

5.1.7. Отстранување отпад

Погледнете точка 5.1.7 од документот CP/CPS.

5.1.8. Резервни копии (бекап) надвор од деловните простории

Погледнете точка 5.1.8 од документот CP/CPS.

5.2. Процедурални контроли

5.2.1. Доверливи улоги

Погледнете точка 5.2.1 од документот CP/CPS.

5.2.2. Број на лица потребни за една работна задача

Погледнете точка 5.2.2 од документот CP/CPS.

5.2.3. Идентификација и автентикација за секоја улога

Погледнете точка 5.2.3 од документот CP/CPS.

5.2.4. Работни улоги за кои е потребно одвојување на должностите

Погледнете точка 5.2.4 од документот CP/CPS.

5.3. Контроли на персоналот

Погледнете точка 5.3 од документот CP/CPS.

5.3.1. Барања за квалификации, искуство и дозволи

Погледнете точка 5.3.1 од документот CP/CPS.

5.3.2. Процедури за проверка на биографијата

Погледнете точка 5.3.2 од документот CP/CPS.

5.3.3. Неопходна обука

Погледнете точка 5.3.3 од документот CP/CPS.

5.3.4. Услови и период на повторна обука

Погледнете точка 5.3.4 од документот CP/CPS.

5.3.5. Период и редослед на ротирање на работните места

Не се спроведува ротирање.

5.3.6. Санкции за неовластени дејствија

Погледнете точка 5.3.6 од документот CP/CPS.

5.3.7. Предуслови за независни лица по договор

Погледнете точка 5.3.7 од документот CP/CPS.

5.3.8. Документација што му се обезбедува на персоналот

Погледнете точка 5.3.8 од документот CP/CPS.

5.4. Процедури за ревизорска трага (Audit logging procedures)

5.4.1. Видови настани што се евидентираат

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

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

- Користење на сертификатот за електронско потпишување.
- Обиди за најава на регистриран корисник.

- Настани поврзани со услугите за електронска идентификација
  - Регистрација на нов корисник на мобилна апликација
  - Верификација на документите за лична идентификација
  - Верификација на живост на лицето
  - Потврда на биометриските податоци при детекција на живост и фотографијата од документот за лична идентификација
  - Проверка на нечиј електронски идентитет од системите на засегната страна
  - Употреба на електронскиот идентитет за автентикација на носителот.
- Настани за доверливи вработени, вклучително:
  - Обиди за најавување и одјавување,
  - Обиди за креирање, отстранување, поставување лозинки или промена на системските привилегии на сите привилегирани корисници,
  - Промени во персоналот.
- Сите важни настани поврзани со сигурноста, кои вклучуваат:
  - Успешни или неуспешни обиди за пристап до PKI системот,
  - Стартување и исклучување на системи и апликации,
  - Поседување на активациски податоци за операциите на приватен клуч на ИС,
  - PKI и безбедносни системски активности спроведени од страна на персоналот на КИБС,
  - Безбедносно чувствителни документи или евиденција што се прочитани, напишани или избришани,
  - Промени на правилата во Политиката за безбедност,
  - Испади на системот, откажување на хардверот и други аномалии,
  - Активности поврзани со огнени зидови (firewall) и мрежниот насочувач (рутер),
  - Влез/излез на посетители во просториите на ИС,
  - Влез/излез за пристап до далечинското QSCD.

Записите во дневникот за евиденција ги вклучуваат следниве елементи:

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

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

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

5.4.2. Интервал на преглед на ревизорски траги

Погледнете точка 5.4.2 од документот CP/CPS.

5.4.3. Период на зачувување на ревизорските траги

Погледнете точка 5.4.3 од документот CP/CPS.

5.4.4. Заштита на ревизорските траги

Погледнете точка 5.4.4 од документот CP/CPS.

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

Погледнете точка 5.4.5 од документот CP/CPS.

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

Погледнете точка 5.4.6 од документот CP/CPS.

5.4.7. Известување до субјектот што го предизвикал настанот

Погледнете точка 5.4.7 од документот CP/CPS.

5.4.8. Проценка за ранливост

Погледнете точка 5.4.8 од документот CP/CPS.

5.5. Архивирање на записите

5.5.1. Видови записи кои се архивираат

КИБС ИС ги архивира:

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

5.5.2. Период на чување во архивата

Периодот на чување во архивата е опишан во дел 5.4.3.

5.5.3. Заштита на архивата

Погледнете точка 5.5.3 од документот CP/CPS.

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

Погледнете точка 5.5.4 од документот CP/CPS.

5.5.5. Барања за временски печат на документацијата

Погледнете точка 5.5.5 од документот CP/CPS.

5.5.6. Систем за архивирање

Погледнете точка 5.5.6 од документот CP/CPS.

5.5.7. Процедури за добивање и верификување на архивските податоци

Погледнете точка 5.5.7 од документот CP/CPS.

5.6. Промена на клучеви

Погледнете точка 5.6 од документот CP/CPS.

5.7. Опоравување од компромитирање и од кризни ситуации

5.7.1. Процедури за справување со инциденти и компромитирање

Погледнете точка 5.7.1 од документот CP/CPS.

5.7.2. Компромитирани компјутерски ресурси, софтвер и/или податоци

Погледнете точка 5.7.2 од документот CP/CPS.

5.7.3. Процедури при компромитирање на приватниот клуч на ИС

Погледнете точка 5.7.3 од документот CP/CPS.

5.7.4. Способност за продолжување на деловните активности по кризна ситуација

Погледнете точка 5.7.4 од документот CP/CPS.

5.8. Прекин на дејноста на ИС или РК

Погледнете точка 5.8 од документот CP/CPS.

6. КОНТРОЛИ НА ТЕХНИЧКАТА СИГУРНОСТ

6.1. Генерирање и инсталирање на пар клучеви

6.1.1. Генерирање на пар клучеви

Погледнете точка 6.1.1 од документот CP/CPS.

6.1.2. Доставување на приватниот клуч на субјектот

Парот клучеви за субјектот - краен корисник се генерира на далечински QSCD управувано од страна на субјектот и не се применува физичко доставување на приватниот клуч на субјектот. Приватниот клуч се активира од страна на носителот и единствено тој може да го користи за електронско потпишување користејќи ги своите кредендијали и применувајќи строга автентикација.

6.1.3. Доставување на јавниот клуч до Издавачот на сертификати

Ова барање не се применува кога парот клучеви на субјектот претходно се генерирани од КИБС.

6.1.4. Доставување на ИС јавниот клуч на засегнатите страни

Погледнете точка 6.1.4 од документот CP/CPS.

6.1.5. Големина на клучевите

Погледнете точка 6.1.5 од документот CP/CPS.

6.1.6. Параметри за генерирање јавен клуч и проверка на квалитетот

Погледнете точка 6.1.6 од документот CP/CPS.

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

Погледнете точка 6.1.7 од документот CP/CPS.

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

Погледнете точка 6.2 од документот CP/CPS.

6.2.1. Стандарди на криптографски модули и контроли

Погледнете точка 6.2.1 од документот CP/CPS.

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

Погледнете точка 6.2.2 од документот CP/CPS.

6.2.3. Давање на чување на приватниот клуч

Погледнете точка 6.2.3 од документот CP/CPS.

6.2.4. Резервни копии (бекап) на приватен клуч

Погледнете точка 6.2.4 од документот CP/CPS.

6.2.5. Архивирање приватен клуч

Погледнете точка 6.2.5 од документот CP/CPS.

6.2.6. Пренос на приватен клуч во или од криптографскиот модул

Погледнете точка 6.2.6 од документот CP/CPS.

6.2.7. Складирање на приватниот клуч на криптографски модул

Погледнете точка 6.2.7 од документот CP/CPS.

6.2.8. Метод на активирање на приватниот клуч

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

Приватните клучеви за електронскиот идентитет на субјектот кои се на далечински QSCD се заштитени со корисничко име, лозинка, OTP кодови и вклучување на биометриска заштита на мобилната апликација на корисникот. Следниве правила се применуваат:

- Потребни се корисничкото име, лозинката и OTP-кодот на QSCD за секоја трансакција,
- Субјектот е должен да креира свој ПИН код за пристап до мобилната апликација во која на сигурен начин се зачувани неговото корисничко име и лозинката
- ПИН кодот е потребен за да се креира OTP за секоја трансакција.
- Корисникот на мобилната апликација може да постави биометриска автентикација за да не мора да го внесува ПИН кодот.
- Во случај на 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 го смени ПИН-кодот на мобилната апликација.
- Корисникот може да ја смени лозинката преку веб порталот откако ќе се автентицира.

Приватниот клуч на ИС се активира онлајн со ограничен број чувари на удели, како што е дефинирано во дел 6.2.2 од CP/CPS, 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

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

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

6.2.10. Метод на уништување на приватниот клуч

Онаму каде што е потребно, КИБС ги уништува ИС приватните клучеви и приватните клучеви на субјектот 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.

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

Погледнете точка 6.3.1 од документот CP/CPS.

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

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

Сертификат издаден од:	Употреба на приватен клуч	Период на важност
Коренски ИС	Не е пропишано со одредба	Нормално до 20 години
Издавачки ИС	Не е пропишано со одредба	Нормално до 10 години
Сертификат со долготрајна важност	Не е пропишано со одредба	Нормално 1-3 години
Сертификат на далечински QSCD	Автентикација и електронски потпис	2 години

Табела : Оперативен период на сертификатите

Покрај тоа, КИБС ИС престануваат да издаваат нови сертификати на соодветен датум (60 дена плус максималниот рок на важење на издадени сертификати) пред истекот на ИС сертификатот, така што ниту еден сертификат, издаден од подреден ИС не истекува по истекот на сите надредени ИС сертификати. Времетраењето на сертификатите на субјектот нема да го надмине животниот век на сертификатот за потпишување на ИС.

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

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

6.4. Податоци за активирање

6.4.1. Генерирање и инсталирање податоци за активирање

Погледнете точка 6.4.1 од документот CP/CPS.

6.4.2. Заштита на податоците за активирање

Погледнете точка 6.4.2 од документот CP/CPS.

6.4.3. Други аспекти на податоците за активирање

Погледнете точка 6.4.3 од документот CP/CPS.

6.5. Контроли за сигурност на компјутерите

6.5.1. Посебни технички услови за компјутерска сигурност

Погледнете точка 6.5.1 од документот CP/CPS.

6.5.2. Рангирање на сигурноста на компјутерите

Не се применува.

6.6. Технички контроли на животниот циклус

6.6.1. Контроли на развојот на системот

Погледнете точка 6.6.1 од документот CP/CPS.

6.6.2. Контроли за управување со сигурноста

Погледнете точка 6.6.2 од документот CP/CPS.

6.6.3. Безбедносни контроли на животниот циклус

Погледнете точка 6.6.3 од документот CP/CPS.

6.7. Контроли за сигурност на мрежата

Погледнете точка 6.7 од документот CP/CPS.

6.8. Временски жиг

Погледнете точка 6.8 од документот CP/CPS.

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

7.1. Профил на сертификатот

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.

Погледнете точка 7.1 од документот CP/CPS за повеќе детали.

7.2. CRL профил

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

Погледнете точка 7.1 од документот CP/CPS за повеќе детали.

7.3. OCSP профил

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

Погледнете точка 7.1 од документот CP/CPS за повеќе детали.

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 секогаш кога е направена голема промена во работата на доверлива услуга, врз база на ETSI стандардите наведени во дел 9.15.

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

КИБС има право да изврши надворешни ревизии на договарачи кои се поврзани со КИБС за да работат како агенти за автентикација.

8.1. Интервали и околности на проценките

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

8.2. Идентитет и квалификации на ревизијата

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

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

8.3. Однос на проценителот со проценуваниот субјект

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

8.4. Прашања опфатени со проценката

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

Областите на активност, предмет на внатрешна ревизија се следниве:

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

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

8.5. Дејствија што се преземаат како резултат на пропусти

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

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

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

8.6. Соопштување на резултатите

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

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

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

8.7. Самопроценки

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

9. ОСТАНАТИ ДЕЛОВНИ И ПРАВНИ РАБОТИ

9.1. Надоместоци

9.1.1. Надоместоци за издавање на средство за електронска идентификација

KIBSTrust наплатува за своите услуги на електронска идентификација за своите клиенти. Клиенти се првенствено правни лица - засегнати страни но зависно од потребите клиенти може да бидат и физички лица. Надоместокот вклучува но не се ограничува на број на електронски препознавања на далечина, број на согласности за пренос на атрибутите од средството за електронска идентификација, број на користења на квалификуваниот сертификат за електронски потписи.

9.1.2. Надоместоци за пристап до сертификатите

KIBSTrust може да 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

KIBSTrust не наплатува надоместок за пристап до информациите за поништување или за статус на сертификатот. Информации за статусот на сертификатот е преку OCSP и CRL коишто се достапни преку складиштето или на друг начин достапни на засегнатите страни. KIBSTrust не дозволува пристап до информациите за статусот на сертификатите во своите складишта на трети лица, кои при обезбедување на производи или услуги користат вакви информации за статусот на сертификатите, без претходно јасно изразена согласност од страна на субјектот.

9.1.4. Надоместоци за други услуги

KIBSTrust не наплатува надоместоци за пристап до овој документ. 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 (поврат на средства)

9.1.5.1. Продажба од далечина

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

9.2. Финансиска одговорност

9.2.1. Покритие на осигурување

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

Правилата за обештетување во согласност со осигурувањето од професионална одговорност на давателот на доверливи услуги КИБС (во натамошниот текст: Правила) го следат законот МК-eIDAS. Следејќи го подзаконскиот акт[6] на МК-eIDAS, TSP КИБС е целосно прилагоден на утврдените барања за износот на покривање на ризик од одговорност за штета. За секоја доверлива услуга, КИБС јавно издава „Правила и услови“ за користење на услугата. Овие правила и услови вклучуваат соодветни информации за осигурување од професионална одговорност на давателот на доверливи услуги.

9.2.2. Други средства

КИБС има доволно финансиски средства да ги одржува своите операции и да ги извршува своите должности, како и разумна можност да го понесе ризикот од одговорност кон субјектите 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 Практики.

9.3. Доверливост на деловните информации

9.3.1. Опсег на доверливи информации

Сите информации што станале познати при обезбедување услуги, а кои не се наменети за објавување (на пр. информации што биле познати на KIBSTrust заради функционирање и обезбедување на своите услуги) се доверливи. Субјектот има право да добие информации за себе од KIBSTrust, 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 KIBSTrust се наведени во делот 2.2 од овие Практики.

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

9.3.3. Одговорност за заштитата на доверливите информации

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

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

9.4. Приватност на личните информации

9.4.1. План за лични податоци

КИБС применува Политика за приватност, која е поставена на: http://pki.kibstrust.com/repository во согласност со важечките закони.

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

9.4.2. Информации што се третираат како приватни

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

9.4.3. Информации што не се сметаат за приватни

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

9.4.4. Одговорност за заштита на приватните податоци

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

9.4.5. Известување и согласност за користење на личните податоци

Согласно важечкиот закон за заштита на личните податоци, применливата Политиката за приватност и прифатените услови и правила за користење, личните податоци не се користат без согласност на страната на која се однесува информацијата.

9.4.6. Откривање што произлегува од судски или административен процес

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

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

Овој дел подлежи на применливите закони на територијата на државата.

9.4.7. Откривање по барање на сопственикот

Политиката за приватност содржи одредби поврзани со откривање на лични податоци на лицето кое му ги доставило тие податоци на КИБС. Овој дел е во согласност со важечкиот закон за заштита на лични податоци.

9.4.8. Други околности на откривање информации

Не се применува.

9.5. Права на интелектуална сопственост

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

9.5.1. Права на сопственост на информациите во сертификатите и информациите за поништување

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

9.5.2. Права на сопственост на информациите во оваа Практика

Субјектите прифаќаат дека КИБС ги задржува сите права на интелектуална сопственост на овие Практики и релевантните CP/CPS.

9.5.3. Права на сопственост на имиња

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

9.5.4. Права на сопственост на клучевите и материјалот со клучеви

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

9.5.5. Прекршување на правата на сопственост

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

9.6. Изјави и гаранции

9.6.1. Изјави и гаранции на издавачот на средства за електронска идентификација

KIBSTrust гарантира дека:

- ги обезбедува своите услуги во согласност со барањата и процедурите дефинирани во овие Практики и поврзаните документи;
- е во согласност со MK-eIDAS, eIDAS и поврзаните правни акти утврдени во овие Практики и поврзаните документи;
- ги објавува своите Практики и поврзаните документи и ја гарантира нивната достапност во мрежата за комуникација со јавни податоци;
- ги објавува и исполнува барањата на правилата и условите за субјекти и гарантира нивна достапност и пристап во мрежата за комуникација со јавни податоци;
- ја одржува доверливоста на информациите што ги добива во текот на снабдувањето со услугата и што не подлежат на објавување;
- води сметка за средствата з електронска идентификација, издадени од него и нивната валидност, и обезбедува можност за проверка на важноста на сертификатите;
- обезбедува пристап до приватните клучеви на далечинското QSCD на овластениот субјект на клучевите;
- обезбедува правилно управување и усогласеност на далечинското QSCD;
- го известува Надзорното тело за какви било промени во јавниот клуч што се користи за давање доверливи услуги;
- без непотребно одложување, но во секој случај во рок од 24 часа откако ќе дознае за какво било нарушување на сигурноста или загубата на интегритетот што има значајно влијание врз пружената услуга или врз личните податоци што се содржат во неа, ќе го извести Надзорниот орган и, кога е соодветно, другите релевантни тела како националниот CERT или Инспекторатот за податоци.
- кога постои можност прекршувањето на сигурноста или загубата на интегритетот да влијае негативно на физичко или правно лице на кое му е обезбедена услуга, без одложување ќе го извести физичкото или правното лице за повредата на сигурноста или за губењето на интегритетот;
- ја чува целата документација, евиденција и записи поврзани со услугите според точките 5.4 и 5.5;

- обезбедува проценка на усогласеноста според барањата и го презентира заклучокот на телото за проценка на усогласеноста на Надзорното тело за да обезбеди континуиран статус на услуги регистрирани во Регистарот при МИОа;
- има финансиска стабилност и ресурси потребни за да работи во согласност со овие Практики;
- ги објавува условите на политиката за задолжително осигурување и заклучокот на телото за проценка на усогласеноста во мрежата за комуникација со јавни податоци;
- овозможува пристап до своите услуги за лица со посебни потреби, доколку тоа е можно;
- нема материјално погрешно претставување на факт во средствата за електронска идентификација, познат или што потекнува од ентитетите преку кои се одобрува барањето за издавање средство за електронска идентификација.

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

9.6.2. Изјави и гаранции на издавачот на сертификат

KIBSTrust гарантира дека:

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

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

9.6.3. Изјави и гаранции на субјектот

Субјектите гарантираат дека:

- Сите изјави направени од субјектот во барањето за креирање на средство за електронска идентификација се вистинити, а субјектот е свесен за тоа дека KIBSTrust може да одбие да ја обезбеди услугата ако субјектот намерно претставил лажни, неточни или нецелосни информации во барањето за услуга;
- Субјектот ги почитува барањата дадени од KIBSTrust во овие Практики и поврзаните документи;
- Сите информации доставени од субјектот и содржани во средството се вистинити и во случај на промена на доставените податоци, субјектот треба да ги извести точните податоци во согласност со правилата утврдени со овие Практики и поврзаните документи;
- Средството се користи исклучиво за овластени и правни цели, во согласност со овие Правила;
- Секој е-потпис или е-печат креиран со употреба на приватниот клуч кој одговара на јавниот клуч, наведен во квалификуваниот сертификат е квалификуван е-потпис или е-печат на субјектот и квалификуваниот сертификат е прифатен и оперативен (не е истечен или поништен) во моментот кога се креира квалификуван е-потпис или е-печат,
- Податоците како ПИН, корисничко име, лозинка, OTP и т.н. со кои се пристапува до приватниот клуч се заштитени и дека ниту едно неовластено лице досега немало пристап до нив,
- Квалификуванот е-потпис се креира само на QSCD,
- Субјектот не е издавач на сертификати, и не го користи приватниот клуч што одговара на јавен клуч наведен во сертификатот за целите на дигитално потпишување на кој било сертификат (или кој било друг формат на овластен јавен клуч) или CRL, како ИС или поинаку;
- Субјектот без одложување ќе го извести КИБС, доколку приватниот клуч на субјектот е украден или потенцијално компромитиран, или пак контролата врз него е изгубена.

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

9.6.4. Изјави и гаранции на засегнатата страна

Според Правилата и условите на КИБС за користење на услугата се предвидува засегнатата страна да потврди дека поседува доволно информации за да донесе одлука за обемот до кој таа ќе одбере да се потпре на информациите во сертификатот кој е дел од средството за електронска идентификација, 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 неуспевањето да ги изврши обврските на засегната страна согласно овие Практики.

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

9.6.5. Изјави и гаранции на други учесници

Не се применува.

9.7. Одрекување на гаранциите

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

КИБС не е одговорен за:

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

9.8. Ограничувања на одговорност

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

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

9.9. Обесштетувања

9.9.1. Обесштетување од страна на субјектите

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

- Фалсификување или погрешно интерпретирање на факти од страна на субјектот во барањето на сертификат,
- Неприкажување на материјален факт во барањето за сертификат, од страна на субјектот, ако погрешната интерпретација или пропустот се направени од небрежност или со намера да се измами некоја од страните,
- Неуспехот на субјектот да го заштити претплатничкиот приватен клуч, да го користи доверливиот систем или неуспевањето на друг начин да спречи компромитирање, губење, откривање, изменување или неовластено користење на претплатничкиот приватен клуч, или

- Користењето на име (вклучително и без ограничувања во рамките на општото име, името на доменот, или електронската адреса) од страна на субјектот кое ги прекршува правата на интелектуална сопственост на трето лице.

Претплатничкиот договор може да вклучи дополнителни обврски за обесштетувања.

9.9.2. Обесштетување од страна на засегнатите страни

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

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

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

9.10. Период и прекин на важност

9.10.1. Период на важност

Овие Практики стапуваат во сила по објавувањето во складиштето на КИБС. Измените и дополнувањата на овие Практики стапуваат во сила по објавувањето во складиштето на КИБС.

9.10.2. Прекин на важност

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

9.10.3. Ефекти од прекинот на важност и продолжување

Без оглед на прекинувањето на важноста на Овие Практики, КИБС PKI учесниците , се обврзани со сите услови за сите издадени сертификати до крајот на периодот на важност на таквите сертификати.

9.11. Индивидуални известувања и комуникација со учесниците

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

Делот 1.5.1 ги дава сите достапни средства за комуникација.

9.12. Измени и дополнувања

9.12.1. Процедура на измени и дополнувања

Измените и дополнувањата на овие Практики ги прави Одборот за управување со политики (ОУП) на KIBSTrust. Измените и дополнувањата се во форма на документ кој содржи изменета и дополнета форма на документот или ажурирање. Верзиите со измените и дополнувањата или ажурирањата поврзани со складиштето на КИБС се објавени на https://pki.kibstrust.com/repository/.

Ажурирањата ги заменуваат сите наведени или спротивставени одредби на наведената верзија на документот.

9.12.2. Механизам и период на известување

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

Предложените измени и дополнувања на овие Практики и поврзаните CP/CPS се објавени со складиштето на КИБС лоцирано на: https://pki.kibstrust.com/repository/.

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

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

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

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

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

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

9.13. Одредби за решавање на спорови

9.13.1. Спорови помеѓу КИБС, претставништва и клиенти

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

9.13.2. Спорови со субјекти - крајни корисници или засегнати страни

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

9.14. Меродавно право

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

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

9.15. Усогласеност со меродавното право

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

- MK-eIDAS - Закон за електронски документи, електронска идентификација и доверливи услуги (Службен весник на Република Северна Македонија 101/19...215/19);
- eIDAS - Регулатива (ЕУ) бр. 910/2014 на Европскиот парламент и на Советот од 23 јули 2014 година за електронски услуги за идентификација и доверливи услуги за електронски трансакции на внатрешниот пазар и укинување на Директивата 1999/93 / ЕЗ;

- Закони за лични податоци донесени во Република Северна Македонија и поврзаната ЕУ регулатива;
- Поврзани европски стандарди:

  а) ETSI EN 319 401 Електронски потписи и инфраструктури (ESI); Општи барања за политика за даватели на доверливи услуги ;
  б) ETSI EN 319 411-1 Електронски потписи и инфраструктури (ESI); Барања за политика и сигурност за давателите на доверливи услуги кои издаваат сертификати; Дел 1: Општи барања;
  в) ETSI EN 319 411-2 Електронски потписи и инфраструктури (ESI); Барања за политика и сигурност за давателите на доверливи услуги кои издаваат сертификати; Дел 2: Барања за органи за сертификација за издавање квалификувани сертификати;

- Основни барања на CA / Browser Форумот,

Овие Практики подлежат на македонските закони.

9.16. Останати одредби

9.16.1. Целосност на договорот

Не се применува.

9.16.2. Доделување

Сите субјекти кои работат според овие Практики не можат да ги доделат своите права или обврски без претходна писмена согласност од KIBSTrust. 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 Практики се прогласат за неспроведливи од соодветен суд или од друг надлежен авторитет, останатиот дел од овие Практики 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 Практики не го одрекува правото на КИБС да ја спроведе истата одредба подоцна или правото да спроведе друга одредба од овие Практики. За да бидат во сила, одрекувањата мора да бидат во писмена форма и потпишани од КИБС.

9.16.5. Виша сила

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

9.17. Други одредби

Не се применува.

Додаток А. Табела на кратенки и дефиниции

Табела на кратенки

Кратенка	Опис
CA (ИС)	Certificate Authority (Издавач на сертификати)
CP	Certificate Policy (Политика за сертификати)
CPS	Certification Practice Statement (Постапки/Практика за издавање на квалификувани сертификати)
CRL	Certificate Revocation List (Регистар на поништени сертификати)
OCSP	Протокол за електронско добивање на статусот на сертификат
OID	Предметен идентификатор, единствен код на предметен идентификатор
OTP	One Time Password (Еднократна лозинка)
PIN ПИН	Персонален идентификациски број
PKI	Public Key Infrastructure (Инфраструктура на јавен клуч)
PMA	Policy Management Authority (Одбор за управување со политиката)
QSCD	Средство за креирање квалификуван електронски потпис/печат
RA (РК)	Registration Authority (Регистрациона канцеларија)
RFC	Request for Comment (Барање за забелешка)
SSL	Протокол Secure Socket Layer
TSP (ДДУ)	Trusted Services Provider (Давател на доверлива услуга)

Дефиниции

Термин	Дефиниција
Администратор	Доверливо лице во организацијата на процесирачки центар, услужен центар или управуваниот PKI клиент, кое врши валидација и други ИС или РК функции.
Администраторски сертификат	Сертификат што му се издава на администраторот и кој може да се користи само за извршување на функции на ИС или РК.
Напреден електронски потпис	Електронски потпис што ги исполнува следниве услови: • тој е единствено поврзан со потписникот; • тој е способен да го идентификува потписникот; • се креира со употреба на податоци за креирање електронски потпис така што потписникот може, со високо ниво на доверба, да ги користи под своја единствена контрола; и тој е поврзан со податоците потпишани со него, на таков начин што може да се детектира секоја последователна промена во податоците.
Сертификат за електронски потпис	електронска потврда која ги поврзува податоците за валидација на електронскиот потпис со физичко лице и која го потврдува најмалку името или псевдонимот на тоа лице. Технички тоа е јавен клуч на корисник, заедно со некои други информации, кој е шифриран со приватниот клуч на издавачот на сертификати што го издал, за да не може да се фалсификува.
Политика за сертификати (CP)	Именуван пакет правила што укажува на применливост на сертификат за одредена заедница и / или класа на примена со заеднички безбедносни барања.
Регистар на поништени сертификати (CRL)	Потпишан список што означува збир на сертификати што се поништени од Издавачот на сертификати.
Барање за потпишување сертификат (CSR)	Порака која го пренесува барањето за издавање сертификат.
Издавач на сертификати (ИС)	Орган овластен да креира и доделува сертификати.
CP/CPS	Правила за практиките што ги користи органот за сертификација при издавање, управување, поништување и обновување или сертификати со обновување на клучеви.

Термин	Дефиниција
Компромитирање	Прекршување (или претпоставено прекршување) на безбедносната политика, при кое може да се случи неовластено откривање или губење на контролата врз чувствителни информации. Во однос на приватните клучеви, компромитирање претставува губење, кражба, откривање, изменување, неовластено користење или друг вид на компромитирање на сигурноста на тој приватен клуч.
eIDAS	Регулатива на ЕУ бр. 910/2014 на Европскиот парламент и на Советот од 23 јули 2014 година за услуги за електронска идентификација и доверливи услуги за електронски трансакции на внатрешниот пазар и укинување на Директивата 1999/93 / ЕЗ.
Електронски потпис	Податоци во електронска форма кои се приложени или логички се поврзани со други електронски податоци, и кој потписникот го користи за потпишување.
Правила и услови за користење на услуги	Обврзувачки документ во кој се наведени правилата и условите според кои физичко или правно лице дејствува како субјект или како засегната страна за соодветните доверливи услуги кои ги обезбедува КИБС.
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.
Складиште (Repository)	Веб-базирано место за јавно информирање за политики и практики за издавање сертификати и средства за електронска идентификација и други релевантни информации на КИБС, достапни онлајн.
Сертификат со долготрајна важност	Квалификуван сертификат кој е валиден 1 до 3 години.
MK-eIDAS	Закон за електронски документи, електронска идентификација и доверливи услуги. (Службен весник на Република Северна Македонија 101/19… 275/19).
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 подоцнежен датум и време ако е така наведено во сертификатот), а завршува на датумот и во времето кога сертификатот истекува или е претходно поништен.
Учесник	Лице или организација како што е КИБС, клиент, Издавач на сертификат, Регистрациона канцеларија, субјект или засегната страна.
Одбор за управување со политиките на KIBSTrust (ОУП)	Група во рамките на КИБС одговорна за објавување на оваа Практика и поврзаните документи.
Приватен клуч	Клучот од парот клучеви што безбедно се чува од страна на носителот на клучот, и тој се користи за креирање квалификуван сертификат или за дешифрирање на електронски записи или датотеки што биле шифрирани со соодветниот јавен клуч.
Јавен клуч	Клучот од парот на клучеви што може да биде јавно обелоденет од носителот на соодветниот приватен клуч и кој се користи од страна на засегнатата страна за да потврди квалификуван сертификат, односно електронскиот потпис креиран со соодветниот приватен клуч на носителот.
Инфраструктура на јавен клуч (PKI)	Архитектура, организација, техники, практики и процедури кои заеднички ги поддржуваат имплементацијата и функционирањето на криптографскиот систем на јавни клучеви базирани на сертификат. КИБС PKI се состои од системи кои соработуваат за обезбедување и имплементирање на криптиграфски систем за јавен клуч врз основа на сертификат.
Квалификуван електронски потпис	Напреден електронски потпис што е креиран од квалификуван уред за креирање електронски потпис и се заснова на квалификуван сертификат за електронски потпис.
Квалификуван сертификат	Квалификуван сертификат е сертификат издаден од ИС, кој е акредитиран и надгледуван од органи назначени од земја-членка на ЕУ.
Квалификуван сертификат за електронски потпис	Сертификат за електронски потписи, издаден од квалификуван давател на доверливи услуги кој ги исполнува условите утврдени во Анекс I на eIDAS.
Средство за креирање квалификуван потпис/печат (QSCD)	Уред кој е одговорен за квалификување на дигитални потписи со употреба на специфичен хардвер и софтвер со што се гарантира дека единствено потписникот има контрола врз неговиот приватен клуч.

Термин	Дефиниција
Давател на квалификувани доверливи услуги	Давател на доверливи услуги кој обезбедува една или повеќе квалификувани доверливи услуги и на кој му е доделен квалификуван статус од страна на надзорно тело.
Регистрациона канцеларија (РК)	Ентитет одобрен од ДДУ за да им помогне на барателите на сертификати при поднесување на барањата за сертификати и да ги одобри или одбие барањата за сертификати, да ги поништи сертификатите или да ги обнови сертификатите.
Засегната страна	Поединец или организација која делува потпирајќи се на сертификат и / или електронски потпис.
Далечинско QSCD	Серверски базиран HSM што се користи за централно генерирање и употреба на претплатнички приватни клучеви.
Далечинска верификација на идентитет	Методот / процесот со кој субјектот се идентификува преку сесија за видео повик и е еквивалентен на валидација со физичко присуство.
Коренски ИС	Орган за сертификација кој е на највисоко ниво во доменот на TSP и кој се користи за потпишување подредени ИС.
Тајни удели	Делови 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.
Secure Sockets Layer (SSL)	Метод на индустриски стандарди за заштита на веб комуникации. SSL безбедносниот протокол обезбедува шифрирање на податоци, серверска автентикација, интегритет на пораките и опционално, автентикација на клиент за конекција на Протоколот за контрола на трансмисија/Интернет протоколот.
Подреден ИС (Sub CA)	Издавач на сертификати чијшто издавачки сертификат е потпишан од надреден ИС.
Субјект	може да биде: - физичко лице; - физичко лице идентификувано дека е поврзано со правно лице; - правно лице (тоа може да биде организација или единица или оддел идентификуван дека е поврзана со организација);
Субјект на електронска идентификација	Физичко или правно лице кое поведува постапката за барање за издавање на средство електронска идентификација пред издавач на средства за електронска идентификација.
Претплатник	Субјект што се претплатува кај давателот на доверливи услуги и кој е законски обврзан на сите обврски на субјект.
Надзорно тело	Органот што е назначен од страна на земја-членка за извршување на надзорни активности на доверливите услуги и давателите на услуги според eIDAS. Според МК-eIDAS тое е Министерството за информатичко општество и администрација.
Доверлива услуга	Согласно законот МК-eIDAS доверливи услуги се: - издавање на сертификати за електронски потпис, - издавање на сертификати за електронски печат, - издавање на сертификати за автентичност на веб страници - зачувување и валидација на електронски потпис. - зачувување и валидација на електронски печат. - издавање на електронски временски печати. - електронска препорачана достава - доверлива услуга за електронско складирање на документи.
Давател на доверлива услуга	Правно лице кое обезбедува една или повеќе доверливи услуги.
Давател на квалификувана доверлива услуга	Давател на доверлива услуга кој обезбедува една или повеќе квалификувани доверливи услуги и чиј статус на давател на квалификувана доверлива услуга е доделен од страна на министерот за информатичко општество и администрација со регистрација во Регистарот на шеми за електронска идентификација и на доверливи услуги. Давател на квалификувана доверлива услуга е правно лице на кое му се доделени јавни овластувања, согласно со одредбите од законот МК-eIDAS.

Термин	Дефиниција
Доверливо лице	Вработен, соработник под договор или консултант на ентитет одговорен за управување со инфраструктурната сигурност на ентитетот, неговите производи, услуги, неговите простории и/или практики како што е поконкретно дефинирано во CP/CPS дел 5.2.1 .
Доверлива улога	Позиција во KIBSTrust на која мора да биде поставено доверливо лице.
Валиден сертификат	Сертификат што ја поминува постапката за валидација наведена во RFC 5280.
Период на валидност	Временскиот период измерен од датумот на издавање на сертификатот до датумот на истекување.
Електронска идентификација	Процес на користење на податоци за идентификација на лица во електронска форма кои на уникатен начин го претставуваат физичкото или правно лице или овластено лице на правно лице.
Средства за електронска идентификација	Материјални или нематеријални средства кои содржат податоци за идентификација на лица, а се користат за автентикација кај електронски услуги.
Издавач на средство за електронска идентификација	Правно лице кое ги исполнува условите утврдени во закон за издавачи на средство за електронска идентификација.
Шема за електронска идентификација	Систем за електронска идентификација според кој средствата за електронска идентификација се издаваат на физички или правни лица или овластено лице на правно лице.

Крај на документот