Правила и постапки
за издавање на квалификувани временски жигови

KIBSTrust Momentum

Верзија 5.0

Датум : 09.09.2022

111.06

OID 1.3.6.1.4.1.16305.1.1.6

КИБС АД Скопје

http://www.kibstrust.com/

Белешка за документот и заштитен знак

КИБС и KIBSTrust се регистрирани заштитни знаци на КИБС АД Скопје. Другите имиња наведени во овој документ може да бидат заштитни знаци на нивните сопственици. Давателот на доверливи услуги претставува организациски дел на КИБС, но функционира како бренд под името KIBSTrust, така што терминот „Давател на доверливи услуги КИБС“ се поистоветува со „KIBSTrust“.

КИБС АД Скопје како правно лице во овој документ е претставен скратено како КИБС.

Овој документ е изработен од KIBSTrust и ги содржи условите според кои KIBSTrust дејствува како Квалификуван давател на доверливи услуги (QTSP) и Квалификуван давател на услуга за издавање временски жигови (QTSSP).

Овој документ се заснова и е компатибилен со стандардот ETSI EN 319 421 „Електронски потписи и инфраструктура (ESI); Политика и безбедносни услови за даватели на доверливи услуги кои издаваат временски жигови“.

Право на интелектуална сопственост

Историја на промени

Верзија	Дата	Промени
5.0	09.09.2022	Нов издавачки сертификат за креирање временски жигови во хиерархијата на приватниот коренски сертификат на KIBSTrust (KIBSTrust Root CA G2).
4.2	03.04.2020	Според новата законска регулатива, во документот на македонскиот јазик настана промена на терминологијата. Дополнување поврзано со престанок на работа на TSA и план за престанок на работа. Дополнување поврзано со одговорност.
4.1	16.10.2018	Во документот на македонскиот јазик настана промена на терминологијата според новата законска регулатива. Дополнување поврзано со престанок на работа на TSA и план за престанок на работа. Дополнување поврзано со одговорност.
4.0	24.10.2018	Политиката е усогласена со документот ETSI EN 319 421 V1.1.1 Електронски потписи и инфраструктури (ESI), Политика и безбедносни услови за Даватели на доверливи услуги кои издаваат временски жигови.
3.0	17.10.2016	Променет е Издавачот и профилот на сертификати за временски жигови. Новиот сертификат е од DigiCert.
2.0	11.04.2016	Политиката е усогласена со документот ETSI TS 102 023 V1.2.2 Услови на Политиката за издавачи на временски жигови. Променети се лицата кои се одредени за изработување и одобрување на документот. Документот е подготвен во македонска и англиска верзија.
1.0	08.05.2012	Нов документ

Содржина

1. Вовед

Компаниите, органите на власт и сите видови на организации низ целиот свет сè повеќе ги генерираат своите процеси електронски за целите на оптимизација, намалување на трошоци и брзина. Така, постојните процеси во хартиена форма се заменуваат со електронски процеси и нови процеси овозможени преку употребата на дигитални информации и комуникација.

Овие нови, подобрени процеси (кои користат електронски информации) се предмет на истите законски одредби, барања за усогласеност и заштита, како и традиционалните процеси во хартиена форма. За да се исполнат овие барања, информациите во хартиена форма и електронските информации треба да бидат заштитени, меѓу другото, од манипулација и загуба. За да може да се процени следењето на барањата за усогласеност во професионалното опкружување, доказот за интегритет, целосност и доверливост се честопати главните критериуми.

Електронскиот временски жиг може да го даде овој доказ за интегритет и целосност на начин што е едноставен, правно безбеден, постојан, евтин и, по барање, анонимен. Временскиот жиг е електронски сертификат, во кој се наведува кога постоеле одредени податоци. Така се документира „кога“ и „што“. Електронски потпис, честопати нарекуван личен потпис, документира „кој“ и „што“. За разлика од електронскиот потпис, временскиот жиг не е врзан за луѓе и нивни постапки. Така може да се интегрира многу поедноставно и целосно автоматски во електронските процеси. Временските жигови се полесни за употреба отколку електронските потписи бидејќи нивната употреба може да биде целосно автоматска и независна за одредени лица, или анонимна.

Временските жигови се користат за да се докаже постоењето на одредени податоци пред одредена временска точка без можност сопственикот да може да го антидатира временскиот жиг. Откако ќе се потпише документот и стави временски жиг, секоја промена на податоците во документот ќе предизвика електронскиот потпис да не биде валиден, а за тоа корисникот ќе биде предупреден. За разлика од електронскиот потпис, временските жигови не се поврзани со лица и нивни постапки.

Овој документ го сочинува Правилата и постапките за издавање на временски жигови на KIBSTrust издавачот на временски жигови за квалификувани услуги на временски жигови. Наменет е да ги опише правилата и оперативните постапки усвоени од KIBSTrust (QTSA CP/CPS), како Квалификуван давател на доверливи услуги (QTSP) за обезбедување квалификувана услуга на издавање на временски жиг, согласно Законот за електронски документи, електронска идентификација и доверливи услуги (MK-eIDAS) и Регулативата (ЕУ) бр. 910/2014 (eIDAS).

Квалификуваната услуга за временски жиг на KIBSTrust докажува дека електронскит запис постоел пред одредено време. Оваа услуга може да се користи за поддршка на неотповикливост, за докажување дека е генериран електронски потпис за време на периодот на важност за јавен клуч на сертификатот, за поддршка на долгорочно електронско архивирање итн.

Квалификуваните услуги за временски жиг на KIBSTrust се дел од PKI услугите на KIBSTrust.

Тековниот документ ги специфицира општите правила што ги користи KIBSTrust квалификуваниот издавач на временски жиг (QTSA) за издавање на токени за временски жиг (TST). Ги дефинира вклучените страни, нивните одговорности, права и опсегот на применливост.

Услугите за временски жиг на KIBSTrust може да се добијат според примените параметри од KIBSTrust.

QTSA не врши долгорочно архивирање на ниту еден токен за временски жиг и апликацијата што ја користи QTSA мора да го зачува издадениот токен за идна употреба.

Услугите за квалификуван временски жиг на KIBSTrust се обезбедуваат согласно законот MK-eIDAS и регулативата eIDAS, стандардите EN 319 421 и EN 319 422 и со овластување на KIBSTrust кој делува како Квалификуван давател на услуги за издавање временски жиг.

Менаџментот може да направи исклучоци од овој QTSA CP/CPS, од случај до случај, за да ги ублажи материјалните, непосредните влијанија врз клиентите, партнери, засегнати страни и/или други каде што не постојат практични решенија. Сите такви исклучоци кои ги прави менаџментот се документираат, следат и се пријавуваат како дел од процесот на ревизија.

KIBSTrust користи инфраструктура на јавен клуч и доверливи извори на време за да обезбеди квалификувани електронски жигови преку услуги под името KIBSTrust Momentum.

1.1. Администрирање на овој документ

1.1.1. Администрирање на Правила и постапки

Организација која го администрира документот

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

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

1.1.2. Постапка на одобрување

Одобрување на овие CP/CPS и последователните измени и дополнувања се прават од страна на Одборот за управување со политиката (PMA). Измените и дополнувањата се во форма на документ што содржи изменета форма на CPS или како забелешка за ревидиран текст. Верзиите со измени и дополнувања или ажурираните одредби се поврзани со складиштето на KIBSTrust и се објавени на: https://www.kibstrust.com/repository.

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

2. Референци

Следниве документи содржат одредби кои се релевантни за KIBSTrust правилата и постапките на Издавачот на квалификуван временски жиг.

[1] Регулатива (ЕУ) бр. 910/2014 на Европскиот парламент и на Советот за електронска идентификација и доверливи услуги за електронски трансакции на внатрешниот пазар и укинување на Директивата 1999/93/ЕС.
[2] ETSI EN 319 401: ,,Електронски потписи и инфраструктури (ESI); Општи услови за Политика за Даватели на доверливи услуги".
[3] ETSI EN 319 421: ,,Електронски потписи и инфраструктури (ESI); Политика и безбедносни услови за Даватели на доверливи услуги кои издаваат временски жигови".
[4] [5] ETSI EN 319 422: ,,Електронски потписи и инфраструктури (ESI); Протокол за временски жиг и профили на токен за временски жигови".
[5] IETF RFC 3161: ,,Интернет X.509 Инфраструктура на јавен клуч: Протокол за временски жиг (TSP)".
[6] IETF RFC 5816: ,,ESSCertIDV2 ажурирано во RFC 3161".
[7] ETSI EN 319 122-1: Електронски потписи и инфраструктури (ESI); CAdES дигитални потписи; Дел 1: Суштински работи и основни CAdES потписи.
[8] ETSI EN 319 122-2: Електронски потписи и инфраструктури (ESI); CAdES дигитални потписи; Дел 2: CAdES потписи со продолжен временски период за успешна валидација.
[9] ETSI EN 319 122-3: Електронски потписи и инфраструктури (ESI); CAdES дигитални потписи; Дел 3: Инкорпорација на механизми на синтакса за евиденција на докази (ERS) во CadES.
[10] ETSI EN 319 411-1: ,, Електронски потписи и инфраструктури (ESI); Политика и безбедносни услови за Давателите на доверливи услуги кои издаваат сертификати; Дел 1: Општи услови".

[11] ETSI EN 319 411-2: ,,Електронски потписи и инфраструктури (ESI); Политика и безбедносни услови за Давателите на доверливи услуги; Дел 2: Услови за давателите на доверливи услуги кои издаваат ЕУ квалификувани сертификати".

3. Дефиниции и кратенки

3.1. Дефиниции

Координирано универзално време (UTS)[1]: временска скала која се заснова на секунда како што е дефинирано во Препораката ITU-R TF.460-6].
Засегната страна: поединец или организација кој дејствува врз основа на сертификат или временски жиг.
Претплатник: ентитет кој аплицира за услуга за издавање временски жиг и кој е законски обврзан со сите претплатнички обврски.
Временски жиг: податоци во електронска форма кои поврзуваат други електронски податоци за одредено време обезбедувајќи докази дека овие податоци постоеле во тој момент.
Правила и постапки за издавање на квалификуван временски жиг или QTSA CP/CPS (овој документ) значи група на правила кои ја специфицираат применливоста на токенот за временски жиг во одредена заедница или класа на примена со општи безбедносни услови, вклучувајќи ја изјавата за практики што QTSA ја применува при издавањето на токени за временски жиг.
Токен за временски жиг (TST): Податочен објект што поврзува претставување на податок со одредено време, со што се обезбедува доказ дека податокот постоел пред тоа време.
Издавач на временски жигови (TSA): Давател на доверливи услуги за временски жиг, кој издава токени за временски жиг.
Единица на временски жиг (TSU): сет од хардвер и софтвер со кој се управува како единица и има еден активен клуч за потпишување со временски жиг во тој момент.
Услуга за временски жиг: доверлива услуга за издавање временски жигови.
Давател на доверливи услуги (TSP): субјект кој обезбедува една или повеќе доверливи услуги.
Доверлива услуга: електронска услуга за:

- креирање, верификација и валидација на дигитални потписи и поврзани сертификати.
- креирање, верификација и валидација на временски жигови и поврзани сертификати.
- регистрирана испорака и поврзани сертификати.
- креирање, верификација и валидација на сертификати за автентикација на веб локации, или
- зачувување на дигитални потписи или сертификати поврзани со тие услуги.

PKI Декларација: множество од изјави за правилата и постапките на издавачот на квалификувани сертификати за е-потписи, е-печати и QTSA кои особено налагаат истакнување или информирање на претплатниците или засегнатите страни.
TSA систем: состав на ИТ производи и компоненти организирани за поддршка на обезбедувањето на услуги за временски жиг.
UTC(k): временска скала реализирана од лабораторијата "k" која се одржува во строга согласност со UTC, со цел да се постигне ±100 ns.
МК-eIDAS: Закон за електронски документи, електронска идентификација и доверливи услуги. Со законот е транспонирана регулативата на ЕУ број 910/2014 позната под кратенката eIDAS.
Национален надзорен орган: согласно законот МК-eIDAS тоа е Министерството за информатичко општество и администрација (МИОа).

3.2. Кратенки

BTSP	Најдобра практика за Правила и постапки за издавање временски жигови
CA	Издавач на дигитален сертификат
CP	Политика за сертификати
CPS	Правила за издавање сертификати
CRL	Регистар на поништени сертификати
CSU	Единица за криптографско потпишување

[1] Координирано универзално време UTC е меѓународен временски стандард што стапи на сила на 1 јануари 1972 година. UTC го замени средното време според Гринич (GMT). Универзалното време се заснова на 24-часовен часовник.

HSM	Хардверски безбедносен модул
IETF	Интернетска инженерска група
GMT	Гринич средно време
IERS	Меѓународна служба за ротација на земјата и референтните системи
ISMS	Систем за управување со информатичка безбедност
IT	Информатичка технологија
PMA	Орган за управување со политика
QTSP	Давател на квалификувани доверливи услуги
QTSSP	Квалификуван давател на услуги за временски жиг
TSA	Издавач на временски жиг
TSP	Давател на доверливи услуги
TST	Токен за временски жиг
TSU	Единица за временски жиг
UTC	Координирано универзално време

4. Општи концепти

4.1. Општи концепти на барањата

Овој документ упатува на стандардот ETSI EN 319 401 [4] за генерички услови на политиката кои се заеднички за сите класи на услуги кои ги обезбедуваат давателите на доверливи услуги.

Овие услови на политиката се засноваат на употребата на криптографија базирана на јавен клуч, сертификати за јавен клуч и доверливи временски извори.

Исто така, упатува на ETSI EN 319 421 [3] за услови на политики и безбедност вообичаени за Давателите на доверливи услуги кои издаваат временски жигови.

4.2. Издавач на временски жиг

KIBSTrust издавачот на квалификуван временски жиг (QTSA) е одговорен за обезбедување на квалификувани услуги за временски жиг како што е опишано во овој документ. Тој има одговорност за работата на релевантните единици за временски жиг (TSUs) кои се креирани и потпишани во име на QTSA. Правното лице одговорно за QTSA е КИБС кој под брендот KIBSTrust обезбедува квалификувани временски жигови.

KIBSTrust издава квалификувани временски жигови според следнава хиерархија:

Коренски ИС

#	Карактеристично име на субјект	Certificate SHA-256 Fingerprint (Метод за обележување датотека) за сертификат
1	**CN** = KIBSTrust Root CA G2 **organizationIdentifier** = NTRMK-5529581 **O** = KIBS AD Skopje **OU** = KIBSTrust Services **C** = MK	9E0D33A6B826F84030A811011E92217731C40CD28DBC2337931286D8A4951235

Издавачки сертификат на QTSA

#	Карактеристично име на субјект	Certificate SHA-256 Fingerprint (Метод за обележување датотека) за сертификат
1	**CN** = KIBSTrust Issuing QTSA CA G2 **organizationIdentifier** = NTRMK-5529581 **O** = KIBS AD Skopje **OU** = KIBSTrust Services **C** = MK	6ED77139F73AE034D69FF21ED6D5E4B9D1004766FB41E9EC973B3C2FD2568274

KIBSTrust QTSA и TSU сертификатите се издаваат според следниве политики за сертификати:

- **OID 0.4.0.2042.1.2:** itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy- identifiers(1) ncpplus(2)
- **OID 0.4.0.2023.1.1**: itu-t(0) identifiedorganization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy (1).

4.3. Претплатници

Претплатник е барателот, физичко или правно лице, на кого му се дава услуга за временски жиг и кој склучува договор со KIBSTrust.

Кога претплатникот е организација, тој вклучува неколку крајни корисници или поединечен краен корисник и некои обврски кои произлегуваат од употребата на услугата на временски жиг што се однесуваат на таа организација мора да важат и за крајните корисници. Во секој случај, организацијата ќе биде одговорна ако обврските на крајните корисници не се соодветно исполнети и затоа од таа организација се очекува уредно да ги извести своите крајни корисници.

Кога претплатникот е краен корисник, крајниот корисник ќе биде директно одговорен ако неговите обврски не се уредно исполнети.

4.3.1. Засегнати страни

Засегната страна е физичко лице или ентитет кому му се доставува дигитален документ со временски жиг и се потпира врз информациите од сертификатот и/или дигиталниот потпис издаден од QTSA. Засегнатата страна мора да ја оцени исправноста и валидноста на самиот документ во контекстот каде што се користи.

Засегнатите страни мора да потврдат дека временскиот жиг е правилно потпишан и дека приватниот клуч што се користел за потпишување на временскиот жиг не е поништен. Засегнатата страна треба да ги разгледа сите ограничувања за користење на временскиот жиг наведен во овој CP/CPS на KIBSTrust QTSA. За време на периодот на важност на TSU сертификатот, статусот на приватниот клуч може да се потврди со користење на соодветните CRL. CRL се објавуваат на http://crl.kibstrust.com/rootg2.crl и http://crl.kibstrust.com/QtsaG2.crl

4.3.2. Други учесници

Не е применливо.

4.3.3. Употреба на временски жигови

Временските жигови издадени од KIBSTrust, како што е наведено во овој документ, се квалификувани според законот MK-eIDAS и Регулативата eIDAS. Временските жигови ќе се користат само до таа мерка до која употребата е во согласност со применливиот закон и во рамките и контекстот наведени во овој документ. Забранета е секаква употреба надвор од границите и контекстите наведени во овој документ или за незаконски цели, спротивно на јавниот интерес или на друг начин што може да му наштети на бизнисот или угледот на KIBSTrust. Индикативно, употребата на временски жигови е забранета за која било од следниве цели:

- незаконски активности (вклучувајќи сајбер-напади).
- издавање нови временски жигови и информации за валидноста на временскиот жиг.
- овозможување на други страни да го користат претплатничкиот TST.
- користење на временскиот жиг издаден на документи со временски жиг што може да се користат за незаконски цели (вклучувајќи временски жиг на такви документи за цели на тестирање).

4.4. Правила и постапки на QTSA

4.4.1. Цел

Овој документ ги специфицира политиките и безбедносните услови кои се однесуваат на работењето и практиките на управување на KIBSTrust како Издавач на временски жиг (QTSA) за издавање на квалификувани временски жигови. Тие може да се користат за поддршка на електронски потписи или за сите апликации за кои е потребно да се докаже дека податокот постоел пред одредено време.

Овој документ може да се користи од независни субјекти како основа за потврдување дека KIBSTrust QTSA е доверлив ентитет за издавање на квалификувани временски жигови во согласност со MK-eIDAS и eIDAS.

Овој документ е јавно достапен. Дистрибуцијата на овој документ е ограничена како што е опишано во делот „Права на интелектуална сопственост“.

QTSA издава временски жигови на сите заинтересирани страни без технички ограничувања. За издавање на временски жигови се плаќа надоместок, кој е дефиниран во тарифата на КИБС АД Скопје, објавен на веб страницата: https://www.kibstrust.mk, или согласно договор. Овој документ TSP/PS и сите поврзани јавни документи може да се преземат од: https://www.kibstrust.mk/repository/.

4.4.2. Ниво на специфичност

Овој документ ги опишува само општите правила за издавање и управување со токен за временски жиг. Детален опис на инфраструктурата и поврзаните оперативни постапки се опишани во дополнителни документи кои не се јавно достапни. Овие дополнителни документи се достапни само на овластен персонал на KIBSTrust и, кога е потребно да се познати, на ревизори на услугите за временски жиг.

4.4.3. Пристап

Овој документ е дефиниран за специфичните детали за оперативното опкружување, организациската структура, оперативните постапки, капацитетите и компјутерската средина на KIBSTrust QTSA.

5. Правила за временски жиг

5.1. Преглед

Оваа Политика на временски жиг дефинира низа процеси за доверливо креирање TST во согласност со ETSI EN 319 421. Приватните клучеви и TSU ги исполнуваат техничките спецификации на ETSI EN 319 422.

KIBSTrust QTSA ги потпишува временските жигови со употреба на приватни клучеви кои се резервирани исклучиво за таа цел. Секој TST содржи идентификација за применливата политика, и временските жигови се издаваат со време прецизно до **±1 секунда од UTC**.

KIBSTrust TSU издава квалификувани електронски временски жигови според законот MK-eIDAS и регулативата eIDAS. KIBSTrust TSU не издава неквалификувани електронски временски жигови.

Временските жигови се бараат по пат на Hypertext Transfer Protocol (HTTP), како што е опишано во RFC 3161.

5.2. Идентификација

Предметниот идентификатор (OID) на KIBSTrust QTSA CP/CPS утврден во овој документ е:

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 доверлива услуга
1.3.6.1.4.1.16305.1.1	Политики за квалификувани сертификати
1.3.6.1.4.1.16305.1.1.6	KIBSTrust QTSA CP/CPS

Овој OID е содржан како референца во секој издаден временски жиг, во KIBSTrust QTSA CP/CPS и во PKI Декларацијата која им е достапна на Претплатникот и на Засегнатите страни.

KIBSTrust ги издава TST во согласност со ETSI EN 319 421 најдобрата практика за политика на временски жиг (BSTP) идентификуван како **OID 0.4.0.2023.1.1**.

5.3. Заедница на корисници и применливост

За квалификуваноста на корисниците или применливоста на испорачаните услуги нема ограничувања. KIBSTrust QTSA може да обезбеди услуги за временски жиг на какви било електронски податоци на секој корисник, вклучително и на затворени заедници.

Оваа политика има за цел исполнување на условите за временски жиг со долгорочна важност (како што е дефинирано во ETSI EN 319 122), но генерално е применлива за секоја употреба која содржи услов за еквивалентен квалитет.

Оваа политика може да се користи за јавни услуги за временски жиг или услуги за временски жиг кои се користат во рамки на затворена група.

5.3.1. Усогласеност

KIBSTrust QTSA го користи идентификаторот во TST како што е дадено во делот 5.2 „Идентификација“.

KIBSTrust QTSA осигурува усогласеност на обезбедените услуги со прописите специфицирани во делот 6.1 „Обврски на QTSA“ и обезбедува сигурност на контролните механизми опишани во делот 7 „Практики на TSA“.

6. Обврски и одговорности

6.1. Обврски на QTSA

6.1.1. Општи обврски

Ова поглавје ги вклучува, директно или преку упатување, сите должности, обврски, гаранции и одговорности на KIBSTrust QTSA, неговите претплатници и корисници на TST (Претплатници и засегнати страни). Овие обврски и одговорности се регулирани со документи како што се налог за купување (припејд формулар за набавка) или договор (постпејд формулар за набавка) прифатени од сите страни.

KIBSTrust управува со KIBSTrust QTSA и презема одговорност дека барањата од делот 7 „Постапки на QTSA“ од овој документ, како и одредбите на MK-eIDAS и eIDAS, се имплементирани во соодветниот KIBSTrust QTSA CP/CPS.

Договорите на KIBSTrust со претплатниците и засегнатите страни ги опишуваат меѓусебните обврски и одговорности, вклучувајќи ги и финансиските одговорности. KIBSTrust QTSA CP/CPS е составен дел од овие договори.

6.1.2. Обврски кон претплатниците за QTSA

KIBSTrust гарантира достапност од 99,00 % од услугите на KIBSTrust QTSA во режим 24/7, со исклучок на планираните технички прекини, кои се однесуваат на одржување на опремата и системот.

KIBSTrust ги презема следниве обврски кон претплатниците на QTSA:

- Да работи во согласност со овој KIBSTrust QTSA CP/CPS и други релевантни оперативни политики и постапки.
- Да се обезбеди дека TSU единиците одржуваат минимална UTC временска точност од ± 1 секунда.
- Да се одржи компетентен и искусен тим кој може да обезбеди континуитет на TSS.
- Да се обезбеди на трајна основа физичката и логичката безбедност, како и интегритетот на материјалите, софтверот и базите на податоци потребни за правилно функционирање на TSS.
- Да се следи и контролира TSS и целата QTSA инфраструктура, со цел да се спречи или ограничи какво било нарушување или недостапност на TSS.
- Да се подложи на внатрешни и надворешни прегледи за да се обезбеди усогласеност со релевантното законодавство и внатрешните политики и процедури на KIBSTrust.
- Да се обезбеди пристап со висока достапност до системите на KIBSTrust QTSA, освен во случај на планирани технички прекини и губење на временска синхронизација.

6.2. Обврски на Претплатникот

Претплатниците треба да ги потврдат потписите креирани од KIBSTrust QTSA на TST. Таквата проверка вклучува:

- Проверка дали е валиден QTSA потписот на TST.
- Верификација на QTSA сертификатот:
    - Потврда на доверливата патека до доверливиот коренски сертификат, и за секој од сертификатите во синџирот (вклучувајќи го и самиот QTSA сертификат)
    - Проверка дали сертификатот не е истечен во моментот на потпишување на QTSA
    - Проверка дали сертификатот не бил поништен во моментот на потпишувањето на QTSA.

Претплатниците мора да користат безбедни криптографски функции за барања за временски жиг.

Обврските на претплатниците се дефинирани и во Одредбите и условите на KIBSTrust за користење на квалификувани доверливи услуги.

6.3. Обврски на Засегнатата страна

Засегнатите страни треба да ги потврдат потписите креирани од KIBSTrust QTSA на TST. Таквата проверка вклучува:

- Проверка дали е валиден потписот на QTSA на TST.
- Верификација на сертификатот QTSA:
    - Потврда на доверливата патека до доверливиот коренски сертификат и за секој од сертификатите во синџирот (вклучувајќи го и самиот QTSA сертификат)
    - Проверка дали сертификатот не е истечен во моментот на потпишување на QTSA
    - Проверка дали сертификатот не бил поништен во моментот на потпишување од QTSA

Засегнатите страни треба да ги разгледаат сите ограничувања за користење на временскиот жиг специфициран со KIBSTrust QTSA CP/CPS. Доколку верификацијата се изврши по истекот на периодот на важност на сертификатот, Засегната страна треба да ги следи упатствата означени во Анекс Д од ETSI EN 319 421.

Се очекува Засегнатите страни да го користат доверливиот список за да утврдат дали единицата за временски жиг или временскиот жиг се квалификувани. Ако јавниот клуч на TSU е наведен во доверливиот список и услугата што ја преставува е квалификувана услуга за временски жиг, тогаш временските жигови издадени од оваа TSU може да се сметаат за квалификувани. qcИзјавата „esi4-qtstStatement-1“ како што е дефинирано во ETSI EN 319 422, клаузула 9.1 се користи како индикација дека временскиот жиг е квалификуван.

6.4. Одговорност

Одговорноста, како и секое ограничување на одговорноста на KIBSTrust што дејствува како QTSSP и на претплатниците и засегнатите страни поврзани со услугите се наведени во Одредбите и условите на

KIBSTrust за користење на релевантниот договор за доверливи квалификувани услуги или е како што е предвидено со важечкото законодавство.

KIBSTrust е одговорен за евентуални штети директни, намерни или поради небрежност, на кое било физичко или правно лице, како резултат на непочитување на обврските утврдени во законот на KIBSTrust QTSA CP/CPS и MK-eIDAS и регулативата eIDAS.

Правилата и условите на KIBSTrust за користење на квалификувани доверливи услуги ја ограничуваат одговорноста на KIBSTrust. Ограничувањата на одговорност вклучуваат исклучување на индиректни, посебни, случајни и последователни штети. Тие, исто така, вклучуваат ограничување на одговорноста во однос на комбинираната збирна одговорност на KIBSTrust (односно КИБС) кон кое било и сите лица која се однесува на услугите за временски жиг, што е ограничено на износ што не го надминува оној од соодветниот договор за услугата за временски жиг, што ќе се пресметува пропорционално, и до вкупно максимално педесет илјади (50.000) евра, без оглед на природата на обврската и видот, износот или обемот на претрпената штета. Ограничувањата на одговорноста ќе бидат исти без оглед на бројот на временски жигови или побарувања поврзани со таквиот временски жиг.

KIBSTrust QTSA одбива секаква одговорност во врска со употребата што се прави со TST што ги доставува и потпишува.

7. Постапки на QTSA

KIBSTrust QTSA спроведува контроли кои ги исполнуваат барањата ETSI EN 319 421 и ETSI EN 319 422.

7.1. Постапки и Декларација

7.1.1. Постапки на QTSA

Овој KIBSTrust QTSA CP/CPS ги утврдува општите правила во врска со техничките, организациските и процедуралните барања на работењето на KIBSTrust QTSA.

Сертификатите за временски жиг важат десет (10) години, но потребно е повторно обновување на пар клучеви секоја година. Затоа, евиденцијата и записите за временски жиг се чуваат една (1) година по истекот на сертификатот за единицата за временски жиг.

Редовно се спроведува проценка на ризикот за да се проценат деловните средства и заканите за тие средства за да се утврдат неопходните безбедносни контроли и оперативни постапки што се преземени.

Правилата и постапките во врска со користењето на услугите за временски жиг, како што се опфатени во Одредбите и условите на KIBSTrust за користење на квалификувани доверливи услуги, се откриваат и се достапни за сите претплатници и засегнати страни како што е наведено во делот 7.1.2 од овој документ.

Органот за управување со политики на KIBSTrust има одговорност за одржување, разгледување и одобрување на сите правила и постапки на KIBSTrust PKI во согласност со условите од делот 1.1 „Администрирање политики“ од овој документ. Менаџментот на KIBSTrust има одговорност да осигура дека правилата и постапките се правилно имплементирани.

7.1.2. PKI Декларација

KIBSTrust QTSA им ги доставува на сите претплатници и потенцијални засегнати страни одредбите и условите во врска со користењето на квалификуваните услугите за временски жиг на KIBSTrust.

PKI Декларацијата на KIBSTrust е во согласност со барањата на ETSI EN 319 421 и содржи изјави за постапките на QTSA, како и правата и обврските на претплатниците и засегнатите страни на поедноставен и сеопфатен начин.

Некои елементи од Декларацијата на KIBSTrust QTSA се наведени подолу:

- Секој TST издаден од KIBSTrust QTSA го вклучува идентификаторот на политиката, дефиниран во делот 5.2 од овој документ.
- Криптографските хаш функции, кои се користат во процесот на временскиот жиг се во согласност со нормативните барања, SHA-256 и SHA-512.
- Очекуваниот период на важност на KIBSTrust TSU е до десет (10) години.
- Точноста на времето, која е дадена во TST, е регулирана во делот 5.1 од овој документ.

- Ограничувањата на применливоста поврзани со системот QTSA се дефинирани во делот 5.3 од овој документ.
- Проверката на TST треба да се изврши со употреба на соодветен софтвер.
- Обврските на Претплатникот се опишани во делот 6.2 од овој документ.
- Обврските на Засегнатата страна се опишани во делот 6.3 од овој документ.
- KIBSTrust безбедно одржува евиденција во врска со работата на KIBSTrust QTSA.
- KIBSTrust може да наплатува такси за услугите обезбедени од KIBSTrust QTSA.

7.2. Управување со животниот циклус на клучот

7.2.1. Генерирање QTSA клуч

Персоналот со доверливи улоги под двојна контрола врши генерирање на TSU клучевите за потпишување во физички обезбедена средина. Персоналот овластен да ја врши оваа функција е ограничен на оние кои се потребни да го сторат тоа според постапките на QTSA.

Генерирањето на TSU клучевите за потпишување се врши во безбедни криптографски уреди, кои ги исполнуваат барањата идентификувани во FIPS 140-2 ниво 3.

Паровите на клучеви се генерираат со користење на безбедни алгоритми и параметри засновани на тековните истражувања и индустриски стандарди следејќи ги препораките на ETSI TS 319 312.

Активностите извршени при секое генерирање клучеви се евидентирани, датирани и потпишани од сите вклучени поединци. Овие записи се чуваат за целите на ревизија и следење во рамките на временски рок што се смета соодветен од страна на KIBSTrust менаџментот.

7.2.2. Заштита на приватниот клуч на TSU

KIBSTrust презема конкретни чекори за да се осигура дека TSU приватните клучеви ќе останат доверливи и ќе го задржат својот интегритет.

Приватните клучеви на TSU се складираат во безбеден хардверски безбедносен модул за извршување операции за потпишување, кои се во согласност со најмалку FIPS 140-2 ниво 3 или еквивалентно на EAL 4+ или повисоко**,** во согласност со ISO/IEC 15408 спецификациите. Поставени се посебни контроли за да се обезбеди дека хардверот не е манипулиран и дека функционира правилно.

TSU приватните клучеви не можат да се извлечат во каква било форма и не се достапни надвор од хардверскиот безбедносен модул.

KIBSTrust креира резервни копии од TSU приватните клучеви, за рутинско обновување и оporавување по откажување на системот. Таквите клучеви се чуваат во шифрирана форма во хардверските криптографски модули. Криптографските модули што се користат за складирање на приватен клуч ги исполнуваат барањата на овој CPS. Приватните клучеви се копираат на резервни хардверски криптографски модули. Враќање на резервните клучеви на TSU бара двојна контрола во физички обезбедена средина.

7.2.3. Дистрибуција на јавниот клуч на TSU

Јавните клучеви на KIBSTrust TSU се достапни во дигитален сертификат.

KIBSTrust TSU сертификатите се достапни за безбедно преземање преку веб-страницата на KIBSTrust складиштето на https://www.kibstrust.com/repository. Тие, исто така, може да се најдат во Регистарот на квалификувани даватели на доверливи услуги и квалификувани доверливи услуги во машински читлив формат (https://trusteid.mioa.gov.mk/TrustedList/TL-MK.xml) како дел од Регистарот на даватели на доверливи услуги и електронски шеми за идентификација објавени од Министерството за информатичко општество и администрација (МИОа) на https://trusteid.mioa.gov.mk/en/home/register-and-lists/.

7.2.4. Обновување на клучот на TSU

Периодот на работа за паровите клучеви на TSU се дефинира со поставување на период на употреба на приватен клуч во сертификатот за јавен клуч на TSU.

KIBSTrust TST се потпишани со KIBSTrust TSU сертификати со десет (10) години важност. KIBSTrust TSU сертификатите со десет (10) години важност се користат само за потпишување на TST за период на употреба од една (1) година.

Постапката на KIBSTrust TSU обнова на пар клучеви се извршува по истекот на периодот на користење (1 година) на сертификатот TSU. Јавните клучеви се архивираат за период од најмалку десет (10) години од датумот на истекување на сертификатот.

7.2.5. Завршеток на животниот циклус на TSU клучот

KIBSTrust QTSA гарантира дека TSU приватните клучеви за потпишување не се користат по крајот на нивниот животен циклус. Особено, постојат оперативни и технички процедури за да се осигура дека е поставен нов клуч пред истекот на периодот на користење на клучот на TSU и дека приватните клучеви на TSU или кој било дел, вклучувајќи ги и сите копии се уништени на таков начин што приватниот клуч не може да се поврати.

Системот за генерирање TST ќе одбие каков било обид за издавање TST ако приватниот клуч за потпишување е истечен или ако периодот на користење на приватниот клуч за потпишување е истечен.

7.2.6. Управување со животниот циклус на криптографскиот модул користен за потпишување временски жиг

KIBSTrust QTSA ја обезбедува сигурноста на HSM во текот на неговиот животен циклус. KIBSTrust има воспоставено постапки за да се обезбеди дека:

- Хардверските безбедносни модули не се менувани при испораката или складирањето.
- Се врши тестирање за прифаќање за да се потврди дали криптографскиот хардвер работи правилно.
- Инсталирањето, активирањето и копирањето на TSU клучевите за потпишување во HSM се врши само од персонал со доверливи улоги, во физички безбедна средина.
- TSU приватните клучеви за потпишување зачувани на HSM се бришат по повлекувањето на уредот во согласност со упатствата на производителот.

7.3. Временски жиг

7.3.1. Токен за временски жиг

KIBSTrust има воспоставено технички процедури за да се осигура дека TST се издаваат безбедно и го вклучуваат точното време. Секој TST вклучува:

- претстава за датумот кој е означен со временски жиг како што е обезбедено од апликантот
- единствен сериски број за идентификација на специфичен TST
- единствен идентификатор на политиката како што е опишано во делот 5.2 од овој документ
- електронски потпис генериран со помош на клуч кој се користи исклучиво за временски жиг
- идентификатор за QTSA и TSU
- вредност на датумот и времето што може да се следи до реалната вредност на UTC времето
- алгоритам за потпис што се користи во TST

KIBSTrust TSU одржуваат ревизорска евиденција за сите калибрации според UTC упатувања.

7.3.2. Синхронизација на часовникот со UTC

KIBSTrust QTSA гарантира дека неговото време е синхронизирано со UTC во рамките на декларираната точност во однос на повеќе независни временски извори. KIBSTrust QTSA го вклучува времето во TST со точност опишана во делот 5.1 од овој документ.

Записите за ревизија и калибрација на синхронизацијата се одржуваат од KIBSTrust. KIBSTrust TSA гарантира дека ако времето што би било означено во TST се помести или отскокне од синхронизацијата со UTC, тоа ќе биде детектирано. Ако TSU времето се помести надвор од декларираната точност и рекалибрацијата не успее, QTSA нема да издава временски жигови додека не се врати точното време.

KIBSTrust спроведува безбедносни контроли за спречување на неовластено работење, насочени кон калибрација на времето на QTSA.

7.3.3. Постапка на справување со престапна секунда

Престапна секунда е прилагодување на UTC со прескокнување или додавање дополнителна секунда во последната секунда од UTC месецот. Прва предност се дава на крајот на декември и јуни, а втора предност се дава на крајот на март и септември.

KIBSTrust следи дека синхронизацијата се одржува кога ќе се појави престапна секунда.

7.4. Управување и работа со QTSA

7.4.1. Управување со сигурност

KIBSTrust QTSA гарантира дека се применуваат административни и управни процедури кои се соодветни и одговараат на признаените најдобри практики.

KIBSTrust ги извршува сите функции на QTSA користејќи доверливи системи кои ги исполнуваат барањата на KIBSTrust ISMS.

7.4.2. Класификација и управување со средства

KIBSTrust одржува попис на сите средства и доделува класификација на барањата за заштита на тие средства во согласност со анализата на ризик.

7.4.3. Безбедност на персоналот

KIBSTrust одржува соодветни контроли на персоналот што ги исполнува најдобрите безбедносни практики и барањата на релевантните стандарди.

Менаџерскиот и оперативниот персонал поседува соодветни вештини и знаења за временски жигови, дигитални потписи и доверливи услуги, како и безбедносни процедури за персоналот со безбедносни одговорности, безбедност на информации и проценка на ризик.

Доверливите лица ги вклучуваат сите вработени кои имаат пристап или контролираат криптографски операции. Доверливите лица вклучуваат, но не се ограничени на:

- Персонал за деловни операции за криптографски работи,
- Безбедносен персонал,
- Персонал за администрација на системот,
- Назначен инженерски персонал, и
- Раководители кои се назначени да управуваат со инфраструктурната доверливост.

За сите вработени кои сакаат да станат доверливи лица, верификацијата на идентитетот се врши преку процесот на човечки ресурси на KIBSTrust, врз основа на проверка на добро препознатливи форми на идентификација (на пример: пасоши или картички за идентификација). Идентитетот дополнително се потврдува преку процедури за проверка на биографијата.

KIBSTrust гарантира дека персоналот има постигнато доверлив статус и дека е дадено одобрение од секторот пред да им се издадат на таквиот персонал:

- Уреди за пристап и даден пристап до бараните капацитети.
- Електронски идентификации за пристап и извршување на специфични функции на KIBSTrust ИС, QTSA или други ИТ системи.

KIBSTrust има имплементирано систем за контрола на пристап, кој ги идентификува надлежните органи и ги регистрира сите корисници на информатичкиот систем KIBSTrust на доверлив начин.

Корисничките сметки се креирани за персонал со специфични улоги на кои им е потребен пристап до соодветниот систем. Сите корисници мора да се пријават со посебно наменета корисничка сметка, а административните команди се достапни само со јасна дозвола и ревизија на извршувањето. Дозволите за системот со датотеки и другите функции достапни во безбедносниот модел на оперативниот систем се користат за да се спречи каква било друга употреба. Корисничките сметки се заклучуваат што е можно поскоро кога промената на улогата го наложува тоа. Правилата за пристап се ревидираат годишно.

KIBSTrust бара ако некој од персоналот сака да стане доверливо лице, треба да презентира доказ за потребната биографија, квалификации и искуство потребни за извршување на нивните потенцијални

работни обврски, како што е наведено во договорот за вработување, описот на работното место и документите за улоги и одговорности кои се целосни и задоволителни како и доказ за какви било владини дозволи, доколку ги има, неопходни за извршување на услугите за сертификација според владини договори, пред да се извршат какви било оперативни или безбедносни функции.

Со договорите за вработување потпишани од вработените во KIBSTrust се предвидени следните обврски:

- Да ја чуваат тајноста на доверливите информации до кои дошле за време на нивното извршување,
- Да ги спречи да имаат деловни интереси во компанија, што може да влијае на нивното расудување во обезбедувањето на услугата
- Да се осигура дека тие не се казнети за намерно недолично однесување
- Целиот персонал со доверливи улоги да нема какви било интереси што може да влијаат на нивната непристрасност во однос на операциите на KIBSTrust.

Пред да започне работата со доверлива улога, KIBSTrust спроведува проверки на биографијата кои го вклучуваат следново:

- Проверка на идентитетот.
- Проверка на претходно вработување и професионална референца (ако е достапна).
- Потврда за стекнат највисок или најрелевантен степен на образование.
- Пребарување во националната кривична евиденција.
- Проверка на финансиската евиденција.

До степен до кој кое било од барањата наметнати со овој дел не може да се исполни поради забрана или ограничување со локалниот закон или други околности, KIBSTrust ќе користи замена за истражна техника дозволена со закон која обезбедува суштински слични информации.

7.4.4. Физичка и просторна безбедност

KIBSTrust ја има имплементирано својата „Политика за физичка и просторна безбедност“, вклучувајќи ги политиките и практиките за безбедност на информациите, што ги поддржува безбедносните барања на овој CP/CPS. Усогласеноста со овие Правила и постапки е вклучена во барањата за ревизија на KIBSTrust. Политиката за физичка безбедност на KIBSTrust содржи чувствителни безбедносни информации и е достапна само по договор со KIBSTrust.

Операциите на KIBSTrust QCA и QTSA се спроведуваат во физички заштитено опкружување што одвраќа, спречува и открива неовластено користење, пристап до или откривање на чувствителни информации и системи, без разлика дали се тајни или не се тајни.

KIBSTrust, исто така, одржува капацитети за оporавување по пад на системот за своите операции на услуги за временски жиг. Објектите за оporавување по пад на системот на KIBSTrust се заштитени со повеќе нивоа на физичка безбедност кое се еднакви на оние во примарниот објект на KIBSTrust.

Системите на KIBSTrust се заштитени со пет (5) нивоа на физичка безбедност, при што е потребен пристап до пониското ниво пред да се добие пристап до повисокото ниво.

Прогресивно рестриктивните привилегии за физички пристап го контролираат пристапот до секое ниво. Чувствителната оперативна активност на QTSA и секоја активност поврзана со животниот циклус на процесот на сертификација, се случуваат во рамките на многу рестриктивни физички нивоа. За влез во секое ниво потребна е бец картичка за пристап на вработениот. Физичкиот пристап автоматски се најавува и се создава видео запис. Некои нивоа спроведуваат индивидуална контрола на пристап со секвенцијална употреба на картички од двајца вработени. На персоналот без придружба, вклучувајќи вработени без овластување или посетители, не им е дозволен влез во таквите заштитени простори.

Системот за физичка безбедност вклучува нивоа за безбедност на управување со клучеви што служи за заштита на онлајн и офлајн складирање на единицата за криптографско потпишување (CSU) и материјалот за клучеви. Деловите што се користат за креирање и складирање на криптографски материјал спроведуваат двојна контрола, секоја преку истовремена употреба на суцесивно користење картички од двајца вработени. Онлајн CSU се заштитени со заклучени ормани. Офлајн CSU се заштитени со заклучени сефови, ормани и контејнери. Пристапот до CSU и материјалот за клучеви е ограничен во согласност со

барањата за поделба на должностите на KIBSTrust. Отворањето и затворањето на ормани или контејнери во овие нивоа се евидентирани за ревизорски цели.

Операциите на KIBSTrust се заштитени со користење на физички контроли за пристап што ги прави достапни само за соодветно овластени лица. Пристапот до безбедните делови од објектите бара употреба на картичка „пристап“ или „пропусница“. Употребата на пристапната картичка е евидентирана од безбедносниот систем на објектот.

Евиденцијата на картичките за пристап и видео записите се прегледуваат на редовна основа. KIBSTrust безбедно ги складира во сигурносни контејнери сите преносливи медиуми и хартиени документи што содржат чувствителни информации во форма на обичен текст, поврзани со неговите операции.

Безбедните капацитети на KIBSTrust се опремени со примарни и резервни:

- Енергетски системи за обезбедување континуиран, непрекинат пристап до електрична енергија.
- Системи за греење/вентилација/климатизација за контрола на температурата и релативната влажност.

KIBSTrust презема разумни мерки на претпазливост за да го минимизира влијанието на изложеност на KIBSTrust системите на вода.

KIBSTrust презема разумни мерки на претпазливост за да спречи и гасне пожари или друга штетна изложеност на пламен или чад. Мерките за спречување и заштита од пожар на KIBSTrust се дизајнирани да се усогласат со локалните прописи за заштита од пожари.

Сите медиуми што содржат продукциски софтвер и податоци, ревизија, архива или резервни информации се чуваат во објектите на KIBSTrust или во безбедна просторија за складирање надвор од локацијата со соодветни физички и логички контроли за пристап дизајнирани да го ограничат пристапот на овластен персонал и да ги заштитат таквите медиуми од случајно оштетување (на пример, вода, оган).

Чувствителните документи и материјали се уништуваат со сечкање пред да се исфрлат. Медиумите што се користат за собирање или пренесување чувствителни информации се прават нечитливи пред да се исфрлат. Криптографските уреди физички се уништуваат или онеспособуваат во согласност со упатствата на производителот пред да се исфрлат. Останатиот отпад се отстранува во согласност со нормалните барања на KIBSTrust за отстранување на отпадот.

7.4.5. Управување со работењето

KIBSTrust QTSA гарантира дека постапките, процесите и инфраструктурата се усогласени со оперативното управување, барањата за процедурална безбедност, управувањето со пристап до системот, доверливите системи за имплементирање и одржување, управувањето со континуитет на бизнисот и справувањето со инциденти како што е дефинирано во ETSI EN 319 421.

Процедурите за управување со работењето за KIBSTrust QTSA се инкорпорирани во севкупните процедури за управување со внатрешните операции на KIBSTrust.

7.4.6. Имплементација и одржување на доверливите системи

KIBSTrust гарантира дека системите што го одржуваат софтверот и датотеките со податоци на QTSA се доверливи системи, заштитени од неовластен пристап и модификација. Покрај тоа, KIBSTrust го ограничува пристапот до продукциските сервери на оние поединци со валидна деловна причина за таков пристап. Корисниците на општите апликации немаат кориснички сметки на продукциските сервери.

7.4.7. Компромитирање на услугите на QTSA

Во случај на компромитирање на работата на TSU (на пр., компромитирање на клучот на TSU), сомнително компромитирање или губење на калибрацијата, TSU нема да издава временски жигови додека не се преземат чекори за закрепнување од компромитирањето. Во случај на компромитирање, или сомневање за компромитирање или губење на калибрацијата при издавањето на временскиот жиг, KIBSTrust им дава на располагање на сите претплатници и засегнати страни опис на компромитацијата што се случила.

Во случај на големо компромитирање на работењето на QTSA, KIBSTrust им става на располагање на сите претплатници и засегнати страни информации што може да се користат за да се идентификуваат

временските жигови кои можеби биле засегнати, освен ако тоа не ја нарушува приватноста на корисниците на QTSA или безбедноста на услугите на QTSA.

7.4.8. Престанок со работа на QTSA

Престанокот на QTSA е:

- со одлука на Управниот одбор или Директорот на КИБС (KIBSTrust).
- со решение на органот што врши надзор на снабдувањето на услугата.
- со судска одлука.
- при ликвидација или престанок на работењето на KIBSTrust.

KIBSTrust гарантира дека потенцијалните проблеми на претплатниците и засегнатите страни се минимизираат поради прекинот на своите услуги и обезбедува континуирано одржување на информациите потребни за да се потврди исправноста на доверливите услуги.

Доколку е неопходно KIBSTrust QTSA да прекине со работа, KIBSTrust прави комерцијално разумни напори да ги извести претплатниците и засегнатите страни за таквото раскинување пред завршувањето на QTSA. KIBSTrust QTSA ги поништува сертификатите на TSU кога ќе ги прекине своите услуги.

7.4.9. Усогласеност со законските барања

KIBSTrust обезбедува усогласеност со законските барања за исполнување на сите важечки законски барања за заштита на записите од губење, уништување и фалсификување, како и барањата за следново:

- MK-eIDAS - Закон за електронски документи, електронска идентификација и доверителски услуги (Службен весник на Република Северна Македонија)
- eIDAS - Регулатива (ЕУ) бр. 910/2014 на Европскиот парламент и на Советот од 23 јули 2014 година за електронска идентификација и доверливи услуги за електронски трансакции на внатрешниот пазар и укинување на Директивата 1999/93/ЕЗ.
- MK-GDPR - Закон за заштита на личните податоци (Службен весник на Република Северна Македонија)
- Закони за лични податоци и регулативи на ЕУ.

Вклучувајќи ги и сродните стандарди на ЕУ:

- ETSI EN 319 401: „Електронски потписи и инфраструктури (ESI); Општи услови за политика за Даватели на доверливи услуги".
- ETSI EN 319 411-1: „Електронски потписи и инфраструктури (ESI); Политика и безбедносни услови за Давателите на доверливи услуги кои издаваат сертификати; Дел 1: Општи услови".
- ETSI EN 319 411-2: „Електронски потписи и инфраструктури (ESI); Политика и безбедносни услови за Давателите на доверливи услуги кои издаваат сертификати; Дел 2: Услови на Политиката за Издавачите на сертификати кои издаваат квалификувани сертификати".
- ETSI EN 319 421: „Електронски потписи и инфраструктури (ESI); Политика и безбедносни услови за Даватели на доверливи услуги кои издаваат временски жигови".
- ETSI EN 319 422: „Електронски потписи и инфраструктури (ESI); Протокол за временски жиг и профили на токен за временски жигови".

KIBSTrust кој делува како QTSP подлежи на ревизии на усогласеност за неговите QTSA услуги и за услугите за временски жиг за да се осигура дека тие ги исполнуваат барањата на eIDAS.

7.4.10. Снимање информации поврзани со работата на услугите на временски жиг

KIBSTrust QTSA гарантира дека сите релевантни информации во врска со работењето на услугите на временски жигови на KIBSTrust се евидентираат за одреден период за обезбедување докази за целите на правните постапки.

KIBSTrust одржува евиденција за сите релевантни информации во врска со работата на KIBSTrust QTSA за временскиот период наведен во дел 7.1.1.

KIBSTrust QTSA одржува евиденција за:

- Синхронизација на часовници кои се користат при креирањето на временскиот жиг.
- Откривање на губење на синхронизацијата.

- Барања за временски жиг и креирани временски жигови.
- Настани поврзани со животниот циклус на TSU клучевите и сертификатите.

7.4.11. Организација

KIBSTrust QTSA гарантира дека е дел од организација која е доверлива како што се бара во ETSI EN 319 421. KIBS ја има финансиската стабилност и ресурси потребни за да работи во согласност со тековниот KIBSTrust QTSA CP/CPS.

Важни документи поврзани со правилата и постапките на KIBSTrust QTSA се достапни на https://www.kibstrust.com/repository.

Овој документ е подготвен на македонски и на други јазици. Во случај на конфликт помеѓу оригиналниот документ на македонски јазик и неговиот превод на друг јазик, преовладува документот на македонски јазик.

Крај на документот