Политика
на издавачот на временски жигови КИБС Моментум

KIBSTrust Momentum

Верзија 4.2

Датум : 03.04.2020

11.45

OID 1.3.6.1.4.1.16305.1.1.3

КИБС АД Скопје

http://www.kibstrust.mk

Информација за документот

Овој документ е подготвен од страна на КИБС АД Скопје (КИБС) и ги содржи условите, според кои КИБС делува како давател на доверливи услуги (TSP) и квалификуван давател на доверливи услуги (QTSP).

Документот е компатибилен со, и се заснова на, стандардот ETSI EN 319 421 „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps“.

Право на интелектуална сопственост

Историја на промени

Верзија	Дата	Автор	Цел на промената
4.2	03.04.2020	Марин Пиперкоски	Терминот „временски печат“ е заменет со терминот „временски жиг“ за да се усогласи о законската регулатива. Дополнување поврзано со престанок на работа на TSA и план за престанок на работа. Дополнување поврзано со одговорност.
4.1	16.10.2018	Марин Пиперкоски	Терминот „временски печат“ е заменет со терминот „временски жиг“ за да се усогласи о законската регулатива. Дополнување поврзано со престанок на работа на TSA и план за престанок на работа. Дополнување поврзано со одговорност.
4.0	24.10.2018	Александар Џамбаски, Сузана Тасевска	Политиката е усогласена со документот ETSI EN 319 421 V1.1.1 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
3.0	17.10.2016	Александар Џамбаски	Променет е издавачот и профилот на сертификатот за временски жигови. Новиот сертификат е од DigiCert. Документот е донесен само во македонска и англиска верзија.
2.0	11.04.2016	Александар Џамбаски	Усогласена е политиката со документот ETSI TS 102 023 V1.2.2 Policy requirements for time-stamping authorities. Променети се лицата кои се дефинирани за изработување и одобрување на документот. Документот е донесен само во македонска и англиска верзија.
1.0	08.05.2012	Александар Џамбаски, Сузана Тасевска	Нов документ

Содржина

Вовед

Компаниите, власта и организациите од сите видови низ целиот свет се повеќе ги генерираат своите процеси електронски за целите на оптимизација, намалувањето на трошоци и брзина. Така, постојните процеси засновани на хартија се заменуваат со електронски процеси и нови процеси овозможени преку употреба 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 традиционални процеси на хартија. За да се исполнат овие барања, и хартиените и електронските информации треба да бидат заштитени, меѓу другото, од манипулација и загуба. За да може да се процени набљудувањето на барањата за усогласеност во професионалното опкружување, доказот за интегритет, комплетност и доверливост се честопати главните критериуми.

Електронскиот временски жиг може да го даде овој доказ за интегритет и комплетност на начин што е едноставен, правно безбеден, постојан, ефтин 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, го документира „кој“ и „што“. За разлика од електронскиот потпис, временскиот жиг не е врзан за луѓето и нивните 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.

Временскиот жиг се користи за да се докаже постоењето на одредени податоци пред одредена временска точка без можност сопственикот да може да го анти-датира временскиот жиг. Откако ќе се потпише датумот, секоја промена на податоците ќе предизвика проверката на електронскиот потпис да не помине со предупредување на корисникот. За разлика од електронскиот потпис, временските жигови не се поврзани со лица и нивните постапки.

Клириншката куќа КИБС АД Скопје (КИБС) користи инфраструктура за јавен клуч и доверливи извори на точно време за да обезбеди квалификувани електронски жигови под името KIBSTrust Momentum.

1. Опсег

Оваа KIBSTrust Политика за издавање на временски жигови/Изјава за практиките (TSP/PS) ја дефинира праксата за работење и управување на Издавачот на временски жигови КИБС (KIBSTrust TSA) со цел претплатниците и засегнатите страни (Relying Parties) да можат да ја проценат доверливоста во работењето со услуги за временски жиг.

KIBSTrust TSA е во сообразност со условите од регулативата (ЕУ) бр. 910/2014 (во понатамошниот текст: регулативата eIDAS) како и согласно Закон за електронски документи, електронска идентификација и доверливи услуги (сл.в. 101/19, 215/19) и подзаконските акти, за издавање на квалификувани електронски временски жигови. Издадените квалификувани временски жигови може да се користат како поддршка на електронските потписи или за апликација која бара доказ дека податокот постоел пред одредено време.

Структурата и содржината на оваа TSP/PS е објавена во согласност со ETSI EN 319 421, „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps“ (Електронски потписи и инфраструктура (ESI); Политика и безбедносни услови за Давателите на доверливи услуги кои издаваат временски жигови).

Интернет адресата на објавените документи е: https://www.kibstrust.mk/repository/.

Во случај на конфликт помеѓу документот на македонски јазик и на англиски јазик, документот на македонски јазик ќе биде меродавен.

2. Референци

2.1. Нормативни референци

[1] Препорака ITU-R TF.460-6 (2002): "Емисии на стандардна фреквенција и временски сигнал".
[2] ISO/IEC 19790:2012: "Информациска технологија – Безбедносни техники – Безбедносни услови за криптографски модули".
[3] ISO/IEC 15408 (делови 1 до 3): " Информациска технологија – Безбедносни техники – Критериуми за евалуација за ИТ безбедност".
[4] ETSI EN 319 401: "Електронски потписи и инфраструктури (ESI); Општи услови за политика за Даватели на доверливи услуги".
[5] ETSI EN 319 422: "Електронски потписи и инфраструктури (ESI); Протокол за временски жиг и профили на токен за временски жиг".
[6] FIPS PUB 140-2 (2001): "Безбедносни услови за криптографски модули".

2.2. Информативни референци

[i.1] ETSI EN 319 122-1: "Електронски потписи и инфраструктури (ESI); CAdES дигитални потписи; Дел 1: Коцки за градење и CAdES основни потписи".
[i.2] IETF RFC 3161 (2001): "Интернет X.509 Инфраструктура за јавен клуч: Протокол за временски клуч (TSP)".
[i.3] IETF RFC 5816: "ESSCertIDV2 ажурирано до RFC 3161".
[i.4] Регулатива (ЕУ) бр 910/2014 на Европскиот Парламент и на Советот за електронска идентификација и услуги за дигитален сертификат за електронски трансакции на интерниот пазар и укинување на Директивата 1999/93/ЕС.
[i.5] Директива на Советот 93/13/ЕЕС од 5 април 1993 за неправедни услови во договори со клиенти.
[i.6] BIPM Циркулар Т.
ЗАБЕЛЕШКА: Достапно од веб страницата на BIPM http://www.bipm.org/.

[i.7] ETSI TS 119 312: " Електронски потписи и инфраструктури (ESI); Криптографски комплети".
[i.8] ETSI TS 102 023: " Електронски потписи и инфраструктури (ESI); Услови на политиката за издавачите на временски потписи".
[i.9] ETSI EN 319 403: " Електронски потписи и инфраструктури (ESI); Даватели на доверливи услуги Оценување на усогласеноста- Услови за органите кои вршат оцена на усогласеноста на Даватели на доверливи услуги".
[i.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".
[i.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".
[i.12] CEN EN 419 231: "Профил за заштита за доверливи системи кои поддржуваат временски жигови".
[i.13] CEN EN 419 221-2: "Профили за заштита за TSP Криптографски модули - Дел 2: Криптографски модул за CSP операции на потпишување со бекап".
[i.14] CEN EN 419 221-3: "Профили за заштита за TSP Криптографски модули - Дел 3: Криптографски модул за CSP услуги за генерирање на клуч".
[i.15] CEN EN 419 221-4: "Профили за заштита за TSP Криптографски модули - Дел 4: Криптографски модул за CSP операции на потпишување без бекап".
[i.16] CEN EN 419 221-5: "Профили за заштита за TSP Криптографски модули - Дел 5: Криптографски модул за дигитални сертификати".

3. Дефиниции и кратенки

3.1. Дефиниции

Координирано универзално време (UTS): временска скала која се заснова на секунда како што е дефинирано во Препораката ITU-R TF.460-6 [1].
Засегната страна: примател на временски жиг кој е засегнат од содржината на тој временски жиг.
Претплатник: правно или физичко лице кому му се издава временски жиг и кое е обврзано со било какви претплатнички обврски.
Временски жиг: податоци во електронска форма која врзува други електронски податоци за одредено време обезбедувајќи докази дека овие податоци постоеле во тој момент.
Политика за временски жиг/ Изјава за практиките" или **TSP/PS** (овој документ) значи група на правила кои ја регулираат применливоста на токен за временски жиг во одредена заедница или класа на примена со општи безбедносни услови.
Давател на доверливи услуги (TSP): субјект кој обезбедува една или повеќе доверливи услуги.
Издавач на временски жиг (TSA): Давател на доверливи услуги кој обезбедува услуги за временски жиг кој користи единици на временски жиг.
Услуга за временски жиг: доверлива услуга за издавање временски жигови.
Единици 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.
Доверлива услуга: електронска услуга која ја зголемува довербата во електронските трансакции.
TSA Изјава за откривање на податоци: сет од изјави за политиките и практиките на TSA кои особено налагаат истакнување или информирање на претплатниците или зависните субјекти, на пример за исполнување на регулаторните услови.
TSA изјава за практиките: изјава за практиките која ја користи TSA при издавање на временски жиг.

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" и 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.

3.2. Кратенки

BTSP	Најдобри практики Политика за временски жиг
CA	Издавач на дигитален сертификат
GMT	Гринич средно време
IERS	Меѓународна служба за ротација на земјата и референтните системи
IT	Информациска технологија
TAI	Temps Atomique International (Меѓународно атомско време)
TSA	Издавач на временски жиг
TSP	Давател на доверливи услуги
TSU	Единица за временски жиг
UTC	Координирано универзално време

4. Општ концепт

4.1. Општ концепт за условите на политиката

Овој документ се референцира на стандардот ETSI EN 319 401 [4] за генерички барања 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.

4.2. Услуга за временски жиг

Услугата за временски жиг ги вклучува следните компоненти:

- Обезбедување на временски жиг: техничката компонента која издава токени за временски жиг (TSTs).
- Управување со временски жиг: услужна компонента која го следи и контролира функционирањето на временскиот жиг, вклучително синхронизација со референтниот UTC временски извор, согласно TSP/PS.

4.3. Издавач на временски жиг

KIBSTrust TSA е давател на доверливи услуги како што е опишано во ETSI EN 319 401 [4] кој обезбедува услуги за временски жиг на јавноста.

KIBSTrust TSA ја презема целокупната одговорност за обезбедување на услугите за временски жиг идентификувани во секција 4.2.

KIBSTrust TSA има одговорност за функционирањето на една или повеќе единици за временски жиг (TSU) кои креираат и потпишуваат TSTs во име на TSA. Секоја TSU има различен клуч.

КИБС управува со KIBSTrust TSA како дел од PKI. KIBSTrust TSA е квалификуван давател на доверливи услуги како што е опишано во eIDAS кој издава временски жигови.

Во продолжение е даден преглед на тековните TSU сертификати и нивните издавачи:

Поле	Вредност
Верзија	3
Сериски број	072ac472580d94c601e7c6fa85e7d10a
Потпис	sha256RSA
DN на издавачот	CN = DigiCert SHA2 Assured ID Timestamping CA OU = www.digicert.com O = DigiCert Inc C = US
Важност	10.05.2019 - 05.10.2022
Предмет DN	CN = KIBSTrust Momentum Timestamp Responder 2016 10 05 1 O = Clearing House Klirinski interbankarski sistemi AD SKOPJE C = MK
Јавен клуч	RSA 2048 bits

КИБС потврдува дека KIBSTrust TSA подлежи на ревизија најмалку на секои 12 месеци извршена од страна на орган за оцена на усогласеноста, кое испорачува извештај за проценката што е можно поскоро и штом истиот е примен. Кога надзорниот орган ќе побара од TSA да исправи било каква повреда на условите, TSA ќе постапува соодветно и навремено. Органот кој врши контрола ќе биде известен за секоја измена во одредбите на TSA.

4.4. Претплатник и засегната страна

Кога претплатникот е правно лице, тој вклучува неколку крајни корисници или поединечен краен корисник и некои од обврските кои важат за тоа правно лице мора да важат и за крајните корисници. Во секој случај, организацијата ќе биде одговорна ако обврските од крајните корисници не се соодветно исполнети и затоа од правното лице 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.

Засегнатата страна е физичко лице или правно лице кој дејствува врз основа на TST генерирани согласно KIBS TSP/PS. Засегнатата страна може и не мора да биде претплатник.

4.5. TSA Политика и изјава за практиката

Политиката за временски жиг на КИБС и изјавата за практиките за временски жиг на КИБС се спојуваат во еден документ – KIBS Политика за временски жиг/Изјава за практиките – TSP/PS.

Овој документ KIBS TSP/PS утврдува политика за временски жиг и изјавата за практиките со цел да се исполнат општите услови за доверливи услуги за временски жиг кои се дефинирани со стандардите во Поглавје 2 од овој Документ.

За дополнителни детали за KIBSTrust TSA, погледнете во Поглавје 5 од овој Документ.

TSA издава временски жигови на сите заинтересирани страни без технички ограничувања. За издавање на временски жигови може да се плаќа надоместок, кој е дефиниран во тарифата на КИБС АД Скопје, објавена 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/.

5. Политика за временски жиг

5.1. Општо

Оваа политика за временски жиг дефинира низа процеси за доверливо креирање на токени за временски жиг во согласност со ETSI EN 319 421. Приватните клучеви и TSU ги исполнуваат техничките спецификации на ETSI EN 319 422 и RFC 3161.

KIBSTrust TSA 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**.

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

TSU сертификатите кои се користат за генерирање на временски жигови се издаваат од страна на DigiCert, Inc., 2801 North Thanksgiving Way, Suite 500, Lehi, Utah 84043. Нивната спецификација е опишана во документите во архивата на политиките на DigiCert кои се наоѓаат на https://www.digicert.com/legal-repository/.

5.2. Идентификација

Идентификацијата на политиката за временски жиг утврдена во овој документ е:

OID: 1.3.6.1.4.1.16305.1.1.3

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) KIBS AD Skopje (16305) Objects Related to PKI-X.509 (1) Certification Policies and CPSs (1) KIBS Momentum TSA Policy (3)}

Овој ОИД е содржан како референца во секој издаден временски жиг, во KIBS TSP/PS и во Декларацијата на TSA која им е достапна на Претплатникот и на засегантите страни.

Поддржана е ETSI идентификацијата за временски жиг **0.4.0.2023.1.1** (BSTP).

5.3. Заедница на корисници и применливост

Оваа политика има за цел исполнување на условите за временски жиг за долготрајна важност (како што е дефинирано во ETSI EN 319 122 [i.1]) 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.

6. Политики и практики

6.1. Проценка на ризик

KIBS врши процена на ризик со цел идентификација, анализа и евалуација на ризиците поврзани со доверливата услуга кои се однесуваат на деловни и технички прашања. Мерките за третирање на ризикот обезбедуваат дека нивото на безбедност е сразмерно на степенот на ризик. Се избираат соодветни мерки за третирање на ризикот, земајќи ги предвид резултатите од проценатa на ризикот.

Проценатa на ризик редовно се прегледува и ревидира со цел да се обезбеди квалитет и доверливост на услугите за временски жиг.

Безбедносните контроли кои се дефинирани во безбедносен концепт на услугите за временски жиг се контролираат редовно со цел да се обезбеди ефикасност на контролите.

Раководството на КИБС ја одобрува проценатa на ризик и го прифаќа идентификуваниот преостанат ризик.

6.2. Изјава за практикување на доверливата услуга

KIBS TSP/PS ги утврдува општите правила во однос на функционирањето на KIBSTrust TSA. Дополнителни интерни документи дефинираат како КИБС ги исполнува техничките, организациските и процедуралните услови идентификувани во TSP/PS.

TSP/PS, Декларацијата на TSA и други јавни документи можат да се најдат на https://www.kibstrust.mk/repository/.

Интерните документи може да се обезбедат само во строго контролирани услови.

KIBS TSP/PS ги идентификува обврските на надворешните организации кои ги поддржуваат TSA услугите вклучувајќи применливи политики и практики.

KIBS TSP/PS е одобрен од Групата за управување со политиките на КИБС. Групата за управување со политиките на КИБС има одговорност да се осигури дека практиките се соодветно имплементирани. Секоја нова верзија веднаш се објавува и ја заменува претходната верзија.

6.2.1. Hash алгоритми

- Прифатливи хашови за барање за временски жиг: SHA-256, SHA-384, SHA-512,
- Потпис: sha256WithRSAEncryption (2048 бит клуч).

6.2.2. Точност на времето

Токените за временски жиг се издаваат со временска прецизност до ±1 секунда на UTC. Ако не може да се обезбеди доверлив UTC временски извор - временскиот жиг нема да биде издаден.

6.2.3. Ограничувања на услугата

Не применливо.

6.2.4. Обврски на претплатникот

Обврските на претплатникот се опишани во точка 6.5.2 од овој документ.

6.2.5. Обврски на засегнатата страна

Обврските на засегнатата страна се опишани во точка 6.6 од овој документ.

6.2.6. Проверка на временскиот жиг

Проверката на временскиот жиг ги вклучува следните задачи:

1. **Проверка на издавачот на временски жиг**

Издавачот е орган кој издава временски жигови кој користи соодветни електронски сертификати за издавање на временски жиг. Јавните клучеви на сертификатите кои се користат кои се вклучени во TSU и CA сертификатите се објавени за да ја овозможат верификацијата дека временскиот жиг е потпишан уредно од страна на TSA.

Сертификатите може да се најдат на следните линкови:

http://cacerts.digicert.com/DigiCertSHA2AssuredIDTimestampingCA.crt и
http://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt.

2. **Проверка на статусот на отповикување на временскиот жиг**

За да се провери статусот на поништување на сертификатите кои се користат во временскиот жиг достапни се услугата OCSP и CRL листата. Адресата за пристап до услугата OCSP е http://ocsp.digicert.com. CRL Дистрибутивните листи се објавени на http://crl3.digicert.com/sha2-assured-ts.crl и http://crl4.digicert.com/sha2-assured-ts.crl.

3. **Проверка на интегритетот на временскиот жиг**

Криптографскиот интегритет на временскиот жиг, на пример ASN.1 структурата е точна и датумот (податокот на кој е ставен временски жиг) припаѓа на апликацијата. Може да се провери соодветна веб страна на веб-услугата на KIBSTrust TSA, која се нуди бесплатно на следната адреса: https://www.kibstrust.mk.

6.2.7. Применливо право

Овој документ е регулиран во согласност со македонското законодавство и регулативата на ЕУ и соодветните стандарди. Во случај на спор помеѓу страните и во отсуство на договор помеѓу страните, единствен надлежен суд за реѓавање на спорот е судот во Скопје.

6.2.8. Достапност на услугата

KIBSTrust TSA ги има имплементирано следните мерки за обезбедување на расположливост на услугата:

- Редундантни ИТ системи за избегнување на поединечни точки на дефекти.
- Редундантни врски за интернет со голема брзина за избегнување на прекин во услугата
- Користење на непрекинато напојување.

Иако овие мерки обезбедуваат расположливост на услугата, КИБС TSA има за цел да обезбеди расположливост на услугата 99% годишно.

6.3. Правила и услови

Условите се опишани во документот „Правила и услови за користење на услугата за времески жиг Моментум“ кој се наоѓа на адресата: https://www.kibstrust.mk/repository/.

6.4. Политика за сигурност на информации

КИБС има имплементирано политика за сигурност на информации во рамки на компанијата. Сите вработени мора да се придржуваат кон прописите утврдени во овој документ и изведените сигурносни концепти. Документот „Политики за сигурност на информациите“ редовно се прегледува а особено кога настануваат значителни измени. Измените на документот ги одобрува раководството на КИБС.

6.5. Обврски на издавачот на временски жигови

6.5.1. Општо

KIBS TSA ги исполнува условите и процедурите опишани во Поглавје 6 од овој документ како и одредбите од eIDAS, кои се имплементирани како применливи за избраната доверлива политика за временски жиг.

КИБС е страна во взаемните договори и обврски помеѓу TSA, претплатниците и засегнатите страни. TSP/PS е составен елемент на овие договори.

6.5.2. Обврски на издавачот на временски жигови кон претплатниците

Овој документ не налага никакви посебни обврски за претплатникот освен услови кои се специфични за TSA и кои се утврдени во документот “Правила и услови за користење на услугата за времески жиг Моментум“.

6.6. Информација за засегнатата страна

Засегнатата страна мода да провери дека временскиот жиг е точно потпишан и дека приватниот клуч кој се користи за потпишување на временскиот жиг не е поништен. Засегнатата страна треба да ги почитува сите ограничувања за користењето на временскиот жиг посочен од КИБС TSP/PS. За време на рокот на важност на сертификатот на TSU, статусот на приватниот клуч може да се верификува со користење на релевантни CRLs, Сертификати на КИБС CA, TSU сертификати и слично. Листите на поништени сертификати (CRLs) се објавени на http://crl3.digicert.com/sha2-assured-ts.crl и http://crl4.digicert.com/sha2-assured-ts.crl.

7. TSA управување и работење

7.1. Вовед

KIBS има имплементирано систем за управување со сигурноста на информациите со цел да се одржува сигурноста на услугата.

Обезбедувањето на временски жиг како одговор на барање е на дискреција на KIBS TSA во зависност од било кој договор за обезбедување ниво на услуга склучен со претплатникот.

7.2. Внатрешна организација

a) КИБС е правен лице согласно македонското законодавство.
КИБС АД Скопје
+389 2 5513 401, +389 2 3297 401
helpdesk@kibstrust.mk
https://www.kibstrust.mk/
Бул. "Кузман Јосифовски Питу", 1,
1000 Скопје, Република Северна Македонија

b) КИБС има систем за управување со квалитет и информациска сигурност соодветен за обезбедуваните услуги за временски жиг.

c) Персоналот на КИБС го има потребното образование, обука, техничко знаење и искуство во однос на видот, опсегот и обемот на работата која е потребна за обезбедување на услугите за временски жиг.

7.3. Безбедност на вработените

KIBS обезбедува дека вработените и изведувачите ја поддржуваат доверливоста на операциите на TSA.

KIBS вработува персонал и, доколку е применливо, подизведувачи, кои ја поседуваат потребната стручност, искуство и квалификации и кои имаат поминато обука во однос на безбедноста и правилата за заштита на личните податоци како што е соодветно за услугите кои се нудат и функцијата на работното место.

Персоналот на KIBS е способен за исполнување на условот за „стручно знаење, искуство и квалификации“ преку формална обука и препораки, или фактичко искуство или комбинација од

двете. Ова треба да вклучува редовни (најмалку на секои 12 месеци) ажурирања за нови закани и тековни безбедносни практики.

Против персоналот кој врши повреда на политиките или процедурите на КИБС ќе се применуваат соодветни дисциплински санкции.

Безбедносните улоги и одговорности, како што е специфицирано во Политиките за сигурност на информации, се документирани во описите на работните места и му се расположливи на целиот засегнат персонал.

Доверливи улоги, од кои зависи безбедноста на операциите на KIBS TSA, се јасно дефинирани, именувани од страна на раководството и прифатени од страна на раководството и лицето кое треба да ја исполнува улогата.

Кај целиот персонал на KIBS кој е на доверлива позиција не смее да постои конфликт на интереси кои можат да ја загрозат објективноста на операциите на KIBS TSA.

7.4. Управување со средствата

Сите ИТ системи кои се користат во рамки на услугата се јасно дефинирани, категоризирани и внесени во база на податоци за управување со средства.

Со сите медиуми се постапува на безбеден начин.

Податоците од користените медиуми се безбедно избришани, било со електронско бришење на податоци или со физичко уништување на искористените медиуми.

7.5. Контрола на пристап

Различни нивоа на безбедност во врска со физички и логички пристап обезбедуваат безбедно функционирање на услугата за временски жиг. На пример:

- Безбедна физичка средина
- Сегрегација на мрежни сегменти
- Сегрегација на должности
- Огнени ѕидови, IPS/IDS
- Следење на мрежата и услугата
- Зајакнување на ИТ системи
- Во случај одредено лице кое извршува операции за услугите за временски жиг, да ја смени улогата или да ја напушти организацијата, сите безбедносни токени од тоа лице се повлекуваат.

7.6. Криптографски контроли

7.6.1. Општо

TSA користи приватни клучеви за обезбедување на неговата услуга. Се користи еден пар од приватни клучеви за издавање на сертификат за временски жиг за јавен клуч, кој се користи во рамки на TSU. Еден пар од приватни клучеви се користи во рамки на TSU за издавање на временски жигови.

Сите приватни клучеви се складираат во хардвер со ниво на безбедност FIPS 140-2 Ниво 3 (HSM).

7.6.2. Генерирање на клуч на TSU

TSU користи RSA пар клучеви со должина од 2048-бита. Овој пар клучеви се користи само за потпишување на TST.

Сите криптографски модули се поврзани со истиот сертификат за јавен клуч.

a) Генерирањето на клучевите за потпишување на TSU се врши во физички обезбедена средина (согласно секција 7.8) од страна на доверлив персонал на соодветни позиции (согласно секција 7.3), барем под контрола на двајца членови на доверливиот персонал. Персоналот овластен за вршење на оваа функција е ограничен на оние кои се обврзани на тоа согласно практиките на TSA.

b) Генерирањето на клучот за потпишување на TSU се врши во рамки на криптографски модул кој е во согласност со FIPS PUB 140-2 [I.9], ниво 3, или ISO 15408 Common Criteria EAL 4+.

c) Алгоритамот за генерирање на клуч за TSU, алгоритамот за потпишување, должината на клучот кој се користи за потпишување на временските жигови, ги признава националниот надзорен орган и моменталната техничка состојба се утврдува како соодветна за потпишување на временските жигови издадени од TSA.

7.6.3. Заштита на TSU приватен клуч

Се применуваат Практиките на заштита на клучот на TSU, складирањето, сигурносната копија и обновувањето, опишани во секциите 6.2 и 6.3 на KIBS TSA/PS.

Приватниот клуч на TSU ќе биде снимен и складиран безбедно за неверојатен настан на губење на клуч поради неочекуван прекин на напојување или испад на хардвер.

Копија од клучот ќе биде прибавена во Церемонијата за генерирање на клучеви. Копијата од приватен клуч се чува во тајност и неговиот интегритет и веродостојност се чува во сеф.

7.6.4. TSU Сертификат за јавен клуч

TSA гарантира интегритет и веродостојност на клучевите за проверка на потпис на TSU како што следува:

a) Поверката на потписот (јавни клучеви) е достапна на засегнатите страни кои веруваат во сертификатот со јавен клуч. Сертификатите се објавени на следниот линк: https://www.kibstrust.mk/mk-MK/Home/Support.
b) TSU не издава временски жиг пред проверка на неговиот потпис (јавен клуч). Кога сертификатот е внесен во TSU, TSA верификува дека сертификатот е уредно потпишан (вклучително проверка на ланецот на сертификати на доверлив орган за сертификација).
c) Се издава само еден TSU сертификат со негов приватен клуч.
d) TSU сертификатите не се продолжуваат.
e) Информациите за важноста во однос на TSU сертификатите се ажурира периодично и CRL или OCSP услугите се достапни со референците кои се наоѓаат во сертификатите.

7.6.5. Продолжување на клуч на TSU

Важноста на TSU сертификатот зависи од периодот на избраниот алгоритам и должината на клучот (видете точка 7.6.2c).

Сертификатот може да се издаде за целиот очекуван рок. Рокот на важност на TSU класата е ограничена од:

- Рокот на важност на издавачот на основниот сертификат на издавачот.
- Еднаш годишно или кога ќе настане значајна измена, лицето кое е носител на улогата службеник за безбедност ги верификува сите криптографски алгоритами кои се користат во TSA проверка дека секој алгоритам е признаен како соодветен, како што е утврдено во секција 7.6.2c.

Ако алгоритам влезе во ситуација на ризик повеќе нема да се смета за адекватен; Менаџерот за безбедност ќе му наложи на TSA да прекине со користење на засегнатите клучеви и да внесат нови клучеви.

7.6.6. Управување со рокот на важност на криптографски хардвер

Користениот криптографски хардвер се проверува од страна на доверлив персонал (во присуство на две лица) за време на испораката и складирањето. Хардверот особено се верификува за:

a) Оштетувања во безбедносните пломби
b) Било какви оштетувања во куќиштето на хардверот (на пр. Гребнатинки, нерамнини..)
c) Било какви оштетувања во пакувањето на хардверот

За инспекцијата се прави записник.

Покрај тоа, важи следното:

a) Инсталацијата, активирањето на клучевите за потпис на TSU во криптографскиот хардвер го врши само персонал на доверливи позиции со употреба на, како минимум, двојна контрола во физички безбедна средина.
b) Приватните клучеви за потпишување на TSU кои се складираат во TSU криптографски модул се бришат по повлекување на уредот на начин на кој е практично невозможно да се повратат.

7.6.7. Крај на рокот на важност на клучот на TSU

По истекот на приватните клучеви, приватните клучеви во рамки на криптографскиот модул се уништуваат на начин на кој приватните клучеви не можат да се обноват.

Службеникот за безбедност ја дефинира важноста на клучот во согласност со клаузула 7.6.2c.

7.6.8. Издавач на коренски сертификат

KIBS TSA е потпишан од страна на DigiCert. Политиките на DigiCert се достапни на https://www.digicert.com/legal-repository/.

7.7. Временски печат

7.7.1. Издавач на временски печат

KIBS TSA нуди услуги за временски жиг со користење на RFC 3161 “Протокол за временски жиг (TSP)”. Услугата URL е специфицирана во договорот со претплатникот. Секој TST содржи идентификација на Политиката за временски жиг, единствен сериски број и сертификат кој ги содржи идентификациските информации на TSU на KIBS TSA.

TSU во временскиот жиг бара и прифаќа SHA256, SHA384, SHA512 хаш алгоритми и ја користи SHA-256 криптографската функција за потпишување на TST.

TSU клучевите се 2048-битни RSA клучеви. Клучот се користи само за потпишување на TST.

TSA ги евидентира сите издадени TST. TSTs се евидентираат за неограничен рок. KIBS TSA може да го докаже постоењето на TST на барање на засегнатата страна. KIBS TSA може да бара зависниот субјект да ги покрие трошоците за таа услуга.

TSU не издава TST кога крајот на рокот на важност на TSU приватниот клуч е достигнат.

7.7.2. Синхронизација на часовникот со UTC

КИБС мора да се осигури дека неговиот часовник е синхронизиран со UTC со прецизност до 1 (една) секунда или поголема прецизност, со употреба на NTP протокол.

КИБС ја следи синхронизацијата на часовникот и обезбедува дека, ако времето наведено во TST отстапува од синхронизацијата со UTC, истото е детектирано. Доколку часовникот на TSA отстапува од точното време, временскиот жиг нема да биде издаден се додека не се изврши синхронизација на часовникот.

Посебно се опфатени следниве теми:

- Постојана калибрација на TSU часовникот
- Следење на точноста на TSU часовникот
- Анализа на закани од напади на временските сигнали
- Однесување при прескокнување/додавање на престапна секунда
- Однесување при отстапување поголемо од 1 секунда од UTS.

7.7.3. Профили на токен за временски жиг (TCT)

Поле	Значење/Вредност
Верзија	1
Хаш алгоритам	SHA-256, SHA-384, SHA-512
Податоци за пораката	Hash value of data
Политика OID	OID=1.3.6.1.4.1.16305.1.1.3 (enchances OID=0.4.0.2023.1.1)
Сериски број	TST serial number
Генерирано време	TST generation time
Прецизност	±1 second of UTC
Налог	FALSE
Nonce	supported
TSA	CN = KIBSTrust Momentum Timestamp Responder 2016 10 05 1 O = Clearing House Klirinski interbankarski sistemi AD SKOPJE C = MK
	CN = DigiCert SHA2 Assured ID Timestamping CA OU = www.digicert.com O = DigiCert Inc C = US

7.8. Физичка безбедност и безбедност на средината

TSA е сместен во високо безбедна физичка средина.

Капацитетите за функционирање на услугата временски жиг се управуваат во средина која е физички и логички ја заштитува услугата со контроли на неовластен пристап во системите или податоците. Секој влез во физички безбедна област подлежи на независен мониторинг на TSA. Во безбедната област, лицето кои пристапува во објектите е придружувано, се регистрира неговиот идентитет, влезот и излезот. Мерките преземени во однос на физичката заштита се

дел од системот за информациска сигурност кој е развиен и имплементиран во КИБС, во согласност со условите од ISO/IEC 27001:2013, ETSI EN 411 401 и ETSI EN 411 421 стандардите.

КИБС има имплементирано безбедносни контроли за избегнување на:

- губење, оштетување или компромитирање и прекин на деловните активности;
- губење, оштетување или компромитирање на ресурси;
- компромитирање или кражба на информации и капацитети за обработка на информации.

Физичката заштита се постигнува преку јасно дефинирани безбедносни параметри (на пример физички бариери) околу управувањето со временски жигови и физичкиот пристап до критичните компоненти на TSA системот е ограничена на овластени лица.

Критичните компоненти на TSA се наоѓаат во заштитен безбедносен периметар со физичка заштита од упад, контроли на пристапот преку безбедносниот периметар и аларми за детектирање на упад.

Контролите на пристапот се применуваат за HSM уредите со цел исполнување на условите за безбедност на криптографските модули како што е идентификувано во точка 7.6.

Контролите се применуваат за заштита од неовластено однесување од локацијата на опрема, информации, медиуми и софтвер кои се поврзани со услугите за временски жиг.

Безбедносните физички контроли и контроли на средината го заштитуваат капацитетот во кој се сместени системските ресурси, самите системски ресурси, и капацитетите кои се користат за поддршка на нивното работење. Политиката на КИБС за физичката безбедност и безбедноста на средината за системите поврзани со управувањето со временски жигови како минимум опфаќаат контрола на физичкиот пристап, заштита од временски непогоди, фактори за противпожарна заштита, испад на придружните услуги (на пример напојување, телекомуникации), испад на структурата, протекувања на водоводната мрежа, заштита од кражба, провала и влегување, и оправување од катастрофа.

7.9. Оперативна безбедност

KIBS TSA има имплементирано напреден систем за контрола и безбедносни контроли со цел да обезбеди квалитет и расположливост на услугите. Таквите контроли се:

a) Анализата на безбедносните услови се врши на спецификациите на дизајнот и условите за секоја фаза од проектот за развој на системот преземена од страна на организацијата или во име на TSP за да се обезбеди дека безбедноста е вградена во системите за информациска технологија.

b) Како процедури за контрола на промените, контролата на верзијата се применува за измените и корекциите на софтверот.

c) Интегритетот на системите и информациите на TSP е заштитен од вируси, злонамерен и неовластен софтвер.

d) Средствата кои се користат во рамки на TSP системите се безбедни и заштитени од оштетување, кражба, неовластен пристап и застареност.

e) Во рамки на рокот во кој евиденцијата мора да се чува, процедурите за управување со медиуми обезбедуваат заштита од застареност и пропаѓање на средствата за телекомуникација.

f) Примената на соодветни процедури за сите административни функции од доверба и кои имаат влијание врз испораката на услугата.

g) TSP има специфицирано и применува процедури за обезбедување дека се применуваат безбедносни закрпи со разумно време откако станале достапни. Безбедносната закрпа не треба да се применува ако воведува дополнителна ранливост или нестабилност која преовладува пред користа од примената на безбедносната закрпа. Причината за неприменување на безбедносните закрпи ќе бидат документирани.

7.10. Мрежна безбедност

TSP ја штити својата мрежа и системи од напади:

a) TSP мрежата е сегментирана во мрежи или зони врз основа на проценка на ризик земајќи го во предвид функционалниот, логичкиот и физичкиот (вклучително локација) однос помеѓу доверливите системи и услуги.

b) TSP го ограничува пристапот и комуникациите помеѓу зони на оние кои се неопходни за функционирањето на TSP. Непотребните приклучоци и услуги се изречно забранети или деактивирани. Утврдената низа правила редовно се прегледува.

c) Сите елементи од критичките системи на TSP (на пример коренски CA систем, TSU) се чуваат во безбедна зона.

d) Воспоставена е наменска мрежа за администрирање на ИТ системи, која е одвоена од оперативната мрежа. Системите кои се користат за администрирање нема да се користат за административни цели.

e) Платформата за тестирање и платформата за производство се одвоени. Платформата за тестирање се наоѓа во средина која не е засегната со операции во живо (на пример развој).

f) Комуникацијата помеѓу различни доверливи системи може да се утврди само преку доверливи канали кои логички се разликуваат од други комуникациски канали и обезбедуваат сигурна идентификација на нејзините крајни точки и заштита на податоците од измена и откривање.

g) Надворешната мрежна конекција на интернет е редундантна за да се обезбеди расположливост на услугите во случај на еднократен испад.

h) TSP врши редовно скенирање на ранливоста за јавните и приватните IP адреси идентификувани од TSP, анализата на ранливости ја врши лице или субјект со вештини, алатки, стручност, етички кодекс и независност кои се потребни за обезбедување на веродостоен извештај.

i) TSP, после конфигурацијата на инфраструктурата со ажурирања или измени кои TSP ги смета за релевантни, извршува тестирање на пенетрација во системите.

j) TSP прибавува доказна евиденција дека секој тест на пенетрација е извршен од страна на лице или субјект со вештини, алати, стручност, етички кодекс и независно кои се потребни за обезбедување на веродостоен извештај.

7.11. Управување со инциденти

Дополнителни информации можат да се добијат во документот „Контрола на неусогласености, инциденти и проблеми“.

Системските активности во однос на пристапот до ИТ системите, корисничките системи, и барањата за услуги се надгледуваат. Особено:

a) Следење на активностите земајќи ја во предвид чувствителноста на сите информации кои се собрани или анализирани.

b) Абнормални системски активности кои упатуваат на потенцијална повреда на безбедноста, вклучително упад во TSP мрежата, се детектираат и пријавуваат како аларми.

c) ИТ системите на TSP ги следат следните настани: Вклучување и исклучување на функциите за зачувување ревизорска трага (log); расположливост и искористување на потребните услуги со TSP мрежа.

d) TSP дејствува навремено и координирано со цел брзо да одговори на инцидентите и да го ограничи влијанието на безбедносните повреди. TSP назначува персонал на доверливи функции за следење на предупредувањата за потенцијално критични безбедносни настани и обезбедува дека предметните инциденти се пријавени во согласност со процедурите на TSP.

e) TSP ги известува соодветните страни, во согласност со применливите регулаторни правила за секоја безбедносна повреда или губење на интегритет кои имаат значително влијание врз доверливата услуга која се обезбедува и врз личните податоци кои се одржуваат во истата.

f) Националниот надзорен орган се известува во рок од 24 часа по откривање на критична безбедносна повреда.

g) Дневниците од ревизијата редовно се следат и прегледуваат со цел да се идентификуваат докази за злонамерна активност.

h) TSP ќе ги решава критичните ранливости во разумен рок по нивното откривање. Ако тоа не е возможно TSP ќе изготви и ќе имплементира план за намалување на критичката ранливост или TSP ќе ја документира фактичката основа за одлуката на TSP дека ранливоста не бара санирање.

i) Процедурите за известување за инциденти и одговор се користат на начин на кој штетата од безбедносните инциденти и неисправности се сведува на минимум.

7.12. Прибирање докази

Во моментот кога безбедносниот инцидент е детектиран, тоа може да не биде очигледно, ако тој безбедносен инцидент е предмет на дополнителни истраги. Затоа, важно е секој доказ, статусот на ИТ системот или информациите кои безбедно се зачувуваат пред да станат некорисни или уништени.

Евиденцијата на TSP е пристапна одреден период, вклучително и по престанување на активностите на TSP. Сите релевантни информации во однос на податоците кои се издадени и примени од страна на TSP се чуваат за да обезбедат докази во правни постапки и да се обезбеди континуитет на услугите. Особено:

a) Се одржува доверливоста и интегритетот на тековните и архивираните податоци во однос на обезбедувањето на услугите.

b) Евиденцијата во однос на управувањето со услугите е доверлива и е поднесена во согласност со опишаните деловни практики.

c) Евиденцијата во однос на управувањето со услугите, доколку е потребно, се става на располагање за целите на обезбедување докази за исправното функционирање на услугите за правни постапки.

d) TSP го регистрира точниот момент, значајните настани во средината, управувањето со клуч и синхронизацијата на часовникот. Времето кое се користи за евиденција на настани, како што се бара во дневникот од ревизијата, постојано се синхронизира со UTC.

e) Евиденцијата во однос на услугите се чуваат во текот на периодот по истекот на важноста на клучевите за потпишување или на токенот за услуги за да се обезбеди нивно чување за потребните правни докази во согласност со овој документ.

f) Настаните се евидентираат на начин на кој истите не може да бидат избришани или уништени (освен ако можат безбедно да се префрлат на долгорочен медиум).

7.13. Управување со деловниот континуитет

Резервна копија од базите на податоци за сите издадени TSTs од страна на КИБС TSA се чуваат надвор од локацијата.

Ако TSU приватниот клуч е компромитиран или постои сомнение за компромитација, KIBS TSA ќе ги извести претплатниците и засегнатите страни и ќе прекине со употреба на компромитираниот клуч.

7.14. Престанок на TSA и план за престанок

Во примена е праксата утврдена во документот „План за престанок на дејноста на довереният услуги на услуги“. Понатаму, КИБС како квалификуван давател на доверливи услуги презеде неопходни мерки со кои се обезбедува зачувувањето на сите релевантни архивирани записи пред прекинувањето на услугата.

7.15. Усогласеност

КИБС TSA обезбедува усогласеност со важечкиот закон и стандарди.

a) MK-eIDAS
b) Регулатива (EU) N°910/2014
c) ETSI TS 319 421, ETSI EN 319 401, ETSI TS 319 421
d) IETF (RFC 3161)

Проверката на усогласеност со овие прописи се врши за време на проценката на усогласеност.

Анекс А: Потенцијална одговорност за давање на услуга издавање временски жиг

Одговорноста на КИБС, кој дејствува како QTSSP, на претплатниците и засегнатите страни поврзани со услугата е одредена во документот „Услуви и правила за користење н услугата Momentum“ или како што е предвидено во постојното важечко законодавство.

КИБС не може да биде одговорен за каква било штета што произлегува од каква било погрешна употреба на услугата за издавање временски жиг, Моментум, освен оној што е предвидено со оваа TSA/PS на КИБС за услугата Моментум и документот „Услови и правила за користење на услугата Моментум“.

КИБС е одговорен за евентуална директно утврдена штета, намерна или од небрежност, за било кое физичко или правно лице, како резултат на неисполнување на обврските утврдени во TSP/PS на КИБС.

КИБС како квалификуван давател на доверлива услуга за временски жиг ја ограничува својата одговорност. Ограничувањето на одговорноста вклучува: исклучување на индиректни, специјални, инциденти и последователни штети. Ова исто така вклучува максимална финансиска одговорност во врска со комбинираната агрегатна одговорност на КИБС кон кое било и сите лица во врска со издавачот на временски жиг, што е ограничено на сума која не ја надминува соодветната сумата наведена во документот „ Услови и правила за користење на услугата Моментум“ или претплата за услугата за времеснки жиг, што ќе се пресметува врз основа на пропорционална стапка, без оглед на природата на одговорност, видот, висината или обемот на претрпената штета.

Ограничувањата на одговорноста се исти без оглед на бројот на издадени временски жигови или побарувања поврзани со таков временски жиг.

TSA КИБС одбива каква било одговорност во однос на употребата на испорачаните временски токени кои ги испорачува и потпишува.

Анекс Б: Декларација на TSA

Декларацијата на TSA КИБС е дадена во документот “Декларација за користење на услугата временски жиг Momentum” лоцирана на адреса: https://www.kibstrust.mk/repository.

Анекс B: Координирано универзално време (UTC)

Координираното универзално време (UTC) е меѓународен временски стандард кој стапил на сила на 1 јануари 1972 година. UTC го заменил Средното време по Гринич (GMT). Универзалното време се заснова на часовник од 24 часа.

Координираното универзално време (UTC) го сочинува временската скала, заснована на секунда, дефинирана и препорачана од Меѓународниот комитет за телекомуникациско радио (ITU-R), управувано од Меѓународното атомско време (TAI), и пресметувано од Bureau International des Poids et Mesures (BIPM) од отчитувањата на повеќе од 200 атомски часовници лоцирани во метролошки институти и опсерватории во повеќе од 30 земји низ целиот свет. Информациите за TAI се достапни секој месец во Циркуларот T на BIPM (ftp://62.161.69.5/pub/tai/publication). Оваа пресметка е помогната од Меѓународната служба за следење на ротацијата на земјата (IERS) (http://hpiers.obspm.fr/) за да се обезбеди дека се земени предвид сите неправилности.

Целосната дефиниција за UTC е содржана во препораката ITU-R TF.460-6 [1].

Анекс Г: Долгорочна проверка на временскиот жиг

Доколку во моментот на проверката (верификацијата):

- приватниот клуч на TSU не е компромитиран во ниту еден момент се до моментот кога засегнатата страна го потврдува временскиот жиг;
- алгоритмите за хаш користени во временската жиг се соодветни за време на проверката;
- алгоритмот за потпис и големината на клучот за потпис под кој е потпишан временскиот жиг е сè уште надвор од дофатот на криптографски напади во моментот на проверката;

тогаш проверката на временскиот жиг сè уште може да се изврши надвор од крајот на периодот на важење на сертификатот од TSU.

Валидноста може да се задржи со ставање на дополнителен временски жиг за заштита на интегритетот на претходниот. Алтернативно, податоците врз кои е ставен временски жиг може да бидат ставени во безбедно складиште.

Крај на документот