Политика

на

Издавачот на временски печати КИБС Моментум

Верзија 3.0

Датум : 17.10.2016

11.45

OID 1.3.6.1.4.1.16305.1.2.3

КИБС АД Скопје

http://www.kibstrust.mk

Содржина:

Вовед

Клириншката куќа КИБС АД Скопје (во понатамошниот текст: КИБС) како **Издавач на временски печати** (во понатамошниот текст: Издавач), им нуди на своите клиенти услуги за временски печат кои се во согласност со Законот за податоци во електронски облик и електронски потпис[1].

Овој документ е **Политика на Издавачот на временски печати КИБС Моментум** (во понатамошниот текст: Политика). Тој ги опишува услугите за временски печати и ги специфицира обврските на КИБС како Издавач во врска со тие услуги. Оваа Политика исто така ги опишува обврските и барањата на претплатниците и засегнатите страни. Нејзината структура и содржина е компатибилна со стандардот ETSI TS 102 023 V1.2.2[2].

Временските печати издадени во согласност со оваа Политика може да се користат за долгорочно архивирање на електронски потпишани документи[3], трансакции и други електронски записи.

1. Опсег

Овој документ може да се користи од страна на засегнатите страни и претплатниците на Издавачот на сертификати КИБС, како основа за обезбедување на сигурност и надежност на услугите, кои се предмет на овој документ. Политиката на Издавачот КИБС Моментум е базирана на X.509 сертификати, доверлив временски извор и алгоритмите за криптографија со приватен и јавен клуч.

2. Публикации и обврски околу документите

КИБС Моментум, како Издавач на временски печати ја објавува Политиката. Овој документ е достапен на web адресата: http://www.kibstrust.mk/Repository/repositoryMK.aspx.

Издавачот јавно ги објавува следните информации:

- Политиката
- Правилата за квалификувани сертификати, донесени од издавачот на сертификати КИБС
- Сертификатите на уредите за генерирање на временски печати.

Нова верзија на оваа политика се објавува кога:

- има значајни промени кои влијаат на Политиката
- промените во законската регулатива имаат влијание на оваа Политика.

Сертификатите на уредите за генерирање на временски печати се објавуваат најмногу 24 часа по нивното генерирање и пред нивното активирање.

Документите кои содржат информации за Издавачот, процедурите, законските регулативи и директивите се наведени во оваа политика, а останатата литература е објавена во Правилникот на КИБС за издавање на квалификувани сертификати (http://www.kibstrust.mk/Repository/repositoryMK.aspx).

Сите промени на информациите се ограничени на авторизиран персонал на КИБС.

---

[1] Службен весник на Република Македонија 34/01 ... 98/08

[2] ETSI TS 102 023 V1.2.2 Policy requirements for time-stamping authorities

[3] IETF RFC 3126, Electronic Signature Formats for long term electronic signatures, September 2001

3. Дефиниции и кратенки

3.1. Дефиниции

Претплатник: Ентитет кој бара услуга обезбедена од Издавачот.

Засегната страна: Единка или ентитет која се потпира на временскиот печат генериран според Политиката на Издавачот. Засегната страна може, но не мора да биде претплатник.

Ревизор: Лице кое прави ревизија на работата на Издавачот.

CRL: Регистар на поништени сертификати е листа дигитално потпишана од Издавачот на сертификати која содржи идентификатори на сертификати поништени пред истекување на нивната важност.

Hash (хеш) вредност: Податок со фиксна големина (на пример 256-бита) кој е добиен со примена на еднонасочна математичка функција – hash алгоритам (на пример SHA-256) од одредена количина на влезни податоци. Ако постојат промени во влезните податоци, hash вредноста се менува.

Временски печат: Податочен објект кој ја поврзува претставата за еден податок со одредено време, изразено во Координирано универзално време (UTC), со што се обезбедува доказ дека податокот во тоа време постоел.

Услуги на издавачот на временски печати: Група на операции потребни да се управува и генерира Временски печат.

Уред за генерирање на временски печати (УГВП): Хардвер и софтвер кој се користи за креирање на временски печати, карактеризирани преку идентификатор на Уредот сертифициран од одреден Издавач, во кој има единствен клуч за потпишување на временските печати.

Систем за издавање на временски печати: Група на сите Уреди за издавање на временски печати, со одредени административни и надгледувани компоненти кои се користат за обезбедување на Услугата за Издавачот на временски печати.

3.2. Кратенки

CA:	Certification Authority	**ИС**	**Издавач на сертификати**
CRL:	Certificate Revocation List	**РПС**	**Регистар на поништени сертификати**
OID:	Object Identifier	**ИО**	**Идентификатор на објекти**
TSA:	Time-Stamping Authority	**Издавач**	**Издавач на временски печати**
TSP:	Time-Stamping Policy	**Политика**	**Политика на издавачот на временски печати**
TSS:	Time-Stamping Service	**Услуги на Издавачот**	**Услуги на издавачот на временски печати**
TST:	Time-Stamp Token	**/**	**Временски печат**
TSU:	Time-Stamping Unit	**УГВП**	**Уред за генерирање на временски печат**

4. Општи одредби

4.1. Услуги на издавачот на временски печати

Информатичко-комуникациската инфраструктура на КИБС Моментум за издавање и управување со временските печати се состои од две компоненти:

- Издавање на временски печати – Услуга за генерирање на временски печати
- Управување со временските печати – Управување, надгледување и контрола на оперативноста на издавањето на временски печати. Со оваа услуга, меѓу другото се обезбедува часовникот кој се користи за временските печати да е прецизно синхронизиран со Координираното универзално време (UTC).

4.2. Издавач на временски печати

Институцијата на која и веруваат корисниците на услугите за издавање на временски печати (претплатниците и засегнатите страни) се вика Издавач на временски печати. Издавачот има обврска за издавање на временски печати преку услугата дефинирана во Глава 4.1. Издавачот исто така има обврска да управува и користи еден или повеќе Уреди за генерирање на временски печати, кои се идентификувани како во описот наведен во Глава 7.3.1.

4.3. Претплатници

Претплатник може да биде правно или физичко лице.

Обврските за правното лице, се пренесуваат на корисниците на услугата кои се вработени кај правното лице. Во било кој случај, правното лице ќе биде одговорно ако обврските од страна на тие корисници не се исполнети и соодветно на тоа, се очекува правното лице да ги информира нив.

Кога претплатникот е физичко лице, тоа ќе биде директно одговорно ако неговите обврски не се целосно исполнети.

4.4. Општи одредби и политики

Оваа политика е дел од Правилата на КИБС за квалификувани сертификати, кои ја регулираат работата на КИБС Моментум и придружните сервиси.

Издавачот издава временски печати на сите заинтересирани страни без технички ограничувања. За издавањето на временските печати се плаќа надоместок дефиниран во тарифата на КИБС АД Скопје, објавена на веб страната http://www.kibstrust.mk.

4.4.1. Цел

Овој документ е јавно објавен. Дистрибуцијата на овој документ е ограничена според Правилата на КИБС за квалификувани сертификати, Глава 9.5 Права на интелектуална сопственост.

Персоналот и физичката безбедност се исто така опишани во Правилата на КИБС за квалификувани сертификати.

4.4.2. Ниво на специфичност

Овој документ ги опишува општите правила за издавање и управување со временските печати. Детален опис на системот е даден во дополнителната документација којашто не е јавна. Документите кои не се јавни, заедно со извештаите, резултатите од внатрешните ревизии и

останатата документација за типот на опремата која се користи, се достапни само на авторизиран персонал и на надворешните ревизори на системот на КИБС.

4.4.3. Приод

Оваа политика е општ документ и не содржи технички детали за информатичко комуникацискиот систем, структурата на организацијата, оперативните процедури или техничката заштита. Оваа политика исто така не ја дефинира околината во која работи системот за издавање на временски печати. Техничките и оперативните детали се вклучени во Правилата на КИБС за квалификувани сертификати и други документи.

5. Политика за издавање на временски печати

5.1. Преглед

Политиката е „множество на правила кои укажуваат на применливоста на временскиот печати на одредена заедница и/или класа на апликации со заеднички сигурносни барања“ (Глава 3.1 и Глава 4.4).

Временските печати се издаваат со точност од 1 секунда или подобро.

За да можат да ја проверат валидноста на временските печати по истекот на важноста на сертификатот на Издавачот, засегнатите страни треба да преземат одредени мерки дефинирани во Анексот на оваа политика.

Профилот на јавниот клуч на сертификатот, кој се користи кај Издавачот е усогласен со IETF[4] препораките. Сертификатите во уредите за генерирање на временски печати на Издавачот издадени се од DigiCert, Inc, 2600 West Executive Parkway, Suite 500, Lehi, UT 84043, USA . Нивната спецификација е опишана во документите сместени во складот на издавачот на сертификати DigiCert (https://www.digicert.com/ssl-cps-repository.htm). Профилот на основните полиња на сертификатот за временски печати е даден во следната табела:

Поле	Вредност
Верзија	3
Сериски број	0d 77 17 79 73 2f 19 c9 d2 ab 9e 94 7e 53 da c9
Потпис	RSA/SHA-256
DN на издавачот	CN = DigiCert SHA2 Assured ID Timestamping CA OU = www.digicert.com O = DigiCert Inc C = US
Валидност	Од 05.10.2016, до 05.11.2021
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

Издавачот КИБС Моментум издава временски печати во согласност со ETSI TS 101 861[5] препораките. Секој временски печат ја содржи идентификацијата на политиката, опишана во Глава 5.2 на овој документ.

[4] IETF RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), August 2001
[5] ETSI TS 101 861 Time stamping profile V1.4.1, July 2011

5.2. Идентификација на Издавачот на временски печати

Оваа Политика е идентификувана, во рамките на документацијата на КИБС со својот единствен идентификациски број (OID): 1.3.6.1.4.1.16305.1.2.3

Овој OID е произлезен на следниот начин:

1.3.6.1.4.1.16305	Број на КИБС регистриран во IANA
1.3.6.1.4.1.16305.1	Гранка за објекти поврзани со PKI-X.509
1.3.6.1.4.1.16305.1.2	Гранка за политики и правилници
1.3.6.1.4.1.16305.1.2.3	Политика на издавачот на временски печати

Единствениот идентификатор (OID) упатува кон временскиот печат кој е во склад со оваа Политика. Таа вредност е вклучена во полето „Policy“ на временскиот печат. Исто така постојат и други значајни елементи (име, верзија, датум на промена) кои можат да ја идентификуваат Политиката.

5.3. Област на применливост

Оваа Политика е насочена кон задоволување на барањата за издавање на временски печати за архивирање (Long Term Validity) на потпишани документи со квалификувани дигитални сертификати, како што е дефинирано во ETSI 101 733, но генерално е применлива за било која друга намена со еквивалентни барања.

Оваа Политика може да се користи за затворени корпорациски системи или за јавни услуги за издавање на временски печати, како што се електронски трансакции, архивирани податоци или формулари.

5.4. Усогласеност

Издадените временски печати содржат идентификатор опишан во Глава 5.2 на овој документ. Издавачот ги поддржува само барањата кои имаат временски печати од оваа политика.

Издавачот гарантира исполнување на обврските дефинирани во Глава 6.1 и имплементираните контроли опишани во Глава 7 на овој документ.

6. Обврски и одговорности

6.1. Обврски на Издавачот

6.1.1. Општо

Издавачот ги исполнува барањата и процедурите дефинирани во Глава 7 на овој документ.

Издавачот ги исполнува сите обврски во согласност со неговите дефинирани услови за користење на услугите.

Издавачот обезбедува технички услови за издавање на временски печати.

Издавачот гарантира дека се применуваат Правилата на КИБС за квалификувани сертификати и дека се задоволени специфицираните барања во тековната Политика.

6.1.2. Обврски на Издавачот кон претплатниците

КИБС гарантира перманентен пристап до услугата КИБС Моментум секој ден 24/7 со исклучок на планирани технички прекини, дефинирани во други документи за одржување на опремата и инфраструктурата. Времето кое се става во временските печати е со прецизност подобра од една секунда во однос на Координираното универзално време (UTC). КИБС гарантира дека:

- Неговите активности и услуги се легални и не кршат интелектуални права, лиценци и останати права
- Издадените временски печати не содржат неточни податоци или грешки.

Останатите информации кои го дефинираат КИБС Моментум се опишани во Правилата на КИБС за квалификувани сертификати.

6.2. Обврски на претплатниците

При барање за издавање на временски печат, претплатникот треба да ја провери валидноста на сертификатот од уредот, преку кој се добиваат временски печати со проверка на CRL листата на DigiCert (http://crl3.digicert.com/sha2-assured-ts.cr и http://crl4.digicert.com/sha2-assured-ts.crl) и дали приватниот клуч на сертификатот за издавање на временски печати е компромитиран.

Оваа Политика не бара врска помеѓу hash податокот на кој треба да се стави временски печат и содржината на оригиналните електронски податоци од кои е добиен hash-от. Претплатникот е единствено одговорен за таа врска.

6.3. Обврски на засегнатата страна

Засегнатата страна мора да провери дека:

- временскиот печат е коректно потпишан со сертификат од уредот за временски печати. За таа цел, мора да се провери дали временските печати вклучуваат референца кон уред на КИБС
- во времето на верификација, сертификатот не е поништен. За таа цел тие мора да се проверат јавните CRL листи објавени од DigiCert (http://crl3.digicert.com/sha2-assured-ts.cr и http://crl4.digicert.com/sha2-assured-ts.crl)
- Криптографската hash функција која се користи во процесот на барање на временски печат е сеуште доволно сигурна
- Големината на клучот на сертификатот на Издавачот и останатите криптографски алгоритми се сеуште сигурни.

Ако верификацијата на временските печати се прави по истекот на важноста на соодветниот сертификат на Издавачот, засегнатите страни треба да ги следат препораките дефинирани во Анексот на овој документ.

Засегнатите страни треба да ги земат во предвид ограничувањата опишани во Политиката.

6.4. Одговорност

Одговорноста на секој субјект поврзан со услугата за издавање на временски печати е специфицирана во меѓусебен договор. Сите останати одговорности се опишани во Правилата на КИБС за квалификувани сертификати.

7. Барања што треба да ги исполни Издававачот

Издавачот имплементира контроли со кои се обезбедува издавање или неотповикливост на услугите дефинирани во регулативата на оваа политика. За надгледување на оперативноста на

услугата за издавање на временски печати, како и за надгледување на активностите на персоналот и корисниците во информатичкиот систем се водат дневници на настани.

Потребно е секоја страна којашто е на некој начин поврзана со процедурите за временски печат, да води записи за своите активности. Записите за овие информации треба да бидат дел од соодветен дневник на настани и треба да се чуваат на начин со кој ќе се обезбеди адекватен пристап на сите засегнат страни во процесот. На тој начин правилно и точно ќе се обезбеди информирање на засегнатите страни за разрешување на евентуални спорови или пропусти во безбедноста на информатичко комуникациските системи. Тие записи треба редовно да се вклучат во процесот за изработка на резервни копии. Процедурата за изработка на резервни копии е интерна процедура на КИБС.

7.1. Правила за работа и информации за неоддавање

7.1.1. Правила за работа

Издавачот гарантира дека има капацитет за обезбедување на услуги за издавање на временски печати на начин опишан во политиката.

Издавачот извршува анализа на ризици заради проценка на заканите на средствата, со цел определување на соодветни потребни контроли и оперативни процедури.

Издавачот воспоставува процедури за имплементирање на правилата за работа идентификувани во оваа Политика.

Издавачот јавно ги објавува соодветните документи за да корисниците и засегнатите страни можат да ја проценат усогласеноста на своите активности со Политиката.

Издавачот воспоставува соодветна организациска структура за одобрување и верификација на Политиката.

Одговорните лица на Издавачот се грижат за правилната имплементација на правилата за работа.

Издавачот дефинира процедури за периодична контрола, за да се провери примената и усогласеноста на правилата за работа со Политиката.

Издавачот е управуван од страна на раководството на Издавачот. Раководството на Издавачот ја донесува Политиката и документите поврзани со услугите на Издавачот, кои ги обезбедува Издавачот. Раководството на Издавачот е одговорно за:

- Специфицирање и одобрување на инфраструктурата и работењето на услугата на Издавачот;
- Одобрување на Политиката;
- Ажурноста на Политиката од аспект на функционални, организациски и технички барања;
- Усогласеноста при имплементација на уредите за генерирање на временски печат со Политиката на Издавачот;
- Објавување на Политиката на Издавачот, како и соодветните ревизии на документите кон корисниците и засегнатите страни.

7.1.2. Јавно објавени информации дефинирани во Политиката

Политиката на Издавачот и Правилата на КИБС за квалификувани сертификати се јавно објавени документи.

Информациите за контактите поврзани со содржината на овој документ се наведени во Правилата на КИБС за квалификувани сертификати, Глава 1.5.

Секој временски печат издаден од КИБС Моментум вклучува идентификатор на политиката, дефиниран во Глава 5.2 на овој документ.

Криптографските Hash функции, користени во процесот на издавање на временски печати се во согласност со нормативните референци на NIST[6].

Валидноста на временскиот печат е 6 години од моментот на престанок на важност на соодветниот сертификат, сметајќи дека условите опишани во Глава 6.3 на овој документ се исполнети.

Прецизноста на часовникот во временските печати е синхронизирано со универзалното време (UTC) со точност до една секунда.

Ограничувањата поврзани со системот на Издавачот се дефинирани во Глава 5.3 на оваа политика.

Обврските на претплатниците се опишани во Глава 6.2, додека на засегнатите страни во Глава 6.3 на оваа политика.

Верификацијата на временските печати треба да се изврши според упатствата за користење на софтверите поврзани со работата на издавањето на временски печати и Анексот на политиката.

Дневникот на настани се чува во период дефиниран во Правилата на КИБС за квалификувани сертификати.

Овој документ е регулиран согласно македонските закони и регулативата на ЕУ. Во случај на спор помеѓу страните кој резултира од толкување, барање и/или извршување на меѓусебен договор, а во отсуство на заемен договор меѓу двете страни, единствен надлежен суд е судот во Скопје.

Ограничувањата од одговорност се опишани во Глава 6.4.

Сите сугестии, поплаки и забелешки во врска со функционирањето на КИБС Моментум треба да бидат адресирани до контактите опишани во Глава 1.5 на Правилата на КИБС за квалификувани сертификати.

КИБС прави резервни копии на податоци и критични функции надвор од примарната локација со цел исполнување на обврските за обезбедување на континуитет после настанат инцидент. КИБС се грижи за изнесување на резервните копии надвор од примарната локација и нивна заштита во поглед на доверливост и интегритет.

7.2. Управување со животниот циклус на клучевите

7.2.1. Генерирање на клуч

КИБС гарантира дека сите криптографски клучеви се генерирани во контролирана средина.

Генерирањето на криптографски клучеви на уредот за генерирање на временски печат се извршува од страна на овластен персонал во хардверски безбедносни модули (HSM) сертифицирани FIPS 140-1 Level 3.

Уредите за генерирање на временски печат користат RSA приватни клучеви со должина од 2048 bits.

[6] National Institute of Standards and Technology, http://www.nist.gov/

7.2.2. Заштита на приватниот клуч

КИБС гарантира дека приватните клучеви на уредите за генерирање на временски печати се чуваат тајно и гарантира нивен интегритет.

Клучевите се чуваат во хардверски безбедносни модули (HSM) сертифицирани FIPS 140-1 Level 3.

Приватните клучеви на уредите за генерирање на временските печати не можат да се извезуваат надвор од овие модули.

КИБС забранува архивирање и изработка на резервна копија од приватните клучеви од уредите за генерирање на временски печати.

7.2.3. Дистрибуција на јавниот клуч

Сертификатите за временски печати, заедно со соодветните јавни клучеви се објавени на веб страната http://www.kibstrust.mk.

Барањето за сертификат од уредите за генерирање на временски печат се праќа до Издавачот на сертификати DigiCert, во согласност со правилата дефинирани во соодветната Политика на издавачот на сертификати.

Сертификатите добиени од издавачот на сертификати се во согласност со профилот дефиниран во политиката за сертификати.

Издавачот се придржува до неговите обврски дефинирани во Политиката на издавачот на сертификати.

Издавачот при импортирање на сертификатот во уредот за генерирање на временски печат проверува дека истиот е издаден од DigiCert.

7.2.4. Нови клучеви за Издавачот

КИБС гарантира дека животниот век на сертификатите во уредите за генерирање на временски печати нема да биде поголем од периодот во кој криптографските алгоритми и должината на клучевите е дозволено да се прикладни за намената.

Издавачот генерира нови клучеви по истекот на важноста на сертификатот на Издавачот. Клучевите на сертификатите со истечена важност се чуваат во период од 5 години. Потоа тие се уништуваат. Јавните клучеви на Издавачот се чуваат дополнителни 20 години за да може да се извршува верификација на временските печати издадени во минатото.

7.2.5. Уништување на приватните клучеви

Издавачот гарантира дека приватните клучеви за потпишување во уредите за генерирање на временски печати нема да се користат по завршувањето на нивното времетраење.

КИБС гарантира дека приватните клучеви на уредот за издавање на временски печати се уништуваат по завршување на периодот на нивното чување.

Системот за издавање на временски печати КИБС Моментум ќе го одбие било кое барање поврзано со употребата на клучевите со истечено времетрање.

7.2.6. Управување со хардверските безбедносни модули (HSM)

Издавачот ја гарантира безбедноста на криптографскиот хардвер во текот на неговиот животен век.

HSM уредите наменети за клучевите за временски печат се доставуваат и чуваат во КИБС, во строго контролирана околина. КИБС гарантира дека уредите не се отварани во текот на транспортот, ниту дека се манипулирани додека се чуваат во склад.

Инсталацијата и иницијализацијата на овие уреди се извршува од доверлив персонал, во присуство на сведок, во физички обезбедена околина (Глава 7.4.4).

Во случај на замена на уред или трансфер на уред заради сервисирање, клучевите се бришат и уништуваат во согласност со препораките на производителот.

КИБС гарантира дека бројот на активни уреди во било кое време е доволен за обезбедување на надежна услуга.

7.3. Временски печати

7.3.1. Карактеристики на временскиот печат

Издавачот гарантира дека временските печати се генерирани безбедно и го вклучуваат точното време.

Секој временски печат издаден од КИБС Моментум има свој единствен идентификатор и го вклучува идентификаторот на политиката.

Временските печат имаат запис за датум и време поврзано со UTC референтното време, додека времето кое што го користи КИБС Моментум е обезбедено од временските сервери ntp.kibs.mk и time.kibs.mk (сателитско време и атомски часовник). Времето е синхронизирано со Координираното универзално време (UTC) со точност дефинирана во овој документ.

Во случај на загрозување, реално или претпоставено, или губење на калибрацијата на уредот за генерирање на временски печати, кое би можело да влијае на генерираниот временски печат, КИБС ќе ги преземе сите потребни мерки уредите да не генерираат нови временски печати додека не се воспостави нормална состојба.

КИБС издава временски печати во согласност со документот RFC 3161. Временски печат е електронски потпишана потврда од страна на Издавачот, за одредена содржина на податоци во точно одредено време и датум. Со временскиот печат се потврдува дека одреден податок постои во одредено време. За таа намена, временскиот печат еднозначно ги поврзува претставата на податокот (т.е. неговата hash вредност заедно со идентификатор на hash алгоритамот) со одреденото време. Содржината на временските печати е потпишана со сертификат базиран на 2048 битен RSA приватен клуч, кој има профил и екстензии дефинирани во Глава 5.1 на овој документ.

Временскиот печат е потпишана структура која вклучува:

- Hash вредност на податокот на кој е ставен временски печат
- Датум и Координирано универзално време (UTC)
- Идентификатор на Издавачот КИБС Моментум и идентификатор на сертификатот

7.3.2. Синхронизација на часовникот со UTC

Системот за временска синхронизација за услугите за временски печати на КИБС Моментум, му гарантира на претплатникот испорака на временски печат со временска отстапка помала од 1 (една) секунда во однос на Координираното универзално време (UTC), и тоа:

- Калибрацијата на времето кај уредите за генерирање на временски печати се одржува на тој начин да времето не отстапува повеќе од декларираната точност;

- Времето во уредите е заштитено од закани поврзани со околината кои можат да доведат до десинхронизација во однос на UTC, надвор од декларираната точност;
- КИБС гарантира дека отстапувањата на интерното време кај уредите надвор од декларираните рамки ќе биде веднаш забележано. КИБС ќе се погрижи информациите за отстапувањата да бидат достапни на веб страница http://www.kibstrust.mk.
- Ако времето на некој од уредите за генерирање на временски печати е надвор од дозволените граници, тогаш нема да се генерираат временски печати.

Часовниците на уредите за генерирање на временски печати се локално мониторирани од референтни сервери за точно време во КИБС. Овие сервери се автономни и синхронизирани со UTC референтното време. Механизмите кои се применуваат му овозможуваат на системот заштита од напади чија цел е десинхронизација на изворот на време, дури и од напади врз радио или сателитски сигнали.

КИБС гарантира дека ќе се одржува синхронизацијата на времето кога ќе се појави престапна секунда, нотифицирано од релевантно тело. Промената за престапната секунда ќе се направи во последната минута од денот на примена на истата. Записот за тој настан (во рамките на декларираната точност) ќе биде направен по настанувањето на промената.

7.4. Контрола и управување на системот на Издавачот

7.4.1. Безбедносни контроли

Издавачот има имплементирано административни и оперативни процедури кои соодветствуваат на најдобрите практики во соодветната област. Сите субјекти поврзани со безбедносните контроли се опишани во Глава 5.2 од Правилата на КИБС за квалификувани сертификати.

7.4.2. Управување и класификација на средствата

Издавачот има имплементирано процедури за соодветна заштита на информациите и средствата за работа.

Издавачот одржува точен попис на сите средства и има имплементирано процедури за класификација на средствата во согласност со интерните процедури на КИБС АД Скопје за анализа на ризици.

7.4.3. Контрола на персонал

Карактеристиките на персоналот, како и доверливоста на улогите кои ги извршуваат се опишани во Глава 5.3 од Правилата на КИБС за квалификувани сертификати.

7.4.4. Просторна контрола и контрола на условите за работа

Описот на контролите за физичкиот простор и на условите за работа се опишани во Глава 5 од Правилата на КИБС за квалификувани сертификати. Овие безбедносни контроли соодвествуваат со нормативните барања на стандардот ISO 27001.

7.4.5. Контрола на оперативното работење

Издавачот гарантира дека компонентите на системот за издавање на временски печати се безбедни и дека со нив точно и прецизно се управува, со минимален ризик од испад. КИБС АД Скопје има безбедносни процедури кои се дел од интерната документација на компанијата. На таа документација периодично и се извршува контрола од страна на внатрешни и надворешни ревизори.

7.4.6. Управување со пристапот

Контролите за идентификација и автентикација се дефинирани во согласност со примената на политиката за контрола на пристап и одговорноста во работењето.

Услугите на Издавачот се поставени на систем заштитен со мрежни бариери (firewalls). Овие уреди се конфигурирани да ги прифаќаат исклучиво потребните поврзувања.

КИБС се грижи процедурите за безбедност да се издвоени од стандардните процедури за оперативна работа и тие секогаш да се извршуваат под надзор на вработен со доверлива улога.

Профилите и правата на пристап до опремата на Издавачот се назначени и документирани заедно со процедурите за пријава/одјава на операторите.

Применети се контроли на безбедност за заштита од неовластен пристап до локалните компоненти на информациониот систем.

Системите, апликациите и базите на податоци еднозначно вршат идентификација и автентикација на операторите и администраторите. Интеракција меѓу системот и оператер е возможна само откако ќе се изврши успешна идентификација и автентикација. За секоја интеракција, системот го проверува идентитетот на операторот.

Информациите за автентикација се чуваат така што само овластените корисници имаат пристап до нив.

Лице кое не е овластен корисник не може да доделува или одзема права на пристап до објекти. Исто така, само овластени корисници може да креираат нови корисници, да оневозможуваат или исклучуваат постојни корисници.

Издавачот води дневник на зписи кој содржи записи поврзани со следниве настани:

- Генерирање на временски печати;
- Администрирање на системот за издавање на временски печати;
- Синхронизација и одржување на точното време;

Секој запис во дневникот содржи датум и време на настанот.

Доверливоста на дневникот на записи е обезбедена преку соодветни физички мерки, како и преку дефинирани системски и мрежни контроли за пристап.

Физичкиот пристап до компонентите на информатичкиот систем е дефиниран во Глава 5.1.2 од Правилата на КИБС за квалификувани сертификати.

7.4.7. Управување и одржување на доверливите системи

Услугите на Издавачот се поставени на доверливи компоненти кои се заштитени од надворешни модификации. Конкретно, уредите за генерирање временски печат ги задоволуваат регулаторните барања.

Анализа на ризици се спроведува на услугите на Издавачот за да се одредат можни закани за уредите за генерирање временски печат. Поставените контроли се во согласност со стратегијата на КИБС за управување со ризици за информационите системи.

Инфраструктурите за развој и тестирање се издвоени од продукциската инфраструктура на услугите на Издавачот.

Критериумите за прифаќање и проверување на нови системи, надградби и нови верзии се документирани, а за истите се извршува потребното тестирање пред нивно прифаќање и ставање во продукција.

7.4.8. Загрозување на услугите на Издавачот

Во случај на настани кои влијаат на безбедноста на услугите на Издавачот и кои би можеле да влијаат на генерираните временски печати, КИБС гарантира дека соодветна информација ќе биде достапна на претплатниците и засегнатите страни.

Загрозувањето на Издавачот може да е причинето од:

- Загрозување на приватните клучеви на уредите за генерирање на временски печати
- Загрозување на приватниот клуч на издавачот на сертификати кој се користи при генерирање на сертификатите за уредите за генерирање на временски печати
- Оперативен проблем

Потенцијалното загрозување на услугите на Издавачот е земено во предвид во Планот за оправување од катастрофа на КИБС.

Планот за опоравување од катастрофа ги опишува реалните или претпоставени загрозувања на приватниот клуч за потпишување на уредот за генерирање на временски печати, или губењето на калибрацијата на времето на уредот за генерирање на временски печати, што може да влијае на издадените временски печати.

КИБС гарантира дека се преземени сите неопходни мерки со цел да се избегнат оперативни инциденти.

КИБС постојано го ажурира Планот за опоравување од катастрофа со цел да обезбеди најдобра можна заштита од следните закани:

- Загрозување на приватниот клуч;
- Испади на мрежата;
- Недостапност на квалификуван кадар;
- Проблеми со калибрацијата на времето;
- Испади на хардверските компоненти.

Генерално, инцидентите кај услугите на издавачот на временски печати ќе се решаваат според процедурата за пријавување и справување со сигурносни инциденти која е на сила во КИБС.

Во случај на загрозување, реално или претпоставено, или губење на калибрацијата на уредот за генерирање на временски печати, кое би можело да влијае на генерираниот временски печат, КИБС ќе обезбеди соодветна информација достапна на претплатниците и засегнатите страни.

Во случај на загрозување на операциите на КИБС или губење на калибрацијата што би можело да влијае на издадените временски печати, КИБС за своите претплатници и засегнати страни ќе обезбеди информации кои може да се искористат за идентификување на евентуално засегнатите временски печати, освен во ситуации кога ова ја нарушува безбедноста на услугите на издавачот на временски печати.

7.4.9. Крај на работењето на Издавачот

Процедурите за управување со крајот на работењето се дефинирани од страна на КИБС. Преку овие процедури, КИБС обезбедува дека во случај на прекин на услугите на Издавачот, потенцијалните нарушувања за претплатниците и засегнатите страни ќе бидат минимизирани. Попрецизно, КИБС гарантира дека ќе ги обезбеди сите информации за да ја верификува исправноста на временските печати, дури и по прекинот на услугите на Издавачот.

Пред прекинување со услугите на Издавачот, ќе бидат превземени следните активности:

- КИБС ќе ги извести сите свои претплатници и засегнати страни за очекуваниот прекин со објавување на информација на својата веб страна

- КИБС ќе ги повлече сите овластувања на своите партнери со кои тие можат да делуваат во негово име за било која функција поврзана со издавањето на временски печати
- КИБС ќе ги пренесе задолженијата на соодветното надлежно тело со цел во разумен временски период да се сочува евиденцијата на настани и ревизорските архиви кои се потребни за да се потврди правилното работење на Издавачот
- КИБС ќе ја задржи обврската да овозможи достапност на јавните клучеви и сертификати кон засегнатите страни во разумен временски период
- Приватните клучеви на уредот за генерирање на временски печати ќе бидат неповратно уништени, согласно со процедурата опишана во Глава 7.2.5

КИБС ги превзема сите потребни мерки за да ги покрие трошоците за исполнување на минимумот од барања во случај на банкрот, или доколку од други причини не е во состојба самостојно да ги покрие трошоците.

Одредбите за прекинување на услугите вклучуваат:

- Известување до претплатниците и другите засегнати страни
- Трансфер на обврските на КИБС кон други надлежни тела

Издавачот ќе ги поништи сите сертификати на уредите за генерирање на временски печати.

7.4.10. Усогласеност со правната рамка

Издавачот работи во согласност со регулативите на позитивните законски прописи во Република Македонија.

Претплатниците се информирани дека личните податоци кои ги даваат на КИБС, може да бидат пренесени и процесирани од КИБС и неговите партнери вклучени во процесот.

КИБС ги презема сите потребни мерки за да ги чува личните податоци сигурно и доверливо, согласно Законот за заштита на лични податоци. Од вработените во КИБС се бара да ги почитуваат актите на Законот за заштита на лични податоци.

Вработените немаат право да соберат или да користат на несоодветен начин лични податоци до кои имаат пристап и општо земено, да дејствуваат на начин кој најверојатно ќе биде штетен за приватниот живот или личната репутација на сопственикот на податоците.

КИБС е должен доверливо да ги чува информациите обезбедени од страна на претплатниците, освен ако нивното прикажување е одобрено од страна на Претплатникот или дозволено со закон.

7.4.11. Дневник на записи кај Издавачот

Надгледување на работењето на Издавачот е овозможено преку преглед на евидентираните настани, конкретно за обезбедување на докази за правни дејства. Секој настан е запишан во база на податоци од која може да се следат сите настани за услугата, вклучувајќи ги и инцидентите. Доколку се случи инцидент, КИБС ќе постапи на соодветен начин со цел брзо да интервенира, да го ограничи влијанието на инцидентот на безбедноста и да го обнови сервисот во најбрзо можно време.

Специфичните записите од системот на Издавачот се посебно документирани.

Издавачот ги гарантира интегритетот и доверливоста на тековните и архивираните записи во врска со работењето на услугата.

Записите во врска со работењето на Издавачот ќе бидат целосно и доверливо архивирани според интерни процедури на КИБС АД Скопје. Сите медиуми со доверливи информации за услугите на Издавачот се вклучени во процедурите за одржување со цел обезбедување на

достапност на функциите и информациите. Расходувањето на опремата е документирано за да се обезбеди неоткривање на доверливите информации кои може да ги содржи истата.

Записите во врска со работењето на Издавачот ќе бидат објавени ако има потреба за обезбедување на доказ наменет за правни дејства во врска со одредена активност со услугата на Издавачот.

Точното време на значајните настани поврзани со управувањето со клучевите или синхронизацијата на часовниците ќе бидат запишано.

Записите за услугата за издавање на временски печати ќе се чуваат доволно долг период по истекот на валидноста на клучевите, соодветен за обезбедување на правен доказ и опишан во Јавно објавените информации дефинирани во Политиката, Глава 7.1.2.

Начинот на чување на записите не овозможува едноставно уништување и бришење.

Сите информации поврзани со претпланиците доверливо ќе се чуваат, освен во случај ако тоа договорно не е овозможено тие податоци да се користат за поширок аудиториум.

Сите записи во врска со животниот циклус на клучевите и сертификатите се посебно документирани.

Сите записи поврзани со синхронизацијата или рекалибрацијата на часовниците, како и загубата на синхронизација се посебно документирани.

7.5. Организациска шема

КИБС Моментум е дел од КИБС АД Скопје.

Организацијата е со седиште во Република Македонија.

КИБС ја има документирано безбедноста на информациите за човечките ресурси. Вработените во КИБС, на кои им е доделена доверлива улога внимателно се избираат и јасно се информираат за работата и правилата кои треба да ги следат.

Лицата на кои им е доделена доверлива улога, се обврзале за заштита на доверливоста при нивната работа. КИБС гарантира дека професионалните вештини на вработените со доверлива улога се во согласност со потребните квалификации за нивните функции. Раководството на КИБС поседува соодветна стручност и познавање на процедурите за безбедност. Секое лице со доверлива улога е информирано за неговите одговорности преку описот на неговата работа и/или процедурите поврзани со безбедноста на системот и контролата на вработени.

Вработените кои работат со услугите на Издавачот имаат соодветни познавања од:

- технологијата на временски печат
- технологијата на електронски потпис
- механизмите за нагодување или синхронизација на часовниците на уредот за генерирање временски печат со Универзалното координирано време
- процедурите за безбедност, за вработените одговорни за безбедноста
- безбедност на информациите и процена на ризиците

Барањата во поглед на под-изведувачи се регулираат со договори.

Обврските вклучуваат договори за обезбедување услуга и доверливост на информации.

Вработените се информираат за безбедносните правила поврзани со нивната улога веднаш по нивното пропишување. На лицата кои работат за услугите на Издавачот и имаат оперативна улога им се доставуваат процедурите поврзани со нивната работа.

Анекс: Долгорочна верификација на временски печат

Вообичаено, временскиот печат не може да се верификува по истекот на периодот на важност на сертификатот од уредите за генерирање на временски печати. Сепак, верификацијата на временскиот печат може да се изврши и покрај овие ограничувања на сертификатите во уредите за генерирање на временски печат, ако во времето на верификација може да се знае дека:

- приватниот клуч во уредот не е компромитиран во било кое време се до моментот кога засегнатата страна бара верификација на печатот
- Hash алгоритмите кои се користени за генерирање на временскиот печат се сеуште дозволени во времето на верификација
- Алгоритмите за потпишување и големината на клучевите на сертификатите кога е потпишан временскиот печат се сеуште отпорни на криптографски напади во времето на верификација

Ако овие услови не можат да се одржат, тогаш валидноста може да се продолжи преку додавање на дополнителен временски печат за да се заштити интегритетот на претходниот. Алтернативно, податоците кои временски се потпишуваат може да се складираат на безбедно место.

Како дополнување на овој процес се записите кои ги води КИБС Моментум за hash (хеш) вредностите кои временски се потпишуваат и со тоа може да се обезбеди доказ за постоењето на податокот пред точно определеното време. Оваа техника, се нарекува „Временско-маркирање“ и претставува важна алтернатива за долгорочна верификација на дигиталните потписи.

***