ПОЛИТИКА ЗА ИЗДАВАЊЕ НА ВРЕМЕНСКИ ЖИГ(TS) НА МАКЕДОНСКИ ТЕЛЕКОМ TSA

Јавен дел од правилата дефинирани од страна на Македонски Телеком АД – Скопје како давател на доверливи услуги за временски жиг Македонски Телеком TSA

Јавен дел од правилата дефинирани од страна на Македонски Телеком АД – Скопје како издавач на временски жиг.

Идентификационен бр.	POL 009
Верзија Бр.	4.0
Одговорна организациска единица	Оперативна служба на Македонски Телеком TSA

Извршен преглед

Верзија	Датум	Краток опис на промените
4.0	Септември 2024	Издавање на нов сертификат за Временски жиг. Промена на терминологијата во документот на македонски јазик, согласно законската регулатива.

Историјат*

Верзија	Датум	Подготвено од:	Краток опис на промените
3.0	Ноември 2022	Оперативна служба на Македонски Телеком TSA	Издавање на нов сертификат за Временски жиг
2.0	Ноември 2020	Оперативна служба на Македонски Телеком TSA	Согласно барањата од Законот за електронски документи, електронска идентификација и доверливи услуги
1.0	Јули 2017	Оперативна служба на Македонски Телеком TSA	Согласно барањата на стандардот ETSI TS 102 023 V1.2.2 (2008-10) Electronic Signatures and Infrastucrture (ESI); Policy requirements for time-stamping authorities изработена е Политиката за издавање на временски жиг (TS) на Македонски Телеком АД Скопје како Time Stamp Authority (TSA). Истата во целост ги задоволува барањата на стандардот и преставува потврда за целесообразноста на барањата со решението.

Содржина

1. Македонски Телеком TSA – Давател на доверлива услуга за временски жиг

Македонски Телеком АД - Скопје нуди услуга, издавање на временски жиг, како Давател на доверлива услуга за временски жигови Македонски Телеком TSA кој што функционира во рамките на Македонски Телеком CA како давател на доверливи услуги за дигитални сертификати.

Временскиот жиг е наменет за потврда на содржината и веродостојноста на податоци во електронска форма во конкретен момент.

Со овој документ се определуваат правилата на работењето на Македонски Телеком TSA како давател на доверливи услуги за временски жиг. Сите услуги, издадени временски жигови на издавачот Македонски Телеком TSA се обработуваат согласно истите.

Известувањата, упатствата, правилата и другите важни документи за користење на услугите на Давателот за доверливи услуги за временски жиг Македонски Телеком TSA се објавени на веб-страната на издавачот https://timestamp.telekom.mk.

Правилата се изработени во согласност со меѓународните стандарди и тоа:

- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles;
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps како и
- RFC 3161 - Time-Stamp Protocol (TSP).

2. Вовед

Политиката го претставува јавниот дел на правилата на Македонски Телеком TSA како давател на доверлива услуга на временски жиг дефинирани од страна на Македонски Телеком АД - Скопје. Истите се однесуваат на системот за издавање на временски жиг и ја одредуваат целта, работата и методологијата на управување со издавањето на временски жиг, одговорноста на издавачот, како и предусловите кои мораат да бидат исполнети од страна корисниците и трети лица кои користат временски жиг.

Македонски Телеком TSA како Давател на доверлива услуга за временски жиг, издава временски жиг, за кој што важи највисокот степен на заштита и функционираат согласно важечките законски прописи и препораките од меѓународните стандарди.

Временскиот жиг е наменет за:

- верификација на содржината на документ во одреден временски период,
- докажување на временските карактеристики на документите, трансакциите и други услуги,
- други потреби каде што е потребена потврда во единица време.

Давателот на доверлива услуга за временски жиг, Македонски Телеком TSA https://timestamp.telekom.mk, функционира во рамките на Македонски Телеком CA како давател на доверливи услуги за дигитални сертификати.

Оваа политика го одредува работењето на Македонски Телеком АД - Скопје како Давател на доверлив услуга за временски жиги, Македонски Телеком TSA, за издавање временски жигови за потребите на било кое правно или физичко лице.

Македонски Телеком TSA издава временски жигови со точност помала од една (1) секунда во однос на Координираното универзално време (UTC-CoordinatedUniversalTime).

3. Значење на кратенките и изразите

3.1 Кратенки

CA	Физичко или правно лице кое издава дигитални сертификати или врши други услуги во врска со сертифицирање или електронски потписи, англ. Certification Authority.
CPName	Име на политиката на работењето на издавачот (англ. Certification Policy Name), поврзано со меѓународниот број на политиката на работа (спореди ја скратеницата CPOID).
CPOID	Меѓународен број кој еднолично ја определува политиката на работата согласно меѓународниот стандард ITU-T препораките од X.208 (ASN.1), англ. Certification Policy Object Identifier.
ETSI	Меѓународни препораки од областа на телекомуникациите, англ. European Telecommunications Standards Institut, http://www.etsi.org.
GPS	Сателитски систем за одредување на положбата, англ. Global Positioning System.
NTP	Протокол за синхронизација на времето, англ. Network Time Protocol,
PKI	Инфраструктура на јавните клчеви, англ. Public Key Infrastructure.
RFC	Меѓународни препораки за Интернет групата IETF, англ. Internet Engineering Task Force и IESG, англ. Internet Engineering Steering Group , англ. Request for Comments, http://www.ietf.org/rfc.html.
TSA	Издавач на временски жигови, англ. Timestamping Authority.
UTC	Координирано универзално време, англ. Coordinated Universal Time, меѓународен стандард за мерење на времето, со важност од I. 1972.

3.2 Изрази

Општите изрази што се користат во оваа политика се дадени во табелата:

Временски жиг	Временскиот жиг претставува збир на податоци во електронска форма кој поврзува други податоци во електронска форма со конкретно време и претставува доказ дека поврзаните податоци постоеле во конкретниот момент. Тоа се недвосмислени и точни податоци за датумот, точното време, прецизно на најмалку една секунда и за издавачот кој го создал временскиот жиг. Временскиот жиг може да се додаде на документот или да се приложи и/или поврзе со него.
Дигитален потпис	Квалификуван електронски потпис.
Апликација	Компјутерска програма со која управува организацијата и која за својата работа користи услуги на издавачот на временски жиг.

Инфраструктура на Македонски Телеком TSA	Сите простории на издавачот, потребната инфраструктура софтвер како и заштитните механизми потребни за безбедна работа.
Македонски Телеком TSA	Давател на доверлив ауслуга за временски жиг, кој функционира во рамките на Македонски Телеком СА, англ. МКТ Timestamp authority.
Организација	Деловен субјект, јавни или државни институции, согласно важечките прописи во Република Македонија или пак странско лице кое врши дејност и кое својата истоветност може да ја докаже во согласност со важечките прописи.
Корисник	Краен корисник или апликација кои ги користат услугите на Македонски Телеком TSA за издавање на временски жигови.
Место на објава	Јавна објава на веб- страницата на Македонски Телеком TSA односно на страницата на Македонски Телеком АД Скопје, https://timestamp.telekom.mk
Известувања	Сите упатства, објаснувања, листи, услови, поединечни известувања, препораки, стандарди и други документи кои се одредени или препорачани од Македонски Телеком TSA и кои ги објавува или на друг начин ги проследува до корисниците на временски жигови, организациите или на трети лица.

4. Податоци за издавачот Македонски Телеком TSA

4.1 Услуга – издавање на временски жиг

Процесот е поделен во два дела и тоа издавање на времески жиг и управување со издадените временски жиг. Истиот е во согласност со меѓународните стандарди.

4.2 Идентитет на издавачот Македонски Телеком TSA

Меѓународниот број кој ја означува политиката на работење на Македонски Телеком TSA е: CPOID: 1.3.6.1.4.1.18560.1.3.0.0.0.0

Податоците за контакт со Македонски Телеком TSA се дадени подолу:

Адреса:	Кеј 13-ти Ноември бр.6, Скопје
Е-пошта:	tsainfo@telekom.mk
Контактен центар:	070120
УРЛ:	https://timestamp.telekom.mk

4.3 Корисници на временските жиг

Корисници на временски жиг на Македонски Телеком TSA имаат Договор за користење на услугата Временски жиг.

Меѓусебните односи помеѓу корисниците и Македонски Телеком TSA се уредени со меѓусебен Договор за користење на услугата временски жиг како и оваа Политика.

Трети лица се субјекти кои се потпираат на издадените временски жиги на издавачот Македонски Телеком TSA.

4.3.1 Цел на употреба

Услугите на Македонски Телеком TSA се наменети за издавање временски жигови кои може да се користат за:

- Потврда на документ во одреден временски период, и тоа така што датумот и времето на потврда со жиг се поврзуваат со содржината на документот на криптографски безбеден начин,
- секаде каде што е потребно на безбеден начин да се докажат временските карактеристики на трансакциите и други услуги,
- за други потреби каде што е потребен временски жиг.

4.3.2 Специфики и целесообразност

Издавачот Македонски Телеком TSA работи во согласност со:

- Законот за електронски документи, електронска идентификација и доверливи услуги како и правилниците и други прописи донесени врз основа на овој закон,
- европските директиви и регулативи поврзани со оваа проблематика,
- препораките на RFC за потврдување со временски жиг: RFC 3161 »Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)«,
- и други важечки прописи.

Македонски Телеком TSA работи согласно оваа политика при што за секој временски жиг се доделува идентификатор на CPOID.
Формата и содржината на јавниот дел на внатрешните правила на издавачот Македонски Телеком TSA се усогласени со препораките на:

- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- RFC 3628 “Policy requirements for Time-Stamping Authorities (TSAs)”.

4.3.3 Приод

Политика за временски жиг е општ документ кој што во себе не содржи технички детали. Истиот не ги објаснува ниту опишува организациската структура, инфраструктурата на системот за временски жиг како ни другите системи во сопственост на Македонси Телеком АД - Скопје.

5. Политика за издавање на временски жиг

5.1 Преглед

Политиката е документ кој што во себе ги содржи и обајаснува правилата дефинирани, јавниот дел, од страна на Македонски Телеком АД – Скопје како издавач на временски жиг и се во согласност со барањата на релевантните важечки регулативи и стандарди.

Давателот на доверливи услуги на дигитални сертификати Македонски Телеком CA на Давателот на доверлива услуга за временски жиг Македонски Телеком TSA му издаде соодветни дигитални сертификати за серверски издавач согласно важечката политика на Македонски Телеком CA.

Дигиталниот сертификат на издавачот Македонски Телеком TSA, т.е. сертификатот „ TimeStamp Authority MKT TSA 4“ ги содржи следните податоци:

Назив на полето	Вредност за сертификатот на „TimeStamp Authority MKT TSA 4“
Верзија, англ. Version	3
Идентификациска ознака, англ. Serial Number	38291afe55cca238000000005f26b089
Алгоритам за јавен клуч, англ. Signature Algorithm	sha256 With RSA Encryption
Издавач на сертификат, англ. Issuer	CN = Makedonski Telekom CA O = Makedonski Telekom C = MK
Сопственик на сертификат, англ. Subject	CN=TimeStamp Authority MKT TSA 4 O=Makedonski Telekom AD - Skopje 2.5.4.97=VATMK-4030997339640 c=MK
Почеток на важноста, англ. Validity: Not before	22.8.2024 07:54 GMT
Крај на важноста, англ. Валидиту: Validity: Not after	22.8.2029 08:24 GMT
Алгоритам за јавен клуч, англ. Public Key Algorithm	RSA (2048 bits)
Сопственици на јавен клуч кој припаѓа на соодветен пар клучеви, шифриран со алгоритам на RSA, англ. RSA Public Key	клуч со должина од 2048 бита
Политика на издавачот, англ. Certificate Policy	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.18560.1.3.1.1.0.0 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.telekom.mk/CPS
Употреба на клуч, англ. Key Usage	Digital Signature (80)
Enhaced Key Usage (Critical)	Time Stamping (1.3.6.1.5.5.7.3.8)
SHA-256 отпечаток (Thumbprint)	f6e62ab114671749f174990347553345ca0db5c1

5.2 Идентификација на Издавачот на временски жиг

Оваа Политика за времески жиг е идентификувана со рамките на Македонски телеком АД – Скопје со својот единствен идентификацики број 1.3.6.1.4.1.18560.1.3.0.0.0 каде што:

- ISO (1)
- Org (3)
- Dod (6)
- Internet (1)
- Private (4)
- Enterprise (1)
- MKT (18560)
- TSA (1)
- Политика за временски жиг (3)

5.3 Област на применливост

Оваа политика е во корелација со барањата за издавање на временски жиг за архивирање на потпишани документи со квалификувани сертификати.

Истата е широко применлива покривајќи различни сегменти и видови како електронски трансакции, архивирани податоци или формулари.

5.4 Усогласеност

Издадените временски жигови имаат единствен OID број кој е во согласност и произлегува од дефинираниот начин на идентификацијата опишана во точката 5.2 од оваа Политика.

6. ОБВРСКИ И ОДГОВОРНОСТ

6.1 Обврски на издавачот Македонски Телеком TSA

6.1.1 Генерални обврски

Издавачот Македонски Телеком TSA е должен:

- Да работи согласно своите внатрешни правила и останатите важечки закони и прописи,
- Да работи согласно меѓународните препораки,
- Да ги објавува сите важни документи со кои се определува неговата работа (политики на работење, обрасци, ценовник, упатства за безбедна употреба на временските жигови),
- Да издава временски жигови согласно оваа политика и останатите прописи и препораки.

6.1.2 Обврски на Македонски Телеком TSA кон корисниците

Издавачот Македонски Телеком TSA има обврска:

- да обезбеди точност на податоците на временскиот жиг,
- да обезбеди соодветна физичко обезбедување на просториите и пристапите до самите простории на издавачот,
- да се грижи за непречено работење и што поголема достапност на услугите,
- да се грижи за непречено работење на сите останати пропратни услуги,
- да се обиде да ги отстрани настанатите проблеми во најбрз можен рок,

- да се грижи за оптимизацијата на машинската и програмската опрема
- да ги известува корисниците и третите лица за поважните работи и
- да ги исполнува сите други стандарди согласно оваа политика.

Издавачот Македонски Телеком TSA обезбедува максимална достапност на своите услуги за потврда со временски жиг, и тоа 24часа/7дена/365дена, освен во следните случаи:

- планирани и однапред најавени технички или сервисни интервенции на инфраструктурата,
- непланирани технички или сервисни интервенции на инфраструктурата како последица на непредвидени дефекти,
- технички или сервисни интервенции поради дефекти на инфраструктурата надвор од надлежноста на издавачот на временски жигови и
- недостапност на услугите на потврдување со временски жиг како последица на виша сила или вонредни настани.

Останатите обврски на издавачот Македонски Телеком TSA со корисниците се определуваат со меѓусебен договор.

6.2 Обврски на корисниците

Корисниците мораат:

- на издавачот да му даваат точни и целосни податоци за идентитетот односно други податоци за искажување на истоветноста,
- при активирање на услугата временски жиг да постапат согласно упатствата на издавачот Македонски Телеком TSA поставени на МКТ сајтот,
- при евентуални дефекти или проблеми веднаш да го известат издавачот Македонски Телеком TSA,
- да се запознаат со оваа политика и да ги почитуваат сите одредби во врска со нивните обврски, одговорности и ограничувања за доверливоста и користењето на временските жигови,
- да ги почитуваат сите други препораки на Македонски Телеком TSA во врска со сигурната употреба на временските жигови,
- редовно да ги следат сите известувања и објави на Македонски Телеком TSA и да постапуваат согласно истите,
- согласно препораките на издавачот да се грижат за архивот на електронски документи и потребните податоци за проверка на временски означените документи,
- да ги исполнуваат сите други стандарди согласно оваа политика односно договорот и
- да ги почитуваат евентуалните други правила кои се надвор од надлежноста на издавачот и се определени на друго место.

6.3 Обврски на трети лица

Третите лица, кои се потпираат на временскиот жиг на Македонски Телеком TSA, мораат:

- временскиот жиг да го проверат согласно упатствата на издавачот Македонски Телеком TSA,
- при евентуални дефекти или проблеми веднаш да го известат издавачот Македонски Телеком TSA,
- да се запознаат со оваа политика и да ги почитуваат сите одредби во врска со нивните обврски, одговорности и ограничувања за доверливоста и користењето на временските жигови,
- да ги почитуваат сите други препораки на Македонски Телеком TSA во врска со сигурната употреба на временските жигови,
- да ги следат сите известувања и објави на Македонски Телеком TSA и да постапуваат согласно истите,

- да ги почитуваат евентуалните други правила кои се надвор од надлежноста на издавачот и се определени на друго место.

6.4 Одговорност на издавачот Македонски Телеком TSA

Македонски Телеком TSA е одговорен:

- Издадениот временски жиг да ги содржи сите пропишани податоци согласно оваа политика и другите прописи,
- Да ги чува податоците за издадените временски жиг во период од 10 години
- за изведбата на сите свои обврски, наведени во потпоглавје 6.1.2.

Македонски Телеком TSA не е одговорен за директна или индиректна штета, изгубен документ и слично, која би настанала поради употреба на временските жиг на издавачот Македонски Телеком TSA, доколку:

- временскиот жиг е издаден како резултат на дефект, неверодостојни податоци или други грешки на корисникот,
- услугата на издавање временски жиг била побарана по објава на отповикани серверски дигитални сертификати на Македонски Телеком TSA или Македонски Телеком CA,
- била предизвикана поради пад на системот односно недостапност и нерасположливост на инфраструктурата, што не е во доменот на управување Македонски Телеком TSA, вклучувајќи ја програмската и машинската опрема на корисникот,
- корисникот не ги почитувал одредбите на оваа политика и меѓусебниот договор и други објавени препораки на издавачот во врска со целта и начинот на користење на своите услуги,
- корисникот не ги почитувал другите важечки прописи.

Македонски Телеком АД – Скопје поседува осигурително покритие за Општа одговорност и одговорност од производ, вклучувајќи и чиста финасиска загуба, вообичаени за основната дејност. Осигурителното покритие се однесува на евентуални грешки или пропусти од небрежност направени од страна на Македонски Телеком TSA во процесот на издавање и управување со временските жиговии. Лимитот на покритие за осигурување од одговорност за временски жиг е во согласност со Законот за електронски документи, електронска идентификација и доверливи услуги и Правилникот за утврдување на најниските износ од осигурувањето од евентуалната штета предизвикана од Издавачот и минималниот износ или видот на покритието на осигурување од ризикот од одговорност за штета причинета од страна на Давателот на квалификувана доверлива услуга .

Јавните клучеви по истекот на важноста, се чуваат уште 5 години а потоа се уништуваат. Јавните клучеви на Издавачот се чуваат дополнителни 10 години за да може да се прави верификација на временски жиг издаден во минатото.

7. Барања кои треба издавачот да ги исполни

Македонски Телеком АД – Скопје го има имплементирано стандардот ISO 27001:2022, Information Security Management System (ISMS). Согласно барањата на истиот ги има имплементиртано сите принципи и контроли за информатичка сигурност со што во целост се покриени барањата за безбедност што се бараат од издавачот на временски жиг.

Опремата на Македонски Телеком TSA е инсталирана во посебни, одвоени простории во рамките на инфраструктурата на Македонски Телеком, а дел и надвор од неа. Обезбедена е со систем од повеќе нивоа за физичко и електронско обезбедување. Обезбедувањето на инфраструктурата на Македонски Телеком TSA се изведува согласно препораките на струката за највисоко ниво на безбедност.

Деталните одредби за физичко обезбедување се во согласност со Уредбата на Македонски Телеком АД – Скопје.

7.1 Правила и изјава за на работењето на Македонски Телеком TSA

7.1.1 Правила на работа

Македоснки Телеком АД - Скопје во целост ги исполнува предусловите и ја гарантира услугата издавање на временски жиг. Истото е во целост опишано и подржано со оваа Политика.

Издавачот, согасно имплементираните стандарди спроведува анализи на ризик се со цел обезбедување на неопходните безбедносни контроли и оперативни процедури.

Издавачот има воспоставено практики и процедури неопходни за идентификација и имплемантација на барањата дефинирани во Политиката.

Сите документи кои се однесуваат на Политиката Давателот на доверлива услуга за временски жиг ги објавува со што овозможува сите заинтересирани страни да ја проверат својата усогласеност со Политика.

Давателот на доверлива услуга за временски жиг има воспоставена времена организација со посебни овластувања за одобрување на Политиката.

Преставниците на менаџментот кои се дел од времената организација на TSA се со посебни овластувања и одговорности за проверка на начинот на имплементација, контрола како и периодична проверка. Исто така се одговорни и за ажурирање на Политиката, усогласеноста, нејзиното одобрување, верзионирање и објавување.

7.1.2 TSA релевантни информации

Сите одредби од оваа точка, доколку не се детално дадени во другите точки од оваа политика, се опишани во интерните правила на Македонски Телеком.

Начинот на користење на услугата на временски жиг на Македонски Телеком TSA е објавен во упаството на веб страницата: https://timestamp.telekom.mk

За решавање на евентуални спорови надлежен е судот во Скопје според правото на Република Македонија.

Македонски Телеком СА јавно го објавува сижето на одлуките на инспекцискиот надзор.

7.2 Управување со клучевите на Македонски Телеком TSA

7.2.1 Генерирање на клучеви на Македонски Телеком TSA

Парот клучеви за потпишување и верификација на временскиот жиг се генерирани во физички и електронски безбедна средина на Македонски Телеком TSA според посебна постапка за генерирање клучеви.

Генерирањето на клучеви се врши во доверливи хардверски криптографски модули, кои се имаат безбедносни сертификати во согласност со одредбите на FIPS 140-2 ниво 3 и во согласност со eIDAS CC EAL4+, со посебна церемонија за издавање на клучеви за потребите на TSA системи.

Јавниот клуч на издавачот Македонски Телеком TSA е потпишан од Давателот на доверливи услуги Македонски Телеком СА и му е издаден дигитален сертификат.

Дигиталниот сертификат со јавниот клуч и приватниот клуч на Македонски Телеком TSA се генерираат со алгоритми и на начин кој е во согласност со интерните правила на Македонски Телеком TSA и во согласност со меѓународно прифатените стандарди и препораки.

Деталните одредби за генерирање на клучеви на Македонски Телеком TSA се во согласност со Политиката и интерните регулативи на Македонски Телеком CA.

7.2.2 Заштита на приватниот клуч на Македонски Телеком TSA

Приватниот клуч на издавачот Македонски Телеком TSA за потпишување временски жиг се чува во доверливи хардверски криптографски модули кои се во согласност со одредбите на FIPS PUB 140-2 ниво 3 како и eIDAS CC EAL4+.

Македонски Телеком забранува изработка и умножување на приватните клучеви од уредите (HSM) за генерирање на временски жиг.

7.2.3 Достава на дигитални сертификати на Македонски Телеком TSA

Сертификатите за временски жиг како и јавниот клуч на издавачот на Македонски Телеком TSA е објавен и доставен во согласност со политиката на Македонски Телеком TSA, секогаш во форма на дигитален сертификат на Давателот на доверливи услуги Македонски Телеком CA.

Карактеристиките и податоците за сертификатите односно јавните клучеви на издавачот Македонски Телеком TSA се објавени и на веб-страниците на Македонски Телеком TSA.

7.2.4 Обновување на јавен клуч од Македонски Телеком TSA

Почетокот и крајот на важноста на јавните клучеви на издавачот Македонски Телеком TSA е определена со оваа политика во точка 5.1.

По истекот на важност на јавниот клуч, треба да се отпочне со постапка за обновување на јавниот клуч за нов 5 годишен период.

Јавниот клуч кој има истечена важност треба да се чува согласно обврските на издавачот регулирани во точка 7.2.5

7.2.5 Истекување на важноста на клучевите на Македонски Телеком TSA

Македонски Телеком TSA гарантира дека нема да ги употребува клучевите по истекот на нивната важност.

Македонски Телеком TSA гарантира дека навремено и безбедно ќе ги замени клучеви со помината важност со важечки.

Постапката на Македонски Телеком TSA за поништување на приватните клучеви по нивното истекување се одвива на безбеден начин во согласност со одредбите на интерните правила на Македонски Телеком CA. Приватните клучеви се поништуваат така што да не може повторно да се активираат.

7.2.6 Управување со криптографски модули за временски жиг

Македонски Телеком TSA се грижи за безбедноста на хардверските безбедносни модули (HSM) задолжени за криптографија за време на целиот животен век на инфрастурктурата.

Деталните одредби во врска со криптографските модули на Македонски Телеком TSA се во согласност со интерните правила на Македонски Телеком TSA.

7.3 Потврда со временски жиг

7.3.1 Временски жиг

Македонски Телеком TSA гарантира дека временските жигови се издадени на безбеден начин со точно време и со прецизност од една (1) секунда или попрецизно во однос на UTC.

Македонски Телеком TSA издава само еден вид на токен за временски жиг во согласност со оваа политика. Секој еден токен го содржи идентификацискиот број на Политика за издавање на времески жиг (OID) и единствен сериски број на издадениот токен.

Македонски Телеком TSA за формирање на електронскиот потпис на токенот за времеснки жиг користи RSA алгоритам со кој е шифриран "Hash-от", направен со алгоритмот SHA 256 RSA

Токенот содржи електронски сертификат со кој се проверува електронскиот потпис на токенот за временскиот жиг.

Формата на барањето за добивање временски жиг, како и самиот временски жиг се во согласност со протоколот Time Stamp Protocol (TSP).

Упатството на Македонски Телеком TSA е објавено на веб-страницата на Македонски Телеком TSA.

Профилот на временскиот жиг е во согласност со RFC 3161. Сервисот издава RSA2048 енкриптиран временски жиг кои прифаќаат еден од следниве hash алгоритми: SHA256, SHA384, SHA512.

Field	Value/Meaning
Version	1
Hash Algorithm	SHA256, SHA384, SHA512.
OID	1.3.6.1.4.1.18560.1.3.0.0.0
Serial Number	38291afe55cca238000000005f26b089
Generated Time	22.08.2024 07:55:03 GMT
Accuracy	+- 1 sec of UTC
Ordered	FALSE
Nonce	Supported
TSA	cn=TimeStamp Authority MKT TSA 4 o=Makedonski Telekom AD - Skopje 2.5.4.97=VATMK-4030997339640 c=MK
	CN = Makedonski Telekom CA O = Makedonski Telekom C = MK

7.3.2 Синхронизации на времето

Времето на серверите на Македонски Телеком TSA на безбеден начин се усогласува со времето на UTCсо серверот за синхронизација на времето по Network Time Protocol (NTP), кој го користи референтното време по GPS или DCF77 или референтен осцилатор.

Усогласеноста на времето на серверите на Македонски Телеком TSA со референтното време постојано се проверува и во случај на евентуални отстапки Македонски Телеком TSA превзема соодветни мерки.

7.4 Управување и организација

7.4.1 Управување со безбедноста

Управувањето со безбедноста, генерално, се врши во согласност со важечките прописи и барањата на стандардот ISO 27001:2022(Менаџмент систем за управување со безбедноста на информациите.)

Обезбедувањето на ифраструктурата на издавачот Македонски Телеком TSA се врши во согласност со барањата на стандардот ISO 27001:2022, Менаџмент систем за управување со безбедноста на информациите и истата е обезбедена со систем за физичка и електронска контрола на пристап на повеќе нивоа.

Целосниот опис на инфраструктурата на Македонски Телеком TSA и постапките за управување и обезбедување на истите се определени со интерните регулативи и техничката документација на Македонски Телеком.

Пристап до инфраструктурата на Македонски Телеком TSA, односно издавачот, имаат само одредени лица на Македонски Телеком АД – Скопје согласно нивните задачи и соодветни овластувања дефинирани во интерните регулативи и посебните овластувања.

Сите пристапи се надгледувани и обезбедени согласно законот и интерните регулативи.

7.4.2 Класификација и управување

Македонски Телеком TSA гарантира за нивото на заштита над целата опрема со која што располага и која се користи во процесот на работење.

Македонски Телеком TSA врши процена на можните ризици од работењето и за истите води записи и презема превентивни и корективни мерки за ибегнување на несакани настани.

Македонски Телеком TSA врши ажурирање на средствата, нивна соодветна класификација и третман, како и ажурирање на процедурите и воспоставените контроли за безбедност и превенција.

7.4.3 Надзор над персоналот

Деталните одредби во врска со надзорот на персоналот се определени во Интерните регулативи на Македонски Телеком.

Во согласност со стандардите, персоналот на Македонски Телеком TSA ги има потребните квалификации и искуство за управување со опремата која е составен дел од Македонски Телеком TSA.

На персоналот на Македонски Телеком TSA му се обезбедува соодветна обука за системите кои се составен дел на TSA инфраструктурата.

Персоналот на Македонски Телеком TSA се обучува за потребите односно новините во врска со работата на издавачот Македонски Телеком TSA.

Санкциите во случај на неовластено или невнимателно вршење на задачите за овластените лица на Македонски Телеком TSA се изведуваат согласно важечкото законодавство.

За евентуални надворешни изведувачи важат истите барања како и за овластените лица на Македонски Телеком TSA.
На овластените лица на Македонски Телеком TSA им е на располагање целата потребна документација согласно нивните задолженија и задачи.

7.4.4 Физичко обезбедување

Опремата на Македонски Телеком TSA е поставена во посебни, обезбедени, одвоени простории во рамките на инфраструктурата на Македонски Телеком CA.

Обезбедена е со систем за физичко и електронско обезбедување на повеќе нивоа.

Деталните одредби се наоѓаат во интерните правила за безбедост кои се во согласност со барањата за сигурност кај вакви системи и стандардот ISO 27001:2022.

Пристап до инфраструктурата на Македонски Телеком TSA односно издавачот имаат само овластени лица на Македонски Телеком TSA согласно нивните задачи и овластувања.

Сите пристапи се обезбедени согласно интерните правила за безбедост

7.4.5 Управување и контрола на работењето

7.4.5.1 Конкретни технички барања за безбедноста на инфрастуктурата

Македонски Телеком CA имплементираше голем број на технички контроли за безбедноста на инфраструктурата на која што се извршува TS процесот кои се во согласност со законските барања и со препораките ISO 27001 и тоа на:

- Пристапот до HSM уредите
- Строга поделба на задолженијата и улогите на оперативните лица на TSA
- Користење на smart картички за складирање на профилот на службениците за безбедност на TSA и администраторите на сертификати
- Енкриптирани сесии меѓу TSA апликацијата и PKI корисничките апликации на претплатникот
- Енкриптирање на чувствителни податоци во базата на податоци на CA
- Архивирање на историјатот на клучеви и податоци за ревизијата на CA и на претплатникот
- Ревизија на настани поврзани со безбедноста
- Механизми за обновување на клучевите и на CA апликацијата

Главните оперативни системи и останатите користени производи се комерцијални готови производи.

7.4.6 Технички контроли за управување со векот на траење

7.4.6.1 Контроли на развојот

Сите апликации и производи што ги користи Македонски Телеком TSA се комерцијални готови производи.

7.4.6.2 Контроли за управување со безбедноста

Македонски Телеком CA има имплементирано постапки за управување со проблеми, промени и конфигурации за сите софтверски и хардверски компоненти на PKI кои се во согласност со препораките ISO/IEC 27001 и ISO 20000-1:2018.

7.4.6.3 Контрола на безбедноста во текот на животниот циклус

Македонски Телеком CA го тестира целокупниот софтвер и постапки во контролирана средина.

7.4.6.4 Контрола на безбедноста на мрежата

Мрежната инфраструктура на Македонски Телеком CA е составена од поврзани мрежни сегменти на кои се наоѓаат серверите и работните станици. Сегментите се меѓусебно поврзани со firewall-и. Компјутерската мрежа на Македонски Телеком CA е поврзана на Интернет преку повеќе нивоа на firewall-и. Безбедносните правила на firewall-ите дозволуваат сообраќај само за протоколите кои се неопходно потребни за пристап до сервисите на Македонски Телеком CA.

7.4.6.5 Напојување и вентилација

Инфраструктурата на Македонски Телеком TSA има обезбедено непрекинато напојување и соодветни клима системи. Деталните информации за инфрастуктурата се дефинирани во постоечката техничка документација достапна за ревизија од страна на надлежен орган.

7.4.6.6 Заштита од поплава

Заради обезбедување на континуитет на услугата, истата е дел од Планот за континуитет на деловното работење.

7.4.6.7 Заштита од пожари

Просториите на Македонски Телеком CA се обезбедени и соодветно опремени за заштита од евентуално избувнување на пожар како и справување со истиот, наведено во интерните регулативи и правила на МКТ.

7.4.6.8 Чување на носачите на податоци

Носачите на податоци, во хартиена или електронска форма, безбедно се чуваат во заштитени објекти.

Паралелна инфраструктура е поставена на различна, оддалечена локација и е во оперативна состојба. Истата редовно се ажурира согласно интерните правила на МКТ.

7.4.6.9 Отстранување на непотребни информации

Македонски Телеком TSA обезбедува сигурно отстранување и уништување на документите во хартиена или електронска форма.

Отстранувањето го врши посебна комисија во согласност со интерните правила на Македонски Телеком.

7.4.7 Управување со инфраструктурата

Деталите за управувањето со инфраструктурата е дефинирана и е во во согласност со интерните правила на Македонски Телеком.

7.4.8 Управување со пристап до инфраструктурата

Пристапот до инфраструктурта е дефиниран со одредбите се наоѓаат во интерните правила за безбедост кои се во согласност со барањата за вакви ситеми и препораките на стандардот ISO 27001:2022.

7.4.9 Воспоставување и одржување на инфраструктурата

Издавачот Македонски Телеком TSA ги врши своите услуги во рамките на инфраструктурата која е сертифицирана во согласност со највисоките стандарди за безбедност.

Согласно Уредбата деталите се опишани во Интерната политика на Македонски Телеком TSA.

7.4.10 Загрозување на инфраструктурата

Во случај на загрозена безбедност на инфраструктурата на Македонски Телеком TSA во издавањето временски жиг, издавачот Македонски Телеком TSA ќе ги преземе мерките определени во Интерната политика на Македонски Телеком TSA. Информацијата за евентуалното загрозување на работата на Македонски Телеком TSA ќе биде јавно објавена за сите претплатници и засегнати страни, како и причините за настанувањето на истата кои може да бидат од повеќе оперативни или технички причини.

7.4.11 Престанок на работата на Македонски Телеком TSA

Доколку Македонски Телеком TSA престане со вршење на својата дејност или издавачот Македонски Телеком TSA престане со издавање на временски жиг, тогаш Македонски Телеком TSA ќе постапи согласно важечките закони. Информацијата за престанокот на работата на Македонски Телеком TSA ќе биде јавно објавена за сите претплатници и засегнати страни.

7.4.12 Дневници за доверливи записи

Македонски Телеком TSA врши складирање на сите релевантни записи за настани од TSA системот со чија помош може да идентификуваат инциденти и други доверливи настани и да се искористат истите за евентуални правни дејствија. Истите се чуваат во временски период предвиден со интерните политики на Македонски Телеком TSA. Овие записи обезбедуваат информации за:

- Безбедноста на инфраструктурата,
- Непречената работа на сите доверливи системи и
- Дали во меѓувреме дошло до упад или обид за упад на неовластени лица до опремата или податоците.

7.5 Управување со документацијата

Македонски Телеком TSA го задржува правото за промена на овој документ без претходно известување на корисниците, доколку промените не влијаат на целта на употреба и на постапките на управување кои би можеле да го изменат нивото на доверливост.

Измените во политиката на Македонски Телеком TSA се објавуваат на веб-страниците на издавачот Македонски Телеком TSA.