



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

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



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

Идентификационен бр.	POL 009
Верзија Бр.	1.0
Одговорна организациска единица	Оперативна служба на Македонски Телеком TSA

Извршен преглед

Верзија	Датум	Краток опис на промените
1.0	Јули 2017	Согласно барањата на стандардот ETSI TS 102 023 V1.2.2 (2008-10) Electronic Signatures and Infrastructure (ESI); Policy requirements for time-stamping authorities изработена е Политиката за издавање на временски печат (TS) на Македонски Телеком АД Скопје како Time Stamp Authority (TSA). Истата во целост ги задоволува барањата на стандардот и преставува потврда за целесобразноста на барањата со решението.

Историјат*

Верзија	Датум	Подготвено од:	Краток опис на промените



Содржина

1.	Македонски Телеком TSA - издавач на временски печат	5
2.	Вовед	5
3.	Значење на кратенките и изразите	6
3.1	Кратенки	6
3.2	Изрази	6
4.	Податоци за издавачот Македонски Телеком TSA	7
4.1	Услуга – издавање на временски печат	7
4.2	Идентитет на издавачот Македонски Телеком TSA	7
4.3	Корисници на временските печат	8
4.3.1	Цел на употреба	8
4.3.2	Специфики и целесообразност	8
4.3.3	Приод	8
5.	Политика за издавање на временски печат	9
5.1	Преглед	9
5.2	Идентификација на Издавачот на временски печати	10
5.3	Област на применливост	10
5.4	Усогласеност	10
6.	ОБВРСКИ И ОДГОВОРНОСТ	10
6.1	Обврски на издавачот Македонски Телеком TSA	10
6.1.1	Генерални обврски	10
6.1.2	Обврски на Македонски Телеком TSA кон корисниците	11
6.2	Обврски на корисниците	11
6.3	Обврски на трети лица	12
6.4	Одговорност на издавачот Македонски Телеком TSA	12
7.	Барања кои треба издавачот да ги исполни	13
7.1	Правила и изјава за на работењето на Македонски Телеком TSA	13
7.1.1	Правила на работа	13
7.1.2	TSA релевантни информации	13
7.2	Управување со клучевите на Македонски Телеком TSA	14
7.2.1	Генерирање на клучеви на Македонски Телеком TSA	14
7.2.2	Заштита на приватниот клуч на Македонски Телеком TSA	14
7.2.3	Достава на дигитални сертификати на Македонски Телеком TSA	14



7.2.4	Обновување на јавен клуч од Македонски Телеком TSA	14
7.2.5	Истекување на важноста на клучевите на Македонски Телеком TSA.....	14
7.2.6	Управување со криптографски модули за временски печати.....	15
7.3	Потврда со временски печат.....	15
7.3.1	Временски печат.....	15
7.3.2	Синхронизации на времето	16
7.4	Управување и организација.....	16
7.4.1	Обезбедување на инфраструктурата	16
7.4.2	Пристап до инфраструктурата на издавачот MKT- TSA.....	Error! Bookmark not defined.
7.4.3	Надзор над персоналот	17
7.4.4	Физичко обезбедување.....	17
7.4.4.1	Локација и структура на Македонски Телеком TSA.....	Error! Bookmark not defined.
7.4.4.2	Физички пристап до инфраструктурата на Македонски Телеком TSA	Error! Bookmark not defined.
7.4.5	Контрола на работењето	17
7.4.5.1	Конкретни технички барања за безбедноста на компјутерите	17
7.4.5.2	Ниво на безбедност на компјутерите	Error! Bookmark not defined.
7.4.6	Технички контроли за управување со векот на траење.....	18
7.4.6.1	Контроли на развојот.....	18
7.4.6.2	Контроли за управување со безбедноста	18
7.4.6.3	Контрола на безбедноста во текот на животниот циклус.....	18
7.4.6.4	Контрола на безбедноста на мрежата	18
7.4.6.5	Напојување и вентилација.....	18
7.4.6.6	Заштита од поплава	18
7.4.6.7	Заштита од пожари	19
7.4.6.8	Чување на носачите на податоци.....	19
7.4.6.9	Отстранување на непотребни информации	19
7.4.7	Управување со инфраструктурата.....	19
7.4.8	Управување со пристап до инфраструктурата.....	19
7.4.9	Воспоставување и одржување на инфраструктурата.....	19
7.4.10	Загрозување на инфраструктурата	19
7.4.11	Престанок на работата на Македонски Телеком TSA.....	19
7.4.12	Сообразност со важечката законодавност	Error! Bookmark not defined.
7.4.13	Дневници за доверливи записи.....	20
7.5	Управување со документацијата.....	Error! Bookmark not defined.



1. Македонски Телеком TSA - издавач на временски печат

Македонски Телеком АД - Скопје нуди услуга, издавање на временски печат, како доверлив издавач на временски печати или Time Stamp Authority (TSA).

Временскиот печат или временскиот жиг се наменети за потврда на содржината и веродостојноста на документот во конкретен миг.

Со овој документ се определуваат правилата на работењето на издавачот Македонски Телеком TSA. Сите услуги, издадени временски печати, на издавачот Македонски Телеком TSA се обработуваат согласно истите.

Известувањата, упатствата, правилата и другите важни документи за користење на услугите на издавачот Македонски Телеком TSA се објавени на веб-страницата на издавачот <https://timestamp.telekom.mk>.

Правилата се изработени во согласност со меѓународните стандарди и тоа ETSI TS 102 023 V1.2.2 (2008-10) Electronic Signatures and Infrastructure (ESI) - Policy requirements for time-stamping authorities; ETSI TS 101 861 V1.4.1 (2011-07) Electronic Signatures and Infrastructure (ESI) - Time stamping profile; како и RFC 3161 - Time-Stamp Protocol (TSP).

2. Вовед

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

Македонски Телеком TSA како издавач на временски печат, издава временски печат, за кој што важи највисокиот степен на заштита и функционираат согласно важечките законски прописи и препораките од меѓународните стандарди.

Временскиот печат 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 потребна потврда во единица време.

Издавачот на временски печат, Македонски Телеком TSA <https://timestamp.telekom.mk>, функционира во рамките на Македонски Телеком СА.

Оваа политика го одредува работењето на Македонски Телеком АД - Скопје како издавач на временски печати, Македонски Телеком TSA, за издавање временски печати за потребите на било кое правно или физичко лице.

Македонски Телеком TSA издава временски печати со точност помала од една (1) секунда во однос на Координираното универзално време (UTC-Coordinated Universal Time).



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 сертификаирање 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 ИТУ-Т 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, http://www.ntp.org .
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 печати, англ. Time-Stamping Authority.
UTC	Координирано универзално време, англ. Coordinated Universal Time, меѓународен стандард за мерење на времето, со важност од 1. 1972.

3.2 Изрази

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

Временски печат	Временскиот печат, односно временски жиг претставува електронски потпишан сертификат на издавачот, со кој се потврдува содржината на податоците на кои се однесува, во точно наведено време и датум. Тоа се недвосмислени и точни податоци за датумот, точното време, прецизно на најмалку една секунда и за издавачот кој го создал временскиот печат. Временскиот печат може да се додаде на документот или да се приложи и/или поврзе со него.
Дигитален потпис	Безбедносен електронски потпис.



Апликација	Компјутерска програма со која управува организацијата и која за својата работа користи услуги на издавачот на временски печати
Инфраструктура на издавачот Македонски Телеком TSA	Сите простории на издавачот, потребната инфраструктура софтвер како и заштитните механизми потребни за безбедна работа.
Македонски Телеком TSA	Издавач на временски печат, кој функционира во рамките на Македонски Телеком СА, англ. MKT Time-stamp 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 печати
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 печати, организациите или на трети лица.

4. Податоци за издавачот Македонски Телеком TSA

4.1 Услуга – издавање на временски печат

Процесот е поделен во два дела и тоа издавање на времески печат и управување со издадените времески печати. Истиот е во согласност со меѓнародните 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, 1000, Скопје



Е-пошта: tsainfo@telekom.mk

Контактен центар: 070120

УРЛ: <https://timestamp.telekom.mk>

4.3 Корисници на временските печат

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

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

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

4.3.1 Цел на употреба

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

- Потврда на документ во одреден временски период, и тоа така што датумот и времето на потврда со печат 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 печат.

4.3.2 Специфики и целесобразност

Издавачот Македонски Телеком TSA работи во согласност со:

- Законот за податоците во електронски облик и електронски потпис 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 печат: 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 печат 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 TS 102 023 V1.2.2 (2008-10) Electronic Signatures and Infrastructure (ESI) - Policy requirements for time-stamping authorities;
- ETSI TS 101 861 V1.4.1 (2011-07) Electronic Signatures and Infrastructure (ESI) - Time stamping profile
- RFC 3628 "Policy requirements for Time-Stamping Authorities (TSAs)".

4.3.3 Приод

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



5. Политика за издавање на временски печат

5.1 Преглед

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

Издавачот на дигитални сертификати Македонски Телеком СА на издавачот на временски печат Македонски Телеком TSA му издаде соодветни дигитални сертификати за серверски издавач согласно важечката политика на Македонски Телеком СА.

Дигиталниот сертификат на издавачот Македонски Телеком TSA, т.е. сертификатот MKT TSA-1 ги содржи следните податоци:

Назив на полето	Вредност за сертификатот на MKT-TSA-1
Верзија, англ. Version	3 (што значи верзија 3)
Идентификациска ознака, англ. Serial Number	57 f8 c1 de
Алгоритам за јавен клуч, англ. Signature Algorithm	sha256RSA
Издавач на сертификат, англ. Issuer	CN = Makedonski Telekom CA O = Makedonski Telekom C = MK
Сопственик на сертификат, англ. Subject	CN = TimeStamp Authority MKT TSA 1 CN = Makedonski Telekom CA O = Makedonski Telekom
Почеток на важноста, англ. Validity: Not before	среда, 28 декември 2016 13:59:03
Крај на важноста, англ. Валидиту: Validity: Not after	вторник, 28 декември 2021 14:29:03
Алгоритам за јавен клуч, англ. Public Key Algorithm	RSA (2048)
Сопственици на јавен клуч кој припаѓа на соодветен пар клучеви, шифриран со алгоритам на PCA, 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
Употреба на клуч, англ. Key Usage	Digital Signature
Дополнителна одредба за употреба, англ. Extended Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8)
Идентитет на клуч (по алг. SHA-1): англ. Subject Key Identifier	45 c8 bb a6 1d 63 76 85

5.2 Идентификација на Издавачот на временски печати

Оваа Политика за временски печат е идентификувана со рамките на Македонски телеком АД – Скопје со својот единствен идентификачки 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 врменски печат (3)

5.3 Област на применливост

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

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

5.4 Усогласеност

Издадените временски печати 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 печати),
- Да издава временски печати 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 печат,
- 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 печат, и тоа 24 часа/7 дена/365 дена, 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 печати и
- недостапност на услугите на потврдување со временски печат 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 печат да постапат согласно упатствата на издавачот Македонски Телеком TSA поставени на MKT 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 печати,
- да ги почитуваат сите други препораки на Македонски Телеком TSA во врска со сигурната употреба на временските печати,
- 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 временските печати на Македонски Телеком TSA, мораат:

- временскиот печат 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 печати,
- да ги почитуваат сите други препораки на Македонски Телеком TSA во врска со сигурната употреба на временските печати,
- 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

Издавачот Македонски Телеком TSA е одговорен:

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

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

- временскиот печат е издаден како резултат на дефект, неверодостојни податоци или други грешки на корисникот
- услугата на издавање временски печат била побарана по објава на отповикани серверски дигитални сертификати на Македонски Телеком TSA или издавачот Македонски Телеком SA,
- била предизвикана поради пад на системот односно достапност 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 Издавачот Македонски Телеком TSA во процесот на издавање и управување со временските печати. Лимитот на покритие по настан и по временски печат е во висина до 1 200 000 денари.

Јавниот клуч со 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 времски печат издаден во минатото.



7. Барања кои треба издавачот да ги исполни

Македонски Телеком АД – Скопје го има имплементирано стандардот ISO 27001:2013, Information Security Management System (ISMS). Согласно барањата на истиот ги има имплементирани сите принципи и контроли за информатичка сигурност со што во целост се покриени барањата за безбедност што се бараат од издавачот на временски печат.

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 структурата 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

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

Издавачот, согласно 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 имплементација на барањата дефинирани во Политиката.

Сите документи кои се однесуваат на Политиката издавачот ги објавува со што овозможува сите заинтересирани страни да ја проверат својата усогласеност со Политика.

Издавачот има воспоставена временска организација со посебни овластувања за одобрување на Политиката.

Преставниците на менаџментот кои се дел од временската 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 печат на Македонски Телеком TSA е објавен во упатството 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 временските печати 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 во согласност со одредбите на FIPS PUB 140-2 ниво 3 со посебна церемонија за издавање на клучеви за потребите на TSA системи.

Јавниот клуч на издавачот Македонски Телеком TSA е потпишан од издавачот Македонски Телеком CA 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 регулативина Македонски Телеком CA.

7.2.2 Заштита на приватниот клуч на Македонски Телеком TSA

Приватниот клуч на издавачот Македонски Телеком TSA за потпишување временски печати се чува во доверливи хардверски криптографски модули кои се во согласност со одредбите на FIPS PUB 140-2 ниво 3.

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

7.2.3 Достава на дигитални сертификати на Македонски Телеком TSA

Сертификатите за временски печат 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 издавачот 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 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 издавачот 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 SA. Приватните клучеви се поништуваат така што да не може повторно да се активираат.

7.2.6 Управување со криптографски модули за временски печати

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

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 печат

7.3.1 Временски печат

Македонски Телеком TSA гарантира дека временските печати 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 печат во согласност со оваа политика. Секој еден токен го содржи идентификацискиот број на Политика за издавање на временски печат (OID) и единствен сериски број на издадениот токен.

Македонски Телеком TSA за формирање на електронскиот потпис на токениот за временски печат користи RSA алгоритам со кој е шифриран "Hash-от", направен со алгоритмот SHA -1

Токенот содржи електронски сертификат со кој се проверува електронскиот потпис на токениот за временскиот печат.

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

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

Профилот на временскиот печат содржи четири (4) дела на податоци, дадени во табелата во продолжение

Податоци за временски временски печат, англ. SignedInfo	<i>Каноникализациски метод</i>
	<i>Алгоритам за потпис (RSA, со кој е шифриран "Hash-от", направен со алгоритмот SHA -1)</i>
	<i>Податоци за временскиот печат:</i> - <i>"Hash" алгоритам (SHA -1)</i> - <i>"Hash"</i>
	<i>Податоци за издавачот Македонски Телеком TSA</i> - <i>алгоритам (SHA -1)</i> - <i>дел кое го означува издавачот MKT TSA</i>

Потпис, англ. SignatureValue	<i>Потпис</i>
Дигитален сертификат на Македонски Телеком TSA англ. KeyInfo of	<i>Отисок на сертификатот</i>
Податоци за временскиот печат, англ. TimeStampInfo	<i>Ознака на политиката, под која е издаден временскиот печат</i>
	<i>Структура на пораката која се потврдува со временски печат</i>
	<i>Сериски број, кој е единствен за сите временски печати издадени од MKT-TSA</i>
	<i>Време на издавање на временскиот печат, и тоа како универзално време</i>
	<i>Произволно генериран број кој е опционално вклучен во временскиот печат, доколку корисникот тоа го бара</i>
	<i>Други незадолжителни податоци</i>

7.3.2 Синхронизации на времето

Времето на серверите на Македонски Телеком TSA на безбеден начин се усогласува со времето на UTC со 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 27001:2013 (Менаџмент систем за управување со безбедноста на информациите.)

Обезбедувањето на инфраструктурата на издавачот Македонски Телеком TSA се врши во согласност со барањата на стандардот ISO 27001:2013, 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 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 избегнување 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 издавачот 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 SA.

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 27001:2013.

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 инфраструктурата



Македонски Телеком СА имплементираше голем број на технички контроли за безбедноста на инфраструктурата на која што се извршува TS процесот 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 СА
- Архивирање на историјатот на клучеви и податоци за ревизијата на СА и на претплатникот
- Ревизија на настани поврзани со безбедноста
- Механизми за обновување на клучевите и на СА апликацијата

TSA апликацијата што ја користи Македонски Телеком АД – Скопје е рангирана на EAL 4+ зголемено ниво на заштита.

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 СА 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 20000-1:2011.

7.4.6.3 Контрола на безбедноста во текот на животниот циклус

СА го тестира целокупниот софтвер и постапки во контролирана средина.

7.4.6.4 Контрола на безбедноста на мрежата

Компјутерската мрежа на Македонски Телеком СА 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 СА 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 СА.

7.4.6.5 Напојување и вентилација

Инфраструктурата на Македонски Телеком TSA има обезбедено непрекинато напојување и соодветни клима системи. Деталните информации за инфраструктурата 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 СА 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 согласност со интерните правила на Македонски Телеком.

7.4.8 Управување со пристап до инфраструктурата

Пристапот до инфраструктурата е дефиниран со одредбите се наоѓаат во интерните правила за безбедност кои се во согласност со барањата за вакви системи и препораките на стандардот ISO 27001:2013.

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 загрозување на безбедност на инфраструктурата на Македонски Телеком TSA во издавањето временски печати, 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 печати, 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.