ЈАВНО ПРЕДУЗЕЋЕ „ПОШТА СРБИЈЕ“, БЕОГРАД
Таковска 2, Београд

ПРАКТИЧНА ПРАВИЛА ЗА ПРУЖАЊЕ УСЛУГЕ ИЗДАВАЊА КВАЛИФИКОВАНИХ ЕЛЕКТРОНСКИХ ВРЕМЕНСКИХ ЖИГОВА ЈАВНОГ ПРЕДУЗЕЋА „ПОШТА СРБИЈЕ“, БЕОГРАД

(*Time-Stamp Practice Statement*)

Верзија: 1.0

Историја промена

Верзија	Датум	Разлог промене
1.0	02.04.2021.	Иницијална верзија

САДРЖАЈ

УВОД

Практичним правилима за пружање услуге издавања квалификованих електронских временских жигова Јавног предузећа „Пошта Србије“, Београд (*Time-Stamp Practice Statement*) (у даљем тексту: Практична правила) уређују се правила којих се Јавно предузеће „Пошта Србије“, Београд, као издавалац временског жига, придржава у свом раду, услови издавања временских жигова и правила оперативног рада.

Јавно предузеће „Пошта Србије“, Београд (у даљем тексту: Пошта) изградило је инфраструктуру за издавање временских жигова. Услуге намењене трећој страни, везане за проверу издатих временских жигова и приступ јавним информацијама о раду издаваоца временских жигова, слободно су доступне свим заинтересованим странама у складу са правима и обавезама наведеним у овим практичним правилима.

Временски жигови потврђују постојање електронских података у одређеном времену на поверљив и проверљив начин. Електронски подаци оверени временским жигом не могу се непримећено мењати.

Захтев за издавање временског жига, који садржи криптографски отисак података које треба оверити временским жигом, корисник шаље систему издаваоца временског жига. Систем затим генерише структуру података временског жига (токен) која, поред осталог, садржи достављени криптографски отисак података и тачно време, а затим електронски потпише/печатира тај објекат и на тај начин заштити његов интегритет.

Пошта као издавалац временског жига (у даљем тексту: Пошта *TSA*) врши издавање временских жигова у складу са законом и подзаконским актима (у даљем тексту: прописи), општим актима и упутствима Пошта *TSA*, који регулишу ову област.

Прописи акта чине правни оквир за обављање делатности издавања временских жигова Пошта *TSA*.

Пошта *TSA* издавање временских жигова врши у складу са одговарајућим међународним стандардима и препорукама, односно другим стандардима, документима и препорукама, које се односе на издавање временских жигова.

1. ОПСЕГ ДОКУМЕНТА

Практична правила описују практична правила издавања временског жига Пошта *TSA* и дефинишу процесе издавања жига, као и управљање тим процесима тако да корисници и трећа лица могу да имају пуно поверење у рад система за издавање временског жига.

Структура и садржај Практичних правила су у складу са документом ETSI EN 319 421 „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps“. Практична правила су у складу са Правилником о ближим условима за квалификоване електронске временске жигове („Службени гласник РС“, број 59/19) и подржава издавање временских жигова када је потребно доказати да су електронски подаци постојали пре одређеног времена.

Пошта *TSA* за потписивање/печатирање формираних токена временског жига користи електронске сертификате које издаје Сертификационо тело Поште, у складу са Политиком сертификације Сертификационог тела Јавног предузећа „Пошта Србије“, Београд за квалификоване електронске сертификације са новог система („Службени ПТТ-гласник“, број 1307/20) и Практичним правилима пружања услуге сертификације Сертификационог тела Јавног предузећа „Пошта Србије“, Београд за квалификоване електронске сертификате са новог система („Службени ПТТ-гласник“, број 1307/20) и услугу пружа у складу са стандардом ETSI

EN 319 411-2 "Electronic Signatures and Infrastructures (ETSI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

Пошта *TSA* објављује податке и сву документацију која се односи на издавање временских жигова на веб сајту https://www.ca.posta.rs која је јавно доступна, као и сви подаци и сва документација која се на њој налази.

Пошта *TSA* објављује на свом веб сајту:

- Опште услове, Политику издавања временског жига иова пПрактична правила, након ступања на снагу,
- моделе комерцијалних уговора,
- корисничка упутства,
- друга акта и обавештења.

Практична правила издавања временског жига Поште као издаваоца временског жига, креира и ажурира:

ЈАВНО ПРЕДУЗЕЋЕ „ПОШТА СРБИЈЕ“, БЕОГРАД
Сертификационо тело Поште
Таковска 2
11000 Београд
Србија
Телефон: 011/3607-895
Факс: 011/3651-412
Е-пошта: cepp@posta.rs
Веб сајт: https://www.ca.posta.rs

Практична правила одобрена су од стране директора Јавног предузећа „Пошта Србије“, Београд.

2. ЛИТЕРАТУРА

[1] Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС“, број 94/17).

[2] Правилником о ближим условима за квалификоване електронске временске жигове.

[3] ETSI EN 319 421 "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[4] ETSI EN 319 422 "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[5] RFC 3161, „Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)“.

[6] Уредба Европског парламента и Европског савета број 910/2014 од 23. јула 2014. године о електронској идентификацији и услугама од поверења за електронске трансакције на унутрашњем тржишту, која замењује Директиву 1999/93/ЕС (REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC).

[7] ETSI EN 319 411-2 "Electronic Signatures and Infrastructures (ETSI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

3. ДЕФИНИЦИЈЕ И СКРАЋЕНИЦЕ

3.1. Дефиниције

Издавалац временског жига (*Time-Stamping Authority - TSA*) је тело које издаје временски жиг.

Корисник (*Subscriber*) је правно или физичко лице, које користи услуге издаваоца временског жига, и које је изричито или подразумевано прихватило прописе и услове *TSA*.

Политика издавања временског жига (*Time-Stamp Policy*) је скуп правила која показују да је издавање временских жигова у складу са одређеним захтевима и прописима.

Практична правила (*Time-Stamp Practice Statement*) су описани скуп поступака и процедура оперативног рада, којих се *TSA* придржава при издавању временског жига.

Криптографски отисак је *hash* вредност електронског документа, која се формира коришћењем криптографског *hash* алгоритма.

Структура података временског жига, односно токен (*Time-Stamp Token*), је објекат који повезује криптографски отисак електронског документа са одређеним временом и на тај начин доказује да је електронски документ постојао пре тог времена (у даљем тексту: токен временског жига).

Јединица за формирање временског жига (*Time-Stamping Unit*) је криптографско средство за формирање временског жига, којим се генерише и електронски потписује/печатира токен временског жига издат у име *TSA*.

3.2. Скраћенице

Пошта *TSA* - Јавно предузеће „Пошта Србије“, Београд, као издавалац временског жига
UTC - Координисано универзално време (*Coordinated Universal Time*)
OID - Идентификациони број Политике издавања временског жига

4. ОПШТИ КОНЦЕПТ

4.1. Услуга издавања временског жига

Процес издавања временског жига је за потребе ових практичних правила подељен на два дела:

- **Издавање временског жига**: део услуге који формира токен временског жига.
- **Управљање издавањем**: део услуге који надзире и контролише операције издавања временског жига, а обезбеђује да је пружена услуга у складу са одредбама Практичних правила Пошта *TSA*. На пример, део за управљање издавањем гарантује да је време уписано у издати временски жиг правилно синхронизовано са извором тачног времена.

4.2. Издавалац временског жига

Пошта поседује изграђену инфраструктуру за издавање временског жига у складу са Законом о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању [1]. Пошта *TSA* има потпуну одговорност за обезбеђење свих услова за поуздано пружање услуге издавања временског жига и њену доступност, заштиту и ресурсе, како је дефинисано овим практичним правилима и одговарајућим прописима.

Приватни кључеви који се користе за потписивање/печатирање токена временског жига су увек власништво Пошта *TSA*.

Пошта *TSA* је регистровани издавалац временског жига у складу са Законом о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању [1] и правилником [2] . Пошта *TSA* је регистровани пружалац услуге по стандарду ETSI EN 319 421 [3], као тело које издаје токене временског жига.

4.3. Корисник

Корисник може да буде правно лице, државни орган или организација, која обухвата неколико крајњих корисника или појединачни крајњи корисник (физичко лице). Када је корисник правно лице, државни орган или организација, обавезе које се примењују на то правно лице, државни орган или организацију, примењиваће се и на крајње кориснике. При том су правно лице, државни орган или организација одговорни, уколико крајњи корисници правилно не испуне своје обавезе, јер се од правног лица или организације очекује да на одговарајући начин обавести крајње кориснике.

У случају појединачних крајњих корисника, корисници су сами одговорни за испуњење својих обавеза.

Коришћењем услуге Пошта *TSA*, корисници имплицитно прихватају обавезе одређене овим практичним правилима.

5. ПРАКТИЧНА ПРАВИЛА ИЗДАВАЊА ВРЕМЕНСКОГ ЖИГА

5.1. Преглед

Пошта *TSA* издаје временски жиг у складу са законом [1], правилником [2], стандардима [3, 4, 5], уредбом [6] и овим практични правилима.

Пошта *TSA* издаје временски жиг са тачним *UTC* временом (координисано универзално време - *Coordinated Universal Time*) уз одступање од највише ±1 секунде.

Пошта *TSA* за потписивање/печатирање токена временског жига користи приватне кључеве генерисане искључиво за ту намену, са периодом коришћења од највише једне године.

Пошта *TSA* користи електронске сертификате које издаје Сертификационо тело Поште, које је регистровано у складу са законом [1] и пружа услуге у складу са стандардом ETSI EN 319 411-2 [7]. Рок важности електронског сертификата је шест година.

Време одзива система, као разлика између времена примљеног захтева и времена у временском жигу, је мање од једног минута.

5.2. Идентификација

Идентификациони број Политике издавања временског жига (*OID*) је:
1.3.6.1.4.1.15672.11.801.1.0.

5.3. Применљивост

Практична правила су у складу са:
- правилником [2] и
- стандардом ETSI EN 319 421 [3].

Пошта *TSA* пружа услугу издавања временског жига корисницима који је по свом профилу у складу са стандардом ETSI EN 319 422 [4] и документом *RFC* 3161 [5].

Ова практична правила се користе за издавање временског жига у складу са законом [1].

5.4. Усаглашеност

Пошта *TSA* у издатим временским жиговима уписује идентификациони број Политике издавања временског жига (*OID*).

У циљу доказивања усклађености, Пошта *TSA*:

- испуњава своје обавезе,
- имплементира контроле,
- подлеже провери испуњености услова за регистрацију издаваоца временског жига и провери оперативног рада издаваоца временског жига у складу са законом [1] и правилником [2].

6. ОБАВЕЗЕ И ОДГОВОРНОСТ

Пошта *TSA* испуњава своје обавезе и прихвата преузете одговорности дате у овим практичним правилима.

6.1. Обавезе издаваоца временског жига

6.1.1. Опште обавезе

Пошта *TSA* обезбеђује да сви услови издавања временског жига, наведени у поглављу 7. ових практичних правила, буду имплементирани у складу са овим практичним правилима.

Пошта *TSA* обезбеђује усаглашеност са процедурама прописаним у овим практичним правилима.

Пошта *TSA* обезбеђује поштовање обавеза наведених у временском жигу, директно или уграђених преко референце.

Пошта *TSA* обезбеђује да све услуге издавања временског жига буду у складу са правилима оперативног рада издаваоца временског жига.

Пошта *TSA* је припремио и периодично ажурира анализу ризика за критичне сервисе који захтевају висок ниво сигурности.

6.1.2. Обавезе према корисницима

Пошта *TSA* обезбеђује стални приступ сервису издавања временског жига, осим у периоду сервисног одржавања, у ванредним ситуацијама (када поуздани извор тачног времена није доступан и др.) или услед других догађаја, природних или друштвених, који нису под контролом, нити су могли бити предвиђени, отклоњени или спречени од стране Пошта *TSA* (виша сила).

Планирани периоди одржавања биће објављени на веб сајту Пошта *TSA*.

Осим тога, Пошта *TSA*:

- имплементира и користи поуздану инфраструктуру за размену информација и комуникацију,
- чува све релевантне податке који се тичу издавања временских жигова у временском периоду који је прописан законом,
- поштује робне марке и интелектуалну својину,
- пружа услугу издавања временског жига у складу са опште прихваћеним стандардима и правилима,
- издаје само исправне временске жигове, примењујући правила оперативног рада како је наведено у поглављу 7. ових практичних правила.

6.2. Обавезе корисника временског жига

Захтев за формирање временског жига мора да буде креиран у складу са стандардом ETSI EN 319 422 [4] и документом *RFC* 3161 [5], и мора да садржи захтев за уградњу електронског сертификата (*certReq=True*) у формираном токену временског жига, којим се проверава електронски потпис/печат токена временског жига.

За формирање криптографског отиска података у захтеву за формирање временског жига, користи се један од следећих алгоритама: *SHA*-256, *SHA*-384 или *SHA*-512.

Захтев за формирање временског жига може да садржи идентификациони број Политике издавања временског жига (*OID*) (из поглавља 5.2.), али може да буде и без идентификационог броја Политике.

Пошта *TSA* ће одбити издавање временског жига уколико захтев није потпун или сагласан са обавезама корисника и доставити одговор кориснику како је дефинисано у документу *RFC* 3161 [5].

Приликом добијања токена временског жига, корисник треба да провери да ли је токен временског жига исправно електронски потписан/печатиран и да сертификат којим се проверава потпис/печат токена временског жига није опозван до тренутка провере.

Додатни захтеви могу да буду прописани уговором између Пошта *TSA* и корисника.

6.3. Обавезе треће стране

Обавеза треће стране је да, када се ослања на токене временског жига издате од стране Пошта *TSA,* провери исправност електронског потписа/печата токена временског жига и увери се у исправност токена временског жига.

Услови који су на располагању трећим странама садрже обавезе треће стране. Када се трећа страна ослања на токене временског жига издате од стране Пошта *TSA*, треба да:

- провери да ли је токен временског жига исправно електронски потписан/печатиран и да сертификат којим се проверава потпис/печат токена временског жига није опозван до тренутка провере,
- узме у обзир сва ограничења о коришћењу временског жига која су назначена у политици и практичним правилима издавања временског жига,
- узме у обзир било које друге мере потписане у споразумима (уговорима) или другим документима.

Сваки издати токен временског жига садржи електронски сертификат, којим се проверава електронски потпис/печат токена временског жига.

За проверу опозваности електронског сертификата токена временског жига користи се регистар опозваних сертификата или OCSP сервис, доступан као услуга Сертификационог тела Поште, у складу са Политиком сертификације и Практичним правилима пружања услуге сертификације Сертификационог тела Јавног предузећа „Пошта Србије“, Београд за квалификоване електронске сертификате са новог система.

6.4. Одговорност

Пошта *TSA* неће бити одговоран за питања које се налазе изван Пошта *TSA* сфере утицаја и одговорности.

Пошта *TSA* биће одговоран само у складу са законом и правилима оперативног рада издаваоца временског жига.

Спорови између Пошта *TSA*, корисника и треће стране прво се решавају договором, а уколико то није могуће, надлежан је суд у Београду.

Пошта *TSA* имплементира контроле испуњавања услова пружања услуге, у складу са овим практичним правилима.

Пошта *TSA* бележи и безбедно чува, уз обезбеђену тајност, све релевантне податке који се тичу издавања временских жигова, у периоду од најмање 1 године од издавања, ради обезбеђивања доказа о издатим токенима временског жига.

Пошта *TSA* врши оперативни рад у складу са овим практичним правилима и нивоом услуге који је уговорен са корисницима. Пошта *TSA* неће давати додатне изјаве или гаранције које се односе на доступност или тачност услуге издавања временског жига.

7. УСЛОВИ ЗА ПРАВИЛА ОПЕРАТИВНОГ РАДА ПОШТА *TSA*

Пошта *TSA* пружа услугу издавања временског жига коришћењем две јединице за формирање временског жига, које се налазе у *load balancer* конфигурацији.

7.1. Изјава о правилима оперативног рада и општим условима

7.1.1. Изјава о правилима оперативног рада издаваоца временског жига

Садржај изјаве о правилима оперативног рада уграђен је у ова практична правила, поглавље 6.1.1. и даље.

7.1.2. Изјава о општим условима издавања временског жига

Општи услови су посебан документ чији је део уграђен у одговарајућа поглавља ових практичних правила. Структура и садржај токена временског жига дефинисан је у поглављу 7.3.1. Обавезе корисника и треће стране, укључујући и начин провере токена временског жига, наведене су у поглављима 6.2. и 6.3. ових практичних правила. Обавезе и одговорност Пошта *TSA* наведене су у поглављима 6.1. и 6.4. ових практичних правила.

7.2. Животни циклус кључева јединице за формирање временског жига

7.2.1. Генерисање кључева

Асиметрични парови кључева јединице за формирање временског жига Пошта *TSA* за електронски потпис/печат формираних токена временског жига, увек су генерисани под контролисаним условима.

Детаљан опис:

- генерисање кључева јединице за формирање временског жига Пошта *TSA* за потписивање/печатирање биће извршено у физички обезбеђеној средини (видети поглавље 7.4.4.) од стране најмање две особе са поверљивим улогама (видети поглавље 7.4.3.),
- генерисање кључева јединице за формирање временског жига Пошта *TSA* за потписивање/печатирање биће извршено у оквиру хардверског криптографског модула који је сертификован у складу са сигурносним критеријумом *EAL* 4+.
- кључеви јединице за формирање временског жига Пошта *TSA* су *RSA* кључеви дужине 2048 бита.

7.2.2. Заштита приватног кључа

Пошта *TSA* ће обезбедити да приватни кључеви јединице за формирање временског жига остану тајни и сачувају свој интегритет.

Детаљан опис:

- приватни кључеви јединице за формирање временског жига Пошта *TSA* за потписивање/печатирање биће чувани и коришћени у хардверском криптографском модулу, који је сертификован у складу са сигурносним критеријумом *EAL* 4+,
- неће бити прављене копије приватних кључева јединице за формирање временског жига Пошта *TSA* за потписивање/печатирање у отвореном облику изван хардверског криптографског модула.

7.2.3. Дистрибуција јавног кључа

Пошта *TSA* доставља надлежном министарству електронске сертификате за електронски потпис/печат токена временског жига који садрже јавни кључ за проверу потписа/печата, у циљу објављивања у Јавној листи квалификованих услуга од поверења.

Пошта *TSA* осигурава да дистрибуирани електронски сертификати сачувају свој интегритет и веродостојност током дистрибуције.

7.2.4. Обнављање кључева

На највише сваких годину дана Пошта *TSA* ће генерисати нови асиметрични пар кључева за потписивање/печатирање токена временског жига.

7.2.5. Крај животног циклуса приватног кључа

Пошта *TSA* ће осигурати да се приватни кључеви јединице за формирање временског жига не користе после истека планиране употребе. Приватни кључ биће замењен пре истека планиране употребе, што ће означити престанак употребе кључа, а замењени приватни кључ биће трајно уништен.

Уколико истекне период планиране употребе приватног кључа од једне године, Пошта *TSA* неће издавати токене временског жига, све док истекли приватни кључ не буде замењен новим приватним кључем.

7.2.6. Управљање хардверским криптографским модулом

Пошта *TSA* ће током рада осигурати заштиту хардверског криптографског модула, у коме се креирају и чувају кључеви јединице за формирање временског жига за потписивање/печатирање и у коме се обавља потписивање/печатирање формираног токена временског жига.

Пре премештања или другог нарушавања безбедног окружења хардверског криптографског модула, Пошта *TSA* ће престати да користи и трајно ће уништити приватне кључеве јединице за формирање временског жига.

7.3. Издавање временског жига

7.3.1. Структура података временског жига

Пошта *TSA* осигурава да токен временског жига буде издат на сигуран начин и да садржи тачно време.

Пошта *TSA* издаје само једну врсту токена временског жига, у складу са овим практичним правилима. Сваки токен садржи идентификациони број Политике издавања временског жига (*OID*) и јединствени серијски број издатог токена.

Токен је електронски потписан/печатиран приватним кључем јединице за формирање временског жига Пошта *TSA*. Пошта *TSA* за формирање електронског потписа/печата токена временског жига користи *RSA* алгоритам применом стандарда *PKCS#*1, уз дужину *RSA* кључа од 2048 бита. Токен садржи електронски сертификат којим се проверава електронски потпис/печат токена временског жига.

Токен садржи *UTC* време преузето из извора тачног времена, упоредиво са *UTC* тачним временом, уз максимално дозвољено одступање у односу на *UTC* тачно време како је прописано овим практичним правилима. Пошта *TSA* не издаје токене са већом тачношћу.

Очекивано време важења токена временског жига одређено је роком важења електронског сертификата, којим се проверава електронски потпис/печат токена временског жига.

7.3.2. Синхронизација времена са *UTC*

Пошта *TSA* ће осигурати да време, у издатим токенима временског жига, одступа највише ±1 секунду, у односу на *UTC* тачно време и неће издавати временске жигове изван наведене тачности.

Пошта *TSA* обезбеђује аутоматску синхронизацију времена јединице за формирање временског жига Пошта *TSA* са извором тачног времена, у складу са предвиђеном прецизношћу. Пошта *TSA* користи извор тачног времена са *NTP* (*Network Time Protocol*) синхронизацијом, а *NTP* синхронизација се врши са *Stratum* 1 и 2 серверима.

Уколико дође до губитка синхронизације времена јединице за формирање временског жига Пошта *TSA* са извором тачног времена, Пошта *TSA* ће престати да издаје токене временског жига, до постизања синхронизације.

Синхронизација времена јединице за формирање временског жига Пошта *TSA* вршиће се тако да се не очекује одступање веће од декларисане тачности.

Извор тачног времена, на који се временски синхронизује јединица за формирање временског жига Пошта *TSA*, биће заштићен од напада и обезбеђен од препознатих ризика који могу да доведу до неадекватних промена.

7.4. Управљање и рад издаваоца временског жига

7.4.1. Управљање безбедношћу

Управљање безбедношћу Пошта *TSA* врши се у складу са одговарајућим стандардима заштите.

Целокупна инфраструктура Пошта *TSA* осигурана је системом физичке и логичке заштите.

Целокупан опис инфраструктуре Пошта *TSA*, начина и поступка заштите наведен је у интерним правилима Пошта *TSA*.

7.4.2. Процена ризика

Пошта *TSA* ће осигурати да сва опрема има адекватан ниво заштите. Процена ризика је неопходна да би се евидентирала пословна средства и претње којима су та средства угрожена, како би се одредиле неопходне сигурносне контроле и процедуре. Пошта *TSA* ће периодично

вршити процену ризика, вршити класификацију средстава и ревизију сигурносних контрола и процедура.

7.4.3. Кадровски капацитет

Пошта *TSA* ће осигурати да особље поседује потребно знање и искуство, у складу са својом улогом.

Пошта *TSA* додатно обезбеђује:

- поверљиве улоге и одговорности су документоване у описима радних места Пошта *TSA* особља,
- у описима послова Пошта *TSA* особља, раздвојеност дужности је дефинисана, наведене су потребне вештине и искуство, а адекватан ниво знања, образовања и обуке за коришћење информатичке опреме пружен је запосленима,
- особље Пошта *TSA* спроводи администраторске процедуре у складу са правилима оперативног рада,
- особље Пошта *TSA* са поверљивим улогама нема сукоб интереса са делатношћу Пошта *TSA*,
- особље Пошта *TSA* похађа обуке за обнављање и усавршавање знања најмање једанпут годишње,
- особље Пошта *TSA* чине особе које нису осуђиване.

7.4.4. Физичко обезбеђење

Пошта *TSA* осигурава да је физички приступ инфраструктури за издавање временског жига контролисан:

- физички приступ је дозвољен само ауторизованом особљу,
- уведене су интерним правилима дефинисане процедуре контроле приступа за спречавање губитка, оштећења или компромитовања инфраструктуре, крађе података и нарушавање пословног процеса,
- уведене су интерним правилима дефинисане процедуре контроле приступа хардверском криптографском модулу, у складу са сигурносним захтевима за генерисање и чување кључева,
- инфаструктура Пошта *TSA* је у сервер сали, која физички штити сервере од неовлашћеног приступа и не дели се са другим организацијама,
- опрема, подаци, медији и софтвер Пошта *TSA* не могу да се изнесу из просторија Пошта *TSA* без одговарајућег одобрења.

7.4.5. Управљање опертивним радом

Пошта *TSA* ће осигурати да компоненте за издавање временског жига буду заштићене и да исправно функционишу, са минималним ризиком од квара.

Детаљан опис:

- интегритет Пошта *TSA* је заштићен од вируса и недозвољеног софтвера,
- примењује се сигурно руковање са медијима коришћеним у оквиру Пошта *TSA*, како би се медији заштитили од оштећења, крађе и неовлашћеног приступа,
- успостављене су и имплементиране процедуре за све поверљиве и администраторске улоге, које учествују у обављању Пошта *TSA* услуга,
- Пошта *TSA* сигурносне улоге су раздвојене од осталих улога,
- капацитети се прате и предвиђају, како би се обезбедило да довољна процесорска снага и смештајни капацитети буду на располагању,

- уведено је извештавање о сигурносним инцидентима, а процедуре реаговања су такве да штета од сигурносних инцидената буде минимална,
- Пошта *TSA* реагује брзо на сигурносне инциденте, како би се ограничио утицај инцидената, а у најкраћем року биће сачињен извештај о сваком сигурносном инциденту.

7.4.6. Контрола приступа

Пошта *TSA* ће обезбедити приступ само овлашћеним особама:
- заштита интерне мреже Пошта *TSA* од неовлашћеног приступа извршена је употребом *firewall* и *IPS* (*Intrusion Prevention System*) система,
- Пошта *TSA* ће осигурати ефективну администрацију корисничких налога за приступ систему, како би се обезбедио потребан ниво заштите,
- приступ подацима и апликацијама ограничен је у складу са политиком контроле приступа,
- особље Пошта *TSA* биће идентификовано помоћу сертификата за аутентификацију пре администрације критичних апликација,
- евидентирају се све активности Пошта *TSA* особља,
- Пошта *TSA* локалне мрежне компоненте (*firewall, load balancer, switch*) се чувају у сервер сали, у физички заштићеном окружењу. Њихова конфигурација се периодично проверава, у складу са захтевима.

7.4.7. Безбедно окружење

Пошта *TSA* користи проверене и сигурне системе који су заштићени од модификација:
- анализа сигурносних захтева биће извршена у процесу пројектовања и спецификације захтева, за било који развојни пројекат, како би се обезбедила сигурна имплементација у Пошта *TSA* систем,
- контрола промена биће употребљена за све верзије, модификације и хитне измене на коришћеним апликацијама.

7.4.8. Компромитовање услуге издавања временског жига

У случају компромитовања или сумње у компромитовање свог приватног кључа или поремећаја система калибрације и синхронизације са извором тачног времена, Пошта *TSA*:
- престаје са издавањем временских жигова,
- информише све кориснике и друге заинтересоване стране о компромитацији и другим догађајима,
- јавно објављује информације о томе како установити који временски жигови нису важећи, на начин да се не угрози заштита података о личности.

7.4.9. Престанак рада издаваоца временског жига

Пошта *TSA* ће обезбедити да у случају престанка рада потенцијална штета корисницима и трећим странама буде минимална, као и да се одржи могућност провере исправности издатих токена временског жига.

Пре престанка рада, Пошта *TSA* ће:
- обавестити све кориснике о престанку рада,
- поузданој организацији пренети обавезу чувања свих релевантних података неопходних за доказивање исправности издатих токена временског жига, у временском периоду који је прописан законом,

- поузданој организацији пренети обавезу да електронски сертификат који садржи јавни кључ за проверу потписа/печата издатих токена временског жига буде расположив свим заинтересованим странама, у временском периоду који је прописан законом,
- уништити приватни кључ јединице за формирање временског жига.

7.4.10. Усклађеност са законским оквиром

Пошта *TSA* ће осигурати усклађеност са законским оквиром Републике Србије, а нарочито прописима који се односе на издавање временског жига, заштиту интелектуалне својине, приватност и заштиту личних података корисника.

7.4.11. Чување података о раду услуге издавања временског жига

Пошта *TSA* ће осигурати да се сви релевантни подаци у вези издатог токена временског жига чувају у периоду од најмање једне године од датума издавања токена, тако што ће бити:
- записани и безбедно архивирани сви догађаји и подаци у вези рада Пошта *TSA*,
- одржавана поверљивост и интегритет актуелних и архивираних записа у вези рада Пошта *TSA*,
- комплетно и поверљиво сачувани записи у вези рада Пошта *TSA* сервиса,
- доступни записи у вези рада Пошта *TSA* сервиса, уколико је потребно доказати правилно функционисање Пошта *TSA* сервиса за потребе судског поступка,
- забележено тачно време значајних промена у окружењу, управљања кључевима и синхронизације времена,
- чувани записи у вези Пошта *TSA* сервиса, довољно дуго, после истека важења *TSA* сертификата, ради могућности пружања одговарајућег правног доказа,
- чувани записи догађаја, на начин који обезбеђује да се не могу лако обрисати или уништити,
- поверљиво чувани сви подаци о корисницима, осим уколико се са корисником договори да подаци могу да буду јавно објављени,
- записани догађаји који се тичу:
- животног циклуса Пошта *TSA* кључева за потписивање/печатирање и сертификата,
- синхронизације времена јединице за формирање временског жига Пошта *TSA* са извором тачног времена,
- губитка синхронизације времена јединице за формирање временског жига Пошта *TSA* са извором тачног времена.

7.5. Организација

Пошта *TSA* ће обезбедити да је организација рада сигурна:
- Политика и процедуре по којима Пошта *TSA* функционише неће бити дискриминаторске,
- Пошта *TSA* ће своје услуге пружити свима у оквиру дефинисаног опсега своје делатности,
- Пошта *TSA* је део Јавног предузећа „Пошта Србије“, Београд,
- Пошта *TSA* има финансијску стабилност и ресурсе потребне да послује у складу са овим практичним правилима,
- Пошта *TSA* запошљава довољан број особља, које поседује потребно образовање, обуку и техничко знање да пружа услугу издавања временског жига,
- Пошта *TSA* је правилно документовао све споразуме и уговоре.

8. ОСТАЛЕ ОДРЕДБЕ

Пошта *TSA* наплаћује издавање временских жигова на основу ценовника, који је објављен на веб сајту Пошта *TSA* и који је доступан на захтев свим заинтересованим лицима.

Пошта *TSA* дужно је да се у свом пословању придржава одредби закона којим се уређује заштита података о личности.

Пошта *TSA* гарантује пружање услуге издавања временског жига, у складу са прописима, овим практичним правилима и другим општим актима Поште, који су усклађени са прописима Републике Србије.

Пошта *TSA* има обавезу да обезбеди услове за поуздано пружање услуге, а нарочито:

- ресурсе потребне за издавање временског жига у складу са објављеним општим условима, политиком и практичним правилима издавања временског жига,
- доступност својих услуга свим корисницима чије су активности у складу са политиком и практичним правилима издавања временског жига,
- заштиту личних података корисника,
- ефикасно поступање у решавању рекламација и спорова са корисницима или другим заинтересованим странама у вези издавања временског жига.

Корисник је обавезан да поступа у складу са прописима и уговором који је закључен у складу са прописима.

Пошта *TSA* признаје права корисника која су у складу са прописима.

Пошта *TSA* дужно је да чува доказе о томе да је поступало у складу са прописима.

Корисник је одговоран за штету која је настала његовом кривицом.

Корисник није одговоран за штету, ако докаже да је поступао у складу са законом, подзаконским актима и закљученим уговором.

Сви спорови између Пошта *TSA*, корисника и трећег лица биће решавани договором, а у случајевима када то није могуће, спор ће решавати надлежни суд у Београду.

Пошта *TSA* се ослобађа одговорности за било коју штету причињену кориснику, другом учеснику или трећем лицу, приликом пружања услуге издавања временског жига, уколико је до штете дошло услед разлога који су изван контроле Пошта *TSA*, односно, услед више силе.

Ова практична правила и друга акта објављују се на српском језику.

Ова практична правила ступају на снагу осмог дана од дана објављивања у „Службеном ПТТ - гласнику“ и објављују се и на веб сајту Поште *TSA*.

ВРШИЛАЦ ДУЖНОСТИ ДИРЕКТОРА
ЈАВНОГ ПРЕДУЗЕЋА „ПОШТА СРБИЈЕ“,
БЕОГРАД

Зоран Ђорђевић