РЕПУБЛИКА СРБИЈА
ВЛАДА РЕПУБЛИКЕ СРБИЈЕ
КАНЦЕЛАРИЈА ЗА ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ
И ЕЛЕКТРОНСКУ УПРАВУ

Практична правила пружања услуге издавања квалификованог електронског временског жига

Назив	Практична правила пружања услуге издавања квалификованог електронског временског жига
Верзија документа	1.0
Датум објављивања документа	28. мај 2021. године
Рок важности	Документ је важећи до следећег издања

Садржај

На основу члана 31. Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС“, бр. 94/17 и 52/21) и члана 4. став 1. Правилника о ближим условима за квалификоване електронске временске жигове („Службени гласник РС“, број 59/19), директор Канцеларије за информационе технологије и електронску управу доноси

ПРАКТИЧНА ПРАВИЛА ПРУЖАЊА УСЛУГЕ ИЗДАВАЊА КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ВРЕМЕНСКОГ ЖИГА

1. Увод и преглед основних претпоставки

1.1 Увод

Овим документом дефинишу се практична правила пружања услуге издавања квалификованог електронског временског жига од стране Канцеларије за информационе технологије и електронску управу.

Структура и садржај овог документа је у складу са стандардом ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps, укључујући захтеве из других стандарда на које се из тог стандарда директно и индиректно упућује, а који се односе на политику издавања временских жигова.

Канцеларија за информационе технологије и електронску управу (у даљем тексту: Канцеларија), као служба Владе у чијој је надлежности обављање стручних послова који се односе на пројектовање, усклађивање, развој и функционисање система електронске управе, је регистровани издавалац временског жига сагласно Закону о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС“, бр. 94/17 и 52/21). Канцеларија је регистровани пружалац услуге у складу са ЕУ уредбом која се односи на електронску идентификацију у услуге од поверења за електронске трансакције на унутрашњем тржишту (видети члан 3. тачка 20), као тело које издаје токене временског жига.

Канцеларија је изградила инфраструктуру за издавање квалификованих електронских временских жигова за потребе државних органа, органа локалне самоуправе и јавних служби Републике Србије. Услуге намењене трећој страни, везане за проверу издатих квалификованих електронских временских жигова и приступ јавним информацијама о раду издаваоца електронских временских жигова су слободно доступне свим заинтересованима у складу са правима и обавезама наведеним у овом документу.

1.2 Основне претпоставке

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

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

Канцеларија за потписивање формираних токена временског жига користи електронске сертификате које издаје Јавно предузеће „Пошта Србије“ – Сертификационо тело Поште у складу са политиком издавања сертификата и правилима сертификације које објављује тај пружалац квалификованих услуга од поверења.

2. Појмови који се користе у документу

Поједини појмови који се користе у овом документу имају следеће значење:

- **издавалац временског жига** је тело које издаје временски жиг;
- **корисник** је правно или физичко лице, које користи услуге издаваоца временског жига, које је изричито или подразумевано прихватило прописе и услове издаваоца временског жига;
- **политика издавања временског жига (енгл. Time-stamp Policy)** је скуп правила који показује да је издавање временских жигова у складу са одређеним захтевима и прописима;
- **структура података временског жига - токен временског жига (енгл. Time-stamp Token)** је објекат који повезује репрезентацију података са одређеним временом и на тај начин доказује да је податак постојао пре тог времена (у даљем тексту: токен временског жига);
- **практична правила услуге издавања временских жигова (енгл. Practice Statement)** је скуп правила којима су дефинишу оперативне процедуре у циљу испуњења захтева које треба да испуњава услуга издавања квалификованих електронских временских жигова, тј. начин на који пружалац услуге издавања квалификованих електронских временских жигова испуњава техничке, организационе и процедуралне захтеве пословања који су одређени у политици издавања временских жигова;
- **криптографски отисак (енгл. hash)** је хеш вредност електронског документа која се формира коришћењем криптографских хеш алгоритама;
- **јединица временског жига** је криптографско средство за формирање временског жига којим се генерише и електронски потписује токен временског жига издат у име издаваоца временског жига;
- Канцеларија за информационе технологије и електронску управу као издавалац временског жига у даљем тексту се означава: Канцеларија (RS-GOV TSA).

3. Назив документа и идентификација

Овај документ описује практична правила пружања услуге издавања квалификованог електронског временског жига Канцеларије као издаваоца временског жига (RS-GOV TSA) и дефинише скуп правила који показује да је издавање квалификованих електронских временских жигова у складу са одређеним захтевима и прописима издавања жига, као и управљање процесима који обезбеђују да корисници и трећа лица могу имати пуно поверење у рад сервиса за издавање временског жига.

Практична правила пружања услуге издавања квалификованог електронског временског жига Канцеларије (RS-GOV TSA) је 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 одређени подаци постојали и пре одређеног времена.

Примарни извор овог документа се налази на веб презентацији Канцеларије https://www.ite.gov.rs/tekst/6058/vremenski-zig.php

Назив	Практична правила пружања услуге издавања временског жига Канцеларије за информационе технологије и електронску управу
Верзија	1.1
Датум	28. мај 2021. године
Рок важности	Документ је важећи до следећег издања

Документу је додељен јединствени идентификатор:

OID	1.3.6.1.4.1. 55016.1.1.0 {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1 Канцеларија за информационе технологије и електронску управу (55016) timestamp policy (1) version (1) subversion (0)}

Канцеларија (RS-GOV TSA) за потписивање формираних токена квалификованог електронског временског жига користи електронске сертификате које издаје Јавно предузеће „Пошта Србије“ – Сертификационо тело Поште у складу са политиком издавања сертификата и правилима сертификације које објављује тај пружалац квалификованих услуга од поверења.

У циљу доказивања усклађености, Канцеларија (RS-GOV TSA):

- испуњава своје обавезе као што је дефинисано у поглављу 6.1 овог документа;
- имплементира контроле који испуњавају услове наведене Практичним правилима;
- подлеже провери испуњености услова за регистрацију издаваоца временског жига и провери оперативног рада издаваоца квалификованог електронског временског жига.

Канцеларија (RS-GOV TSA) утврђује опште услове пружања услуге издавања квалификованог електронског временског жига (у даљем тексту: општи услови). којима се одређују:

1. Политика издавања временског жига;
2. Практична правила.

Општи услови за пружање услуге су доступни свим корисницима услуга и поуздајућим странама у овом документу и у документу Политика пружања услуге издавања квалификованог електронског временског жига, а који су објављени су на веб презентацији Канцеларије (RS-GOV TSA).

Политика издавања квалификованог електронског временског жига наводи „шта ће се поштовати”, док практична правила пружања услуге издавања квалификованог електронског временског жига од стране Канцеларије (RS-GOV TSA) (у даљем тексту: Практична правила) одређују „како се поштују“, односно опис процеса које ће издавалац користити при формирању временског жига и како ће одржавати синхронизацију са извором тачног времена.

Практична правила прилагођена су организационој структури, оперативним процедурама, ресурсима и рачунарском окружењу Канцеларије (RS-GOV TSA).

3.1 Администрација Практичних правила

Канцеларија (RS-GOV TSA) је одговорна је за периодичан преглед и ажурирање овог документа у којем су дефинисана Практична правила, као и ванредне промене одговарајућих

одредби које проистичу из евентуалних промена у законској регулативи или техничким карактеристикама временског жига.

Овај документ се редовно периодично прегледа и по потреби ажурира. Интерном процедуром се дефинише период прегледа, а који не може бити ређи од једном у току календарске године.

Према датој интерној процедури, овај документ се може ажурирати и чешће него једном годишње уколико се за то стекну услови. Такви услови се односе, између осталог, и на ванредне промене у законској регулативи.

3.1.1 Контакт особа

Контакт подаци особе Канцеларије (RS-GOV TSA) за документ Практична правила пружања услуге издавања квалификованог електронског временског жига: jovana.bujosevic@ite.gov.rs

4. Правни основ

Пружање услуге издавања квалификованог електронског временског жига усклађено је са:

- Законом о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС“, бр. 94/17 и 52/21);
- Правилником о ближим условима за квалификоване електронске временске жигове („Службени гласник РС“, број 59/19);
- Законом о заштити података о личности[1].

5. Учесници

5.1 Пружалац услуге

Канцеларија (RS-GOV TSA) регистровани је пружалац услуге издавања квалификованог електронског временског жига.

Пружалац услуге обезбеђује техничке и безбедносне услове и успоставља хијерархијску и организациону структуру за безбедно и континуирано пружање наведене услуге.

Канцеларија користи услуге Јавног предузећа „Пошта Србије“ – Сертификационо тело Поште као пружаоца услуге издавања квалификованих електронских сертификата у Републици Србији.

Приватни кључеви који су коришћени за генерисање токена временског жига су увек власништво Канцеларије (RS-GOV TSA).

Процес издавања временског жига је за потребе овог документа 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 Политике издавања квалификованог електронског временског жига. На пример, део за управљање издавањем гарантује да време уписано у издати временски жиг правилно синхронизовано са извором тачног времена.

[1] Закон о заштити података о личности, „Службени гласник РС“, број 87/18

5.2 Корисник

Корисник може бити организација, која обухвата неколико крајњих корисника или појединачни крајњи корисник. Када је корисник организација, обавезе које се примењују на ту организацију ће се примењивати и на крајње кориснике. При том је организација одговорна уколико крајњи корисници правилно не испуне своје обавезе јер се од организације очекује да на одговарајући начин обавести крајње кориснике.

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

Канцеларија (RS-GOV TSA) пружа услугу издавања квалификованог електронског временског жига за потребе државних органа, органа локалне самоуправе и портала електронске управе Републике Србије.

Коришћењем услуге Канцеларије (RS-GOV TSA) корисници имплицитно прихватају обавезе одређене овом политиком.

6. Обавезе и одговорности

6.1 Обавезе и одговорности пружаоца услуге

6.1.1 Администрирање Политике издавања квалификованог електронског временског жига, Практичних правила

Канцеларија (RS-GOV TSA) усваја и примењује Политику издавања квалификованог електронског временског жига и Практична правила, у складу са прописима и домаћим и међународним стандардима у области електронских временских жигова, као и Политику приватности у складу са прописима Републике Србије.

Политику издавања квалификованог временског жига, практична правила и политику приватности, Канцеларија (RS-GOV TSA) објављује на веб презентацији пружаоца услуге (https://ite.gov.rs/).

Канцеларија (RS-GOV TSA) је одговорна је за периодичан преглед и ажурирање Практичних правила, као и ванредне промене одговарајућих одредби које проистичу из евентуалних промена у законској регулативи или техничким карактеристикама временског жига.

6.1.2 Обезбеђивање услова дефинисаних Практичним правилима

Канцеларија (RS-GOV TSA) дефинише скуп правила којима су описане оперативне процедуре у циљу испуњења захтева које треба да испуњава услуга издавања квалификованих електронских временских жигова, тј. начин на који пружалац услуге издавања квалификованих електронских временских жигова испуњава техничке, организационе и процедуралне захтеве пословања који су одређени у Политици пружања услуге издавања временских жигова и обезбеђује да сва наведена правила буду имплементирана у складу са наведеном политиком.

Ова Практична правила садрже процедуре које се односе на изјаву о правилима рада и општим условима, животни циклус приватног кључа јединице временског жига, издавање временског жига, управљање квалификованим електронским временским жигом и организацију рада Канцеларије (RS-GOV TSA) у вези са пружањем услуге.

6.1.3 Обавезе према корисницима

Канцеларија (RS-GOV 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 више силе, односно других догађаја, природних или

друштвених, који нису под контролом нити су могли бити предвиђени, отклоњени или спречени од стране Канцеларије (RS-GOV TSA). Планирани периоди одржавања објављују се на веб презентацији Канцеларије.

Осим наведеног, Канцеларија (RS-GOV TSA):

- имплементира и користи поуздану инфраструктуру за размену информација и комуникацију;
- чува све релевантне податке који се тичу издавања временских жигова у временском периоду у складу са прописима о временском жигу;
- поштује робне марке и интелектуалну својину;
- пружа своје услуге издавања временског жига у складу са опште прихваћеним стандардима и овом политиком;
- издаје само тачне временске жигове, примењујући правила оперативног рада на начин који је описан у Практичним правилима.

6.1.4 Одговорност пружаоца услуге

Канцеларија (RS-GOV TSA) обавља оперативни рад у складу са Практичним правилима и нивоом услуге уговореним са корисницима. Канцеларија (RS-GOV TSA) неће давати додатне изјаве или гаранције које се односе на доступност или тачност услуга временског жига.

Канцеларија (RS-GOV TSA) неће бити одговорна за питања које се налазе изван своје сфере утицаја и одговорности.

Канцеларија (RS-GOV TSA) ће бити одговорна у складу са законом и правилима оперативног рада издаваоца временског жига.

Ако не постоји могућност споразумног решавања евентуалних спорова, за решавање тих спорова надлежан је одговарајући суд у Београду.

Канцеларија (RS-GOV TSA) спроводи контроле испуњености услова пружања услуге у складу са овом политиком.

Канцеларија (RS-GOV TSA) бележи и на безбедан начин чува све релевантне податке који се тичу издавања временских жигова у периоду од најмање 10 година од издавања, ради обезбеђивања доказа о издатим токенима временског жига. Приликом бележења и чувања, Канцеларија (RS-GOV TSA) обезбеђује и тајност наведених података.

6.2 Обавезе и одговорности корисника

Захтев за формирање временског жига обавезно садржи захтев за укључивање сертификата којим се проверава потпис токена временског жига и других сертификата у формираном токену, као и Изјаву о Практичним правилима којом корисник потврђује да је упознат са условима наведеним у овом документу.

За формирање криптографског отиска података у захтеву за формирање временског жига користи се алгоритам SHA-256 (Secure Hash Algorithm), OID 2.16.840.1.101.3.4.2.1.

Захтев за формирање временског жига садржи ознаку ове политике.

Приликом добијања токена временског жига, корисник ће проверити да је токен временског жига исправно потписан и да сертификат којим се проверава потпис токена временског жига није повучен до тог тренутка. У одељку 6.3 овог документа наведен је препоручени поступак провере исправности формираног токена временског жига.

Додатни захтеви могу бити уговорени између Канцеларије (RS-GOV TSA) и корисника.

6.3 Обавезе трећих страна

Обавеза треће стране је да, када се ослања на издате токене временског жига од стране Канцеларије (RS-GOV TSA), провери валидност електронског потписа временског жига и увери се у исправност токена временског жига.

Услови који су на располагању трећим странама садрже обавезе треће стране да, када се ослања на временске жигове издате од стране Канцеларије (RS-GOV TSA):

- провери је ли временски жиг исправно потписан и да сертификат којим се проверава електронски потпис временског жига није повучен до тренутка верификације и
- узме у обзир било какво ограничење о коришћењу временског жига које је назначено у политици издавања временског жига.

Трећа страна на веб презентацији Канцеларије (RS-GOV TSA) може добити информацију о активном периоду употребе приватног потписног кључа придруженог сертификату.

Сваки издати токен временског жига садржи јавни сертификат којим се проверава електронски потпис и сертификате из пуне путање сертификације.

За проверу електронског потписа токена временског жига користи се регистар опозваних сертификата и сервис опозваности доступан као услуга пружаоца квалификоване услуге од поверења Јавно предузеће „Пошта Србије“ – Сертификационо тело Поште у складу са политиком тог сертификационог тела.

7. Дозвољена употреба

Услуга издавања квалификованог електронског временског жига од стане Канцеларије (RS-GOV TSA) користи се за потврђивање постојања електронских података у одређеном временском тренутку на поверљив и проверљив начин. Електронски подаци оверени временским жигом се не могу непримећено мењати.

8. Услови за Практична правила

8.1 Изјава о Практичним правилима

Захтев за формирање временског жига обавезно садржи и Изјаву о Практичним правилима којом корисник потврђује да је упознат са условима наведеним у овом документу.

8.2 Животни циклус приватног кључа јединице временског жига

8.2.1 Креирање кључа

Асиметрични пар кључева јединице временског жига Канцеларије (RS-GOV TSA) за електронски потпис формираних токена су увек генерисани под контролисаним условима.

Детаљан опис:

- генерисање потписних кључева јединице временског жига ће бити извршено у физички обезбеђеној средини (видети одељак 8.4.4 овог документа) од стране особља са поверљивим улогама (видети одељак 8.4.3 овог документа), под најмање двојном контролом.

- генерисање потписних кључева јединице временског жига ће бити извршена у оквиру хардверског модула заштите који је сертификован у складу са EAL 4+ или вишим критеријумом.
- дужина потписних кључева и алгоритам коришћен за потписивање токена временског жига према овом документу су наведени у одељку 6.2 овог документа.

8.2.2 Заштита тајног кључа

Канцеларија (RS-GOV TSA) обезбеђује да приватни кључеви јединице временског жига остану тајни и сачувају свој интегритет.

Детаљан опис:

- приватни потписани кључеви Канцеларије (RS-GOV TSA) се чувају и користе у хардверском модулу заштите који је сертификован у складу са EAL 4+ или вишим сигурносним критеријумима;
- не праве се копије приватних кључева за потписивање Канцеларије (RS-GOV TSA).

8.2.3 Дистрибуција јавног кључа

Канцеларија (RS-GOV TSA) објављује издате сертификате за електронски потпис који садрже јавни кључ за верификовање потписа, као и све зависне параметре укључујући и период активног коришћења на веб презентацији Канцеларије путем везе https://www.ite.gov.rs/tekst/94/vremenski-zig.php.

Канцеларија (RS-GOV TSA) осигурава доступност ових података, као и чување интегритета и веродостојности објављених података током дистрибуције заинтересованим лицима.

8.2.4 Обнављање кључа

На највише годину дана Канцеларија (RS-GOV TSA) генерише нови пар потписних кључева и подноси захтев за издавање новог сертификата.

8.2.5 Престанак коришћења кључа

Канцеларија (RS-GOV TSA) осигурава да се приватни кључеви не користе након истека планиране употребе. Ако се приватни кључ јединице временског жига замени пре истека планиране употребе, означава се престанак употребе кључа, након чега се кључ трајно уништава.

Уколико период планиране употребе приватног кључа истекне, Канцеларија (RS-GOV TSA) не издаје токене временског жига.

8.2.6 Управљање хардверским модулом заштите

Канцеларија (RS-GOV TSA) током употребе осигурава заштиту хардверског модула заштите у коме се креирају и чувају потписни кључеви јединице временског жига и обавља потписивање формираног временског жига.

Пре премештања или другог нарушавања безбедног окружења хардверског модула заштите, Канцеларија (RS-GOV TSA) престаје да користи и трајно уништава приватне кључеве јединице временског жига.

8.3 Издавање временског жига

8.3.1 Структура података временског жига

Канцеларија (RS-GOV TSA) осигурава да токен временског жига буде издат на сигуран начин и да садржи тачно време.

Канцеларија (RS-GOV TSA) издаје само једну врсту токена временског жига, у складу са овим документом. Сваки токен садржи OID ознаку документа политике, како је наведено у одељку 6.2 овог документа и јединствени идентификатор издатог токена.

Канцеларија (RS-GOV TSA) захтева од корисника коришћење криптографског отиска података по SHA-256 алгоритму у захтеву за издавање временског жига који је дефинисан у документу FIPS 180-2 „Secure Hash Standard“. Токен садржи достављени криптографски отисак електронског документа који ће бити оверени временском жигом.

Токен садржи идентификујући назив јединице временског жига Канцеларија (RS-GOV TSA) која је издала временски жиг.

Токен је електронски потписан приватним кључем јединице временског жига Канцеларије (RS-GOV TSA). Канцеларија (RS-GOV TSA) за формирање електронског потписа токена временског жига користи RSA алгоритам применом стандарда PKCS#1 уз дужину RSA модулуса n од 2048 бита, коришћењем SHA-256 алгоритма за рачунање криптографског отиска. Ознака у профилу сертификата којим се проверава електронски потпис гласи sha256WithRSAEncryption. Токен садржи сертификат којим се проверава електронски потпис и пуну путању сертификације.

Токен садржи UTC време преузето из јединице временског жига упоредиво са UTC тачним временом, уз максимално дозвољено одступање у односу на тачно UTC време како је прописано Политиком пружања услуге издавања квалификованог временског жига. Канцеларија (RS-GOV TSA) не издаје токене са већом тачношћу.

Очекивано време важења временског жига одређено је роком важења издатог сертификата којим се проверава електронски потпис токена временског жига.

8.3.2 Синхронизација времена

Канцеларија (RS-GOV TSA) осигурава да време у издатим токенима временског жига одступа највише ±1 секунду у односу на UTC тачно време и не издаје временске жигове ван наведене тачности.

Канцеларија (RS-GOV TSA) обезбеђује аутоматску синхронизацију времена јединице временског жига са извором тачног временом у складу са предвиђеном прецизношћу.

Канцеларија (RS-GOV TSA) користи извор тачног времена који обезбеђује орган у саставу органа државне управе који је надлежан за дистрибуцију времена – Дирекција за мере и драгоцене метале, са GPS синхронизацијом и интерним часовником, уз тачност од највише 1ms одступања од тачног времена. Извор тачног времена даје време само уколико је сигуран у тачност.

Уколико дође до губитка синхронизације времена извора тачног времена, Канцеларија (RS-GOV TSA) зауставља издавање токена временског жига до постизања синхронизације.

Синхронизација времена јединице временског жига се врши тако да се не очекује одступање веће од декларисане тачности.

Извор тачног времена Канцеларије (RS-GOV TSA) је заштићен од напада и обезбеђен од препознатих ризика који могу резултовати неадекватним променама.

8.4 Управљање и рад издаваоца временског жига

8.4.1 Управљање безбедношћу

Управљање безбедношћу Канцеларије (RS-GOV TSA) се врши у складу са одговарајућим стандардима заштите.

Целокупна инфраструктура Канцеларије (RS-GOV TSA) је осигурана системом физичког и логичког обезбеђења.

Целокупан опис инфраструктуре Канцеларије (RS-GOV TSA) и начина и поступка заштите су наведени у интерним правилима Канцеларије (RS-GOV TSA).

8.4.2 Процена ризика

Канцеларија (RS-GOV TSA) осигурава да сва опрема има адекватан ниво заштите. Процена ризика је неопходна да би се одредили пословна средства и претње којима су та средства угрожена како би се одредиле неопходне сигурносне контроле и процедуре. Канцеларија (RS-GOV TSA) периодично врши процену ризика, односно класификацију средстава и ревизију сигурносних контрола и процедура.

8.4.3 Кадровска безбедност

Канцеларија (RS-GOV TSA) осигурава да особље поседује потребно знање и искуство у складу са својом улогом.

Поверљиве улоге у Канцеларији (RS-GOV TSA) су:

- начелник Одељења за стандардизацију, сертификацију и смернице развоја - врши надзор рада система за електронско издавање временског жига;
- руководилац Групе за праћење и вредновање Одељења за стандардизацију, сертификацију и смернице развоја - пружа стручну подршку у вођењу пројеката везаних за примену електронског временског жига;
- аналитичар за праћење и вредновање примене стандарда ИКТ-а у Групи за праћење и вредновање Одељења за стандардизацију, сертификацију и смернице развоја - врши послове администратора и оператора на систему за електронско издавање временског жига;
- систем администратор информационих система и технологија у Групи за праћење и вредновање Одељења за стандардизацију, сертификацију и смернице развоја - врши послове администратора и оператора на систему за електронско издавање временског жига;
- техничар одржавања информационих система и технологија у Групи за праћење и вредновање Одељења за стандардизацију, сертификацију и смернице развоја - врши послове администратора и оператора на систему за електронско издавање временског жига.

Канцеларија (RS-GOV TSA) обезбеђује и:

- да поверљиве улоге и одговорности, наведене у овом документу, буду документоване у опису радног места;
- да у описима радних места особља Канцеларије (RS-GOV TSA), раздвојеност дужности буде прецизно дефинисана, да су наведене потребне вештине и искуство, као и да ће адекватан ниво знања, школовања и обуке за коришћење информатичке опреме бити пружени запосленима;
- да особље спроводи административне процедуре у складу са правилима оперативног рада;
- да особље Канцеларије (RS-GOV TSA) са поверљивим улогама нема сукоб интереса са делатношћу Канцеларије (RS-GOV TSA);
- да особље Канцеларије (RS-GOV TSA) не чине особе које су осуђиване за кривична дела.

8.4.4 Физичко обезбеђење окружења

Канцеларија (RS-GOV TSA) осигурава да је физички приступ инфраструктури за издавање временског жига контролисан, односно да је:

- физички приступ дозвољен само овлашћеном особљу;
- обезбеђена примена уведених и интерним правилима дефинисаних процедура контроле приступа за спречавање губитка, оштећења или компромитовања инфраструктуре, крађе информација и нарушавање пословног процеса;
- обезбеђена примена уведених и интерним правилима дефинисаних процедура контроле приступа хардверском модулу заштите у складу са сигурносним захтевима за генерисање и чување кључева;
- инфраструктура Канцеларије (RS-GOV TSA) у систем сали, која физички штити сервере од неовлашћеног приступа и да се не дели са другим организацијама;
- обезбеђена сигурност опреме, података и информација Канцеларије (RS-GOV TSA) који се не могу изнети из просторија Канцеларије (RS-GOV TSA) без одговарајућег одобрења.

8.4.5 Управљање радом

Канцеларија (RS-GOV TSA) осигурава да компоненте за издавање временског жига буду заштићене и да исправно функционишу са минималним ризиком од квара.

Детаљан опис:

- интегритет Канцеларије (RS-GOV TSA) је заштићен од вируса, малициозног и недозвољеног софтвера;
- уведено је извештавање о сигурносним инцидентима, а процедуре реаговања су такве да штета од сигурносних инцидената буде минимизирана;
- обезбеђено је сигурно руковање са медијима коришћеним у оквиру Канцеларије (RS-GOV TSA), како би се медији заштитили од оштећења, крађе и неовлашћеног приступа;
- успостављене су и имплементиране процедуре за све поверљиве и административне улоге које утичу на обављање услуга Канцеларије (RS-GOV TSA);
- капацитети се прате и предвиђају како би се обезбедило да довољна процесорска снага и смештајни капацитети буду на располагању;
- Канцеларија (RS-GOV TSA) реагује брзо и координирано на инциденте како би се ограничио утицај сигурносних инцидената и у најкраћем року израђује извештај о било ком сигурносном инциденту;
- сигурносне улоге Канцеларије (RS-GOV TSA) су раздвојене од осталих улога.

8.4.6 Контрола приступа

Канцеларија (RS-GOV TSA) обезбеђује приступ само овлашћеним особама.

Детаљан опис:

- заштита интерне мреже Канцеларије (RS-GOV TSA) од неовлашћеног приступа је извршена употребом фајервол (енгл. firewall) система;
- Канцеларија (RS-GOV TSA) обезбеђује ефективну администрацију корисничких налога за приступ систему како би обезбедила потребан ниво заштите;
- приступ информацијама и апликацијама је ограничен у складу са политиком контроле приступа;
- особље Канцеларије (RS-GOV TSA) је идентификовано помоћу сертификата за аутентификацију пре администрације критичних апликација временског жига;
- евидентирају се све активности особља Канцеларије (RS-GOV TSA);

– локалне мрежне компоненте (рутери) Канцеларије (RS-GOV TSA) се чувају у систем сали у физички заштићеном окружењу и периодично се проверава њихова конфигурација у складу са захтевима.

8.4.7 Безбедно окружење

Канцеларија (RS-GOV TSA) користи проверене и сигурне системе који су заштићени од модификације:

– анализа сигурносних захтева се врши у процесу пројектовања и спецификације захтева за било који развојни пројекат како би се обезбедила сигурна имплементација у систем Канцеларије (RS-GOV TSA);
– контрола промена се користи за све верзије, модификације, и хитне измене на коришћеном софтверу.

8.4.8 Компромитовање издавања временског жига

У случају компромитовања или сумње у компромитовање или губитак синхронизације, Канцеларија (RS-GOV TSA) објављује свим корисницима детаље догађаја, и то:

– план опоравка Канцеларије (RS-GOV TSA) од непогоде који је део интерних правила садржи начин реаговања на компромитовање или сумњу у компромитовање приватних кључева јединице временског жига, или губитак синхронизације сата, као и процедуру обавештавања свих корисника у вези са:
  – врстом догађаја и
  – идентификацијом погођених временских жигова, на начин да то не крши приватност корисника Канцеларије (RS-GOV TSA) и сигурност услуге Канцеларије (RS-GOV TSA).
– у случају компромитовања или сумње у компромитовање или губитак синхронизације, Канцеларија (RS-GOV TSA) ће престати са издавањем токена временског жига док се не предузму кораци за опоравак.

8.4.9 Престанак издавања временског жига

Канцеларија (RS-GOV TSA) обезбеђује да, у случају престанка рада издаваоца временског жига, потенцијална штета корисницима и трећим странама буде минимална и да се одржи могућност валидације токена временског жига.

Пре престанка издавања временског жига, Канцеларија (RS-GOV TSA):

– обавештава све кориснике;
– поузданој страни преноси обавезе чувања записа неопходних за доказивање исправности функционисања Канцеларије (RS-GOV TSA) најмање у законом прописаном временском периоду;
– поузданој страни преноси обавезу да јавни кључ или сертификат буде расположив зависним странама, током тог временског периода;
– уништава приватни кључ јединица временског жига.

8.4.10 Усклађеност за законским оквиром

Канцеларија (RS-GOV TSA) осигурава 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.

8.4.11 Чување информација у вези услуге издавања временског жига

Канцеларија (RS-GOV TSA) осигурава да се све релевантне информације у вези токена временског жига чувају у периоду од најмање 10 година од датума издавања токена, тако што:

- записује и безбедно архивира све догађаје и податке у вези са услугом Канцеларије (RS-GOV TSA);
- одржава поверљивост и интегритет актуелних и архивираних записа у вези са радом Канцеларије (RS-GOV TSA);
- комплетно и поверљиво чува записе у вези са радом сервиса Канцеларије (RS-GOV TSA);
- чини доступним записе у вези са радом сервиса Канцеларије (RS-GOV TSA), уколико је потребно доказати правилно функционисање сервиса Канцеларије (RS-GOV TSA) за потребе судских поступака;
- бележи тачно време значајних промена у окружењу, управљања кључевима, или синхронизације времена;
- чува записе у вези са сервисима Канцеларије (RS-GOV TSA), довољно дуго након истека важења TSA сертификата, ради могућности пружања одговарајућег правног доказа;
- чува записе о догађајима, на начин који обезбеђује да се не могу лако обрисати или уништити;
- поверљиво чува све информације о корисницима, осим уколико се са корисником договори да информације могу бити јавно објављене;
- чува записе о догађајима који се односе на:
  - животни циклус потписних кључева Канцеларије (RS-GOV TSA) и сертификата;
  - синхронизацију времена јединице временског жига Канцеларије (RS-GOV TSA) са извором тачног времена;
  - губитак синхронизације извора тачног времена и времена јединице временског жига Канцеларије (RS-GOV TSA).

8.5 Организација

Канцеларија (RS-GOV TSA) обезбеђује да је сигурност у погледу организације рада тако што:

- усваја, мења и примењује политику и процедуре по којима Канцеларија (RS-GOV TSA) функционише и које нису дискриминаторске;
- своје услуге пружа свима у оквиру дефинисаног опсега своје делатности;
- Канцеларија (RS-GOV TSA) чини део Канцеларије;
- поседује финансијску стабилност и ресурсе потребне да послује у складу са Практичним правилима;
- запошљава довољан број особља, које поседује потребно образовање, обуку и техничко знање да пружа услуге издавања временског жига;
- правилно документује све споразуме и уговоре, где пружање услуге укључује подизвођаче или изнајмљивање опреме треће стране.

9. Заштита података о личности

Прикупљање, обрада и коришћење података о личности врши се у складу са Законом о заштити података о личности и у циљу пружања услуге издавања квалификованог електронског временског жига.

Услуга се пружа искључиво кориснику који је упознат и сагласан са општим условима и политиком приватности и који је потврдио своју сагласност за обраду података о личности.

Канцеларија (RS-GOV TSA) гарантује кориснику да ће се његови лични подаци користити у складу са прописима из области заштите података о личности, и да интегритет и поверљивост личних података ни на који начин неће бити угрожени.

У смислу одредби из области заштите података о личности, руковалац обраде података о личности и обрађивач је пружалац услуге - Канцеларија за информационе технологије и електронску управу, Немањина 11, 11000 Београд, контакт телефон +381 11 7358-400, адреса електронске поште kancelarija@ite.gov.rs. Контакт подаци службеника за заштиту личних података менаџера обраде су: lzzpol@ite.gov.rs.

Корисник чији су подаци о личности предмет обраде, има право да захтева приступ, исправку, брисање, преносивост и ограничење обраде и да поднесе приговор на обраду личних података који се односе на њега, ако су за то испуњени услови прописани законом из области заштите личних података.