

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

Политика пружања услуге издавања квалификованог електронског временског жига

Назив	Политика 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

1. Увод и преглед основних претпоставки.....	2
1.1 Увод.....	2
1.2 Основне претпоставке.....	2
2. Појмови који се користе у документу.....	3
3. Назив документа и идентификација.....	3
3.1 Администрација Политике пружања услуге издавања квалификованог временског жига.	4
3.1.1 Контакт особа.....	5
4. Правни основ.....	5
5. Учесници.....	5
5.1 Пружалац услуге.....	5
5.2 Корисник.....	6
6. Обавезе и одговорности.....	6
6.1 Обавезе и одговорности пружаоца услуге.....	6
6.1.1 Администрирање Политике издавања квалификованог електронског временског жига, Практичних правила.....	6
6.1.2 Обезбеђивање услова дефинисаних Практичним правилима.....	6
6.1.3 Обавезе према корисницима.....	6
6.1.4 Одговорност пружаоца услуге.....	7
6.2 Обавезе и одговорности корисника.....	7
6.3 Обавезе трећих страна.....	7
7. Дозвољена употреба.....	8
8. Заштита података о личности.....	8

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

ПОЛИТИКУ ПРУЖАЊА УСЛУГЕ ИЗДАВАЊА КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ВРЕМЕНСКОГ ЖИГА

1. Увод и преглед основних претпоставки

1.1 Увод

Овим документом дефинише се политика 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 податка 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 политику 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.

Политика 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/94/vremenski-zig.php>

Назив	Политика пружања услуге издавања квалификованог електронског временског жига
-------	--

Верзија	1.0
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) који се уграђују у документа:

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

Наведена документа која садрже опште услове су доступни свим корисницима услуга и поуздајућим странама и 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.

Политика издавања квалификованог електронског временског жига садржана у овом документу дефинисана је независно од конкретних детаља и специфичног оперативног окружења Канцеларије (RS-GOV TSA), док су Практична правила прилагођена организационој структури, оперативним процедурама, ресурсима и рачунарском окружењу Канцеларије (RS-GOV TSA).

Овај документ, као мање специфичан, поставља захтеве, али не одређује техничке детаље рачунарског и оперативног окружења Канцеларије (RS-GOV TSA).

3.1 Администрација Политике пружања услуге издавања квалификованог временског жига

Канцеларија (RS-GOV TSA) је одговорна је за периодичан преглед и ажурирање овог документа у којем је дефинисана Политика пружања услуге издавања квалификованог

временског жига (у даљем тексту: Политика), 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 Политика 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 личности¹.

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://www.ite.gov.rs/tekst/6058/vremenski-zig.php>).

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 и обезбеђује да сва наведена правила буду имплементирана у складу са наведеном политиком.

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 токenu, 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 стране 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. 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.