РЕПУБЛИКА СРБИЈА
МИНИСТАРСТВО УНУТРАШЊИХ ПОСЛОВА
СЕРТИФИКАЦИОНО ТЕЛО

ПОЛИТИКА ПРУЖАЊА УСЛУГЕ ИЗДАВАЊА КВАЛИФИКОВАНИХ ЕЛЕКТРОНСКИХ СЕРТИФИКАТА НА ЛИЧНИМ КАРТАМА

Београд, мај 2020

Верзија: 1.0

РЕПУБЛИКА СРБИЈА
МИНИСТАРСТВО УНУТРАШЊИХ ПОСЛОВА
СЕРТИФИКАЦИОНО ТЕЛО

На основу члана 31. став 2. Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС“, број 94/17) и члана 4. Уредбе о условима за пружање квалификованих услуга од поверења („Службени гласник РС“, број 37/18),

министар унутрашњих послова доноси

Политика пружања услуге издавања квалификованих електронских сертификата на личним картама

1. Увод

Министарство унутрашњих послова (у даљем тексту: „МУП“) као пружалац квалификоване услуге од поверења издавања квалификованих сертификата за електронски потпис, пружа услугу издавања квалификованих електронских сертификата (у даљем тексту „сертификат“) на личним картама са чипом у складу са важећим законским прописима и сагласно препорученим стандардима.

МУП је одговоран за пружање комлетне услуге издавања сертификата која обухвата регистрацију корисника, формирање сертификата, дистрибуцију сертификата корисницима, управљање животним веком сертификата, обезбеђивање поузданог и јавно доступног сервиса за проверу статуса сертификата.

МУП је изградио инфраструктуру система са јавним кључевима, ПКИ систем (*PKI - Public Key Infrastructure),* чија је основна улога поуздано успостављање електронског идентитета корисника специфицираног у облику електронског сертификата. ПКИ систем МУП-а је хијерархијске структуре. На првом нивоу хијерархије је врховно самопотписујуће сертификационо тело, а на следећем нивоу су подређена сертификациона тела, издаваоци корисничких сертификата. Учесници ПКИ система су сертификационо тело, регистрациона тела, корисници и поуздајуће стране.

Сертификационо тело (*CA - Certificate Authority*) представља највишу тачку поверења у ПКИ систему. Основна улога сертификационог тела је да процедуром електронског потписа на бази асиметричног криптографског алгоритма и свог приватног кључа, који мора бити најстроже чувана тајна, гарантује везу између јавног кључа и идентитета корисника сертификата.

Регистрациона тела су организационе јединице МУП-а које врше регистарацију корисника за издавање сертификата, односно организационе јединице надлежне за издавање личних идентификационих докумената. Захтеви за издавање квалификованих електронских сертификата се подносе регистрационим телима.

Корисници су физичка лица којима се пружа услуга издавања квалификованих

електронских сертификата.

Поуздајуће стране су физичка или правна лица која се поуздају у квалификоване електронске сертификате, у циљу верификовања квалификованог електронског потписа и потврде идентитета корисника.

Квалификовани електронски сертификат се може користити за већину сервиса електронске управе и електронског пословања који су базирани на употреби електронских сертификата. Корисник је дужан да сертификат користи у складу са важећим законским прописима. Свака употреба сертификата која није у складу са важећим законским прописима није дозвољена.

2. Објављивања информација и локација где се објављују

Све инфомације које се односе на пружање услуге издавања квалификованих електронских сертификата МУП објављује на веб страни сертификационог тела МУП-а, http://ca.mup.gov.rs , која је јавно доступна.

На сајту су објављена правна акта која се односе на пружање услуге издавања квалификованих електронских сертификата, обрасци захтева и уговора неопходни за пружање услуге издавања сертификата, сертификати сертификационог тела (CA сертификати), листе опозваних сертификата, корисничка упутства, друга акта и обавештања.

3. Идентификација и аутентикација

У квалификованим електронским сертификатима које издаје МУП, име сертификационог тела које издаје сертификате и имена корисника сертификата су јединствена имена.

Име корисника сертификата једнозначно потврђује идентитет корисника. Корисници не могу да буду анонимни и не могу да користе псеудониме. Имена корисника сертификата представљена су одговарајућим националним писмом, онако како су представљена на самом обрасцу личне карте. Јединственост имена корисника сертификата се остварује помоћу јединственог серијског броја X.509 сертификата.

Додавање заштитног знака имену корисника сертификата није дозвољено. Имена којима би се кршила интелектуална или ауторска права других нису дозвољена.

Након подношења захтева за издавање квалификованог електронског сертификата врши се провера идентитета корисника коме се издаје сертификат. Идентитет корисника се потврђује на основу важећег идентификационог документа.

Корисник сноси одговорност за тачност података наведених у захтеву за издавање сертификата.

4. Оперативни захтеви у вези животног века сертификата

Захтев за пружање услуге издавања квалификованог електронског сертификата може да поднесе:

-Држављанин Републике Србије, који има важећу личну карту са чипом
-Страни држављанин, који има важећу биометријску личну карту за странце. (Сертификати се не издају на привременим личним картама за странце).

Услови за издавање сертификата кориснику су:

- да корисник поседује важећу личну карту са чипом,
- да корисник регистрационом телу лично поднесе уредно попуњен и својеручно потписан Захтев за пружање услуге издавања квалификованог електронског сертификата,
- да се корисник пре подношења захтева упозна са Општим условима пружања услуге издавања квалификованог електронског сертификата,
- да корисник са МУП-ом закључи Уговор о пружању услуге издавања квалификованог електронског сертификата.

Сертификат се кориснику лично уручује и одмах је активан.
Приватни криптографски кључ корисника се користи за креирање квалификованог електронског потписа. Корисник приступа свом приватном кључу уношењем активационог податка (ПИН-а). Квалификовани електронски сертификат се користи за верификовање квалификованог електронског потписа.

Јавни кључ и квалификовани сертификат корисника поуздајуће стране користи се за верификацију електронског потписа. Поуздајуће стране пре него што се поуздају у сертификат треба да изврше валидацију сертификата, односно да провере ланац поверења (ланац CA сертификата издаваоца) и статус сертификата спрам листе опозваних сертификата.

Сертификат се кориснику издаје са роком важења од 5 година или са роком краћим од 5 година, ако је до истека периода важности личне карте остало мање од 5 година, тада се сертификат издаје на период важности личне карте. Ако је након истека важности сертификата лична карта и даље важећа, корисник може захтевати обнављање сертификата.

Под обнављањем сертификата подразумева се генерисање новог пара криптографских кључева и издавање квалификованог електронског сертификата на личној карти, која већ има уписан квалификовани електронски сертификат, али му је истекла важност.

Опозив сертификата је потпуно укидање важења сертификата и његово објављивање на листи опозваних сертификата.

Опозив сертификата се врши у случајевима када:

1) опозив сертификата захтева власник сертификата,
2) власник сертификата изгуби пословну способност;
3) се утврди да је податак у сертификату погрешан;
4) се утврди да су подаци за проверу квалификованог електронског потписа угрожени на начин који утиче на безбедност и поузданост сертификата;
5) се утврди да су подаци за електронско потписивање угрожени на начин који утиче на безбедност и поузданост електронског потписа;
6) издавалац сертификата престаје са радом или му је рад забрањен.

Корисник је дужан да одмах затражи опозив свог сертификата у случају губитка или оштећења средства или података за креирање електронског потписа или у случају компромитације или сумње у компромитацију свог приватног кључа.

Суспензија сертификата је привремено укидање важења сертификата и његово објављивање на листи опозваних сертификата (CRL листи). Суспензија траје онолико дуго колико трају услови због којих је захтевана. Када ови услови престану да важе, корисник може захтевати реактивацију сертификата. Реактивација сертификата је поновно активирање сертификата који је био суспендован и његово брисање са CRL листе.

5. Физичка, процедурална и кадровска безбедносна контрола

Целокупна опрема безбедних система за издавање сертификата (сервери, криптографски уређаји и остала опрема) смештени су у Београду, у згради Министарства унутрашњих послова у улици Кнеза Милоша број 103. Опрема система за издавање сертификата налази се у просторији, која одговара потребама извршења операција високе безбедности (Фарадејев кавез).

Систем за издавање сертификата прикључен је на систем за непрекидни извор напајања електричном енергијом и систем за климатизацију што омогућава да се напајање и вентилација извршавају са редундансом високог нивоа. Предузете су техничке мере заштите од евентуалних поплава од водоводних инсталација. Фарадејев кавез опремљен је системом за рано откривање и аутоматску дојаву пожара, детекторима дима и системом за гашење пожара.

Сви рачунарски медији, који садрже продукциони софтвер, архиву логова и резервне копије података система за издавање сертификата, смештају се у ватроотпорне безбедне сефове, заштићене системима физичке и логичке контроле приступа.

Након престанка потребе за коришћењем података, документације и уређаја, везаних за рад система за издавање сертификата, подаци, документација и уређаји се уништавају. Папирна документација, се пре бацања уништава пропуштањем кроз машину за сечење папира. Подаци са рачунарских медија се неповратно бришу, а рачунарски медији се физички уништавају. Криптографски уређаји се физички уништавају.

Имплементиран је систем за прављење резервних копија *(backup)* података и логова система за издавање сертификата. Резервне копије се чувају у безбедним сефовима заштићеним системима физичке и логичке контроле приступа. Резервна копија за процедуру опоравка од катастрофе *(disaster recovery)* се чува на удаљеној локацији.

Имплементирана је строга процедурална контрола, која захтева вишеструку ауторизацију за извршавање процедура високог нивоа поверљивости. Неопходна је аутентикација најмање два запослена са поверљивим улогама да би био могућ физички и логички приступ критичним системима за издавање сертификата и криптографским уређајима.

Запослени са поверљивим улогама поседују експертско знање и искуство из области одржавања и безбедности информационих система и редовно похађају обуке и семинаре у циљу обнављања знања о новим безбедносним претњама и актуелним безбедносним процедурама.

Запослени са поверљивим улогама дужни су да предузимају само оне активности за које су ауторизовани и да се придржавају прописаних интерних процедура рада и заштите система издавања сертификата. Неауторизоване активности и кршење прописаних процедура рада сматраће се повредом службене дужности.

Сви догађаји који се односе на обављање делатности пружања услуге издавања сертификата се бележе у лог фајлове, а целокупна документација примљена уз захтев за издавање сертификата се чува у евиденцијама у складу са законом који уређује евиденције и обраду података у области унутрашњих послова.

У случају појаве инцидента, током рада система за издавање сертификата, запослени са поверљивим улогама поступају у складу са својим интерним процедурама рада.

У случају штете настале на техничким средствима (хардверу и софтверу) или подацима, сервиси апликације система за издавање сертификата биће поново успостављени у најкраћем могућем року.

Након катастрофе и отклањања њених последица МУП ће у најкраћем року да доведе систем у продукционо стање и настави са пружањем услуге издавања сертификата.

МУП у случају компромитације или сумње у компромитацију приватног кључа сертификационог тела:

- престаје са издавањем сертификата;
- информише све кориснике и поуздајуће стране о компромитацији приватног кључа;
- јавно објављује информације о томе да издати сертификати, као и информације о статусу опозваности сертификата, више нису важеће;
- врши опозив свих издатих сертификата одмах, а најкасније у року од 24 часа у складу са Законом.

У случају престанка пружања услуге издавања сертификата МУП ће настојати да

корисницима обезбеди наставак пружања услуге код другог пружаоца услуге од поверења, коме ће доставити сву документацију и неопходна техничка средства. Ако није могуће обезбедити наставак пружања услуге код другог пружаоца услуге, МУП ће три месеца пре престанка пружања услуге обавестити кориснике и поуздајуће стране о намери престанка обављања делатности, након чега ће извршити раскид уговора и опозив свих издатих сертификата.

6. Техничке безбедносне контроле

Приватни криптографски кључеви сертификационог тела генеришу се и чувају у криптографским HSM *(Hardver securuty module)* уређајима, који задовољавају одговарајуће захтеве у складу са међународним стандардом *FIPS 140-2 L3*. Испуњење овог стандарда гарантује да је било који покушај нарушавања интегритета уређаја или криптографске меморије истовремено детектован. Приватни криптографски кључ сертификационог тела се користи за потписивање сертификата које издаје и за потписивање листе опозваних сертификата. Јавни криптографски кључ сертификационог тела се користи за верификацију потписа.

Приватни криптографски кључеви корисника генеришу се на смарт картицама (личним картама) корисника и за њихово чување одговоран је корисник. Приватни криптографски кључ корисника се користи за креирање квалификованог електронског потписа. Јавни криптографски кључ корисника се користи за верификовање квалификованог електронског потписа и обезбеђивање непорецивости.

HSM уређаји смештени су у Фарадејевом кавезу, коме физички приступ имају само запослени са поверљивим улогама. Приватни криптографски кључеви који се чувају у HSM уређајима никад не напуштају уређај у отвореном облику. Процедуре чувања и руковања приватним криптографским кључевима су део Посебних интерних правила рада и заштите система издавања сертификата.

Активациони подаци су лозинке или ПИН кодови потребни за активацију приватног криптографског кључа.

Активациони подаци приватног кључа сертификационог тела, лозинке, генеришу се током извођења „Церемоније кључева“ и користе их искључиво запослени са поверљивим улогама током извршавања интерних процедура рада и заштите система за издавање сертификата. Запослени са поверљивим улогама су дужни да чувају лозинке за активацију приватног кључа сертификационог тела у складу са прописаним интерним процедурама рада.

Активациони податак корисника, ПИН код, генерише се у процесу персонализације идентификационог документа (личне карте) и заједно са њим се уручује кориснику у заштићеној коверти. Кориснички ПИН има четири нумеричка карактера. Корисник је дужан да чува свој ПИН за активацију приватног кључа од неовлашћеног приступа и употребе.

Сервери система за издавање сертификата заштићени су системима физичке и логичке заштите. Сервери се налазе у Фарадејевом кавезу, коме физички могу приступити само

запослени са поверљивим улогама. Логички приступ серверима остварује се вишеструком ауторизацијом.

Конфигурација система за издавање сертификата, као и све модификације и надоградње система се документују и контролишу. Имплементиране безбедносне контроле се по потреби унапређују. Имплементиран је механизам мрежне безбедности високог нивоа, заснован на примени firewall уређаја и система за превенцију и заштиту од напада.

Сертификати и листе опозваних сертификата имају временску ознаку датума и времена издавања, датума и времена престанка важења сертификата и датума и времена издавања следеће листе опозваних сертификата.

7. Профили сертификата, CRL листе и OCSP

Профили сертификата сертификационог тела и корисника су у складу са препорученим стандардима:

- *ITU-T Recommandation X.509 Version 3*
- *ETSI EN 319 412-1 „Electronic Signatures and Infrastructures (ESI) – Certificate Profiles Part 1: Overview and common data structures"*
- *ETSI EN 319 412-2 „Electronic Signatures and Infrastructures (ESI) – Certificate Profiles Part 2: Certificate profile for certificates issued to natural persons"*
- *IETF RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"*

Профили листе опозваних сертификата (CRL листе) су у складу са стандардом

- *IETF RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"*

Министарство унутрашњих послова омогућава on-line проверу статуса квалификованог електронског сертификата посредством OCSP протокола. OCSP профил је у складу са документом *RFC 2560: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.*

8. Ревизија усклађености и друге процене

МУП врши интерну ревизију усклађености пружања услуге издавања сертификата са важећим законским прописима, који регулишу област квалификованих услуга од поверења и одредбама овог документа. Екстерну ревизију врши тело за оцењивање усаглашености у складу са законом. Након извршене ревизије сачињава се извештај о оцени усаглашености.

Ревизијом се проверава усклађеност пружања услуге издавања сертификата са важећим законским прописима, који регулишу област квалификованих услуга од поверења и

препорученим стандардима.

У случају да се интерном или екстерном ревизијом утврде неправилности у пружању услуге издавања сертификата, предузимају се мере да се у што краћем року неправилности отклоне.

Након извршене ревизије сачињава се извештај о оцени усаглашености.

9. Други пословни и правни аспекти

МУП бесплатно пружа услугу издавања квалификованих електронских сертификата на личним картама са чипом.

МУП сноси материјалну одговорност за пружање услуге издавања сертификата у складу са важећим законским прописима. Дужан је да обезбеди најнижи износ осигурања од ризика за могућу штету насталу вршењем квалификоване услуге од поверења тако да осигурана сума на коју мора бити уговорено осигурање по једном штетном догађају не може износити мање од 20.000 (двадесет хиљада) евра у динарској противвредности за квалификовану услугу од поверења. Укупна осигурана сума на коју мора бити уговорено осигурање од одговорности кумулативно на годишњем нивоу, по свим штетним догађајима, не може бити нижа од 1.000.000 (милион) евра у динарској противвредности укупно за све квалификоване услуге од поверења које пружа.

МУП не прихвата било какву другу одговорност осим оне која је изричито одређена овим актом, Уговором и важећим законским прописима. МУП је ослобођен одговорности за било коју штету причињену корисницима приликом пружања услуге издавања сертификата, уколико је до штете дошло услед разлога, који су ван контроле МУП-а, односно услед више силе.

МУП је дужан да се приликом пружања услуге издавања сертификата, према личним подацима корисника односи сагласно одредбама Закона о заштити података о личности и да у случају повреде података о личности о томе обавести Повереника и лице на које се подаци односе, на начин прописан Законом о заштити података о личности.

МУП је у обавези да чува податке коришћене у регистрацији корисника и све информације о животном циклусу издатог сертификата корисника; да води ажурну и безбедну евиденцију неважећих (опозваних и суспендованих) сертификата и мора за сваки сертификат, за који је издао информацију о његовој валидности, ту информацију учинити јавно доступном путем сервиса за проверу статуса опозваности електронских сертификата. Евиденција се води у складу са законом који уређује евиденције и обраду података у области унутрашњих послова.

МУП је дужан да изврши опозив сертификата када:

- опозив сертификата захтева власник сертификата или његов пуномоћник;
- власник сертификата изгуби пословну способност;
- утврди да је податак у сертификату погрешан;

- утврди да су подаци за проверу квалификованог електронског потписа угрожени на
- начин који утиче на безбедност и поузданост сертификата;
- утврди да су подаци за електронско потписивање угрожени на начин који утиче на безбедност и поузданост електронског потписа;
- престаје са радом или му је рад забрањен.

МУП је у обавези да у случају компромитације свог приватног асиметричног кључа:

- престаје са издавањем сертификата;
- информише све кориснике и друге заинтересоване стране о компромитацији приватног кључа;
- јавно објављује информације о томе да издати сертификати, као и информације о статусу опозваности сертификата, више нису важеће;
- врши опозив свих издатих сертификата одмах, а најкасније у року од 24 часа у складу са Законом.

Корисник је у обавези да:

- достави тачне и комплетне информације у складу са дефинисаном процедуром регистрације;
- искључиво користи свој асиметрични приватни кључ за формирање квалификованог електронског потписа у складу са одредбама Закона;
- онемогући неовлашћен приступ свом приватном кључу;
- одмах обавести издаваоца сертификата ако се пре истека важности сертификата назначеног у самом сертификату: корисников приватни кључ изгуби, украде или наступи основана сумња да је компромитован, престане контрола над коришћењем корисниковог приватног кључа из разлога компромитације активационог податка (ПИН) за средство за формирање квалификованог електронског потписа (лична карта) или других разлога, установи нетачност или измена садржаја сертификата;
- прекине коришћење свог приватног кључа уколико постоји основана сумња у компромитацију кључа или контролу над активационом податком.

Корисник је дужан да одмах затражи опозив свог сертификата у случају губитка или оштећења средства или података за креирање електронског потписа.

Свака употреба сертификата која није у сагласности са важећим законским прописима и овим актом није дозвољена. МУП не прихвата одговорност за штету насталу при коришћењу сертификата ван оквира истакнутих ограничења. За евентуалну штету насталу неправилним и недозвољеним коришћењем сертификата одговоран је корисник сертификата.

Корисник има право на обештећење за штету насталу коришћењем сертификата, ако се докаже да је штета настала при коришћењу сертификата сагласно важећим законским прописима и у оквиру истакнутих ограничења.

Поуздајуће стране су у обавези пре него што се поуздају у сертификат:

- да изврше проверу статуса сертификата, спрам ажурне листе опозваних сертификата,

- да се упознају са одговорностима и ограничењима од одговорности дефинисаним овим актом, Уговором и важећим законским прописима.

Међусобна права, обавезе и одговорности корисника и МУП-а у вези са пружањем услуге издавања сертификата регулисана су Уговором о пружању услуге издавања квалификованог електронског сертификата, који се закључује између уговорених страна.

Спорови настали између уговорних страна у вези међусобних права и обавеза, тумачења уговора и овог акта решаваће се споразумно, а уколико споразум није могућ, спор ће решавати надлежни суд у Београду.

Доношењем ове политике престаје да важи „Политика сертификације сертификационог тела МУП РС 02/2010, 08/2014 и 06/2016".

У Београду, 08 JUN 2020
01 Број: 1122/20-2

Министар,

др Небојша Стефановић