ПРАВИЛНИК
О ИЗДАВАЊУ ВРЕМЕНСКОГ ЖИГА

На основу члана 12. став 4. Закона о електронском потпису Републике Српске („Службени гласник Републике Српске“, број 106/15) и члана 82. став 2. Закона о републичкој управи („Службени гласник Републике Српске“, бр. 118/08, 11/09, 74/10, 86/10, 24/12, 121/12, 15/16 и 57/16) , министар науке и технологије 11. новембра 2016. године доноси

ПРАВИЛНИК
О ИЗДАВАЊУ ВРЕМЕНСКОГ ЖИГА

Члан 1.

Правилником о издавању временског жига утврђују се услови које мора да испуњава систем за формирање временског жига, садржај захтјева за формирање временског жига, садржај структуре података временског жига и поступак означавања времена које је садржано у временском жигу.

Члан 2.

Цертификационо тијело које издаје временски жиг у даљем тексту: (издавалац временског жига) примјењује информационе технологије и техничка и програмска средства чије је дјеловање усклађено са важећим међународним стандардима, а који се односе на:

1) политику пружања услуге издавања временског жига,
2) профил временског жига,
3) сигурност криптографских модула за израду временског жига,
4) сигурност система за издавање временског жига

Члан 3.

(1) Издавалац временског жига прије почетка пружања услуге издавања временских жигова подноси захтјев за упис у Евиденцију односно Регистар издавалаца временских жигова.

(2) Поступак уписа у Евиденцију односно Регистар издавалаца временских жигова врши се у складу са прописом о евиденцији цертификационих тијела односно прописом о поступку издавања дозволе и уписа у Регистар цертификационих тијела за издавање квалификованих електронских цертификата.

Члан 4.

(1) Издавалац временског жига креира документ о правилима пружања услуга издавања временског жига – Политику пружања услуга издавања временског жига, која дефинише захтјеве пословања издаваоца временског жига као и процесе и ресурсе издаваоца временског жига у циљу испуњења тих захтјева.

(2) Политика пружања услуга издавања временског жига обезбјеђује довољно информација на основу којих корисници могу донијети одлуку о прихватању тих услуга и о њиховом обиму.

(3) Политика пружања услуга издавања временског жига треба да буду усклађена са међународним стандардима и стручним правилима, а посебно са ETSI EN 319 421 (Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps).

Члан 5.

(1) Профил временског жига се базира на моделу утврђеном у документу RFC 3161 (Request for Comments: 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)) , уз допуне дефинисане документом RFC 5816 (Request for Comments: 5816 ESSCertIDv2 Update for RFC 3161).

(2) Уз спецификацију из става 1. овог члана, у изради профила временског жига преузимају се и атрибути утврђени актуелном верзијом документа ETSI EN 319 422 (Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles).

Члан 6.

(1) Захтјев за издавање временског жига садржи криптографски отисак (hash вриједност) електронског документа, односно електронског потписа одређеног електронског документа, који се формира коришћењем криптографског hash алгоритма, као и идентификатор алгоритма којим је формиран криптографски отисак.

(2) Захтјев за издавање временског жига мора да испуњава услове прописане документом RFC 3161.

(3) За формирање криптографског отиска из става 1. овог члана користи се један од алгоритама SHA фамилије, SHA 256 или SHA 512, минимално SHA 256 у складу са документом ETSI TS 119 312 (Electronic Signatures and Infrastructures (ESI); Cryptographic Suites).

Члан 7.

Систем за формирање временског жига мора да испуњава услове који обезбјеђују да издавање временског жига буде у складу са овим Правилником, међународним стандардима и стручним правилима протокола и профила временског жига ETSI EN 319 422 (Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles) и RFC 3161 (Request for Comments: 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)).

Члан 8.

Садржај структуре података временског жига је у складу са стандардом RFC 3161 и укључује:

1) Идентификатор издаваоца временског жига,
2) Серијски број временског жига,
3) Објекат за формирање временског жига, кога чини криптографски отисак из захтјева за формирање временског жига,
4) Идентификатор алгоритма којим је формиран криптографски отисак из тачке 3. овог члана,
5) Датум и вријеме формирања временског жига,
6) Електронски потпис структуре података временског жига,
7) Електронски цертификат путем кога се може верификовати електронски потпис из тачке 6. овог члана,
8) Идентификатор алгоритма који је коришћен при формирању електронског потписа из тачке 6. овог члана,
9) Ознаку Политике пружања услуге издавања временског жига

Члан 9.

(1) Асиметрични пар криптографских кључева – јавни и приватни кључ, који се користи за формирање временског жига мора бити јединствен и придружен систему за формирање временског жига.

(2) Приликом генерисања новог асиметричног пара криптографских кључева, генерише се и нови електронски цертификат система за формирање временског жига, без опозива претходног цертификата.

(3) Електронске цертификате система за формирање временског жига издаје цертификационо тијело регистровано у складу са овим Правилником.

(4) Период ваљаности електронског цертификата система за формирање временског жига дефинише се у складу са најбољим праксама према документима ETSI EN 319 421 и ETSI TS 119 312, при чему је минимални период ваљаности поменутог електронског цертификата пет година, док је максимални рок ваљаности приватног кључа три мјесеца.

Члан 10.

(1) Издавалац временског жига потписује временски жиг асимтеричним приватним кључем, одређеним искључиво у ту сврху.

(2) За формирање поменутог електронског потписа користи се један од следећих криптографских алгоритама RSA минималне дужине 2048, DSA уз минималну вриједност параметара "p" і "q" од 3072 и 256 бита, респективно и ECDSA уз минималну вриједност параметра „n“ од 256 бита, а у складу са документом ETSI TS 119 312.

(3) На основу једног захтјева за издавање временског жига може се издати више временских жигова само у случају да су ти временски жигови потписани коришћењем различитих приватних кључева.

Члан 11.

Издавалац временског жига обезбјеђује да је асиметрични пар криптографских кључева генерисан и чуван у строго контролисаним и безбједним условима, а нарочито да се:

1) генерисање и чување асиметричног пара криптографских кључева врши у физички заштићеном окружењу под контролом овлашћених запослених лица, а у складу са условима дефинисаним интерним правилницима, као и у складу са Политиком пружања услуга издавања временског жига;

2) генерисање асиметричног пара криптографских кључева врши се у средству које задовољава захтјеве из стандарда FIPS PUB 140-2 ниво 3, односно виши ниво, CEN Workshop Agreement (CWA) 14167-2 ili ISO/IEC 15408 ниво EAL 4+, односно виши ниво;

3) услов из тачке 2. овог члана потврђује одговарајућим цертификатом о испуњавању стандарда и

4) не креирају копије приватног кључа.

Члан 12.

(1) Издавалац временског жига обезбјеђује да се његови асиметрични приватни кључеви не користе након истека њиховог животног циклуса, као што је дефинисано Политиком пружања услуга издавања временског жига и интерним правилницима.

(2) Асиметрични приватни кључеви након истека њиховог животног циклуса морају бити уништени на начин којим се обезбјеђује да се не могу реконструисати.

Члан 13.

(1) Издавалац временског жига осигурава безбједност криптографских уређаја који се користе за генерисање и чување асиметричног пара криптографских кључева и формирање електронског потписа временских жигова током животног циклуса уређаја, у складу са интерним правилницима

(2) Издавалац временског жига посебно треба осигурати да:

1) криптографски уређај није компромитован током транспорта,

2) криптографски уређај није компромитован за вријеме чувања код издаваоца временског жига,

3) процедуре инсталације и активације врши само уз истовремену контролу запослених лица са безбједносним функцијама,

4) криптографски уређај исправно функционише,

5) изврши уништавање асиметричних приватних кључева издаваоца временског жига који су чувани у криптографском уређају на крају животног циклуса кључева или уређаја.

Члан 14.

(1) Издавалац временског жига обезбјеђује да у случају хаварија и догађаја који утичу на безбједност система за издавање временских жигова, укључујући и компромитовање асиметричних приватних кључева или поремећаја калибрације и синхронизације са извором тачног времена, оперативни рад буде обновљен што је могуће прије, у складу са Политиком пружања услуга издавања временског жига, која мора укључивати план нормалног успостављања у случају компромитовања приватног кључа или поремећаја система калибрације и синхронизације са извором тачног времена.

(2) У случају компромитације свог приватног кључа или поремећаја система калибрације и синхронизације са извором тачног времена, издавалац временског жига је у обавези да:

1) обустави издавање временских жигова,

2) обавијести све кориснике и друге укључене стране о компромитацији и другим догађајима и

3) јавно објави информације на који начин установити који временски жигови нису важећи, на начин да се не угрози заштита података о личности.

Члан 15.

(1) Вријеме које је садржано у временском жигу одређује се коришћењем специјализованог уређаја који представља извор тачног времена, који мора бити заштићен од непримјећених промјена.

(2) Свака промјена рада уређаја изван дозвољених параматера се мора одмах установити.

Члан 16.

Систем за формирање временског жига мора осигурати вријеме одзива мање од једног минута, мјерено као разлика између времена када сервис прими захтјев и времена које ће се појавити у временском жигу.

Члан 17.

(1) Издавалац временског жига мора да користи безбједне системе и производе који су заштићени од неовлаштених модификација.

(2) Издавалац временског жига мора имати дефинисан процес периодичне анализе и одржавања Политике пружања услуга издавања временског жига.

(3) Издавалац временског жига обезбјеђује услове за поуздано пружање услуга, а нарочито:

1) доступност својих услуга свим корисницима чије су активности у складу са објављеном Политиком пружања услуга издавања временског жига,

2) заштиту личних података корисника,

3) ресурсе потребне за издавање временског жига у складу са Практичним правилима пружања услуга издавања временског жига,

4) ефикасно поступање у рјешавању рекламација и спорова са корисницима ли другим заинтересованим странама у вези издавања временског жига

Члан 18.

(1) У Политици пружања услуга издавања временског жига мора бити одређено поступање у случају престанка рада издаваоца временског жига.

(2) Поступање у случају престанка рада из става 1. овог члана мора бити одређено тако да обезбједи да су потенцијалне сметње корисницима и трећим лицима што мање, да обезбједи даље чување свих релевантних података о исправности издатих временских жигова, а посебно да предвиди:

1) јавно објављивање информација о престанку рада,

2) обезбјеђивање даљег поузданог чувања свог јавног кључа или цертификата и свих релевантних података потребних за доказивање валидности издатих временских жигова, што може бити повјерено другој организацији

3) поуздано уништавање приватних кључева,

4) опозив свих цертификата издаваоца временског жига.

Члан 19.

(1) Издавалац временског жига утврђује и интерна правила рада и заштите система.

(2) Интерна правила рада и заштите система представљају пословну тајну издаваоца временског жига.

(3) Интерна правила уређују:

1) систем физичке контроле приступа у поједине просторије издаваоца временског жига,

2) систем логичке контроле приступа рачунарским ресурсима издаваоца временског жига,

3) систем за чување приватног кључа издаваоца временског жига,

4) систем дистрибуиране одговорности при активацији приватног кључа издаваоца временског жига,

5) поступање у ванредним ситуацијама (пожари, поплаве, земљотреси, друге временске непогоде, злонамјерни упади у просторије или информациони систем издаваоца временског жига)

Члан 20.

Издавалац временског жига мора обезбједити наопходне кадровске ресурсе, и са њима повезане предуслове, а нарочито сљедеће:

1) Запослени у издаваоцу временског жига морају да посједују искуство и неопходну квалификацију за услуге које издавалац временског жига нуди, као и за одговарајуће пословне функције,

2) улоге и пословне функције запослених, утврђене у Политици пружања услуга издавања временског жига, морају бити документоване и детаљно специфициране, са описима сваког радног мјеста у издаваоцу временског жига а пословне функције од највишег нивоа повјерљивости, од којих највише зависи безбједност функционисања издаваоца временског жига, морају бити посебно и јасно идентификоване као бебједносне функције

Члан 21.

(1) Издавалац временског жига обезбјеђује контролу физичког приступа својим безбједносно критичним ресурсима, како би се ризик неовлашћеног приступа свео на најмању могућу мјеру.

(2) Издавалац временског жига мора обезбједити сљедеће:

1) физички приступ просторијама у којима се обавља генерисање временских жигова мора се ограничити само на овлашћене особе,

2) морају бити имплементиране неопходне мјере у циљу избјегавања губитака, оштећења или компромитовања кључних ресурса и елиминисање могућности прекида пословних активности,

3) Морају бити имплементиране одговарајуће мјере за спречавање комппромитовања или крађе информација и/или уређаја за обраду информација,

4) просторије у којима се врши генерисање временских жигова морају бити такве да се оперативни рад у њима одвија у окружењу које обезбјеђује физичку заштиту безбједносно критичних дијелова система за формирање временског жига од компромитације пруозроковане неовлашћеним приступом систему и подацима,

5) просторије из тачке 4. овог става се не смију дијелити са другим организацијама,

6) морају бити имплементиране одговарајуће физичке мјере и контроле безбједносног окружења у циљу заштите просторија и системских елемената издаваоца временског жига,

7) морају бити имплементиране одговарајуће мјере у циљу заштите уређаја, информација, медија и софтвера од отуђивања са локације без прописане ауторизације.

Члан 22.

Издавалац временског жига обезбјеђује да је приступ систему за издавање временског жига ограничен искључиво на поздано ауторизоване особе, а нарочито обезбјеђује:

1) имплементацију контрола на мрежном нивоу у циљу заштите интерне мреже издаваоца временског жига од екстерних мрежних домена којима може приступити трећа страна,

2) поуздану заштиту осјетљивих података, који укључују и податке о корисницима, током проласка кроз дјелове мреже који нису безбједни,

3) ефикасну и поуздану администрацију корисничких приступа (укључујући операторе, администраторе и било које специфичне кориснике који имају директан приступ систему) у циљу одржавања безбједности система, укључујући и управљање налозима корисника, евидентирање и могућност модификације и забране приступа,

4) строго ограничен приступ информацијама и апликативним функцијама система у складу са Политиком пружања услуга издавања временског жига и интерним правилима, као и

довољну рачунарско-безбједносну контролу у циљу раздвајања безбједносних функција у систему, укључујући раздвајање функција администратора безбједности и оператера, као и посебно ограничен и строго контролисан рад са корисничким програмима за управљање системом

5) поуздану идентификацију запослених у издаваоцу временског жига прије коришћења критичних операција везаних за процедуре издавања временског жига,

6) евидентирање свих активности запослених у издаваоцу временског жига на основу одговарајућих корисничких налога и лог фајлова,

7) поуздану заштиту безбједносно осјетљивих података, који укључују и регистрационе податке корисника, од неауторизованог приступа на основу поновног коришћења претходно обрисаних или архивираних података,

8) да се локалне мрежне компоненте чувају у физички заштићеном окружењу и да се њихова конфигурација периодично контролише у циљу испитивања усклађености са захтјевима из интерних правила,

9) уређаје за континуирано надгледање и алармирање (системи за детекцију напада и системи за надгледање контроле приступа и аларма) за поуздану детекцију, регистрацију и реакцију на било какав неауторизовани и/или нерегуларни покушај приступа ресурсима који се користе за издавање временских жигова.

Члан 23.

(1) Систем за формирање временског жига мора да обезбједи чување свих релевантних података који се тичу издавања временских жигова у временском периоду дефинисаном у складу са овим законом и Политиком пружања услуга издавања временског жига, и то посебно у циљу обезбјеђивања доказа о издатим временским жиговима за службене поступке и друге правне сврхе.

(2) Подаци из става 1. овог члана, укључују податке о корисницима и информације о значајним догађајима везаним за оперативни рад издаваоца временског жига, као и издавања временских жигова.

Члан 24.

Издавалац временског жига обезбјеђује :

1) документовање специфичних догађаја и података који требају да се евидентирају,

2) тајност и интегритет текућих и архивираних записа о временским жиговима,

3) комплетно и поудано архивирање информација о издавању временских жигова у складу са обајевљеним Политиком пружања услуге издавања временског жига,

4) да су записи у вези издавања временских жигова расположиви за потребе службених поступака као доказ правилно извршеног издавања временског жига,

5) евидентирање свих догађаја на начин да се не могу лако обрисати или уништити (изузев у циљу преноса на дуготрајне медије за чување) у оквиру временског периода у коме се морају чувати,

6) заштиту приватности података корисника, осим ако је корисник изричито пристао на другачије услове,

7) евидентирање свих догађаја у вези са животним циклусом асиметричних кључева и цертификата,

8) евидентирање свих догађаја у вези са синхронизацијом са извором тачног времена, укључујући и уобичајене рекалибрације и синхорнизације сатова који се употребљавају при издавању временских жигова,

9) евидентирање свих губитака синхронизације.

Члан 25.

Овај Правилник ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Српске“.

Број:
Датум:

МИНИСТАР
Проф. др Јасмин Комић