# PRAVILNIK
## O MJERAMA I POSTUPCIMA UPORABE I ZAŠTITE ELEKTRONIČKOG POTPISA, SREDSTAVA ZA FORMIRANJE ELEKTRONIČKOG POTPISA I SUSTAVA CERTIFICIRANJA

Članak 1.
(Predmet Pravilnika)

(1) Ovim Pravilnikom propisuju se tehničko-tehnološki postupci za formiranje sigurnog elektroničkog potpisa i bliži kriterijumi koje moraju zadovoljavati sredstva za formiranje sigurnog elektroničkog potpisa.
(2) Tehničko-tehnološki postupci i bliži kriterijumi iz stavka (1) ovoga članka moraju biti sukladni međunarodnim standardima i preporukama, odnosno drugim standardima, dokumentima i preporukama, koje se odnose na formiranje i provjeru sigurnog elektroničkog potpisa, utvrđenih ovim Pravilnikom.

Članak 2.
(Uvjeti za siguran elektronički potpis)

Sigurni elektronički potpis, pored uvjeta iz članka 14. Zakona o elektroničkom potpisu (u daljnjem tekstu: Zakon), mora da zadovolji i sljedeće bliže uvjete:

a) da je formiran primjenom sredstva za formiranje sigurnog elektroničkog potpisa (engl. SSCD: Secure Signature-Creation Device);
b) da se provjerava na temelju kvalificirane potvrde potpisnika, koja je validna u trenutku formiranja sigurnog elektroničkog potpisa.

Članak 3.
(Formiranje elektroničkog potpisa)

(1) Sigurni elektronički potpis formira se primjenom standardiziranih algoritama iz skupine RSA (engl. Rivest Shamir Adleman) odnosno DSA (engl. Digital Signature Algorithm).
(2) Kod izrade sigurnog elektroničkog potpisa obvezno se koristi hash funkcija iz skupine SHA-1 (Secure Hash Algorithm), odnosno RIPEMD 160 (engl. RACE Integrity Primitives Evaluation Message Digest).
(3) Kod izrade sigurnog elektroničkog potpisa u slučaju primjene sustava dva kriptografska ključa, duljina ključa za izradu sigurnog elektroničkog potpisa mora biti najmanje 1024 bita, uz primjenu kriptografskih algoritama iz skupine RSA/DSA i usklađeno sa međunarodnim standardom PKCS#1.
(4) Kriptografski moduli moraju se temeljiti na algoritmima i parametrima koji predstavljaju radno okruženje za izradu sigurnog elektroničkog potpisa suglasno trenutno važećim obrascima ugrađenim u dokument ETSI (European Telecommunications Standards Institute) ESI (Electronic Signatures and Infrastructures) SR (Special Report) 002 176 "Algorithms and Parameters for Secure Electronic Signatures".

Članak 4.
(Sredstva za formiranje sigurnog elektroničkog potpisa)

(1) Sredstva za formiranje sigurnog elektroničkog potpisa mora imati svojstva koja omogućuju naknadnu ugradnju novih algoritama sukladno daljnjim razvitkom kriptografskih tehnika i standarda.
(2) Sredstva za formiranje sigurnog elektroničkog potpisa iz stavka (1) ovoga članka moraju zadovoljavati sljedeće kriterijume, i to:
   a) da se podaci za formiranje sigurnog elektroničkog potpisa generiraju u samom sredstvu za formiranje sigurnog elektroničkog potpisa i da ga nikad ne napuštaju;
   b) da se sigurni elektronički potpis formira u samom sredstvu za formiranje sigurnog elektroničkog potpisa;
   c) da se osigura korištenje sredstva za formiranje sigurnog elektroničkog potpisa isključivo od strane potpisnika uz prethodno realiziranu pouzdanu proceduru autentikacije i
   d) da sredstvo mora biti takvo da je potpisnik u mogućnosti da ga koristi u različitim aplikacijama i informatičko-tehnološkim okruženjima.

Članak 5.
(Razmjena elektroničkih dokumenata)

Elektronička dokumenta potpisana sigurnim elektroničkim potpisom razmjenjuju se u formatu dokumenata u kojima su ugrađeni temeljni podaci o postupku, algoritmu i kvalificiranoj potvrdi potpisnika, kako bi primaltelj elektroničkog dokumenta mogao provjeriti sigurni elektronički potpis na bazi usaglašene tehnologije i postupaka.

Članak 6.
(Usklađivanje elektroničkog dokumenta)

Format elektroničkog dokumenta koji je potpisan sigurnim elektroničkim potpisom mora biti usklađen sa nekim od dokumenata:

a) PKCS#7 (engl. Cryptographic Message Syntax Standard) preporuka,
b) RFC 3852 "Cryptographic Message Syntax (CMS)",
c) ETSI ESI TS (engl. Technical Specification) 101 733 "CMS Advanced Electronic Signatures (CAdES)",
d) RFC 3275 XMLDSIG, ETSI ESI TS 101 903 "XML Advanced Electronic Signatures (XAdES)" ili
e) ETSI ESI TS 102 778 "PDF Advanced Electronic Signatures (PAdES)".

Članak 7.
(Kvalificirana potvrda)

(1) Kvalificirana potvrda mora biti usklađena sa preporukom ITU-T X.509 i dokumentima:
   a) ETSI ESI TS 101 862 "Qualified Certificate Profile",
   b) RFC 3739 "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile",
   c) RFC 3280 "Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL) Profile" i
   d) ETSI TS 102 280 "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons".
(2) Postupci za formiranje sigurnog elektroničkog potpisa trebaju biti sukladna dokumentima:
   a) ETSI ESI TR 102 272 "ASN.1 format for signature policies" ili
   b) ETSI ESI TR 102 038 "XML format for signature policies".

Članak 8.
(Način popunjavanja kvalificirane potvrde)

Polje "subject" kvalificirane potvrde mora da ima atribut "commonName". U atribut "commonName" se upisuje puno ime i prezime potpisnika i jedinstveni identifikator potpisnika unutar ovjeritelja. Podaci se upisuju sljedećim redom: ime, razmak, prezime, razmak i jedinstveni identifikator unutar ovjeritelja. Za atribut "commonName" se koristi UTF8String kodiranje, tako da sva slova iz imena i prezimena budu vjerno predstavljena odgovarajućim karakterima.

Članak 9.
(Postupak provjere)

(1) Postupak provjere sigurnog elektroničkog potpisa obuhvaća i postupak provjere kvalificirane potvrde potpisnika, koji se sastoji od:
   a) provjere roka važnosti date potvrde;

b) provjere podataka o ovjeritelju koje je izdalo kvalificiranu potvrdu potpisnika;
c) provjere da li se data potvrda nalazi na listi opozvanih potvrda.

(2) Moguće je izvršiti i dodane provjere u odnosu na stavak (1) ovoga članka ukoliko je to definirano u Pravilima nadležnog ovjeritelja koji je izdao kvalificiranu potvrdu.

Članak 10.

(Formiranje i provjera sigurnog elektroničkog potpisa)

Formiranje i provjera sigurnog elektroničkog potpisa se vrši primjenom:

a) sredstva za formiranje sigurnog elektroničkog potpisa (SSCD);
b) sigurne aplikacije za formiranje i provjeru sigurnog elektroničkog potpisa (SSCA: Secure Signature Creation Application i SSVA: Secure Signature Verification Application, respektivno);
c) tehničkih komponenata ovjeritelja;
d) kvalificirane potvrde.

Članak 11.

(Sigurna aplikacija za izradu sigurnog elektroničkog potpisa)

(1) Sigurna aplikacija za izradu sigurnog elektroničkog potpisa (SSCA: Secure Signature Creation Application) se koristi zajedno i neodvojivo od SSCD: Secure Signature Creation Device.
(2) SSCA u sebi može da sadrži i sigurnu aplikaciju za provjeru sigurnog elektroničkog potpisa (SSVA - Secure Signature Verification Application) i validaciju kvalificirane potvrde potpisnika, kao i prikaz rezultata.

Članak 12.

(Tehničke komponente)

Tehničke komponente iz djelatnosti overitelja jesu softverski i hardverski proizvodi koji:

a) kreiraju podatke za formiranje sigurnog elektroničkog potpisa i prenose ih u odgovarajući hardverski uređaj sa karakteristikama utvrđenim ovim Pravilnikom, ili ih generiraju izravno na datom hardverskom uređaju;
b) čine raspoloživim kvalificirane potvrde korisnika i statuse potvrda, odnosno liste opozvanih potvrda za naknadnu verifikaciju i provjeru statusa opozvanosti i, ako je potrebno, za preuzimanje od strane zainteresiranih stranaka.

Članak 13.

(Standardi za sredstvo za formiranje sigurnog elektroničkog potpisa)

Sredstvo za formiranje sigurnog elektroničkog potpisa (SSCD) iz članka 4. ovoga Pravilnika mora biti sukladne jednim od sljedećih standarda:

a) preferirano CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)";
b) FIPS 140-2 (Federal Information Processing Standard) razine 2 ili viših.

Članak 14.

(Aplikacija za izradu sigurnog elektroničkog potpisa)

Aplikacija za izradu sigurnog elektroničkog potpisa (SSCA) iz članka 11. stavak (1) ovoga Pravilnika treba da bude sukladan sljedećem standardu: CEN (European Committee for Standardization) Workshop Agreement 14170 "Security requirements for signature creation applications".

Članak 15.

(Aplikacija za provjeru sigurnog elektroničkog potpisa)

Aplikacija za provjeru sigurnog elektroničkog potpisa (SSVA) iz članka 13. stavak (2) ovoga Pravilnika treba da bude sukladan sljedećim standardom: CEN Workshop Agreement 14171 "General guidelines for electronic signature verification".

Članak 16.

(Standardi za tehničke komponente ovjeritelja)

Tehničke komponente ovjeritelja iz članka 12. ovoga Pravilnika moraju biti sukladni sljedećim standardima:

a) za generiranje asimetričnih kriptografskih ključeva u ovjeritelju sukladno nekim od standarda:
   1) CEN Workshop Agreement 14167-3: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Modules for CSP Key Generation Services - Protection Profile (CMCKG-PP)", (2) CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)",
   2) FIPS 140-2 (Federal Information Processing Standard) razine 3 ili viši;
b) za generiranje kvalificiranih potvrda sukladno nekim od standarda:
   1) CEN Workshop Agreement 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection profile (MCSO-PP)",
   2) CEN Workshop Agreement 14167-4: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic Module for CSP Signing Operations - Protection profile (CMCSO-PP)",
   3) CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)",
   4) FIPS 140-2 (Federal Information Processing Standard) razine 3 ili viši.

Članak 17.

(Programska oprema i postupci)

Programska oprema i postupci primjenom kojih se vrši provjera sigurnog elektroničkog potpisa moraju u cjelosti onemogućiti dobivanje podataka za formiranje sigurnog elektroničkog potpisa pomoću podataka za njegovu provjeru.

Članak 18.

(Zaštita podataka za formiranje sigurnog elektroničkog potpisa)

(1) Potpisnik je dužan da zaštiti podatke za formiranje sigurnog elektroničkog potpisa od neovlaštenog pristupa, otuđivanja i nepravilne uporabe.
(2) Zaštita iz stavka (1) ovoga članka dodano obuhvaća primjenu lozinki ili PIN kodova, biometrijskih postupaka ili drugih zaštitnih tehnika.

Članak 19.

(Stupanje na snagu)

Ovaj Pravilnik stupa na snagu narednog dana od dana objave u "Službenom glasniku BiH".

VM broj 9/17
25. siječnja 2017. godine
Sarajevo

Predsjedatelj
Vijeća ministara BiH
Dr. **Denis Zvizdić**, v. r.

---

На основу члана 17. Закона о Савјету министара Босне и Херцеговине ("Службени гласник БиХ", бр. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 и 24/08) и члана 26. став (1) Закона о електронском потпису ("Службени гласник БиХ", број 91/06), на приједлог министра комуникација и транспорта Босне и Херцеговине, Савјет министара Босне и

Херцеговине на 89. сједници, одржаној 25. јануара 2017. године, донио је

# ПРАВИЛНИК
## О МЈЕРАМА И ПОСТУПЦИМА УПОТРЕБЕ И ЗАШТИТЕ ЕЛЕКТРОНСКОГ ПОТПИСА, СРЕДСТАВА ЗА ФОРМИРАЊЕ ЕЛЕКТРОНСКОГ ПОТПИСА И СИСТЕМА СЕРТИФИКОВАЊА

Члан 1.

(Предмет Правилника)

(1) Овим Правилником прописују се техничко-технолошки поступци за формирање безбједног електронског потписа и ближи критеријуми које морају задовољавати средства за формирање безбједног електронског потписа.

(2) Техничко-технолошки поступци и ближи критеријуми из става (1) овог члана морају бити у складу са међународним стандардима и препорукама, односно другим стандардима, документима и препорукама, које се односе на формирање и провјеру безбједног електронског потписа, утврђених овим Правилником.

Члан 2.

(Услови за безбједан електронски потпис)

Безбједни електронски потпис, поред услова из члана 14. Закона о електронском потпису (у даљем тексту: Закон), мора да задовољи и сљедеће ближе услове:

а) да је формиран примјеном средства за формирање безбједног електронског потписа (енгл. SSCD: Secure Signature-Creation Device);

б) да се провјерава на основу квалификоване потврде потписника, која је валидна у тренутку формирања безбједног електронског потписа.

Члан 3.

(Формирање електронског потписа)

(1) Безбједни електронски потпис формира се примјеном стандардизованих алгоритама из групе RSA (енгл. Rivest Shamir Adleman) односно DSA (енгл. Digital Signature Algorithm).

(2) Код израде безбједног електронског потписа обавезно се користи хасх функција из групе SHA-1 (Secure Hash Algorithm), односно RIPEMD 160 (енгл. RACE Integrity Primitives Evaluation Message Digest).

(3) Код израде безбједног електронског потписа у случају примјене система два криптографска кључа, дужина кључа за израду безбједног електронског потписа мора бити најмање 1024 бита, уз примјену криптографских алгоритама из групе RSA/DSA и усклађено са међународним стандардом PKCS#1.

(4) Криптографски модели морају се заснивати на алгоритмима и параметрима који представљају радно окружење за израду безбједног електронског потписа сагласно тренутно важећим обрасцима уграђеним у документ ETSI (European Telecommunications Standards Institute) ESI (Electronic Signatures and Infrastructures) SR (Special Report) 002 176 "Algorithms and Parameters for Secure Electronic Signatures".

Члан 4.

(Средства за формирање безбједног електронског потписа)

(1) Средства за формирање безбједног електронског потписа мора имати својства која омогућавају накнадну уградњу нових алгоритама у складу са даљим развојем криптографских техника и стандарда.

(2) Средства за формирање безбједног електронског потписа из става (1) овог члана морају задовољавати сљедеће критеријуме, и то:

а) да се подаци за формирање безбједног електронског потписа генеришу у самом средству за формирање безбједног електронског потписа и да га никад не напуштају;

б) да се безбједни електронски потпис формира у самом средству за формирање безбједног електронског потписа;

ц) да се обезбједи коришћење средства за формирање безбједног електронског потписа искључиво од стране потписника уз претходно реализовану поуздану процедуру аутентикације и

д) да средство мора бити такво да је потписник у могућности да га користи у различитим апликацијама и информатичко-технолошким окружењима.

Члан 5.

(Размјена електронских докумената)

Електронска документа потписана безбједним електронским потписом размјењују се у формату докумената у којима су уграђени основни подаци о поступку, алгоритму и квалификованој потврди потписника, како би прималац електронског документа могао провјерити безбједни електронски потпис на бази усаглашене технологије и поступака.

Члан 6.

(Усклађивање електронског документа)

Формат електронског документа који је потписан безбједним електронским потписом мора бити усклађен са неким од докумената:

а) PKCS#7 (engl. Cryptographic Message Syntax Standard) препорука,

б) RFC 3852 "Cryptographic Message Syntax (CMS)",

ц) ETSI ESI TS (engl. Technical Specification) 101 733 "CMS Advanced Electronic Signatures (CAdES)",

д) RFC 3275 XMLDSIG, ETSI ESI TS 101 903 "XML Advanced Electronic Signatures (XAdES)" ili

е) ETSI ESI TS 102 778 "PDF Advanced Electronic Signatures (PAdES)".

Члан 7.

(Квалификована потврда)

(1) Квалификована потврда мора бити усклађена са препоруком ITU-T X.509 и документима:

а) ETSI ESI TS 101 862 "Qualified Certificate Profile",

б) RFC 3739 "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile",

ц) RFC 3280 "Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL) Profile" i

д) ETSI TS 102 280 "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons".

(2) Поступци за формирање безбједног електронског потписа требају бити у складу са документима:

а) ETSI ESI TR 102 272 "ASN.1 format for signature policies" ili

б) ETSI ESI TR 102 038 "XML format for signature policies".

Члан 8.

(Начин попуњавања квалификоване потврде)

Поље "subject" квалификоване потврде мора да има атрибут "commonName". У атрибут "commonName" се уписује пуно име и презиме потписника и јединствени идентификатор потписника у оквиру овјериоца. Подаци се уписују сљедећим редом: име, размак, презиме, размак и јединствени идентификатор у оквиру овјериоца. За атрибут "commonName" се користи UTF8String кодирање, тако да сва

слова из имена и презимена буду вјерно представљена одговарајућим карактерима.

Члан 9.

(Поступак провјере)

(1) Поступак провјере безбједног електронског потписа обухвата и поступак провјере квалификоване потврде потписника, који се састоји од:
   а) провјере рока важности дате потврде;
   б) провјере података о овјериоцу које је издало квалификовану потврду потписника;
   ц) провјере да ли се дата потврда налази на листи опозваних потврда.
(2) Могуће је извршити и додатне провјере у односу на став (1) овог члана уколико је то дефинисано у Правилима надлежног овјериоца који је издао квалификовану потврду.

Члан 10.

(Формирање и провјера безбједног електронског потписа)

Формирање и провјера безбједног електронског потписа се врши примјеном:
   а) средства за формирање безбједног електронског потписа (SSCD);
   б) безбједне апликације за формирање и провјеру безбједног електронског потписа (SSCA: Secure Signature Creation Application i SSVA: Secure Signature Verification Application, респективно);
   ц) техничких компонената овјерилаца;
   д) квалификоване потврде.

Члан 11.

(Безбједна апликација за израду безбједног електронског потписа)

(1) Безбједна апликација за израду безбједног електронског потписа (SSCA: Secure Signature Creation Application) се користи заједно и неодвојиво од SSCD: Secure Signature Creation Device.
(2) SSCA у себи може да садржи и безбједну апликацију за провјеру безбједног електронског потписа (SSVA - Secure Signature Verification Application) и валидацију квалификоване потврде потписника, као и приказ резултата.

Члан 12.

(Техничке компоненте)

Техничке компоненте из дјелатности оверилаца јесу софтверски и хардверски производи који:
   а) креирају податке за формирање безбједног електронског потписа и преносе их у одговарајући хардверски уређај са карактеристикама утврђеним овим Правилником, или их генеришу директно на датом хардверском уређају;
   б) чине расположивим квалификоване потврде корисника и статусе потврда, односно листе опозваних потврда за накнадну верификацију и провјеру статуса опозваности и, ако је потребно, за преузимање од стране заинтересованих страна.

Члан 13.

(Стандарди за средство за формирање безбједног електронског потписа)

Средство за формирање безбједног електронског потписа (SSCD) из члана 4. овог Правилника мора бити у складу са једним од сљедећих стандарда:
   а) преферирано CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)";
   б) FIPS 140-2 (Federal Information Processing Standard) нивоа 2 или виших.

Члан 14.

(Апликација за израду безбједног електронског потписа)

Апликација за израду безбједног електронског потписа (SSCA) из члана 11. став (1) овог Правилника треба да буде у складу са сљедећим стандардом: CEN (European Committee for Standardization) Workshop Agreement 14170 "Security requirements for signature creation applications".

Члан 15.

(Апликација за провјеру безбједног електронског потписа)

Апликација за провјеру безбједног електронског потписа (SSVA) из члана 13. став (2) овог Правилника треба да буде у складу са сљедећим стандардом: CEN Workshop Agreement 14171 "General guidelines for electronic signature verification".

Члан 16.

(Стандарди за техничке компоненте овјериоца)

Техничке компоненте овјериоца из члана 12. овог Правилника морају бити у складу са сљедећим стандардима:
   а) за генерисање асиметричних криптографских кључева у овјериоцу у складу са неким од стандарда:
      1) CEN Workshop Agreement 14167-3: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Modules for CSP Key Generation Services - Protection Profile (CMCKG-PP)", (2) CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)",
      2) FIPS 140-2 (Federal Information Processing Standard) нивоа 3 или виши;
   б) за генерисање квалификованих потврда у складу са неким од стандарда:
      1) CEN Workshop Agreement 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection profile (MCSO-PP)",
      2) CEN Workshop Agreement 14167-4: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic Module for CSP Signing Operations - Protection profile (CMCSO-PP)",
      3) CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)",
      4) FIPS 140-2 (Federal Information Processing Standard) нивоа 3 или виши.

Члан 17.

(Програмска опрема и поступци)

Програмска опрема и поступци примјеном којих се врши провјера безбједног електронског потписа морају у потпуности онемогућити добијање података за формирање безбједног електронског потписа помоћу података за његову провјеру.

Члан 18.

(Заштита података за формирање безбједног електронског потписа)

(1) Потписник је дужан да заштити податке за формирање безбједног електронског потписа од неовлашћеног приступа, отуђивања и неправилне употребе.

(2) Заштита из става (1) овог члана додатно обухвата примјену лозинки или ПИН кодова, биометријских поступака или других заштитних техника.

Члан 19.
(Ступање на снагу)

Овај Правилник ступа на снагу наредног дана од дана објављивања у "Службеном гласнику БиХ".

СМ број 9/17
25. јануара 2017. године
Сарајево

Предсједавајући
Савјета министара БиХ
Др **Денис Звиздић**, с. р.

---

Na osnovu člana 17. Zakona o Vijeću ministara Bosne i Hercegovine ("Službeni glasnik BiH", br. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 i 24/08) i člana 26. stav (1) Zakona o elektronskom potpisu ("Službeni glasnik BiH", broj 91/06), na prijedlog ministra komunikacija i prometa Bosne i Hercegovine, Vijeće ministara Bosne i Hercegovine na 89. sjednici, održanoj 25. januara 2017. godine, donijelo je

# PRAVILNIK
## O MJERAMA I POSTUPCIMA UPOTREBE I ZAŠTITE ELEKTRONSKOG POTPISA, SREDSTAVA ZA FORMIRANJE ELEKTRONSKOG POTPISA I SISTEMA CERTIFICIRANJA

Član 1.
(Predmet Pravilnika)

(1) Ovim Pravilnikom propisuju se tehničko-tehnološki postupci za formiranje sigurnog elektronskog potpisa i bliži kriterijumi koje moraju zadovoljavati sredstva za formiranje sigurnog elektronskog potpisa.
(2) Tehničko-tehnološki postupci i bliži kriterijumi iz stava (1) ovog člana moraju biti u skladu sa međunarodnim standardima i preporukama, odnosno drugim standardima, dokumentima i preporukama, koje se odnose na formiranje i provjeru sigurnog elektronskog potpisa, utvrđenih ovim Pravilnikom.

Član 2.
(Uvjeti za siguran elektronski potpis)

Sigurni elektronski potpis, pored uvjeta iz člana 14. Zakona o elektronskom potpisu (u daljem tekstu: Zakon), mora da zadovolji i slijedeće bliže uvjete:

a) da je formiran primjenom sredstva za formiranje sigurnog elektronskog potpisa (engl. SSCD: Secure Signature-Creation Device);
b) da se provjerava na osnovu kvalificirane potvrde potpisnika, koja je validna u trenutku formiranja sigurnog elektronskog potpisa.

Član 3.
(Formiranje elektronskog potpisa)

(1) Sigurni elektronski potpis formira se primjenom standardiziranih algoritama iz grupe RSA (engl. Rivest Shamir Adleman) odnosno DSA (engl. Digital Signature Algorithm).
(2) Kod izrade sigurnog elektronskog potpisa obavezno se koristi hash funkcija iz grupe SHA-1 (Secure Hash Algorithm), odnosno RIPEMD 160 (engl. RACE Integrity Primitives Evaluation Message Digest).
(3) Kod izrade sigurnog elektronskog potpisa u slučaju primjene sistema dva kriptografska ključa, dužina ključa za izradu sigurnog elektronskog potpisa mora biti najmanje 1024 bita, uz primjenu kriptografskih algoritama iz grupe RSA/DSA i usklađeno sa međunarodnim standardom PKCS#1.
(4) Kriptografski moduli moraju se zasnivati na algoritmima i parametrima koji predstavljaju radno okruženje za izradu sigurnog elektronskog potpisa saglasno trenutno važećim obrascima ugrađenim u dokument ETSI (European Telecommunications Standards Institute) ESI (Electronic Signatures and Infrastructures) SR (Special Report) 002 176 "Algorithms and Parameters for Secure Electronic Signatures".

Član 4.
(Sredstva za formiranje sigurnog elektronskog potpisa)

(1) Sredstva za formiranje sigurnog elektronskog potpisa mora imati svojstva koja omogućavaju naknadnu ugradnju novih algoritama u skladu sa daljim razvojem kriptografskih tehnika i standarda.
(2) Sredstva za formiranje sigurnog elektronskog potpisa iz stava (1) ovog člana moraju zadovoljavati slijedeće kriterijume, i to:
   a) da se podaci za formiranje sigurnog elektronskog potpisa generiraju u samom sredstvu za formiranje sigurnog elektronskog potpisa i da ga nikad ne napuštaju;
   b) da se sigurni elektronski potpis formira u samom sredstvu za formiranje sigurnog elektronskog potpisa;
   c) da se osigura korištenje sredstva za formiranje sigurnog elektronskog potpisa isključivo od strane potpisnika uz prethodno realiziranu pouzdanu proceduru autentikacije i
   d) da sredstvo mora biti takvo da je potpisnik u mogućnosti da ga koristi u različitim aplikacijama i informatičko-tehnološkim okruženjima.

Član 5.
(Razmjena elektronskih dokumenata)

Elektronska dokumenta potpisana sigurnim elektronskim potpisom razmjenjuju se u formatu dokumenata u kojima su ugrađeni osnovni podaci o postupku, algoritmu i kvalificiranoj potvrdi potpisnika, kako bi primalac elektronskog dokumenta mogao provjeriti sigurni elektronski potpis na bazi usaglašene tehnologije i postupaka.

Član 6.
(Usklađivanje elektronskog dokumenta)

Format elektronskog dokumenta koji je potpisan sigurnim elektronskim potpisom mora biti usklađen sa nekim od dokumenata:

a) PKCS#7 (engl. Cryptographic Message Syntax Standard) preporuka,
b) RFC 3852 "Cryptographic Message Syntax (CMS)",
c) ETSI ESI TS (engl. Technical Specification) 101 733 "CMS Advanced Electronic Signatures (CAdES)",
d) RFC 3275 XMLDSIG ETSI ESI TS 101 903 "XML *Advanced* Electronic Signatures (XAdES)" ili
e) ETSI ESI TS 102 778 "PDF Advanced Electronic Signatures (PAdES)".

Član 7.
(Kvalificirana potvrda)

(1) Kvalificirana potvrda mora biti usklađena sa preporukom ITU-T X.509 i dokumentima:
   a) ETSI ESI TS 101 862 "Qualified Certificate Profile",
   b) RFC 3739 "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile",
   c) RFC 3280 "Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL) Profile" i
   d) ETSI TS 102 280 "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons".
(2) Postupci za formiranje sigurnog elektronskog potpisa trebaju biti u skladu sa dokumentima:

a) ETSI ESI TR 102 272 "ASN.1 format for signature policies" ili
b) ETSI ESI TR 102 038 "XML format for signature policies".

Član 8.
(Način popunjavanja kvalificirane potvrde)

Polje "subject" kvalificirane potvrde mora da ima atribut "commonName". U atribut "commonName" se upisuje puno ime i prezime potpisnika i jedinstveni identifikator potpisnika unutar ovjerioca. Podaci se upisuju slijedećim redom: ime, razmak, prezime, razmak i jedinstveni identifikator unutar ovjerioca. Za atribut "commonName" se koristi UTF8String kodiranje, tako da sva slova iz imena i prezimena budu vjerno predstavljena odgovarajućim karakterima.

Član 9.
(Postupak provjere)

(1) Postupak provjere sigurnog elektronskog potpisa obuhvata i postupak provjere kvalificirane potvrde potpisnika, koji se sastoji od:
a) provjere roka važnosti date potvrde;
b) provjere podataka o ovjeriocu koje je izdalo kvalificiranu potvrdu potpisnika;
c) provjere da li se data potvrda nalazi na listi opozvanih potvrda.
(2) Moguće je izvršiti i dodatne provjere u odnosu na stav (1) ovog člana ukoliko je to definirano u Pravilima nadležnog ovjerioca koji je izdao kvalificiranu potvrdu.

Član 10.
(Formiranje i provjera sigurnog elektronskog potpisa)

Formiranje i provjera sigurnog elektronskog potpisa se vrši primjenom:
a) sredstva za formiranje sigurnog elektronskog potpisa (SSCD);
b) sigurne aplikacije za formiranje i provjeru sigurnog elektronskog potpisa (SSCA: Secure Signature Creation Application i SSVA: Secure Signature Verification Application, respektivno);
c) tehničkih komponenata ovjerilaca;
d) kvalificirane potvrde.

Član 11.
(Sigurna aplikacija za izradu sigurnog elektronskog potpisa)

(1) Sigurna aplikacija za izradu sigurnog elektronskog potpisa (SSCA: Secure Signature Creation Application) se koristi zajedno i neodvojivo od SSCD: Secure Signature Creation Device.
(2) SSCA u sebi može da sadrži i sigurnu aplikaciju za provjeru sigurnog elektronskog potpisa (SSVA - Secure Signature Verification Application) i validaciju kvalificirane potvrde potpisnika, kao i prikaz rezultata.

Član 12.
(Tehničke komponente)

Tehničke komponente iz djelatnosti overilaca jesu softverski i hardverski proizvodi koji:
a) kreiraju podatke za formiranje sigurnog elektronskog potpisa i prenose ih u odgovarajući hardverski uređaj sa karakteristikama utvrđenim ovim Pravilnikom, ili ih generiraju direktno na datom hardverskom uređaju;
b) čine raspoloživim kvalificirane potvrde korisnika i statuse potvrda, odnosno liste opozvanih potvrda za naknadnu verifikaciju i provjeru statusa opozvanosti i, ako je potrebno, za preuzimanje od strane zainteresiranih strana.

Član 13.
(Standardi za sredstvo za formiranje sigurnog elektronskog potpisa)

Sredstvo za formiranje sigurnog elektronskog potpisa (SSCD) iz člana 4. ovog Pravilnika mora biti u skladu sa jednim od slijedećih standarda:
a) preferirano CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)";
b) FIPS 140-2 (Federal Information Processing Standard) nivoa 2 ili viših.

Član 14.
(Aplikacija za izradu sigurnog elektronskog potpisa)

Aplikacija za izradu sigurnog elektronskog potpisa (SSCA) iz člana 11. stav (1) ovog Pravilnika treba da bude u skladu sa slijedećim standardom: CEN (European Committee for Standardization) Workshop Agreement 14170 "Security requirements for signature creation applications".

Član 15.
(Aplikacija za provjeru sigurnog elektronskog potpisa)

Aplikacija za provjeru sigurnog elektronskog potpisa (SSVA) iz člana 13. stav (2) ovog Pravilnika treba da bude u skladu sa slijedećim standardom: CEN Workshop Agreement 14171 "General guidelines for electronic signature verification".

Član 16.
(Standardi za tehničke komponente ovjerioca)

Tehničke komponente ovjerioca iz člana 12. ovog Pravilnika moraju biti u skladu sa slijedećim standardima:
a) za generiranje asimetričnih kriptografskih ključeva u ovjeriocu u skladu sa nekim od standarda:
1) CEN Workshop Agreement 14167-3: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Modules for CSP Key Generation Services - Protection Profile (CMCKG-PP)", (2) CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)",
2) FIPS 140-2 (Federal Information Processing Standard) nivoa 3 ili viši;
b) za generiranje kvalificiranih potvrda u skladu sa nekim od standarda:
1) CEN Workshop Agreement 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection profile (MCSO-PP)",
2) CEN Workshop Agreement 14167-4: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic Module for CSP Signing Operations - Protection profile (CMCSO-PP)",
3) CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)",
4) FIPS 140-2 (Federal Information Processing Standard) nivoa 3 ili viši.

Član 17.
(Programska oprema i postupci)

Programska oprema i postupci primjenom kojih se vrši provjera sigurnog elektronskog potpisa moraju u potpunosti onemogućiti dobijanje podataka za formiranje sigurnog elektronskog potpisa pomoću podataka za njegovu provjeru.

Član 18.

(Zaštita podataka za formiranje sigurnog elektronskog potpisa)

(1) Potpisnik je dužan da zaštiti podatke za formiranje sigurnog elektronskog potpisa od neovlaštenog pristupa, otuđivanja i nepravilne upotrebe.

(2) Zaštita iz stava (1) ovog člana dodatno obuhvata primjenu lozinki ili PIN kodova, biometrijskih postupaka ili drugih zaštitnih tehnika.

Član 19.

(Stupanje na snagu)

Ovaj Pravilnik stupa na snagu narednog dana od dana objave u "Službenom glasniku BiH".

VM broj 9/17
25. januara 2017. godine
Sarajevo

Predsjedavajući
Vijeća ministara BiH
Dr. **Denis Zvizdić**, s. r.

**214**

Na temelju članka 17. Zakona o Vijeću ministara Bosne i Hercegovine ("Službeni glasnik BiH", br. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 i 24/08) i članka 26. stavak (1) Zakona o elektroničkom potpisu ("Službeni glasnik BiH", broj 91/06), na prijedlog ministra komunikacija i prometa Bosne i Hercegovine, Vijeće ministara Bosne i Hercegovine, na 88. sjednici, održanoj 18. siječnja 2017. godine, donijelo je

# PRAVILNIK
## O EVIDENCIJI OVJERITELJA

Članak 1.

(Predmet Pravilnika)

Ovim Pravilnikom propisuje se sadržaj i način vođenja evidencije ovjerilaca koji obavljaju usluge izdavanja kvalificiranih potvrda (u daljnjem tekstu: ovjeritelj), obrasci prijave za upis u evidenciju, prijave za upis promjena, kao i vrsta, sadržaj i način dostavljanja dokumentacije neophodne za uvođenje u evidenciju.

Članak 2.

(Evidencija ovjeritelja)

(1) Evidenciju ovjeritelja (u daljnjem tekstu: evidencija), sukladno članku 20. Zakona o elektroničkom potpisu, vodi Nadzorno tijelo.

(2) U evidenciju se upisuju sljedeći podaci:
   a) redni broj upisa u evidenciju ovjeritelja;
   b) datum upisa u evidenciju;
   c) naziv ovjeritelja;
   d) sjedište ovjeritelja (ulica i broj, poštanski broj i mjesto, država);
   e) poresko-identifikacijski broj (PIB);
   f) šifru i opis djelatnosti;
   g) broj telefona i faksa;
   h) elektronička adresa;
   i) ime i prezime, broj osobne iskaznice, adresa, telefon/faks, e-mail, stručna sprema odgovorne osobe, stručna sprema vlasnika/suvlasnika;
   j) vrsta i datum promjene podataka upisanih u evidenciju;
   k) datum brisanja iz evidencije.

Članak 3.

(Način vođenja evidencije)

(1) Evidencija se vodi u papirnom i elektroničkom obliku.

(2) Evidencija u elektroničkom obliku javno je dostupna na Internet stranici Nadzornog tijela.

(3) Prilikom vođenja evidencija iz stavka (1) ovoga članka, Nadzorno tijelo obrađuje osobne podatke sukladno propisima kojim je uređena zaštita osobnih podataka.

Članak 4.

(Prijava za upis u evidenciju)

(1) Prijava za upis u evidenciju (u daljnjem tekstu: prijava) podnosi se u pismenom obliku, neposredno ili poštom, na Obrascu 1 koji je privitak ovoga Pravilnika i čini njegov sastavni dio.

(2) Ovjeritelj je dužan da prijavu podnese odmah nakon početka obavljanja usluga izdavanja kvalificiranih potvrda.

Članak 5.

(Dokumentacija uz prijavu)

(1) Uz prijavu ovjeritelj prilaže sljedeću dokumentaciju:
   a) izvod o upisu pravne osobe u registar;
   b) bilans stanja i bilans uspeha za posljednju poslovnu godinu;
   c) interna pravila rada;
   d) akt o unutarnjem ustroju ovjeritelja;
   e) spisak uposlenih, stručnu spremu, osposobljenost i radni status uposlenih na poslovima koji se odnose na usluge izdavanja potvrda.

(2) Dokumentacija iz stavka (1) ovoga članka podnosi se u originalu ili se prilaže preslika ovjerena od strane nadležnog tijela.

Članak 6.

(Sastavni dio evidencije)

(1) Pored podataka navedenih u članku 2. ovoga Pravilnika sastavni dio evidencije čini i dokumentacija na temelju koje se vrši upis u evidenciju.

(2) Dokumentacija iz stavka (1) ovoga članka čuva se sukladno propisima kojim je uređeno čuvanje arhivske građe.

Članak 7.

(Način podnošenja prijave)

(1) Prijava se može podnijeti i elektroničkim putem, tako što podnositelj unosi podatke u Obrazac iz članka 4. stavak (1) ovoga Pravilnika, koji se objavljuje na Internet stranici Nadzornog tijela, a dokumentacija koja se prilaže uz prijavu dostavlja se u elektroničkoj formi na elektroničku adresu Nadzornog tijela.

(2) Podnositelj je dužan da u roku od pet dana od dana podnošenja prijave elektroničkim putem, dostavi Nadzornom tijelu dokumentaciju iz članka 5. stavak (2) ovoga Pravilnika.

(3) Ako dokumentacija nije dostavljena na način i u roku iz stavka (2) ovoga članka smatrat će se da prijava nije podnijeta.

(4) Kao datum i vrijeme podnošenja prijave uzima se datum i vrijeme dostavljanja dokumentacije iz članka 5. Nadzornom tijelu.

Članak 8.

(Upis u evidenciju)

Nadzorno tijelo vrši upis ovjeritelja u evidenciju odmah nakon podnošenja prijave.

Članak 9.

(Prijava promjene podataka)

Ovjeritelj je dužan da prijavi svaku promjenu podataka koji se vode u evidenciji, a koja nastupi tijekom obavljanja djelatnosti i to u roku od deset dana od dana nastanka promjene, kao i činjenicu da je prestalo da obavlja usluge izdavanja potvrda, radi brisanja iz evidencije.

Članak 10.

(Ovlaštenje za podnošenje prijave)

(1) Prijavu za upis promjene ili brisanje iz evidencije podnosi ovjeritelj na Obrascu 2 koji je privitak ovoga Pravilnika i čini njegov sastavni dio.