Pravilnik o uslovima koje moraju da ispunjavaju kvalifikovani elektronski sertifikati

Pravilnik je objavljen u "Službenom glasniku RS", br. 34/2018 i 81/2018.

I. UVODNE ODREDBE

Član 1.

Ovim pravilnikom propisuju se uslovi koje moraju da ispunjavaju kvalifikovani elektronski sertifikati za elektronski potpis, elektronski pečat i autentikaciju sajtova.

Član 2.

Kvalifikovani elektronski sertifikati za elektronski potpis, elektronski pečat i autentikaciju sajtova moraju da budu u skladu sa odgovarajućim međunarodnim standardima i preporukama, odnosno drugim standardima, dokumentima i preporukama, koje se odnose na format i sadržaj elektronskih sertifikata.

Pružalac usluge izdavanja kvalifikovanog elektronskog sertifikata (u daljem tekstu: izdavalac sertifikata), kvalifikovane elektronske sertifikate izdaje u skladu sa preporukom ITU X.509 i dokumentima ETSI EN 319 412-1 "Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 1: Overview and common data structures" i IETF RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

Član 3.

Kvalifikovani elektronski sertifikat obavezno sadrži jednu ili više izjava da se sertifikat koristi kao kvalifikovani elektronski sertifikat (polje "qcStatements") prema dokumentu ETSI EN 319 412-5 "Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 5: QCStatements" zasnovano na dokumentu IETF RFC 3739 "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile", u skladu sa politikom izdavanja sertifikata koju primenjuje izdavalac sertifikata i uslovima propisanim ovim pravilnikom za pojedinačne vrste sertifikata.

Član 4.

Izdavalac sertifikata izdaje kvalifikovani elektronski sertifikat u skladu sa politikom izdavanja sertifikata koju primenjuje za izdavanje sertifikata, tako što formira napredni elektronski potpis ili napredni elektronski pečat na osnovu svog asimetričnog privatnog ključa.

Izbor algoritma naprednog elektronskog potpisa treba da bude u skladu sa dokumentom ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI) - Cryptographic Suites".

Kvalifikovani elektronski sertifikat obavezno sadrži oznaku politike pružaoca koja je primenjena za izdavanje sertifikata.

Član 5.

Kvalifikovani elektronski sertifikat obavezno sadrži tačno vreme izdavanja sertifikata.

II. KVALIFIKOVANI ELEKTRONSKI SERTIFIKATI ZA ELEKTRONSKI POTPIS

Član 6.

Kvalifikovani elektronski sertifikat za elektronski potpis obavezno ima sadržaj u skladu sa članom 43. Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju ("Službeni glasnik RS", broj 94/17 - u daljem tekstu: Zakon) u delu koji se odnosi na sertifikat za elektronski potpis i potpisnika.

Izdavalac sertifikata izdaje kvalifikovane elektronske sertifikate za elektronski potpis u skladu dokumentom ETSI EN 319 412-2 "Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 2: Certificate profile for certificates issued to natural persons".

Član 7.

Polje "Subject" kvalifikovanog elektronskog sertifikata za elektronski potpis sadrži skup atributa koji jedinstveno identifikuju potpisnika, a najmanje:

1) Atribut "countryName" koji sadrži dvoslovnu oznaku zemlje prema standardu EN ISO 3166-1:2013 "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes", sa značenjem koje je definisano politikom pružaoca usluge izdavanja sertifikata;

2) Oba atributa "givenName" i "surname" koji redom sadrže puno ime i prezime potpisnika, ukoliko sertifikat ne sadrži pseudonim, odnosno samo atribut "pseudonym", koji sadrži pseudonim ukoliko je pseudonim upotrebljen u sertifikatu;

3) Atribut "commonName" koji počinje vrednostima atributa "givenName" i "surname" razdvojenih razmakom ukoliko sertifikat ne sadrži pseudonim, odnosno vrednošću atributa "pseudonym" ukoliko je pseudonim upotrebljen u sertifikatu;

4) Jedan ili više atributa "serialNumber" koji sadrže identifikaciju potpisnika prema formatu iz dokumenta ETSI EN 319 412-1 "Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 1: Overview and common data structures", odeljak 5.1.3.

Atribut "commonName" ne sme da se završava sa 13 ili više uzastopnih numeričkih karaktera, niti da se završava crticom iza koje slede dva slovna karaktera i niz numeričkih karaktera.

Atributi "givenName", "surname", "pseudonym" i "commonName" obavezno se predstavljaju u UTF8String kodiranju tako da sva slova budu verno predstavljena odgovarajućim karakterima.

Atribut "serialNumber" predstavlja se u PrintableString kodiranju prema ASN.1 specifikaciji u skladu sa dokumentom IETF RFC 5280.

Atribut "serialNumber" iz ovog člana definisan prema dokumentu ITU-T X.520 predstavlja deo jedinstvenog imena potpisnika u polju "Subject" i razlikuje se od polja "serialNumber" sertifikata. Polje "serialNumber" sertifikata obavezno sadrži serijski broj kvalifikovanog elektronskog sertifikata, jedinstven u okviru izdavaoca kvalifikovanog elektronskog sertifikata u skladu sa članom 43. Zakona, iskazan kao pozitivan ceo broj predstavljen saglasno dokumentu IETF RFC 5280.

Član 8.

Ukoliko je u zahtevu za izdavanje sertifikata potpisnik zahtevao da sertifikat sadrži JMBG i kada sertifikat sadrži JMBG, izdavalac sertifikata upisuje JMBG u samo jedan od atributa "serialNumber" iz polja "Subject" na način određen u dokumentu ETSI EN 319 412-1, odeljak 5.1.3, za referencu tipa "PNO" i to u formatu: troslovna oznaka PNO (prema ASCII kodiranju sekvenca 80, 78, 79), zatim dvoslovna oznaka zemlje RS (prema ASCII kodiranju sekvenca 82, 83), crtica (45 prema ASCII kodiranju) i na kraju JMBG potpisnika.

Član 9.

Ukoliko kvalifikovani elektronski sertifikat za elektronski potpis sadrži jedan ili više brojeva putne isprave potpisnika, svaki broj putne isprave se upisuje u jedan od atributa "serialNumber" iz polja "Subject" na način određen u dokumentu ETSI EN 319 412-1 odeljak 5.1.3 za referencu tipa "PAS" i to u formatu: troslovna oznaka PAS (prema ASCII kodiranju sekvenca 80, 65, 83), dvoslovna oznaka zemlje izdavaoca putne isprave prema standardu EN ISO 3166-1:2013 predstavljena ASCII karakterima, crtica (45 prema ASCII kodiranju) i na kraju broj putne isprave potpisnika.

Ukoliko se u kvalifikovanom elektronskom sertifikatu za elektronski potpis pojavljuje više atributa sa brojem putne isprave, oznaka zemlje izdavaoca putne isprave mora biti jedinstvena u svakom od njih.

Ukoliko kvalifikovani elektronski sertifikat za elektronski potpis sadrži broj putne isprave, izdavalac sertifikata je obavezan da politikom izdavanja sertifikata obezbedi da sertifikat neće biti validan nakon datuma isteka bilo koje putne isprave čiji je broj sadržan u sertifikatu.

Član 10.

Kvalifikovane elektronske sertifikate za elektronski potpis koji sadrže JMBG ili broj putne isprave potpisnika izdavalac sertifikata ne sme da učini javno dostupnim, osim ako za to nema saglasnost potpisnika.

Član 11.

Kvalifikovani elektronski sertifikat za elektronski potpis u polju "Subject" može da sadrži i dodatne atribute "serialNumber" prema jednoj od šema iz standarda ETSI EN 319 412-1, odeljak 5.1.3 uključujući i lokalno definisane šeme.

Upotreba lokalnih šema "CA:" (prema ASCII kodiranju sekvenca 67, 65, 58) i "SN:" (prema ASCII kodiranju sekvenca 83, 78, 58) sa dvoslovnom oznakom zemlje RS rezervisana je za potrebe izdavaoca sertifikata na način i kada je to predviđeno politikom izdavaoca sertifikata.

Član 12.

Kvalifikovani elektronski sertifikat za elektronski potpis u polju "qcStatements" obavezno sadrži predefinisanu izjavu "qcStatement-2" prema dokumentu IETF RFC 3739 koja uključuje semantički identifikator "id-etsi-qcs-semanticsId-Natural" koji je određen u standardu ETSI EN 319 412-1, odeljak 5.1.2.

Ukoliko se u kvalifikovanom elektronskom sertifikatu za elektronski potpis pojavljuje jedan ili više atributa "serialNumber" prema šemi rezervisanoj za potrebe izdavaoca, izjava "qcStatement-2" obavezno sadrži listu "nameRegistrationAuthorities" i u toj listi referencu na politiku izdavaoca ili drugi dokument koji definiše semantiku lokalne šeme, u skladu sa standardom ETSI EN 319 412-1, odeljak 5.1.3.

Član 13.

Polje "Subject" kvalifikovanog elektronskog sertifikata za elektronski potpis može da sadrži i druge atribute koji, na primer, povezuju potpisnika sa pravnim licem ili drugom organizacijom, a u skladu sa ovim pravilnikom i politikom izdavaoca.

U polju "Subject" atributi "countryName" i "commonName" pojavljuju se samo jednom.

Član 14.

Polje "Key Usage" kvalifikovanog elektronskog sertifikata za elektronski potpis mora uključivati "Non-Repudiation" tj. "contentCommitment" bit.

Član 15.

Kvalifikovani elektronski sertifikat za elektronski potpis u polju "Certificate Policies" obavezno sadrži najmanje identifikator politike QCP-n-qscd u skladu sa dokumentom ETSI EN 319 411-2 "Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 2: Requirements for trust service providers issuing EU qualified certificates", odeljak 4.2.5.

Član 16.

Kvalifikovani elektronski sertifikat za elektronski potpis obavezno sadrži u polju "qcStatements" izjave QcCompliance, QcSSCD i, izjavu QcType sa identifikatorom "id-etsi-qcs-esign", a prema dokumentu ETSI EN 319 412-5.

III. KVALIFIKOVANI ELEKTRONSKI SERTIFIKATI ZA ELEKTRONSKI PEČAT

Član 17.

Kvalifikovani elektronski sertifikat za elektronski pečat obavezno ima sadržaj u skladu sa članom 43. Zakona u delu koji se odnosi na sertifikat za elektronski pečat i pečatioca.

Ukoliko je pečatilac pravno lice ili fizičko lice u svojstvu registrovanog subjekta, izdavalac sertifikata izdaje kvalifikovane elektronske sertifikate za elektronski pečat u skladu dokumentom ETSI EN 319 412-3 "Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 3: Certificate profile for certificates issued to legal persons".

Ukoliko je pečatilac fizičko lice, naziv iz člana 43. stav 1. tačka 3. podtačka 2. Zakona uključuje svojstvo u kome se lice predstavlja, a koje se dokazuje javnom ispravom izdatom na osnovu zakona.

U slučaju iz stava 3. ovog člana shodno se primenjuju odredbe ovog pravilnika koje se odnose na fizičko lice u svojstvu registrovanog subjekta.

Član 18.

Polje "Subject" kvalifikovanog elektronskog sertifikata za elektronski pečat sadrži skup atributa koji jedinstveno identifikuju pečatioca, a najmanje:

1) Atribut "countryName" koji sadrži dvoslovnu oznaku zemlje prema standardu EN ISO 3166-1:2013 u kojoj je pečatilac registrovan;
2) Atribut "organizationName" koji sadrži naziv odnosno puno poslovno ime pečatioca;
3) Atribut "commonName" koji počinje vrednošću atributa "organizationName".

Kvalifkovani elektronski sertifikat za elektronski pečat ne sme da u polju "Subject" sadrži atribute "givenName" i "surname".

Član 19.

Polje "Subject" kvalifikovanog elektronskog sertifikata za elektronski pečat može da sadrži jedan ili više atributa "organizationIdentifier" koji sadrže identifikaciju pečatioca prema formatu iz dokumenta ETSI EN 319 412-1 "Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 1: Overview and common data structures", odeljak 5.1.4.

Ukoliko pečatilac ima matični broj koji je pečatiocu dodelio Republički zavod za statistiku (matični broj) polje "Subject" obavezno sadrži atribut "organizationIdentifier" prema dokumentu ETSI EN 319 412-1 odeljak 5.1.4 za referencu lokalne šeme "MB:" i to u formatu: oznaka MB: (prema ASCII kodiranju sekvenca 77, 66, 58), zatim dvoslovna oznaka zemlje RS (prema ASCII kodiranju sekvenca 82, 83), crtica (45 prema ASCII kodiranju) i na kraju matični broj.

Ukoliko pečatilac ima poreski identifikacioni broj (PIB) koji je pečatiocu dodelio nadležan poreski organ polje "Subject" obavezno sadrži atribut "organizationIdentifier" prema dokumentu ETSI EN 319 412-1 odeljak 5.1.4 za referencu tipa "VAT" i to u formatu: troslovna oznaka VAT (prema ASCII kodiranju sekvenca 86, 65, 84), zatim dvoslovna oznaka zemlje RS (prema ASCII kodiranju sekvenca 82, 83), crtica (45 prema ASCII kodiranju) i na kraju PIB.

Član 20.

Kvalifikovani elektronski sertifikat za elektronski pečat u polju "qcStatements" obavezno sadrži predefinisanu izjavu "qcStatement-2" prema dokumentu IETF RFC 3739 koja uključuje semantički identifikator "id-etsi-qcs-semanticsId-Legal" koji je određen u standardu ETSI EN 319 412-1, odeljak 5.1.2.

Ukoliko kvalifikovani elektronski sertifikat za elektronski pečat sadrži matični broj izjava "qcStatement-2" obavezno sadrži listu "nameRegistrationAuthorities" i u toj listi referencu na politiku izdavaoca ili drugi dokument koji upućuje na ovaj pravilnik i semantiku lokalne šeme "MB:", u skladu sa standardom ETSI EN 319 412-1, odeljak 5.1.4.

Član 21.

Atributi "commonName" i "organizationName" obavezno se predstavljaju u UTF8String kodiranju tako da sva slova budu verno predstavljena odgovarajućim karakterima.

Član 22.

Polje "Subject" kvalifikovanog elektronskog sertifikata za elektronski pečat može da sadrži i druge atribute, a u skladu sa ovim pravilnikom i politikom izdavaoca.

U polju "Subject" atributi "countryName" i "commonName" pojavljuju se samo jednom.

Član 23.

Polje "Key Usage" kvalifikovanog elektronskog sertifikata za elektronski pečat mora uključivati "Non-Repudiation" tj. "contentCommitment" bit.

Član 24.

Kvalifikovani elektronski sertifikat za elektronski pečat u polju "Certificate Policies" obavezno sadrži najmanje identifikator politike QCP-l-qscd u skladu sa dokumentom ETSI EN 319 411-2 "Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 2: Requirements for trust service providers issuing EU qualified certificates" odeljak 4.2.5.

Član 25.

Kvalifikovani elektronski sertifikat za elektronski pečat obavezno sadrži u polju "qcStatements" izjave QcCompliance, QcSSCD i, izjavu QcType sa identifikatorom "id-etsi-qcs-seal", a prema dokumentu ETSI EN 319 412-5.

IV. KVALIFIKOVANI ELEKTRONSKI SERTIFIKATI ZA AUTENTIKACIJU SAJTOVA

Član 26.

Kvalifikovani elektronski sertifikat za autentikaciju sajtova obavezno ima sadržaj u skladu sa članom 59. Zakona.

Izdavalac sertifikata izdaje kvalifikovane elektronske sertifikate za autentikaciju sajtova u skladu dokumentom ETSI EN 319 412-4 "Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 4: Certificate profile for web site certificates".

Član 27.

Sadržaj kvalifikovanog elektronskog sertifikata za autentikaciju sajtova koje izdavalac sertifikata izdaje pravnom licu, fizičkom licu ili fizičkom licu kao registrovanom subjektu mora da bude u skladu sa dokumentom CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

Sadržaj kvalifikovanog elektronskog sertifikata za autentikaciju sajtova sa proširenom validacijom koje izdavalac sertifikata izdaje pravnom licu ili fizičkom licu kao registrovanom subjektu mora da bude u skladu sa dokumentom CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates".

Član 28.

Kvalifikovani elektronski sertifikat za autentikaciju sajtova u polju "Certificate Policies" obavezno sadrži najmanje identifikator politike QCP-w u skladu sa dokumentom ETSI EN 319 411-2 "Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 2: Requirements for trust service providers issuing EU qualified certificates" odeljak 4.2.5.

Član 29.

Kvalifikovani elektronski sertifikat za autentikaciju sajtova obavezno sadrži u polju "qcStatements" izjave QcCompliance i QcType sa identifikatorom "id-etsi-qcs-web", a prema dokumentu ETSI EN 319 412-5.

V. PRELAZNE I ZAVRŠNE ODREDBE

Član 30.

Sertifikaciona tela iz člana 73. stav 3. Zakona mogu da izdaju kvalifikovane elektronske sertifikate za elektronski potpis u skladu sa Pravilnikom o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata („Službeni glasnik RS”, broj 26/08) do dana donošenja akta Ministarstva o ispunjenosti obaveze iz člana 73. stav 5. Zakona.

Član 31.

Danom stupanja na snagu ovog pravilnika prestaje da važi Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata ("Službeni glasnik RS", broj 26/08).

Član 32.

Ovaj pravilnik stupa na snagu osmog dana od dana objavljivanja u "Službenom glasniku Republike Srbije".