PATVIRTINTA

Valstybės įmonės
Registrų centro direktoriaus
2012 m. gegužės 31 d. įsakymu
Nr. v-159

ELEKTRONINIO PARAŠO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Šios elektroninio parašo taisyklės (toliau- Taisyklės) nustato Valstybės įmonės Registrų centro (toliau- Registrų centro) elektroninio parašo sudarymo ir tikrinimo tvarką, asmenų, dalyvaujančių pasirašymo procese, teises ir pareigas, nurodo techninius standartus ir veiksmus, kurie turi būti atliekami kuriant ir tikrinant elektroninių dokumentų kvalifikuotą elektroninį parašą.

2. Sertifikatų naudotojai elektroninius dokumentus pasirašo per centralizuoto elektroninių dokumentų pasirašymo sistemą (toliau – CEDPS) ir teikia juos Registrų centro informacinėms sistemoms.

3. Taisyklėmis turi vadovautis:

3.1. sertifikatų savininkai, turintys kvalifikuotą sertifikatą ir pasirašantys elektroninius dokumentus kvalifikuotu elektroniniu parašu;

3.2. sertifikatais pasitikinčios šalys, kurios atlieka elektroninių dokumentų kvalifikuoto elektroninio parašo tikrinimą.

4. Taisyklių aktuali redakcija, taikoma konkrečiam elektroniniam dokumentui, nustatoma pagal to elektroninio dokumento elektroninio parašo laiko žymoje nurodytą datą.

5. Aktuali šių Taisyklių redakcija skelbiama adresu http://www.registrucentras.lt/rcsc/apie/taisykles.php

6. Taisyklės parengtos vadovaujantis Lietuvos Respublikos elektroninio parašo įstatymu (Žin., 2000, Nr. 61-1827), Reikalavimų elektroninio parašo tikrinimo procedūrai aprašu (Žin., 2011, Nr. 48-2351) bei kitais teisės aktais, Europos Sąjungos elektroninio parašo standartizavimo iniciatyvos dokumentais bei minimaliais techninių standartų reikalavimais, apibrėžiančiais pakankamas sąlygas, kurioms esant elektroninis parašas tenkina kvalifikuotam elektroniniam parašui keliamus reikalavimus, apibrėžtus standartuose:

6.1. ETSI TS 102 778, v 1.1.2. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles;

6.1.1. Part 1: PAdES Overview;

6.1.2. Part 2: PAdES Basic - Profile based on ISO 32000-1.

6.2. ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.

6.3. ETSI TS 102 023, v.1.2.1 and v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

6.4 ETSI TS 101 861 V1.3.1 Time stamping profile.

6.5. IETF RFC 3125, Electronic Signature Policies.

6.6. IETF RFC 3161 updated by RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

6.7. IETF RFC 5280, RFC 4325 and RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.

6.8 IETF RFC 5652, RFC 4853 and RFC 3852, Cryptographic Message Syntax (CMS).

6.9. ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

6.10. ETSI TR 102 272 v1.1.1: „Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies“.

6.11. ETSI TR 102 041 v1.1.1: „Signature policy report“.

6.12. ETSI TR 102 045 v1.1.1: „Signature Policy for Extended Business Model“.

6.13. RFC 3125 – Electronics Signature Policies.

6.14. CWA 14168 „Secure Signature-Creation Devices „EAL 4“.

6.15. CWA 14170:2004 „Security Requirements for Signature Creation Applications“.

6.16. CWA 14171:2004: „General guidelines for electronic signature verification“.

6.17. ETSI TS 101 733 v1.5.1: „Electronics Signatures formats“.

6.18. ETSI TS 102 023 v1.2.1 „Policy requirements for time-stamping authorities“.

6.19. ETSI TS 101 861 V1.2.1 „Time stamping profile“.

6.20. ETSI TS 101 456 v1.2.1: „Policy requirements for certification authorities issuing qualified certificates“.

6.21. ETSI TS 102 231: v2.1.1 „Requirements for Trust Service Provider status information“.

7. Priimtinas elektroninio parašo formatas - PAdES (PDF saugūs elektroniniai parašai) formato parašai, sudaryti pagal techninę specifikaciją ETSI TS 102 778-3.

II. ELEKTRONINIO PARAŠO FORMAVIMAS

8. CEDPS, kurioje kuriami elektroniniai parašai, į pasirašomą elektroninį dokumentą įterpia parašo galiojimo patvirtinimą. Jei tokių patikrinimų pasirašymo metu atlikti negalima, atitinkama sistema turi atlikti patvirtinimą prieš priimant failą. Jei kuris nors iš šių patikrinimų yra neteisingas, parašo formavimo procesas bus sustabdytas.

III. ELEKTRONINIO PARAŠO TIKRINIMAS

9. Pagal šias taisykles tikrintojas gali naudoti bet kurį metodą suformuotam parašui patikrinti. Parašui patvirtinti turi būti įvykdyti šie minimalūs reikalavimai:

9.1. duomenys po parašymo nebuvo pakeisti;

9.2. sertifikatas pasirašymo momentu galiojo;

9.3. sertifikatas išduotas Kvalifikuoto sertifikatų centro, kuris registruotas Lietuvos ir Europos sąjungos prižiūrimų ir/ar akredituotų sertifikavimo paslaugų teikėjų paslaugų patikimame sąraše- TSL (*Trusted Services List*);

9.4. iš sertifikate esančių duomenų ir atributų turi būti galima vienareikšmiai identifikuoti pasirašiusįjį asmenį (vardas, pavardė, asmens kodas);

9.5. laiko žymos buvimas, ją išdavusios Laiko žymų tarnybos patikimumas.

10. Taisyklės pasirašančiajam asmeniui:

10.1. Pasirašantysis asmuo privalo užtikrinti, kad PDF formato byloje, kuri turi būti pasirašyta, nebūtų dinamiško turinio. Jei pasirašantis asmuo nesukūrė pasirašomos bylos, jis privalo

įsitikinti, kad bylos medžiagoje nėra dinaminio turinio.

10.2. Parašas turi būti suformuotas PAdES-CMS pagrindu: šios taisyklės apibrėžia CMS/PKCS#7 skaitmenį parašą, kuris sukurtas pagal ISO 32000-1 standartą, reikalaujantį, kad PDF formato bylos skaitmeninio parašo žodyno /ByteRange raktas apimtų visą bylą ir kad /subFilter raktas būtų įtrauktos tik adbe.pkcs7.detached ir adbe.pkcs7.sha1 reikšmės. Be to, šis aprašas rekomenduoja, kad laiko žyma būtų įtraukta kaip CMS/PKCS#7 nepasirašytas atributas.

11. Taisyklės tikrinančiam asmeniui:

11.1. saugaus elektroninio parašo bazinėje formoje nėra informacijos apie patvirtinimą, išskyrus pasirašymo sertifikato atributą. Tikrinantis asmuo gali naudoti šiuos atributus patikrinti, ar įvykdyti parašo taisyklių reikalavimai, pagal kuriuos buvo sukurtas parašas:

11.2. Pasirašymo laiko elementas bus naudojamas tik elektroniniam parašui patikrinti, kaip nuoroda, skirta sertifikatų būklei patikrinti konkrečiai datai. Pasirašymo laikas turi būti patvirtintas laiko žyma.

11.3. Parašo sertifikato elementas bus naudojamas sertifikato statusui patikrinti (ir, jei yra, sertifikato sekai) parašo generavimo momentu, jei sertifikato galiojimo laikas nesibaigė ir paraše yra sertifikato galiojimą patvirtinantys duomenys (*OCSP*- sertifikatų būklės patikrinimas realiuoju laiku, *CRL*- atšauktų sertifikatų sąrašas).

11.4. Jei viename dokumente yra keli elektroniniai parašai, turi būti laikomasi to paties patikrinimo proceso, kuris buvo taikomas pirmajam parašui tikrinti.

12. Elektroniniam parašui formuoti gali būti naudojami bet kuris iš šių šifravimo ir maišos (*hash*) algoritmų:

12.1. RSA/SHA 1 (rekomenduojama pakeisti šį formatą stipresniais algoritmais);

12.2 RSA/SHA 2 (RSA/SHA256

12.3. RSA/SHA512.