UAB „SKAITMENINIO SERTIFIKAVIMO CENTRAS“

EUROPKI SERTIFIKATO TAISYKLĖS

OID: 1.3.6.1.4.1.5255.1.1.1

Versija 1.1

2004 m. sausis

Dokumento istorija

Data	**Redakcinės pastabos**
2000 m. spalio 15 d.	Pradinė Versija.
2004 m. sausio 29 d.	Ištaisytos spaudos klaidos ir perfrazuota keletas sakinių.

Turinys

1 Įvadas

EuroPKI yra ne pelno siekianti organizacija, įkurta europinės Viešųjų Raktų Infrastruktūros (PKI) kūrimui ir plėtotei. Ji prasidėjo nuo ICE-TEL projekto PKI, kurią vėliau plėtojo ICE-CAR 1 projektas. Abu šiuos projektus kaip Telematikos Tyrimams programos dalį finansavo Europos Komisija. Daugiau informacijos apie tai galite rasti http://www.europki.org/ca/root/. Šio dokumento struktūra atitinka RFC 2527 [1], todėl kelios jo dalys paliktos dėl suderinamumo, nors EuroPKI teikiamoms paslaugoms jos tiesiogiai netaikomos.

1 Priede pateiktas šiame dokumente naudojamų terminų glosarijus. Jis daugiausia remiasi RFC 2527 [1].

Šiame dokumente esantys žodžiai „PRIVALO“, „NEPRIVALO“, „BŪTINA“, „TURI“, „NETURI“, „TURĖTŲ“, „NETURĖTŲ“, „REKOMENDUOJAMA“, „GALI“, „PASIRINKTINAI“ turi būti aiškinami taip, kaip aprašyta RFC 2119 [2] (žr. 2 Priedą).

Šiame dokumente posakis „atitinkama CA“ naudojamas nusakyti CA, kurios veikla atitinka šiame dokumente nurodytas sąlygas.

1.1 Bendra apžvalga

Šis dokumentas aprašo taisyklių rinkinį, apibrėžiantį atitinkamos CA išleistų sertifikatų taikymą tarp PKI sistemos dalyvių ir/ar bendrų saugumo reikalavimų lygį.

Sertifikato taisyklėmis sertifikato naudotojas GALI naudotis, norėdamas nustatyti, ar sertifikatas ir jį išleidusi institucija yra pakankamai patikima, kad jį būtų galima taikyti kurioje nors srityje. Atitinkamos CA išleistas X.509 3 versijos sertifikate TURĖTŲ būti nuoroda į šiuos sertifikavimo veiklos nuostatus.

Daugiau informacijos apie atitinkamų CA sertifikavimo praktiką ir jų veiklą rasite Sertifikavimo Veiklos Nuostatuose (CPS).

Kiekviena atitinkama CA PRIVALO išleisti savo CPS, kad potencialiems CA klientams būtų tinkamai pateikta informacija apie pagrindines CA technines, procedūrines ir teisines sąlygas, kurios nėra nurodytos šiame dokumente.

1.2 Identifikavimas

Šios sertifikato taisyklės identifikuojamos pagal šį unikalų įregistruotą Objekto Identifikatorių (OID):

1.3.6.1.4.1.5255.1.1.1

OID sudarytas iš šių dalių:

ISO assigned 1	1
Organization acknowledged by ISO 3	3
US Department of Defense 6	6
Internet 1	1
Private 4	4
IANA registered private enterprises 1	1
EuroPKI 5255	5225
Root CA 1	1
Major version 1	1
Minor version 1	1

1.3 PKI sistemos dalyviai ir taikymo sritys

Atitinkama CA gali laisvai pasirinkti tai, kas gali būti PKI sistemos dalyviais ir apibrėžti savo išleistų sertifikatų taikymo sritį, bet ji PRIVALO tai aiškiai nurodyti savo CPS. Kiekvienu atveju atitinkama CA NEPRIVALO išleisti sertifikatų PKI sistemai nepriklausantiems naudotojams arba programoms, kurios nebuvo kruopščiai įvertintos (pavyzdžiui, programinė įranga, skirta didelės vertės B2B sandoriams). Be to, atitinkama CA TURĖTŲ laikytis visų atitinkamų šio dokumento dalimis nustatytų apribojimų.

1.3.1 Sertifikavimo Tarnybos

Atitinkama sertifikatus išleidžianti CA turi atkreipti tinkamą dėmesį, nuspręsdama, ar tam tikra juridinis asmuo arba asmuo gali atlikti žemesnio lygio CA, atitinkančius visus šiame dokumente nurodytus sertifikatų taisyklių reikalavimus, funkcijas.

Atitinkama CA GALI pasitelkti tiek RA (Registravimo tarnybų), kiek ji nori. Jei atitinkama CA pati gali atlikti asmens identifikaciją, CA taip pat GALI atlikti RA funkcijas. Žemesnio lygio CA PRIVALO pasirašyti susitarimą su CA, pareikšdama įsipareigojanti laikytis sutartų procedūrų.

1.3.2 Registravimo Tarnybos

Registravimo Tarnybos (RA) reikalingos fiziniam naudotojų identifikavimui/autentifikavimui. Šioms tarnyboms NEGALI BŪTI suteikta teisė išleisti sertifikatus.

Registravimo tarnyba (RA) yra

- asmuo ar
- juridinio asmens paskirta žmonių grupė ar organizacinis vienetas, kuriuo pasitiki CA, ir kuris veikia kaip naujų galutinių naudotojų, t.y., galutinių naudotojų, kurie nori gauti sertifikatą, kontaktinis taškas. Registravimo Tarnybos turi tinkamu būdu patikrinti sertifikato prašančiojo asmens/juridinio asmens tapatybę.

RA PRIVALO pasirašyti susitarimą su CA, prisiimdama įsipareigojimą laikytis nustatytų procedūrų.

1.3.3 Galutiniai naudotojai

Pagal šias CP Galutiniais naudotojais, norinčiais gauti sertifikatą, gali būti fizinis asmuo (asmuo ar juridinio asmens atstovas) arba kompiuterinė/programinė įranga (pvz., kompiuteris, mašrutizatorius ar programa), galinti atlikti kriptografines operacijas.

Kiekviena atitinkama CA savo CPS PRIVALO aprašyti, kas gali būti sertifikatus išduoti prašančiais galutiniais naudotojais.

1.3.4 Taikymo sritys

Vienas iš šių sertifikato taisyklių tikslų yra skatinti platų viešųjų raktų sertifikatų naudojimą įvairiose programose. Tam, kad būtų skatinamas suderinamumas, šie CA nuostatai tvirtai palaiko S/MIME naudojimą saugiam elektroniniam paštui. Juose taip pat patariama, kad TURĖTŲ būti palaikomi IPsec (saugumo užtikrinimui tinklo lygiu) ir SSL/TLS (HTTP, Telnet, FTP funkcijas naudojančių programų saugumo užtikrinimui transportiniu lygiu) protokolai. Svarbu pažymėti, kad šiais nuostatais, iš esmės, nenorima nustatyti *a priori* apribojimų sertifikatų naudojimui, išskyrus tuos atvejus, kai sertifikatai naudojami tokiu būdu, kaip tai draudžia daryti šalių, kuriose įsikūrusi sertifikatus išleidžianti CA, įstatymai. Vis tik tam, kad būtų patikrinta, ar pagal šias taisykles išleisti sertifikatai tinkami tam tikroms funkcijoms atlikti, turi būti įdėmiai perskaitytas ir visiškai suprastas 2 Bendrųjų nuostatų skyrius.

1.4 Informacija Kontaktams

1.4.1 CPS administruojantis juridinis asmuo

EuroPKI vardu šias CP tvarko Turino Politechnikos Instituto Kompiuterinio ir Tinklo saugumo grupė (Computer and Network Security Group (CNSG) of Politecnico di Torino, Italy) (http://security.polito.it/).

1.4.2 Asmuo kontaktams

Asmuo kontaktams dėl su šiomis taisyklėmis susijusių klausimų:

adresas	Prof. Antonio Lioy EuroPKI Šakninė CA c/o Politecnico di Torino Dip. Automatica e Informatica corso Duca degli Abruzzi, 24 10129 Torino (Italy)
Tel.	+39 0115647021 / +39 0115647054
Fax:	+39 0115647099
URL	http://www.europki.org/ca/root/
E-paštas	ca@europki.org

1.4.3 Tinkamą CP vykdymą prižiūrintis asmuo

Tam, kad būtų įvertinta, ar atitinkamų Sertifikavimo Tarnybų CPS tinkamai laikomasi šių CP, pastarosios turi kreiptis į 1.4.2 skyriuje nurodytą asmenį. Su CPS patikros procedūrų detalėmis galite susipažinti 8.3 skyriuje.

2 Bendrosios nuostatos

Šiame skyriuje numatyti šalių įsipareigojimai ir nuostatos dėl atsakomybės bei finansinių/ekonominių klausimų, be to, yra konfidencialumui skirtas skyrelis, nusakantis informacijos skirstymą į konfidencialią ir viešai prieinamą bei platinamą informaciją. Šiame skyriuje taip pat reglamentuojami CA veiklos patikros principai.

2.1 Įsipareigojimai

2.1.1 CA įsipareigojimai

Atitinkama CA TURI teikti sertifikavimo tarnybos paslaugas.
Pagrindiniai CA įsipareigojimai yra:

● tvarkyti prašymus išduoti sertifikatus ir atlikti naujų sertifikatų išdavimo funkcijas:
o priimti ir patvirtinti prašymus išduoti sertifikatą iš asmenų, sertifikato prašančių pagal šiose taisyklėse ir CPS nustatytas procedūras
o nustatyti sertifikato prašančių asmenų tapatybę, galimai su atskirai paskirtų RA pagalba
o nustačius tapatybę, šiems asmenims išduoti sertifikatus
o pranešti pareiškėjams apie sertifikato išdavimą
o išleistus sertifikatus padaryti viešai prieinamais
● tvarkyti sertifikatų galiojimo nutraukimo prašymus ir atšaukti sertifikatus
o priimti ir patvirtinti prašymus asmenų, pagal šiame CP/CPS apibrėžtas procedūras prašančių atšaukti sertifikatą
o nustatyti sertifikatą atšaukti prašančių asmenų tapatybę
o padaryti viešai prieinamais CRL sąrašus

2.1.2 RA įsipareigojimai

RA TURI teikti RA paslaugas. Tai apima:

● subjekto tapatybės nustatymą
● ryšio tarp viešojo rakto ir prašymo pateikėjo, naudojant tinkamą to įrodymo būdą, patvirtinimą
● tokio ryšio patvirtinimą sertifikavimo tarnybai
● įsipareigojimą tvirtai laikytis su CA pasirašytos sutarties

2.1.3 Pasirašančiųjų asmenų įsipareigojimai

Galutinis naudotojas TURI elgtis sutinkamai su sertifikatus išleidžiančios CA CPS. Tai apima:
● [CPS] perskaitymą ir tvirtą sutikimą laikytis išdėstytų procedūrų
● tinkamą savo privačiojo rakto saugojimą, būnant vieninteliu jo turėtoju, jei sertifikatas buvo išduotas asmeniui. Kompiuterinės įrangos ar programinės įrangos komponento privačiojo rakto apsauga ir kontrolė GALI tekti daugiau, kaip vieno įgalioto asmens atsakomybei.
● sutikti, kad naudojant viešųjų raktų sertifikatus, su tuo susijusi CA atsakomybė būtų ribojama, kaip apibrėžta 2.2 skyriuje
● leidimą apdoroti ir saugoti asmeninius duomenis
● įsipareigojimą nedelsiant pranešti CA apie privačiojo rakto sukompromitavimą

2.1.4 Sertifikatais pasitikinčių šalių įsipareigojimai

Sertifikatais pasitikinčios šalys su šiomis taisyklėmis ir CPS PRIVALO susipažinti dar prieš darydamos bet kokias išvadas dėl pasitikėjimo atitinkamos CA išleistu sertifikatu. Sertifikatais pasitikinčios šalys

sertifikatų galiojimo patikrai PRIVALO naudotis CRL sąrašais. Be to, sertifikatais pasitikinčios šalys sertifikatą PRIVALO naudoti TIKTAI leistinais būdais ir sertifikatų PRIVALO NENAUDOTI įstatymų draudžiamiems veiksmams.

2.1.5 Informacinės tarnybos įsipareigojimai

Kiekviena atitinkama CA TURĖTŲ išlaikyti viešam naudojimui skirtą dokumentų talpyklą, kurioje laikomi sertifikatai ir Atšauktų Sertifikatų Sąrašai (CRL).

Talpykla TURĖTŲ būti prieinama, kiek tai įmanoma iš praktinės pusės tiek, kiek leidžia pagrindinės techniniu CA valdymu užsiimančios juridinio asmens galimybės.

2.2 Atsakomybė

2.2.1 CA atsakomybė

Atitinkama CA GALI prisiimti tam tikrą atsakomybę. Turint omeny, kad šios nuostatos iš esmės skirtos sertifikatų, kaip priemonės kompiuterių ir tinklų saugumui padidinti, vartojimo skatinimui daugelyje taikymo sričių, 1.3.4 skyrius nustato, kad šiose taisyklėse nėra jokių a priori apribojimų pagal šias nuostatas išleistų sertifikatų pritaikymui. Jei sertifikatų taikymui nėra apribojimų, šios taisyklės CA atsakomybę siūlo apriboti iki įsipareigojimo imtis reikiamos kontrolės, užtikrinančios tinkamą kiekvieno sertifikato prašančio asmens tapatybės nustatymą, kaip tai aprašyta CPS ir imtis minimalių saugumo priemonių, būtinų CA privačiojo rakto apsaugai. Kiekvienu atveju CPS PRIVALO būti nurodytas pilnas, tiksliai išvardintas prisiimamų įsipareigojimų sąrašas.

2.2.2 RA atsakomybė

Atitinkanti 2.2.1 skyriaus nuostatas.

2.3 Finansinė atsakomybė

Atsižvelgiant į tai, kas išdėstyta 1.3.4, 2.2.1 skyriuose ir 2.5 paragrafe, už pagal šias taisykles išleistus sertifikatus jokios atsakomybės neprisiimama.

2.3.1 Kompensacija Sertifikatais pasitikinčioms šalims

Sąlygų nėra

2.3.2 Pasitikėjimu grindžiami santykiai

Sąlygų nėra

2.3.3 Administraciniai procesai

Sąlygų nėra

2.4 Aiškinimas ir Teisės taikymas

2.4.1 Teisės taikymas

Šios taisyklės aiškinamos pagal valstybės, kurioje yra įsikūrusi atitinkama CA, įstatymus. Tai PRIVALO būti nuodugniai aprašyta CPS.

2.4.2 Atskiriamumas, išlikimas, apjungimas, pranešimas

Sąlygų nėra

2.4.3 Ginčų sprendimo tvarka

Sąlygų nėra

2.5 Mokesčiai

2.5.1 Mokesčiai už sertifikato išdavimą ar pratęsimą

Šiose taisyklėse rekomenduojama, kad už sertifikato išdavimą nebūtų imami mokesčiai. Bet kokiu atveju, CA už tai GALI imti mokesčius, bet tai PRIVALO būti aiškiai išdėstyta CPS.

2.5.2 Mokesčiai už priėjimą prie sertifikato

Šiose taisyklėse rekomenduojama, kad už sertifikato prieinamumą talpykloje ar kitokį priėjimą prie jų nebūtų imami mokesčiai. Bet kokiu atveju, CA už tai gali imti mokesčius, bet tai PRIVALO būti aiškiai išdėstyta CPS.

2.5.3 Mokesčiai už sertifikato atšaukimą ar informaciją apie sertifikato statusą

Šiose taisyklėse rekomenduojama, kad už leidimą atšaukti sertifikatą ar priėjimą prie informacijos apie sertifikato statusą mokesčiai nebūtų imami.

2.5.4 Mokesčiai už kitas paslaugas, tokias, kaip informacija apie šias CP

Šiose taisyklėse rekomenduojama, kad už priėjimą prie informacijos apie šias taisykles (CP) ir CPS informacijos mokesčiai nebūtų imami.

2.5.5 Nuostolių padengimo tvarka

Sąlygų nėra

2.6 Informacijos skelbimas ir Talpykla

2.6.1 CA informacijos skelbimas

Atitinkama CA TURI užtikrinti priėjimą prie:

- sertifikato taisyklių ir CPS, ir pagal jas veikti
- visų išleistų sertifikatų, išskyrus sertifikatus, kurių turėtojai aiškiai nurodė, kad jų sertifikatas NETURI būti viešai prieinamas
- pasirašytų atšauktų sertifikatų sąrašų

2.6.2 Informacijos skelbimo dažnumas

Sertifikatai TURI būti skelbiami iškart po to, kai bus išleisti. CRL skelbimo dažnumas nurodytas 4.4.9 skyriuje. Taip pat sertifikato taisyklės ir CPS TURI būti skelbiami iškart po jų atnaujinimo.

2.6.3 Prieigos kontrolė

Priėjimui prie sertifikato taisyklių, CPS ir CRL NETURI būti taikoma priėjimo kontrolė. Ji GALI būti taikoma priėjimui prie sertifikatų (pavyzdžiui, kad būtų išvengta duomenų, tokių, kaip e-pašto adresų perėmimo arba kai CA nusprendžia imti mokesčius už sertifikavimo paslaugas).

2.6.4 Talpyklos

TURI būti bent viena talpykla aukščiau išdėstytos informacijos skelbimui.

2.7 Veiklos atitikimo auditas

Atitinkamos CA veiklos atitikimui išorinis auditas NEPRIVALOMAS. CA veiklos atitikimą Sertifikavimo veiklos nuostatoms ir Sertifikato taisyklėms atlieka atitinkamą CA valdanti juridinis asmuo, bet leidžiama bet kokia išorinė veiklos atitikimo kontrolė. Kiekviena atitinkama CA savo CPS GALI pateikti detalesnes nuostatas dėl veiklos atitikimo audito.

2.7.1 Subjekto veiklos atitikimo audito dažnumas

Sąlygų nėra

2.7.2 Auditoriaus identifikacija/kvalifikaciniai reikalavimai

Sąlygų nėra

2.7.3 Auditoriaus santykiai su audituojamu subjektu

Sąlygų nėra

2.7.4 Audituojamos veiklos sritys

Sąlygų nėra

2.7.5 Veiksmai, kurių imamasi, aptikus trūkumų

Sąlygų nėra

2.7.6 Pranešimas apie audito rezultatus

Sąlygų nėra

2.8 Konfidencialumas

CA renka asmenų, prašančių išduoti sertifikatą, asmens duomenis (pvz., pilnas vardas, juridinis asmuo, ir e-pašto adresas). Šie duomenys PRIVALO būti apdorojami tokiais būdais, kurie užtikrina privatumo apsaugą pagal valstybės, kurioje įsikūrusi atitinkama CA, įstatymus.

2.8.1 Konfidencialia laikomos informacijos rūšys

Konfidencialia laikoma informacija apie visus galutinius naudotojus ir informacija, kurios nėra atitinkamos CA išleistuose sertifikatuose ar CRL, ir trečiosioms šalims ji NETURI būti atskleista be aiškaus galutinio naudotojo sutikimo.

2.8.2 Viešai teikiamos informacijos rūšys

Konfidencialia nelaikoma atitinkamos CA išleistuose viešai prieinamuose sertifikatuose ir CRL sąrašuose esanti informacija.

2.8.3 Informacijos apie sertifikato galiojimo nutraukimą/sustabdymą atskleidimas

Jei sertifikatas nutraukiamas/sustabdomas jo galiojimas, to priežastis GALI būti nurodoma Atšauktų sertifikatų sąraše. Duomenys apie sertifikato galiojimo nutraukimo/galiojimo sustabdymo priežastį nelaikomi konfidencialiais ir gali būti paskleisti visiems kitiems naudotojams ir sertifikatais pasitikinčioms šalims. Bet kokiu atveju, esant įprastinėms sąlygoms, jokia kita su sertifikato atšaukimu susijusi informacija neatskleidžiama.

2.8.4 Informacijos atskleidimas teisėsaugos institucijoms

Atitinkama CA neatskleidžia su sertifikatu susijusios informacijos ar galutinio naudotojo asmens duomenų jokiai trečiajai šaliai, išskyrus atvejus, kai to reikalauja teisėsaugos institucijų atstovai, tam pateikę teisės aktų reikalaujamus leidimus.

2.8.5 Informacijos atskleidimas kaip civilinio proceso dalis

Sąlygų nėra.

2.8.6 Informacijos atskleidimas, gavus sertifikato turėtojo prašymą

Atitinkama CA neatskleidžia sertifikato ar su sertifikatu susijusios informacijos jokiai trečiajai šaliai, išskyrus atvejus, kai to pasirašytu prašymu reikalauja sertifikato turėtojas.

2.8.7 Kitos informacijos atskleidimui būtinos aplinkybės

Sąlygų nėra.

2.9 Intelektinės Nuosavybės Teisės

Atitinkama CA PRIVALO nereikšti jokių pretenzijų dėl išleistų sertifikatų intelektinės nuosavybės teisių. Be to, bet kam leidžiama atlikti EuroPKI CPS ar Sertifikato taisyklių kopijas, tik būtina pateikti teisingą nuorodą į šaltinį.

3 Identifikacija ir autentifikacija

Šis skyrius aprašo procedūras, taikomas sertifikato prašančio asmens identifikacijai ir autentifikacijai CA ar RA prieš tai, kai bus išduoti sertifikatai. Jis taip pat nurodo, kaip identifikuojami asmenys, prašantys pakeisti raktą ar jį atšaukti. Šis skyrius taip pat nustato su vardų naudojimu susijusias taisykles ir pretenzijų dėl teisių į vardą (pavadinimą), prekių ženklą sprendimo tvarką.

3.1 Pradinė Registracija

3.1.1 Vardų [pseudonimų] tipai

Sertifikato prašančio asmens vardo atributai, reikalingi identifikuoti ir autentifikuoti sertifikato prašantį asmenį, priklauso nuo jo prašomo sertifikato tipo.
Pasirenkant sertifikato laukeliuose naudojamų vardų tipus ir formatą, EuroPKI CP atitinka RFC 2459 [3].
Atitinkama CA savo CPS PRIVALO nurodyti naudojamų vardų tipus ir formatą.

3.1.2 Reikalavimas, kad vardai [pseudonimai] būtų reikšminiai

Sertifikate esantys Subject ir Issuer vardiniai laukai PRIVALO būti reikšminiais, kad sertifikatus išduodanti CA turėtų tinkamą ryšio tarp šių vardų ir asmenų, kuriems priklauso sertifikatai, buvimo įrodymą.

Jei sertifikate nurodomas e-pašto adresas, jis nebūtinai turi būti sudarytas pagal semantines taisykles, kurios gali būti naudojamos asmeniui ir/ar juridiniam asmeniui identifikuoti.

3.1.3 Taisyklės įvairių vardų [pseudonimų] formų aiškinimui

Atitinkama CA CPS PRIVALO išdėstyti taisykles, numatančias, kaip turi būti aiškinamos įvairios sertifikatuose naudojamos vardų formos.

3.1.4 Vardų unikalumo svarba

Kiekvieno subjekto, kurį sertifikavo CA, skiriamųjų požymių turintis pavadinimas (kaip tai nurodyta sertifikato sudarytojo pavadinimo laukelyje) turi būti unikalus.

3.1.5 Pretenzijų dėl teisių į prekinį vardą [ženklą] sprendimo tvarka

Pretenzijos sprendžiamos pagal valstybės, kurioje yra įsikūrusi CA, įstatymus.

3.1.6 Prekių ženklų pripažinimas, tapatybės nustatymas ir vaidmuo

Sąlygų nėra.

3.1.7 Privataus rakto turėjimo įrodymo būdas

Labai REKOMENDUOJAMAS privačiojo rakto, atitinkančio viešąjį raktą, turėjimo tinkamo įrodymo metodo sertifikavimas. Pasirinktas metodas PRIVALO būti išsamiai išdėstytas CPS. Jei rakto turėjimo įrodymo metodas pasirinktas, atitinkama CA NEPRIVALO išduoti sertifikatų, kol nepateikiamas pakankamas privačiojo rakto turėjimo įrodymas. Šios sertifikato taisyklės CA atlikto privataus rakto generavimo tokiu įrodymu nelaiko.

3.1.8 Juridinio asmens tapatybės nustatymas

Kiekvieną kartą, kai sertifikato prašantis asmuo į sertifikatą reikalauja įtraukti tam tikros juridinio asmens pavadinimą, sertifikatus išduodanti CA PRIVALO turėti įrodymą, kad tokia juridinis asmuo žino viską apie šį faktą. Tam, kad tuo įsitikintų, sertifikatus išduodanti CA PRIVALO pareikalauti keleto dokumentų. Visais atvejais sertifikuojamus duomenis įrodantys tinkami juridiniai dokumentai PRIVALO būti pateikti per specialų kanalą. Tapatybės nustatymą GALI atlikti CA ar RA. Tapatybės nustatymo detalės PRIVALO būti nurodytos CPS.

3.1.9 Individualaus asmens tapatybės nustatymas

Daugeliu atvejų viešųjų raktų sertifikatai esti priemone, galinčia garantuoti patikimą kriptografinę autentifikaciją tarpusavyje bendraujantiems galutiniams naudotojams. Turint omeny šią prielaidą, EuroPKI sertifikato taisyklės nustato, kad kiekvieno konkretaus asmens autentifikavimas yra BŪTINAS dalykas. REKOMENDUOJAMAS autentifikacijos metodas reikalauja, kad konkretus asmuo CA ar RA asmeniškai pateiktų tinkamus asmens tapatybę įrodančius dokumentus (pvz., pasą, vairuotojo pažymėjimą, pareigūno pažymėjimą ir pan.). GALI būti priimtini ir kiti metodai - tokie, kaip videokonferencijos. Jei sertifikuojamas subjektas yra programinės įrangos komponentas, paraišką pateikęs asmuo PRIVALO įrodyti, kad jis yra tinkamai autorizuotas (Pavyzdžiu jūs galite laikyti užklausą www.europki.org tinklo serveriui: ją gali atlikti tik žmonės, kuriems prieigos prie to teisę tiesiogiai suteikė europki.org domeną užregistravę žmonės). Tiksli procedūra PRIVALO būti išsamiai išdėstyta CPS.

3.2 Bendroji sertifikato pratęsimo tvarka

Šios sertifikato taisyklės nesuteikia įgaliojimų jokiam privalomam naujų sertifikatų išdavimui. Kai baigiasi sertifikato galiojimas, CA GALI išduoti naują sertifikatą tam pačiam ar naujam raktui. Naujo sertifikato išdavimas GALI būti atliekamas pagal tą pačią 3.1 skyriuje aprašytą procedūrą, aprašančią pradinę registraciją arba naudojant skaitmeniniais parašais pasirašytus prašymus. Šie prašymai CA PRIVALO būti atsiųsti prieš pasibaigiant sertifikato galiojimui.
CA GALI išduoti daugiau, kaip vieną sertifikatą tam pačiam raktui.

3.3 Naujo sertifikato išdavimo, jį atšaukus, tvarka

Viešasis raktas, kurio sertifikatas buvo atšauktas dėl privačiojo rakto sukompromitavimo, NEPRIVALO būti iš naujo sertifikuojamas. Viešasis raktas GALI būti iš naujo sertifikuojamas, jei sertifikatas atšauktas tik dėl įgaliojimo sustabdymo. Kitais atvejais, išduodant naują sertifikatą, autentifikavimas GALI būti atliekamas pagal tą pačią 3.1 skyriuje aprašytą procedūrą, aprašančią pradinę registraciją arba naudojant skaitmeniniais parašais pasirašytus prašymus. Šie prašymai CA PRIVALO būti atsiųsti prieš pasibaigiant sertifikato galiojimui.

3.4 Prašymas atšaukti sertifikato galiojimą

Tam, kad būtų priimtas prašymas atšaukti sertifikatą, būtina naudoti tinkamą autentifikavimo metodą. Atitinkama CA kaip prašymą atšaukti sertifikatą PRIVALO priimti skaitmeniniu parašu pasirašytą pranešimą, jei nesibaigęs parašo galiojimas ir pranešimas pasirašytas pagal šias taisykles išleistu ir anksčiau neatšauktu sertifikatu. Taip pat laikomos tinkamomis pirminio registravimo metu autentifikavimui naudojamos procedūros. GALI būti palaikomos alternatyvios procedūros, tokios kaip PIN (Personal Identification Number) atšaukimas, naudojant saugų ryšį.

Palaikomos procedūros PRIVALO būti išsamiai išdėstytos CPS.

4 Reikalavimai veiklai

Šis skyrius naudojamas nustatyti reikalavimams, keliamiems asmenims, atliekantiems sertifikavimo ir sertifikatų galiojimo nutraukimo procesus.

4.1 Prašymas Sertifikatui sudaryti

Šios sertifikato taisyklės leidžia dvi alternatyvias sertifikato taikymo procedūras:
● išimtinai CA atliekamą asmenų sertifikavimą. Šią procedūrą aprašančios detalės PRIVALO būti nurodytos CPS
● asmuo generuoja savo nuosavą raktų porą ir viešąjį raktą bei kitus reikiamus duomenis pateikia CA. Po to prašymas PRIVALO būti apdorojamas pagal šiose taisyklėse (CP)ir CPS nurodytas procedūras, aprašančias identifikavimą ir autentifikavimą.

4.2 Sertifikato Išdavimas

Atitinkama CA ir RA PRIVALO atidžiai patikrinti prašymą pateikusių asmenų pateiktų dokumentų galiojimą ir atitikimą jų tapatybei. Po to, kai pagal 3.1 skyriuje aprašytus būdus autentifikavimas atliktas, CA TURĖTŲ išduoti sertifikatą. Išdavimo atveju CA PRIVALO apie tai pranešti sertifikato prašančiam asmeniui. Jei dėl kokių nors priežasčių CA nusprendžia neišduoti sertifikato (net jei patikra ir autentifikavimas atlikti sėkmingai) ji savo sprendimo priežastį TURĖTŲ pranešti sertifikato prašiusiam asmeniui.

4.3 Sertifikato Priėmimas

Sąlygų nėra.

4.4 Sertifikato Atšaukimas ir Galiojimo sustabdymas

Atitinkama CA yra atsakinga už CRL sąrašų leidimą ir pasirašytų versijų skelbimą. Net jei [3] iš CA nereikalaujama išleisti CRL sąrašų, atitinkama CA PRIVALO reguliariai išleisti CRL sąrašus.

CA TURĖTŲ atnaujinti savo CRL, į jį įtraukdama atšauktus asmens sertifikatus.

4.4.1 Galutinio Naudotojo sertifikato galiojimo nutraukimo aplinkybės

Sertifikato galiojimas TURĖTŲ būti nutrauktas, kai atsiranda įtarimų dėl sertifikate esančios informacijos arba jis buvo sukompromituotas. Tai apima atvejus, kai:
● pasikeičia sertifikato turėtojo duomenys
● sukompromituojamas sertifikato turėtojo privatusis raktas arba yra įtariama, kad jis buvo sukompromituotas
● yra įtarimų, kad sertifikate esanti jo turėtojo informacija yra netiksli
● išaiškėja, kad sertifikato turėtojas nesilaikė savo įsipareigojimų

4.4.2 Asmenys, galintys prašyti atšaukti sertifikatą

Atitinkama CA PRIVALO priimti prašymą atšaukti sertifikatą, kurį atsiuntė norimo atšaukti sertifikato turėtojas. Be to, prašymas atšaukti sertifikatą GALI būti atsiųstas iš sertifikatą išdavusios CA ar su ja susijusios RA.

Kiti asmenys GALI pareikalauti atšaukti sertifikatą, pateikdami akivaizdų įrodymą, kad buvo sukompromituotas privatusis raktas arba pasikeitė sertifikato turėtojo duomenys.

4.4.3 Prašymo atšaukti sertifikatą procedūra

TURĖTŲ būti tinkamai nustatyta sertifikatą atšaukti prašančio asmens tapatybė. Autentifikavimo metodas TURĖTŲ būti toks pat patikimas, kaip tas, kuris naudojamas sertifikatų išdavimo procedūroje. Atitinkama CA PRIVALO kaip prašymą atšaukti sertifikatą priimti skaitmeniniu parašu pasirašytą pranešimą, jei nesibaigė jo parašo galiojimas ir pranešimas pasirašytas pagal šias taisykles išduotu ir anksčiau neatšauktu sertifikatu. Alternatyvi procedūra iš asmens GALI reikalauti apsilankyti RA ar CA ir pateikti galiojantį asmens tapatybę patvirtinantį dokumentą.
Jei šis asmuo yra CA, CA papildomai TURĖTŲ:
- Informuoti sertifikatų turėtojus ir kryžminio sertifikavimo CA tarnybas.
- Nutraukti sertifikato galiojimą ir CRL skelbimo paslaugos teikimą sertifikatams/CRL sąrašams, išleistiems naudojant sukompromituotą privatųjį raktą.

4.4.4 Prašymo atšaukti sertifikatą įvykdymui reikalingas laikotarpis

Atitinkama CA pati nusprendžia, kiek laiko jai reikia priimti prašymui.

4.4.5 Galutinio Naudotojo sertifikato įgaliojimo sustabdymo aplinkybės

CA GALI laikinai sustabdyti galiojimą sertifikato turėtojo , kuris reikalauja tokios paslaugos.
Skirtingai nuo galiojimo nutraukimo, galiojimo sustabdymas naudotojui po kurio laiko leidžia vėl įgalinti sertifikatą. Kiekvienu atveju iš atitinkamos CA teikti sertifikato įgaliojimo sustabdymo paslaugą nereikalaujama.
Informacija apie sustabdyto galiojimo viešuosius raktus GALI būti prieinama CA talpykloje.

4.4.6 Asmenys, galintys prašyti įšaldyti sertifikatą

Tuo atveju, jei CA teikia sertifikato įgaliojimo sustabdymo paslaugą, CA PRIVALO priimti sertifikato turėtojo prašymą sustabdyti sertifikato galiojimą.

4.4.7 Prašymo įšaldyti sertifikatą procedūra

TURĖTŲ būti tinkamai nustatyta sertifikato galiojimo sustabdymo prašančio asmens tapatybė.
Atitinkama CA PRIVALO kaip prašymą įšaldyti sertifikatą priimti skaitmeniniu parašu pasirašytą pranešimą, jei jis pasirašytas galiojančiu ir pagal šias taisykles išleistu bei anksčiau neatšauktu sertifikatu. Alternatyvi procedūra iš asmens GALI reikalauti apsilankyti RA ar CA ir pateikti galiojantį asmens tapatybę patvirtinantį dokumentą.

4.4.8 Sertifikato įgaliojimo sustabdymo trukmė

Sąlygų nėra.

4.4.9 CRL atnaujinimo dažnumas [jei taikoma]

CRL sąrašus atitinkama CA TURĖTŲ išleisti kas 40 dienų.

4.4.10 Reikalavimas sutikrinti sertifikatą su CRL

Tam, kad būtų patikrintas sertifikato naudojimo galimumas, sertifikatais pasitikinčios šalys PRIVALO sutikrinti sertifikatą su atitinkamos CA išleistu naujausiu CRL sąrašu.

4.4.11 Galimybė atšaukti sertifikatą/patikrinti jo statusą on-line režimu

Atitinkama CA GALI palaikyti sertifikato galiojimo nutraukimo/sertifikato statuso patikrinimo paslaugą on-line režimu. Turint omeny, kad Šios sertifikato taisyklės iš atitinkamos CA reikalauja skelbti CRL, realizuoti on-line galiojimo nutraukimo/statuso patikros procedūras iš jos nereikalaujama. Bet kokiu atveju, šios taisyklės taikant tokį mechanizmą, siūlo atsižvelgti į OCSP [4].

4.4.12 Reikalavimai sertifikato galiojimo nutraukimo patikrai angl. on-line režimu

Sąlygų nėra.

4.4.13 Kiti paskelbimui apie sertifikato atšaukimą naudojami būdai

Sąlygų nėra.

4.4.14 Reikalavimai sertifikato galiojimo nutraukimo patikrai, kai naudojami kiti paskelbimo apie sertifikato atšaukimą būdai

Sąlygų nėra.

4.5 Saugumo Audito Procedūros

Šios sertifikato taisyklės pripažįsta saugumo audito procedūrų svarbą, rekomenduojant, kad atitinkama CA visų rūšių sąlygas dėl patikimumo nustatytų CPS.

4.5.1 Fiksuojamų įvykių tipai

Sąlygų nėra

4.5.2 Užfiksuotos informacijos apdorojimo dažnumas

Sąlygų nėra

4.5.3 Audito įrašų saugojimo laikotarpis

Sąlygų nėra

4.5.4 Audito įrašų apsauga

Sąlygų nėra

4.5.5 Atsarginių audito įrašų kopijų darymo tvarka

Sąlygų nėra

4.5.6 Audito duomenų rinkimo sistema [vidinė prieš išorinę]

Sąlygų nėra

4.5.7 Pranešimas įvykį sukėlusiam subjektui

Sąlygų nėra

4.5.8 Pažeidžiamumo įvertinimas

Sąlygų nėra

4.6 Įrašų Archyvavimas

Šis skyrius aprašo archyviniais tikslais CA ir RA fiksuojamų įvykių tipus ir tai, kaip apdorojami surinkti duomenys. Smulkesnėms, čia neskelbiamoms detalėms pateikta išnaša į atitinkamą CPS skyrių.

4.6.1 Fiksuojamų įvykių tipai

Atitinkama CA TURĖTŲ archyvuoti:
- prašymus išduoti sertifikatus, atitinkančius iš tikrųjų išduotus sertifikatus
- išduotus sertifikatus
- paskelbtus CRL sąrašus
- visas su kitomis suinteresuotomis pusėmis (pvz., RA) pasirašytas sutartis
- iš sertifikato turėtojo registracijos metu surinktus dokumentus
- visus svarbius pranešimus, kuriais keistasi su RA

RA tarnybos TURĖTŲ archyvuoti:
- visą patvirtinančią iš sertifikato turėtojo surinktą informaciją
- visus svarbius pranešimus, kuriais keistasi su CA

4.6.2 Archyvo saugojimo laikotarpis

Minimalus saugojimo laikotarpis - 2 metai.

4.6.3 Archyvo apsauga

Sąlygų nėra

4.6.4 Atsarginių archyvo kopijų darymo tvarka

Sąlygų nėra

4.6.5 Reikalavimai laiko įrašų žymoms

Sąlygų nėra

4.6.6 Archyvinės informacijos rinkimo sistema [vidinė arba išorinė]

Sąlygų nėra

4.6.7 Archyvinės informacijos įgijimo ir sutikrinimo tvarka

Sąlygų nėra

4.7 Rakto pakeitimas

Sąlygų nėra.

4.8 Privataus CA rakto kompromitacija ir Avarinis duomenų atkūrimas

Jei CA privatus raktas sukompromituojamas arba įtariama, kad jis buvo sukompromituotas, CA mažiausiai TURĖTŲ:

● informuoti sertifikatų turėtojus, kryžminio sertifikavimo CA tarnybas ir sertifikatais pasitikinčias šalis
● nutraukti sukompromituotą privatų raktą naudojant išleistų sertifikatų galiojimą ir CRL sąrašų skelbimo paslaugą
● pareikalauti atšaukti CA sertifikatą

Jei sukompromituojamas RA privatus raktas arba yra įtarimų dėl jo sukompromitavimo, RA mažiausiai TURĖTŲ informuoti CA ir pareikalauti atšaukti RA sertifikatą. Jei sukompromituojamas asmens privatus raktas arba yra įtarimų dėl jo sukompromitavimo, asmuo mažiausiai TURĖTŲ informuoti sertifikatais pasitikinčias šalis ir pareikalauti atšaukti savo sertifikatą.

4.8.1 Atvejai, kai pažeidžiama kompiuterinė įranga, programinė įranga ir/arba duomenys

Sąlygų nėra

4.8.2 Atvejai, kai pažeidžiamas asmens viešasis raktas

Sąlygų nėra

4.8.3 Atvejai, kai sukompromituojamas asmens raktas

Sąlygų nėra

4.8.4 Izoliuoto režimo įstaiga stichinių ar kitų nelaimių atveju

Sąlygų nėra

4.9 CA Veiklos nutraukimas

CA veiklos nutraukimu laikoma tokia situacija, kai ilgam nutraukiamos visos su numanoma CA susijusios paslaugos.

Prieš tai, kai CA nutraukia savo teikiamas paslaugas, PRIVALO būti imtasi bent šių minimalių procedūrų:

● informuoti visus galutinius naudotojus, kryžminio sertifikavimo CA tarnybas, aukštesniojo lygio CA tarnybas, ir sertifikatais pasitikinčias šalis, su kuriomis CA yra pasirašiusi sutartis ar palaiko kitokius santykius
● padaryti viešai prieinama informaciją apie savo veiklos nutraukimą
● nutraukti sertifikatų platinimą ir CRL sąrašų skelbimą.
Nuo savo veiklą nutraukiančios CA priklausančios CA tarnybos GALI nutraukti savo veiklą arba ją tęsti, kaip atskiros CA.

5 Fizinė, procedūrinė, ir personalo apsaugos kontrolė

5.1 Fizinė Aplinkos Kontrolė

Atitinkamai CA keliami saugumo reikalavimai nustatomi CPS. Kiekvienu atveju šios taisyklės nurodo, kad CA savo veiklai PRIVALO naudoti išskirtinai sertifikavimo tikslams skirtą ir prie viešųjų ryšių tinklų neprijungtą darbinę (tarnybinę) stotį (*dedicated workstation*). Darbinė stotis PRIVALO būti apsaugota nuo fizinio poveikio.

5.1.1 Patalpoms tinkamos vietos parinkimas ir jų statyba

Sąlygų nėra

5.1.2 Fizinė prieiga

Fizinė prieiga prie patalpų, kuriose vykdoma CA veikla, turi būti uždrausta visiems, išskyrus tik aiškiai tam įgalioti asmenys.

5.1.3 Elektros energijos tiekimas ir oro kondicionavimas

Sąlygų nėra

5.1.4 Apsauga nuo vandens poveikio

Sąlygų nėra

5.1.5 Ugnies prevencija ir priešgaisrinės saugos priemonės

Sąlygų nėra

5.1.6 Laikmenų saugojimas

Sąlygų nėra

5.1.7 Atliekų naikinimas

Sąlygų nėra

5.1.8 Atsarginių duomenų kopijų laikymas už juridinio asmens ribų

Sąlygų nėra

5.2 Procedūrinė kontrolė

Visi su procedūrine kontrole susiję dalykai, tokie, kaip didelės atsakomybės reikalaujančių pareigų apibūdinimas, PRIVALO būti išdėstyti CPS.

5.2.1 Aukštos atsakomybės reikalaujančios pareigos

Sąlygų nėra

5.2.2 Užduočiai atlikti reikalingų asmenų skaičius

Sąlygų nėra

5.2.3 Konkrečias pareigas užimančių asmenų identifikavimas ir tapatybės nustatymas

Sąlygų nėra

5.3 Personalo kontrolė

5.3.1 Biografijai, kvalifikacijai, patirčiai ir patikimumui keliami reikalavimai

CA veiklą vykdantis personalas PRIVALO būti techniškai ir profesiškai kompetentingu. Kiekviena atitinkama CA savo CPS TURĖTŲ aprašyti kitas šį išskirtinį klausimą detalizuojančias nuostatas ir su tuo susijusius dalykus.

5.3.2 Biografijos patikrinimo procedūros

Sąlygų nėra

5.3.3 Apmokymams keliami reikalavimai

Sąlygų nėra

5.3.4 Kvalifikacijos tikrinimų kursų dažnumas ir jiems keliami reikalavimai

Sąlygų nėra

5.3.5 Rotacijos darbe dažnumas ir eiliškumas

Sąlygų nėra

5.3.6 Sankcijos už neautorizuotus veiksmus

Sąlygų nėra

5.3.7 Reikalavimai pagal sutartis dirbančiam personalui

Sąlygų nėra

5.3.8 Dokumentacija, kuria aprūpinamas personalas

Sąlygų nėra

6 Techninės saugos kontrolės priemonės

6.1 Raktų Poros Generavimas ir įdiegimas

Šis skyrius apibrėžią raktų tvarkymo ir atitinkamas techninio saugumo kontrolės priemones.

6.1.1 Raktų poros generavimas

Atitinkamos CA kriptografiniai raktai generuojami, naudojant darbui su sertifikatais skirtą programinės įrangos paketą.
Galutinių naudotojų kriptografiniai raktai naudotojų prašymo dėl sertifikato išdavimo pateikimo metu vietoje generuojami naršyklėje esančiu moduliu arba tai pirminės registracijos procedūros metu atlieka pati CA. Šios sertifikato taisyklės raktų poros, naudojamos neatšaukiamam pasirašymui, generavimui siūlo taikyti ankstesnę procedūrą. Antroji procedūra GALI būti taikoma raktų poros užšifravimui arba masinei raktų porų autentifikacijai.

6.1.2 Privataus rakto perdavimas subjektui

Galutinis naudotojas GALI pats sugeneruoti savo raktų porą. Svarbu pastebėti, kad tuo atveju, kai raktų poros generavimą atlieka CA, raktų pora galutiniam naudotojui PRIVALO būti išduota saugiu būdu. Smulkesnės detalės PRIVALO būti aprašytos CPS.

6.1.3 Privataus rakto perdavimas sertifikato sudarytojui

Individualiam sertifikavimui galutinis naudotojas TURĖTŲ pateikti vietoje sugeneruotą viešąjį raktą turintį prašymą CA/RA tarnybai. Kiekviena atitinkama CA savo CPS PRIVALO aprašyti viešojo rakto pristatymo procedūras.
Atitinkamos CA PRIVALO palaikyti bent jau PKCS#10 ir SPKAC formatus, ir pasirinktinai GALI palaikyti kitus. Jei viešasis galutinio naudotojo raktas generuojamas, nedalyvaujant CA/RA darbuotojams, tai CA NETURĖTŲ priimti formatų, neįrodančių rakto turėjimo.

6.1.4 CA viešojo rakto perdavimas naudotojams

Atitinkama CA PRIVALO pateikti mechanizmą, kaip CA galutiniams naudotojams viešus raktus pristatyti patikimu būdu. Smulkesnės detalės PRIVALO būti išdėstytos CPS.
Kiekvienu atveju CA viešieji raktai PRIVALO būti viešai prieinami talpykloje, naudojantis standartiniu protokolu, tokiu kaip HTTP ar LDAP.

6.1.5 Raktų dydžiai

Minimalų sertifikuojamam galutiniam naudotojui išduodamo privataus rakto ilgį PRIVALO nustatyti sertifikatus išduodanti CA ir jis turi būti ne trumpesnis, kaip 512 bitų. REKOMENDUOJAMA, kad rakto ilgis būtų mažiausiai 1024 bitų ilgio.
CA raktų pora PRIVALO būti bent minimalaus 1024 bitų ilgio, tačiau REKOMENDUOJAMA 2048 bitų ilgio raktų pora.

6.1.6 Viešojo rakto parametrų generavimas

Sąlygų nėra

6.1.7 Parametrų kokybės patikra

Sąlygų nėra

6.1.8 Raktų generavimas, naudojant kompiuterinę įrangą/programinę įrangą

Raktai gali būti generuojami programine įranga arba technine įranga (pvz., kriptografiniu įrenginiu), priklausomai nuo įvairių galutiniams naudotojams prieinamų priemonių.

6.1.9 Raktų naudojimo tikslai (pagal X.509 v3 rakto pritaikymo sritį)

Tikslai, kuriais naudojamas raktas, CA GALI būti apriboti per sertifikato KeyUsage plėtinį - tai yra laukelis, žymintis tikslą, kuriuo naudojamas sertifikuotas viešasis raktas.
Pagal šias taisykles išleistų sertifikatų KeyUsage plėtinys turi būti pažymėtas kaip Critical. Tai reiškia, kad sertifikatas TURĖTŲ būti naudojamas tik tais tikslais, kurių atitinkamų raktų panaudos (*key usage*) bitas prilygintas vienetui.

CA Sertifikatai

CA tarnybų sertifikatuose KeyUsage plėtinio digitalSignature - nonRepudiation - keyCertSign - cRLSign bitai PRIVALO būti prilyginti vienetui.
Tai taip pat GALI turėti kitus vienetui prilygintus bitus.

6.2 Privačiojo Rakto Apsauga

6.2.1 Kriptografinio modulio standartai

Šios sertifikato taisyklės neįpareigoja pasirinkti modulio su iš anksto nustatytais standartais. Kiekviena atitinkama CA CPS GALI pateikti daugiau detalių apie modulio standartų suderinamumą (kalbama apie standartinio modulio suderinamumo pasirinkimą).

6.2.2 Privačiojo rakto (n iš m) daugiaasmenė kontrolė

Privačiam asmens raktui PRIVALO NEBŪTI taikoma daugelio (n iš m) asmenų kontrolė. Tokia kontrolė GALI būti taikoma tik privatiems, CA priklausantiems raktams, techninės įrangos komponentams ar programinės įrangos komponentams: tokiu atveju kontrolės tipas PRIVALO būti aprašytas CPS.

6.2.3 Privačiojo rakto sąlyginis deponavimas [escrow]

Šios sertifikato taisyklės neskatina privačių raktų deponavimo politikos, tiek sertifikatų turėtojų, tiek CA. Tokių politikų vykdymas GALI būti leistas tik ir tada, jei to reikalauja valstybės, kurioje įsikūrusi CA, įstatymai.

6.2.4 Privačiojo rakto dubliavimas

Šios sertifikato taisyklės siūlo, kad visos PKI naudojančios pusės atkūrimo tikslams TURĖTŲ laikyti atsarginę privačiojo rakto kopiją tam, kad rakto sunaikinimo atveju jis būtų atkurtas. Ši atsarginė kopija PRIVALO būti rūpestingai apsaugota, ypač tuo atveju, kai kalbama apie privataus CA rakto kopiją.

6.2.5 Privačiojo rakto archyvavimas

Šios sertifikato taisyklės privataus rakto procedūrą siūlo vykdyti tik užšifravimui/iššifravimui naudojamam privačiam raktui. Žinoma, GALI prireikti laikyti privataus rakto kopiją tam, kad būtų teisingai iššifruojami pranešimai, netgi jei baigėsi atitinkamo viešojo rakto sertifikato galiojimas.

6.2.6 Privačiojo rakto įtraukimas į kriptografinį modulį

Privatūs visų sertifikatų turėtojų raktai TURĖTŲ būti saugojami užšifruota forma. Ši sąlyga ypatingai svarbi, jei sertifikato turėtoje yra CA.

6.2.7 Privačiojo rakto aktyvavimo metodika

Specifinės detalės, nusakančios, kaip aktyvuojamas privatus raktas, TURĖTŲ būti pateiktos CPS. Šios sertifikato taisyklės daugeliu atvejų rekomenduoja, kad privataus rakto aktyvavimui kai kurie specifiniai aktyvavimui reikalingi duomenys PRIVALO būti įvesti į kriptografinį modulį. Aktyvacijai reikalingi duomenys PRIVALO būti sudaryti mažiausiai iš PIN arba slaptažodžio, bet vertingesniam privačiam raktui (pvz., priklausantiems CA) siūloma naudoti kompiuterinės įrangos žetonus (angl. *hardware tokens*) ar biometrinės prieigos įrangą.

6.2.8 Privačiojo rakto deaktyvavimo metodika

Sąlygų nėra

6.2.9 Privačiojo rakto sunaikinimo būdai

Sąlygų nėra

6.3 Kiti raktų poros tvarkymo aspektai

6.3.1 Viešojo rakto archyvavimas

Atitinkama CA PRIVALO archyvuoti visus išduotus sertifikatus. Tam GALI būti naudojami kitokie, negu skaitmeninių parašų, vientisumo kontrolę užtikrinantys mechanizmai.

6.3.2 Viešojo ir privačiojo raktų naudojimo laikotarpis

Sąlygų nėra

6.4 Aktyvavimo duomenys

6.4.1 Aktyvavimo duomenų generavimas ir įdiegimas

Slaptažodžiai arba PIN numeriai TURĖTŲ būti pasirenkami, laikantis geriausios praktikos. Tai reiškia, kad būtina, jog būtų pasiūlytas tinkamas minimalus slaptažodžių ilgis ir įgyvendinti mechanizmai, galintys patikrinti, ar slaptažodžiai yra pakankamai entropiški.

6.4.2 Aktyvavimo duomenų apsauga

Privačių raktų apsaugai skirti slaptažodžiai TURĖTŲ būti prieinami tik teisėtiems naudotojams (pvz., asmeninio sertifikato - sertifikato turėtojui, CA operatoriams, prižiūrintiems CA pasirašymui skirtus raktus ir pan.). Išimtimi šiam nurodymui yra saugaus aktyvacijai reikalingų duomenų

archyvavimo/atsarginių kopijų darymo mechanizmo įgyvendinimas. Toks mechanizmas PRIVALO būti aiškiai aprašytas CPS.

6.4.3 Kiti aktyvavimo duomenų aspektai

Sąlygų nėra

6.5 Kompiuterinės saugos kontrolės priemonės

6.5.1 Specifiniai techniniai reikalavimai kompiuterinei saugai

Sąlygų nėra

6.5.2 Kompiuterių saugos lygio įvertinimas

Sąlygų nėra

6.6 Galiojimo laikotarpio techninė kontrolė

6.6.1 Sistemos plėtojimo kontrolės priemonės

Sąlygų nėra

6.6.2 Saugos vadybos kontrolės priemonės

Sąlygų nėra

6.6.3 Galiojimo laikotarpio saugos lygis

Sąlygų nėra

6.7 Tinklo saugumo kontrolės priemonės

Šios sertifikato taisyklės tvirtai pataria, kad įrenginys, kuriame veikia CA veiklai naudojamas kriptografinis modulis, tinklo atakoms išvengti TURĖTŲ būti atjungtas nuo viešųjų ryšių tinklų. Kiekvienu atveju, priėjimas per tinklą prie CA darbinės stoties PRIVALO būti apribotas tam, kad CA privatus raktas būtų tinkamu būdu apsaugotas nuo atskleidimo.

6.8 Kriptografinio modulio inžinerinės kontrolės priemonės

Sąlygų nėra

7 Sertifikato ir CRL profiliai

7.1 Sertifikato Profilis

Tam, kad būtų skatinamos tinklų sąveikos galimybės, Šios sertifikato taisyklės atitinkamą CA ypač skatina profiliuoti išleidžiamus sertifikatus, atsižvelgiant į [3]. Kiekvienu atveju, CPS PRIVALO išsamiai aprašyti specifinį prisiimtą profilį.

7.1.1 Versijos numeris(iai)

Sertifikato versijos laukelis TURĖTŲ būti bent 2. Atitinkama CA PRIVALO išduoti X.509 3-ios ir didesnės versijos sertifikatus.

7.1.2 Sertifikato plėtiniai

Sutinkamai su [3], REKOMENDUOJAMA įgalinti šiuos sertifikato plėtinius:

Plėtinio pavadinimas	**Plėtinio Vertė**
SubjectKeyIdentifier	NOT CRITICAL
AuthorityKeyIdentifier	NOT CRITICAL
BasicConstraints	CRITICAL
KeyUsage	CRITICAL
CertificatePolicies	NOT CRITICAL

Taip pat REKOMENDUOJAMA naudoti kitus du plėtinius: CRLDistributionPoint, pateikiantį informaciją, naudingą CRL gavimui, ir SubjectAltNames, kai į sertifikatą prireikia įtraukti RFC822 atitinkantį e-pašto adresą. Abu šie plėtiniai TURĖTŲ būti pažymėti kaip NOT CRITICAL.

7.1.3 Algoritmo objekto identifikatoriai

Sąlygų nėra

7.1.4 Vardų [pavadinimų] formos

Visi su tuo susiję dalykai PRIVALO būti išdėstyti CPS

7.1.5 Vardams [pavadinimams] taikomi apribojimai

Visi su tuo susiję dalykai PRIVALO būti išdėstyti CPS

7.1.6 Sertifikavimo taisyklių Objekto Identifikatorius

Kiti Sertifikavimo taisyklių Objektų Identifikatoriai taikomi tik ir tada, jei nustatoma, kad kitos taisyklės suderinamos su šiomis. Atitinkama CA PRIVALO susisiekti su įvairių sertifikavimo taisyklių kūrėjais, kad būtų sutikrintas tarpusavio suderinamumo lygis. Bet kokiu atveju, tam, kad būtų skatinamos tinklų sąveikos galimybės, atitinkamas RFC 2459 šioms taisyklėms siūlo į sertifikatą įtraukti tik vieną Objekto Identifikatorių.

7.1.7 Sertifikavimo taisyklių nustatomų apribojimų išplėtimas

Visi su tuo susiję dalykai PRIVALO būti išdėstyti CPS

7.1.8 Sertifikavimo taisyklių apibrėžimų žodžių sintaksė ir semantika

Sertifikavimo Taisyklių plėtinio laukelis turi perdavimo sąlygą ir kartu su kiekvienu sertifikavimo taisyklių identifikatoriumi, papildomą nuo sertifikavimo taisyklių priklausančią informacijos patikslinimo laukelyje.
Šios sertifikavimo taisyklės pataria, kad patikslinimo laukelis TURĖTŲ būti CPS nuorodų patikslinimo, savyje turintis nuorodą į CA paskelbtus Sertifikavimo veiklos nuostatus (CPS).
Nuoroda pateikiama uniform resource identifier (URI) forma.

7.2 CRL [Atšauktų Sertifikatų Sąrašo] Profilis

7.2.1 Versijos numeris(iai)

CRL sąrašų versijos laukelis TURĖTŲ būti lygus bent 1. Atitinkama CA PRIVALO skelbti X.509 2-os ar didesnės versijos CRL sąrašus.

7.2.2 CRL ir jo papildymas

Sąlygų nėra.

8 Specifikacijų administravimas

8.1 Specifikacijų keitimo procedūros

Sertifikato taisyklėms ir CPS gali būti taikomi redakciniai pakeitimai. Esminių sertifikavimo taisyklių pokyčių atveju apie tai TURĖTŲ būti informuojamos visos CA tarnybos ir galutiniai naudotojai. Be to, jei reikia, visos CA tarnybos TURĖTŲ atnaujinti savo Sertifikavimo veiklos nuostatus, atsižvelgdamos į sertifikavimo taisyklių pasikeitimus aukštesniajame lygyje.

Apie Sertifikavimo veiklos nuostatų pokyčius, sudarančius tik nežymius techninius pagerinimus, TURĖTŲ būti pranešama iš anksto.

8.2 Skelbimų ir pranešimų tvarka

Šios sertifikato taisyklės prieinamos Internete URI http://www.europki.org/ca/root/cps/ adresu.

8.3 CPS peržiūros procedūros

PRIVALO būti įvertinta, ar atitinkama CA atitinka šias Sertifikato taisykles. Tam, kad tai būtų atlikta, atitinkamos CA tarnybos gali išsiųsti savo CPS 1.4.3. skyriuje nurodytiems kontaktiniams asmenims. Po to atitinkama CA PRIVALO laukti atsakymo. Laiko limitas, reikalingas atlikti įvertinimui, lygus 60 dienų. Gali būti priimtina, kad atitinkama CA pati įvertintų savo pačios atitikimą Sertifikato taisyklėms; tokiu atveju, jei vėliau EuroPKI būtų pranešta apie CA neatitikimą Sertifikato taisykles, CA sertifikatas TURĖTŲ būti atšauktas.

1 Priedas: Glosarijus

Sertifikavimo Tarnyba (CA) - Tarnyba, kuriai vienas ar daugiau naudotojų patikėjo kurti ir [pri]skirti viešųjų raktų sertifikatus bei (pasirinktinai) kurti naudotojų raktus. Svarbu pažymėti, kad CA yra atsakinga ne tik už jų išdavimą - už viešųjų raktų sertifikatus ji atsako per visą jų galiojimo laikotarpį.

CA sertifikatas - sertifikatas vienam iš CA viešųjų raktų, kurį išdavė kita CA.

Sertifikato taisyklės (CP) - Pavadinimą turintis taisyklių rinkinys, apsprendžiantis sertifikato taikymą tam tikroje srityje, laikantis bendrų saugumo reikalavimų. Pavyzdžiui, kuri nors atskira sertifikavimo taisyklė gali nurodyti, kad tam tikro tipo sertifikatas gali būti naudojamas EDI sandorių autentifikacijai, leidžiant prekiauti iki nurodytos sumos kainuojančiomis prekėmis.

Sertifikavimo seka - Nuosekli sertifikatų seka, kuri kartu su viešuoju pradinio sekos objekto raktu gali būti panaudota gauti galiniam sekos objektui.

Sertifikavimo Veiklos Nuostatai (CPS) - Veiklos nuostatai, kurių Sertifikavimo Tarnyba laikosi, išduodama sertifikatus.

Atšauktų sertifikatų sąrašas (CRL) - CRL yra laiko žymą turintis sąrašas, pateikiantis informaciją apie CA pasirašytus ir atšauktus sertifikatus, laisvai prieinamas viešam naudojimui skirtoje talpykloje.

Sertifikatą išdavusi tarnyba (issuing CA) - Atskiro sertifikato kontekste sertifikatą išdavusia CA laikoma jį išdavusi CA tarnyba (t.p. žr. Subjektą sertifikavusi tarnyba).

Viešojo Rakto Sertifikatas (PKC) - Duomenų struktūra, kuri yra pasirašyta skaitmeniniu ją išleidusios CA privačiuoju raktu, sudaranti viešąjį galutinio naudotojo raktą ir kai kurią kitą informaciją.

Viešųjų Raktų Infrastruktūra (PKI) - Techninės įrangos, programinės įrangos, žmonių, taisyklių ir procedūrų rinkinys, reikalingas viešųjų raktų kriptografija pagrįstų PKC kūrimui, tvarkymui, saugojimui, platinimui ir atšaukimui.

Registavimo Tarnyba (RA) - Tarnyba, atsakinga už sertifikato subjektų identifikaciją ir autentifikaciją, tačiau neatliekanti sertifikatų pasirašymo ir išdavimo funkcijų (t.y., RA paskirtis - kai kurių užduočių už CA atlikimas). [Pastaba: terminas Vietinė Registravimo Tarnyba (LRA) čia visur naudojamas išreikšti tai pačiai koncepcijai.]

Sertifikatu pasitikinti šalis (RP) - Sertifikato gavėjas, kuris veikia pasitikėdamas sertifikatu ir/ar skaitmeniniais parašais, patikrintais naudojant sertifikatą. Šiame dokumente terminai „sertifikato naudotojas“ ir „sertifikatu pasitikinti šalis“ naudojami pakaitomis.

Subjektą sertifikavusi tarnyba (subject CA) - Atskiro CA sertifikato kontekste subjektą sertifikavusia tarnyba laikoma CA, kurios viešasis raktas sertifikuotas sertifikate.

IPR - Intelektinės Nuosavybės Teisės

2 Priedas: Raktiniai žodžiai, RFC naudojami Nusakyti Reikalingumo Lygiams.

Pagal RFC 2119 [2]: Raktiniai Žodžiai, RFC naudojami Nusakyti Reikalingumo Lygiams, mes nurodome, kaip turi būti aiškinami pagrindiniai RFC dokumentuose naudojami raktiniai žodžiai. Šių principų besilaikantys autoriai savo dokumento pradžioje turėtų įdėti šią frazę:

Raktiniai žodžiai „PRIVALO“, „NEPRIVALO“, „BŪTINA“, „TURI“, „NETURI“, „TURĖTŲ“, „NETURĖTŲ“, „REKOMENDUOJAMA“, „GALI“ ir „PASIRINKTINAI“ šiame dokumente turi būti aiškinami taip, kaip tai aprašyta RFC 2119.

1. PRIVALO - Šis žodis ar terminai „BŪTINA“ ar „TURI“ reiškia, kad definicija esti besąlygine specifikacijos būtinybe.

2. NEPRIVALO - Šis posakis ar posakis „NETURI“ reiškia, kad definicija specifikacijoje yra visiškai draudžiama.

3. TURĖTŲ - Šis žodis arba būdvardis „REKOMENDUOJAMA“ reiškia, kad esant tam tikroms aplinkybėms, gali būti svarių priežasčių, kad būtų ignoruojamas atskiras dalykas, bet prieš pasirenkant kitokį sprendimą, turi būti pilnai suprastos ir nuodugniai įvertintos visos galimos to pasekmės.

4. NETURĖTŲ - Šis posakis ar posakis „NEREKOMENDUOJAMA“ reiškia, kad esant tam tikroms aplinkybėms, gali būti svarių priežasčių, kad būtų priimtinas ar net naudingas kitoks sprendimas, bet prieš pasirenkant tokį sprendimą ir imantis kitokių, negu nurodyta, veiksmų turi būti pilnai suprastos ir nuodugniai įvertintos visos galimos to pasekmės.

5. GALI - Šis žodis arba būdvardis „PASIRINKTINAI“, reiškia, kad dalyką iš tikrųjų galima pasirinkti. Prekių ir paslaugų teikėjas gali jį pasirinkti, jei tai būtina tam tikrai rinkai arba jei jis mano, jog tai pagerins produktą, kai kitas prekių ir paslaugų teikėjas į šį dalyką gali nekreipti dėmesio. Sprendimas, nesuteikiantis pasirinkimo galimybės, PRIVALO būti paruoštas sąveikai su kitais, pasirinkimą suteikiančiais sprendimais, nors jie, galbūt, bus ir mažiau funkcionalūs. Tuo pačiu sprendimas, numatantis pasirinkimo galimybę, PRIVALO būti paruoštas sąveikai su kitu sprendimu, nenumatančiu pasirinkimo (žinoma, išskyrus pasirinkimo suteikiamą galimybę).

Nuorodos

[1] RFC 2527. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. March 1999: [ftp://ftp.isi.edu/in-notes/rfc2527.txt]
[2] RFC 2119. Key words for use in RFCs to Indicate Requirement Levels. March 1997: [ftp://ftp.isi.edu/in-notes/rfc2119.txt]
[3] RFC 2459. Internet X.509 Public Key Infrastructure: Certificate and CRL Profile. January 1999: [ftp://ftp.isi.edu/in-notes/rfc2459.txt]
[4] RFC 2560. Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol. OCSP. June 1999: [ftp://ftp.isi.edu/in-notes/rfc2560.txt]