Parengė: E3P Darbinė Grupė
Patvirtino: E3P Koordinacinis Komitetas – 2007-01-25
Rekomendacija E3P nariams, skelbiama www.parasas.lt

Bendroji PKI Specifikacija

1 Tikslas ir apimtis

Šis dokumentas aprašo *PKI* panaudojimo ypatybes bei nusako šios infrastruktūros elementams keliamus reikalavimus. Šiame dokumente pateikiamos rekomendacijos yra susijusios tik su *kvalifikuoto elektroninio parašo* taikymais ir yra taikomos gyventojams, įmonėms ir institucijoms, siekiantiems tarpusavio **suderinamumo/sąveikumo**.

Elektroninio parašo taikymų *suderinamumas* apibrėžiamas sekančiai:

i) galimybė *vartotojui* pasinaudoti įvairių *Paslaugų Tiekėjų* teikiamomis paslaugomis, kai *vartotojo* identifikavimas įvyksta panaudojant vieną ir tą pačią *saugaus elektroninio parašo formavimo priemonę*;

ii) galimybė šalims keistis elektroniniu parašu *pasirašytais e-dokumentais* taip, jog neiškyla suderinamumo klausimų (nei viena iš šalių nesirūpina papildomu *pasirašytų e-dokumenų* apdorojimu ar konvertavimu).

Užtikrinant suderinamumo principą i), yra siekiama, jog *kvalifikuoto sertifikato* panaudojimo atveju, vartotojui iš *Paslaugų Tiekėjo* pusės nebūtų nurodoma atnaujinti paslaugų teikimo sutartį, kiekvieną kartą, vartotojui atnaujinus/pasikeitus savo *saugaus elektroninio parašo formavimo priemonę*.

Užtikrinant suderinamumo principą ii), yra siekiama apsikeičiant *pasirašytais e-dokumentais*, naudoti sutartą elektroninio parašo formatą.

2 Versijų istorija

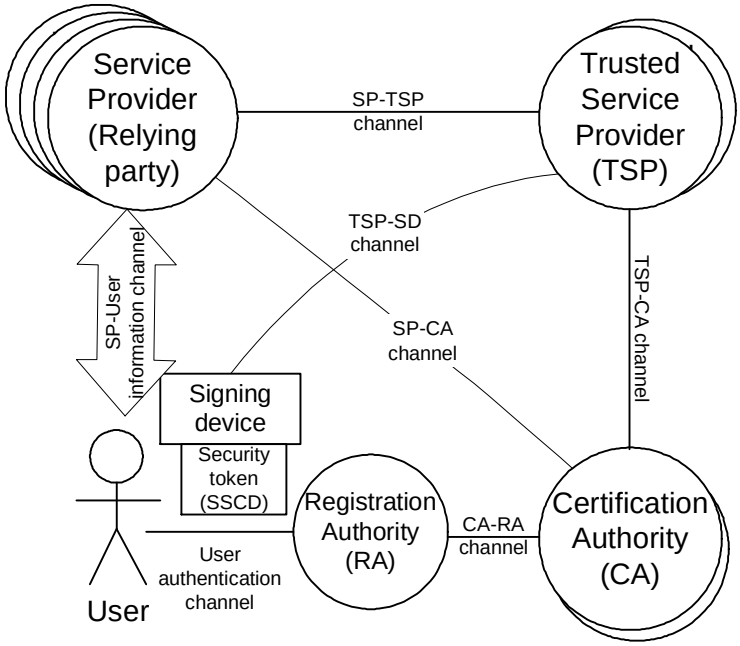
Versija 1.0 2006-11-16 Juodraštinė versija
Versija 1.2 2006-12-04 EPDG narių pastabos
Versija 1.4 2006-12-20 SODROS (AM) pastabos
Versija 1.5 2007-01-08 Revizija
Versija 1.6 2007-01-18 E3P Koordinacinio Komiteto tvirtinama redakcija

3 Terminai

Visi šiame dokumente pateikiami terminai ir santrumpos, pateikiami *pasvirusiu tekstu,* yra suprantami "siaurąja prasme" taip, kaip tai apibrėžta ar išaiškinta šio dokumento **Priede A**.

4 Įvadas (Informacinė dalis)

PKI numatomos sekančios privalomos rolės:



Šios schemos sėkmingam veikimui privalo būti nustatyti sekantys verslo santykiai, užtikrinantys kokybišką paslaugų teikimą:

Vartotojas - CA: dėl *kvalifikuoto sertifikato* paslaugos teikimo
RA - CA: dėl *registravimo paslaugų* teikimo
SP-TSP: dėl *PKI paslaugų* teikimo

Taip pat neprivalo, bet gali būti sudarytos papildomos sutartys tarp:

TSP ir susijusių šalių, pvz. *CA*, *laiko žymų tarnybos, mobiliųjų operatorių* ir pan.
Vartotojo ir SP - dėl paslaugų teikimo, panaudojant *SSCD*.

4.1 Funkcionalumo apžvalga

PKI yra panaudojama *Paslaugų Tiekėjų (SP)* masinei rinkai teikiamose paslaugose per šias funkcijas:

- *Žmogaus identifikavimas* (pvz., prisijungimo prie elektroninės bankininkystės sistemos metu);
- *Duomenų pasirašymas*:
  a) vidiniams *SP* taikymams (pvz., operacijų autentiškumo užtikrinimas, kai parašas naudojamas *SP* vidinėse sistemose ir jis nėra skirtas panaudoti už *SP* ribų),
  b) išoriniams taikymams (pvz., sutarčių sudarymui, kai *pasirašytas e-dokumentas* gali būti panaudotas/perduotas trečiosioms šalims už *SP* ribų);
- *Duomenų užkodavimas*:
  a) saugus teksto perdavimas iš *SP vartotojui* (saugus slaptos informacijos transportavimas),
  b) asmeninės *vartotojo* informacijos apsauga *SP* sistemose (ilgalaikis slaptos informacijos apsaugojimo būdas).

Taip pat *PKI* atlieka papildomą funkciją, kai vartotojo *SSCD* nėra panaudojamas:

- *Pasirašytų duomenų* autentiškumo patikrinimas.

Sertifikavimo Tarnybos (*CA*) per savo įgaliotas *Registravimo Tarnybas (RA)* patikrina **fizinių** asmenų tapatybę ir jiems išduoda *SSCD*. *RA* perduoda į *CA* duomenis apie fizinį asmenį bei jam suteiktą *SSCD*. Šie duomenys panaudojami sukuriant *kvalifikuotą sertifikatą*.
SP teikia paslaugas savo apibrėžiamais būdais - per specialias aplikacijas, internetu, ar balsu. Prieš teikiant tokias paslaugas, *SP*, esant poreikiui, gali su *vartotojais* sudaryti paslaugų teikimo sutartis, tačiau šios sutartys yra susiejamos su *vartotojo* kaip fizinio asmens tapatybe (vardu, pavarde, asmens kodu), o ne su *SSCD*. Dėl šios priežasties, *vartotojui* nereikia iš naujo pasirašinėti paslaugų teikimo

sutarties, jei pasikeičia jo *SSCD*, bet asmens duomenys išlieka tie patys (Vardas, pavardė, asmens kodas), taip pat vienu metu *vartotojas* gali naudotis keletu skirtingų *SSCD*, kurie neturi būti diskriminuojami, t.y. turi būti užtikrinama vartotojo pasirinkimo laisvė.
SP **tiesiogiai su *PKI* nesąveikauja**. Visas su *PKI* susijusias paslaugas *SP* gauna per *TSP*.
TSP užtikrina *SP* ir visų susijusių *PKI infrastruktūros* elementų sąveiką, užtikrina *PKI paslaugų suderinamumą,* galimybę *vartotojams* vienu metu naudotis keletu *SSCD*.
Ryšiai tarp *PKI infrastruktūros* dalyvių užtikrinami saugiais kanalais ir/ar jungtimis ir/arba keičiantis pasirašytais ir, esant reikalui, užšifruotais pranešimais.
Vartotojo pasirašymo priemonė gali būti kompiuteris, mobilusis telefonas ar bet kokia kita įranga, sąveikaujanti su *SSCD* ir įgalinanti *kvalifikuotų sertifikatų* panaudojimą.

4.2 Konceptualus Aprašymas

PKI veikimo konceptualus aprašymas susideda iš 3 procesų: *SSCD* išdavimo ir *kvalifikuoto sertifikato* sukūrimo/aktyvavimo, panaudojimo bei nutraukimo.

4.2.1 *SSCD* išdavimas ir *kvalifikuoto sertifikato* sukūrimas/aktyvavimas

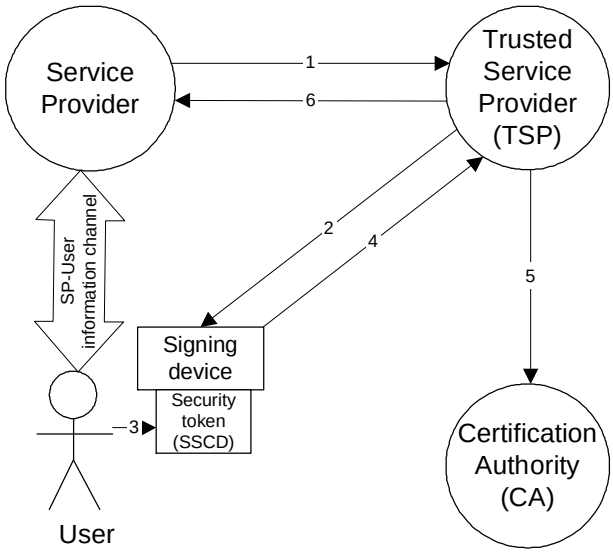
Saugaus elektroninio parašo formavimo priemonė SSCD yra suteikiama fiziniam asmeniui (žmogui) ir šio įrenginio panaudojimas yra reglamentuojamas "*vartotojo* ir *CA*" sutartimi, kuri susieja *SSCD* su konkrečiu asmeniu.
SSCD išdavimo ir *kvalifikuoto sertifikato* sukūrimo/aktyvavimo procesas yra skirtas:

- identifikuoti fizinius asmenis pagal jų galiojančius asmens tapatybės dokumentus,
- pasirašyti "*vartotojo* ir *CA*" sutartį, suteikti *saugaus elektroninio parašo formavimo priemones* (*SSCD*),
- sukurti ir aktyvuoti *kvalifikuotą sertifikatą*.

SSCD išdavimo procedūrą reglamentuoja "*Registracijos Politika*" (*RP*).
Kvalifikuoto sertifikato gamybos aplinką nusako "*Sertifikavimo Veiklos Nuostatai*" (*CPS*).
Kvalifikuotą sertifikatą kaip produktą ir jo panaudojimo sritį aprašo "*Sertifikato Politika*" (*CP*).

4.2.2 Panaudojimas

Panaudojimo atveju, *Paslaugų Tiekėjas* (*SP*) kreipiasi į *TSP* su užklausa suteikti su *PKI paslaugas* (pvz., *autentifikuoti vartotoją* arba *pasirašyti duomenis*):



1. Paslaugų tiekėjas kreipiasi į *TSP* paslaugos, susijusios su *PKI* panaudojimu.
2. *TSP* suformuoja dialogą vartotojo *pasirašymo įrenginyje*.
3. *Vartotojas* patvirtina užklausą, suvesdamas savo *pasirašymo kodą*.
4. *TSP* gauna *parašo duomenis* iš *pasirašymo įrenginio*.
5. *TSP* patikrina *parašo duomenų* teisingumą, *sertifikato* galiojimą, prideda papildomą informaciją.
6. *Paslaugų Tiekėjui* pateikiama *PKI paslauga*.

4.2.3 Nutraukimas

"V*artotojo* ir *CA*" sutaris yra siejama su *vartotojui* suteiktu *SSCD* bei su *kvalifikuotu sertifikatu*, kuris savo ruožtu yra susijęs su *SSCD* saugoma slapta informacija. Galimi du nutraukimo atvejai:

- nutraukti tik *kvalifikuoto sertifikato* galiojimą (pvz., kai pasikeičia asmens duomenys), paliekant galioti "*vartotojo* ir *CA*" sutartį;
- nutraukti "*vartotojo* ir *CA*" sutartį, kartu panaikinant *kvalifikuotą sertifikatą*, jei toks buvo sukurtas/aktyvuotas.

Nuo CA politikos priklauso ar tas pats *SSCD* gali būti panaudojamas tik vieną kartą, (susiejant *SSCD* su konkrečiu *kvalifikuotu sertifikatu*) ar keletą kartų (susiejant naujus *kvalifikuotus sertifikatus* su tuo pačiu SSCD, kai nutraukiamas ankstesniųjų *sertifikatų* galiojimas).
Kvalifikuotų sertifikatų galiojimo nutraukimą reglamentuoja *RP* ir *CP* dokumentai.
Nutraukti "*vartotojo* ir *CA*" sutartį galima keletu būdų:

- *Vartotojui* įspėjus *RA*, kad nebenori naudotis *PKI paslaugomis*,
- *Vartotoui* įspėjus *RA*, kad *SSCD* yra prarastas ar sukompromituotas,
- *RA* arba *CA* gali nutraukti sutartį dėl šios sutarties pažeidimų ar kitų įstatymuose numatytų atvejų,
- *RA* gali nutraukti sutartį atvejais, nurodytais *RP* dokumente.

Sertifikato nutraukimo atvejais *RA* praneša *CA* apie *sertifikato* nutraukimą, CA nutraukia *sertifikato* galiojimą.

5 Verslo modelis

Šiame skyriuje aprašomi verslo santykiai tarp būtinųjų *PKI* rolių atlikėjų.

5.1 *RA* (*registravimo tarnyba*)

Registravimo Tarnyba palaiko verslo santykius su:

- savo klientais (*vartotojais*)
- *CA*, tarpininkaudama santykiuose tarp *vartotojo* ir *CA*.

5.1.1. *RA-vartotojai*

RA nustato vartotojų tapatybę ir tarpininkauja jiems pasirašant "*vartotojo* ir *CA*" sutartį,
RA išduoda *SSCD* ir apmokestina vartotojus (jei taikomi *SSCD* išdavimo ar palaikymo mokesčiai),
RA konsultuoja *vartotojus* iškilusiais *PKI* klausimais, juos apmoko, teikia instrukcijas ir informacinę medžiagą,
RA inicijuoja *kvalifikuotų sertifikatų* sukūrimą/aktyvavimą,
RA inicijuoja *kvalifikuotų sertifikatų* galiojimo nutraukimą/atšaukimą.
RA registruoja visus su *PKI* veikimu susijusius sutrikimus, informuoja *vartotojus* apie sutrikimų pašalinimą.

5.1.2. *RA-CA*

RA išpildo *SSCD* keliamus reikalavimus (žr. **6.1**) ,
RA registruoja *vartotojų* paraiškas, patikrina jų asmens duomenų autentiškumą ir galiojimą, suteikia jiems *SSCD* bei atlieka jų gyvenimo ciklo valdymą (aktyvavimą, deaktyvavimą), prisilaikant *RP*,
RA tarpininkauja tarp *vartotojo* ir kitų *PKI* dalyvių, registruojant ir sprendžiant visas problemas, susijusias šios infrastruktūros veikimu,
RA saugo ir archyvuoja "*vartotojo* ir *CA*" sutartis,
RA atsiskaito su *CA* už *sertifikatų* palaikymą (kai tai yra aktualu).

5.1.3 Mokesčiai

Rekomenduojama, kad *RA* subsidijuotų *SSCD*.
Rekomenduojama, kad *RA* apmokestintų vartotojus minimaliais "palaikymo" mokesčiais taip, kad tie mokesčiai padengtų *RA* kaštus (kad šie kaštai nebūtų perkeliami kitiems *PKI* dalyviams) ir kad vartotojai būtų suinteresuoti ne tik įsigyti SSCD, bet ir juos naudoti.

5.2 *CA* (*sertifikavimo tarnyba*)

Sertifikavimo tarnyba palaiko verslo santykius su *RA* ir teikia viešai prieinamas su *PKI* susijusias (*kvalifikuotiems sertifikatams* privalomas) paslaugas, pagal poreikį, palaiko verslo santykius su *TSP*.

5.2.1. *CA-RA*

CA pagal *RA* pateiktus duomenis sukuria kvalifikuotus skaitmeninius sertifikatus (žr. **6.2**)

CA užtikrina *sertifikatų* gyvenimo ciklo valdymą pagal *RA* arba *vartotojų* pateikiamas užklausas.

5.2.2. *CA-vartotojai*

CA įsipareigoja realizuoti *sertifikavimo paslaugas* taip, kaip šių paslaugų atlikimą reglamentuoja Lietuvos įstatymai bei su šių paslaugų atlikimu susiję dokumentai.

5.2.3 Mokesčiai

Rekomenduojama, kad *CA* nereikalautų išankstinio mokėjimo už *sertifikato* naudojimą į priekį, o kad šis mokestis būtų paskaičiuojamas už faktinį sertifikato panaudojimą (pvz., kas mėnesį).

Rekomenduojama, kad *kvalifikuotų sertifikatų* kaštus padengtų valstybė (t.y. nuosavybės teisė į *kvalifikuotus sertifikatus* priklausytų valstybei).

5.3 *TSP*

TSP atlieka tarpininko vaidmenį tarp *SP* ir kitų *PKI* elementų/dalyvių. Nėra apribojimų, draudžiančių tai pačiai įmonei/įstaigai/institucijai vykdyti *SP* ir *TSP* roles.

5.3.1. *TSP- SP*

TSP teikia *PKI paslaugas Paslaugų Tiekėjui,*

TSP apmokestina *SP* arba teikiamos *PKI paslaugos* gali būti viešos ir nereikalauti *TSP-SP* susitarimo, jei iš *SP* pusės nekeliama reikalavimų šių paslaugų kokybei ir/arba iš *TSP* pusės - apmokėjimui už šias paslaugas,

TSP palaiko verslo santykius (jei tai būtina) su visais *PKI* dalyviais,

TSP užtikrina *PKI paslaugų* kokybę, sprendžia su *PKI paslaugų* teikimu susijusias problemas,

TSP atlieka techninę *PKI paslaugų* priežiūrą/aptarnavimą/palaikymą/monitoringą,

TSP užtikrina prisilaikymą reikalavimų, susijusių su *kvalifikuoto parašo paslaugų* sukūrimu/palaikymu.

5.3.2 Mokesčiai

Rekomenduojama, kad *TSP* apmokestintų *SP* už naudojimąsi *TSP* paslaugomis fiksuotu mėnesiniu mokesčiu, priklausomai nuo teikiamos paslaugos kiekybinių, kokybinių ir kitokių parametrų.

5.4 *SP* (*paslaugų tiekėjas*)

Paslaugų tiekėjai teikia paslaugas (panaudojant *PKI paslaugas*) vartotojams.

5.4.1. *SP-TSP*

SP užtikrina savo sistemų saugumo lygį, būtiną teikti *kvalifikuoto parašo paslaugas* (kai tai aktualu),

SP tarpininkauja tarp *vartotojo* ir kitų *PKI* dalyvių, registruojant ir sprendžiant visas problemas, susijusias šios infrastruktūros veikimu.

5.4.2 Mokesčiai

Rekomenduojama, kad *SP* neapmokestintų *vartotojų* už naudojimąsi *PKI paslaugomis*.

Rekomenduojama, kad *SP* patys padengtų kaštus, susijusius su *PKI paslaugų* panaudojimu (instaliacijos ir operacijų kaštus).

5.5 *Vartotojai* (*SSCD* turėtojai)

5.5.1 *Vartotojas - CA*

Vartotojas įsipareigoja naudoti jam suteiktą *SSCD* tik asmeniškai,

Vartotojas įsipareigoja saugoti savo *pasirašymo kodą,* neatskleisti jo tretiesiems asmenims ir, esant reikalui, jį pasikeisti,

Vartotojas įsipareigoja įspėti *RA* apie galimą nelegalų *SSCD* ir/arba *pasirašymo kodo* panaudojimą,

Vartotojas atsako už *sertifikate* pateikiamų asmens duomenų teisingumą,
Vartotojas privalo suprasti *CA, RA* ir savo atsakomybės ribas, naudojantis SSCD ir *kvalifikuotais sertifikatais*.
Vartotojas privalo laikytis *SSCD* ir *sertifikatų* panaudojimo reglamento, nusakomo "*vartotojo* ir *CA*" sutartimi, bei susijusiais dokumentais.

5.5.2 Mokesčiai

Rekomenduojama, kad *vartotojas* pats padengtų tinklo prieigos (interneto ir/arba mobiliojo ryšio) mokesčius.

6 Pagrindiniai Techniniai Reikalavimai (Normatyvinė dalis)

Šis skyrius nusako pagrindinius reikalavimus, keliamus *PKI* ir šios infrastruktūros elementams/dalyviams.

6.1 Reikalavimai *SSCD* įrenginiams

Yra laikoma, jog *SSCD* įrenginiai išpildo visus būtinus reikalavimus ir yra pritaikyti teikti *kvalifikuoto parašo paslaugoms*.

PKI.1 *SSCD* privalo būti gaminami, laikantis specialių saugumo reikalavimų ir turi būti vertinami kaip saugūs, kai tokio vertinimo patikimumas atitinka standarto "Common criteria - security" (ISO/IEC 15408) EAL4 saugumo lygį, pagal saugumo profilį, apibrėžtą "CEN workshop agreement" CWA 14169". *SCCD* gamintojas privalo *Sertifikavimo Tarnybai* pateikti saugumo bei jo įvertinimo atitikties sertifikatą.
PKI.2 *SSCD* privalo turėti bent vieną *kriptografinių raktų* porą, kuri vartotojo registracijos ir *sertifikato* sukūrimo/ktyvavimo metu susiejama su *kvalifikuotu sertifikatu*, turinčiu *neišsigynimo požymį*.
PKI.3 *SSCD* ir susijusi *pasirašymo įranga* privalo užtikrinti, jog *privataus rakto* ir su juo susijusio *kvalifikuoto sertifikato* negalėtų panaudoti nepatikima programinė įranga, arba *vartotojas* pats priimtų sprendimą dėl tokios įrangos patikimumo, prieš nuspręsdamas šį *privatųjį raktą* panaudoti.
PKI.4 *SSCD* saugomas *privatusis raktas*, susietas su *kvalifikuotu sertifikatu*, negali turėti kopijos ir turi būti neįmanoma šio *privataus rakto* nuskaityti iš *SSCD* jokiomis žinomomis techninėmis priemonėmis.
PKI.5 *SSCD* saugomi *privatieji raktai* privalo būti apsaugoti *"signataro" PIN kodu* (*sPIN*), kuris negali būti trumpesnis, nei 4 skaitmenys ir privalo užsiblokuoti neteisingai suvedus jo reikšmę 5 kartus. *sPIN* kodo atblokavimo procedūros nėra arba ją gali įvykdyti tik *RA* atstovas, šią operaciją registruojant sistemose. *sPIN* reikšmę privalo nustatyti pats *vartotojas*, *sPIN* reikšmė saugoma tik *SSCD* įrenginyje ir nėra atsarginės šio *sPIN* kopijos jokiose kitose sistemose.
PKI.6 *SSCD* privalo būti perduodamas *vartotojui* tokiu būdu, kad nebūtu užkirstas kelias vėliau šį *SSCD* panaudoti sukuriant/aktyvuojant šio *kvalifikuotą sertifikatą*.

6.2 Reikalavimai *kvalifikuotiems sertifikatams* (*Certificate Policy*)

Šie reikalavimai taikomi nustatant naudotinų *kvalifikuotų sertifikatų* politiką (*CP*) taip, jog būtų užtikrinamas teikiamų *PKI paslaugų suderinamumas*. Rekomenduojama visiems *vartotojams*, įsigyjantiems *SSCD*, suteikti galimybę aktyvuoti *kvalifikuotą sertifikatą*, tinkantį *kvalifikuoto parašo paslaugoms*.

PKI.10 *Sertifikato* galiojimo laikas negali būti ilgesnis, nei galiojimo laikas asmens tapatybės dokumento, pateikto *vartotojo* registracijos metu; *sertifikato* aktyvavimo metu asmens tapatybės dokumentas privalo būti galiojantis.
PKI.11 *Sertifikatas* turi atitikti x.509 v3 formatą aprašytą RFC3280.
PKI.12 Rekomenduojama *kvalifikuotuose sertifikatuose* talpinti sekančią informaciją: sertifikatą išleidusios *CA* pavadinimas; sertifikato turėtojo vardai ir pavardės; minėto turėtojo unikalus identifikatorius; sertifikato galiojimo laikotarpis; sertifikato (eilės) numeris (angl. serial number); informacija apie sertifikatui taikomas taisykles; sertifikato paskirtis ir kita sertifikatų naudojimui reikalinga techninė informacija, be to:

i) lauke "Subject" nurodyti sekančius įrašus, apibūdinančius asmenį (*vartotoją,* sertifikato turėtoją):
a) CN - asmens vardas(-ai), pavardė(-s) ir unikalus asmens identifikatorius - atskirti kableliais, lietuviškos raidės pateikiamos su diakritiniais ženklais, koduotėje Unicode, pvz:
CN=Ramūnas,Šablinskas,37102230096
b) Serial Number - unikalus asmens identifikatorius, vienareikšmiškai identifikuojantis asmenį (tam pačiam asmeniui visada suteikiamas tas pats kodas, skirtingų *CA* suteiktuose *sertifikatuose* šis kodas privalo būti vienodas) pvz:
Serial Number=37102230096

c) ID-MD5 - unikalus asmens identifikatorius, suformuotas nacionalinį asmens tapatybės kodą transformuojant MD5 algoritmu, aprašomu RFC1321 (šis įrašas leidžia, žinant asmens kodą, operatyviai patikrinti jo teisingumą, tačiau apsunkina šio kodo reikšmės nustatymą, jo iš anksto nežinant), pvz:

ID-MD5=E20F57ECB7AF05D2A2308C570E18EC9D

d) C - šalį identifikuojantis kodas - konstanta "LT" (žymi šalį, suteikusią asmeniui šią tapatybę- vardus, pavardes bei asmens kodą arba unikalų asmens identifikatorių), pvz: **C=LT**.

ii) lauke "Key usage" turėti reikšmę "Non-Repudiation(40)".

PKI.13 *CA* atsakomybė dėl netinkamos veiklos, kai *sertifikato vartotojai* patiria tiesioginius materialinius nuostolius, turėtų būti ne mažesnė, nei 100 000 EUR (vienas šimtas tūkstančių eurų). Tais atvejais, kai operacijų rizika viršyja šią sumą, *vartotojas* ir *SP* privalo sudaryti papildomą tarpusavio susitarimą dėl *sertifikato* panaudojimo tokiose operacijose.

6.3 *TSP* ir *Suderinamumo* reikalavimai

PKI.19 *TSP* teikia paslaugas/produktus, paremtus *PKI* technologijomis ir siūlo *Paslaugų Tiekėjams* šiomis paslaugomis/produktais naudotis:

- panaudojant standartines sistemines sąsajas, arba tarpusavio sutarimu kuriant specialiąsias sąsajas,
- panaudojant standartines paslaugų realizacijas arba kuriant/adaptuojant šias paslaugas pagal *SP* poreikius.

TSP ir *SP* sutaria dėl *TSP* teikiamų *PKI paslaugų* instaliavimo kainos, šių paslaugų kokybės parametrų ir paslaugų naudojimo sąlygų.

PKI.20 Teikiant *kvalifikuoto parašo paslaugas*, *TSP* privalo šių paslaugų teikimui panaudoti susijusius produktus, turinčius atitikties EAL4 užtikrinimo lygiui sertifikatą, bei deklaruoti paslaugų saugumo lygį (kai vertinimo objektas apibrėžiamas pagal rekomendaciją "CEN workshop agreement" CWA 14170"). Teikiant *kvalifikuoto parašo paslaugas*, *TSP* yra atsakingas už techninio sprendimo įgyvendinimo atitikimą Lietuvos Respublikos teisės aktams.

PKI.21 Teikiant *kvalifikuoto parašo paslaugas*, *TSP* turi užtikrinti, jog paslauga bus prieinama visiems *vartotojams*, turintiems SSCD, susietus su *kvalifikuotais sertifikatais*, sudarytais *CA*, kurie turi bent 10% *kvalifikuotų sertifikatų* rinkos Lietuvoje (su sąlyga, jog šie sertifikatai tenkina šiame dokumente apibrėžiamas rekomendacijas -žr. 6.2).

PKI.22 *TSP, SP* pageidavimu, turi užtikrinti *PKI paslaugų suderinamumą*, kai *SP* teikia paslaugas Europos Sąjungos piliečiams.

PKI.23 Keičiantis pasirašytais elektroniniais dokumentais yra rekomenduojama naudoti:

- kvalifikuotus elektroninius parašus,
- elektroninio parašo formatas apibrėžiamas Lietuvos standartu LST ETSI TS 101 903 "Patobulintieji XML elektroniniai parašai (XAdES)"; atskiru dokumentu (arba vėlesnėje šio dokumento redakcijoje) bus apibrėžtas šio standarto profilis, tinkamas naudoti keičiantis *pasirašytais e-dokumentais* tarp verslo įmonių, valstybės institucijų ir *vartotojų*, užtikrinant *PKI paslaugų suderinamumą*.

PKI.24 *TSP* privalo užtikrinti bet kokios gaunamos informacijos konfidencialumą ir visų atliekamų operacijų informacijos slaptumą.

6.4 *SP* Reikalavimai

PKI.30 Atvejais, kai *SP* ir *vartotojo* valdoma *pasirašymo įranga* dalyvauja *kvalifikuoto parašo paslaugų* procese, SP ir *vartotojas* privalo deklaruoti, jog ši įranga yra saugi (kai vertinimo objektas apibrėžiamas pagal "CEN workshop agreement" CWA 14170").

PKI.31 Atvejais, kai paslaugų teikimui yra būtina pasirašyti "*vartotojo* ir *SP*" sutartis, rekomenduojama nesieti sutarties su *SSCD* ar *sertifikatu*, o suteikti *vartotojui* laisvę rinktis tarp jo turimų *SSCD* įrenginių ir *sertifikatų*, bei laisvę tuos *SSCD* ir *sertifikatus* keisti (taikoma tik *kvalifikuotiems sertifikatams*).

PKI.32 Teikiant paslaugas, apimančias *kvalifikuotą elektroninį parašą*, rekomenduojama naudoti priemones, užtikrinančias sesijų saugumą ir įrangos sertifikatus, įspėjančius *vartotojus* dėl atakų prieš *paslaugų tiekėjų* elektroninę tapatybę. Rekomenduojama aktyviai mokyti *vartotojus* atpažinti atakas prieš *paslaugų tiekėjų* elektroninę tapatybę.