Parengė: E3P Darbo Grupė
Patvirtino: E3P Koordinacinis Komitetas – 2007-05-09
Rekomendacija E3P nariams, skelbiama www.parasas.lt

wPKI Specifikacija

1 Tikslas ir apimtis

Šis dokumentas aprašo *wPKI (bevielei viešojo rakto infrastruktūrai)* keliamus reikalavimus, siejamus su *kvalifikuotu parašu*.

2 Versijų istorija

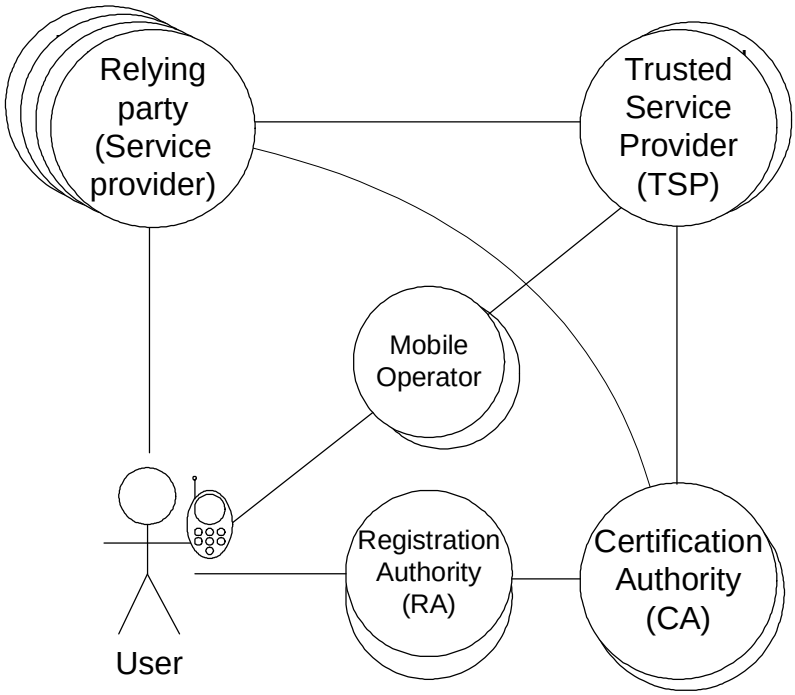
Versija 1.0 2006-11-01 Juodraštinė versija
Versija 1.2 2007-01-05 Revizija
Versija 1.3 2007-01-15 Revizija
Versija 1.4 2007-01-30 Terminų suvienodinimas
Versija 1.5 2007-03-16 Pataisymai pagal DG narių pastabas
Versija 1.6 2007-05-09 E3P Koordinacinio Komiteto tvirtinama redakcija

3 Terminai ir apibrėžimai

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

4 Įvadas (Informacinė dalis)

wPKI infrastruktūroje yra numatytos sekančios privalomos rolės*:



4.1 Funkcionalumo apžvalga

RA išduoda *SIM* su *SSCD* funkcija tiems asmenims, kurie nori naudotis *PKI paslaugomis* (detaliau žr. "PKI specifikacijos" dokumentą).
Paslaugų tiekėjai teikia paslaugas savo apibrėžiamais būdais - per specialias aplikacijas, internetu, mobiliuoju internetu ar balsu. *Autentifikacijos* ir *pasirašymo įranga wPKI* atveju yra mobilusis telefonas.

4.2 Konceptualus Aprašymas

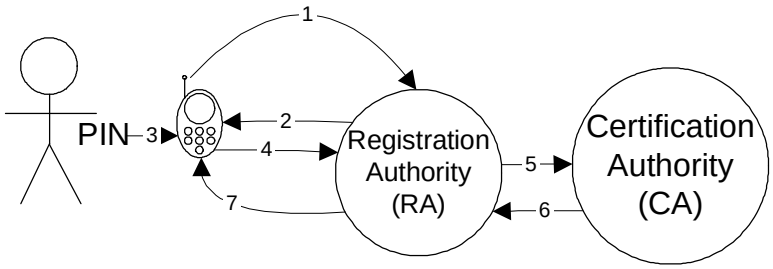
wPKI konceptualus aprašymas susideda iš 4 procesų: *SIM* išdavimo, sertifikato aktyvavimo, panaudojimo bei nutraukimo.
Visų šių procesų aprašymai yra informacinio pobūdžio, o ne privalomi.

4.2.1 *SIM* išdavimas

Šis procesas yra skirtas fiziniams asmenims suteikti saugaus elektroninio parašo formavimo priemones (*SSCD*) - taip, kad vėliau jas būtų galima panaudoti paslaugos aktyvavimo momentu:
1. RA nustato asmens tapatybę ir suteikia *SIM kortelę* vartotojui - GSM abonentui.
2. *SIM kortelę* ir abonento numerį atitinkantis *įrenginio sertifikatas* yra paskelbiamas aktyvuotu ir įrašomas į aktyvių *įrenginių sertifikatų* bazę, prieinamą visiems *TSP*.
3. Asmeniui perduodamas *kvalifikuoto sertifikato* aktyvavimo kodas (*privataus rakto*, atitinkančio *įrenginio sertifikatą*, aktyvavimo kodas).

4.2.2 Sertifikato aktyvavimas

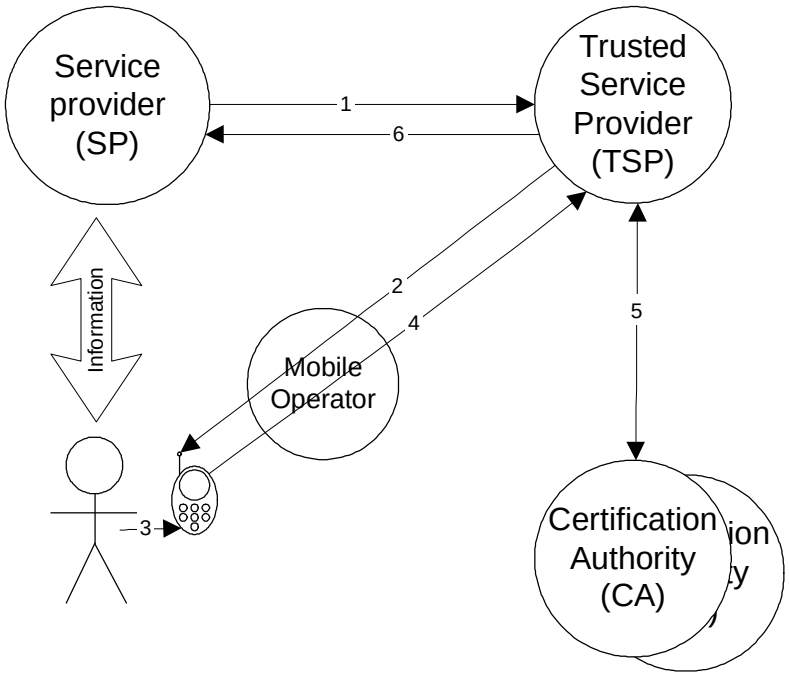
Sertifikato aktyvavimo proceso tikslas yra sukurti ir aktyvuoti *kvalifikuotą sertifikatą*.



1. *Vartotojas* kreipiasi į *RA* aktyvuoti sertifikatą (vartotojo sąsaja - mobili).
2. *RA* siunčia užklausą į *vartotojo* mobilųjį telefoną, prašančią patvirtinti asmens duomenis.
3. *Vartotojas* patikrina asmens duomenų teisingumą ir pasirašo duomenis, įvesdamas aktyvavimo/*pasirašymo kodą* (*sPIN*).
4. *RA* gauna pasirašytus asmens duomenis
5. *RA* prie *vartotojo* pasirašytų duomenų prideda *įrenginio sertifikatą*, telefono numerį ir persiunčia į *CA* užklausą aktyvuoti *kvalifikuotą sertifikatą*.
6. *CA* sukuria ir aktyvuoja *kvalifikuotą sertifikatą*.
7. *Vartotojas* mobiliuoju telefonu informuojamas apie registracijos baigtį, *vartotojui* suteikiama galimybė pasikeisti *sPIN*.

4.2.3 Panaudojimas

Panaudojimo schema aprašinėjama nuo momento, kai *Paslaugų Tiekėjas* (*SP*) iš *TSP* pareikalauja vienos iš elektroniniu parašu pagrįstos paslaugos (pvz., *vartotojo autentifikacijos* arba *duomenų pasirašymo*). Iki to momento, *vartotojas* su *Paslaugų Tiekėju* bendrauja bet kuriuo būdu - tiek akivaizdžiai, tiek elektroniniais informacijos apsikeitimo kanalais:



1. *Paslaugų tiekėjas* kreipiasi į *TSP* paslaugos, susijusios su e-parašo panaudojimu (parametras, nusakantis *vartotoją* - asmens kodas ir/ar GSM abonento numeris).
2. *TSP* suformuoja pasirašymo užklausą ir siunčia ją į *vartotojo* mobilųjį telefoną.
3. *Vartotojas* pasirašo užklausą, suvesdamas *pasirašymo kodą sPIN*.
4. *TSP* gauna *parašo duomenis* (kriptografinės funkcijos rezultatą).
5. *TSP* patikrina *parašo duomenų* teisingumą ir *kvalifikuoto sertifikato* galiojimą, esant reikalui, prideda papildomą informaciją (pvz., laiko žymą).
6. *Paslaugų tiekėjui* pateikiama su elektroniniu parašu susijusi paslauga.

4.2.4 Nutraukimas

Nutraukti elektroninio parašo paslaugų naudojimą (atšaukti *kvalifikuoto sertifikato* galiojimą) galima keletu būdų:
- *Vartotojui* įspėjus *RA*, kad nebenori naudotis šia paslauga,
- *Vartotoui* įspėjus *RA*, kad įranga yra prarasta ar sukompromituota,
- *kvalifikuotas sertifikatas* panaikinamas pasibaigus jo galiojimo laikui,
- *RA* arba *CA* gali nutraukti *kvalifikuoto sertifikato* galiojimą dėl *Vartotojo-CA* sutarties pažeidimų ar kitų įstatymuose numatytų atvejų.

Sertifikato atšaukimo atvejais:
1. *RA* praneša *CA* apie sertifikato nutraukimą, *CA* nutraukia sertifikato galiojimą, *CRL* sąrašas yra papildomas negaliojančiu sertifikatu.
2. *Įrenginio sertifikatas* yra paskelbiamas negaliojančiu (jei *SIM kortelė* negrįžtamai užblokuojama), šis sertifikatas yra išimamas iš aktyvių *įrenginių sertifikatų* bazės, prieinamos visiems *TSP*.

5 Produktai (Normatyvinė dalis)

Šiame skyriuje aprašomi būtinieji *wPKI produktai*, kuriuos privalo pateikti savo roles atliekantys dalyviai.

5.1 *RA* produktai, pateikiami į *CA*

Įrenginių sertifikatai visoms aktyvioms *SIM* kortelėms, šakniniai sertifikatai, kuriais pasirašyti *įrenginių sertifikatai*,
Vartotojo pasirašyta (*įrenginio sertifikatu*) asmeninė informacija,
Kvalifikuotų sertifikatų atšaukimo paslauga,
Priežiūros/palaikymo paslaugos.

5.2 *CA* produktai, pateikiami į *RA*

Vartotojų kvalifikuotų sertifikatų aktyvavimo paslauga,
Vartotojų kvalifikuotų sertifikatų atšaukimo paslauga,
Kvalifikuotų sertifikatų publikavimo paslauga.

5.3 *RA* produktai, pateikiami *Vartotojui*

Vartotojo identifikacija,
SIM kortelės su *wPKI* funkcionalumu,
Sutartis dėl *SSCD* ir *kvalifikuoto sertifikato* panaudojimo,
Vartotojų aptarnavimas/palaikymas,
Vartotojų apmokymas, instrukcijos ir informacinė medžiaga,
Kvalifikuotų sertifikatų aktyvavimas,
Kvalifikuotų sertifikatų atšaukimas.

5.4 *RA* produktai, pateikiami *TSP*

Įrenginių sertifikatai, bei juos atitinkantys mobiliųjų telefonų abonentų numeriai,
Aktyvūs *kvalifikuoti sertifikatai* ir juos atitinkantys asmens duomenys (prieiga prie duomenų, surišančių aktyvius pasirašymo įrenginius su telefonų numeriais ir *kvalifikuotais sertifikatais*).

5.5 *TSP* produktai, pateikiami *Paslaugų Tiekėjams SP*

Sutartys dėl identifikavimo ir pasirašymo paslaugų, pagrįstų *elektroniniu parašu*, pardavimo,
Pasijungimas prie *wPKI* infrastruktūros,
Sistemų palaikymas, monitoringas, problemų sprendimas.

5.6 Mobiliojo Operatoriaus produktai, pateikiami TSP

Sutartis dėl *wPKI* panaudojimo,
Prieiga prie *wPKI* (mobiliojo operatoriaus platformos, bendraujančios su SIM kortelėmis).

6 Pagrindiniai Techniniai Reikalavimai (Normatyvinė dalis)

Šis skyrius nusako pagrindinius reikalavimus, keliamus *wPKI* infrastruktūrai.

6.1 Bendrieji reikalavimai

TR.1 *SIM kortelės*, naudojamos elektroninio parašo projektuose, privalo būti gaminamos laikantis specialių saugumo reikalavimų ir turi atitikti saugumo profilį, apibrėžtą "CEN workshop agreement" CWA 14169, kai vertinimo patikimumas pagal standartą "Common criteria - security" (ISO/IEC 15408) privalo atitikti EAL4+ patikimumo lygį. *SIM kortelių* gamintojas pagal *CA* pareikalavimą privalo pateikti saugumo ir vertinimo patikimumo atitikties sertifikatą konkrečiam *SIM* produktui.

TR.2 *wPKI* yra paremta *SIM* kortele, kuri turi savyje dvi asimetrinių kodavimo raktų poras **Key-S** (taikymams, nesukeliantiems juridinių implikacijų) ir **Key-N** (taikymams, potencialiai sukuriantiems juridines implikacijas) ir sekančias kriptografines funkcijas/primityvus:

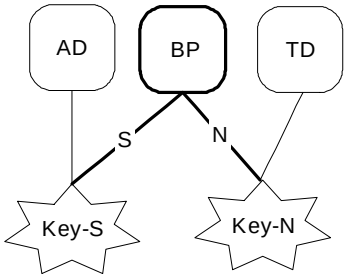
i) binarinės informacijos užkodavimo/pasirašymo funkciją (BP), galinčią panaudoti du skirtingus privačiuosius raktus (ši funkcija panaudojama *autentifikacijos* ir *pasirašymo* taikymuose),

ii) užkoduoto teksto dekodavimo funkciją (TD), susietą su vienu *privačiuoju raktu* (ši funkcija panaudojama slaptos tekstinės informacijos perdavimui iš *Paslaugų tiekėjo vartotojui* tokiu būdu, kad tą informaciją galėtų perskaityti tik *vartotojas*),

iii) asimetrinio binarinės informacijos dekodavimo funkciją (AD), susietą su vienu privačiuoju raktu (ši funkcija panaudojama slaptos vartotojo informacijos apsaugojimui išorinėse sitemose).

TR.3 Kriptografinis raktas Key-N privalo būti apsaugotas "pasirašymo PIN kodu" - *sPIN* (*vartotojas* prašomas šį kodą įvesti prieš kiekvieną Key-N panaudojimą), sudarytu iš 4-8 skaitmenų. Neteisingai panaudojus kodą 5 kartus, jis privalo būti blokuojamas.

Žemiau pavaizduotas kriptografijos funkcijų/primityvų susiejimas su raktų Key-S ir Key-N poromis:



TR.4 Prieiga prie BP funkcijos ir rakto Key-N panaudojimo, turi būti užtikrinta **tik tokiems TSP, kurie teikia *kvalifikuoto parašo* paslaugas** (t.y. deklaruoja savo pasirašymo produkto saugumą, pagal saugumo profilyje "CEN workshop agreement" CWA 14170 pateikiamą aprašymą). Šis apribojimas yra papildoma vartotojų apsaugos priemonė.

6.2 *SIM* išdavimo ir *kvalifikuoto sertifikato* aktyvavimo reikalavimai

TR.12 *Vartotojui kvalifikuoto sertifikato* "aktyvavimo kodas" privalo būti pateikiamas asmeniškai ir tik:

- nustačius asmens tapatybę,
- patikrinus pateikto asmens tapatybės dokumento galiojimo faktą,
- kai *vartotojas* susipažįsta ir pasirašo ant taisyklių, reglamentuojančių šio kodo panaudojimą.

TR.15 Vartotojui privalo būti suteikta galimybė nustatyti privataus rakto Key-N, atitinkančio *kvalifikuotą sertifikatą*, pasirašymo kodą *sPIN* prieš arba po *kvalifikuoto sertifikato* aktyvavimo procedūros. Turi būti numatyta galimybė *vartotojams* saugiai bet kuriuo metu šį kodą pasikeisti į norimą skaičių kombinaciją.

6.3 Reikalavimai paslaugų panaudojimui ir nutraukimui

TR.20 Mobilieji operatoriai privalo sudaryti sutartis ir pateikti prieigą prie *wPKI* visiems *TSP*, tenkinantiems TR.4.

TR.24 Mobilieji Operatoriai privalo nedelsiant informuoti *CA* apie *įrenginių sertifikatus*, kurie paskelbiami negaliojantčiais arba jų galiojimas sustabdomas (atvejais, kai šiems įrenginiams buvo sukurti *kvalifikuoti sertifikatai*).

TR.25 *RA* gavus užklausą sertifikato atšaukimui, yra atliekami šie veiksmai:

- *CA* informuojamas apie *kvalifikuoto sertifikato* galiojimo nutraukimą,
- Tais atvejais, kai panaikinamas *įrenginio sertifikatas*, *RA* privalo nutraukti kontraktinius santykius tarp *CA* ir mobiliojo operatoriaus, atitinkančius konkretų pasirašymo įrenginį (esant reikalui, su *vartotoju* turi būti sudaroma nauja sutartis naujam pasirašymo įrenginiui).