(19) LIETUVOS RESPUBLIKA
VALSTYBINIS PATENTŲ BIURAS
V P B

(10) **LT 5320 B**

(12) **PATENTO APRAŠYMAS**

(11) Patento numeris: **5320**

(51) Int. Cl. (2006): **H04L 9/32**

(21) Paraiškos numeris: **2004 053**

(22) Paraiškos padavimo data: **2004 05 24**

(41) Paraiškos paskelbimo data: **2005 11 25**

(45) Patento paskelbimo data: **2006 03 27**

(62) Paraiškos, iš kurios dokumentas išskirtas, numeris: —

(86) Tarptautinės paraiškos numeris: —

(86) Tarptautinės paraiškos padavimo data: —

(85) Nacionalinio PCT lygio procedūros pradžios data: —

(30) Prioritetas: —

(72) Išradėjas:

Ramūnas ŠABLINSKAS, LT

(73) Patento savininkas:

Uždaroji akcinė bendrovė „OMNITEL“, Ševčenkos g. 25, LT-03229 Vilnius, LT

(74) Patentinis patikėtinis:

Aušra PAKĖNIENĖ, AAA Baltic Service Company, Jasinskio g. 16B, Biurų centras Victoria, LT-01112 Vilnius, LT

LT 5320 B

(54) Pavadinimas:

Elektroninio dokumentų pasirašymo kvalifikuotu elektroniniu parašu sistema

(57) Referatas:

Išradimas susijęs su tolimojo ryšio sistemomis ir būdais, konkrečiai su mobiliųjų telefonų panaudojimu elektroninio parašo infrastruktūrose. Aprašoma sistema leidžia elektroniniu būdu pasirašyti kvalifikuotu elektroniniu parašu bet kokią kompiuterinę bylą, panaudojant mobilųjį telefoną (kaip SMART tipo kortelių skaitytuvą) ir jame esančią GSM SIM kortelę (kuri yra SMART tipo kortelė) kaip elektroninio parašo infrastruktūros dalį. Pasiūlyti būdai leidžia nesaugiose aplinkose (internete, panaudojant elektroninį paštą kaip transportą) formuoti elektroninio parašo duomenis ir išsprendžia daugialypės terpės duomenų atvaizdavimo mobiliajame telefone problemą. Iš vartotojo pusės sistema nereikalauja vartotojo personaliniame kompiuteryje įdiegti jokios techninės ar programinės įrangos. Elektroninio parašo suformavimas atliekamas vartotojui persiunčiant pasirašomą dokumentą tam tikru elektroninio pašto adresu - tam yra panaudojama vartotojui įprasta elektroninio pašto programinė įranga. Naudojimosi prasme sistema yra mažiau patogi, nei įprastinės elektroninio parašo infrastruktūros, todėl ši sistema įprastinių infrastruktūrų nepakeičia, o yra pritaikoma retam arba neprofesionaliam vartojimui.

Išradimas susijęs su tolimojo ryšio sistemomis ir būdais, konkrečiai su mobiliųjų telefonų panaudojimu elektroninio parašo infrastruktūrose.

Technikos lygiu žinomos sistemos ir būdai elektroniniams parašams patvirtinti (WO 03/007133). Taip pat žinomas elektroninių parašų generavimo ir (arba) patvirtinimo būdas, kai generuojama asimetrinių raktų pora, kurią sudaro privatusis parašo raktas ir viešasis patvirtinimo raktas (WO 2004/028076).

Taigi, Mobiliosios Identifikacijos (MI) sistemos, apimančios privataus ir viešojo raktų infrastruktūras (Public Key Infrastructure - PKI) pasaulyje yra žinomos ir turi standartizuotą prieigą (pvz.: Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface, ETSI TS 102 204, v1.1.4, Technical Specification. 650 Route des Lucioles, F-06921 Sophia Antipolis Cedex – France, 2003). Šios infrastruktūros pasaulyje yra naudojamos pasirašyti paprastiems neformatuotiems tekstiniams pranešimams.

Standartiniai dokumentų pasirašymo procesai, kurie vyksta pasirašant (nebūtinai elektroninius) dokumentus yra:

i) Sukuriamas pasirašomas turinys – tai gali būti bet kokio formato ar apimties kompiuterinė byla,
ii) Pasirašomas turinys pristatomas signatarui,
iii) Signataras peržiūri ir įvertina pasirašomą turinį,
iv) Signataras pasirašo turinį – suformuojami elektroninio parašo duomenys konkrečiam turiniui,
v) Signataras perduoda pasirašytą turinį tretiesiems asmenims naudojimui, arba pasirašytas turinys yra archyvuojamas ilgalaikiam saugojimui.

Taikant MI infrastruktūras, iškyla tokios problemos:

1. Integracijos problema, kylanti iš PKI infrastruktūrų tiekėjų siekio sukurti visiškai saugias aplinkas, kuriose elektroninio pasirašymo veiksmo (iv) nebūtų įmanoma suklastoti.
2. Turinio atvaizdavimo problema. Vykdant procesą (iii), pagal ES elektroninio parašo direktyvą, vartotojas turi matyti tai, ką pasirašo, o mobilusis įrenginys nėra pritaikytas įvairialypio turinio atvaizdavimui arba interpretavimui.

Siūloma elektroninio dokumentų pasirašymo kvalifikuotu elektroniniu parašu sistema išsprendžia abi nurodytas problemas.

Siūlomas elektroninio dokumentų pasirašymo kvalifikuotu elektroniniu parašu būdas, apimantis elektroninio parašo duomenų formavimą, naudojant mobiliąją infrastruktūrą kaip privataus ir viešojo raktų infrastruktūros dalį, naujas tuo, kad papildomai formuojama dokumento elektroninio pasirašymo paslauga (DEP), ir būdas apima šiuos etapus:

- vartotojas-iniciatorius siunčia elektroninio pašto žinutę su prisegta bet kokio formato kompiuterine byla specialiu DEP adresu, kuriame nurodomas vartotojas-signataras, DEP adreso formatas gali būti toks: *<Asmens-kodas>@signature.lt*, kur <Asmens-kodas> yra signataro asmens kodas;
- DEP operatorius patikrina, ar vartotojas-signataras turi galiojantį sertifikatą, ir inicijuoja pasirašymo procedūrą, kurios metu sukuriami elektroninio parašo duomenys, vartotojui-signatarui panaudojus GSM SIM kortelę su privačiuoju raktu, kuris aktyvuojamas PIN kodu;
- DEP operatorius surenka elektroninio parašo duomenis į vieną dokumentą ir gautą pasirašytą dokumentą persiunčia į vartotojo-signataro elektroninio pašto dėžutę;
- vartotojas-signataras, gavęs pasirašytą dokumentą, peržiūri ir įvertina jo turinį savo kompiuteryje;
- jei pasirašyto dokumento turinys nepažeistas ir elektroninis parašas šį turinį atitinka, vartotojas-signataras dokumentą perduoda tretiesiems asmenims naudojimui arba archyvuoja ilgalaikiam saugojimui;
- jei pasirašyto dokumento turinys pažeistas ir/arba elektroninis parašas šio turinio neatitinka, vartotojas-signataras dokumentą sunaikina.

Siūlomas kvalifikuotu elektroniniu parašu pasirašyto dokumento peržiūros būdas, apimantis mobiliąją infrastruktūrą kaip privataus ir viešojo raktų infrastruktūros dalį, naujas tuo, kad papildomai formuojama pasirašyto dokumento patvirtinimo paslauga (PDP), o būdas apima šiuos etapus:

- vartotojas-iniciatorius siunčia elektroninio pašto žinutę su prisegtu pasirašytu dokumentu specialiu PDP adresu, PDP adreso formatas gali būti toks: *validate@signature.lt*,
- PDP operatorius tikrina, ar dokumentas nebuvo neteisėtai modifikuotas ir ar visų signatarų elektroniniai parašai yra galiojantys,
- jei patikrinimo rezultatas sėkmingas, PDP operatorius persiunčia vartotojui-iniciatoriui originalią kompiuterinę bylą, bei duomenis apie ją pasirašiusius signatarus,
- jei dokumento turinys buvo pakeistas ir/arba signatarų parašai nėra galiojantys, vartotojas-iniciatorius gauna elektroninio pašto žinutę apie klaidą.

Išradimas iliustruojamas brėžiniais, kuriuose pavaizduota:

Fig. 1 - Mobiliosios Elektroninio Parašo infrastruktūros panaudojimo schema (analogas);

Fig. 2 - Dokumentų Elektroninio Pasirašymo paslaugos mechanizmo veikimas;

Fig. 3 - Pasirašyto Dokumento Patvirtinimo paslaugos mechanizmo veikimas.

Geresniam išradimo esmės ir jo privalumų supratimui nauja elektroninio dokumentų pasirašymo kvalifikuotu elektroniniu parašu sistemos veikimas aprašomas su nuorodomis į pateiktus brėžinius.

Mobiliosios Identifikacijos sistemų bendroji schema

Mobiliosios Identifikacijos (MI) arba Mobilioji *Elektroninio Parašo* (EP) infrastruktūra yra sukuriama, į GSM SIM korteles įdiegiant privačiuosius vartotojų raktus, bei juos užregistruojant sertifikatų centre. Nuo sertifikatų centro atestacijos priklauso, ar tokios infrastruktūros pagalba sukurtas elektroninis parašas bus kvalifikuotas ar ne. Operatoriaus pusėje instaliuojama įranga, suteikianti paslaugų tiekėjams prieigą prie mobiliosios EP infrastruktūros. Vartotojams mobiliuoju telefonu pateikiama patogi, lengvai suprantama ir intuityvi dialogo formos sąsaja, kurios nereikia specialiai mokytis.

Vartotojai, prieš pasinaudodami MI paslaugomis, privalo apsilankyti sertifikatų centro atstovybėje ir gauti savo asmens duomenų įregistravimo sertifikatą, t.y. pateikti asmens duomenis, kurie yra susiejami su elektroninio parašo formavimo duomenimis – privataus ir viešojo rakto pora. Sertifikatų centras vartotojui išduoda specialią GSM SIM kortelę

(joje saugomas privatusis raktas), bei privataus rakto aktyvavimo PIN kodą, kurį vartotojas privalo saugoti ir kuris naudojamas visoms elektroninio pasirašymo operacijoms įvykdyti. Viešasis raktas, atitinkantis privatųjį yra saugomas sertifikatų centre ir vėliau yra viešai naudojamas elektroninio parašo duomenų teisingumui patikrinti.

Įprastinė EP infrastruktūros panaudojimo schema (žr. Fig. 1): vartotojas inicijuoja užklausą paslaugų tiekėjui elektroniniu kanalu (1), paslaugų tiekėjas suformuoja dokumentą, kuris adresuojamas vartotojui (2) ir perduodamas pasirašymui į jo asmeninį mobilųjį telefoną (3) per identifikacijos paslaugų tiekėją. Vartotojas pasirašo užklausą, įvesdamas pasirašymo PIN kodą (4), o paslaugų tiekėjas, gavęs pasirašytą dokumentą (5), patikrina parašo teisingumą ir suteikia paslaugą vartotojui (6).

Didžiausias iššūkis verslui, norinčiam sukurti atsiperkančią EP infrastruktūrą yra – sukurti paslaugą(-as), kurios panaudojimas būtų pakankamai paprastas ir pakankamai fundamentalus, t.y. toks, kad ją būtų galima naudoti kuo įvairesniuose taikymuose. Mūsų atveju pasirinkta sekanti paslauga: "Elektroniniu paštu siunčiamos bet kokio formato kompiuterinės bylos pasirašymas".

Elektroninis paštas yra plačiai paplitusi paslauga, ja naudojasi didžioji interneto vartotojų dalis, elektroninio pašto mobilioji atmaina (SMS žinutės) yra intensyviai naudojama GSM vartotojų tarpe, todėl tikimasi, kad elektroninio pašto sąsaja tiek vartotojams tiek sąveikaujančioms paslaugų tiekėjų sistemoms bus priimtiniausia. Patrauklu ir tai, kad vartotojams į savo personalinius kompiuterius nereikia instaliuoti papildomos programinės įrangos, bei turėti pastovaus internetinio ryšio.

Tam, kad vartotojams nereikėtų rūpintis papildomais įrankiais, yra pateikiamos dvi paslaugos:

- Dokumento Elektroninio Pasirašymo paslauga (**DEP**),
- Pasirašyto Dokumento Patvirtinimo arba perskaitymo paslauga (**PDP**).

Dokumentų elektroninio pasirašymo paslauga (DEP) yra skirta sukurti elektroniniu parašu patvirtintam dokumentui. Įėjimo parametras – bet kokia kompiuterinė byla, išėjimo parametras – pasirašytas dokumentas. Bet kuris elektroninio pašto vartotojas gali inicijuoti pasirašyto dokumento sukūrimą, tačiau elektroniniu parašu patvirtinti konkretų dokumentą gali tik asmuo, turintis mobiliojo EP infrastruktūrą (t.y. turintis galiojantį sertifikatą).

Fig. 2 pateikiamas pasirašymo mechanizmas, kuris iš esmės atitinka *Standartinę dokumentų pasirašymo procesų* schemą, tačiau joje procesai (iii) ir (iv) yra sukeisti vietomis:

1. Vartotojas-iniciatorius siunčia e-pašto žinutę su prisegta bet kokio formato kompiuterine byla specialiu DEP adresu, kuriame nurodamas vartotojas-signataras, adreso formatas: ***<Asmens-kodas>@signature.lt***, kur <Asmens-kodas> yra signataro asmens kodas, pvz.: 37102230096@signature.lt
2. DEP operatorius patikrina, ar vartotojas-signataras turi galiojantį sertifikatą, tinkamą kvalifikuotam elektroniniam parašui sukurti ir inicijuoja pasirašymo procedūrą, kurios metu sukuriami elektroninio parašo duomenys. Šie elektroninio parašo duomenys gali būti sugeneruoti tik panaudojus GSM SIM kortelę, kurią vartotojas gavo sertifikatų centro atstovybėje ir kurioje yra saugomas slaptas privatusis raktas, aktyvuojamas PIN kodu, kurį žino tik signataras.
3. DEP operatorius surenka elektroninio parašo duomenis į vieną dokumentą ir gautą pasirašytą dokumentą persiunčia į signataro elektroninio pašto dėžutę.
4. Signataras, gavęs pasirašytą dokumentą, peržiūri ir įvertina jo turinį savo kompiuteryje.
5. Tuo atveju, jei pasirašyto dokumento turinys yra nepažeistas ir elektroninis parašas šį turinį atitinka, dokumentas yra perduodamas tretiesiems asmenims naudojimui, arba archyvuojamas ilgalaikiam saugojimui.

Sėkmės atveju, elektroniniu vartotojo-signataro parašu patvirtintas dokumentas, atitinka standartą (XML Advanced Electronic Signatures (XAdES), ETSI TS 101 903, v1.1.1, Technical Specification. 650 Route des Lucioles, F-06921 Sophia Antipolis Cedex – France, 2002), šis dokumentas turi tokią pat juridinę galią, kaip ir ranka pasirašytas dokumentas. Vieną dokumentą gali pasirašyti neribotas signatarų skaičius.

Jei dokumento pasirašyti nepavyksta (signataras nepatvirtina dokumento, įvesdamas savo PIN kodą), vartotojas-iniciatorius informuojamas apie nesėkmę e-pašto žinute.

Tais atvejais, kai pasirašomo dokumento turinys yra neformatuotas tekstas, atvaizduojamas mobiliojo telefono ekrane, 5-tasis žingsnis įvykdomas automatiškai.

Pasirašyto Dokumento Patvirtinimo paslauga

Vartotojas, turintis elektroniniu parašu patvirtintą dokumentą negali peržiūrėti jo turinio be specialios programinės įrangos, kadangi pasirašytas dokumentas apima ne tik originalius duomenis, bet ir elektroninio parašo (keleto parašų) duomenis. Vartotojas gali nemokamai parsisiųsti iš interneto ir įdiegti savo kompiuteryje programinę įrangą, sugebančią perskaityti pasirašytus dokumentus. Siekiant vartotojo nesusaistyti tokiais reikalavimais, kaip programinės įrangos instaliavimas, yra sukurta elektroniniu paštu iškviečiama paslauga, atskleidžianti pasirašyto dokumento turinį ir patikrinantį signataro (-ų) elektroninio parašo galiojimą (PDP).

Pasirašyto dokumento patvirtinimo paslaugos įėjimo parametras – pasirašytas dokumentas, atitinkantis standartą (XML Advanced Electronic Signatures (XAdES), ETSI TS 101 903, v1.1.1, Technical Specification. 650 Route des Lucioles, F-06921 Sophia Antipolis Cedex – France, 2002), išėjimo parametras – originali kompiuterinė byla, bei informacija apie dokumentą pasirašiusius signatarus. Bet kuris elektroninio pašto vartotojas gali inicijuoti pasirašyto dokumento patvirtinimo paslaugą.

Fig. 3 yra pateiktas patvirtinimo paslaugos mechanizmo veikimas:

1. Vartotojas siunčia e-pašto žinutę (1) su prisegtu pasirašytu dokumentu specialiu PDP paslaugos adresu: ***validate@signature.lt***.
2. Pasirašyto Dokumento Patvirtinimo operatorius patikrina, ar dokumentas nebuvo neteisėtai modifikuotas ir ar visų signatarų elektroniniai parašai yra galiojantys. Tuo atveju, jei patikrinimo rezultatas yra sėkmingas, PDP operatorius persiunčia vartotojui originalią kompiuterinę bylą, bei duomenis apie ją pasirašiusius signatarus. Jei dokumento turinys buvo pakeistas, arba signatarų parašai nėra galiojantys, vartotojas gauna e-pašto žinutę apie klaidą.

Schemoje nedalyvauja GSM telefonai ar kita įranga, susijusi su signataru, todėl ja be apribojimų gali naudotis bet kuris elektroninio pašto vartotojas.

MI problemų sprendimas: Integracijos problema

Integracijos problema, kyla iš PKI infrastruktūrų tiekėjų siekio sukurti visiškai saugias aplinkas, kuriose elektroninio pasirašymo veiksmo nebūtų įmanoma suklastoti. Standartinėse fiksuoto PKI schemose kompiuterinių aplinkų saugumas yra pasiekiamas specialiomis programinėmis priemonėmis. Galutiniai vartotojai šias programines priemones privalo įdiegti savo kompiuteriuose ir suprasti bent pagrindinius šių priemonių veikimo principus. Paslaugų Tiekėjai privalo įdiegti ištisas posistemes, palaikančias PKI infrastruktūros veikimą ir užtikrinančias sistemų saugumą. Praktika parodė, kad šie reikalavimai tiek galutiniams vartotojams, tiek paslaugų tiekėjams yra praktiškai neįgyvendinami dėl sistemų sudėtingumo, daugelyje pasaulio šalių pradėtos diegti PKI infrastruktūros neturėjo didelio pasisekimo būtent dėl integracijos problemos.

ES direktyva nurodo, kad elektroninis parašas turi būti prilygintas ranka sukurtam parašui, bet nekelia papildomų reikalavimų parašo suklastojimo galimybėms. Ši aplinkybė leido Dokumentų Elektroninio Pasirašymo paslaugoje atsisakyti neefektyvių "saugių" aplinkų ir naudotis nesaugiomis aplinkomis, tokiomis kaip elektroninis paštas. Kadangi elektroniniu paštu naudojasi daugelis interneto vartotojų ir paslaugų teikimo sistemų, sistemų integracijos problema yra panaikinama. Nei galutiniams vartotojams savo kompiuteriuose, nei Paslaugų Tiekėjams savo informacinėse sistemose nereikia instaliuoti papildomos programinės įrangos ir suprasti šios įrangos veikimo principų.

MI problemų sprendimas: Turinio atvaizdavimo problema

Turinio atvaizdavimo mobiliajame telefone problema negali būti išspręsta technologinėmis priemonėmis, kadangi elektroninio parašo technologija negali kelti jokių reikalavimų pasirašomam turiniui – tai gali būti tiek tekstas, tiek grafinė informacija, tiek video informacija tiek formatuoti daugialypės terpės dokumentai. Tuo tarpu tik neformatuota tekstinė informacija gali būti daugiau ar mažiau sėkmingai atvaizduota mobiliojo telefono ekrane. Bet kokia kita informacija telefono ekrane negali būti atvaizduota dėl daugelio priežasčių, tarp kurių: maža telefono ekrano skiriamoji geba,

mažas telefono aparato atminties kiekis, nedidelė telefono aparato procesoriaus greitaveika ir pan.

Signataras, pagal ES elektroninio parašo direktyvą, turi matyti pasirašomo dokumento turinį. Kadangi ši sąlyga mobiliuosiuose telefonuose negali būti įvykdyta, mūsų aprašomoje sistemoje šis reikalavimas išsprendžiamas kitomis priemonėmis: signataras mobiliuoju telefonu tik pasirašo dokumento turinį, ir jau pasirašytą dokumentą gauna į jam vienam prieinamą elektroninio pašto dėžutę. Gavęs savo pasirašytą dokumentą, signataras privalo peržiūrėti jo turinį personaliniame kompiuteryje, prieš perduodant jį tretiesiems asmenims, ar atiduodant saugojimui į archyvą. Atveju, kai dokumento turinys neatitinka signataro lūkesčių, jis paprasčiausiai yra sunaikinamas paties signataro, šį dokumentą ištrinant.

MI saugumo klausimai

Nesaugios aplinkos panaudojimas DEP ir PDV paslaugose padidina elektroninio parašo suklastojimo galimybes: elektroninio pašto žinutė piktavalių vartotojų gali būti perimta bei pasirašomo dokumento turinys pakeistas/modifikuotas, prieš perduodant jį signatarui pasirašyti. Tokios klastojimo galimybės atsiranda tada, kai vartotojo kompiuteris arba prie šio kompiuterio pajungtas duomenų apsikeitimo tinklas, yra pažeidžiami. Pasirašymo procedūra yra vykdoma taip, kad signataras visada gali nustatyti, jog jo parašas yra suklastotas (t.y. buvo pasirašytas ne autentiškas dokumentas). Tačiau tik pasirašymo procedūros prisilaikymas garantuoja, jog signataras tretiesiems asmenims perduos autentišką pasirašytą dokumentą. Procedūrų nesilaikymas padidina elektroninio parašo suklastojimo riziką, ir tik nuo paties signataro priklauso aprašomos sistemos saugumas.

Jei signataras įtaria, kad įvyko pasikėsinimas suklastoti jo parašą konkrečiam turiniui, jis privalo apie tai pranešti teisėtvarkos institucijoms, kurios turi nustatyti kompiuterinių sistemų įsilaužėlius.

DEP ir PDP paslaugų saugumo lygį galima pakelti tuo atveju, kai naudojamos patikimos elektroninio pašto sistemos – saugios korporatyvinės sistemos ir saugios jungtys tarp Paslaugų Tiekėjų informacinių sistemų, bei DEP paslaugos sistemos. Tokiais atvejais signatarams nėra būtina papildomai tikrinti pasirašytų dokumentų autentiškumo. PDP paslaugos saugumo lygį galima pakelti vartotojams persiunčiant pasirašytus ir

standartinėmis elektroninio pašto priemonėmis (pvz. S-MIME) perskaitomus atsakymus, tačiau tai iškelia papildomus reikalavimus vartotojo elektroninio pašto programinei įrangai.

Unikalios sistemos savybės

Iki šiol visos elektroninio parašo formavimo sistemos dirbdavo tik saugiose aplinkose, kurios garantuodavo pasirašomų duomenų saugumą. Aukščiau aprašytoji sistema unikali tuo, kad ji formuoja elektroninio parašo duomenis nesaugioje aplinkoje, perduodant pasirašomą dokumentą elektroniniu paštu į Dokumentų Elektroninio Pasirašymo sistemą. Siekiant užtikrinti elektroninio parašo nepadirbamumą, yra pakeičiama standartinė dokumentų pasirašymo procesų seka – signataras pirmiausia dokumentą mobiliuoju telefonu pasirašo, o tik vėliau jį perskaito savo kompiuteryje. Tik įsitikinęs, jog yra pasirašytas autentiškas dokumentas, signataras jį perduoda tretiesiems asmenims. Taip išsprendžiama dar viena problema, susijusi su pasirašomo dokumento turinio atvaizdavimu mobiliajame telefone.

Sistema taip pat unikali tuo, kad vartotojui, norinčiam elektroniniu būdu pasirašyti bet kokio formato kompiuterinę bylą, nereikia savo kompiuteryje instaliuoti jokios papildomos programinės įrangos bei išmokti ja naudotis. Ši sąlyga iki šiol buvo pagrindinė kliūtis sėkmingai elektroninio parašo infrastruktūrų plėtrai daugelyje pasaulio valstybių. Siūloma sistema dėl savo nepatogumo (reikalavimo signatarui įsitikinti pasirašyto dokumento autentiškumu) nepakeičia įprastinių elektroninio parašo infrastruktūrų, skirtų profesionaliam naudojimui. Ji yra orientuota į vartotojus, kurie pasirašinėja dokumentus labai retai ir dėl šios priežasties nenori rūpintis sudėtingų programų įdiegimu savo personaliniuose kompiuteriuose.

Aprašoma sistema leidžia elektroniniu būdu pasirašyti kvalifikuotu elektroniniu parašu bet kokią kompiuterinę bylą, panaudojant mobilųjį telefoną (kaip SMART tipo kortelių skaitytuvą) ir jame esančią GSM SIM kortelę (kuri yra SMART tipo kortelė) kaip elektroninio parašo infrastruktūros dalį.

Pasiūlyti būdai leidžia nesaugiose aplinkose (internete, panaudojant elektroninį paštą kaip transportą) formuoti elektroninio parašo duomenis ir išsprendžia daugialypės terpės duomenų atvaizdavimo mobiliajame telefone problemą.

Iš vartotojo pusės sistema nereikalauja vartotojo personaliniame kompiuteryje įdiegti jokios techninės ar programinės įrangos. Elektroninio parašo suformavimas atliekamas vartotojui persiunčiant pasirašomą dokumentą tam tikru elektroninio pašto adresu - tam yra panaudojama vartotojui įprasta elektroninio pašto programinė įranga. Naudojimosi prasme sistema yra mažiau patogi, nei įprastinės elektroninio parašo infrastruktūros, todėl ši sistema įprastinių infrastruktūrų nepakeičia, o yra pritaikoma retam arba neprofesionaliam vartojimui.

Išradimo apibrėžtis

1. Elektroninio dokumentų pasirašymo kvalifikuotu elektroniniu parašu būdas, apimantis elektroninio parašo duomenų formavimą, naudojant mobiliąją infrastruktūrą kaip privataus ir viešojo raktų infrastruktūros dalį, besiskiriantis tuo, kad papildomai formuoja dokumento elektroninio pasirašymo paslaugą (DEP), o būdas apima šiuos etapus:

- vartotojas-iniciatorius siunčia elektroninio pašto žinutę su prisegta bet kokio formato kompiuterine byla specialiu DEP adresu, kuriame nurodamas vartotojas-signataras,
- DEP operatorius patikrina, ar vartotojas-signataras turi galiojantį sertifikatą, ir inicijuoja pasirašymo procedūrą, kurios metu sukuriami elektroninio parašo duomenys, vartotojui-signatarui panaudojus GSM SIM kortelę su privačiuoju raktu, kuris aktyvuojamas PIN kodu,
- DEP operatorius surenka elektroninio parašo duomenis į vieną dokumentą ir gautą pasirašytą dokumentą persiunčia į vartotojo-signataro elektroninio pašto dėžutę,
- vartotojas-signataras, gavęs pasirašytą dokumentą, peržiūri ir įvertina jo turinį savo kompiuteryje,
- jei pasirašyto dokumento turinys nepažeistas ir elektroninis parašas šį turinį atitinka, vartotojas-signataras dokumentą perduoda tretiesiems asmenims naudojimui arba archyvuoja ilgalaikiam saugojimui,
- jei pasirašyto dokumento turinys pažeistas ir/arba elektroninis parašas šio turinio neatitinka, vartotojas-signataras dokumentą sunaikina.

2. Būdas pagal 1 punktą, besiskiriantis tuo, kad DEP adreso formatas: *<Asmens-kodas>@signature.lt*, kur <Asmens-kodas> yra signataro asmens kodas.

3. Kvalifikuotu elektroniniu parašu pasirašyto dokumento peržiūros būdas, apimantis mobiliąją infrastruktūrą kaip viešojo ir privataus raktų infrastruktūros dalį.

besiskiriantis tuo, kad papildomai formuoja pasirašyto dokumento patvirtinimo paslaugą (PDP), o būdas apima šiuos etapus:

- vartotojas-iniciatorius siunčia elektroninio pašto žinutę su prisegtu pasirašytu dokumentu specialiu PDP adresu,
- PDP operatorius tikrina, ar dokumentas nebuvo neteisėtai modifikuotas ir ar visų signatarų elektroniniai parašai yra galiojantys,
- jei patikrinimo rezultatas sėkmingas, PDP operatorius persiunčia vartotojui-iniciatoriui originalią kompiuterinę bylą, bei duomenis apie ją pasirašiusius signatarus,
- jei dokumento turinys buvo pakeistas arba signatarų parašai nėra galiojantys, vartotojas-iniciatorius gauna elektroninio pašto žinutę apie klaidą.

4. Būdas pagal 3 punktą, besiskiriantis tuo, kad pasirašyto dokumento patvirtinimo paslaugą (DPP) iškviečia elektroniniu paštu.

5. Būdas pagal 3 punktą, besiskiriantis tuo, kad PDP adreso formatas: *validate@signature.lt.*

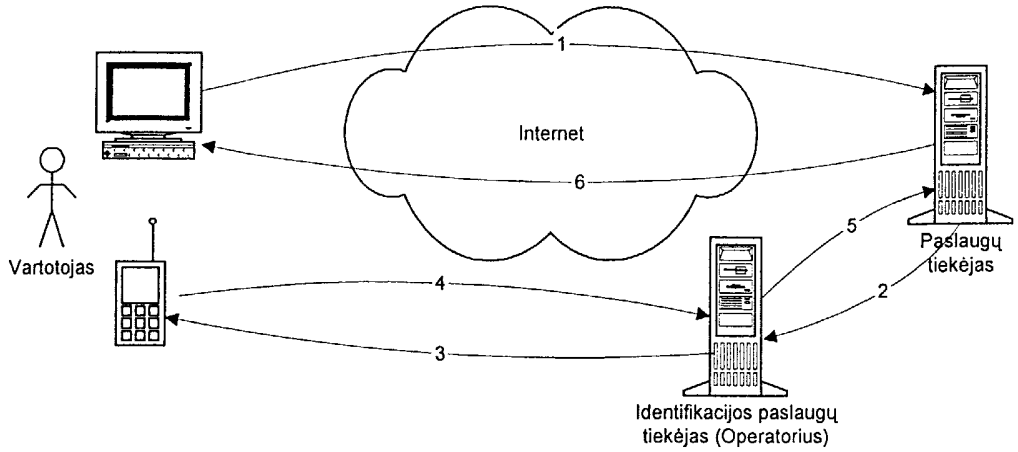
1
Internet
6
Vartotojas
5
Paslaugų
tiekėjas
2
4
3
Identifikacijos paslaugų
tiekėjas (Operatorius)

Fig. 1

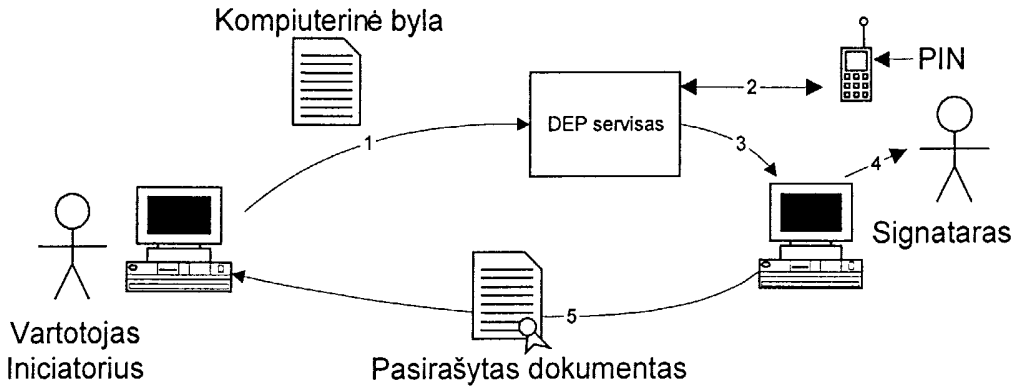
Kompiuterinė byla
PIN
2
DEP servisas
1
3
4
Signataras
Vartotojas
Iniciatorius
5
Pasirašytas dokumentas

Fig. 2

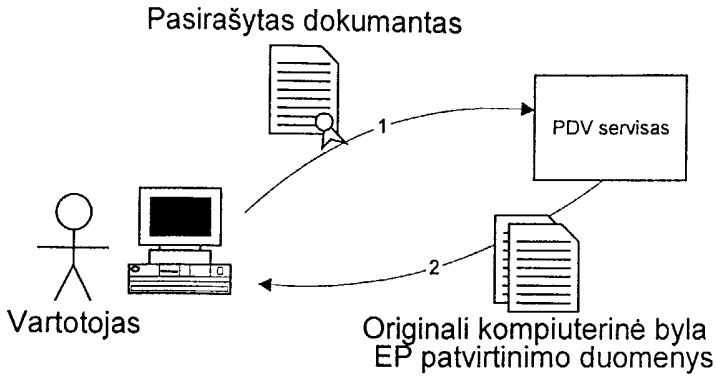
Pasirašytas dokumantas
1
PDV servisas
2
Vartotojas
Originali kompiuterinė byla
EP patvirtinimo duomenys

Fig. 3