VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ KATEDRA

Elektroninio parašo atributų sertifikavimas

Certification of electronic signature attributes

Magistro baigiamasis darbas

Atliko:	Marius Lozda	(parašas)
Darbo vadovas:	doc. dr. Valdas Undzėnas	(parašas)
Recenzentas:	asist. Vytautas Ašeris	(parašas)

Vilnius – 2011

Turinys

Santrauka

Darbe nagrinėjama atributinės informacijos sertifikavimo šiuo metu naudojamuose elektroniniuse parašuose problema. Trumpai apžvelgiami elektroninio parašo principai ir supažindinama su viešųjų raktų infrastruktūra, nurodant galimybes jai išplėsti, iškilus poreikiui užtikrinti aukštesnį saugumo lygį keičiantis papildoma (atributine) informacija. Nagrinėjami įvairūs atributinės informacijos sertifikavimo metodai, viešųjų raktų infrastruktūroje įvedant atributų sertifikato ir atributų sertifikavimo centro sąvokas. Pateikiamas tinkamiausio metodo pritaikymo pavyzdys, modeliuojant elektroninio parašo naudojimo situaciją, artimą dabartinei situacijai Lietuvoje. Sprendimo pritaikymas demonstruojamas apibrėžiant patobulintos elektroninio parašo infrastruktūros prototipą.

Raktiniai žodžiai: atributų sertifikavimas, autorizacija, autentifikacija, atributinė informacija, elektroninis parašas, sertifikavimas, sertifikatas, sertifikavimo centras, X.509, parašo taisyklės, prototipas, skaitmeninis parašas, viešųjų raktų infrastruktūra, sertifikavimo veiklos nuostatai.

Summary

This paper analyses issues of attribute certification in currently used electronic signatures. Fundamentals of electronic signatures and public key infrastructure are briefly described, focusing on possibilities of achieving higher security level in communication when attribute information is important. Various suggestions for attribute certification are analysed, introducing atribute certificates and atribute authorities. Different certification methods are compared and evaluated, applying the most suitable one in the public key infrastructure usage model, that is constructed by simplifying the current situation of electronic signatures. The solution is represented by describing the prototype of improved electronic signature infrastructure.

Keywords: attribute certification, authorization, autentification, digital signature, electronic signature, certificate, certificate authority, X.509, signature policy, prototipe, public key infrastructure, certificate practice statement

Įvadas

Šio darbo tiriamasis objektas yra elektroninio parašo infrastruktūra ir jos tobulinimo galimybės. Darbe nagrinėjama viena iš elektroninio parašo infrastruktūros plėtros krypčių – atributinės informacijos sertifikavimas. Potencialus poreikis sertifikuoti papildomą informaciją elektroniniame paraše iškeliamas kaip pagrindinė problema. Gilesniam jos suvokimui pateikiami bendrieji elektroninio parašo infrastruktūros principai, apibrėžiama dabartinė elektroninio parašo naudojimo situacija Lietuvoje.

Galimi problemos sprendimai formuluojami remiantis moksliniuose straipsniuose ir publikacijose siūlomais atributinės informacijos sertifikavimo būdais. Pagal esamą elektroninio parašo naudojimo situaciją aprašomas elektroninio parašo infrastruktūros modelis. Šiam modeliui parenkamas tinkamiausias atributinės informacijos sertifikavimo metodas. Jo pritaikymo galimybė demonstruojama pateikiant patobulintos elektroninio parašo infrastruktūros prototipą.

Problemos formulavimas

Standartinio elektroninio parašo (EP) pagrindinės dalys yra užšifruota duomenų santrauka, nuoroda į asmens sertifikatą ir nuoroda į pasirašytų duomenų tipą. Dar jame gali būti įrašyti papildomi atributai, tokie kaip parašo taisyklės, pasirašymo laikas, vieta, laiko žyma, pasirašiusiojo pareigos ir kita. Vieni atributai yra asmens pasirašomi, t. y. asmuo už juos atsako, kitus pasirašo specialios el. parašo infrastruktūros tarnybos [Und03]. Būtų gerai, kad asmens pasirašomų atributų teisingumą kažkas paliudytų (sertifikuotų). Vienas iš tokių atributų yra, pvz., pasirašančiojo pareigos (rolė), priklausymas partijai, specialistų asociacijai ar kt. Pasirašytos informacijos gavėjas norės patikrinti, ar iš tikrųjų pasirašymo metu šie duomenys buvo teisingi. Pagrindinį pasirašytą dokumentą jis patikrins, pasinaudodamas į el. parašą įdėtu sertifikatu. Sertifikatus išduoda ir jų galiojimu rūpinasi specialios įstaigos – sertifikatų centrai (CA - *Certificate Authorities*). Atributams paliudyti galima pasinaudoti tuo pačiu sertifikatu, bet siekiant aukštesnio patikimumo ir didesnio lankstumo tam gali būti skirtas atskiras atributinės informacijos sertifikatas (AC – *Attribute Certificate*). Juos išduoda atributinės informacijos sertifikatų centrai (AA – *Attribute Authorities*). Kadangi atributai laikui bėgant gali keistis, o pasirašyto dokumento turinys nebesikeis, AA turi rūpintis ne tik AC išdavimu, bet ir atnaujinimu.

Gilinantis į šią problemą, toliau darbe detaliau nagrinėjama elektroninio parašo infrastruktūra, CA ir AA darbo principai, svarstomi AC pritaikymo el. paraše būdai.

Problemos aktualumas

Elektroninis parašas Lietuvoje reglamentuotas jau 2000 metais. Nors šiuo metu jis dar nėra masiškai naudojamas, tačiau poreikis jį naudoti didėja [Rep07]. El. parašo diegimui paspartinti 2006 metais buvo pradėta vykdyti Elektroninio Parašo Proveržio Programa (E3P).

Dabartinis Lietuvos el. parašo įstatymas nereglamentuoja, kaip konkrečiai į el parašą turi būti įtraukiama, užkoduojama ir vėliau tikrinama pasirašiusiojo asmens atributinė informacija (AI) [LRS00]. Įstatyme tėra paminėta, kad el. parašo kvalifikuotame sertifikate gali būti nurodomi pasirašančiojo asmens specialūs atributai.

Pasirašant el. parašu, į jį visada įtraukiami pasirašiusiojo asmens tapatybės duomenys. Tačiau kai kuriais atvejais į parašą reikia įtraukti ir papildomą informaciją, tokią, kaip pasirašiusiojo pareigos, įgaliojimai, pasirašymo data, vieta ir panašiai. Gavus tokiu būdu pasirašytą dokumentą svarbu mokėti patikrinti šios AI teisingumą. Egzistuoja įvairūs AI sertifikavimo modeliai, paremti viešųjų raktų infrastruktūros principu [FPK07]. Juose pateiktos informaciją pateikiančios ir priimančios šalių komunikavimo schemos, standartai, taisyklės, kaip turi būti perduodama ir tikrinama AI. Šie modeliai orientuojasi į informacijos perdavimo internetu protokolų tobulinimą, tačiau juos galima pabandyti pritaikyti ir el. parašo srityje.

Viešai skelbiamų gatavų pavyzdžių, kaip kokiame nors realiame projekte buvo realizuotas EP su AI sertifikavimu, praktiškai nėra. Tačiau negalima sakyti, kad ši problema dar nėra svarstoma. Internete publikuojami ne tik įprasto EP standartai bei jo taisyklių ir kitų susijusių dokumentų pavyzdžiai, bet ir AI sertifikavimo apybraižos, kuriose orientuojamasi į atributinę informaciją interneto protokoluose. Kompiuterių inžinerijos tyrimų centrai yra paviešinę prezentacijų, kuriose užsimenama apie galimybę sertifikuoti AI elektroniniame paraše.

Darbo naujumas ir tikslas

Šis darbas yra naujas tuo, kad jame nagrinėjami ne tik bendrieji EP klausimai, bet gilinamasi į konkrečią EP infrastruktūros plėtros kryptį – atributų sertifikavimą. Lietuviškų mokslinių publikacijų, kuriose būtų tyrinėjama ši kryptis, šiai dienai nėra. Praktikoje EP patobulinimui daugiau gilinamasi į laiko žymas [IVP03].

Darbu siekiama parodyti, kad AI sertifikavimas elektroniniuose parašuose yra prasmingas ir įgyvendinamas. Atrinkti tinkamiausią AI sertifikavimo metodą esamai EP situacijai. Pateikti pavyzdinį EP infrastruktūros su AI sertifikavimu prototipą.

Darbo uždaviniai

Siekiant apsibrėžtų darbo tikslų, reikia:

1. Išsiaiškinti elektroninio parašo infrastruktūrą.
2. Išnagrinėti Lietuvos elektroninio parašo reglamentą.
3. Ištirti elektroninio parašo realizacijas Lietuvos projektuose.
4. Išanalizuoti, kaip gali būti sertifikuojama AI.
5. Surasti ir palyginti siūlomus elektroninio parašo infrastruktūros (su AI sertifikavimu) modelius, kūrimo metodikas, pavyzdžius.
6. Sudaryti pavyzdinį EP infrastruktūros modelį, kuris atspindėtų labiausiai paplitusią EP panaudojimo situaciją Lietuvoje.
7. Patobulinti modelį, parenkant tinkamiausią AI sertifikavimo metodą, ir pagal jį sukurti EP infrastruktūros su AI sertifikavimu prototipą.
8. Išnagrinėti, kokių standartinių nuostatų turi laikytis AA tarnybos.
9. Suformuluoti prototipe aprašytos AA organizacijos preliminarius nuostatus.

1. Elektroninio parašo principai ir taikymas Lietuvoje

Skyriaus tikslas – pagal informaciją, surinktą iš literatūros šaltinių, sudaryti vaizdą apie dabartinę EP technologinę situaciją Lietuvoje ir užsienyje, atkreipiant dėmesį į AI įtraukimo į EP ir jos tikrinimo galimybes.

Pirmame skyrelyje pateikiami bendrieji EP principai ir jų taikymas Lietuvoje naudojamuose EP. Antrame skyrelyje nagrinėjami įgyvendintų EP projektų pavyzdžiai, pagrindžiantys dabartinę situaciją.

1.1. Elektroninio parašo pagrindai

Kad būtų galima kalbėti apie EP atributinės informacijos sertifikavimą, pirmiausia būtina aptarti pagrindinius EP principus. Šiame skyriuje pateikiama medžiaga iš šaltinių, nagrinėjančių techninius EP įgyvendinimo Lietuvoje klausimus.

1.1.1. EP paskirtis

EP garantuoja pasirašytų el. duomenų (el. dokumentų) autentiškumą ir padeda nustatyti pasirašiusio asmens tapatybę. Jis sudaro prielaidas patikimam, greitesniam, mažesnių sąnaudų reikalaujančiam asmenų bendravimui tarpusavyje ir su įvairiomis institucijomis, padeda greičiau plėtoti verslą, suteikia aukštesnį finansinių operacijų saugumą, pagerina įvairių institucijų veiklą [IVP10].

1.1.2. Duomenų šifravimas

EP idėja yra paremta duomenų šifravimu [Und03, 7]. Dabartiniu metu EP technologija pagrįsta asimetrinio šifravimo metodu. Kitas metodas – simetrinis šifravimas – dažniausiai taikomas duomenų konfidencialumui užtikrinti. Asimetrinio šifravimo algoritmo rezultatas: sugeneruota raktų pora. Raktų porą sudaro privatusis ir viešasis raktas. Duomenys, užšifruoti vienu iš šių raktų gali būti atšifruoti tik kitu raktu. Tokiu algoritmu pagrįsta EP infrastruktūra yra vadinama viešojo rakto infrastruktūra (PKI – *Public Key Infrastructure*).

1.1.3. EP kūrimas

Duomenų, kurie yra pasirašomi EP, apimtis gali būti didelė ir įvairi, todėl pasirašoma yra tik duomenų santrauka (angl. pavadinimai *hash, message digest, imprint*). Be to, dažniausiai EP pasirašomas ne vien pats el. dokumentas, bet ir papildoma informacija (pvz., nuoroda į pasirašiusio asmens sertifikatą ir kt.). El. dokumentui ir papildomai informacijai sugeneruojama

viena duomenų santrauka. Ji užšifruojama pasirašančio asmens privačiuoju raktu. Ši užšifruota informacija ir yra EP. Pasirašyti duomenys – tai duomenys plius EP [IVP10].

Duomenų santrauka turi pasižymėti tokiomis savybėmis [IVP10].:

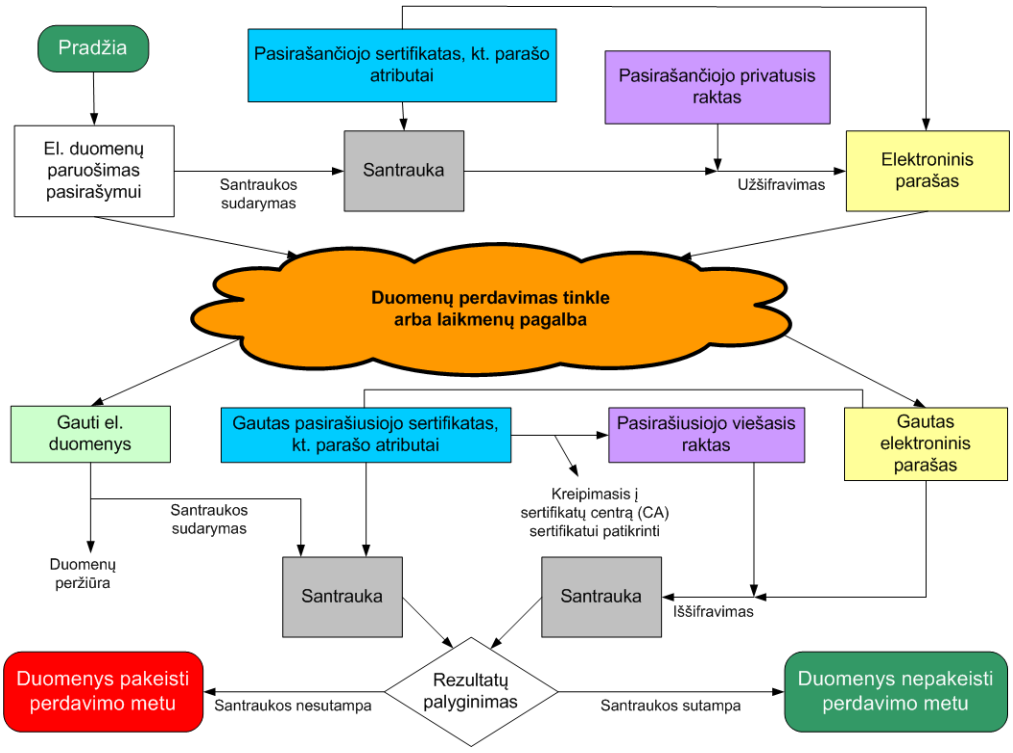
- iš santraukos neįmanoma atstatyti originalių duomenų;
- praktiškai neįmanoma rasti dviejų skirtingų duomenų, kurių santraukos būtų vienodos.

1.1.4. EP tikrinimas

Gavęs pasirašytus duomenis, jų gavėjas parašui tikrinti naudoja atitinkamą įrangą ir siuntėjo viešąjį raktą. Atšifruojant EP siuntėjo viešuoju raktu, atstatoma siuntėjo sukurta duomenų santrauka [IVP10]. Pagal gautą el. dokumentą ir papildomą informaciją gavėjas taip pat sugeneruoja duomenų santrauką. Šią santrauką jis palygina su atšifruota santrauka ir taip įsitikina parašo tikrumu. Jei duomenys nebuvo iškraipyti ir EP sukūrė asmuo, turintis privatųjį raktą, kuris atitinka naudotą viešąjį raktą, šios santraukos sutaps.

Viešasis raktas yra pasirašiusiojo asmens sertifikate, kuris siunčiamas kartu su pasirašytais duomenimis. Galimybę pasitikrinti, ar pasirašytus duomenis ir sertifikatą iš tikro atsiuntė prisistatęs asmuo, suteikia sertifikatų sudarytojai - sertifikavimo paslaugų teikėjai (sertifikavimo centrai). Tikrinant parašą taip pat svarbu įsitikinti, ar parašo kūrimo metu galiojo pasirašiusio asmens sertifikatas, ar nepažeisti sertifikate nustatyti apribojimai.

Pasirašymas EP ir jo tikrinimas pavaizduotas 1 pav.



1 pav. EP kūrimo bei patikrinimo schema [IVP10]

Ši schema vaizduoja vieną paprasčiausių EP kūrimo ir tikrinimo scenarijų. Stebint veiksmus, atliekamus su parašo atributais, galima pamatyti, kad šiuo atveju pasirašančiojo sertifikatas ir kiti parašo atributai tiesiog įtraukiami į duomenų santrauką, kuri vėliau užšifruojama. Jei parašo tikrinimo metu iš sertifikatų centro (CA – *Certificate Authority*) gaunamas patvirtinimas, kad sertifikatas tikrai priklauso pasirašiusiajam asmeniui, ir santraukos sutampa, gavėjas įsitikina šios informacijos tikrumu:

1. Perdavimo metu duomenys nebuvo pakeisti (pavaizduota schemoje – žalias kvadratas).
2. Dokumentą pasirašė tikrai tas pats asmuo, iš kurio buvo gautas EP.
3. Sertifikatas buvo galiojantis pasirašymo metu, t.y. pasirašantysis turėjo teisę pasirašyti dokumentą.
4. Visi parašo atributai yra teisingi. Pavyzdžiui, jei pasirašantysis asmuo į EP įtraukė atributą „pareigos“ ir jame nurodė konkrečias pareigas, vadinasi, parašo sudarymo metu jis tas pareigas tikrai ėjo.

Pirmąjį punktą pagrindžia santraukų sutapimas. Patvirtinimas iš CA pats savaime pagrindžia antrąjį teiginį. Trečio punkto informacija yra iš tikrųjų teisinga, jei CA pakankamai rūpinasi ne tik sertifikatų išdavimu, bet ir jų palaikymu: tikrinimu, suspendavimu ir atšaukimu. Nustatyti, ar EP tikrai buvo sukurtas iki tam tikro laiko galima, jei į EP įtraukiama laiko žyma. Tačiau norint pagrįsti paskutinį punktą, patvirtinimo iš CA gali nepakakti. Sertifikatą pasirašančiajam asmeniui CA išduoda ilgam laikotarpiui, o atributinė informacija (pasirašančiojo pareigos, priklausymas kažkokiai grupei ir kt.) gali keistis dažniau. Kai kuriose situacijose gauto EP atributinės informacijos teisingumas gali būti ypač reikšmingas. Tokiu atveju prireikia papildomų veiksmų šios informacijos patikrinimui.

1.1.5. Sertifikatai

Sertifikatas EP įstatyme apibrėžiamas kaip elektroninis liudijimas, kuries susieja parašo tikrinimo duomenis su pasirašančiu asmeniu ir patvirtina arba leidžia nustatyti pasirašančio asmens tapatybę [LRS00, 2].

Skaitmeninį sertifikatą sudaro sertifikavimo paslaugas teikianti organizacija CA, jį pasirašanti savo privačiuoju raktu. CA taip teikia sertifikatų duomenis parašo naudotojams EP tikrinti [IVP10].

Paprastai skaitmeninis sertifikatas susideda iš:

1. Savininko viešojo rakto.
2. Savininko vardo.
3. Viešojo rakto galiojimo termino.

4. Skaitmeninį sertifikatą teikiančio CA pavadinimo.
5. Skaitmeninio sertifikato serijinio numerio.
6. Sertifikatą teikiančio CA elektroninio parašo.

Tikslesnę skaitmeninio sertifikato struktūrą nustato *RFC 5280* standartas. Jame pateikiamas sertifikato formatas X.509, skirtas Interneto aplikacijoms, apimančiomis WWW, el. paštą, vartotojų autentifikaciją, Interneto protokolo apsaugą (*IPsec*) [CSF08, 5]. Specifinės aplikacijos, siekdamos išpildyti savo reikalavimus, gali pritaikyti šį formatą jį papildydamos.

Sertifikatai skirstomi į paprastus ir kvalifikuotus. Kvalifikuotą sertifikatą sudaro Vyriausybės ar jos įgaliotos institucijos nustatytus reikalavimus atitinkantis sertifikavimo paslaugų teikėjas [LRS00, 3].

Toks sertifikatas talpina daugiau informacijos, nei paprastas. Jame nurodoma:

1. Užrašas, kad tai yra kvalifikuotas sertifikatas.
2. CA ir jo buveinės šalies identifikatoriai.
3. Pasirašančio asmens vardas ir pavardė arba slapyvardis.
4. Pasirašančio asmens specialūs atributai, jei tai reikalinga atsižvelgiant į numatomus sertifikato naudojimo tikslus.
5. Parašo tikrinimo duomenys (viešasis raktas), atitinkantys pasirašančio asmens turimus parašo formavimo duomenis (privatųjį raktą).
6. Sertifikato galiojimo pradžios ir pabaigos terminai.
7. Sertifikato identifikatorius, kurį suteikia CA.
8. CA saugus elektroninis parašas.
9. Sertifikato naudojimo paskirties apribojimai, jei tai nustatyta.
10. Leistina operacijų piniginė vertė, kada sertifikatas gali būti naudojamas, jei tai nustatyta.

Specialūs pasirašančio asmens atributai akcentuojami ketvirtame iš šių punktų. Sąlyga „jei tai reikalinga atsižvelgiant į numatomus sertifikato naudojimo tikslus“ leidžia suprasti, kad įstatymas numato, jog dažniausiai ši informacija nėra reikšminga. Tiesiogiai interpretuojant šį punktą, galima suprasti, kad tais retais atvejais, kai AI yra esminė, jos patvirtinimui užteks patikrinti kvalifikuotame sertifikate skelbiamų atributų sąrašą.

Tarkime, asmuo, pasirašydamas el. dokumentą teigia, kad jis priklauso politinei grupei X. Jis tai įgyvendina sukurdamas parašo atributą „grupė“ su reikšme „X“. Gavėjas, tikrindamas EP, turėtų surasti sertifikate nurodytą atributą „grupė“ ir patikrinti ar šiame atribute nurodyta ta pati reikšmė. Problemos šioje situacijoje gali iškilti tuomet, kai kvalifikuoto sertifikato galiojimo laikas nesutaps su asmens atributų galiojimo laiku. Imant tą patį pavyzdį, tarkime, kad pasirašymo metu sertifikatas, išduotas pasirašančiam asmeniui vis dar galioja, tačiau pasirašantis

asmuo nebepriklauso grupei X. Nenorėdamas to atskleisti, pasirašantis asmuo apsimeta vis dar priklausantis šiai grupei ir sukuria „grupės“ atributą su reikšme „X“. Kadangi sertifikate įrašytas atributas vis dar išlieka toks pats, tikrindamas EP, gavėjas patikės šia informacija ir bus suklaidintas.

1.1.6. Teisiniai aspektai

Įgyvendinant EP sprendimus, svarbu atsižvelgti ne tik į esamas technologines galimybes, bet ir į EP teisinį reguliavimą toje šalyje, kurioje EP diegiamas. Lietuvos elektroninio parašo įstatymo nuostatos numato, kad teisme įrodomąją galią turi tik saugus elektroninis parašas, kuris yra sukurtas saugia parašo formavimo įranga ir patvirtintas galiojančiu kvalifikuotu sertifikatu. Kvalifikuotus sertifikatus teikiantiems sertifikavimo paslaugų teikėjams yra numatyta prievolė registruotis EP priežiūros institucijoje, t.y. Informacinės visuomenės plėtros komitete (IVPK) prie Lietuvos Respublikos Vyriausybės. Akivaizdu, kad EP, patvirtintas kvalifikuotu sertifikatu, yra patikimesnis, nei patvirtintas paprastu.

Svarbu paminėti, kad pagal Europos Sąjungos EP Direktyvos principus, kvalifikuotas sertifikatas gali būti išduotas tik fiziniam asmeniui, kuris veikia savo vardu, arba kito – juridinio ar fizinio asmens arba jo atstovaujamos esybės – vardu [IVP10]. Rašytiniuose šaltiniuose nėra pateikiama statistika apie kvalifikuotų ir “nekvalifikuotų” sertifikatų naudojimą. Matyt tokia statistika dar nėra sukaupta. Bendra tendencija yra tokia, kad viešojo administravimo sferoje, netgi “uždarose” taikomosiose sistemose, tokiose kaip dokumentų apsikeitimas tarp administracijų Europos Sąjungos šalių mastu, yra jau naudojamas ir planuojama pilnai pereiti prie kvalifikuoto sertifikato naudojimo.

1.1.7. EP formatai

EP formatas nusako, kokios formos EP turi būti kuriamas bei apibrėžia papildomus EP funkcionalumus [IVP10]. Vienas iš pirmųjų EP įgyvendinimo techninių sprendimų buvo XMLDSIG rekomendacija. Ji apibrėžė EP formatą XML kalba. Tačiau pirminė XMLDSIG struktūra netenkino saugaus EP reikalavimų ir šis sprendimas buvo tobulinamas toliau. ETSI išleido standartą *TS 101903 „XML saugūs elektroniniai parašai (XAdES)“* [ETS02]. Šiame standarte nurodyta, kad pats parašas yra saugomas XMLDSIG dalyje, o parašo atributai – XAdES dalyje.

XAdES apibrėžia 7 EP formas, iš kurių 4 yra pagrindinės ir 3 – papildomos. Kiekviena forma papildo prieš tai buvusią formą tam tikru funkcionalumu.

Jau pirmoje (paprasčiausioje) XAdES-BES formoje, į EP įtraukiami tokie atributai kaip:

- pasirašiusio asmens nurodytas pasirašymo laikas (*SigningTime*);

- pasirašiusio asmens vaidmuo (*SigningRole*);
- pasirašiusio asmens nurodyta pasirašymo vieta (*SignatureProductionPlace*).

Tačiau šių atributų tikrinimas vistiek atliekamas paprastu būdu: jei EP galiojimas patvirtinamas, daroma išvada, kad šie pateikti atributai yra teisingi. Kitų XAdES formų pridedamas funkcionalumas orientuotas į išreikštinai pateiktų parašo taisyklių tikrinimą (XAdES-EPES), pasirašymo laiko validavimą (XAdES-T), sertifikatų galiojimo tikrinimą (XAdES-C), papildomos laiko žymos pridėjimą (XAdES-X, XAdES-X-L) ir sertifikatų archyvavimą (XAdES-A).

1.1.8. Laiko žymos

Nemažai problemų, susijusių su EP galiojimo patvirtinimu, sprendžia laiko žymų įtraukimas į EP. Laiko žymą galima laikyti dar vienu EP atributu, kuris nėra pasirašomas. Toks atributas numatomas tiek XAdES-T, tiek kitame - CAdES-T el. parašo formato standartuose. Šis EP elementas išsiskiria iš kitų atributų (tokių, kaip, pvz., jau minėtų pasirašančio asmens pareigas ar priklausymą kažkokiai grupei nurodančių atributų, pasirašymo vietos ir kt.) tuo, kad jį sukuria (deda) dar viena patikima trečioji šalis – laiko žymų tarnyba (TSA – *Time Stamping Authority*) [Und03, 12]. EP kūrimo metu, asmuo, norėdamas gauti laiko žymą el. duomenims, nusiunčia į TSA užklausą su tų duomenų santrauka. Laiko žyma yra įrodymas, kad el. duomenys buvo sukurti anksčiau nei žymoje užfiksuotas laiko momentas.

Tikrindamas EP su laiko žyma, gavėjas kreipiasi ne tik į CA dėl pasirašiusiojo asmens autorizavimo bet ir į TSA dėl laiko žymos patikrinimo. Taip į EP infrastruktūrą įtraukiama dar viena dalyvaujanti šalis. Tokią infrastruktūrą galima laikyti pavyzdine ieškant patikimesnio ir lankstesnio būdo pasirašyti ir tikrinti kitą pasirašančiojo atributinę informaciją.

1.1.9. EP pasirašyti dokumentai

EP gali būti taikomas ne vien elektroninių dokumentų pasirašymui – skaitmeniniai sertifikatai naudojami autentifikacijai tarp įvairių komunikuojančių šalių (pavyzdžiui, kliento prisijungimas prie banko sistemos). Šiame darbe orientuojamasi į pirmąjį dokumentų EP panaudojimo atvejį – elektroninių dokumentų pasirašymą.

Kad keitimasis EP pasirašytais elektroniniais dokumentais taptų įmanomas, turi būti nutarta, kokie dokumentai gali būti pasirašomi, kaip jie turi būti parengti, kokie EP turi būti naudojami jų pasirašymui ir daugybė kitų detalių. Lietuvos archyvų departamentas 2009 metais parengė „Elektroniniu parašu pasirašyto elektroninio dokumento specifikaciją ADOC-V1.0“ [LAD09]. Specifikacijoje nurodyti reikalavimai, kuriuos turi tenkinti EP pasirašinėjami elektroniniai dokumentai. Reikalavimai apibrėžia „elektroninio dokumento pakuotę“, kuri

apjungia pasirašomus duomenis ir parašus į vieną rinkmeną. Specifikacijoje išdėstyta elektroninio dokumento loginė struktūra (pagrindinis dokumentas, kiti dokumentai, elektroniniai parašai, metaduomenys) ir jos atvaizdavimas į fizinę struktūrą (katalogai, bylos). Detaliai aprašoma, kuri elektroninio dokumento papildoma informacija (metaduomenys) turi būti pasirašoma, tačiau nustatyta, kad kurdami EP asmenys juose nurodo vienintelį savo asmens sertifikatą. Tai reiškia, kad tikrinant EP gali būti nustatyta tik pasirašiusiojo tapatybė, bet ne kiti jo duomenys.

1.2. EP pritaikymo pavyzdžiai

Skyrelyje trumpai apžvelgiami keli per pastarąjį dešimtmetį įgyvendinti EP diegimo projektai. Visi jie suteikia galimybę išbandyti dokumentų pasirašymą ir EP tikrinimą, išskyrus Project BalticTime, kuris skirtas kurti ir validuoti EP laiko žymas. Išsamiau nagrinėjant šiuos projektus, nustatyta, kad nei vienas iš jų nepateikia galimybės šalia pasirašomų dokumentų pridėti atributinės informacijos (paprasčiausiu atveju pasirašančiojo asmens atributų) ir jos patikrinti.

1.2.1. DigiDoc

DigiDoc – tai dokumentų pasirašymo EP priemonė. Estijoje šis įrankis yra de-facto naudojamas standartas, kurį Lietuvos Elektroninio parašo proveržio programa (E3P) rekomenduoja kaip pasirašymo priemonę [E3P09]. Šiai priemonei buvo sukurtas portalas (*https://digidoccheck.sk.ee*), kuriame vartotojai gali elektroninius dokumentus pasirašyti EP, keistis pasirašytais duomenimis bei patikrinti parašų autentiškumą. Pasirašyti dokumentus galima naudotis įsigijus Omnitel mobilųjį telefoną su specialia įranga ir gavus EP sertifikatą (plačiau aprašyta 2.4 skyrelyje). Dokumentų patikrinimui išduoto sertifikato turėti nebūtina.

Taip pat DigiDoc pateikia taikomąją programą, veikiančią Windows aplinkoje, kuria naudojantis taip pat galima pasirašinėti ir tikrinti el. dokumentus. Į pasirašomus dokumentus įtraukti papildomos informacijos DigiDoc neleidžia.

1.2.2. JustaGE

"Justa GE" – IVPK užsakymu sukurta ir nemokamai platinama EP formavimo ir tikrinimo taikomoji programinė įranga, kurianti EP pagal Lietuvos standartą LST ETSI TS 101 903 "Patobulintieji XML elektroniniai parašai (XAdES)" bei atitinkanti IVPK rekomendacijas [IVP10]. Šios programinės įrangos galimybės ir savybės:

- bet kurio formato failo pasirašymas;
- vieno failo pasirašymas keliais elektroniniais parašais;

- kelių failų pasirašymas vienu metu;
- patogus pasirašymas ir tikrinimas per kontekstinį meniu;
- sertifikato galiojimo būsenos tikrinimas;
- patogi ir informatyvi parašo naudotojo sąsaja;
- pritaikyta Windows ir Linux operacinėms sistemoms.

Atributinės informacijos įtraukimo į EP ir jos patikrinimo galimybės Justa GE nesuteikia.

1.2.3. Project BalticTime – TSA

Šio projekto tikslas buvo sukurti viešai prieinamą laiko žymų išdavimo ir tikrinimo sistemą ir padidinti pasitikėjimą laiko žymų tarnybomis [PFI07]. Projekto svetainėje patalpintas demonstracinis laiko žymų įrankis. Juo naudojantis galima EP pasirašytam dokumentui uždėti laiko žymą ir ją patikrinti.

Projektas demonstruoja, kad egzistuoja poreikis turėti tobulesnį EP. Kaip vienas iš patobulinimų, pateiktas laiko žymos įtraukimas į EP. Tokio patobulinimo sėkmingas realizavimas skatina apsvarstyti tolimesnį EP tobulinimą.

1.2.4. „Omnitel“ mobilusis elektroninis parašas

E3P iniciatyva 2007m. Lietuvoje buvo pradėtas platinti mobiliojo ryšio operatoriaus Omnitel mobilusis elektroninis parašas. Toks EP leidžia atsisakyti papildomų prietaisų, nes pasirašymo įrenginį pakeičia mobilusis telefonas, kuriame įdedama nauja SIM kortelė su EP kūrimo galimybe [Omn07a]. Šitaip kuriamas EP iš pradžių buvo skirtas prisijungti prie internetinės bankininkystės „Hansabanke“ mobiliuoju telefonu. Vėliau vartotojams buvo pristatyta galimybė tokiu būdu pasirašyti el. dokumentus, pasinaudojant DigiDoc projekto portalu [Omn07b].

Galimybė į mobilųjį EP įtraukti papildomą (atributinę) informaciją, šiame projekte svarstoma nebuvo.

1.2.5. „Bitė Lietuva“ mobilusis elektroninis parašas

Dar vienas E3P projektas buvo vykdomas kito mobiliojo ryšio operatoriaus – Bitės. Jo rezultatas – mobiliojo EP paslauga vartotojams. Šis EP leidžia nustatyti pasirašiusio asmens tapatybę ir užtikrina juo pasirašytų elektroninių dokumentų autentiškumą [Bit08]. Klientams, pasirašiusiems EP paslaugos sutartį, suteikiama SIM kortelė su saugiu kriptografiniu moduliu ir iš karto dviem sertifikatais:

- prisijungimo sertifikatas skirtas prisijungti prie sistemų internete. Jis leidžia elektroniniu būdu nustatyti pasirašančio asmens tapatybę;

- pasirašymo sertifikatas skirtas pasirašyti sutartis (ar kitokius el. dokumentus) elektroniniu būdu.

Šie sertifikatai apibrėžiami kaip asmens dokumento atitikmenys, kuriais galima įrodyti savo asmens tapatybę arba teisę prieiti prie reikalingos informacijos internete. Tačiau detalesnės informacijos, kaip sertifikatas užtikrina šių teisių valdymą, nėra.

1.2.6. Lietuviška parašų įranga „Signa“

Gyventojų registro tarnyba, kurios siūlomos paslaugos plačiau aprašytos 3.1 skyrelyje, teikia įrangą, kuri leidžia kurti EP naudojantis naujos kartos asmens tapatybės kortele [GRT11]. Norint naudotis asmens tapatybės kortelės elektroninio parašo funkcijomis visų pirma reikia įsigyti kortelės skaitytuvą. Išduodamose kortelėse įdedamas asmens tapatybės sertifikatas, kuriuo naudojantis galima kurti EP, pasirašant elektroninius dokumentus ar autentifikuojantis sistemose. Elektroninių dokumentų, atitinkančių specifikacijos ADOC-V1.0 reikalavimus (žr. 1.1.9 skyrelį), kūrimui bei tikrinimui siūloma nemokama programinė įranga SIGNA BETA.

1.3. Situacijos apibendrinimas

Apžvelgus dabartinę elektroninio parašo (EP) situaciją Lietuvoje, susidaro įspūdis, kad EP principai yra pakankamai gerai apibrėžti ir įtvirtinti. Nors EP dar nėra paplitęs visuotinai, Informacinės visuomenės plėtros komitetas (IVPK), valstybinės įstaigos ir telekomunikacijų bendrovės aktyviai vykdo EP projektus. Daugumos šių projektų tikslas yra pristatyti viešojo rakto infrastruktūras (*Public key infrastructure* – PKI), suteikiančias galimybę didelei vartotojų grupei naudotis EP. Tokio EP vartotojai gali lengvai patikrinti pasirašytame dokumente nurodyto pasirašiusiojo asmens ar subjekto tapatybę ir taip nuspręsti, ar EP laikyti galiojančiu. Tačiau tokie EP nepatenkintų poreikio oficialiai patikrinti papildomos informacijos apie pasirašiusįjį asmenį. Infrastruktūroje dalyvaujanti trečioji šalis – sertifikatų centras (*Certificate authority* – CA) išduoda sertifikatus, liudijančius tik pasirašiusiojo tapatybę. Tuo tarpu atributinė informacija, įtraukta į EP, tokia kaip pasirašiusiojo pareigos, kai kuriais atvejais gali būti pakankamai svarbi, kad irgi būtų liudijama trečiųjų šalių.

Toliau darbe nagrinėjami, lyginami ir vertinami įvairūs atributinės informacijos (arba tiesiog atributų) sertifikavimo sprendimai. Aprašomas konkretus PKI naudojimo modelis, sukurtas atsižvelgiant į EP naudojimo situaciją Lietuvoje. Pagal šį modelį kuriamas EP su AI sertifikavimu infrastruktūros prototipas, parenkant ir pritaikant tinkamiausią iš išnagrinėtų atributų sertifikavimo variantų. Prototipas pateikiamas aprašant:

- EP taisykles (*Signature policy* – SP), apibrėžiančias modifikuoto EP struktūrą, kūrimo ir tikrinimo procedūras, naudojimo sritis ir sąlygas;

- suformuluotus tarnybų, užsiimančių reikiamų sertifikatų išdavimu, veikimo principus, pateikiant pavyzdinius nuostatus;
- modifikuotas EP kūrimo, perdavimo ir tikrinimo procedūras.

2. Atributų sertifikavimo variantai

Užsienyje atributų sertifikavimo klausimas buvo pradėtas nagrinėti apytiksliai prieš dešimt metų. Moksliniai straipsniai siūlo įvairius sprendimus, kaip atributinės informacijos sertifikavimas galėtų būti įtrauktas į EP infrastruktūrą. Tačiau šiems sprendimams pagrįsti trūksta plačiai paskelbto pavyzdžio, kuris pademonstruotų, kaip tai buvo (ar galėtų būti) įgyvendinta realioje situacijoje.

Daugiausia apžvelgtų atributinės informacijos sertifikavimo idėjų remiasi X.509 standarte numatyta sertifikatų išplėtimo galimybe. Pavyzdžiui, straipsnyje [Nyk00] pristatomi atributų sertifikatai, pritaikyti X.509 karkasui, kurių įvedimas į PKI leistų naudoti šią infrastruktūrą ne tik autentifikavimui bet ir autorizavimui. Galima išskirti dvi pagrindines siūlomų sprendimų kryptis:

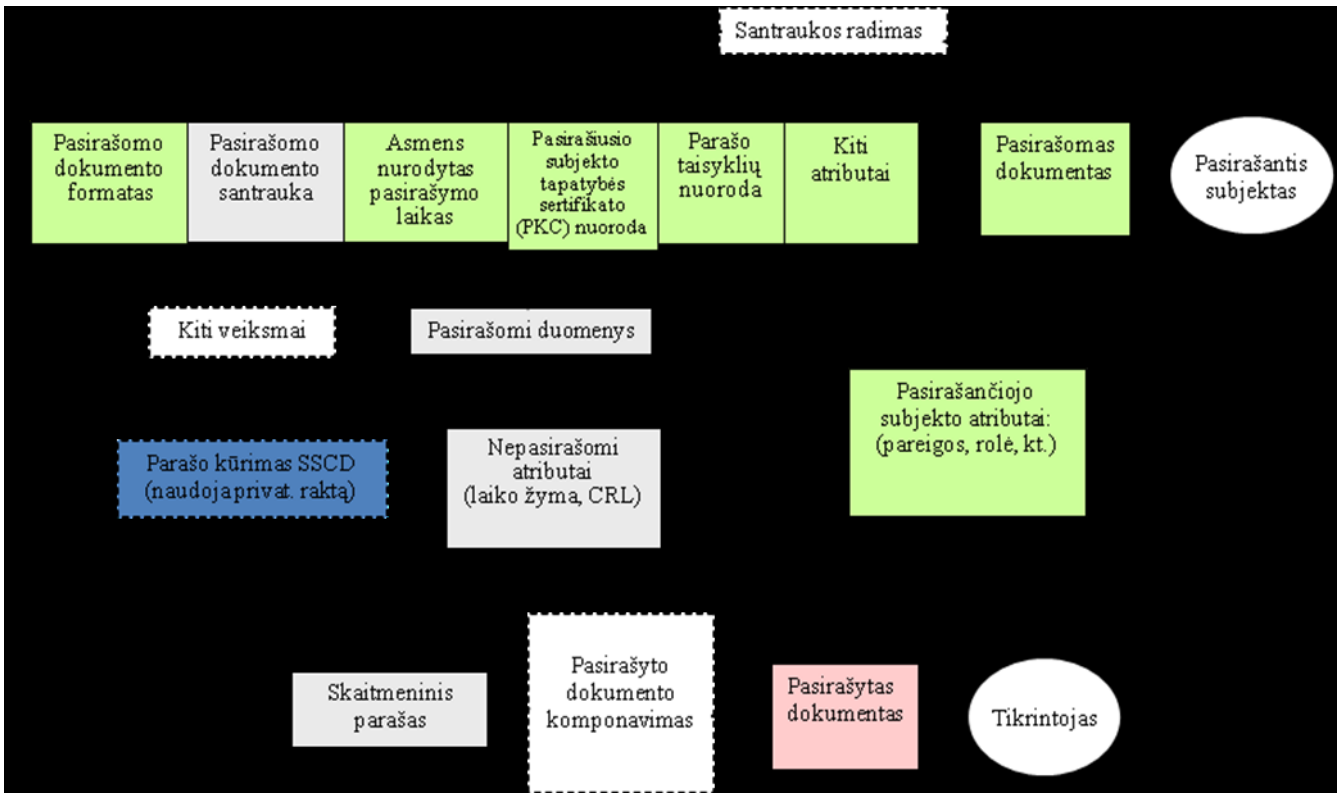
- atributų liudijimą pavesti CA, išduodančiam tapatybės sertifikatus;
- įsteigti papildomas tarnybas ir naudoti atskirus atributų sertifikatus.

Toliau darbe formuluojami konkretūs atributų sertifikavimo variantai, paremti kuria nors iš šių krypčių. Taip pat išvardinami kiekvieno iš jų privalumai ir trūkumai, bei nurodomos taikymui tinkamos situacijos.

2.1. Nesertifikuoti atributai

Pasirašiusiojo subjekto atributinę informaciją galima paprasčiausiai įtraukti šalia kitų parašo atributų, kuriems pasirašymo metu kuriama santrauka ir vėliau skaitmeninis parašas. Už šių atributų teisingumą atsako pasirašantysis, todėl tai nėra pats patikimiausias būdas. Pasirašantysis subjektas, kurdamas parašą, turi laikytis SP nurodytų parašo patvirtinimo taisyklių. Jos nurodo, kokie atributai turi būti pateikti paraše, kad jis būtų laikomas potencialiai galiojančiu [Und10, 90]. Tačiau į šiuos atributus subjektas gali įtraukti kokias nori reikšmes, kurios gali būti ir neteisingos. Pavyzdžiui, parašo patvirtinimo taisyklės reikalauja nurodyti pareigų atributą. Jį pildydamas subjektas gali nurodyti reikšmę „direktorius“, nors iš tikrųjų šių pareigų jis neina.

Tokiame paraše dalyvauja vienintelis prie parašo pridedamas sertifikatas (arba jo nuoroda), išduotas trečiosios šalies – CA. Šis sertifikatas toliau bus vadinamas tapatybės sertifikatu, arba viešojo rakto sertifikatu (*Public key certificate* – PKC). Jis liudija, kad tam tikras viešasis raktas priklauso tam tikram subjektui. Parašo tikrintojas patikrina jo galiojimą ir atšifruoja gautą santrauką jame nurodytu viešuoju raktu. Jei PKC pasirašymo metu buvo galiojantis ir santrauka atšifruojama sėkmingai (t. y. sutampa su paties tikrintojo sugeneruota gauto dokumento santrauka), toks EP laikomas galiojančiu. Kitaip tariant, tikrintojas įsitikina, kad dokumentą pasirašė nurodytas subjektas. Tuo pačiu jis turi patikėti ir parašo atributų teisingumu – o tai kai kuriais atvejais (tokiais, kaip anksčiau pateiktame pavyzdyje) gali būti klaidinga išvada.

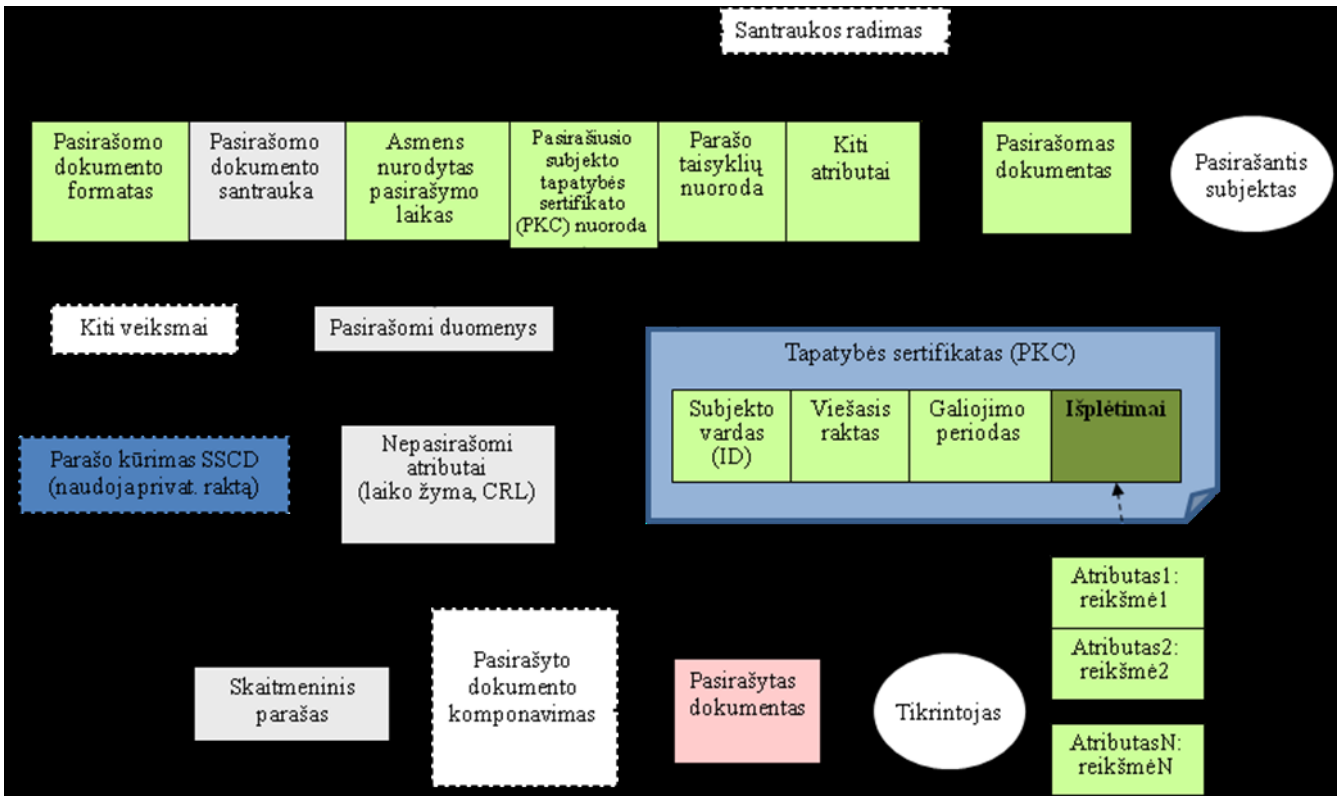


2 pav. Parašo kūrimo (įtraukiant nesertifikuotus atributus) informacinis modelis

Tokį atributinės informacijos įtraukimo į EP sprendimą atitinka 2 pav. pavaizduotas EP kūrimo informacinis modelis. Šiame EP modelyje dalyvauja atributai, kurie nėra sertifikuojami apskritai, todėl tokio sprendimo negalima priskirti nei vienai iš anksčiau paminėtų krypčių. Tokie EP turėtų būti naudojami uždaroje aplinkoje, kurioje pasirašantys asmenys yra pakankamai patikimi ir atributus visada nurodo teisingai. Realybėje tokios situacijos itin retos, todėl šis modelis toliau nebus vertinamas.

2.2. Atributai tapatybės sertifikate

Atviroje aplinkoje, kurioje EP tikrintojai ne itin pasitiki pasirašančiaisiais, atsakomybė už atributinės informacijos teisingumą gali būti perduodama trečioms (patikimoms) šalims. Paprasčiausias sprendimas yra liudyti subjekto atributus kartu su jo tapatybe. Tam galima pasinaudoti CA išduodamais PKC, jei jie atitinka X.509 standartą, kuris reikalauja, kad PKC būtų numatyti išplėtimo laukai. Juose ir įrašoma atributinė informacija (3 pav.)



3 pav. Parašo kūrimo informacinis modelis. Atributai sertifikuojami PKC

SP turi būti nurodyta, kad tam tikri atributai bus nurodomi ne parašuose, bet pasirašančiojo PKC. Pasirašantysis subjektas tuo turi pasirūpinti iš anksto, prieš kurdamas parašus. Prašydamas išduoti PKC, jis pateikia CA ne tik savo tapatybės informaciją, bet ir atributus, kuriuos norės įtraukti į sertifikatą. CA, patikrinusi šiuos duomenis, sukuria įprastą PKC, užpildo jo išplėtimo laukus atributais ir viską pasirašo savo parašu. Taip ji tampa atsakinga ir už subjekto tapatybės ir už jo atributinės informacijos teisingumą.

Tokio modelio privalumai:

1. Nesikeičia PKI infrastruktūra – sertifikavime dalyvauja vienintelė trečioji šalis (CA), nereikia steigti jokių papildomų tarnybų.
2. Parašo tikrinimo procedūra lieka nepakitusi. Jei tikrintojas nustato, kad PKC yra galiojantis, vadinasi jame pateikti atributai yra teisingi.
3. Paprastesnis EP formatas – nereikia paraše papildomų atributų.
4. Nesikeičia komunikavimo protokolas. Laikantis jo ir toliau siunčiami pasirašyti duomenys ir tas pats nepasirašomų atributų komplektas.

Modelio trūkumai:

1. Realybėje subjekto atributai keičiasi ir būna atšaukiami dažniau nei tapatybė. Bent truputį pasikeitus atributinei informacijai, subjektui tenka atšaukti turimą PKC ir prašyti išduoti naują. Taip apkraunamas CA darbu ir greitai plečiasi atšaukiamų sertifikatų sąrašai (*Certificate revocation list* - CRL).

2. CA, prieš išduodamas PKC, turi atlikti papildomus patikrinimus. Ji turi būti įgaliota patikrinti ne tik subjektų tapatybę bet ir kitą informaciją (atributus).
3. Pasirašantysis, naudodamas vieną PKC, negali keisti pridedamų atributų sąrašo. SP gali būti numatyta galimybė EP nurodyti įvairius atributus, be to skirtingiems tikrintojams gali rūpėti skirtingi subjekto atributai. Pavyzdžiui, vienam tikrintojui gali būti svarbios pasirašiusiojo pareigos, o kitam gali rūpėti subjekto priklausymas tam tikrai organizacijai. Tačiau į šiame modelyje naudojamus PKC visada įtraukiamas fiksuotas atributų sąrašas, todėl tikrintojas gauna galimybę prieiti ne tik prie tų atributų, kurie jam aktualūs, bet ir prie tų, kurių subjektas galbūt nenorėtų atskleisti.

Šis modelis ypač tinkamas naudoti tokiose aplinkose, kur atributinės informacijos gyvavimo trukmė yra fiksuota. SP turi būti nurodyta, kad nėra numatyta galimybės atšaukti atributus anksčiau nei pasibaigs PKC galiojimo periodas. Šis tvirtas tapatybės ir atributų susiejimas realybėje pasiteisintų tokiais atvejais:

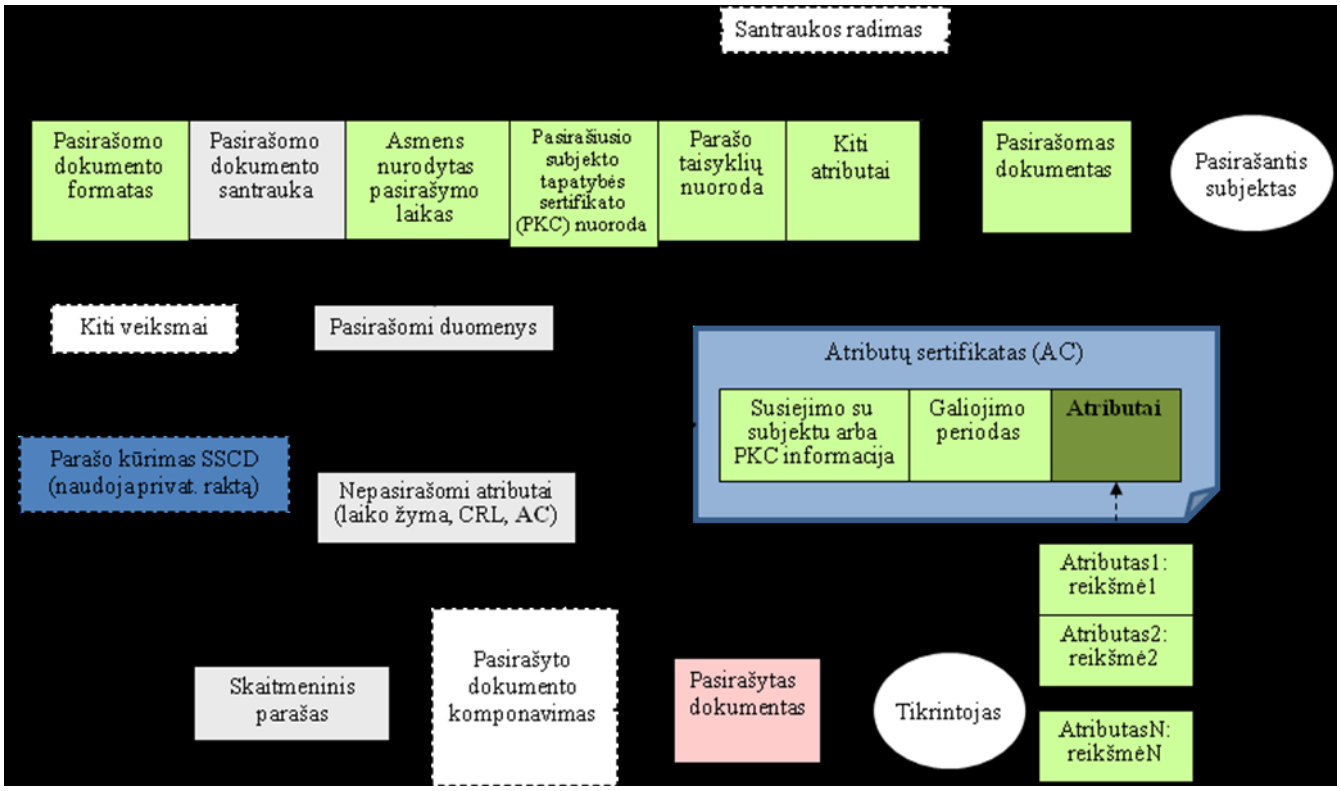
- kai atributo gyvavimo trukmė yra **nesibaigianti**. Tarkime vienas iš subjekto atributų nurodo asmens mokslinį laipsnį ar titulą – tai informacija, kuri galioja iki gyvenimo pabaigos. Toks atributas nustos galioti tik atšaukus PKC ar pasibaigus jo galiojimo periodui. Prireikus išduoti naują PKC, atributas vėl bus įdedamas į šį sertifikatą;
- kai atributo gyvavimo trukmė yra **trumpalaikė**. Tai ypatingi atvejai, kai PKC išduodami ypač trumpam laikotarpiui. Pavyzdžiui, įmonės viduje organizuojama konferencija, kurios nariai naudosis EP komunikavimui tarpusavyje. Įmonė turi įsteigusi vidinę CA, arba užsisako išorinės CA paslaugas. CA kiekvienam konferencijos nariui išduoda PKC, kuris kartu su asmens tapatybe liudija ir asmens poziciją grupėje (vadovas, administratorius, eilinis narys ir kt.). Vykstant konferencijai, nariai keičiasi pasirašytais elektroniniais dokumentais arba komunikacijai naudoja sistemą, autentifikuojančią ir autorizuojančią vartotojus. Pasibaigus konferencijai visi PKC nustoja galioti.

2.3. Atributai atskirame sertifikate („push“ modelis)

Arčiau kasdienybės yra tokie atvejai, kai atributinė informacija keičiasi greičiau nei atšaukiamas ar nustoja galioti PKC. Tada atributams liudyti gali būti naudojamas atskiras sertifikatas (*Attribute certificate* – AC). Šis sertifikatas skirtas susieti subjektą su jo atributais, viešasis raktas jame neskelbiamas (tam yra PKC).

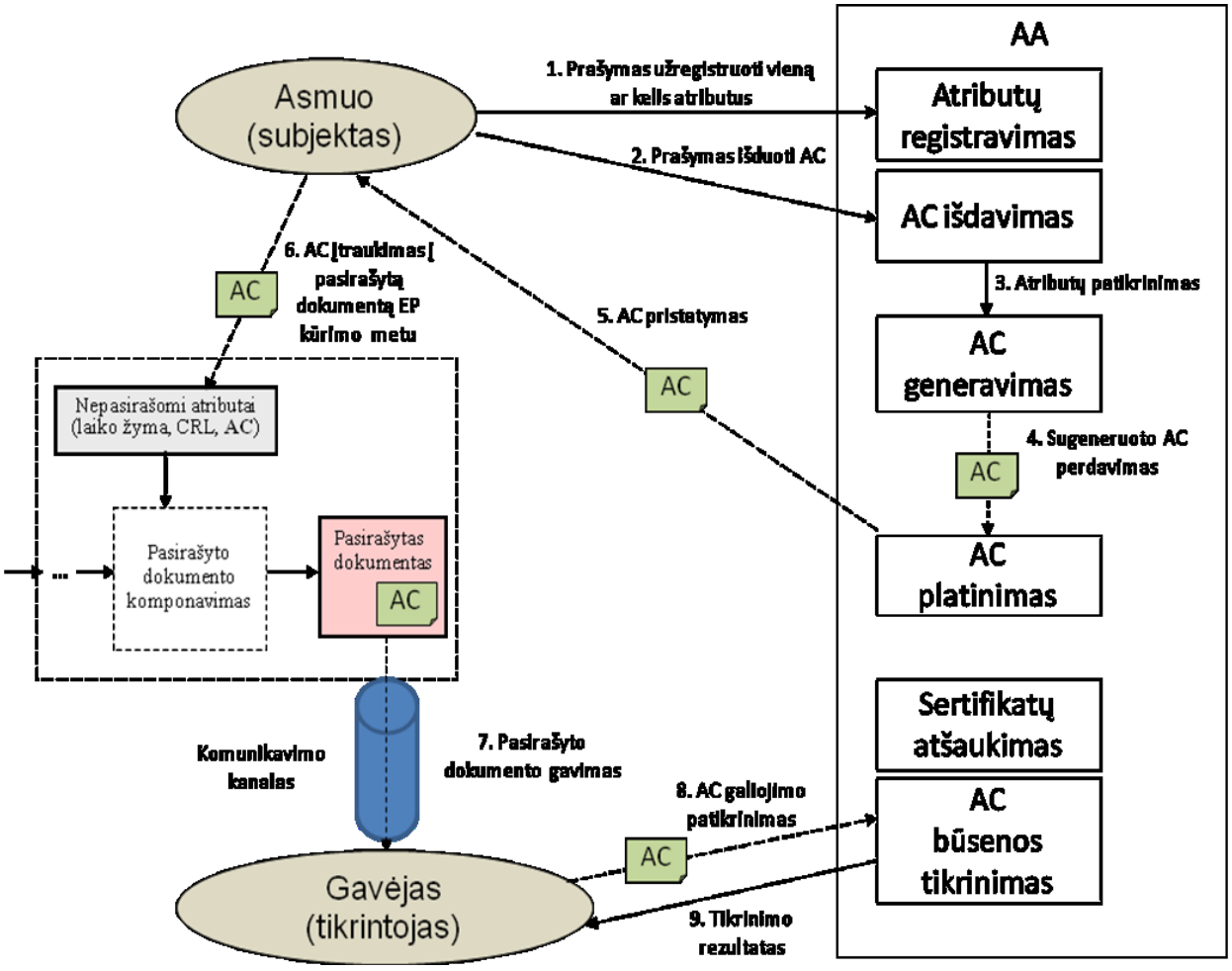
AC gali būti išduodamas to paties sertifikatų centro, kuris išduoda PKC (toliau šis centras bus vadinamas tiesiog CA), arba specialiai tam įsteigtos įstaigos – atributinės informacijos sertifikavimo centro (*Attribute authority* – AA). Rekomenduojama atskirti šias dvi tarnybas, todėl toliau bus laikoma, kad visus AC išduoda AA.

Subjektas, prašydamas AA išduoti AC, turi įrodyti, kad pateikiama atributinė informacija yra teisinga. Skirtingiems atributams paliudyti gali būti reikalingi skirtingi AC, kuriuos vėlgi gali išduoti ta pati arba skirtingos AA. Išduodamas AC yra pasirašomas AA parašu – taip jam perleidžiama atsakomybė už atributų teisingumą.



4 pav. Parašo kūrimo informacinis modelis. Atributai sertifikuojami atskirame sertifikate

4 pav. pavaizduotame modelyje atributai su pasirašytais duomenimis susiejami nurodant papildomą sertifikatą – AC. Vienas AC gali liudyti kelis atributus, arba pasirašyto dokumento komponavime gali dalyvauti keli AC (priklausomai nuo SP nurodymų). AC duomenys (visas sertifikatas arba jo nuoroda) pridedami jau suformavus skaitmeninį parašą – tai subjekto **nepasirašomi atributai** (tokie, kaip laiko žyma ar CRL). PKC (arba jo nuoroda) įtraukiamas į **pasirašomus atributus**, kaip įprastai.



5 pav. AC perdavimo tikrintojui *push* modelis

Tikrintojas, gavęs pasirašytą dokumentą, turi atlikti du patikrinimus. Pirmasis yra tapatybės nustatymas (įprasta procedūra tikrinant PKC). Antrasis yra atributų patikrinimas – tikrintojas turi įsitikinti, ar pasirašytame dokumente nurodyti reikalingi AC. Kokie AC turi būti įtraukti į pasirašytą dokumentą, kaip nepasirašomi atributai, nurodo SP. Tikrintojas patikrina ar visi AC yra galiojantys (nebuvo atšaukti). Modelio privalumai:

1. Galimybė atributinę informaciją keisti ir atšaukti nesukeliant pakeitimų PKC.
2. Nesikeičia CA veikla ir atsakomybės.
3. Į pasirašytą dokumentą gali būti įtraukiami įvairūs AC. Skirtingos SP gali reikalauti skirtingų atributų patvirtinimo, tam išpildyti nereikia kurti papildomų PKC.
4. Nesikeičia EP formatas, į pasirašytus duomenis pridedamas tik vienas papildomas nepasirašomas atributas.

Modelio trūkumai:

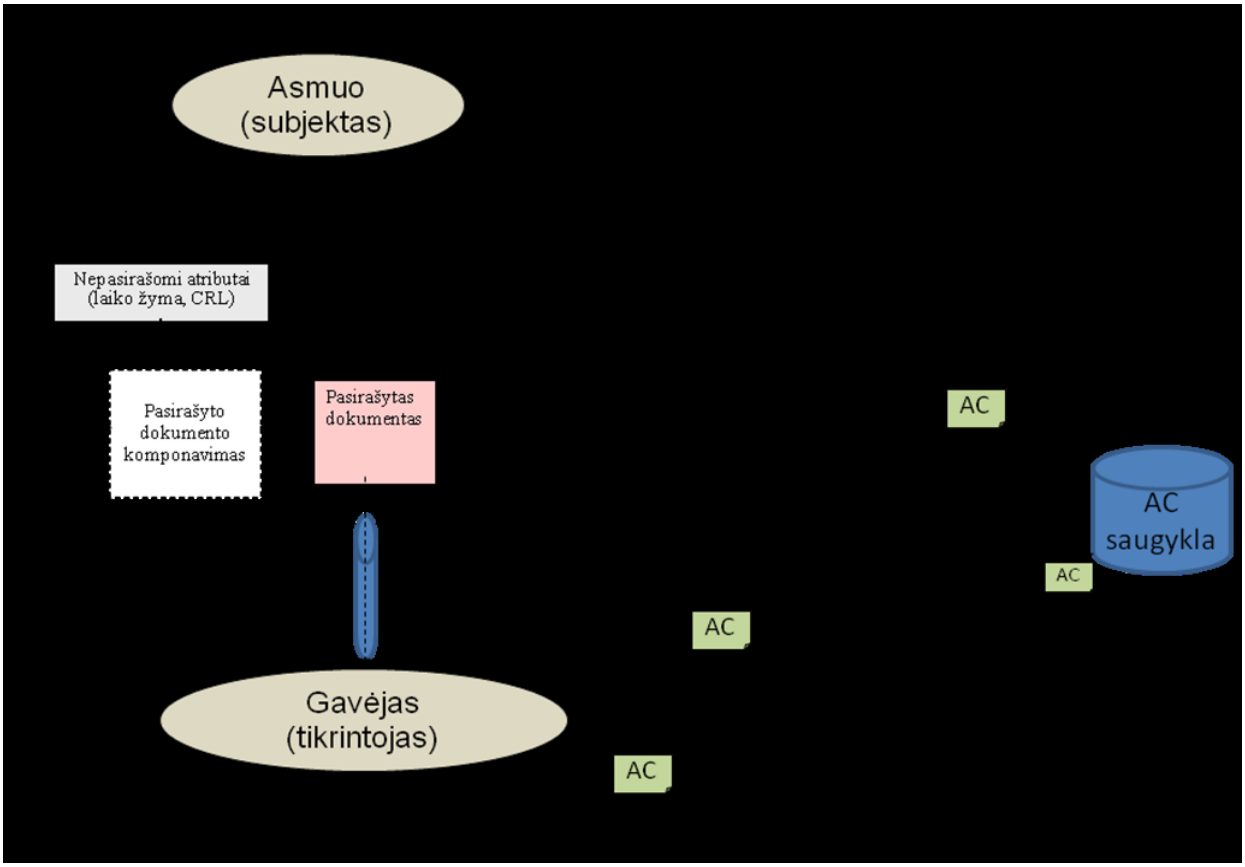
1. Sudėtingesnė infrastruktūra – reikalinga papildoma tarnyba (AA), kuri turi apsibrėžti savo nuostatus, užtikrinti patikimumą, gebėti išduoti ir atšaukti AC, bei suteikti informaciją apie jų galiojimą.

2. Sudėtingesnė tikrinimo procedūra. Tikrintojui reikia tikrinti ir PKC, ir AC galiojimą.
3. Papildomi veiksmai parašo kūrimo procedūroje – kiekvieną kartą kuriant EP reikia parinkti reikiamus AC ir juos įtraukti į nepasirašomus EP atributus. Be to, jei su kiekvienu pasirašytu dokumentu siunčiama ne AC nuoroda, o visas sertifikatas, itin padidėja komunikavimo kanalo apkrova (5 pav.).

2.4. Atributai atskirame sertifikate („pull“ modelis)

Šis modelis nuo prieš tai nagrinėto skiriasi tuo, kad tikrintojas gauna AC informaciją ne iš pasirašytų duomenų, bet autentifikavęs subjektą savarankiškai kreipiasi į AA, prašydamas suteikti reikiamo subjekto AC. Nors EP formavime AC nedalyvauja, pasirašantysis vis vien turi iš anksto pasirūpinti, kad AA jam išduotų reikiamus AC. Skirtingais atvejais gali reikėti skirtingų rinkinių – juos nurodo SP. Pavyzdžiui, jose gali būti numatyti tokie atvejai:

- pasirašant paprastas sutartis AC išvis netikrinami;
- pasirašant pinigų perdavimo aktus reikia AC, liudijančio subjekto pareigas;
- pasirašant rekomendacijas reikia turėti AC, kuriame nurodytas priklausymo organizacijai atributas.



6 pav. AC perdavimo tikrintojui *pull* modelis

Šio modelio privalumai:

1. EP kūrėjui nereikia rūpintis AC įdėjimu į pasirašytus duomenis.
2. Nesikeičia EP formatas ir pasirašytų duomenų struktūra. Komunikacijos kanalu tarp subjekto ir tikrintojo nesiuntinėjami AC duomenys.

Modelio trūkumai:

1. Tikrintojui, gavus pasirašytus duomenis, reikia kreiptis į AA, kad gautų subjekto AC.
2. AA reikia ne tik saugoti išduotus AC, bet ir sugebėti atlikti paieškas AC saugykloje pagal subjekto tapatybės (ar kitokius) duomenis.

Iš tikrųjų tikrintojas bet kokiu atveju turės kreiptis į AA, nes jam reikės patikrinti AC galiojimą. Tačiau naudojantis AC būsenos tikrinimo paslauga dažniausiai prašoma pateikti visą subjekto AC (arba jo nuorodą), bet ne subjekto tapatybės duomenis (ar kitą parametrą). *Push* modelyje tikrintojas gauna AC arba jo nuorodą kartu su pasirašytu dokumentu. Tuo tarpu *pull* modelyje tikrintojas šių duomenų kartu su pasirašytu dokumentu negauna, todėl naudojasi AC platinimo paslauga, teikdamas užklausą gauti reikiamo AC informaciją pagal subjekto duomenis, viešojo rakto ID, ar kitus parametrus (SP turi būti nutarta, su kuo siejami AC: ar su subjekto tapatybe, ar su subjekto PKC nurodytu viešuoju raktu, ar su PKC identifikatoriumi) [PS00, 124-125].

Toks modelis tinkamas uždarose aplinkose, kai sertifikavimu užsiima vidinė tarnyba (pavyzdžiui, įmonė turi įsteigusi savo CA ir AA). Tada dažnesnis tikrintojų komunikavimas su AA nesukelia problemų, o AC saugykloje saugomas nedidelis kiekis sertifikatų užtikrina greitą paiešką. Vykstant dažniems dokumentų mainams tarp subjektų ir tikrintojų, palaikoma nedidelė komunikavimo kanalo apkrova. Tikrintojai, dažnai komunikuodami su tam tikrais subjektais, gali vieną kartą pasinaudoję AA teikiama AC platinimo paslauga, subjektų AC informaciją išsisaugoti trumpalaikėje atmintyje ir taip vėliau sutaupyti laiko (nebereikės kreiptis į AA dar kartą).

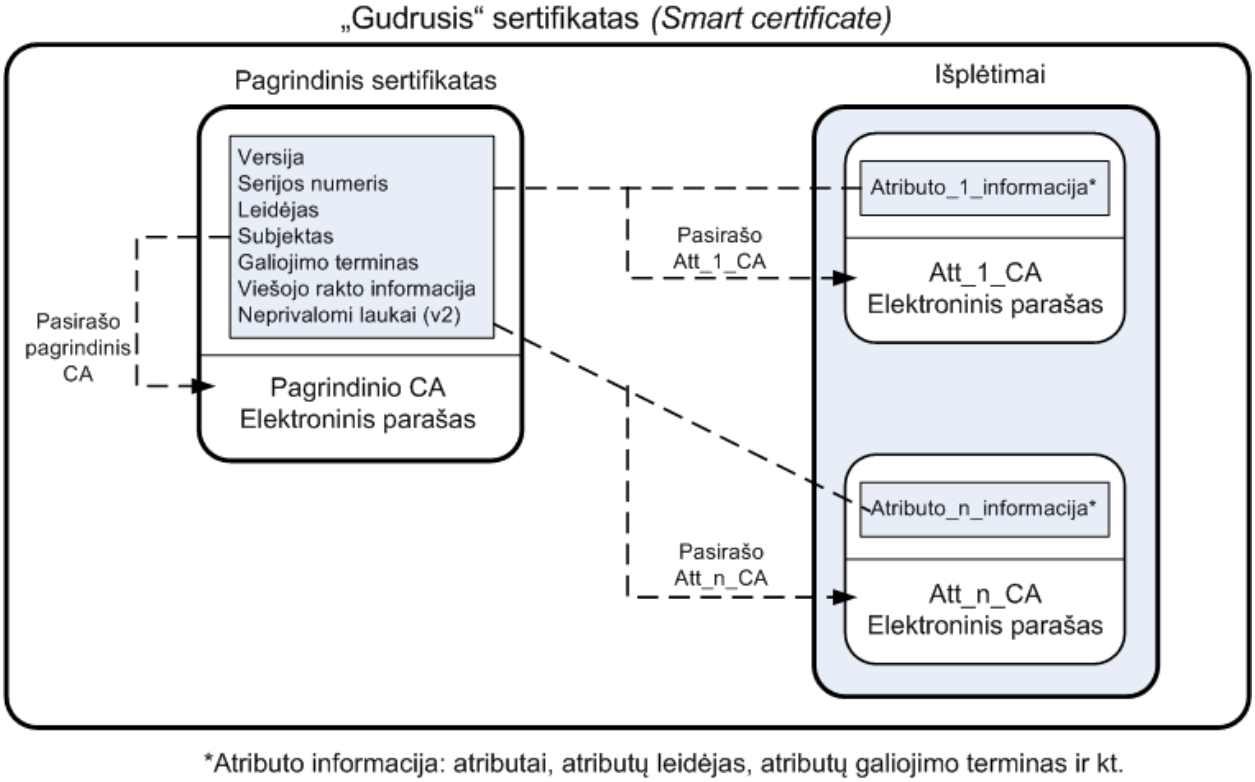
2.5. Kiti atributų sertifikavimo sprendimai

Tarp dviejų kraštutinių AI sertifikavimo variantų (vienas - įvesti AA bei griežtai atskirti CA ir AA, kitas – nenaudoti AC, atributų liudijimą patikėti CA) egzistuoja ir "tarpinių" sprendimų, kurie gali būti lengvai pritaikomi kai kuriose situacijose.

2.5.1. Smart certificates

Smart certificates, pristatyti [PS99], yra suderinami su X.509, nes išlaiko tą patį duomenų formatą. 7 pav. pavaizduotus atributus pasirašo skirtingi AA (paveikslėlyje jie įvardinti kaip Att_n_CA). Atributai susiejami su pagrindiniu sertifikatu, panaudojant išplėtimo laukus (*extensions*). Po to, kai CA išduoda asmeniui pagrindinį X.509 sertifikatą, AA prideda atributus

išplėtimo lauke, dar kartą pasirašo pradinį sertifikatą (kartu su atributais) ir šį parašą įdeda į kitą, specialiai tam skirtą išplėtimą. Šiuos veiksmus kelis kartus gali atlikti kelios skirtingos AA. Tikrinimo metu pirmiausia verifikuojamas pagrindinis sertifikatas (atliekama autentifikacija) ir tik to po tikrinami AC.



7 pav. Atributų pasirašymas Smart certificate struktūroje [PS99, 7]

Smart certificates įgalina prižiūrėti viešųjų raktų ir atributų informaciją nepriklausomai. Pavyzdžiui, jei subjekto atributai, išduoti vienos AA, yra atšaukiami arba pasibaigia jų galiojimo laikas, kitų atributų ir raktų poros informacija lieka galiojanti. Jeigu pasibaigia pagrindinio sertifikato galiojimo laikas, arba sertifikatas atšaukiamas, visi jo atributai tampa bereikšmiai. Be to, nors teoriškai SC leidžia kontroliuoti atributų ir viešųjų raktų informaciją skirtingoms tarnyboms nepriklausomai, apjungus šias tarnybas į vieną sistemos valdymas tampa paprastesnis.

2.5.2. FlexiCert

Publikacijoje [LZ03] apibrėžiama dar viena X.509 sertifikatų klasė, pavadinta *FlexiCert*. Šie sertifikatai įgalina atributinę informaciją saugiai ir efektyviai pridėti prie tapatybės sertifikato jo galiojimo periodu (taip iš karto išsprendžiant sertifikatų suspendavimo, atnaujinimo ir atšaukimo klausimus).

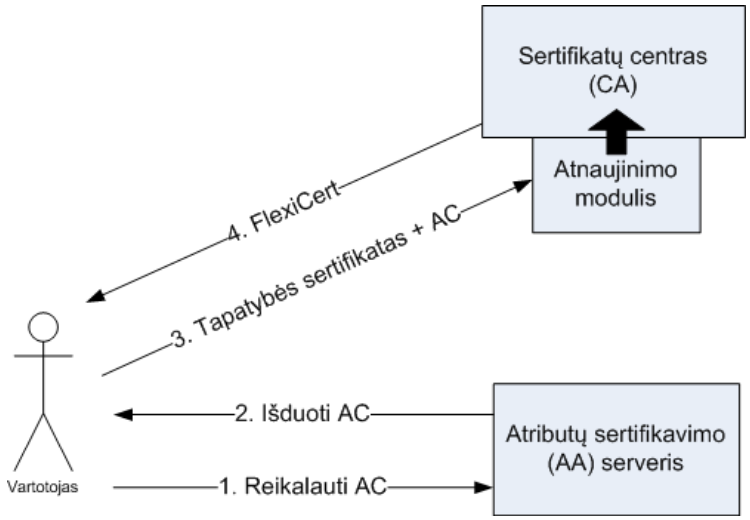
FlexiCert sukurtas remiantis NewPKI [LZ03, 2]. NewPKI pristatoma kaip viešųjų raktų struktūra, kurios palaikymui nereikia išreikštinai rūpintis atšaukimo (*revocation*) klausimais. Maksimalus sertifikato galiojimo laikas padalinamas į trumpus intervalus. Pagal sertifikato

savininko (arba jo viršininko) pageidavimą, sertifikato galiojimas gali būti nutraukiamas ties kiekvieno intervalo pabaiga. Tokio sertifikato tikrintojams nereikia papildomai kreiptis į CA dėl sertifikatų atšaukimo informacijos pateikimo (CRL ar OCSP). Sertifikato turėtojui, norinčiam išlaikyti savo sertifikato galiojimą, suteikiama galimybė kas tam tikrą laiką atnaujinti sertifikato galiojimo pabaigos datą. Norint, kad sertifikatas nebegaliotų, užtenka nebeatlikti šio veiksmo.

Tokia schema gerai pasiteisina verslo srityse, kur CA ir AA yra žinomos viena kitai ir CA leidžiama sertifikuoti AA tapatybę [LZ03, 4]. Pavyzdys: organizacijoje tapatybės sertifikatus išduoda centralizuota CA, o atributų priskyrimu subjektams rūpinasi kelios AA, kurios siejamos su skirtingais organizacijos padaliniais.

Kaip įprasta, X.509 tapatybės sertifikatai dažniausiai nėra modifikuojami per visą savo galiojimo laikotarpį, todėl jo negalima pildyti atributais. Be to, CA dažniausiai neprisiima atsakomybės už jos tiesiogiai nekontroliuojamų atributų atšaukimo valdymą. Tačiau [LZ03, 4] teigiama, kad nemažinant saugumo galima modifikuoti tapatybės sertifikatą jo galiojimo laikotarpiu, jei tik CA palaiko tokią operaciją. Jei su sertifikatu susieto viešojo rakto galiojimas nekeičiamas, galima modifikuoti sertifikatą jo neatšaukiant ir neišduodant iš naujo.

Kokie atributai gali būti pridedami prie tapatybės sertifikato ir kas tokius atributus išduoda, nusprendžia CA. Pagal anksčiau pateiktą organizacijos pavyzdį, CA galės pridėti tuos atributus, kuriuos išduos kitų padalinių AA. Tokiu atveju AC praranda savo paskirtį susieti atributus su tapatybe ir yra naudojami tik atributų, išduotų AA perdavimui CA. Tapatybės sertifikatų atnaujinimu rūpinasi specialus CA modulis. Atnaujinimo modulio veikimo schema pavaizduota 8 pav.



8 Pav. Sertifikatų atnaujinimo procesas [LZ03, 4]

Vartotojas, gavęs AC iš AA, gali jį kartu su tapatybės sertifikatu pateikti šiam moduliui. Tada bus atliekami tokie veiksmai:

1. Atnaujinimo modulis patikrins ar tapatybės sertifikatas vis dar galioja ir buvo išduotas CA, kuriai priklauso atnaujinimo modulis.
2. Modulis patikrins, ar AC buvo išduotas patikimos AA ir ar pateikiamas atributas prisilaiko NewPKI atributų struktūros.
3. Jei tikrinimas praėjo sėkmingai, sukuriamas ir vartotojui grąžinamas naujas FlexiCert sertifikatas, kuriame:
    - išsaugoma visa tapatybės sertifikato informacija;
    - tapatybės sertifikatas išplečiamas pridedant NewPKI atributą;
    - modifikuotam sertifikatui sukuriamas parašas.

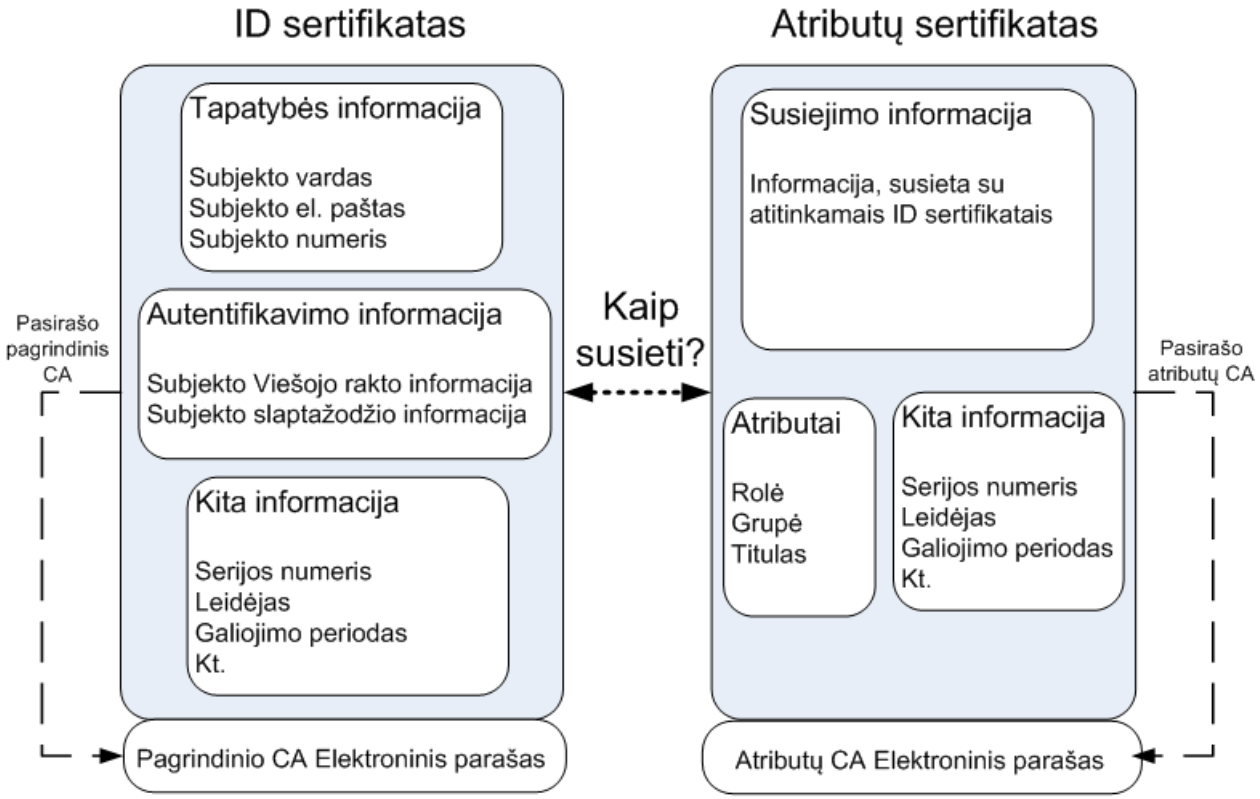
Jei prireikia atšaukti kurį nors atributą, jį išdavusi AA nustoja atnaujinti AC. Atnaujinimo procesas gali būti pakoreguotas taip, kad į atnaujinimo modulį vartotojui nereikėtų perduoti abiejų sertifikatų. AA, išdavusi AC, gali kitu žingsniu jį pati pateikti CA atnaujinimo moduliui. Tačiau tai pasiteisina tik CA ir AA esant vienos organizacijos ribose, nes šios tarnybos tampa susietos ir nebelieka galimybės AA išduotų AC perduoti į kitos organizacijos CA.

Taigi esminė *FlexiCert* savybė yra gebėjimas pernešti atributinę informaciją nenaudojant AC. Kiti FlexiCert privalumai [LZ03, 5]:

- Paprastesnis valdymas tiek vartotojui tiek aplikacijai. Naudojamas tik vienas X.509 sertifikatas vietoje kelių.
- CA dalyvauja atributų, įtraukiamų į tapatybės sertifikatą, patvirtinime. Tikrinant sertifikatus užtenka kreiptis į vienintelę patikimą trečiąją šalį – CA.
- Automatiškai valdomas atributų atšaukimas, kadangi atributai laikosi NewPKI formato.
- Nereikia modifikuoti naudojamų protokolų, kad jie gebėtų perduoti atributų sertifikatus. Komunikuojama tik tapatybės sertifikatais.

2.6. Tapatybės ir atributų sertifikatų susiejimo būdai

Jei atributinė informacija sertifikuojama naudojantis AC, reikia nuspręsti, kokiu būdu šis sertifikatas bus susietas su „identifikaciniu“ PKC. *Smart certificates* autorių straipsnyje [PS00] išskiriami trys metodai, nurodantys, kaip galima susieti PKC, skirtus pasirašančiojo tapatybei nustatyti (PKC šiame skyriuje bus vadinamas “ID sertifikatu”), ir AC, skirtą jam priskirtų atributų galiojimo patikrinimui. Susiejimo klausimas detalizuotas 3 pav.



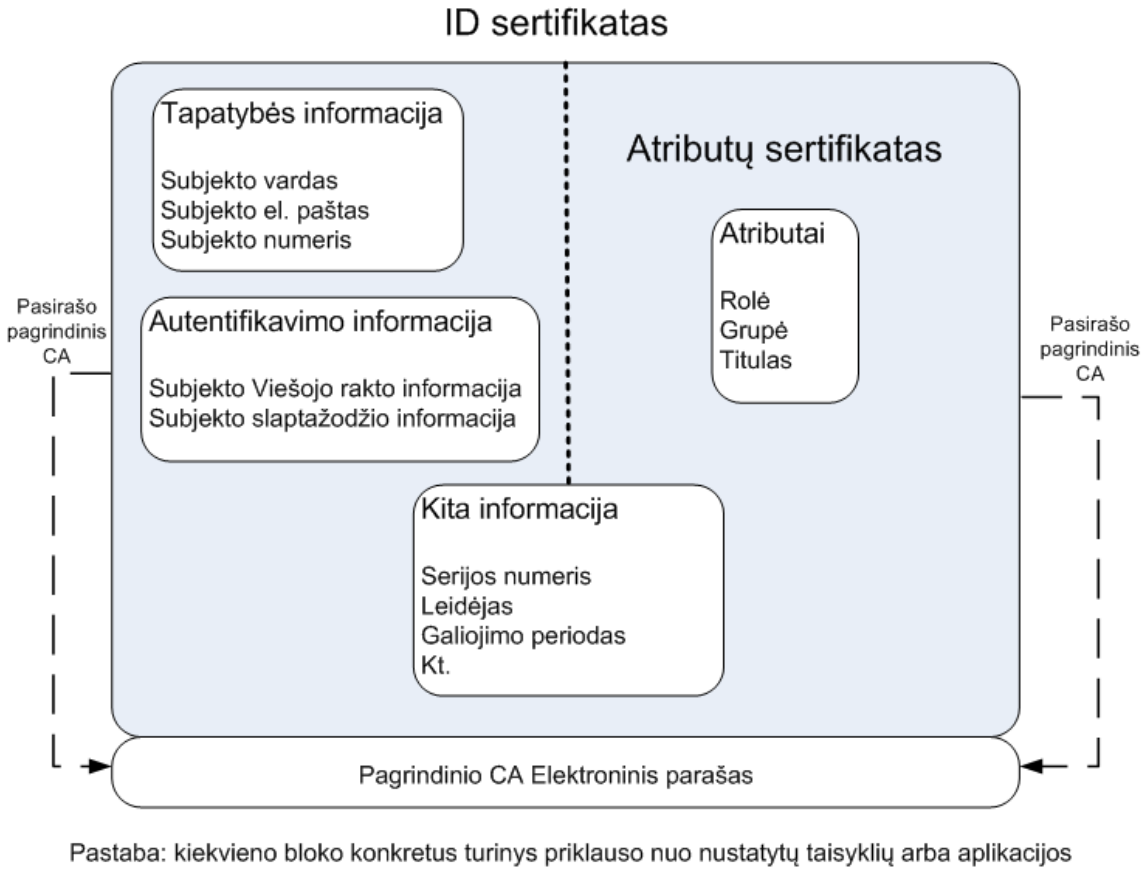
9 pav. ID sertifikato, AC struktūra ir jų susiejimo problema [PS00, 122]

ID sertifikate ir AC esanti informacija 9 pav. padalinta į blokus pagal savo pobūdį. Tapatybės (*identity*) ir autentifikacijos (*authentication*) blokai yra neatsiejama ID sertifikato dalis. Kita informacija (*other info*) yra neprivaloma. Visa ID sertifikato viršutinėje dalyje esanti informacija pasirašoma CA (3 pav. ši tarnyba pavadinta ID CA). Atributų sertifikatas pats savaime neturi prasmės, todėl jame būtinai turi būti apibrėžta, kaip jis siejamas su ID sertifikatu. Dažniausiai AC yra susiejamas su X.509 atitinkančiu ID sertifikatu pagal subjekto vardą ir ID sertifikato (kuriame nurodytas subjekto viešasis raktas) serijos numerį. ID sertifikatas ir AC gali būti komplektuojami į vieną rinkinį arba laikomi atskirai. Vieno rinkinio variantas supaprastina transakcijas, nes tokį sertifikatą galima naudoti tiek autentifikavimui tiek autorizavimui. Taip pat nekyla problemų tokį sertifikatą pradėti naudoti sistemose, palaikančiose tik ID sertifikatus.

Toliau apžvelgiami trys metodai tapatybės ir atributų susiejimui: *monolitinį, autonominį* ir *grandininį* [PS00, 123]. Autonominis metodas leidžia pasirinkti, kokios ID sertifikate esančios informacijos rinkinys bus naudojamas susiejimui su atributų sertifikatais.

2.6.1. Monolitiniai parašai

Jei kontroliuoti tapatybę ir atributus leidžiama tai pačiai tarnybai, ji gali abu informacijos rinkinius pasirašyti vienu parašu. Tokio parašo pavyzdys pateikiamas 10 pav.



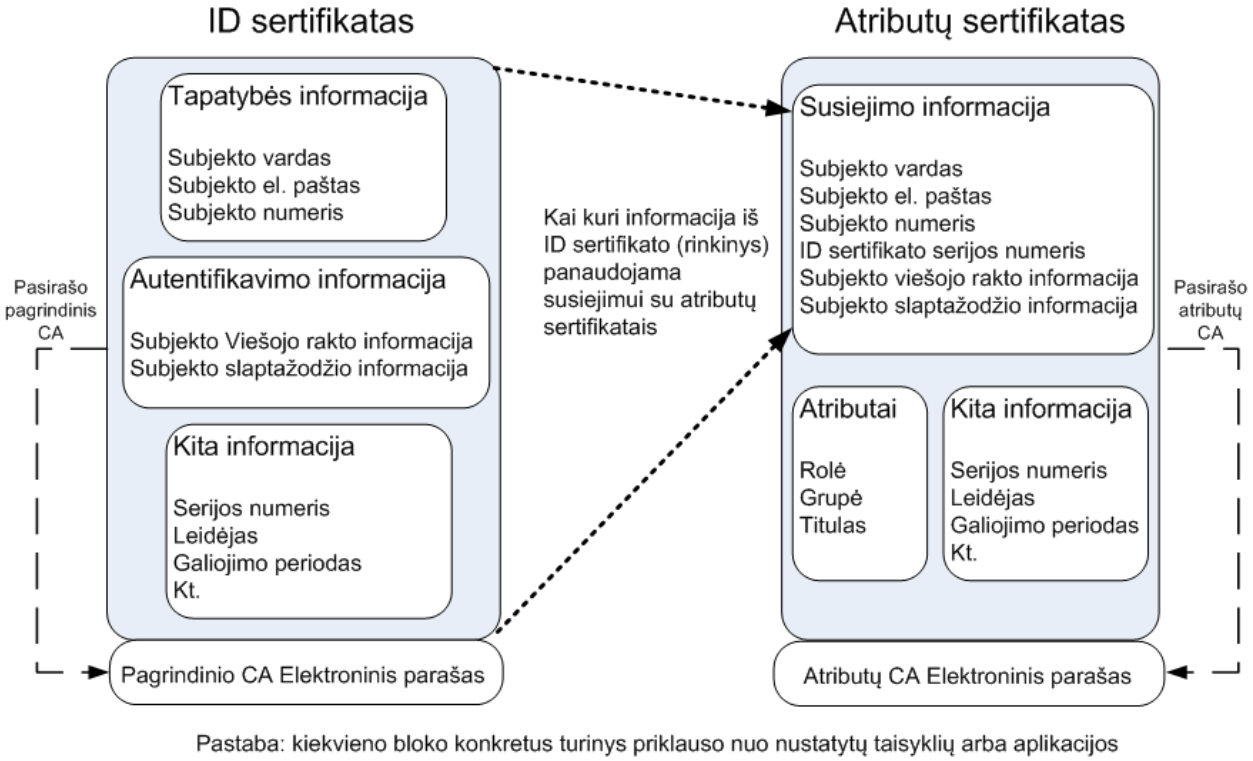
10 pav. Monolitinio parašo schema [PS00, 123]

Kadangi tapatybės ir atributų informacija saugoma viename sertifikate, leidžiama "kitos informacijos" blokus iš ID sertifikato ir AC apjungti į vieną. Toks sertifikatas pasižymi didele tapatybės ir atributų sankiba (*tightly-coupled*), t.y. išdavus tokį sertifikatą, jame esanti informacija negali būti keičiama, nebent išduodamas naujas sertifikatas. Monolitinio sertifikato privalumas yra toks, kad sistemą, naudojančią tokius sertifikatus lengva valdyti. Užtenka patikrinti vienintelės CA parašą, kad būtų įsitikinta sertifikato galiojimu.

Tačiau monolitiniai parašai nepalaiko kelių tarnybų varianto. Jei prireikia nepriklausomai kontroliuoti kiekvieną informacijos tipą (pvz., tapatybę, mokyklos atributą, kompanijos atributą ir kt.) ir šiai informacijai suteikti skirtingus galiojimo terminus, toks parašas nepasiteisina. Taigi, dėl padidėjusio patogumo sumažėja lankstumas.

2.6.2. Autonominiai parašai

Tokiuose parašuose leidžiamas kelių sertifikavimo tarnybų dalyvavimas ir palaikomas skirtingas tapatybės ir atributų galiojimo laikotarpis. ID sertifikatą sukuria ir pasirašo CA, tada įvairios AA gali kurti ir pasirašinėti AC, bei juos susieti su tapatybės sertifikatu pagal pasirinktą informacijos rinkinį (*binder*) iš šio sertifikato. Autonominio parašo schema pavaizduota 11 pav.



11 pav. Autonominio parašo schema [PS00, 124]

Susiejimo informacijos rinkinys dažniausiai sudaromas iš subjekto vardo arba ID sertifikato serijos numerio. Kitokie rinkiniai, pavyzdžiui, subjekto viešasis raktas, viešojo rakto santrauka, užšifruotas slaptažodis ar jo santrauka, taip pat leidžiami. Aplikacijos parenka susiejimo informacijos rinkinius pagal savo dalykinę sritį. Nors šio parašo esmė yra autonomiškumas, techniniu ir fiziniu požiūriu tapatybės ir atributų sertifikatai vistiek gali būti komplektuojami kartu.

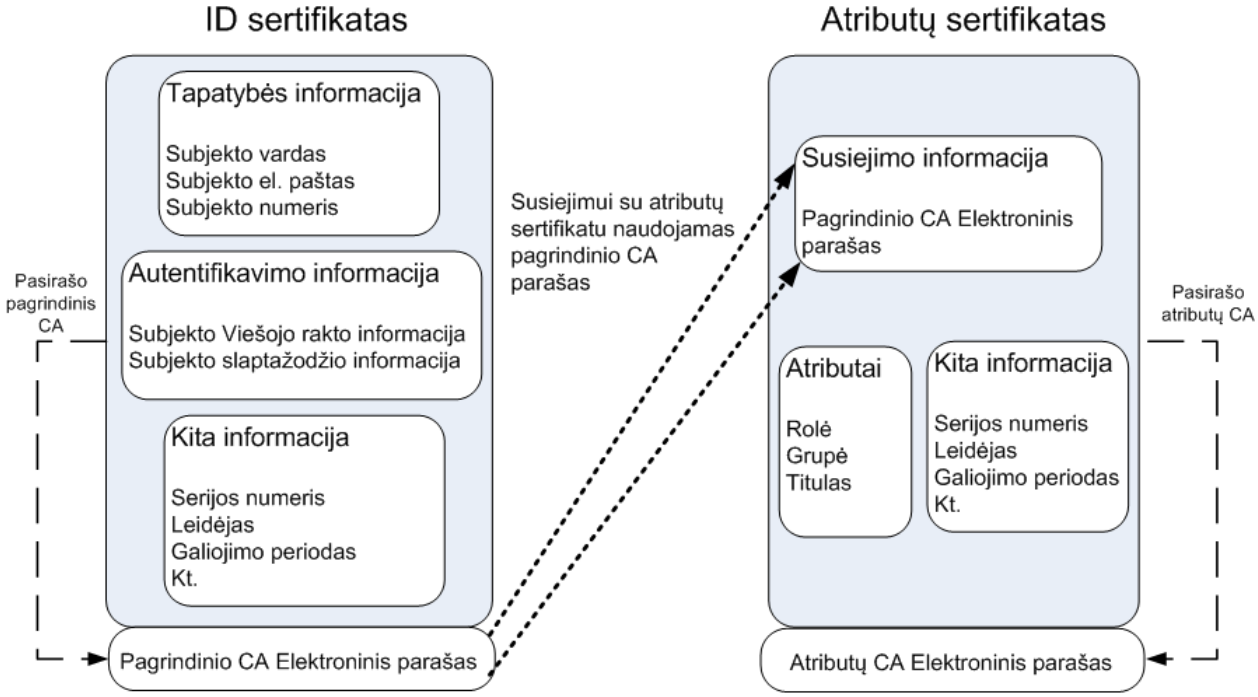
Skirtingos AA gali pasirinkti skirtingus informacijos rinkinius iš tapatybės sertifikato susiejimui su AC. Tarkime, vienam asmeniui CA sugeneravo ir pasirašė ID sertifikatą. AA, atsakinga už, pavyzdžiui, mokslinio laipsnio atributus, išduoda AC, kurio atributų lauke įrašytas asmens mokslinis laipsnis. Taip pat AC nurodomas šio atributo galiojimo periodas ir informacijos rinkinys, naudotas susieti AC su ID sertifikatu (schemoje – “Binder info”). CA parašo reikšmės į šį rinkinį įtraukti neleistina, nes kitaip būtų gautas grandininio parašo atvejis (aprašytas tolimesniame skyrelyje). Taigi, sakykime, susiejimo informacijos rinkinui sudaryti parenkamas asmens viešasis raktas. Tada į “Binder info” bloką įtraukiama asmens viešojo rakto informacija, kuri buvo nurodyta ID sertifikate, ir visai AC informacijai sugeneruojamas AA parašas. Kita AA tarnyba, tarkime, atsakinga už pareigų kompanijoje atributą (sakykime asmens pareigos yra “vadybininkas”), kurdama savo AC gali pasirinkti kitą susiejimo informacijos rinkinį, pavyzdžiui, ID sertifikato serijos numerį.

Taigi AC susiejamas ne su konkrečiu ID sertifikatu, o tik su dalimi juose esančios informacijos. Todėl, jeigu susiejimui buvo pasirinkta informacija, kuri nesikeičia kuriant skirtingus ID sertifikatus tam pačiam asmeniui, AC tikrinimas įgyja tam tikrų niuansų. Tarkime, susiejimui buvo pasirinktas tik asmens slaptažodis. Tuomet tikrinant AC, pirmojo žingsnio (autentifikavimo) metu galima naudoti **bet kurį** iš asmens turimų ID sertifikatų, jei tik juose nurodytas tas pats slaptažodis. Ši autonominio parašo savybė gali būti tiek pageidautina, tiek vengtina, priklausomai nuo aplikacijos dalykinės srities. Todėl susiejant AC su ID sertifikatu, būtina apgalvoti, koks informacijos rinkinys bus naudojamas susiejimui.

Kadangi autonominiame paraše naudojamas tik informacijos, patalpintos ID sertifikate, poaibis, toks parašas yra silpnai sukibęs (*loosely-coupled*). Keičiantis ID sertifikato informacijai, atributų sertifikatai išlieka galiojantys, nebent pasikeičia ta tapatybės sertifikato informacija, kuri buvo panaudota susieti jį su AC. Taigi, autonominis parašas yra lankstesnis nei monolitinis ar toliau aprašytas grandininis.

2.6.3. Grandininiai parašai

Kaip ir autonominiai, šie parašai palaiko skirtingus tapatybės ir atributų galiojimo laikus, taip pat nepriklausomas CA ir AA tarnybas. Tačiau kaip ir monolitinių parašų atveju, jie sukuria stiprią sankibą (*tightly-coupled*) tarp tapatybės ir atributų. Grandininio parašo schema pateikiama 12 pav.



Pastaba: kiekvieno bloko konkretus turinys priklauso nuo nustatytų taisyklių arba aplikacijos

12 pav. Grandininio parašo schema [PS00, 125]

AC susiejimui su ID sertifikatu yra naudojamas vieno iš asmens ID sertifikatų parašas. Taigi visos AA, kurios kurs ir pasirašinės AC, jų susiejimui su ID sertifikatu privalės naudoti tą pačią informaciją – CA parašą. Ši būtinybė palengvina atributų tikrinimą – nereikia papildomai nagrinėti kiekvieno AC struktūros ir aiškintis, koks informacijos rinkinys buvo naudojamas susiejimui su ID sertifikatu. Taip pat kiekvienas AC susiejamas su **vieninteliu** ID sertifikatu – nelieka tikimybės, kad tikrinant atributinę informaciją jos galiojimas priklausys nuo to, koks ID sertifikatas bus pateiktas autentikacijai. Tačiau bent šiek tiek pasikeitus ID sertifikato informacijai, jam naujai sukurtas CA parašas nebeatitiks to, kuris buvo nurodytas visuose AC (susiejimui su ID sertifikatu).

Kai tapatybė ir atributai fiziškai saugomi tame pačiame rinkinyje, tokio sertifikato suradimas (*discovery*) yra ganėtinai lengvas. Suradimo sudėtingumas išauga, jei ID sertifikatas ir AC saugomi ne tame pačiame rinkinyje, nes tokiu atveju reikia papildomai ieškoti nuorodomis susietų sertifikatų. Apibendrintas aptartų schemų palyginimas pateikiamas 1 lentelėje.

1 lentelė. Monolitinių, autonominių ir grandininių parašų palyginimas [PS00, 126]

	Monolitinis parašas	**Autonominis parašas**	**Grandininis parašas**
Sertifikavimo tarnybos	Vienintelė	Galimos kelios	Galimos kelios
ID sertifikatų ir AC galiojimo periodas	Būtinai toks pats	Gali būti skirtingas	Gali būti skirtingas
Sankiba	Stipri	Silpna	Stipri
Sertifikato suradimas	Lengvas	Vidutinio sudėtingumo	Sudėtingas
Pakartotinis panaudojamumas	Mažas	Didelis	Vidutinis

3. Pavyzdinis PKI naudojimo modelis

Viešojo rakto infrastruktūra (PKI) naudojama įvairiais mastais. Paprastu atveju PKI gali būti įdiegta įmonės viduje, siekiant užtikrinti duomenų apsaugą. Žvelgiant plačiau, PKI gali būti pritaikyta didesnei vartotojų grupei, pavyzdžiui, suteikiant galimybę valstybės gyventojams pasirašinėti dokumentus EP ar autentifikuotis bankinėse sistemose.

Šiame skyriuje pateikiamas vienas iš PKI pritaikymo variantų. Atsižvelgiant į praktinį EP taikymą Lietuvoje, kuriamas PKI naudojimo modelis, kuriame apibrėžiama EP vartotojų grupė, jos poreikiai, sertifikavimo centro (CA) veikla ir naudojamos EP taisyklės.

3.1. Lietuvos skaitmeninio sertifikavimo centrai ir jų paslaugos

Paprastas būdas susidaryti vaizdą apie realią PKI naudojimo situaciją yra aplankyti sertifikavimo paslaugų teikėjų internetines svetaines ir pasidomėti, kokias paslaugas jie teikia. Į IVPK skelbiamą Lietuvos Respublikos prižiūrimų ir/ar akredituotų sertifikavimo paslaugų teikėjų „Patikimą Sąrašą“ [IVP11] šie CA:

- VĮ Registrų centro Sertifikatų centras (RCSC);
- gyventojų registro tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos sertifikatų tvarkymo skyrius;
- UAB „Skaitmeninio sertifikavimo centras“ (SSC).

RCSC siūlomos paslaugos „leidžia vartotojams nustatyti savo tapatybę, pasirašyti bei patikrinti pakeistus duomenis dokumente, identifikuoti asmenį elektroninėje erdvėje“ [RSC11]. Šios paslaugos tiekiamos valstybiniu mastu, RCSC registravimo tarnybos veikia visuose Lietuvos rajonuose. Šis CA teikia išduoda bei kontroliuoja PKC, o vartotojams kuriant EP dar ir dalyvauja PKI kaip laiko žymos tarnyba (TSA). RCSC klientai, įsigiję PKC, gali saugiai identifikuotis kai kuriuose el. paslaugų portaluose (www.evaldzia.lt, deklaravimas.vmi.lt ir kt.), bei pasirašinėti PDF dokumentus EP.

Gyventojų registro tarnyba savo paslaugų aprašyme akcentuoja piliečiams išduodamas asmens tapatybės korteles, kuriose įrašomi du sertifikatai – asmens atpažinimo elektroninėje erdvėje sertifikatas, bei kvalifikuotas sertifikatas EP tvirtinti [GRT11]. Nors tapatybės kortelės išduodamos visiems valstybės gyventojams, kvalifikuotus sertifikatus ši tarnyba nuo 2009 m. išduoda siauresnei vartotojų grupei - valstybės tarnautojams.

SSC svetainėje teigiama, kad šis centras šiuo metu yra pagrindinis ir vienintelis sertifikavimo paslaugų teikėjas Lietuvoje [SSC11]. Ši įstaiga nuo 2005 m. IVPK yra užregistruota kaip kvalifikuotas sertifikavimo paslaugų tiekėjas tiekti kvalifikuotas sertifikavimo

paslaugas. SSC yra įgyvendinusi valstybinio masto asmens autentifikavimo sprendimus (www.vmi.lt, www.sodra.lt ir kt.), taip pat teikia virtualių PKI diegimo įstaigose paslaugas.

Galima sakyti, kad praktikoje laikomasi principo turėti kelis patikimus sertifikavimo centrus (CA), kurie aptarnauja dideles vartotojų grupes. Atsižvelgiant į šią realią PKI naudojimo situaciją, toliau konstruojamas pavyzdinis PKI naudojimo modelis vaizduoja tariamos organizacijos vartotojų grupę, kuriai aktualus saugus vidinis komunikavimas ir kuri naudojasi viešomis sertifikavimo paslaugomis.

3.2. PKI taikymo apimtis

Tarkime, kad turime vidutinę vartotojų grupę (pavyzdžiui, vidutinio dydžio įmonė ir jos darbuotojai), kurioje PKI naudojama autentifikuotis įmonės informacinėje sistemoje bei pasirašinėjant elektroninius dokumentus (kuriant ir tikrinant EP). Vartotojas, norėdamas pasinaudoti šiomis galimybėmis, privalo turėti jam išduotą kvalifikuotą sertifikatą (šis sertifikatas susieja asmens tapatybę su jo viešuoju raktu, todėl ir toliau bus vadinamas PKC). Teoriškai sertifikavimo paslaugų tiekėjų gali būti keletas, be to, kai kurie iš jų gali sudaryti sertifikavimo paslaugų grandines, t. y. aukštesnio lygio CA išduoti sertifikatus kitiems CA ir įgalioti juos teikti sertifikavimo paslaugas. Sekdami RCSC bei SSC pavyzdžiais iš praktikos, sutarkime, kad įmonė nutaria sertifikavimo paslaugas užsakyti iš **vienintelės** įstaigos – pavadinkime ją tiesiog CA. Šis patikimas sertifikatų centras pats sau išduoda sertifikatą, leidžiantį kurti PKC ir tampa „šakniniu“ CA.

Dėl paprastumo, laikysime, kad visi vartotojai yra fiziniai asmenys, todėl jų tapatybės nustatymo procedūra nėra komplikuota ir CA turi pakankamai įgaliojimų nustatyti bet kurio iš esamų ar naujų vartotojų tapatybę. Vartotojų tikslas, savaime suprantama, yra saugi komunikacija. EP naudojimo atveju laikysime, kad jis yra pasiektas, jei bet kuris EP gavėjas, tikrindamas pasirašiusiojo subjekto tapatybę, nėra suklaidinamas. Kitaip sakant, EP yra naudojamas tik autentiškumui patvirtinti. Vartotojų autentifikacija informacinėje sistemoje PKI naudojimo požiūriu yra panaši į EP kūrimo bei tikrinimo procedūras, todėl šių atvejų atskirai nenagrinėsime.

3.3. CA principai ir paslaugos

Sertifikavimo centro (CA) tikslas yra suteikti galimybę vartotojams naudotis kvalifikuotais sertifikatais. Jam pasiekti, CA užtenka teikti tokias paslaugas:

1. Registruoti asmenis, prašančius sudaryti sertifikatą, patikrinti jų tapatybę.
2. Sudaryti sertifikatus.
3. Tvarkyti sertifikatų duomenis.

4. Sustabdyti arba atšaukti sertifikatų galiojimą, gavus atitinkamą prašymą.
5. Teikti atšauktų sertifikatų duomenis EP tikrintojams.

Sekant SSC pavyzdžiu, modelyje turėtų dalyvauti vienintelis CA, kuris atšauktų sertifikatų duomenis teikia ne CRL pavidalu, bet naudoja OCSP (*Online Certificate Status Protocol*) [MAM99, 2] ir leidžia kiekvieno išduoto PKC būseną tikrinti realiu laiku.

Tarkime, kad vartotojų grupė yra parengusi sertifikato taisykles (*Certificate policy* – CP), kuriose nurodyta, kad naudojami PKC yra formato, pavaizduoto 2 lentelėje. Šis formatas gautas supaprastinus X.509 v3 standarte rekomenduojamą formatą [ETS01, 8].

2 lentelė. Pavyzdinio PKC laukai.

PKC	
Laukas	**Paaiškinimas**
Versija	Sertifikato versija.
Serijos numeris	Jį priskiria CA. Unikalus tarp visų PKC, išduotų CA.
Galiojimas	PKC galiojimo periodas.
Asmuo	Asmens tapatybės ID
Subjekto viešojo rakto informacija	Subjekto viešasis raktas
Parašo algoritmas	Algoritmas, kuris buvo naudojamas CA pasirašant šį PKC.
Parašo reikšmė	CA parašo, sugeneruoto pasirašant šį PKC, reikšmė.

Į šį formatą nebuvo įtraukti versijos ir leidėjo laukai. Dėl paprastumo tarkime, kad sertifikato versija yra nekintanti. PKC leidėjas šiame modelyje yra visada tas pats CA, todėl šis laukas taip pat nebūtinas. Dar dėl paprastumo subjekto viešojo rakto informacijoje nenurodomas algoritmas (ar jo identifikatorius), pagal kurį jis buvo sugeneruotas. Taip pat nenurodomas algoritmas, kurį naudoja CA, išduodama ir pasirašydama PKC. Laikysime, kad abiem atvejais taikomas vienas iš populiariausių algoritmų, pavyzdžiui, RSA.

Tarkime, kad CA yra paskelbusi vartotojų grupei savo veiklos nuostatus (*Certificate practice statement* – CPS), kuriose nurodyta, kad CA išduoda PKC, atitinkančius pasirinktos vartotojų grupės pageidaujamas CP. Laikysime, kad šios CP yra pripažįstamos ir taikomos plačiai, o CA CPS dokumentuoti pasirinktai įmonei priimtina tvarka. Detalus šių dokumentų turinys nepateikiamas.

3.4. Laiko žymos tarnyba

Kad būtų galima tvirtinti pasirašymo laiką, į šį modelį įtrauksime laiko žymos tarnybą (*Time stamping authority* – TSA). Jos pagrindinis tikslas yra generuoti laiko žymas, kurios pridedamos prie pasirašyto dokumento kaip vienintelis nepasirašomas atributas. Laikysime, kad

TSA atlieka savo funkcijas nepriekaištingai, ir kiekvienas sukurtas EP turi laiko žymos atributą (kaip nurodyta toliau aprašytose SP).

Sekant RCSC pavyzdžiu, galima būtų TSA sutapatinti su CA – laikyti, kad šis pagrindinis sertifikavimo centras ne tik išduoda PKC, bet ir išduoda laiko žymas vartotojams, kuriantiems EP. Nepaisant šio pavyzdžio, modelyje TSA ir CA laikysime atskiromis įstaigomis.

3.5. Parašo taisyklės

Tarkime, kad vartotojų grupė yra nutarusi naudotis vieneriomis SP. Jos yra parašytos laisvo teksto pavidalu, suprantamu žmonėms ir laisvai prieinamos internetu. Todėl kuriant EP, kad būtų paprasčiau, SP ar jų nuoroda į pasirašomus atributus nėra įtraukiamos. Kitaip sakant, šiame PKI naudojimo pavyzdiniame modelyje SP nurodomos **netiesioginiu būdu**. Kiekvienam (potencialiam) vartotojui leidžiama susipažinti su SP ir nuspręsti, ar jos yra priimtinos.

Kadangi vartotojų grupė yra vidutinė, SP gali būti pritaikytos naudoti tiek **uždaroje**, tiek **atviroje aplinkoje**. Dėl paprastumo, laikysime, SP naudojamos įmonės ribose, t. y. uždaroje aplinkoje.

Parašo taisyklės yra tinkamos įvairioms **vieno parašo** transakcijoms, t. y. SP leidžia tikrintojui priimti sprendimą, ar EP yra galiojantis, patikrinant vienintelį pasirašiusiojo nurodytą PKC.

Šiose SP nurodyta, kad pasirašantysis asmuo gali pasirašinėti tik **savo iniciatyva**, t. y. negali nurodyti, kad EP yra sukūręs vykdydamas tam tikras pareigas. Taip pat SP nurodyta, kad kartu su pasirašytu dokumentu subjektas neturi galimybės pateikti papildomos informacijos (pavyzdžiui, nurodyti savo rolę, privilegijas, priklausymą grupei, organizacijai ir kt.).

SP nurodo tokias parašo patvirtinimo taisykles:

1. Pasirašęs asmuo formuojamame paraše pateikia:
   - 1.1. Pasirašomus atributus:
     - 1.1.1. Pasirašomo dokumento formatą (tarkime, kad leidžiami tik vienintelio sutarto formato dokumentai, kaip, pavyzdžiui, RCSC atveju – tik PDF dokumentai).
     - 1.1.2. Pasirašomo dokumento santrauką (pavyzdžiui, sugeneruotą SHA-1 algoritmu).
     - 1.1.3. Nurodytą pasirašymo laiką (priimto standarto formatu).
     - 1.1.4. Nuorodą į PKC.
     - 1.1.5. Parašo paskirties tipą (duomenims patvirtinti, duomenų gavimo faktui patvirtinti ar kt.)
   - 1.2. Nepasirašomus atributus:
     - 1.2.1. Laiko žymą, sugeneruotą TSA.
2. Tikrinantis asmuo laiko parašą galiojančiu, jei;

2.1. Subjekto nurodytas pasirašymo laikas yra ne vėlesnis nei laiko žymoje nurodytas laikas.

2.2. Paraše nurodytas PKC buvo galiojantis pasirašymo metu (remiantis laiko žyma).

2.3. Gauta pasirašyto dokumento santrauka sutampa su santrauka, sugeneruota tikrintojo, naudojantis subjekto viešuoju raktu.

SP nurodyta, kad pasirašantysis asmuo kartu prie suformuoto EP visada turi pridėti pasirašomąjį dokumentą. SP yra bendros **visiems** parašų tipams.

Taisyklėse prie PKC patikimumo sąlygų nurodoma, kad visi tapatybės sertifikatai turi būti išduoti pagrindinės (ir šiuo atveju vienintelės) CA. PKC galiojimo statusas tikrinamas OCSP protokolu.

Kita bendroji informacija, esanti SP, tokia kaip leidėjo pavadinimas, SP identifikatorius ar išleidimo data nebus detalizuojama. Laikysime, kad šioms vienintelėms naudojamoms SP nereikalinga papildoma jų autentiškumo ar vientisumo apsauga.

4. EP infrastruktūros su atributų sertifikavimu prototipas

Prieš tai aprašytas pavyzdinis PKI naudojimo modelis pakankamai tenkina vartotojų grupės poreikius, kol jie susiję tik su autentifikacija. Šiame skyriuje nagrinėjama situacija, kai pavyzdinėje įmonėje iškyla poreikis autorizuoti vartotojus. Atsiranda atributo sąvoka, kai tampa svarbu nustatyti ne tik pasirašiusiojo tapatybę, bet ir jo atributinę informaciją (toliau naudojamas pareigų atributo pavyzdys). Skyriuje formuluojamas pasikeitusios infrastruktūros prototipas, kuris tenkina iškilusius poreikius.

Tolesniuose skyreliuose išdėstomi pavyzdiniai sukonkretinti įmonės reikalavimai, kuriuos turi tenkinti modifikuota PKI, samprotavimai apie atributinės informacijos sertifikavimo variantus. Tinkamiausias sprendimas detalizuojamas, pateikiant naujai steigiamos AA struktūrą ir teikiamas paslaugas, aprašant pasikeitusias SP.

4.1. Autorizacijos poreikis

Bandymą kai kuriuos vartotojus išskirti iš bendros grupės, pagal kažkokią jų savybę (atributus) šiandien jau galime pastebėti ir Lietuvoje. RCSC svetainėje [RSC11] pažymėta, kad kvalifikuoti sertifikatai yra išduodami fiziniams asmenims, tačiau tam tikrai jų grupei – valstybės tarnautojams – išduodami dar ir kitokie sertifikatai. „Kvalifikuotu sertifikatu“ RCSC vadina fizinio asmens tapatybę liudijantį sertifikatą. Tuo tarpu valstybės tarnautojams išduodami „autentifikavimo“ ir „kvalifikuoti“ sertifikatai, kurie įrašomi į tarnautojo pažymėjimą. Prašydamas išduoti šiuos sertifikatus, tarnautojas įsipareigoja „informuoti RCSC, dėl kvalifikuotų sertifikatų galiojimo nutraukimo, kai:

- asmuo, kuriam išduotas kvalifikuotas sertifikatas, perkeltas į kitas pareigas;

- asmuo, kuriam išduotas kvalifikuotas sertifikatas, prarado valstybės tarnautojo statusą“. Nors šio antrojo, „kvalifikuoto“ sertifikato struktūra nėra viešai skelbiama, tačiau iš šio įsipareigojimo galima spręsti, kad sertifikatas liudija asmens pareigas bei statusą. Galime teigti, kad jis yra panašus į anksčiau pristatytą AC, taigi turime AI sertifikavimo pavyzdį praktikoje. RCSC atveju tapatybės („autentifikavimo“) ir atributų („kvalifikuoti“) sertifikatai pateikiami viename komplekte, o už jų išdavimą atsakinga ta pati organizacija, todėl šis AI sertifikavimo sprendimas panašiausias į aprašytą 2.2 skyrelyje.

Kadangi valstybės tarnautojų nėra daug, palyginus su visais fiziniais asmenims, ir jų pareigos bei statusas kinta ne taip dažnai, toks sprendimas šiai dienai galbūt yra tinkamiausias. Tačiau vartotojų grupę ateityje gali prireikti skaidyti ir pagal kitokius požymius, kurie keisis dažniau. Todėl toliau darbe modeliuojamas autorizacijos poreikis, kylantis panašioje, bet šiek tiek kitokioje situacijoje. Vietoje realios vartotojų grupės (fizinių asmenų) bei jos poaibio

(valstybės tarnautojų), imama paprastesnė – menamos įmonės darbuotojai, kurie išsiskiria vieni nuo kitų pareigomis, t.y. toliau nagrinėjamas ir plečiamas EP infrastruktūros modelis, aprašytas 3 skyriuje.

Tarkime, kad pavyzdinės įmonės viduje keičiantis elektroniniais dokumentais iškilo poreikis nustatyti ne tik pasirašiusiojo asmens tapatybę, bet ir pareigas, kurias pasirašymo metu asmuo vykdė. To gali prireikti ir už įmonės ribų, elektroniniais parašais pasirašant sutartis su kitomis įmonėmis. Pavyzdžiui, viena įmonė, nežinodama apie kitos įmonės darbuotojus (kas kokias pareigas eina), gali pageidauti, kad tam tikros sutartys būtų pasirašomos tik direktoriaus (sekretorės, administratoriaus). Pasirašiusiojo tapatybę paliudys į EP įtrauktas pasirašiusiojo asmens sertifikatas, tačiau išlieka poreikis taip pat greitai ir saugiai įsitikinti, kad asmuo tikrai ėjo tokias pareigas, kokias jis nurodė pasirašydamas.

Tarkime, kad sukonkretinti poreikiai pateikiami šiais reikalavimais:

Reikalavimas nr. 1. Tam tikrus dokumentus turi būti leidžiama pasirašyti tik asmenims, einantiems tam tikras pareigas. Įmonės nuostatuose nurodoma, kokiais atvejais kokios pareigos reikalaujamos. Pasirašiusiojo dokumentą subjekto pareigos ir tapatybė turi būti nustatoma EP tikrinimo metu. Pasirašytus dokumentus tikrinantys asmenys neturi galimybės oficialiai nustatyti pasirašiusiojo tapatybės bei jo pareigų kitu būdu.

Komentaras. Galima nurodyti ir kitus atributus, kurių reikalaujama tam tikrais atvejais. Pavyzdžiui, kai kuriuos dokumentus gali pasirašyti tik tam tikrame skyriuje dirbantis darbuotojas. Tada galima reikalauti, kad tam tikrais atvejais pasirašančiajam būtina nurodyti ir pareigų ir priklausymo skyriui atributus. Dėl paprastumo toliau bus kalbama tik apie vienintelį subjekto atributą – pareigas.

Reikalavimas nr. 2. Įmonei turi būti suteikta galimybė suteikti atributus asmenims, nustatyti jų galiojimo trukmę ir prireikus juos atšaukti. Atributus bei jų galimas reikšmes tvirtina tam tikra tarnyba (atributų tvirtinimo padalinys), kurios patvirtinti atributai yra pripažįstami įmonėje. Komunikuojant tarp įmonių, turi būti sutarta, kad šios tarnybos išduotus atributus kitos įmonės taip pat pripažins

Komentaras. Šiuo atveju yra tik vienas pareigų atributas. Jo reikšmės, sakykime, yra tokios: „darbuotojas“, „skyriaus vadovas“, „sekretorė“. Šias reikšmes gali redaguoti (keisti, atšaukti, pridėti naujų) atributų tvirtinimo tarnyba (paprastesniu atveju, kai komunikuojama vienos įmonės viduje – tos pačios įmonės padalinys, kuris toliau bus vadinamas „Atributų tvirtinimo padaliniu“).

Reikalavimas nr. 3. Įmonė neturi būti verčiama steigti papildomų tarnybų savo viduje. Sertifikavimo paslaugas jai ir toliau turi teikti **tik** išorinės organizacijos – sertifikatų centrai (CA).

Komentaras. Papildoma tarnyba nėra laikomas „atributų tvirtinimo padalinys“. Ši sąvoka įvedama tik tokiu atveju, kai komunikacija vyksta tik vienos įmonės viduje. Šis „padalinys“ gali net nepriklausyti įmonei, bet tada jis turi būti pakankamai patikimas, kad galėtų teikti jai (sudėtingesniu atveju – ir kitoms įmonėms) atributų tvirtinimo paslaugas.

Reikalavimas nr. 4. Tobulinant naudojamą PKI, joje naudojami komunikacijos kanalai, dokumentų perdavimo protokolai bei EP formatas turi keistis kiek įmanoma mažiau.

Komentaras. Manykime, kad įmonė yra tvirtai prisitaikiusi prie dabartinės PKI. Todėl kiekviena infrastruktūros modifikacija turės savo kainą bei įtaką įprastinei įmonės veiklai. Įmonė, žinoma, nori įgyvendinti naujus reikalavimus kuo mažesniais kaštais.

Toks poreikis, žinoma, gali atsirasti nebūtinai įmonės viduje ar įmonėms bendraujant tarpusavyje. Atskiri subjektai taip pat tam tikrose situacijose gali pareikalauti patvirtinti papildomą informaciją apie pasirašiusįjį. Tai mažiau tikėtina, nes atributinė informacija dažniausiai nurodo kažkokį bendrai sutartą dalyką (priklausymą grupei, mokslinį laipsnį). Dėl vaizdingumo, toliau nagrinėjamas įmonių ir jų darbuotojų variantas.

4.2. Reikalavimų analizė ir atributų sertifikavimo sprendimo pritaikymas

Akivaizdu, kad įmonė nori patobulinti EP paskirtį. Todėl visų pirma reikia modifikuoti naudojamas SP. Tada priderinti CA (ir galbūt kitų organizacijų) sertifikavimo paslaugas prie pasikeitusių SP.

Atsižvelgiant į realybę, atsakomybės už atributų teisingumą paprasčiausiai perduoti vartotojams negalima – tai būtų pernelyg nesaugu. Todėl 2.1 skyrelyje aprašytą sprendimą (nesertifikuoti subjekto atributai) galima atmesti iš karto.

Nagrinėjant pirmąjį reikalavimą, reikėtų įsivaizduoti, kad įmonė ir toliau norės pasirašinėti dalį dokumentų įprastu būdu – kai EP tikrintojui svarbu nustatyti tik pasirašiusiojo tapatybę. Todėl vienas iš galimų sprendimų SP nurodyti, kad atributai yra liudijami tapatybės sertifikate (2.2 skyrelis) nėra itin tinkamas. Visu pirma, keičiantis PKC struktūrai, reikėtų pakeisti naudojamas CP. Antra, kiekvieno vartotojo PKC reikėtų atšaukti ir išduoti naują, kartu liudijantį ir tapatybę, ir atributus. Tai gerokai padidintų atšauktų sertifikatų sąrašą, kurį turi palaikyti CA. Be to, atliekant tokią procedūrą CA turėtų surinkti duomenis apie kiekvieno vartotojo atributinę informaciją (šiuo atveju tik apie pareigas). Kol ši procedūra nebus baigta, vartotojai negalės pasirašinėti dokumentų. Dar daugiau, kad CA galėtų atlikti tokius veiksmus ir išdavinėti modifikuotus PKC, ji turėtų pakeisti savo CPS. Kadangi CA yra nepriklausoma organizacija, ji vargu ar sutiks keisti savo veiklą dėl vienoje iš aptarnaujamų įmonių atsiradusių poreikių. Įsteigti nuosavą CA, įmonei neapsimoka (žr. trečiąjį reikalavimą).

Taigi šiai situacijai tinkamesnis sprendimas yra atributus liudyti atskiruose sertifikatuose (AC). Priimti sprendimą, ar AC ir PKC išduos tas pats centras, ar bus įsteigtas atskiras AA, vėlgi padeda esama situacija. Vėlgi, nepanašu, kad CA sutiktų teikti papildomas paslaugas (administruoti AC), dėl to, kad tam tikrai vartotojų grupei iškilo toks poreikis. Šiuo atveju geriausia yra visiškai nesikišti į CA veiklą, paliekant šį centrą atsakingu tik už PKC išdavimą ir tvarkymą. Taip padidės sprendimo lankstumas, t.y. vartotojai galės kurti ir tikrinti EP atsižvelgdami į atributus arba juos ignoruodami (įprastas variantas).

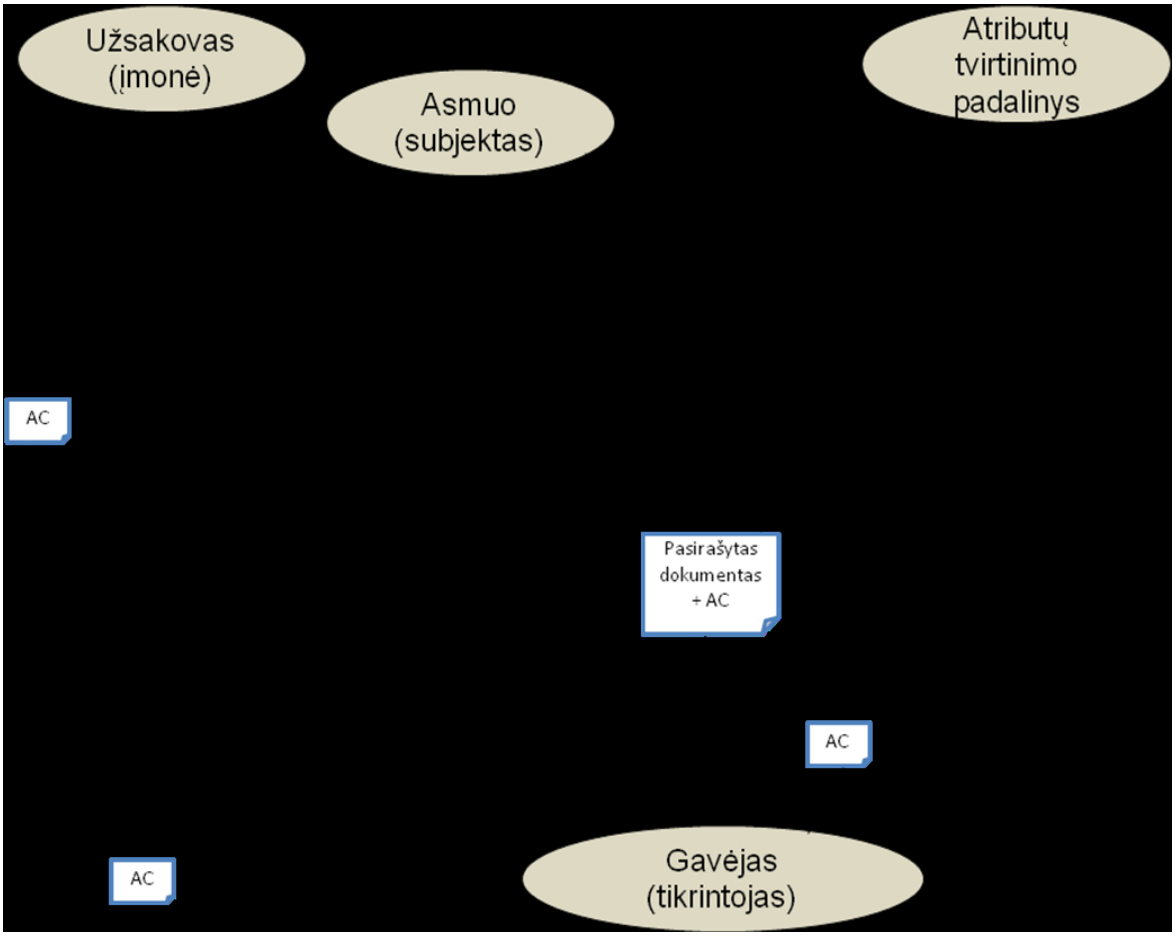
Šioje vietoje galima prisiminti tokius atributų sertifikavimo variantus, kaip *Smart Certificates* bei *FlexiCert*. Nenaudoti AC, griežtai atskirtų nuo PKC, atrodytų paprastesnis ir tinkamesnis variantas (ypač jei atributai yra reikšmingi tik vienos įmonės ribose). Tačiau tokie sprendimai prieštarautų nuostatai nemodifikuoti CA veiklos ir palikti išduodamus PKC tokius, kokie yra.

Kitas žingsnis yra pasirinkti vieną iš dviejų AC perdavimo modelių. *Push* modelio (2.3 skyrelis) įgyvendinimas šiek tiek apkrautų komunikacijos kanalą, būtų keičiamas duomenų perdavimo protokolas ir pats EP formatas (ne taip gerai įgyvendinamas ketvirtas reikalavimas). Tačiau tikrintojui, gavusiam pasirašytą dokumentą, nebereikėtų kiekvieną kartą kreiptis į AA, prašant surasti tam tikro subjekto reikiamus AC. Jam beliktų tik įsitikinti, ar subjekto AC galiojo EP sukūrimo metu. *Pull* modelis (2.4 skyrelis) šiuo atveju nėra tinkamiausias, nes jis reikalauja specialių AA paslaugų, tokių kaip išduotų AC paieška pagal subjekto tapatybę bei perdavimas tikrintojams. Šiame modelyje laikomės principo, kad sertifikavimo paslaugų tiekėjai **nėra** įmonės vidinės tarnybos, t. y. yra vieši CA ir AA, kurie aptarnauja ne vieną įmonę. Reikia priimti sprendimą, kuris patenkins ne tik šiuo metu modeliuojamą vienos įmonės atributų sertifikavimo poreikį, bet ir galės būti pritaikytas kitose panašiose situacijose. AA struktūrą ir veiklos pobūdį mažiau įtakoja *push* modelis, todėl jis ir turėtų būti įgyvendintas.

4.3. AA veiklos

AA tikslas yra teikti vartotojams tokias sertifikavimo paslaugas [ETS03]:

1. Registruoti atributus.
2. Priimti prašymus išduoti AC.
3. Generuoti AC.
4. Platinti AC.
5. Atšaukti AC.
6. Patikrinti AC galiojimą remiantis AC CRL.



13 pav. AA paslaugos ir jų vartotojai

13 pav. vaizduojama, kaip įvairūs vartotojai naudojasi AA paslaugomis. Atributų tvirtinimo padalinys tvarko atributus ir jų reikšmes. Vartotojų grupei nutarus pakeisti SP, šis padalinys kreipiasi į AA su tam tikru prašymu. Jei viena iš atributų reikšmių yra šalinama (pavyzdžiui, nebelieka pareigų „sekretorė“), atributų tvirtinimo padalinys prašo atšaukti visus išduotus AC, kurie liudijo atributus, turinčius tokią reikšmę. Jei keičiasi (ar yra šalinamas) visas atributas (pavyzdžiui, pareigų atributas tampa nebereikšmingas), atšaukiami visi AC kuriuose buvo liudijami šie atributai.

Užsakovui (šiuo atveju – įmonei) gali prireikti priskirti atributo reikšmę tam tikram subjektui arba atšaukti tam tikrą išduotą AC. Ji naudojasi AA atributų registravimo ir AC atšaukimo paslaugomis.

Norėdamas pradėti naudotis AC, vartotojas (subjektas) turi pasitikrinti, ar reikiami atributai jam yra priskirti (AA atributų registravimo paslauga) bei pateikti prašymą išduoti AC, liudijantį šiuos atributus. Prašymas išduoti AC patikrinamas AA viduje ir pasinaudojant AC generavimo paslauga sukuriamas AC. Laikantis *push* modelio, sugeneruotas AC perduodamas prašymą pateikusiam vartotojui, kuris pasirašydamas duomenis AC įtraukia į EP.

Tikrintojas gauna AC informaciją kartu su pasirašytais duomenimis ir jam, nustačius pasirašiusiojo tapatybę, belieka pasinaudoti AA teikiama AC būsenos tikrinimo paslauga.

4.4. AA nuostatai

Veiklos, kuriomis užsiima AA, turėtų būti apibrėžtos oficialiame dokumente – sertifikavimo veiklos nuostatuose (CPS). CPS paaiškina, kaip tam tikras CA (ar AA) įgyvendina sertifikatų taisykles (CP). Nenorėdama atskleisti visų sertifikatų gamybos ir palaikymo detalių, CA arba AA gali viešai paskelbti tik nuostatų santrauką (*CPS abstract*).

Kurdama savo CPS, CA arba AA gali remtis viešai skelbiamomis rekomendacijomis. Pavyzdžiui, pagal schemoje [RFC3647] nurodytą CPS dokumento struktūrą, AA nuostatų struktūros prototipas galėtų būti toks:

1. Įvadas.
    1.1. Apžvalga. Šis pavyzdinis CPS glaustai apibūdina konkrečios AA veiklą. Dokumentas sudarytas laikantis [RFC3647] rekomenduojamos struktūros, remiantis CA CPS pavyzdžiais .
    1.2. Pavadinimas ir identifikatorius. „AA veiklos nuostatai“ (AACPS-1).
    1.3. PKI dalyviai:
        1.3.1. AC išduodanti AA. Atsakinga už AC gyvavimo ciklo palaikymą. Sudėtingesniais atvejais, kai vienoje AA įkuriami keli registravimo padaliniai, jie gali būti išskirti į atskirą dalyvių grupę, su savo atsakomybėmis.
        1.3.2. AC užsakovai. Įmonės, kurios užsako atributų sertifikavimo paslaugas ir jomis naudojasi. Kaip pavaizduota 13 pav., jos registruoja atributus (pavyzdiniu atveju tai bus vienintelis atributas – asmens pareigos), bei reikalui esant prašo atšaukti subjekto AC.
        1.3.3. AC subjektai. Šiuo atveju, tai fiziniai asmenys, turintys išduotą AC.
        1.3.4. Susijusios šalys. Atributų tvirtinimo padalinys, kuris atstovauja vartotojų grupei ir tvirtina bei atšaukia atributus (dėl paprastumo laikome, kad patvirtintas vienintelis galimas atributas – pareigos).
    1.4. Sertifikatų naudojimo sritys.
        1.4.1. Sertifikatų tipai. Viešai AA išduoda tik vieno tipo sertifikatus – asmeninius pareigų sertifikatus. Kitais atvejais sertifikatų tipų gali būti daugiau, pavyzdžiui, sertifikatas, skirtas saugiai komunikacijai tarp serverių SSL kanalu. Šis prototipas apsiriboja vieninteliu panaudojimo atveju – kai AA išduotus sertifikatus asmenys (subjektai) naudoja pasirašydami elektroninius dokumentus EP. Į parašą įtrauktas AC leis tikrintojui nustatyti pasirašiusiojo pareigas. Vienintelis ne atributus

liudijantis sertifikatas, išduotas AA pačios sau, naudojamas pasirašyti išduodamus AC.

1.5. Atsakingoji institucija. Čia turėtų būti pateikti AA, kaip vienintelio aukščiausio lygio patikimo taško, kontaktiniai duomenys.

1.6. Apibrėžimai ir santrumpos. Šiame CPS naudojamų santrumpų paaiškinimai yra šio darbo pabaigoje.

2. Informacijos teikimas ir teikėjo atsakomybė. AA nekaupia ir neteikia duomenų, nesusijusių su AC sertifikatais. AA publikuoja:

2.1. CRL duomenis. Taip pat teikia atsakymo į OCSP užklausas paslaugą.

2.2. Šakninio sertifikato duomenis (sertifikato sudaryto AA pačios sau).

2.3. AC duomenis, kuriuos pagal prašymą išduoda tik asmeniui, kuris yra AC turėtojas. (Jei prototipas laikytųsi *pull* modelio, AC būtų išduodami tikrintojams, pateikusiems pasirašiusiojo tapatybės duomenis).

AA pasilieka teisę prireikus publikuoti AC informaciją trečiosioms šalims.

3. Asmenų atributų autentiškumo tikrinimas.

3.1. Reikalavimai atributų pavadinimams. Kadangi šios AA išduodami sertifikatai gali liudyti vienintelį atributą - pareigas, reikalavimų atributų pavadinimams galima ir nenumatyti. Tačiau, patvirtinus daugiau atributų bei atsiradus daugiau nei vienam AC užsakovui, gali kilti atributų identifikavimo problema. Kad būtų galima atskirti AC vartotojų grupes, atributo pavadinimas turi būti sudarytas iš užsakovo unikalaus identifikacinio numerio (pavyzdžiui, OID) bei atributo identifikacinio numerio. Pavyzdys: pareigų atributas įmonėje A identifikuojamas kaip: „A_OID_00001-Pareigos_0001“.

3.2. Pradinis asmens atributų autentiškumo patikrinimas. Atributų autentiškumą nustato atributų registravimo padalinys. Jei į registravimo padalinį kreipiasi AC užsakovas, nurodydamas subjektus ir jiems priskirtinas atributų reikšmes (pavyzdžiui, įmonė pateikia darbuotojų sąrašą su jų pareigomis), papildomi tikrinimo veiksmai neatliekami. Jei AC prašo išduoti subjektas, kurio atributo reikšmė AA dar nėra žinoma, registravimo padalinys kreipiasi į AC užsakovą su prašymu pateikti (arba patvirtinti) subjekto duomenis.

3.3. Prašymų pakeisti AC raktus tikrinimas. Tokių prašymų AA neaptarnauja.

3.4. Prašymų atšaukti sertifikatų galiojimą tikrinimas. Gavusi prašymą atšaukti sertifikatą (ar atributą) iš bet kurio PKI dalyvio, AA atlieka procedūras dalyvio tapatybei nustatyti. Priklausomai nuo to, ar tapatybė buvo nustatyta sėkmingai, AA atšaukia sertifikatą arba atributą (t.y. visus AC, išduotus su nurodytu atributu).

4. Sertifikatų tvarkymo operaciniai reikalavimai.
   4.1. Prašymas sudaryti sertifikatą. Tokie prašymai gali būti priimami iš vienintelio PKI dalyvio - subjekto. Prašymą subjektas pateikia siųsdamas užklausą AC išdavimo padaliniui. Kad prašymas būtų pradėtas vykdyti, turi būti patvirtinta subjekto tapatybė.
   4.2. Prašymo sudaryti sertifikatą vykdymas. AC išdavimo padalinys atlieka procedūrą subjekto nurodyto atributo reikšmės patikrinimui. Jei atributas su nurodyta reikšme priklauso subjektui, kreipiamasi į AC generavimo padalinį.
   4.3. Sertifikato sudarymas. Į sertifikatą įrašomi subjekto tapatybės duomenys (pagal kuriuos AC galės būti siejamas su PKC), atributo tipas (pareigos), reikšmė ir kiti sertifikato duomenys (galiojimo periodas, serijos numeris, vartotojų grupė ir kt.). Ši informacija pasirašoma AA privačiuoju raktu (AA raktų pora saugoma paties sau išduoto AA sertifikate), kad sugeneruotą AC vėliau būtų galima patikrinti. Pastaba: dėl specifinės AC paskirties, priešingai, nei kuriant PKC sertifikatą, į AC nėra įrašoma naujai sugeneruota (ar subjekto pateikta) raktų pora.
   4.4. Sertifikato patvirtinimas. Išpildžius subjekto prašymą sudaryti AC, platinimo padalinys turi pristatyti AC subjektui. Jei subjektas AC nepriima (dėl AC duomenų netikslumo ar kitų priežasčių), sertifikatas turi būti nedelsiant atšaukiamas ir (pagal pageidavimą) išduodamas iš naujo. Išduoto sertifikato duomenų AA nesaugo ir AC platinimo teisė paliekama subjektui.
   4.5. Sertifikatų naudojimas. Subjektai naudoja AC prireikus į kuriamus EP įtraukti paliudytą atributinę informaciją (šiuo atveju - pareigas). Į pasirašomus duomenis subjektas pagal poreikį įtraukia AC. Tikrintojas gali įsitikinti subjekto nurodytų atributų teisingumu, tikrindamas AC galiojimą.
   4.6. Sertifikatų atnaujinimas. Sertifikatų atnaujinimo, kaip ir galiojimo sustabdymo, paslauga neteikiama.
   4.7. Sertifikatų modifikavimas. Sertifikatą gali prireikti modifikuoti tik pasikeitus atributų reikšmei. Tokiu atveju atšaukiamas anksčiau subjektui išduotas AC ir išduodamas naujas.
   4.8. Sertifikatų atšaukimas ir galiojimo sustabdymas.
      4.8.1. Prašymai atšaukti sertifikatą turi būti priimami nuolat (24/7). Atsakymus apie prašymo patenkinimą ar atmetimą AA turi pateikti nedelsiant.
      4.8.2. Jei prašymas patvirtinamas (pagal 3.4), AC turi būti atšauktas nedelsiant (atšaukimas turi užtrukti ne ilgiau nei minutę).
      4.8.3. Nauja CRL versija turi būti išleidžiama po kiekvieno patenkinto AC atšaukimo.
      4.8.4. Tarp atšaukimo ir naujos CRL versijos išleidimo leistinas maksimalus 1 valandos intervalas.

4.8.5. Sertifikatų galiojimo sustabdymo paslauga neteikiama.

4.9. Informacijos apie sertifikatų būseną teikimo paslaugos. AC tikrintojams turi būti nuolat prieinama OCSP paslauga.

4.10. Abonemento pabaiga. AC nustoja galioti pasibaigus jame nurodytam galiojimo laikotarpiui.

Be šių skyrių, CPS dar turi būti nurodomi fizinės aplinkos reikalavimai, kontrolės principai, techninis saugumas, sertifikatų, CRL ir OSCP profiliai, atitikties audito procedūra, bei kiti veiklos ir teisiniai klausimai. Šie CPS skyriai turėtų būti detaliai aprašyti prototipą derinant prie realių AA steigimo aplinkybių.

Toks CPS patvirtina, kad įkuriama AA turi būti nepriklausoma organizacija (niekuo nesusijusi su, pavyzdžiui, CA, kurios paslaugomis taip pat naudojasi vartotojų grupė), ji turi būti vienintelė, pagrindinė ir patikimai bei efektyviai administruoti atributų sertifikatus. Praktikoje gali atsirasti poreikis įsteikti papildomas AA, ar bent kelias atributų registravimo tarnybas (vartotojų patogumui), tuomet šiuos nuostatus reikėtų patobulinti.

4.5. Pakeitimai parašo taisyklėse

Kad vartotojų grupė pradėtų naudotis pasikeitusia infrastruktūra, ji turi būti sutarusi dėl pakeitimų SP. Laikydamiesi anksčiau apibrėžtų SP, tarkime, kad jos išlieka parašytos laisvo teksto pavidalu ir vartotojams prieinamos viešai.

SP aplinka vėlgi gali likti tiek uždara, tiek tapti atvira. Kol atributinė informacija bus svarbi vienos įmonės ribose, užtenka, kad SP laikytųsi visi jos darbuotojai. Komunikuojant AC papildytais EP tarp įmonių, jos turi būti susipažinusios su SP iš anksto.

Atsiradus sertifikuojamiems atributams EP gavėjui ne visada pakaks patikrinti vienintelį pasirašiusiojo nurodytą PKC. SP atsiranda nurodymas, kokias atvejais tikrintojas turi papildomai kreiptis į AA su gautu pasirašiusiojo AC ir įsitikinti jo galiojimu. Taip pat SP turi būti išvardinti atvejai, kuriais subjektas į formuojamą parašą privalo įtraukti AC. Anksčiau aprašytų SP skyriuose turėtų atsirasti tokie nauji punktai (paryškinta):

1. Pasirašęs asmuo formuojamame paraše pateikia:
   1.1. Pasirašomus atributus:
      1.1.1. Pasirašomo dokumento formatą.
      1.1.2. Pasirašomo dokumento santrauką.
      1.1.3. Nurodytą pasirašymo laiką.
      1.1.4. Nuorodą į PKC.
      1.1.5. Parašo paskirties tipą.
   1.2. Nepasirašomus atributus:

1.2.1. Laiko žymą, sugeneruotą TSA.

1.2.2. Sertifikatą, liudijantį pasirašiusiojo pareigas (AC).

2. Tikrinantis asmuo laiko parašą galiojančiu, jei;

2.1. Subjekto nurodytas pasirašymo laikas yra ne vėlesnis nei laiko žymoje nurodytas laikas.

2.2. Paraše nurodytas PKC buvo galiojantis pasirašymo metu (remiantis laiko žyma).

2.3. Paraše nurodytas AC buvo galiojantis pasirašymo metu (remiantis laiko žyma).

2.4. Gauta pasirašyto dokumento santrauka sutampa su santrauka, sugeneruota tikrintojo, naudojantis subjekto viešuoju raktu.

Atvejais, nenurodytais papildytose SP, pasirašymas ir tikrinimas išlieka toks pats, t.y. punktai 1.2.2 ir 2.3 ignoruojami. Taigi SP nebelieka nurodymo, kad kartu su pasirašytu dokumentu subjektas neturi galimybės pateikti papildomos informacijos. Sutarus, kad AI sertifikavimo paslaugas teikia vienintelis AA, prie patikimumo sąlygų SP turi būti nurodyta, kad visi AC turi būti išduoti šios tarnybos. Dėl paprastumo, SP nurodoma, kad AC galiojimo statusas (taip pat kaip ir PKC) tikrinamas OCSP protokolu.

4.6. AC formatas

Šiame skyrelyje apibrėžiamas pavyzdinis supaprastintas AC formatas. 3 lentelėje apibūdinami esminiai šio sertifikato laukai. Standartinė AC struktūra detaliai aprašyta RFC 3281 standarte [FH02, 10].

3 lentelė. Pavyzdinio AC laukai

AC	
Laukas	**Paaiškinimas**
Savininkas	AC turėtojas. Šiuo lauku AC susiejamas su subjektu.
Serijos numeris	Jį priskiria AA. Unikalus tarp visų AC, išduotų AA.
AC galiojimo periodas	AC galiojimo laikotarpis.
Vartotojų grupė	Nurodomas vartotojų grupės identifikatorius, kurioje šis AC turės prasmę. Jei AC yra viešas, šio lauko galima nepildyti. Pagal pavyzdinį atvejį, šiame lauke bus įrašomas tariamos įmonės identifikatorius.
Atributai	Esminė informacija: atributai, kurie susiejami su AC turėtoju.
Parašo reikšmė	Rezultatas, gautas AA pasirašius AC.

Tarkime, kad papildytose SP nurodyta, jog AC yra susiejami (žr. 2.6 „Tapatybės ir atributų sertifikatų susiejimo būdai“) su subjekto tapatybe (savininko laukas AC). Tai reiškia, kad pasikeitus ar nustojus galioti asmens PKC, AC liks galiojantis. Kai subjektas gaus naują PKC, jis vėl galės pasirašinėti dokumentus. Dėl paprastumo, AC standarte nurodyti laukai „versija“, „leidėjas“, „leidėjo unikalus ID“, bei „Parašo algoritmas“, neįtraukiami. Laikysime, kad versija

yra nekintanti, o AC leidėjo bei jo naudojamo parašo algoritmo duomenys pateikiami papildytose SP.

4.7. AA ir AC autonomiškumas

Siūlomas PKI patobulinimas leidžia vartotojams naudotis įvairiais AC (pagal atvejus, nurodytus SP) nepriklausomai nuo turimų PKC. Atributui nustojus galioti, jį liudijantys AC atšaukiami ir tai užfiksuojama AA saugomuose CRL. PKC išduodančios CA veikla nesusiejama su AC išduodančios AA veikla, todėl atšaukus vieną ar kelis subjekto AC, jo PKC lieka galiojantis. Tačiau jei atšaukiamas PKC, subjektas nebegalės kurti EP, nesvarbu, kad visi jam išduoti AC yra galiojantys. Kitaip sakant, naudoti PKC be AC išlieka prasminga (atvejais, kai tikrintojui nesvarbi atributinė informacija), o AC be galiojančio PKC prasmės neturi.

Šiame sprendime į PKI įtraukiamas viešas AA (derinantis prie CA apibrėžimo) , todėl jis galėtų teikti paslaugas įvairioms vartotojų grupėms. Tarkime, jei panašus atributų sertifikavimo poreikis iškiltų kitoje panašioje įmonėje (jau besinaudojančia CA paslaugomis), ji taip pat galėtų kreiptis į AA, kuris išdavinėtų AC, skirtus naudoti šios įmonės ribose. Kuriai vartotojų grupei yra skirtas AC, galima atskirti pagal lauką „Vartotojų grupė“.

Rezultatai ir išvados

Rezultatai

Darbe išnagrinėta el. parašų (EP) atributinės informacijos sertifikavimo problema ir šiuo metu įmanomi jos sprendimo būdai.

Atliktas dabartinės EP infrastruktūros Lietuvoje tyrimas parodė, kad el. parašas jau yra tapęs rimta el. komercijos dalimi (išleisti įstatymai, specifikacijos, vykdomi projektai). Pastebėta, kad šiandien naudojantis el. parašu pasirašančiojo asmens atributinė informacija dar nėra tokia svarbi ir nėra akivaizdaus poreikio ją sertifikuoti.

Darbe išanalizuoti ir palyginti įvairūs atributinės informacijos sertifikavimo metodai, suformuluotas jų tinkamumas tam tikrose situacijose. Parodyta atributų sertifikato, kaip atskiro dokumento, svarba, pateiktos galimybės šiuos sertifikatus ir juos išduodančias įstaigas įtraukti į įprastą EP infrastruktūrą.

Galimybė diegti atributinės informacijos sertifikavimo siūlomą sprendimą darbe demonstruojama remiantis sukurtu EP infrastruktūros modeliu, atspindinčiu dabartinę el. parašo naudojimo situaciją Lietuvoje. Prognozuojant atributinės informacijos sertifikavimo poreikį, esamam EP infrastruktūros modeliui yra iškelti nauji reikalavimai, atlikta šių reikalavimų analizė, pasiūlytas tinkamiausias sprendimo metodas. Rekomenduojamo sprendimo pagrįstumas parodytas pateikiant pavyzdinę atributų sertifikavimo tarnybos struktūrą, jos veiklos nuostatų metmenis, naujai įvedamo atributų sertifikato esmines dalis.

Išvados

Atributinės informacijos sertifikavimo problemos sprendimas reikalauja gero EP infrastruktūros principų supratimo.

Lietuvoje ši problema dar nėra aktuali, todėl darbo praktinė reikšmė turėtų padidėti vėlesniame el. parašo naudojimo etape.

Remiantis užsienio publikacijose siūlomais metodais, konkretus atributinės informacijos sertifikavimo sprendimas gali būti taikomas tik gerai žinant realią EP infrastruktūros naudojimo situaciją: kokia yra vartotojų grupė ir jos interesai, kaip jie naudojasi asmens tapatybės sertifikavimo centrų paslaugomis, kokių parašo taisyklių laikosi infrastruktūros dalyviai.

Iškilus realiam atributų sertifikavimo poreikiui, sukurto EP infrastruktūros modelio tobulinimo rekomendacijos turėtų būti tikslinamos, prisiderinant prie esamų galimybių.

Šaltiniai

[Bit08] Bitė – Mobilusis elektroninis parašas, 2008. [žiūrėta 2010-06-21]. Prieiga per internetą: <http://www.bite.lt/lt/bc/esign>

[CAC06] CAcert, the Community Certification Authority Certification Practice Statement draft (2006-07-26), CAcert Community.

[CFS03] S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Network Working Group, 2003.

[CSF08] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk. RFC 5280 on Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Public-Key Infrastructure (X.509) Working Group of the IETF, 2008.

[E3P09] Elektroninio Parašo Proveržio Programa (E3P), 2009.

[ETS01] ETSI TS 101 862 V1.3.3 (2001-06) Technical Specification. Qualified certificate profile. European Telecommunications Standards Institute, 2001.

[ETS02] ETSI TS 101 903 V1.4.1 (2009-06) Technical Specification. XML Advanced Electronic Signatures (XAdES). European Telecommunications Standards Institute, 2002.

[ETS03] ETSI TS 102 158 V1.1.1 (2003-10) Technical Specification. Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates. European Telecommunications Standards Institute, 2003.

[FH02] Stephen Farrell and Russell Housley. RFC 3281. An Internet Attribute Certificate Profile for Authorization. The Internet Society Standards Track, 2002.

[FPK07] Federal Public Key Infrastructure Policy Authority. Rich Attribute Exchange with PKI Certificates, Version 1.0.0, June 2007.

[GRT11] Gyventojų registro tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos. Sertifikavimo paslaugų svetainė, 2011.

[GS10] GlobalSign Certification Practice Statement, v.6.7 (2010-05-12). GlobalSign, GMO Internet group.

[IVP10] Informacinės visuomenės plėtros komitetas prie Lietuvos Respublikos Vyriausybės. Nuotolinė elektroninio parašo mokymo sistema. [žiūrėta 2010-06-21]. Prieiga per internetą: <http://epp.ivpk.lt/lt/epp/>

[IVP11] Informacinės visuomenės plėtros komitetas prie Lietuvos Respublikos Vyriausybės. Lietuvos Respublikos prižiūrimų ir/ar akredituotų Sertifikavimo paslaugų teikėjų sąrašas.

[IVP03] Informacinės visuomenės plėtros komitetas prie Lietuvos Respublikos Vyriausybės. Įsakymas dėl laiko žymos formavimo paslaugų teikimo tvarkos patvirtinimo. 2003. Valstybės Žinios, 2011-04-23, Nr 48, publikacijos Nr.: 2349

[LAD09] Lietuvos archyvų departamentas. Elektroniniu parašu pasirašyto elektroninio dokumento specifikacija ADOC-V1.0, 2009.

[LRS00] Lietuvos Respublikos Seimas. Lietuvos Respublikos elektroninio parašo įstatymas. Liepa 2000. Valstybės Žinios, 2000-07-26, Nr 61, publikacijos Nr.: 1827.

[LZ03] A.Lakshminarayanan and Jianying Zhou. FlexiCert: Merging X.509 Identity Certificates and Attribute Certificate. 14th International Workshop on Database and Expert Systems Applications (DEXA'03), 2003.

[MAM99] M. Myers , R. Ankney, A. Malpani, S. Galperin, C. Adams. X.509 Internet Public Key InfrastructureOnline Certificate Status Protocol – OCSP. Network Working Group, 1999.

[Nyk00] T. Nykänen. Attribute Certificates in X.509. Tik-110.501 Seminar on Network Security, 2000. [žiūrėta 2010-06-21]. Prieiga per internetą: <http://www.tml.tkk.fi/Opinnot/Tik-110.501/2000/papers/nykanen.pdf>

[Omn07a] Omnitel pranešimai spaudai. „Šiandien Lietuvoje pradeda veikti mobilusis e-parašas“, 2007. [žiūrėta 2010-06-21]. Prieiga per internetą: <http://www.omnitel.lt/apie-omnitel/ziniasklaidai/pranesimai-spaudai/siandien-lietuvoje-pradeda-veikti-mobilusis-e-parasas-/7991?s=1>

[Omn07b] Omnitel pranešimai spaudai. „Omnitel klientai mobiliuoju e.parašu jau gali pasirašyti visus dokumentus“, 2007. [žiūrėta 2010-06-21]. Prieiga per internetą: <http://www.omnitel.lt/apie-omnitel/ziniasklaidai/pranesimai-spaudai/omnitel-klientai-mobiliuoju-eparasu-jau-gali-pasirasyti-visus-dokumentus-/7989?s=1>

[PFI07] Puslaidininkių fizikos institutas. Project BalticTime, 2007.

[PS00] J. S. Park, R. Sandhu. Binding Identities and Attributes Using Digitally Signed Certificates. In proceedings of the 16th Annual Computer Security Applications Conference, 2000.

[PS99] J. S. Park, R. Sandhu. Smart Certificates: Extending X.509 for Secure Attribute Services on the Web. In proceedings of the 22nd National Information Systems Security Conference, 1999.

[Rep07] Gytis Repečka. Elektroninis parašas. Kas tai? Naujoji Komunikacija, Nr. 16, 2007. Prieiga per Internetą: <http://www.nk.lt/archyvas/aktualijos/elektroninis-parasas>

[RSC11] Valstybės įmonės Registrų centro sertifikatų centras. 2011.

[SSC11] Skaitmeninio sertifikavimo centras (SSC), 2011.

[Und03] V. Undzėnas. Elektroninio parašo infrastruktūra ir elektroninė komercija. Mokomoji medžiaga, 2003 (atnaujinta 2008), Vilniaus universitetas, MIF, PS katedra.

[Und10] V. Undzėnas. Elektroninio parašo infrastruktūra ir elektroninė komercija. Paskaitų skaidrės, 2010, Vilniaus universitetas, MIF, PS katedra.

Santrumpos

AA - *Attribute Authority,* Atributų sertifikatų centras

AC - *Attribute Certificate,* Atributų sertifikatas

AI - *Attribute Information*, Atributinė informacija

CA - *Certificate Authority,* Sertifikatų centras

CP - *Certificate Policy*, Sertifikato taisyklės

CPS - *Certificate Practice Statement*, Sertifikavimo paslaugų tiekėjo nuostatai

CRL - *Certificate Revocation List*, Atšauktų sertifikatų sąrašas

EP - Elektroninis parašas

IVPK - Informacinės visuomenės plėtros komitetas

OCSP - *Online Certificate Status Protocol*, Sertifikatų galiojimo patikrinimo realiu laiku protokolas

PKC - *Public Key Certificate*, Tapatybės sertifikatas, pagrindinis sertifikatas

PKI - *Public Key Interface*, Viešųjų raktų infrastruktūra

RCSC - Registrų centro sertifikatų centras

SP - *Signature Policy*, Parašo taisyklės

SSC - Skaitmeninio sertifikavimo centras

TSA - *Time Stamping Authority*, Laiko žymų tarnyba