Įvadas į „Sweden Connect“ techninę sistemą

2024-12-04

Nuorodos numeris: **2019-267**

Turinys

1. Įvadas

1.1. Apžvalga

„Sweden Connect“ techninė sistema pritaikyta tapatybės susiejimams, pagrįstiems SAML 2.0.

Naujausioje techninės sistemos versijoje taip pat buvo įdiegtos „OpenID Connect“ specifikacijos. Šiuo metu nėra „OpenID Connect“ susiejimo palaikymo. Jis bus įdiegtas 2025 m.

Likusiose šio dokumento dalyse aprašomas tik SAML susiejimas. Kai „OpenID Connect“ bus visiškai įdiegta, šis dokumentas taip pat apims šią technologiją.

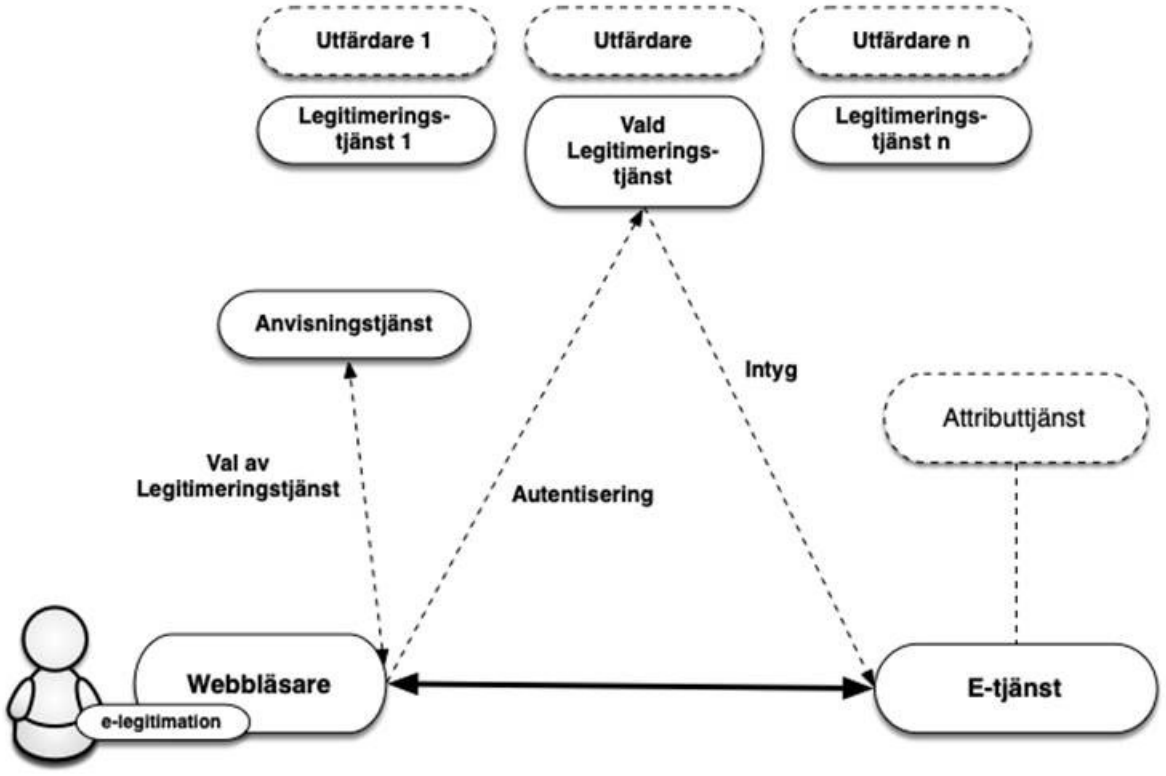
Pasikliaujančiosios šalys iš tapatumo nustatymo paslaugos gauna standartizuoto formato tapatybės sertifikatus[1].

E. paslaugų, kurioms reikalingas parašas, nereikia pritaikyti prie skirtingų naudotojų e. ID, kad būtų galima sukurti elektroninius parašus. Vietoj to e. paslauga tai paveda parašo paslaugai, kur naudotojams, palaikomiems tapatumo nustatymo paslaugos, suteikiama galimybė pasirašyti elektroninius dokumentus.

Susiejimo metu e. paslaugos ir atitinkamos pasikliaujančiosios šalys atlieka paslaugų teikėjo (SP) vaidmenį, o tapatybės sertifikatus išduodančios tapatumo nustatymo paslaugos atlieka tapatybės teikėjo (IdP), taip pat naudotojo atpažintuvo vaidmenį, nesvarbu dėl kokios e. paslaugos nustatoma naudotojo tapatybė.

Tais atvejais, kai e. paslaugai reikia daugiau informacijos apie naudotoją, pvz., informacijos apie teisnumą, galima pateikti klausimą susiejimo požymių paslaugai, Požymių institucijai (AA), jei yra tokia atitinkama požymių paslauga. Pateikus prašymą suteikti požymį, e. paslauga gali gauti reikiamos papildomos informacijos, kad suteiktų naudotojui leidimą ir prieigą prie e. paslaugos ar lygiavertės paslaugos.

Kadangi asmens tapatybės duomenys ir kiti su naudotojais susiję požymiai teikiami naudojant tapatybės sertifikatus ir požymių sertifikatus, visų rūšių e. ID, dėl kurių pasikliaujančiosios šalys yra sudariusios susitarimą ir kurios yra susiejimo dalis, gali būti naudojamos tapatumui nustatyti teikiant e. paslaugą, kuriai reikia ir asmens tapatybės numerio, ir papildomos informacijos, net jei e. ID nėra jokių konkrečių asmens duomenų (pvz., kodų langelių vienkartiniams slaptažodžiams generuoti).



Utfärdare 1	Išleidėjas 1
Utfärdare n	Išleidėjas n

Legitimeringstjänst 1	Tapatumo nustatymo paslauga 1
Vald legitimeringstjänst	Pasirinkta tapatumo nustatymo paslauga
Legitimeringstjänst n	Tapatumo nustatymo paslauga n
Anvisningstjänst	Aptikimo paslauga
Intyg	Sertifikatas
Val av legitimeringstjänst	Tapatumo nustatymo paslaugos pasirinkimas
autentisering	tapatumo nustatymas
attributtjänst	požymių paslauga
Webbläsare	Naršyklė
E-tjänst	E. paslauga

1 pav. *Ryšių tarp skirtingų paslaugų susiejant tapatybę iliustracija.*

> [1]: Tapatumo nustatymo paslauga taip pat minima kituose Digg dokumentuose kaip tapatybės paslauga ir sertifikavimo paslauga. Tačiau šiame dokumente vartojama tik sąvoka „tapatumo nustatymo paslauga“.

1.2. Patikimumo sistema ir saugos lygiai

Saugos lygis, taikomas nustatant naudotojo tapatumą, grindžiamas e. atpažinties saugumo užtikrinimo lygiu, kurio reikalaujama e. paslaugai. Kad šiuos saugos lygius būtų galima palyginti susiejimo sistemoje, Švedijos e. atpažinties patikimumo užtikrinimo sistemoje [Digg.Tillit] nustatyti keturi saugumo užtikrinimo lygiai (1–4), o ES eIDAS reglamente – trys saugumo užtikrinimo lygiai (žemas, pakankamas, aukštas). Visi tapatybės sertifikatus išduodantys subjektai turi įrodyti, kad visas procesas, kuriuo grindžiamas tapatybės sertifikatų išdavimas, atitinka reikalaujamo saugumo užtikrinimo lygio reikalavimus, įskaitant:

- tapatybės sertifikato sukūrimo reikalavimus;
- elektroninio identifikavimo (tapatumo nustatymo) reikalavimus;
- išdavimo proceso reikalavimus;
- pačios e. ID ir jos naudojimo reikalavimus;
- reikalavimus e ID išleidėjui;
- reikalavimus nustatyti e. ID prašytojo tapatybę.

1.3. Metaduomenų rinkimo, administravimo ir skelbimo paslauga

SAML susiejimas teikia informaciją apie susiejimo dalyvius per SAML metaduomenis. Tiek subjektai, teikiantys tapatumo nustatymo ir priskyrimo paslaugas susiejime, tiek pasikliaujančiosios šalys, t. y. subjektai, kurie naudojasi šiomis paslaugomis, pvz., e. paslaugomis, laikomi susiejimo dalyviais.

Susiejimo metaduomenys suteikia dalyviams galimybę gauti informaciją apie kitų dalyvių paslaugas, įskaitant duomenis, būtinus saugiai keistis informacija tarp dalyvių. Kiekviena šalis turi nuolat atnaujinti metaduomenis, laikydamasi sutarties sąlygų.

Pagrindinis metaduomenų tikslas – pateikti raktus ir (arba) sertifikatus, reikalingus saugiam ryšiui ir paslaugų keitimuisi informacija. Metaduomenys apima ne tik raktus, bet ir kitą paslaugų sąveikai svarbią informaciją, pavyzdžiui, reikiamų funkcijų adresus, informaciją apie saugumo užtikrinimo lygius, paslaugų kategorijas, naudotojo sąsajos informaciją ir t. t.

Tapatybės susiejimą apibrėžia XML formato registras, kuris pasirašomas susiejimo veiklos vykdytojo pažymėjimu. Faile pateikiama informacija apie tapatybės susiejimo narius, įskaitant jų sertifikatus. Kadangi metaduomenų failas yra pasirašytas, pakanka palyginti sertifikatą su jo metaduomenų atitikmeniu. Centriniu susiejimo registru grindžiamai infrastruktūrai reikia, kad registras būtų nuolat atnaujinamas ir kad susiejimo nariai visada naudotų naujausią failo versiją.

1.4. Aptikimo paslauga

Tapatybės susiejime galima pasiūlyti ir naudoti bendrą aptikimo paslaugą, kurioje išvardijamos naudotojo galimos pasirinkti tapatumo nustatymo paslaugos. Tokios aptikimo paslaugos tikslas – pašalinti atskiras e. paslaugas, kurios yra tapatybės susiejimo dalis, nuo palaikymo, atsižvelgiant į tai, kaip naudotojai pasirenka tapatumo nustatymo paslaugą (arba prisijungimo būdą), įgyvendinimo.

Kadangi aptikimo paslauga teikiama tapatybės susiejime, e. paslaugos gali ten nukreipti savo naudotojus, kad jie galėtų pasirinkti tapatumo nustatymo paslaugą. Aptikimo paslauga sąveikauja su pasirinkusiu naudotoju, o naudotojas kartu su naudotojo pasirinkimu nukreipiamas atgal į e. paslaugą, kuri dabar žino, į kurią tapatumo nustatymo paslaugą naudotojas turėtų būti siunčiamas tapatumui nustatyti.

Šiuo metu „Sweden Connect“ susiejimas neturi bendros aptikimo paslaugos.

1.5. Integracija pasikliaujančiojoje šalyje

Pasikliaujančiosios šalys, pvz., e. paslaugos, integruojasi su tapatumo nustatymo paslaugomis standartizuotais pranešimais ir naudoja tapatybės sertifikatus, kurie taip pat yra standartizuoto formato.

„Sweden Connect“ techninei sistemai įtakos turi sąveikumo profilis „SAML V2.0 Diegimo profilis susiejimo sąveikumui“ [SAML2Int]. Profilis palaikomas įvairiais komerciniais produktais ir atvirojo kodo sprendimais, palengvinančiais integraciją į e. paslaugas.

Daugelyje e. paslaugų naudojami atskiri tapatumo nustatymo sprendimai, o tai reiškia, kad integracijos pritaikymas prie techninės sistemos turi ribotą poveikį pačiai e. paslaugai.

1.6. Parašas

Pasirašant „Sweden Connect“ techninė sistema suteikia galimybę naudoti įvairių rūšių e. ID, net ir tas, kurios nėra grindžiamos sertifikatais, nereikalaujant specialių e. paslaugos pakeitimų. Taip yra todėl, kad elektroniniu būdu išduotas tapatybės sertifikatas (naudojamas

naudotojų tapatybei nustatyti pasirašant) yra to paties formato, neatsižvelgiant į naudotojo naudojamos e. ID rūšį.

Pasirašymo paslauga siekiama sudaryti sąlygas parašams tapatybės susiejimuose, atitinkančiuose techninę sistemą, naudojant visų rūšių e. ID, kuriomis užtikrinamas pakankamas saugumo lygis.

Perkant[1] ir įdiegiant parašo paslaugą, pasikliaujančioji šalis, kuri yra susiejimo dalis, gali leisti naudotojui pasirašyti elektroninį dokumentą naudojantis parašo paslauga. Naudotojo elektroninį parašą ir susijusį pasirašymo sertifikatą sukuria parašo paslauga po to, kai naudotojas sutinka pasirašyti, patvirtindamas savo tapatybę parašo paslaugai[2].

[1]: Taip pat galima įdiegti parašo paslaugą pagal techninės sistemos specifikacijas arba kitaip įsigyti parašo paslaugą.

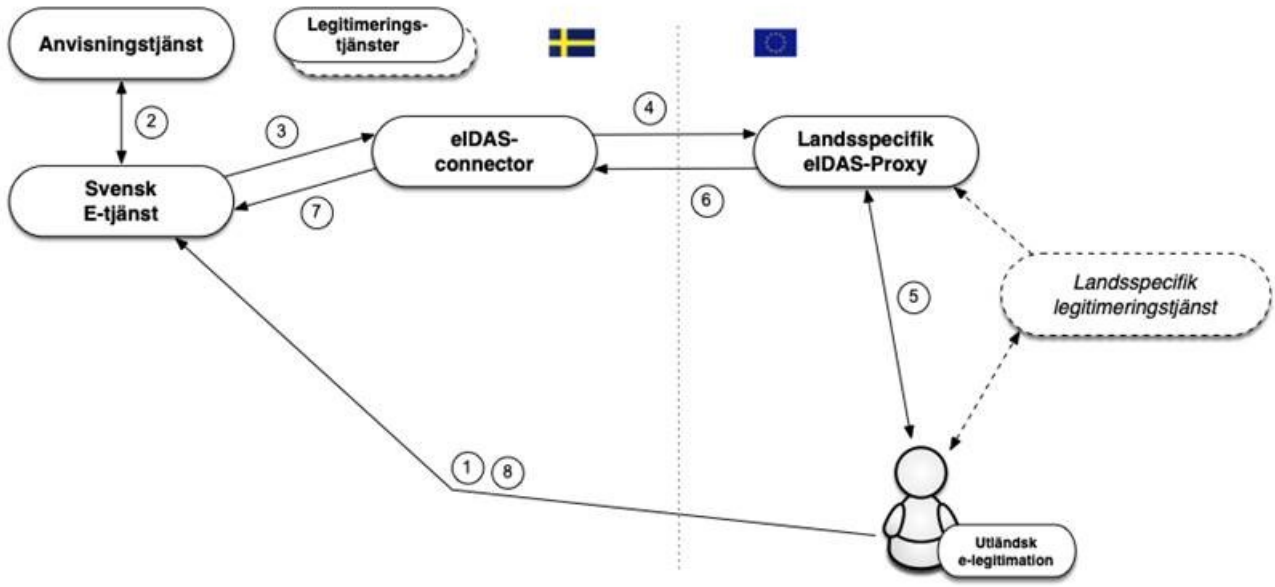
[2]: Svarbu pažymėti, kad ypač svarbu, jog naudotojas suvoktų šį procesą kaip dokumento pasirašymą. Todėl tai palaikančioms e. ID turėtų būti naudojamas parašo srautas, susijęs su „tapatumo nustatymu parašui“.

1.7. Techninė sistema ir eIDAS

Reglamente (ES) Nr. 910/2014 dėl elektroninės atpažinties ir patikimumo užtikrinimo paslaugų (eIDAS) reikalaujama, kad Švedijos viešosios įstaigos pripažintų e. ID, apie kurias pranešė kitos eIDAS šalys. Tai reiškia, kad tam tikromis taisyklėmis grindžiama Švedijos viešoji e. paslauga turi turėti galimybę pripažinti prisijungimą, atliktą naudojant kitoje šalyje išduotą e. ID.

1.7.1. Tapatumo nustatymas, naudojant užsienio e. ID

eIDAS techninės specifikacijos, kaip ir techninė sistema, grindžiamos SAML standartais, ir nors yra daug panašumų, šios specifikacijos taip pat skiriasi. Tačiau Švedijos e. paslauga neturėtų būti tiesiogiai susijusi su eIDAS techninėmis specifikacijomis. Toliau pateiktame paveikslėlyje parodyta, kaip Švedijos eIDAS mazgas (*eIDAS jungtis*) veikia kaip tiltas tarp kitų šalių ir Švedijos susiejimo, kai asmens tapatybė nustatoma naudojantis užsienio e. ID Švedijos e. paslaugoje. Švedijos eIDAS mazgas atitinka techninę sistemą.



Anvisningstjänst	Aptikimo paslauga
Legitimeringstjänster	Tapatumo nustatymo paslauga
Svensk E-tjänst	Švedijos e. paslauga
EiDAS-connector	eIDAS jungtis
Landsspecifik Eidas Proxy	Konkrečioms šalims skirtas eIDAS tarpinis serveris
Landsspecifik legitimeringstjänst	Konkrečios šalies tapatumo nustatymo paslauga
utländsk e-legitimation	užsienio e. ID

Srautas yra toks:

1. Naudotojas, turintis užsienio e. ID, prašo prieigos prie Švedijos e. paslaugos (t. y. prisijungia).

2. E. paslauga suteikia galimybę naudotojui pasirinkti prisijungimo būdą naudojantis aptikimo paslauga. Rodoma parinktis „Užsienio e. ID“, kurią naudotojas pasirenka eIDAS atveju.

3. Teikiant e. paslaugą pagal šią techninę sistemą sukuriama tapatumo nustatymo užklausa ir naudotojas nukreipiamas į Švedijos eIDAS mazgą (*jungtį*), už kurį atsakingas DIGG. eIDAS mazgas veikia kaip tapatumo nustatymo paslauga (*Tapatybės teikėjas*) susiejime Švedijos pasikliaujančiųjų šalių atžvilgiu, o tai reiškia, kad ryšys su šia paslauga vykdomas taip pat, kaip ir su kitomis tapatumo nustatymo paslaugomis susiejimuose, kurie atitinka techninę sistemą.

4. Gauta užklausa apdorojama ir eIDAS mazge rodomas pasirinkimo puslapis, kuriame naudotojas pasirenka „savo šalį“[1]. Tada Švedijos eIDAS mazgas gautą tapatumo nustatymo užklausą konvertuoja į eIDAS tapatumo nustatymo užklausą ir nukreipia naudotoją į pasirinktos šalies „eIDAS tarpinio serverio paslaugą“.

5. Kai pasirinktos šalies eIDAS tarpinio serverio paslauga gauna tapatumo nustatymo užklausą, perimama šios šalies tapatumo nustatymo technologija. Ne visos eIDAS šalys naudoja SAML tapatumui nustatyti, tačiau jei taip būtų mūsų pavyzdyje, naudotojas būtų nukreiptas į tapatumo nustatymo paslaugą (*Tapatybės teikėjas*), o prieš tai galbūt ir į aptikimo paslaugą, skirtą tapatumo nustatymo paslaugai pasirinkti.

6. Atlikus tapatumo nustatymo patvirtinimą, sukuriamas sertifikatas (*Tvirtinimas*) pagal eIDAS specifikacijas. Šis sertifikatas apima eIDAS būdingus požymius, pagal kuriuos identifikuojamas naudotojas. Šis sertifikatas dabar perduodamas Švedijos eIDAS mazgui.

7. Mazgas gauna sertifikatą ir patikrina jo tikslumą. Šis sertifikatas iš eIDAS formato transformuojamas į sertifikatą, suformatuotą pagal techninę sistemą, ir siunčiamas į e. paslaugą.

8. Pasikliaujančioji šalis prideda bet kokios papildomos informacijos ir nusprendžia, ar naudotojui turėtų būti suteikta prieiga prie paslaugos.

Todėl Švedijos e. paslaugoms reikia tik palaikyti techninę sistemą, kad būtų galima tvarkyti tapatumo nustatymą, atliekamą naudojant Europos e. ID. Tačiau e. paslauga turi gebėti elgtis su pateikta tapatybe, kuri nebūtinai yra asmens tapatybės numeris. Taigi gali būti atvejų, kai naudojantis e. paslauga naudotojo tapatybė nustatoma per eIDAS sistemą, tačiau naudotojo pateikta tapatybė negali būti naudojama e. paslaugoje. Daugiau apie tai – 1.7.3 skyriuje.

> [1]: Iš tiesų naudotojas pasirenka „eIDAS tarpinio serverio paslaugą“, kuriai turėtų būti persiųsta užklausa. Tai priklauso nuo šalies, kuriai priklauso naudotojo e ID išleidėjas.

1.7.2. Parašai, naudojant užsienio e. ID

Kaip jau minėta, šioje techninėje sistemoje taikomas elektroninio parašo modelis, vadinamas susietuoju parašu. Serverio pagrindu veikianti parašo paslauga yra susieta su e. paslauga, kuri savo ruožtu prašo parašo. Naudotojui pasirašius dokumentą, e. paslauga siunčia parašo užklausą parašo paslaugai. Tada parašo paslauga paprašo naudotojo, kad jis patvirtintų savo tapatybę. Prisijungdamas prie tapatumo nustatymo, naudotojas patvirtina parašą. Parašo paslauga siunčia duomenis atgal į e. paslaugą, o tada išsaugomi parašo duomenys, susiję su pasirašytu dokumentu.

Ši procedūra suteikia galimybę pasirašyti ir naudojant užsienio e. ID, nes parašo paslauga gali pasirinkti patvirtinti naudotojo tapatybę naudodama užsienio e. ID pagal 1.7.1 skirsnyje aprašytą procedūrą.

Šiuo atveju pasirašant Švedijos eIDAS mazgas yra atsakingas už naudotojo informavimą, kad tapatumo nustatymo tikslas yra pasirašyti dokumentą, kas paprašė parašo, ir bet kokią informaciją apie tai, kas pasirašoma. Tapatybės sertifikatas išduodamas tik tada, kai naudotojas patvirtina savo tapatybę (parašui), ir jis siunčiamas parašo paslaugai, kuri savo ruožtu sugeneruoja parašą.

1.7.3. Tapatybių valdymas

Kitų šalių tapatybės sertifikatai atitinka ES masto technines specifikacijas, parengtas eIDAS reglamento pagrindu. Šiame reglamente nustatyti požymiai, kuriuos kiekviena šalis visada turi nurodyti fiziniams asmenims ir organizacijoms (minimalus duomenų rinkinys, MDS). Kiekviena šalis turi priskirti unikalų identifikatorių kiekvienai e. ID, atstovaujantį tik vienam fiziniam asmeniui. Kai kuriose šalyse šie vieno asmens identifikatoriai bus unikalūs ir nuolatiniai, kaip, pavyzdžiui, Švedijos asmens tapatybės numeriai, tačiau šių identifikatorių sudėtis ir savybės gali labai skirtis. Viena iš savybių, kuri gali skirtis, yra tokio identifikatoriaus išliekamumas, t. y. ar toks identifikatorius išlieka nepakitęs per asmens gyvenimą arba pasikeičia, jei, pavyzdžiui, asmuo persikelia į kitą regioną, pakeičia savo vardą ar pavardę arba tiesiog pakeičia savo e. ID. Kai kuriose šalyse (pvz., Jungtinėje Karalystėje) identifikatorius skirsis priklausomai nuo to, kurią šalies e. ID naudotojas šiuo metu pasirinkęs naudoti.

Siekiant supaprastinti Švedijos e. paslaugų naudotojų valdymą, Švedijos eIDAS mazgas sukuria standartizuotą ID požymį naudotojams, kurių tapatybė buvo patvirtinta naudojant užsienio e. ID, vadinamą *laikinuoju ID* (sutrumpintai PRID). Be to, sukuriamas susijęs požymis, kuriuo deklaruojamas tikėtinas šio ID požymio išliekamumas arba gyvavimo trukmė. PRID požymis generuojamas remiantis požymių vertėmis, gautomis iš užsienio tapatumo nustatymo patvirtinimo pagal konkrečiai šaliai nustatytus metodus. Kiekvienas šalies ir metodo derinys skirstomas į kategorijas pagal tikėtiną išliekamumą, t. y. kokia tikimybė, kad laikui bėgant to paties asmens tapatybė pasikeis. Tai leidžia Švedijos e. paslaugoms pritaikyti ryšį su vartotoju ir aktyviai teikti funkcijas, padedančias naudotojui, kurio tapatybė pasikeitė, atgauti savo informacijos kontrolę e. paslaugoje.

Kai kuriais atvejais asmuo, kurio tapatybė patvirtinta naudojant užsienio e. ID, taip pat gali turėti Švedijos asmens tapatybės numerį. Tai gali būti, pavyzdžiui, Švedijos pilietis, persikėlęs į užsienį ir gavęs užsienio e. ID, arba Švedijoje registruotas užsienio pilietis, kuriam suteiktas asmens tapatybės numeris.

Tai, kad užsienio e. ID turintis asmuo turi Švedijos asmens tapatybės numerį, užsienio tapatumo nustatymo paslaugai paprastai nėra žinoma, todėl ši informacija neįtraukiama į šalies, kurioje patvirtinta asmens tapatybė, tapatybės sertifikatą. Kita vertus, Švedijos mazgas turi galimybę pateikti užklausą dėl požymių paslaugos Švedijoje[1], ar yra registruotas asmens, kurio tapatybė patvirtinta, tapatybės numeris ir, jeigu taip, gali pridėti tokią informaciją prie e. paslaugai siunčiamo tapatybės sertifikato.

> [1]: Rengiant šį dokumentą, nebuvo požymių paslaugos, kuri susietų eIDAS tapatybes ir Švedijos asmens tapatybės numerius.

1.7.4. Švedijos e. ID užsienio e. paslaugose

Švedija pranešė apie Švedijos e. ID, kurių saugumo užtikrinimo lygiai pagal eIDAS yra pakankami ir aukšti.

Užklausa dėl tapatumo nustatymo iš užsienio e. paslaugos pateikiama Švedijos eIDAS mazgui (tarpinio serverio paslauga) per eIDAS jungtį e. paslaugos šalyje. Švedijos eIDAS mazge naudotojas pasirenka, kurią Švedijos e. ID jis nori naudoti tapatybei nustatyti, ir tada tapatumo nustatymo užklausa siunčiama tapatumo nustatymo paslaugai (*Tapatybės teikėjas*),

kuri tvarko pasirinktą e. ID. Ši užklausa suformatuota pagal techninę sistemą, o tai reiškia, kad Švedijos tapatumo nustatymo paslauga neturi atitikti eIDAS techninių specifikacijų.

Švedijos tapatumo nustatymo paslauga patvirtina naudotojo tapatybę ir išduodamas tapatybės sertifikatas (pagal techninę sistemą). Šį sertifikatą gauna Švedijos eIDAS tarpinio serverio paslauga ir jis paverčiamas sertifikatu pagal eIDAS specifikacijas prieš jį persiunčiant į užsienio eIDAS jungtį, o vėliau – į skambinančiąją e. paslaugą (*Paslaugų teikėjas*).

2. Vietos skirstomojo tinklo operatoriaus

Šiame skyriuje pateikiamos tapatybės susiejimų specifikacijos ir profiliai, atitinkantys „Sweden Connect“ techninę sistemą, ir tam tikros susijusios paslaugos. Jei nenurodyta kitaip, šie dokumentai yra privalomi teikiant paslaugas tapatybės susiejimuose, įgyvendinančiuose techninę sistemą.

2.1. SAML profiliai ir specifikacijos

„Sweden Connect“ techninę sistemą atitinkantys tapatybės susiejimai kuriami remiantis „Švedijos e. ID sistemos diegimo profiliu“ [SAML.Profile]. Šiam profiliui įtakos turi „SAML V2.0 susiejimo sąveikumo diegimo profilis“ [SAML2Int], tačiau jis nėra nuo jo privalomai priklausomas. [SAML.Profile] taip pat apima Švedijos jungties techninei sistemai būdingas taisykles ir gaires.

2.1.1. Švedijos e. ID sistemos diegimo profilis

„Švedijos e. ID sistemos diegimo profilis“ (SAML.Profile) yra pagrindinis techninės sistemos dokumentas, kuriame, be kita ko, nurodyta:

- kaip turi būti sudaromi ir aiškinami SAML metaduomenys;
- kaip turi būti suformatuota tapatumo nustatymo užklausa;
- kaip tvarkoma tapatumo nustatymo užklausa ir kaip kuriamas, tikrinamas ir tvarkomas tapatybės sertifikatas;
- saugumo reikalavimai;
- konkretūs SAML reikalavimai, taikomi parašo paslaugoms ir „tapatumo nustatymo parašui“.

2.1.2. Švedijos e. ID sistema – identifikatorių registras

Švedijos e. ID infrastruktūrai įdiegti reikia įvairių formų identifikatorių, kad būtų galima pavaizduoti objektus duomenų struktūrose. Dokumente „Sweden Connect“ – identifikatorių registras“ [SC.Registry] apibrėžiama pagal techninę sistemą priskirtų identifikatorių struktūra, taip pat apibrėžtų identifikatorių registras.

2.1.3. Švedijos e. ID sistemos požymių specifikacija

Specifikacija „Švedijos e. ID sistemos požymių specifikacija“ [SAML.Attributes] deklaruoja SAML požymių profilius, kurie yra naudojami tapatybės susiejimuose, atitinkančiuose techninę sistemą, įskaitant tuos, kurie prisijungia prie eIDAS per Švedijos eIDAS mazgą.

2.1.4. Švedijos e. ID sistemos subjektų kategorijos

Subjektų kategorijos susiejime naudojamos įvairiais tikslais:

- Paslaugų subjektų kategorijos – naudojamos metaduomenyse siekiant parodyti e. paslaugų saugumo užtikrinimo lygiams ir prašomiems požymiams taikomus reikalavimus, taip pat tapatumo nustatymo paslaugų saugumo užtikrinimo lygiams pasiekti ir požymiams pateikti.

- Paslaugų savybių kategorijos – naudojamos konkrečiai paslaugos savybei nurodyti.

- Paslaugų rūšies subjektų kategorijos – naudojamos įvairioms susiejimo paslaugų rūšims nurodyti.

- Paslaugų sutarčių subjektų kategorijos – naudojamos paslaugų susitarimų formoms paskelbti ir pan.

- Bendrosios subjektų kategorijos – subjektų kategorijos, kurios nepriklauso nė vienai iš pirmiau nurodytų kategorijų.

Specifikacijoje „Švedijos e. ID sistemos subjektų kategorijos“ [SAML.EntCat] nurodomos subjektų kategorijos, apibrėžtos techninėje sistemoje, ir apibūdinama jų reikšmė.

2.1.5. eIDAS sukurtų požymių specifikacija Švedijos e. ID sistemai

Specifikacija „eIDAS sukurtų požymių specifikacija Švedijos e. ID sistemai“ [SC.eIDAS.Attrs] nustato procesus ir taisykles, kaip ID požymiai yra sukurti remiantis požymiais, gautais per tapatumo nustatymą eIDAS.

2.1.6. „BankID“ tapatybės paslaugų teikėjų įgyvendinimo profilis Švedijos e. ID sistemoje

Specifikacija „BankID“ tapatybės paslaugų teikėjų įgyvendinimo profilis Švedijos e. ID sistemoje“ [SAML.BankID] apibrėžia taisykles, kaip tapatumo nustatymo paslauga, kuri įgyvendina paramą „BankID“, turi būti suprojektuota.

> **Atkreipkite dėmesį į šiuos dalykus:** Ši specifikacija nėra privaloma siekiant užtikrinti atitiktį techninei sistemai. Tai aktualu tik toms tapatumo nustatymo paslaugoms, kurios įgyvendina „BankID“ palaikymą, ir elektroninėms paslaugoms, kurios jomis naudojasi. Tačiau tapatumo nustatymo paslaugos, kurios įdiegia „BankID“ palaikymą ir nori prisijungti prie „Sweden Connect“ susiejimo, turi atitikti šią specifikaciją.

2.1.7. Pagrindinio subjekto pasirinkimas SAML tapatumo nustatymo užklausose

Specifikacijoje „Pagrindinio subjekto pasirinkimas SAML tapatumo nustatymo užklausose“ [SAML.Principal] apibrėžiamas SAML plėtinys, leidžiantis pasikliaujančiajai šaliai informuoti tapatumo nustatymo paslaugą, kurios tapatybę ji nori patvirtinti.

2.1.8. Naudotojo pranešimo plėtinys SAML tapatumo nustatymo užklausose

Specifikacijoje „Naudotojo pranešimo plėtinys SAML tapatumo nustatymo užklausose“ [SAML.UMessage] apibrėžiamas SAML plėtinys, leidžiantis pasikliaujančiajai šaliai į tapatumo nustatymo užklausą, siunčiamą tapatumo nustatymo paslaugai, įtraukti vaizdinį pranešimą. Tapatumo nustatymo paslauga gali parodyti šį pranešimą naudotojui tapatumo nustatymo žingsnio metu.

2.2. „OpenID Connect“ profiliai ir specifikacijos

2.2.1. „OpenID Connect“ profilis, skirtas „Sweden Connect“

Profilis „OpenID Connect“ profilis, skirtas „Sweden Connect“, [OIDC.Profile], remiasi Švedijos „OpenID Connect“ profiliu, kuris yra „OpenID Connect“ profilis, sukurtas „OIDC Sweden“, siekiant skatinti sąveikumą ir saugumą Švedijos OIDC sprendimuose.

[OIDC.Profile] prideda papildomų reikalavimų, susijusių su „Sweden Connect“ susiejimu.

2.2.2. „OpenID Connect“ pretenzijų ir taikymo sričių specifikacija, skirta „Sweden Connect“

Specifikacija „OpenID Connect“ pretenzijų ir taikymo sričių specifikacija, skirta „Sweden Connect“ [OIDC.Claims], remiasi specifikacija „Pretenzijų ir taikymo sričių specifikacija, skirta Švedijos „OpenID Connect“ profiliui iš „OIDC Sweden“.

2.3. Parašo specifikacijos

Šiame skirsnyje pateikiamos nuorodos į dokumentus, kuriais apibrėžiamos parašo paslaugos susiejimuose, atitinkančiuose „Sweden Connect“ techninę sistemą.

2.3.1. OASIS DSS naudojimo pagrindinio pasirašymo paslaugose įgyvendinimo profilis

Įgyvendinimo profilis „OASIS DSS naudojimo pagrindinio pasirašymo paslaugose įgyvendinimo profilis“, [Sign.DSS.Profile], nurodo profilį parašo užklausai ir atsakymui pagal OASIS standartą „Skaitmeninio parašo paslaugos pagrindiniai protokolai, elementai ir įsipareigojimai“ [DSS].

2.3.2. DSS plėtinys sietinėms pagrindinio pasirašymo paslaugoms

„DSS plėtinys sietinėms pagrindinio pasirašymo paslaugoms“ [Sign.DSS.Ext] yra OASIS standarto „Skaitmeninio parašo paslaugos pagrindiniai protokolai, elementai ir

įsipareigojimai“ [DSS], kuriame pateikiamos pasirašymui pagal techninę sistemą būtinos apibrėžtys, plėtinys.

2.3.3. Pagrindinio pasirašymo paslaugų išduodamų sertifikatų profilis

Sertifikato profilis „Pagrindinio pasirašymo paslaugų išduodamų sertifikatų profilis“ [Sign.Cert.Profile] nurodo pasirašymo sertifikatų turinį. Šiame profilyje naudojamas naujas sertifikato plėtinys, kad būtų galima teikti parašo paslaugas.

Šiame profilyje nurodomas „Tapatumo nustatymo konteksto sertifikato plėtinys“ [AuthContext], kuriame aprašoma, kaip „Tapatumo nustatymo kontekstas“ pateikiamas X.509 sertifikatuose.

2.3.4. Sietinio pasirašymo parašo aktyvavimo protokolas

Specifikacijoje „Sietinio pasirašymo parašo aktyvavimo protokolas“ [Sign.Activation] apibrėžiamas „Parašo aktyvavimo protokolas“ (SAP), skirtas „Vienos kontrolės 2 užtikrinimo lygiui“ (SCAL2) įgyvendinti pagal standartą „prEN 419241 – Patikimos sistemos, palaikančios serverio pasirašymą“.

3. Nuorodų sąrašas

3.1. DIGG

[Digg.Tillit]

Švedijos e. atpažinties patikimumo sistema.

[SC.Registry]

„Sweden Connect“ – identifikatorių registras.

[SAML.Profile]

Diegimo profilis Švedijos e. ID sistemai.

[SAML.Attributes]

Švedijos e. ID sistemos požymių specifikacija.

[SAML.EntCat]

Švedijos subjektų kategorijos e. ID sistemai.

[SC.eIDAS.Attrs]

eIDAS sukurtų požymių specifikacija Švedijos e. ID sistemai.

[SAML.BankID]

Įgyvendinimo profilis „BankID“ tapatybės paslaugų teikėjams Švedijos e. ID sistemoje.

[SAML.Principal]

Pagrindinio subjekto pasirinkimas SAML tapatumo nustatymo užklausose.

[SAML.UMessage]

Naudotojo pranešimo plėtinys SAML tapatumo nustatymo užklausose.

[OIDC.Profile]

„OpenID Connect“ profilis, skirtas „Sweden Connect“.

[OIDC.Claims]

„OpenID Connect“ pretenzijų ir taikymo sričių specifikacija, skirta „Sweden Connect“.

[Sign.DSS.Profile]

OASIS DSS naudojimo pagrindinio pasirašymo paslaugose įgyvendinimo profilis.

[Sign.DSS.Ext]

DSS plėtinys sietinėms pagrindinio pasirašymo paslaugoms.

[Sign.Cert.Profile]

Centrinio pasirašymo paslaugų išduodamų sertifikatų profilis.

[Sign.Activation]

Sietinio pasirašymo parašo aktyvavimo protokolas.

3.2. Kitos nuorodos

[SAML2Int]

SAML V2.0 Diegimo profilis susietajai sąveikai.

[DSS]

OASIS standartas – Skaitmeninio parašo paslaugos pagrindiniai protokolai, elementai ir įsipareigojimai, 1.0 versija, 2007 m. balandžio 11 d.

[AuthContext]

RFC-7773 Tapatumo nustatymo konteksto sertifikato plėtinys.