Sissejuhatus Sweden Connecti tehnilisse raamistikku

2024-12-04

Viitenumber: **2019-267**

Sisukord

1. Sissejuhatus

1.1. Ülevaade

Sweden Connecti tehniline raamistik on kohandatud SAML 2.0-l põhinevatele identiteediföderatsioonidele.

> Tehnilise raamistiku viimases versioonis on kasutusele võetud ka spetsifikatsioonid OpenID Connecti jaoks. Praegu puudub OpenID Connecti jaoks föderatsiooni tugi. See võetakse kasutusele 2025. aastal.
>
> Käesoleva dokumendi ülejäänud osades kirjeldatakse ainult SAMLi föderatsiooni. Kui OpenID Connect on täielikult kasutusele võetud, käsitleb see dokument ka seda tehnoloogiat.

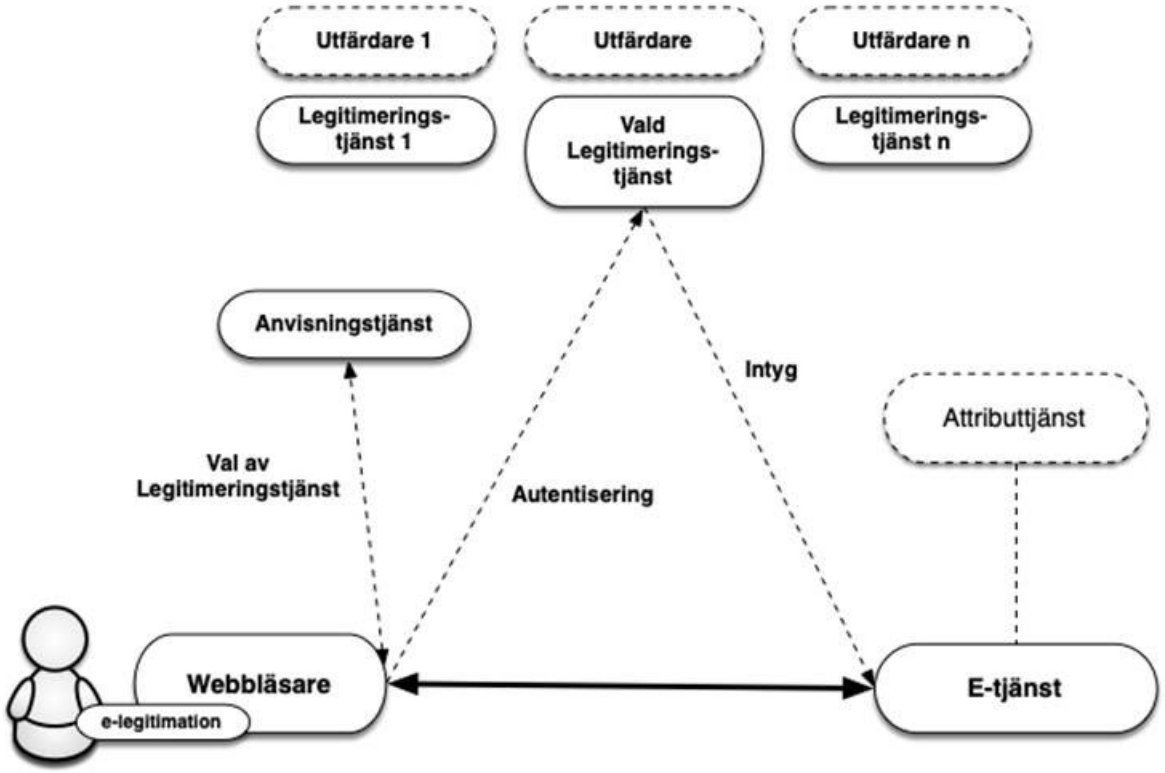
Tuginevad isikud saavad autentimisteenuselt standardses vormingus identiteedisertifikaadid[1].

Allkirja nõudvaid e-teenuseid ei ole vaja kohandada eri kasutajate eID-de jaoks, et luua e-allkirju. Selle asemel delegeerib e-teenus selle allkirjastamisteenusele, kus kasutajatele antakse autentimisteenuse kaudu autentimise toel võimalus allkirjastada elektroonilisi dokumente.

Föderatsioonis täidavad e-teenused ja vastavad tuginevad isikud teenuseosutaja (SP) rolli, samas olenemata e-teenusest, mille jaoks kasutaja autenditakse, võtavad identiteedisertifikaate väljastavad autentimisteenused endale identiteedipakkuja (IdP) ja seega kasutaja autentimise rolli.

Juhtudel, kui e-teenus vajab kasutaja kohta rohkem teavet, nt teavet õigus- ja teovõime kohta, võib esitada küsimuse föderatsiooni kuuluvale atribuuditeenusele, atribuudiasutusele (AA), kui selline asjakohane atribuuditeenus on olemas. Atribuuditaotluse kaudu saab e-teenus vajalikku täiendavat teavet kasutaja volitamiseks ja e-teenusele või samaväärsele teenusele juurdepääsu võimaldamiseks.

Kuna nii isikuandmed kui ka muud kasutajatega seotud atribuudid esitatakse identiteedi- ja atribuudisertifikaatide kaudu, saab igat liiki eID-sid, mille suhtes tuginevad isikud on kokku leppinud ja mis on osa föderatsioonist, kasutada autentimiseks e-teenuses, mis nõuab nii isikukoodi kui ka täiendavat teavet, isegi kui eID ei sisalda konkreetseid isikuandmeid (nt koodikastid ühekordsete paroolide genereerimiseks).



Utfärdare 1	Väljastaja 1
Utfärdare n	Väljastaja n
Legitimeringstjänst 1	Autentimisteenus 1
Vald legitimeringstjänst	Valitud autentimisteenus

Legitimeringstjänst n	Autentimisteenus n
Anvisningstjänst	Avastusteenus
Intyg	Sertifikaat
Val av legitimeringstjänst	Autentimisteenuse valik
autentisering	autentimine
attributtjänst	atribuuditeenus
Webbläsare	Brauser
E-tjänst	E-teenus

Joonis 1. *Illustratsioon identiteediföderatsiooni eri teenistuste vahelisest suhtlusest.*

[1]: Autentimisteenusele viidatakse muudes Diggi dokumentides ka kui identiteediteenusele ja sertifitseerimisteenusele. Käesolevas dokumendis kasutatakse siiski ainult mõistet „autentimisteenus“.

1.2. Usaldusraamistik ja turvalisuse tasemed

Turvalisuse taseme kohaldamise alus kasutaja autentimisel on e-teenusega nõutava e-identimise usaldustase. Selleks et need turvalisuse tasemed oleksid föderatsiooni raames võrreldavad, on Rootsi e-identimise usaldusraamistikus [Digg.Tillit] määratletud neli usaldusväärsuse taset (1–4) ja ELi eIDAS-e määruses kolm usaldusväärsuse taset (madal, märkimisväärne, kõrge). Kõik identiteedisertifikaatide väljaandjad peavad tõendama, et kogu identiteedisertifikaatide väljaandmise aluseks olev protsess vastab nõutava usaldusväärsuse taseme nõuetele, sealhulgas:

- identiteedisertifikaadi loomise nõuded;
- e-identimise (autentimise) nõuded;
- nõuded väljaandmisprotsessile;
- nõuded eID-le endale ja selle kasutamisele;
- eID väljastajale esitatavad nõuded;
- eID taotleja isikusamasuse tuvastamise nõue.

1.3. Metaandmete kogumise, haldamise ja avaldamise teenus

SAMLi föderatsioon annab SAMLi metaandmete kaudu teavet föderatsiooni osalejate kohta. Nii föderatsioonis autentimis- ja atribuuditeenuseid pakkuvaid üksusi kui ka tuginevaid isikuid, st üksusi, kes neid teenuseid tarbivad, nt e-teenused, käsitatakse föderatsiooni osalistena.

Föderatsiooni metaandmed võimaldavad osalejatel saada teavet teiste osalejate teenuste kohta, sealhulgas andmeid, mis on vajalikud turvaliseks teabevahetuseks osalejate vahel. Metaandmeid peavad kõik osapooled ajakohasena hoidma vastavalt lepingutingimustele.

Metaandmete peamine eesmärk on esitada võtmed/sertifikaadid, mis on vajalikud turvaliseks suhtluseks ja teabevahetuseks teenuste vahel. Lisaks võtmetele sisaldavad metaandmed ka muud teavet, mis on oluline teenustevaheliseks suhtluseks, näiteks nõutavate funktsioonide aadressid, teave usaldusväärsuse tasemete, teenusekategooriate, kasutajaliidese teabe jms kohta.

Identiteediföderatsioon määratletakse XML-vormingus registri kaudu, mis on allkirjastatud föderatsiooni käitaja sertifikaadiga. Fail sisaldab teavet identiteediföderatsiooni liikmete, sealhulgas nende sertifikaatide kohta. Kuna metaandmete fail on allkirjastatud, piisab sertifikaadi võrdlemisest metaandmete vastega. Kesksel föderatsiooniregistril põhinev taristu nõuab registri pidevat ajakohastamist ja seda, et föderatsiooni liikmed kasutaksid alati faili uusimat versiooni.

1.4. Avastusteenus

Identiteediföderatsioonis on võimalik pakkuda ja tarbida jagatud avastusteenust, milles loetletakse autentimisteenused, mille vahel kasutaja saab valida. Sellise avastusteenuse eesmärk on vabastada identiteediliitu kuuluvad üksikud e-teenused kasutaja autentimisteenuse (või sisselogimismeetodi) valimisel toe rakendamisest.

Kuna avastusteenus on identimisföderatsioonis saadaval, saavad e-teenused suunata oma kasutajad autentimisteenuse valimiseks sinna. Avastusteenus suhtleb kasutajaga, kes teeb oma valiku, ja kasutaja suunatakse koos oma valikuga tagasi e-teenusesse, mis nüüd teab, millisesse autentimisteenusesse tuleks kasutaja autentimiseks saata.

Sweden Connecti föderatsioonil ei ole praegu ühist avastusteenust.

1.5. Integratsioon tugineva isiku juures

Tuginevad isikud, nt e-teenused, integreeruvad autentimisteenustega standardiseeritud sõnumite kaudu ja kasutavad identiteedisertifikaate, millel on ka standardiseeritud vormingud.

Sweden Connecti tehnilist raamistikku mõjutab koostalitlusprofiil „SAML V2.0 Deployment Profile for Federation Interoperability“ [SAML2Int]. Profiili toetavad mitmed kommertstooted ja avatud lähtekoodiga lahendused, mis hõlbustavad integreerimist e-teenustes.

Paljud e-teenused kasutavad eraldiseisvaid autentimislahendusi, mis tähendab, et integratsiooni kohandamisel tehnilise raamistikuga on e-teenusele kui sellisele piiratud mõju.

1.6. Allkiri

Allkirjastamisel võimaldab Sweden Connecti tehniline raamistik kasutada eri liiki eID-sid, isegi neid, mis ei ole sertifikaadipõhised, ilma et e-teenuses oleks vaja teha erikohandusi. Seda seetõttu, et elektrooniliselt väljastatud isikutunnistusel (mida kasutatakse kasutajate tuvastamiseks allkirjastamisel) on sama vorming, olenemata kasutaja kasutatavast e-identimise liigist.

Allkirjateenuse eesmärk on võimaldada identiteediföderatsioonides allkirju, mis vastavad tehnilisele raamistikule ja mida toetavad igat liiki eID-d, mis pakuvad piisavat turvalisust.

Hankimise[1] kaudu ning võttes kasutusele allkirjateenuse, saab föderatsiooni kuuluv tuginev isik lubada kasutajal allkirjastada elektroonilise dokumendi allkirjateenuse toel. Kasutaja e-allkirja ja sellega seotud allkirjasertifikaadi loob allkirjateenus pärast seda, kui kasutaja on nõustunud allkirja andma, autentides end allkirjateenuse[2] kaudu.

[1]: Samuti on võimalik rakendada tehnilise raamistiku spetsifikatsioonidel põhinevat allkirjateenust või muul viisil omandada allkirjateenus.

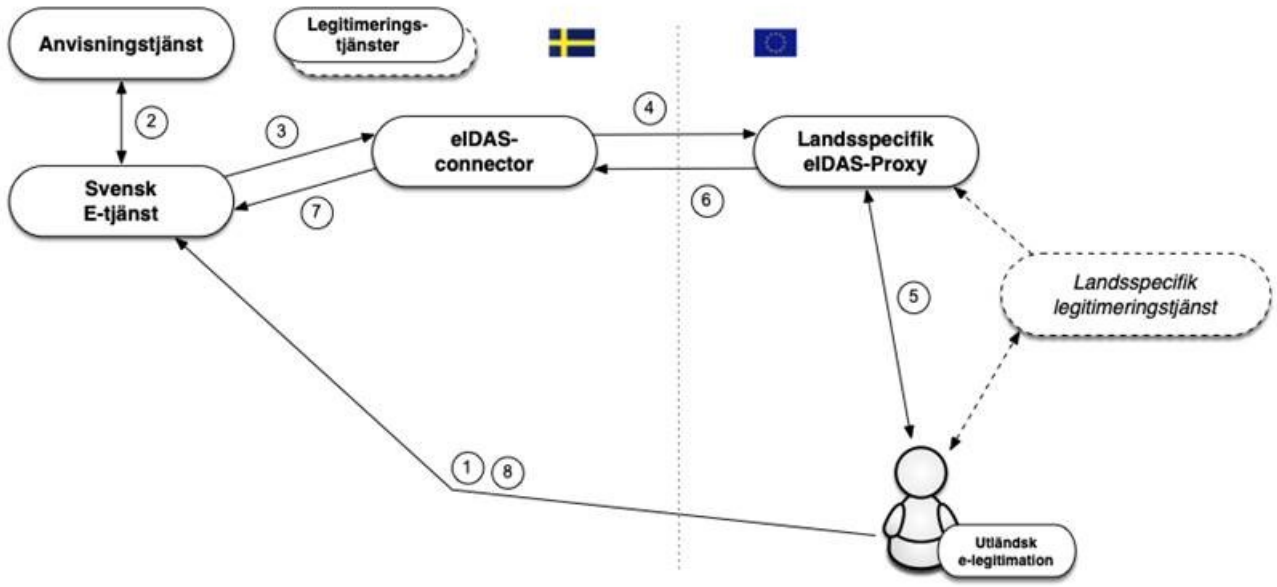
[2]: Oluline on märkida, et on äärmiselt tähtis, et kasutaja tajuks seda protsessi dokumendi allkirjastamisena. Seepärast tuleks seda toetavate e-identimise vahendite puhul kasutada allkirjavoogu seoses „autentimisega allkirjastamiseks“.

1.7. Tehniline raamistik ja eIDAS

ELi määruses (EL) nr 910/2014 e-identimise ja usaldusteenuste kohta (eIDAS) nõutakse, et Rootsi ametiasutused tunnustaksid e-iD-sid, millest teised eIDAS-e riigid on teatanud. See tähendab, et Rootsi avalikul e-teenusel, mis põhineb teatud reeglitel, peab olema võimalik aktsepteerida sisselogimist, mis on tehtud teises riigis väljastatud eID abil.

1.7.1. Autentimine välisriikide eID-de abil

eIDAS-e tehnilised kirjeldused põhinevad, sarnaselt tehnilise raamistikuga, SAMLi standarditel ja kuigi on palju sarnasusi, on ka nendes kirjeldustes erinevusi. Rootsi e-teenus ei tohiks siiski olla otseselt seotud eIDAS-e tehniliste kirjeldustega. Alljärgnev pilt illustreerib, kuidas Rootsi eIDAS-e sõlm (*eIDAS-e ühendaja*) toimib sillana teiste riikide ja Rootsi föderatsiooni vahel, kui isiku autentimiseks kasutatakse Rootsi e-teenuses välisriigi eID-d. Rootsi eIDAS-e sõlm vastab tehnilisele raamistikule.



Anvisningstjänst	Avastusteenus
Legitimeringstjänster	Autentimisteenused
Svensk E-tjänst	Rootsi e-teenus
EiDAS-connector	eiDAS-e ühendaja

Landsspecifik Eidas Proxy	Riigipõhine eIDAS-e asendaja
Landsspecifik legitimeringstjänst	Riigipõhine autentimisteenus
utländsk e-legitimation	välisriigi eID

Voog on järgmine:

1. Välisriigi eID kasutaja taotleb juurdepääsu Rootsi e-teenusele (s.t logib sisse).

2. E-teenus võimaldab kasutajal avastusteenuse abil valida sisselogimismeetodi. Kuvatakse valik „Välismaine eID“, mille kasutaja valib eIDAS-e puhul.

3. E-teenus loob sellele tehnilisele raamistikule vastava autentimistaotluse ja suunab kasutaja Rootsi eIDAS-e sõlme (*ühendaja*), mille eest DIGG vastutab. eIDAS-e sõlm toimib föderatsioonis autentimisteenusena (*identiteedi pakkuja*) Rootsi tuginevate isikute suhtes, mis tähendab, et teabevahetus selle teenusega toimub samamoodi nagu muude autentimisteenustega föderatsioonides, mis vastavad tehnilisele raamistikule.

4. Saadud taotlust töödeldakse ja eIDAS-e sõlm kuvab valikulehe, kus kasutaja valib „oma riigi“[1]. Rootsi eIDAS-e sõlm konverteerib saadud autentimistaotluse nüüd eIDAS-e autentimistaotluseks ja suunab kasutaja valitud riigi eIDAS-e puhverserveriteenuse juurde.

5. Kui eIDAS-e puhverserveri teenus saab valitud riigi autentimistaotluse, võtab selle riigi autentimistehnoloogia üle. Mitte kõik eIDAS-e riigid ei kasuta SAMLi autentimiseks, kuid kui see oleks nii meie näites, suunataks kasutaja autentimisteenusesse (*identiteedi pakkuja*) ja enne seda võib-olla ka autentimisteenuse valimise otsinguteenusesse.

6. Kui autentimine on tehtud, luuakse sertifikaat (*kinnitus*) vastavalt eIDAS-e spetsifikatsioonidele. Sertifikaat sisaldab eIDAS-e spetsiifilisi atribuute, mis tuvastavad kasutaja. Sertifikaat on nüüd edastatud Rootsi eIDAS-e sõlme.

7. Sõlm saab sertifikaadi ja kontrollib selle täpsust. Sertifikaat muudetakse eIDAS-e vormingust tehnilise raamistiku kohaselt vormindatud sertifikaadiks ja saadetakse e-teenindusse.

8. Tuginev isik lisab mis tahes täiendavat teavet ja otsustab, kas kasutajale tuleks anda juurdepääs teenusele.

Rootsi e-teenused peavad seega üksnes toetama tehnilist raamistikku, et hallata Euroopa eID abil tehtavat autentimist. E-teenus peab siiski suutma käsitleda esitatud identiteeti, mis ei pruugi olla isikukood. Seega võib esineda juhtumeid, kus e-teenus autendib kasutaja eIDAS-e raamistiku kaudu, kuid kasutaja esitatud identiteeti ei saa e-teenuses kasutada. Rohkem teavet selle kohta on esitatud allpool jaotises 1.7.3.

[1]: Tegelikult valib kasutaja „eIDAS-e puhverserveri teenuse“, millele päring edastada tuleks. See sõltub riigist, kuhu kasutaja eID väljastaja kuulub.

1.7.2. Välisriikide eID-dega antud allkirjad

Nagu juba kirjeldatud, kasutatakse selles tehnilises raamistikus e-allkirja mudelit, mida nimetatakse föderatiivseks allkirjaks. E-teenusega on seotud serveripõhine allkirjastamisteenus, mis omakorda nõuab allkirja. Kui kasutaja dokumendi allkirjastab, saadab e-teenus allkirjataotluse allkirjateenusele. Seejärel palub allkirjastamisteenus kasutajal end autentida. Autentimisega seoses kinnitab kasutaja allkirja. Allkirjateenus saadab andmed tagasi e-teenindusse ja seejärel salvestatakse allkirjastatud dokumendiga seotud allkirjaandmed.

See protseduur võimaldab allkirja anda ka välisriigi eID-ga, kuna allkirjastamisteenus saab kasutaja autentida välisriigi eID-ga vastavalt punktis 1.7.1 kirjeldatud protseduurile.

Allkirjastamisel vastutab sellisel juhul Rootsi eIDAS-e sõlm kasutaja sellest teavitamise eest, et autentimise eesmärk on allkirjastada dokument, kes on allkirja küsinud ja selle eest, et anda mis tahes teavet selle kohta, mida allkirjastatakse. Identiteedisertifikaat väljastatakse alles siis, kui kasutaja on end autentinud (allkirjastamiseks) ja see saadetakse allkirjateenusele, mis omakorda genereerib allkirja.

1.7.3. Identiteetide haldamine

Teiste riikide isikutunnistused vastavad kogu ELi hõlmavatele tehnilistele kirjeldustele, mis on välja töötatud eIDAS-e määruse raames. Atribuudid, mida iga riik peab alati hõlmama nii füüsiliste isikute kui ka organisatsioonide puhul („miinimumandmestik“, MDS), on sätestatud käesolevas määruses. Iga riik peab iga eID kohta lisama kordumatu tunnuse, mis tähistab ainult üht füüsilist isikut. Mõnes riigis on need identifikaatorid isiku kohta kordumatud ja püsivad samamoodi nagu näiteks Rootsi isikukoodid, kuid neil identifikaatoritel võivad olla väga erinevad koostised ja omadused. Üks tunnus, mis võib varieeruda, on sellise identifikaatori püsivus, st kas selline identifikaator jääb isiku eluea jooksul muutumatuks või muutub näiteks siis, kui isik kolib teise piirkonda, muudab oma nime või muudab lihtsalt oma e-identimist. Mõnes riigis (nt Ühendkuningriigis) varieerub identifikaator sõltuvalt sellest, millist riigi eID-d kasutaja praegu kasutab.

Rootsi e-teenustes kasutajate haldamise lihtsustamiseks loob Rootsi eIDAS-e sõlm standarditud ID-atribuudi kasutajatele, kes on autenditud välismaise eID abil, mida tuntakse kui *esialgset identifitseerimisnumbrit* (lühendatult PRID). Lisaks luuakse seotud atribuut, mis deklareerib selle ID-atribuudi eeldatava püsivuse või eluea. PRID-atribuut luuakse atribuudiväärtuste põhjal, mis on saadud välismaise autentimise teel vastavalt konkreetse riigi jaoks kindlaksmääratud meetoditele. Iga riigi ja meetodi kombinatsioon on liigitatud eeldatava püsivuse alusel, s.t kui tõenäoline on, et sama isiku identiteet aja jooksul muutub. See võimaldab Rootsi e-teenustel kohandada suhtlust kasutajaga ja pakkuda ennetavalt funktsioone, mis hõlbustavad kasutajal, kelle identiteet on muutunud, taastada e-teenuses kontroll oma teabe üle.

Mõnel juhul võib välisriigi eID abil autenditud isikul olla ka Rootsi isikukood. Ta võib olla näiteks Rootsi kodanik, kes on kolinud välismaale ja saanud välisriigi eID, või välisriigi kodanik, kes on registreeritud Rootsis ja kellele on antud isikukood.

Asjaolu, et välisriigi eID-ga isikul on Rootsi isikukood, ei ole välisriigi autentimisteenistusele tavaliselt teada ja seetõttu ei sisaldu see teave isiku autentimise riigi isikutõendis. Rootsi sõlmpunktil on seevastu võimalus teha Rootsis[1] atribuuditeenusele päring, kas autenditud

isikul on registreeritud isikukood, ja kui see on nii, lisada selline teave e-teenusele saadetavale isikutunnistusele.

> [1]: Kirjutamise ajal puudub atribuuditeenus, mis looks seose eIDAS-e identiteetide ja Rootsi isikukoodide vahel.

1.7.4. Rootsi eID-d välisriikide e-teenustes

Rootsi on teatanud Rootsi eID-dest, mille usaldusväärsuse tase on eIDAS-e kohaselt märkimisväärne ja kõrge.

Välisriigi e-teenusest autentimise taotlus esitatakse Rootsi eIDAS-e sõlme (asendusteenuse) kaudu eIDAS-e konnektori abil e-teenuse riigis. Rootsi eIDAS-e sõlmes valib kasutaja, millise Rootsi eID abil ta soovib end autentida, ning seejärel saadetakse autentimisteenusele autentimistaotlus (*identiteedi pakkuja*), mis käitleb valitud eID-d. Taotlus on vormindatud vastavalt tehnilisele raamistikule, mis tähendab, et Rootsi autentimisteenus ei pea vastama eIDAS-e tehnilistele kirjeldustele.

Kasutaja autenditakse Rootsi autentimisteenuse abil ja isikutunnistus antakse välja (vastavalt tehnilisele raamistikule). Selle sertifikaadi võtab vastu Rootsi eIDAS-e puhverserver ja see muudetakse sertifikaadiks vastavalt eIDAS-e spetsifikatsioonidele, enne kui see edastatakse välismaisele eIDAS-e konnektorile ja seejärel päringut tegevale e-teenusele (*teenuseosutaja*).

2. Kohaliku jaotusvõrgu ettevõtja

See peatükk sisaldab Sweden Connecti tehnilisele raamistikule vastavate identiteediföderatsioonide ja teatavate seotud teenuste kirjeldusi ja profiile. Kui ei ole sätestatud teisiti, on need dokumendid nõutavad teenuste osutamiseks tehnilist raamistikku rakendavates identiteediföderatsioonides.

2.1. SAMLi profiilid ja spetsifikatsioonid

Sweden Connecti tehnilisele raamistikule vastavad identiteediföderatsioonid põhinevad Rootsi eID raamistiku kasutuselevõtuprofiilil [SAML.Profile]. Seda profiili mõjutab „SAML V2.0 kasutuselevõtuprofiil föderatsiooni koostalitlusvõime jaoks“ (SAML2Int), kuid see ei ole normatiivselt sellest sõltuv. [SAML.Profile] sisaldab ka Sweden Connecti tehnilise raamistikuga seotud eeskirju ja suuniseid.

2.1.1. Kasutuselevõtu profiil Rootsi eID raamistiku jaoks

„Kasutuselevõtu profiil Rootsi eID raamistiku jaoks“ [SAML.Profile] on peamine tehniline raamdokument ja selles täpsustatakse muu hulgas järgmist:

- kuidas SAMLi metaandmeid koostatakse ja tõlgendatakse;
- kuidas autentimistaotlus vormistatakse;
- kuidas autentimistaotlust käsitletakse ning kuidas identiteedisertifikaati koostatakse, kontrollitakse ja käsitletakse;

- turvanõuded;
- SAMLi erinõuded allkirjastamisteenustele ja „allkirjastamiseks autentimisele“.

2.1.2. Rootsi eID raamistik – identifikaatorite register

Rootsi eID taristu rakendamiseks on vaja eri liiki identifikaatoreid, et esindada objekte andmestruktuurides. Dokumendis „Sweden Connect – identifikaatorite register“ [SC.Registry] määratletakse tehnilise raamistiku alusel määratud identifikaatorite struktuur ning määratletud identifikaatorite register.

2.1.3. Atribuudi spetsifikatsioon Rootsi eID raamistiku jaoks

Spetsifikatsioon „Atribuudi spetsifikatsioon Rootsi eID raamistiku jaoks“ [SAML.Attributes], määratleb SAMLi atribuudiprofiilid, mis on kasutusel identiteediföderatsioonides, mis vastavad tehnilisele raamistikule, sealhulgas sellised, mis ühenduvad eIDAS-ega Rootsi eIDAS-sõlme kaudu.

2.1.4. Üksuste kategooriad eID raamistiku jaoks

Üksuste kategooriaid kasutatakse föderatsioonis mitmel erineval eesmärgil.

- Teenusüksuse kategooriad – kasutatakse metaandmetes, et kajastada e-teenuste nõudeid usaldusväärsuse tasemetele ja nõutud atribuutidele, samuti autentimisteenuste vastavust usaldusväärsuse tasemetele ja atribuutide edastamist.
- Teenusomandi kategooriad – kasutatakse teenuse konkreetse omaduse väljendamiseks.
- Teenusetüübi üksuse kategooriad – kasutatakse föderatsiooni eri teenuseliikide tähistamiseks.
- Teenuslepingu üksuste kategooriad – mida talitused kasutavad lepinguvormide jms väljakuulutamiseks.
- Üldiste üksuste kategooriad – üksuste kategooriad, mis ei kuulu ühegi eespool nimetatud liigi alla.

Spetsifikatsioonis „Üksuste kategooriad eID raamistiku jaoks“ [SAML.EntCat] täpsustatakse tehnilise raamistikuga määratletud üksuste kategooriad ja kirjeldatakse nende tähendust.

2.1.5. eIDAS-e konstrueeritud atribuutide spetsifikatsioon Rootsi eID raamistiku jaoks

Spetsifikatsioon „eIDAS-e konstrueeritud atribuutide spetsifikatsioon Rootsi eID raamistiku jaoks“ [SC.eIDAS.Attrs], määratleb protsessid ja reeglid selle kohta, kuidas ID-atribuudid koostatakse atribuutide põhjal, mis on saadudautentimise käigus eIDAS-is..

2.1.6. Rakendusprofiil BankID identiteedipakkujatele Rootsi eID raamistikus

Spetsifikatsioon „Rakendusprofiil BankID identiteedipakkujatele Rootsi eID raamistikus“ [SAML.BankID], määratleb reeglid selle kohta, kuidas autentimisteenus, mis rakendab toetust BankID jaoks, peab olema kavandatud.

> **Palun pange tähele järgmist:** Käesolev spetsifikatsioon ei ole tehnilise raamistiku järgimiseks kohustuslik. See on asjakohane ainult autentimisteenuste puhul, mis toetavad BankID-d ja neid kasutavaid e-teenuseid. Autentimisteenused, mis toetavad BankID-d ja soovivad liituda Sweden Connecti föderatsiooniga, peavad siiski vastama sellele spetsifikatsioonile.

2.1.7. SAMLi autentimistaotluste põhivalik

Spetsifikatsioonis „SAMLi autentimistaotluste põhivalik“ (SAML.Principal) määratletakse SAMLi laiendus, mis võimaldab tugineval isikul teatada autentimisteenusele, millist identiteeti ta soovib autentida.

2.1.8. Kasutajasõnumi laiendamine SAMLi autentimistaotlustes

Spetsifikatsiooniga „Kasutajasõnumi laiendamine SAMLi autentimistaotlustes“ [SAML.UMessage] määratakse kindlaks SAMLi laiendus, mis võimaldab tugineval isikul lisada autentimisteenusele saadetavasse autentimistaotlusse kuvateate. Autentimisteenus saab seejärel seda teadet autentimisetapis kasutajale näidata.

2.2. Profiilid ja spetsifikatsioonid OpenID Connecti jaoks

2.2.1. OpenID Connecti profiil Sweden Connecti jaoks

Profiil „OpenID Connecti profiil Sweden Connecti jaoks“ [OIDC.Profile], põhineb Rootsi OpenID Connect profiilil, mis on OpenID Connecti profiil, mille on arendanud OIDC Sweden, et edendada Rootsi OIDC lahenduste koostalitlusvõimet ja turvalisust.

[OIDC.Profile] lisab Sweden Connecti föderatsioonile täiendavad nõuded.

2.2.2. OpenID Connecti nõuete ja kohaldamisalade spetsifikatsioon Sweden Connecti jaoks

Tootespetsifikatsioon „OpenID Connecti nõuete ja kohaldamisalade spetsifikatsioon Sweden Connecti jaoks“ [OIDC.Claims], põhineb OIDC Swedeni spetsifikatsioonil „Nõuete ja kohaldamisalade spetsifikatsioon Rootsi OpenID Connecti profiili jaoks“.

2.3. Spetsifikatsioonid allkirja jaoks

See jaotis sisaldab viiteid dokumentidele, millega määratakse kindlaks allkirjastamisteenused föderatsioonides, mis vastavad Sweden Connecti tehnilisele raamistikule.

2.3.1. Rakendusprofiil OASIS DSSi kasutamiseks keskses allkirjastamisteenuses

Rakendusprofiil „Rakendusprofiil OASIS DSSi kasutamiseks keskses allkirjastamisteenuses“ [Sign.DSS.Profile], täpsustab profiili allkirjataotluse ja vastuse jaoks vastavalt OASISe standardile „Digitaalse allkirja teenuse põhiprotokollid, -elemendid ja -sidemed“ [DSS].

2.3.2. DSSi laiendus föderaalse keskse allkirjastamisteenuse jaoks

„DSS laiendus föderaalse keskse allkirjastamisteenuse jaoks“ [Sign.DSS.Ext] on OASISe standardi „Digitaalse allkirja teenuse põhiprotokollid, -elemendid ja -sidemed“ [DSS] laiendus, millega täpsustatakse tehnilises raamistikus allkirjastamiseks vajalikke määratlusi.

2.3.3. Sertifikaadiprofiil keskse allkirjastamisteenuse poolt väljaantud sertifikaatide puhul

Sertifikaadiprofiil „Sertifikaadiprofiil keskse allkirjastamisteenuse poolt väljaantud sertifikaatide puhul“ [Sign.Cert.Profile], täpsustab sertifikaatide allkirjastamise sisu. See profiil rakendab allkirjastamisteenuste toetamiseks uue sertifikaadilaiendi.

See profiil viitab „Autentimise kontekstisertifikaadi laiendusele“ [AuthContext], mis kirjeldab, kuidas „autentimise kontekst“ on esitatud X.509 sertifikaatides.

2.3.4. Allkirjastamise aktiveerimise protokoll föderaalseks allkirjastamiseks

Spetsifikatsioonis „Allkirjastamise aktiveerimise protokoll föderaalseks allkirjastamiseks“ [Sign.Activation] määratletakse „allkirja aktiveerimise protokoll“ (SAP) „Ühtse kontrolli 2. taseme“ (SCAL2) rakendamiseks vastavalt standardile „prEN 419241 – Usaldusväärsed serveripõhist allkirjastamist toetavad süsteemid“.

3. Võrdlusnimekiri

3.1. DIGG

[Digg.Tillit]

Rootsi e-identimise usaldusraamistik.

[SC.Registry]

Sweden Connect – identifikaatorite register.

[SAML.Profiil]

Rootsi eID raamistikule vastav kasutuselevõtu profiil.

[SAML.Attributes]

Rootsi eID raamistiku atribuudi spetsifikatsioon.

[SAML.EntCat]

Üksuse kategooriad Rootsi eID raamistikus.

[SC.eIDAS.Attrs]

eIDAS-e konstrueeritud atribuutide spetsifikatsioon Rootsi eID raamistiku jaoks.

[SAML.BankID]

Rakendusprofiil BankID identiteedipakkujatele Rootsi eID raamistikus.

[SAML.Principal]

SAMLi autentimistaotluste põhivalik.

[SAML.UMessage]

Kasutaja sõnumi laiend SAMLi autentimistaotlustes.

[OIDC.Profile]

OpenID Connecti profiil Sweden Connecti jaoks.

[OIDC.Claims]

OpenID Connecti nõuete ja ulatuse spetsifikatsioon Sweden Connecti jaoks.

[Sign.DSS.Profile]

Rakendusprofiil OASIS DSSi kasutamiseks allkirjastamise keskteenustes.

[Sign.DSS.Ext]

DSSi laiendus föderaalsete kesksete allkirjastamisteenuste jaoks.

[Sign.Cert.Profile]

Sertifikaadiprofiil sertifikaatide puhul, mille on välja andnud kesksed allkirjastamisteenused.

[Sign.Activation]

Allkirja aktiveerimise protokoll föderaalse allkirjastamise jaoks.

3.2. Muud viited

[SAML2Int]

SAML V2.0 kasutuselevõtuprofiil föderatiivse koostalitlusvõime jaoks.

[DSS]

OASIS Standard – digiallkirja teenuse põhiprotokollid, elemendid ja sidemed, versioon 1.0, 11. aprill 2007.

[AuthContext]

RFC-7773 Autentimiskonteksti sertifikaadi laiendus.