Uvod u Tehnički okvir za Sweden Connect

2024-12-04

Referentni broj: **2019-267**

Sadržaj

1. Uvod

1.1. Pregled

Tehnički okvir za Sweden Connect prilagođen je federacijama identiteta na temelju SAML 2.0.

U najnovijoj verziji tehničkog okvira također su uvedene su specifikacije za OpenID Connect. Trenutačno ne postoji podrška federacije identiteta za OpenID Connect. Uvest će se 2025.

Ostali dijelovi ovog dokumenta opisuju samo federaciju identiteta SAML. Nakon što se OpenID Connect u potpunosti uvede, ovaj će dokument obuhvaćati i tu tehnologiju.

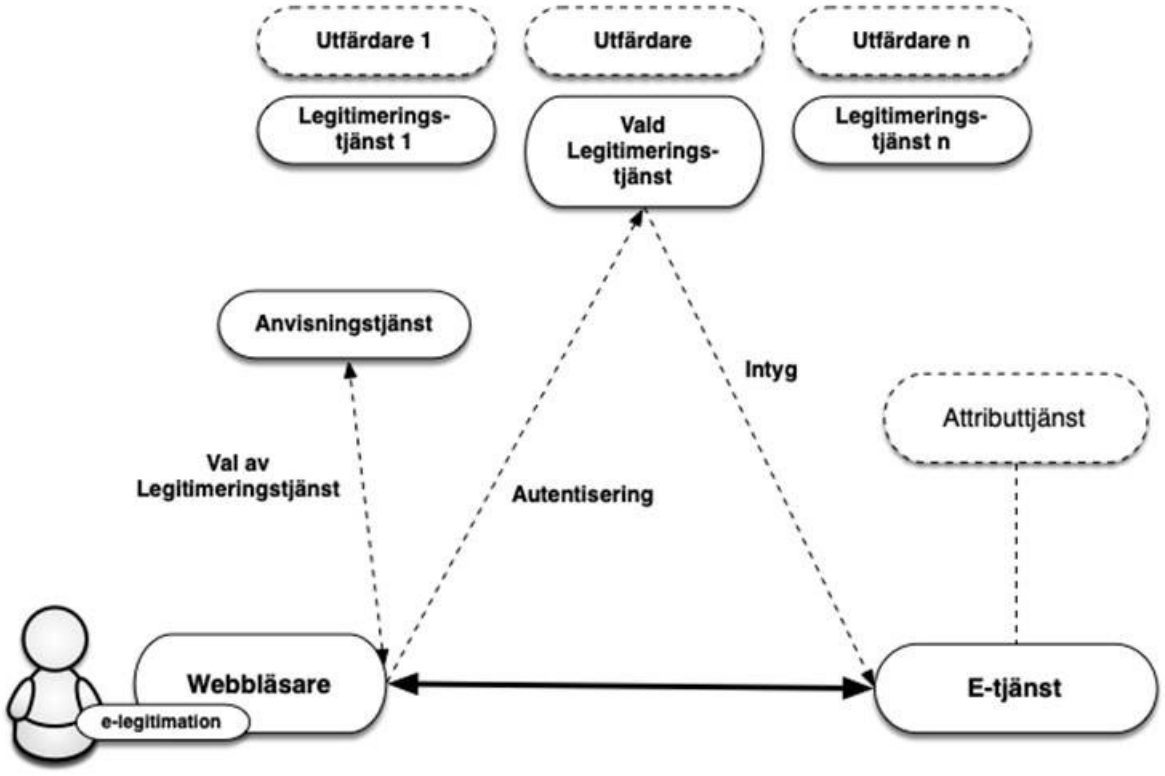
Pouzdajuće strane od usluge autentifikacije dobivaju certifikate o identitetu u standardiziranom formatu[1].

E-usluge za koje je potreban potpis ne moraju se prilagoditi eID-ovima različitih korisnika kako bi se izradili elektronički potpisi. Umjesto toga, e-usluga to delegira usluzi potpisivanja, pri čemu korisnici, uz autentifikaciju putem usluge autentifikacije, imaju priliku potpisati elektroničke dokumente.

Unutar povezivanja, e-usluge i odgovarajuće pouzdajuće strane preuzimaju ulogu pružatelja usluga (SP), dok usluge autentifikacije koje izdaju certifikate o identitetu preuzimaju ulogu pružatelja identiteta (IdP), a time i autentifikatora korisnika, bez obzira na e-uslugu za koju se korisnik autentificira.

U slučajevima u kojima su e-usluzi potrebne dodatne informacije o korisniku, npr. informacije o pravnoj sposobnosti, može se postaviti pitanje usluzi atributa, tijelu za atribute (AA), unutar povezivanja, ako takva relevantna usluga atributa postoji. Zahtjevom za dodjelu atributa e-usluga može dobiti potrebne dodatne informacije kako bi ovlastila korisnika i omogućila pristup e-usluzi ili jednakovrijednoj usluzi.

Budući da se osobni podaci o identitetu i drugi atributi povezani s korisnicima pružaju putem potvrda o identitetu i potvrda o atributima, sve vrste eID-ova o kojima pouzdajuće strane imaju dogovor i koji su dio federacije identiteta mogu se upotrebljavati za autentifikaciju u odnosu na e-uslugu za koju su potrebni i osobni identifikacijski broj i dodatne informacije, čak i ako eID ne sadržava nikakve posebne osobne podatke (npr. okviri za kodiranje za generiranje jednokratnih lozinki).



Utfärdare 1	Izdavatelj 1
Utfärdare n	Izdavatelj n

Legitimeringstjänst 1	Usluga autentifikacije 1
Vald legitimeringstjänst	Odabrana usluga autentifikacije
Legitimeringstjänst n	Usluga autentifikacije n
Anvisningstjänst	Usluga otkrivanja
Intyg	Certifikat
Val av legitimeringstjänst	Odabir usluge autentifikacije
autentisering	autentifikacija
attributtjänst	usluga atributa
Webbläsare	Preglednik
E-tjänst	E-usluga

Slika 1. *Prikaz komunikacije između različitih službi unutar federacije identiteta.*

> [1]: Usluga autentifikacije spominje se i u ostaloj dokumentaciji tvrtke Digg kao usluga identiteta i usluga certificiranja. Međutim, u ovom se dokumentu upotrebljava samo pojam „usluga autentifikacije".

1.2. Okvir povjerenja i razine sigurnosti

Osnova za primjenu razine sigurnosti prilikom autentifikacije korisnika jest razina osiguranja za e-identifikaciju koja se zahtijeva e-uslugom. Kako bi te razine sigurnosti bile usporedive u okviru federacije identiteta, četiri razine jamstva (1-4) definirane su u Okviru pouzdanosti za švedsku elektroničku identifikaciju [Digg.Tillit] i tri razine jamstva (niska, znatna, visoka) u Uredbi EU-a eIDAS. Svi izdavatelji potvrda o identitetu moraju dokazati da cijeli postupak na kojem se temelji izdavanje potvrda o identitetu ispunjava zahtjeve potrebne razine jamstva, uključujući:

- zahtjeve za izradu potvrde o identitetu;
- zahtjeve za elektroničku identifikaciju (autentifikaciju);
- zahtjeve za postupak izdavanja;
- zahtjeve za samu elektroničku identifikaciju i njezinu uporabu;
- zahtjeve za izdavatelja eID-a;
- zahtjev za utvrđivanje identiteta podnositelja zahtjeva za elektroničku identifikaciju.

1.3. Služba za prikupljanje, upravljanje i objavljivanje metapodataka

Federacija identiteta SAML pruža informacije o sudionicima federacije identiteta putem metapodataka SAML. Subjekti koji pružaju usluge autentifikacije i atributa u federaciji te pouzdane strane, tj. subjekti koji upotrebljavaju te usluge, npr. e-usluge, smatraju se sudionicima u federaciji identiteta.

Metapodaci federacije identiteta omogućuju sudionicima dobivanje informacija o uslugama drugih sudionika, uključujući podatke potrebne za sigurnu razmjenu informacija među

sudionicima. Svaka strana mora ažurirati metapodatke i održavati ih ažurnima u skladu s ugovornim uvjetima.

Glavna je svrha metapodataka osigurati ključeve/potvrde potrebne za sigurnu komunikaciju i razmjenu informacija među službama. Osim ključeva, metapodaci također sadržavaju druge informacije koje su važne za interakciju među uslugama, kao što su adrese potrebnih funkcija, informacije o razinama osiguranja, kategorijama usluga, informacijama o korisničkom sučelju itd.

Federacija identiteta definirana je registrom u formatu XML koji je potpisan certifikatom operatora federacije identiteta. Datoteka sadrži informacije o članovima federacije identiteta, uključujući njihove certifikate. Budući da je datoteka s metapodacima potpisana, dovoljno je usporediti certifikat s njegovim istovjetnim metapodacima. Infrastruktura koja se temelji na središnjem registru federacije identiteta zahtijeva da se registar stalno ažurira i da članovi federacije identiteta uvijek koriste najnoviju verziju datoteke.

1.4. Usluga otkrivanja

U federaciji identiteta moguće je ponuditi i upotrebljavati zajedničku uslugu otkrivanja, u kojoj su navedene usluge autentifikacije koje korisnik može odabrati. Svrha takve usluge otkrivanja jest osloboditi pojedinačne e-usluge koje su dio federacije identiteta od uvođenja podrške u pogledu načina na koji korisnici odabiru uslugu autentifikacije (ili metodu prijave).

Budući da je usluga otkrivanja dostupna unutar federacije identiteta, e-usluge mogu tamo usmjeriti svoje korisnike kako bi odabrali uslugu autentifikacije. Usluga otkrivanja u interakciji je s korisnikom koji donosi odluku, a korisnik se, zajedno s korisnikovim izborom, vraća na e-uslugu, koja sada zna kojoj usluzi autentifikacije treba poslati korisnika na autentifikaciju.

> Trenutačno ne postoji zajednička usluga otkrivanja za federaciju identiteta Sweden Connect.

1.5. Integracija kod pouzdajuće strane

Pouzdajuće strane, npr. e-usluge, integriraju se s uslugama autentifikacije putem standardiziranih poruka i upotrebljavaju certifikate o identitetu koji također imaju standardizirane formate.

Na tehnički okvir za Sweden Connect utječe profil interoperabilnosti „SAML V2.0 Deployment Profile for Federation Interoperability” [SAML2Int]. Profil je podržan brojnim komercijalnim proizvodima i rješenjima otvorenog koda, što olakšava integraciju na e-uslugama.

Mnoge e-usluge upotrebljavaju samostalna rješenja za autentifikaciju, što znači da prilagodba integracije kako bi bila u skladu s tehničkim okvirom ima ograničen učinak na e-uslugu kao takvu.

1.6. Potpis

Pri potpisivanju tehnički okvir za Sweden Connect omogućuje upotrebu različitih vrsta elektroničke identifikacije, čak i onih koje se ne temelje na certifikatima, bez potrebe za

posebnim prilagodbama u e-usluzi. To je zato što elektronički izdani certifikat o identitetu (koji se upotrebljava za identifikaciju korisnika pri potpisivanju) ima isti format bez obzira na vrstu elektroničke identifikacije koju korisnik upotrebljava.

Svrha usluge potpisivanja jest omogućiti potpise unutar federacija identiteta koje su u skladu s tehničkim okvirom, uz potporu svih vrsta elektroničke identifikacije koje pružaju dovoljan stupanj sigurnosti.

Nabavom[1] i uvođenjem usluge potpisivanja, pouzdajuća strana koja je dio federacije identiteta može korisniku omogućiti potpisivanje elektroničkog dokumenta uz podršku usluge potpisivanja. Elektronički potpis korisnika i pripadajući certifikat za potpisivanje izrađuje usluga potpisivanja nakon što je korisnik pristao potpisati se autentifikacijom putem usluge potpisivanja[2]

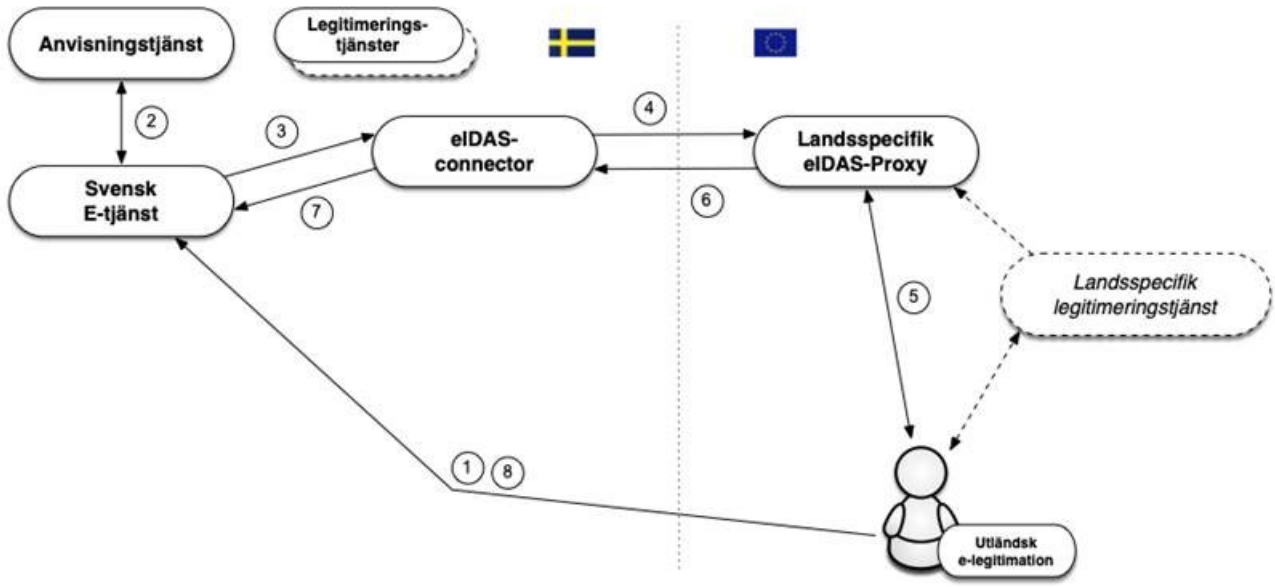
> [1]: Također je moguće implementirati uslugu potpisivanja na temelju specifikacija tehničkog okvira ili na drugi način nabaviti uslugu potpisivanja.
>
> [2]: Važno je napomenuti da je od najveće važnosti da korisnik taj postupak doživljava kao potpisivanje dokumenta. Stoga bi se protok potpisa trebao koristiti za elektroničke osobne iskaznice koje to podržavaju u vezi s „autentifikacijom za potpis".

1.7. Tehnički okvir i eIDAS

Uredbom EU-a (910/2014) o elektroničkoj identifikaciji i uslugama povjerenja (eIDAS) od švedskih javnih tijela zahtijeva se da priznaju elektroničke osobne iskaznice koje su prijavile druge zemlje eIDAS-a. To znači da javna švedska e-usluga koja se temelji na određenim pravilima mora moći prihvatiti prijavu izvršenu s pomoću elektroničke identifikacije izdane u drugoj zemlji.

1.7.1. Autentifikacija uporabom inozemnih eID-ova

Tehničke specifikacije za eIDAS temelje se, kao i tehnički okvir, na standardima SAML; iako postoje mnoge sličnosti, postoje i razlike u tim specifikacijama. Međutim, švedska e-usluga ne bi se trebala izravno odnositi na tehničke specifikacije eIDAS-a. Na slici u nastavku prikazano je kako švedski čvor eIDAS (*eIDAS-connector*) djeluje kao most između drugih zemalja i švedske federacije identiteta kada se osoba autentificira upotrebom strane elektroničke identifikacije u švedskoj e-usluzi. Švedski čvor eIDAS usklađen je s tehničkim okvirom.



Anvisningstjänst	Usluga otkrivanja
Legitimeringstjänster	Usluga autentifikacije
Svensk E-tjänst	Švedska e-usluga
EiDAS-connector	eiDAS-connector
Landsspecifik Eidas Proxy	eIDAS proxy poslužitelj specifičan za zemlju
Landsspecifik legitimeringstjänst	Servis za autentifikaciju specifičan za zemlju
utländsk e-legitimation	inozemni eID

Protok je sljedeći:

1. Korisnik s inozemnim eID-om traži pristup švedskoj e-usluzi (tj. prijavljuje se).

2. E-usluga omogućuje korisniku da odabere metodu prijave s pomoću usluge otkrivanja. Prikazuje se opcija „inozemni eID" koju korisnik odabire u slučaju eIDAS.

3. E-usluga kreira zahtjev za autentifikaciju u skladu s ovim tehničkim okvirom i usmjerava korisnika na švedski čvor eIDAS (*konektor*) za koji je nadležan DIGG. Čvor eIDAS djeluje kao usluga autentifikacije (*Pružatelj identiteta*) u federaciji identiteta prema švedskim pouzdajućim stranama, što znači da se komunikacija s tom uslugom odvija na isti način kao s drugim uslugama autentifikacije unutar federacija identiteta koje su u skladu s tehničkim okvirom.

4. Primljeni zahtjev obrađuje se, a čvor eIDAS prikazuje stranicu za odabir na kojoj korisnik odabire „svoju zemlju".[1]. Švedski čvor eIDAS sada pretvara primljeni zahtjev za autentifikaciju u zahtjev za autentifikaciju eIDAS-om i usmjerava korisnika na „eIDAS uslugu proxy poslužitelja" odabrane zemlje.

5. Nakon što eIDAS usluga proxy poslužitelja primi zahtjev za autentifikaciju za odabranu zemlju, tehnologija autentifikacije te zemlje preuzima zahtjev. Ne

upotrebljavaju sve zemlje eIDAS SAML za autentifikaciju, ali ako bi to bio slučaj u našem primjeru, korisnik bi bio preusmjeren na uslugu autentifikacije (*Pružatelj identiteta*), a prije toga možda i uslugu otkrivanja za odabir usluge autentifikacije.

6. Nakon autentifikacije, certifikat (*Potvrda*) izrađuje se u skladu sa specifikacijama eIDAS-a. Taj certifikat uključuje atribute specifične za eIDAS kojima se identificira korisnik. Ta se potvrda sada prosljeđuje švedskom čvoru eIDAS.

7. Čvor prima certifikat i potvrđuje njegovu točnost. Taj se certifikat pretvara iz formata eIDAS u certifikat formatiran u skladu s tehničkim okvirom i šalje e-usluzi.

8. Pouzdajuća strana dodaje dodatne informacije i utvrđuje treba li korisniku odobriti pristup usluzi.

Stoga švedske e-usluge trebaju podupirati samo tehnički okvir za obradu autentifikacije koja se provodi pomoću europske elektroničke identifikacije. Međutim, e-usluga mora moći obraditi predstavljeni identitet, koji nije nužno osobni identifikacijski broj. Stoga mogu postojati slučajevi u kojima e-usluga autentificira korisnika putem okvira eIDAS, ali se predstavljeni identitet korisnika ne može upotrebljavati u e-usluzi. To je podrobnije razrađeno u poglavlju 1.7.3. u nastavku.

[1]: Korisnik zapravo odabire „eIDAS uslugu proxy poslužitelja” kojoj treba proslijediti zahtjev. To ovisi o državi kojoj pripada izdavatelj eID-a korisnika.

1.7.2. Potpisi uporabom inozemnih eID-ova

Kao što je već opisano, u ovom se tehničkom okviru primjenjuje model za elektronički potpis koji se naziva potpisivanje s pomoću federacije identiteta. Usluga potpisivanja na poslužitelju povezana je s e-uslugom, koja pak zahtijeva potpis. Kad korisnik potpiše dokument, e-usluga šalje zahtjev za potpis službi za potpis. Usluga potpisivanja zatim zahtijeva od korisnika da se autentificira. U vezi s autentifikacijom, korisnik odobrava potpis. Usluga potpisivanja šalje podatke natrag u e-uslugu, a zatim se pohranjuju podaci o potpisu povezani s potpisanim dokumentom.

Tim se postupkom omogućuje potpisivanje i upotrebom stranog eID-a jer usluga potpisivanja može odlučiti autentificirati korisnika upotrebom stranog eID-a u skladu s postupkom opisanim u odjeljku 1.7.1.

Pri potpisivanju, u ovom slučaju, švedski čvor eIDAS odgovoran je za obavješćivanje korisnika da je svrha autentifikacije potpisivanje dokumenta, tko je zatražio potpis i svih informacija o tome što se potpisuje. Potvrda o identitetu izdaje se tek nakon što se korisnik autentificira (radi potpisivanja) i šalje se službi za potpisivanje koja generira potpis.

1.7.3. Upravljanje identitetima

Potvrde o identitetu iz drugih zemalja u skladu su s tehničkim specifikacijama na razini EU-a razvijenima u okviru Uredbe eIDAS. Atributi koje svaka zemlja uvijek mora uključiti za fizičke osobe kao i za organizacije („minimalni skup podataka”, MDS) utvrđeni su u ovoj Uredbi. Svaka zemlja mora uključiti jedinstveni identifikator po eID-u koji predstavlja samo jednu fizičku osobu. U nekim će zemljama ti identifikatori biti jedinstveni i nepromijenjeni po osobi na isti način kao, na primjer, švedski osobni identifikacijski brojevi, ali ti identifikatori

mogu imati vrlo različite sastave i značajke. Jedno od obilježja koje se može razlikovati jest koliko je nepromijenjen takav identifikator, tj. ostaje li takav identifikator nepromijenjen tijekom života osobe ili se mijenja ako se, na primjer, osoba preseli u drugu regiju, promijeni ime ili samo promijeni svoju elektroničku identifikaciju. U nekim zemljama (npr. u Ujedinjenoj Kraljevini) identifikacijska oznaka razlikovat će se ovisno o tome koju od nacionalnih elektroničkih osobnih iskaznica korisnik trenutno odluči upotrebljavati.

Kako bi se pojednostavnilo upravljanje korisnicima u švedskim e-uslugama, švedski čvor eIDAS generira standardizirani atribut ID-a za korisnike koji su autentificirani s pomoću strane eID-a, poznat kao *privremena identifikacijska oznaka* (skraćeno PRID). Osim toga, stvara se povezani atribut koji izjavljuje očekivanu nepromjenjivost ili životni vijek ovog ID atributa. Atribut PRID generira se na temelju vrijednosti atributa dobivenih inozemnom autentifikacijom prema određenim metodama za tu određenu zemlju. Svaka kombinacija zemlje i metode kategorizirana je s obzirom na očekivanu nepromjenjivost, tj. koliko je vjerojatno da će se identitet iste osobe s vremenom promijeniti. Time se švedskim e-uslugama omogućuje prilagodba komunikacije s korisnikom i proaktivno pružanje značajki koje korisniku čiji se identitet promijenio olakšavaju ponovnu uspostavu kontrole nad informacijama u e-usluzi.

U nekim slučajevima osoba koja je autentificirana inozemnim eID-om može imati i švedski osobni identifikacijski broj. To može biti, na primjer, švedski državljanin koji se preselio u inozemstvo i dobio inozemni eID ili strani državljanin koji je registriran u Švedskoj i kojem je dodijeljen osobni identifikacijski broj.

Činjenica da osoba s inozemnim eID-om ima švedski osobni identifikacijski broj obično nije poznata inozemnoj usluzi autentifikacije, zbog čega te informacije nisu uključene u potvrdu o identitetu iz zemlje u kojoj je osoba autentificirana. S druge strane, švedski čvor ima mogućnost pretraživanja usluge atributa u Švedskoj[1] o tome postoji li registrirani osobni identifikacijski broj za autentificiranu osobu te, ako je to slučaj, može dodati takve informacije potvrdi o identitetu koja se šalje e-usluzi.

> [1]: U trenutku pisanja ovog teksta ne postoji usluga atributa kojom se uspostavlja veza između identiteta u sustavu eIDAS i švedskih osobnih identifikacijskih brojeva.

1.7.4. Švedski eID-ovi u inozemnim e-uslugama

Švedska je prijavila švedske eID-ove na razinama pouzdanosti znatna i visoka prema eIDAS-u.

Zahtjev za autentifikaciju strane e-usluge podnosi se švedskom čvoru eIDAS (usluga proxy poslužitelja) putem eIDAS priključka u zemlji e-usluge. U švedskom čvoru eIDAS korisnik odabire švedski eID s kojim se želi autentificirati, a zatim se zahtjev za autentifikaciju šalje usluzi autentifikacije (*Pružatelj identiteta*) koja obrađuje odabrani eID. Taj je zahtjev oblikovan u skladu s tehničkim okvirom, što znači da švedska usluga autentifikacije ne mora biti u skladu s tehničkim specifikacijama eIDAS-a.

Korisnika autentificira švedska služba za autentifikaciju i izdaje se potvrda o identitetu (u skladu s tehničkim okvirom). Švedska eIDAS usluga proxy poslužitelja prima taj certifikat i

pretvara ga u certifikat u skladu sa specifikacijama eIDAS-a prije nego što ga proslijedi stranom priključku eIDAS-a, a zatim e-usluzi pozivanja (*Pružatelj usluga*).

2. Tehničke specifikacije

Ovo poglavlje sadržava specifikacije i profile za federacije identiteta koje su u skladu s tehničkim okvirom za Sweden Connect i određene povezane usluge. Ako nije drugačije navedeno, ti su dokumenti obvezujući za pružanje usluga unutar federacija identiteta koji provode tehnički okvir.

2.1. Profili i specifikacije za SAML

Federacije identiteta koje su usklađene s tehničkim okvirom za Sweden Connect temelje se na „Profilu za implementaciju za švedski okvir za elektroničku identifikaciju", [SAML.Profile]. Na taj profil utječe „SAML V2.0 Deployment Profile for Federation Interoperability" [SAML2Int], ali on o njemu ne ovisi normativno. [SAML.Profil] također sadrži pravila i smjernice specifične za tehnički okvir za Sweden Connect.

2.1.1. Profil za implementaciju za švedski okvir za eID

„Profil za implementaciju za švedski okvir za eID", [SAML.Profil], glavni je dokument tehničkog okvira i u njemu se među ostalim navodi sljedeće:

- kako se konstruiraju i tumače metapodaci SAML;
- način na koji će zahtjev za autentifikaciju biti formatiran;
- kako se postupa sa zahtjevom za autentifikaciju te kako se certifikat o identitetu kreira, provjerava i kako se s njim postupa;
- sigurnosni zahtjevi;
- posebni zahtjevi SAML-a za usluge potpisivanja i „autentifikaciju za potpisivanje".

2.1.2. Švedski okvir za eID – Registar identifikatora

Uvođenje švedske eID infrastrukture zahtijeva različite oblike identifikatora za predstavljanje objekata u strukturama podataka. U dokumentu „Sweden Connect – Registar identifikatora", [SC.Registry], definirana je struktura identifikatora dodijeljenih na temelju tehničkog okvira, kao i registar definiranih identifikatora.

2.1.3. Specifikacija atributa za švedski okvir za eID

Specifikacija „Specifikacija atributa za švedski okvir za eID", [SAML.Atributi], definira SAML profile atributa koji se koriste unutar federacije identiteta koji ispunjavaju zahtjeve tehničkog okvira uključujući one koji se povezuju na eIDAS putem švedskog eIDAS čvora.

2.1.4. Kategorije subjekata za švedski okvir za eID

Kategorije subjekata upotrebljavaju se unutar federacije identiteta za niz različitih svrha:

- Kategorije subjekta usluge – upotrebljavaju se u metapodacima za predstavljanje zahtjeva e-usluge u pogledu razina osiguranja i zatraženih atributa, kao i za ispunjavanje razina osiguranja usluga autentifikacije i isporuku atributa.
- Kategorije svojstava usluga – upotrebljavaju se za predstavljanje specifičnih karakteristika usluge.
- Kategorije vrste subjekta usluga – upotrebljavaju se za predstavljanje različitih vrsta usluga unutar federacije identiteta.
- Kategorije ugovora subjekta usluge – upotrebljavaju ih usluge za objavljivanje obrazaca sporazuma i slično.
- Kategorije općih subjekta – kategorije subjekata koje ne spadaju ni u jednu od prethodno navedenih vrsta.

U specifikaciji „Kategorije subjekata za švedski okvir za eID" [SAML.EntCat] navode se kategorije subjekata definirane tehničkim okvirom i opisuje njihovo značenje.

2.1.5. Specifikacija izrađenih atributa za eIDAS za švedski okvir za eID

Specifikacija „Specifikacija izrađenih atributa za eIDAS za švedski okvir za eID", [SC.eIDAS.Attrs], određuje procese i pravila za načine kako se ID-atributi konstruiraju na temelju atributa primljenih tijekom autentifikacije u eIDAS-u.

2.1.6. Profil za implementaciju za pružatelje identiteta BankID unutar švedskog okvira eID

Specifikacija „Profil za implementaciju za pružatelje identiteta BankID unutar švedskog okvira eID", [SAML.BankID], definira pravila za načine razvijanja za uslugu autentifikacije koja implementira podršku za BankID.

> **Imajte na umu sljedeće:** Ova specifikacija nije obvezujuća za usklađenost s tehničkim okvirom. Relevantna je samo za usluge autentifikacije koje primjenjuju podršku za BankID i e-usluge koje ih upotrebljavaju. Međutim, usluge autentifikacije koje primjenjuju podršku za BankID i žele se povezati s federacijom identiteta Sweden Connect moraju biti u skladu s ovom specifikacijom.

2.1.7. Glavni odabir u zahtjevima za autentifikaciju SAML

U specifikaciji „Glavni odabir u zahtjevima za autentifikaciju SAML", [SAML.Principal], definirano je proširenje na SAML kojim se pouzdajućoj strani omogućuje da obavijesti uslugu autentifikacije koji identitet želi autentificirati.

2.1.8. Proširenje korisničke poruke u zahtjevima za autentifikaciju SAML

U specifikaciji „Proširenje korisničke poruke u zahtjevima za autentifikaciju SAML”, [SAML.UMessage], definirano je proširenje SAML-a koje pouzdajućoj strani omogućuje uključivanje prikazne poruke u zahtjev za autentifikaciju poslan usluzi autentifikacije. Usluga autentifikacije zatim može prikazati ovu poruku korisniku tijekom koraka autentifikacije

2.2. Profili i specifikacije za OpenID Connect

2.2.1. Profil OpenID Connect za Sweden Connect

Profil „Profil OpenID Connect za Sweden Connect”, [OIDC.Profile], temelji se na švedskom profilu OpenID Connect profilu koji je OpenID Connect profil razvijen od strane OIDC Sweden za promicanje interoperabilnosti i sigurnosti unutar švedskih OIDC rješenja.

[OIDC.Profile] dodaje dodatne zahtjeve povezane s federacijom identiteta Sweden Connect.

2.2.2. Zahtjevi za OpenID Connect i specifikacije opsega za Sweden Connect

Specifikacija „Zahtjevi za OpenID Connect i specifikacije opsega za Sweden Connect”, [OIDC.Claims], temelji se na specifikaciji Zahtjevi i opseg specifikacije za švedski profil OpenID Connect Profile koji razvija OIDC Sweden.

2.3. Specifikacije za potpisivanje

Ovaj odjeljak sadržava upućivanja na dokumente kojima se definiraju usluge potpisivanja unutar federacija identiteta koje su u skladu s tehničkim okvirom za Sweden Connect.

2.3.1. Profil za implementaciju za korištenje OASIS DSS-a u središnjim uslugama potpisivanja

Profil za implementaciju „Profil za implementaciju za korištenje OASIS DSS-a u središnjim uslugama potpisivanja”, [Sign.DSS.Profile], određuje profil za zahtjev za potpis i odgovor u skladu sa standardom OASIS-a „Osnovni protokoli, elementi i veze za usluge digitalnog potpisa”, [DSS].

2.3.2. Proširenje DSS za usluge centraliziranog potpisivanja s pomoću federacije identiteta

„Proširenje DSS za usluge centraliziranog potpisivanja s pomoću federacije identiteta”, [Sign.DSS.Ext], proširenje je OASIS-ova standarda „Osnovni protokoli, elementi i veze za usluge digitalnog potpisa”, [DSS], u kojem se navode definicije potrebne za potpisivanje u skladu s tehničkim okvirom.

2.3.3. Profil certifikata za certifikate koje izdaju usluge centraliziranog potpisivanja

Profil certifikata „Profil certifikata za certifikate koje izdaju usluge centraliziranog potpisivanja”, [Sign.Cert.Profile], utvrđuje sadržaj potpisnih certifikata. Ovaj profil primjenjuje novo proširenje certifikata za podršku uslugama potpisivanja.

Ovaj se profil odnosi na „Proširenje konteksta certifikata autentifikacije”, [AuthContext], u kojem se opisuje kako je „kontekst autentifikacije” prikazan u X.509 certifikatima.

2.3.4. Protokol za aktivaciju potpisa za potpisivanje s pomoću federacije identiteta

U specifikaciji „Protokol za aktivaciju potpisa za potpisivanje s pomoću federacije identiteta” [Sign.Activation] definira se „Protokol za aktivaciju potpisa” (SAP) za implementaciju „Sole Control Assurance Level 2” (SCAL2) u skladu s normom „EN 419241 – Vjerodostojni sustavi za potporu potpisivanja na poslužitelju”.

3. Referentni popis

3.1. DIGG

[Digg.Tillit]

Okvir povjerenja za švedsku e-identifikaciju.

[SC.Registry]

Sweden Connect – Registar identifikatora.

[SAML.Profile]

Profil za implementaciju za švedski okvir za eID.

[SAML.Attributes]

Specifikacija atributa za švedski okvir za eID.

[SAML.EntCat]

Kategorije subjekata za švedski okvir za eID.

[SC.eIDAS.Attrs]

eIDAS Specifikacija izrađenih atributa za švedski okvir za eID.

[SAML.BankID]

Profil za implementaciju za pružatelje identiteta BankID unutar švedskog okvira eID.

[SAML.Principal]

Glavni odabir u zahtjevima za autentifikaciju SAML.

[SAML.UMessage]

Proširenje korisničke poruke u zahtjevima za autentifikaciju SAML.

[OIDC.Profile]

Profil OpenID Connect za Sweden Connect.

[OIDC.Claims]

Zahtjevi za OpenID Connect i specifikacije opsega za Sweden Connect.

[Sign.DSS.Profile]

Profil za implementaciju za korištenje OASIS DSS-a u središnjim uslugama potpisivanja.

[Sign.DSS.Ext]

Proširenje DSS za usluge centraliziranog potpisivanja s pomoću federacije identiteta.

[Sign.Cert.Profile]

Profil certifikata za certifikate koje izdaju usluge centraliziranog potpisivanja.

[Sign.Activation]

Protokol za aktivaciju potpisa za potpisivanje s pomoću federacije identiteta.

3.2. Ostala upućivanja

[SAML2Int]

SAML V2.0 Profil za implementaciju za interoperabilnost federacija identiteta.

[DSS]

OASIS Standard – Osnovni protokoli, elementi i veze za usluge digitalnog potpisa, verzija 1.0, 11. travnja 2007.

[AuthContext]

RFC-7773 Proširenje konteksta certifikata autentifikacije.