Uvod v tehnični okvir Sweden Connect

2024-12-04

Referenčna št.: **2019-267**

Kazalo

1. Uvod

1.1 Pregled

Tehnični okvir Sweden Connect je prilagojen identitetnim zvezam, ki temeljijo na SAML 2.0.

> V najnovejši različici tehničnega okvira so bile uvedene tudi specifikacije za OpenID Connect. Trenutno ni na voljo zvezna podpora za OpenID Connect. To bo uvedeno leta 2025.
>
> Preostali deli tega dokumenta opisujejo samo zvezo SAML. Ko bo OpenID Connect v celoti uveden, bo ta dokument zajemal tudi to tehnologijo.

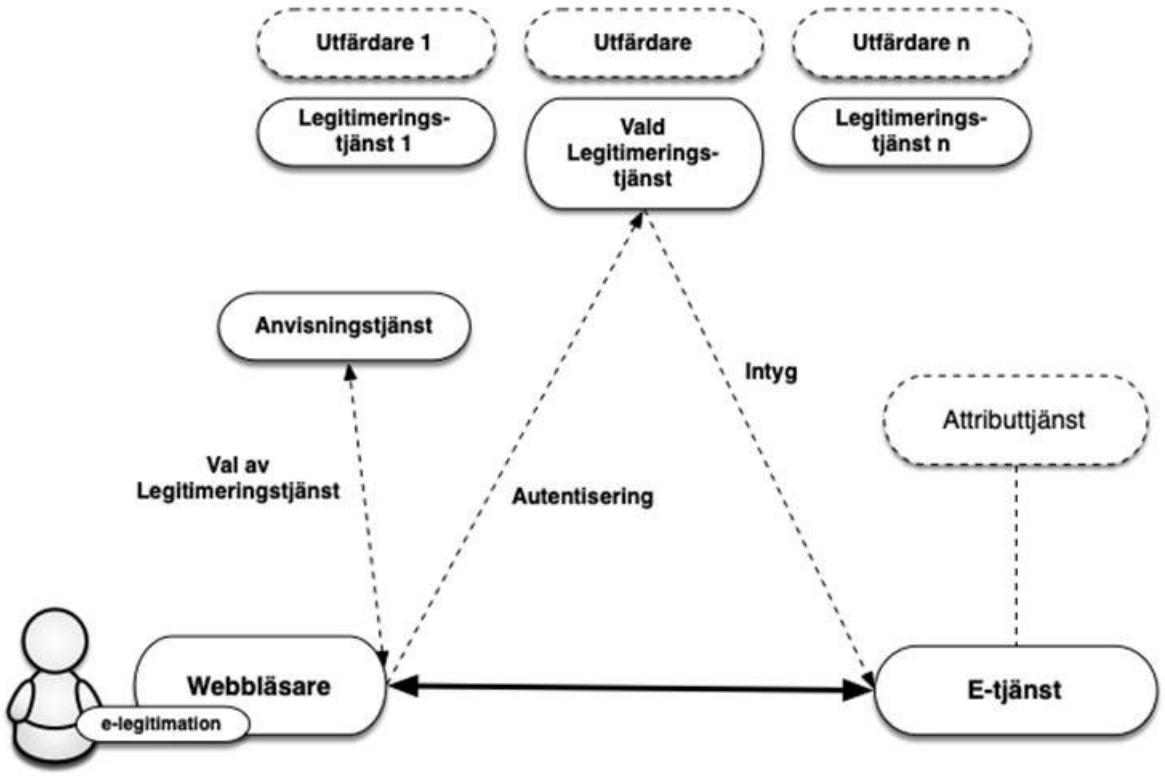
Zanašajoče se stranke pridobijo potrdila o identiteti v standardizirani obliki od storitve za avtentikacijo[1].

Elektronskih storitev, za katere je potreben podpis, ni treba prilagoditi različnim elektronskim identifikacijam uporabnikov, da bi se ustvarili elektronski podpisi. Namesto tega elektronska storitev to prenese na storitev podpisovanja, pri kateri imajo uporabniki, podprti z avtentikacijo prek storitve za avtentikacijo, možnost podpisovanja elektronskih dokumentov.

Elektronske storitve in ustrezne zanašajoče se stranke znotraj zveze prevzamejo vlogo ponudnika storitev (SP), medtem ko storitve za avtentikacijo, ki izdajajo potrdila o identiteti, prevzamejo vlogo ponudnika identitete (IdP) in s tem avtentikatorja uporabnika, ne glede na elektronsko storitev, za katero se opravi avtentikacija uporabnika.

Če elektronska storitev potrebuje več informacij o uporabniku, npr. informacije o pravni sposobnosti, se lahko opravi poizvedba pri storitvi za atribute (AA) znotraj zveze, če takšna ustrezna storitev za atribute obstaja. Z zahtevo za atribute lahko elektronska storitev pridobi potrebne dodatne informacije, da lahko pooblasti uporabnika in mu omogoči dostop do elektronske storitve ali enakovrednega.

Ker se osebni podatki o identiteti in drugi atributi, povezani z uporabniki, zagotavljajo s potrdili o identiteti in potrdili o atributih, se lahko vse vrste elektronske identifikacije, o katerih so se zanašajoče se stranke dogovorile in ki so del zveze, uporabljajo za avtentikacijo v okviru elektronske storitve, ki zahteva osebno identifikacijsko številko in dodatne informacije, tudi če elektronska identifikacija ne vsebuje nobenih posebnih osebnih podatkov (npr. šifranti za ustvarjanje enkratnih gesel).



Utfärdare 1	Izdajatelj 1
Utfärdare n	Izdajatelj n
Legitimeringstjänst 1	Storitev za avtentikacijo 1
Vald legitimeringstjänst	Izbrana storitev za avtentikacijo
Legitimeringstjänst n	Storitev za avtentikacijo n

Anvisningstjänst	Storitev odkrivanja
Intyg	Potrdilo
Val av legitimeringstjänst	Izbira storitve za avtentikacijo
autentisering	avtentikacija
attributtjänst	storitev za atribute
Webbläsare	Brskalnik
E-tjänst	Elektronska storitev

Slika 1: *Prikaz komunikacije med različnimi storitvami znotraj identitetne zveze.*

> [1]: Storitev za avtentikacijo je v drugi dokumentaciji agencije Digg navedena tudi kot storitev identitete in storitev certificiranja, vendar se v tem dokumentu uporablja samo izraz „storitev za avtentikacijo“.

1.2 Okvir zaupanja in ravni varnosti

Podlaga za uporabo ravni varnosti pri avtentikaciji uporabnika je raven zanesljivosti za elektronsko identifikacijo, ki jo zahteva elektronska storitev. Da bi bile te ravni varnosti primerljive v okviru zveze, so v okviru zaupanja za švedsko elektronsko identifikacijo [Digg.Tillit] opredeljene štiri ravni zanesljivosti (1–4), v uredbi eIDAS pa tri ravni zanesljivosti (nizka, znatna, visoka). Vsak izdajatelj potrdila o identiteti mora dokazati, da celoten postopek, na katerem temelji izdaja potrdila o identiteti, izpolnjuje zahteve zahtevane ravni zanesljivosti, vključno z:

- zahtevami glede izdaje potrdila o identiteti;
- zahtevami glede elektronske identifikacije (avtentikacije);
- zahtevami glede postopka izdaje;
- zahtevami glede same elektronske identifikacije in njene uporabe;
- zahtevami glede izdajatelja elektronske identifikacije;
- zahtevo glede ugotavljanja identitete prosilca za elektronsko identifikacijo.

1.3 Storitev za zbiranje, upravljanje in objavo metapodatkov

Zveza SAML zagotavlja informacije o udeležencih zveze prek metapodatkov SAML. Za udeležence zveze se štejejo subjekti, ki zagotavljajo storitve avtentikacije in storitve atributov v zvezi, ter zanašajoče se stranke, tj. subjekti, ki uporabljajo te storitve, npr. elektronske storitve.

Metapodatki zveze udeležencem omogočajo pridobitev informacij o storitvah drugih udeležencev, vključno s podatki, potrebnimi za varno izmenjavo informacij med udeleženci. Vsaka stranka mora metapodatke posodabljati v skladu s pogodbenimi pogoji.

Glavni namen metapodatkov je zagotoviti ključe/potrdila, potrebna za varno komunikacijo in izmenjavo informacij med storitvami. Metapodatki poleg ključev vsebujejo tudi druge

informacije, ki so pomembne za interakcijo med storitvami, na primer naslove zahtevanih funkcij, informacije o ravneh zanesljivosti, kategorijah storitev, uporabniškem vmesniku itd.

Identitetno zvezo določa register v formatu XML, ki je podpisan s potrdilom operaterja zveze. Datoteka vsebuje informacije o udeležencih identitetne zveze, vključno z njihovimi potrdili. Ker je datoteka z metapodatki podpisana, zadostuje primerjava potrdila z njegovim metapodatkovnim ustreznikom. Infrastruktura, ki temelji na osrednjem registru zveze, zahteva, da se register stalno posodablja in da udeleženci zveze vedno uporabljajo najnovejšo različico datoteke.

1.4 Storitev iskanja

V identitetni zvezi je mogoče ponuditi in uporabljati skupno storitev iskanja, ki navaja, med katerimi storitvami za avtentikacijo lahko uporabnik izbira. Namen te storitve iskanja je razbremeniti posamezne elektronske storitve, ki so del identitetne zveze, da bi morale izvajati podporo v zvezi s tem, kako uporabniki izberejo storitev avtentikacije (ali metodo prijave).

Ker je storitev iskanja na voljo znotraj identitetne zveze, lahko elektronske storitve svoje uporabnike usmerijo tja, da izberejo storitev avtentikacije. Storitev iskanja komunicira z uporabnikom, ki se sam odloči, uporabnik pa je skupaj z njegovo izbiro usmerjen nazaj na elektronsko storitev, ki tako ve, kateri storitvi avtentikacije se uporabnik pošlje v avtentikacijo.

> Skupna storitev iskanja za zvezo Sweden Connect trenutno ni na voljo.

1.5 Integracija pri zanašajoči se stranki

Zanašajoče se stranke, npr. elektronske storitve, se integrirajo s storitvami avtentikacije prek standardiziranih sporočil in uporabljajo potrdila o identiteti, ki imajo tudi standardizirane oblike.

Na tehnični okvir Sweden Connect vpliva profil interoperabilnosti „SAML V2.0 Deployment Profile for Federation Interoperability“ [SAML2Int]. Profil je podprt s številnimi komercialnimi izdelki in odprtokodnimi rešitvami, kar olajša integracijo v elektronskih storitvah.

Številne elektronske storitve uporabljajo neodvisne rešitve za avtentikacijo, kar pomeni, da ima prilagajanje integracije tehničnemu okviru omejen vpliv na elektronsko storitev kot tako.

1.6 Podpis

Tehnični okvir Sweden Connect pri podpisovanju omogoča uporabo različnih vrst elektronske identifikacije, tudi tistih, ki ne temeljijo na potrdilih, brez potrebe po posebnih prilagoditvah v elektronski storitvi. Elektronsko izdano potrdilo o identiteti (ki se uporablja za identifikacijo uporabnikov pri podpisovanju) ima namreč enako obliko, ne glede na vrsto elektronske identifikacije, ki jo uporablja uporabnik.

Namen storitve podpisovanja je omogočiti podpise znotraj identitetnih zvez, ki so skladne s tehničnim okvirom, podprte z vsemi vrstami elektronske identifikacije, ki zagotavljajo zadostno stopnjo varnosti.

Z nabavo[1] in uvedbo storitve podpisovanja lahko zanašajoča se stranka, ki je del zveze, uporabniku dovoli podpis elektronskega dokumenta s podporo storitve podpisovanja. Storitev podpisovanja ustvari elektronski podpis uporabnika in z njim povezano potrdilo o podpisu, potem ko se uporabnik strinja s podpisom z avtentikacijo pri storitvi podpisovanja[2].

[1]: Prav tako je mogoče izvesti storitev podpisovanja, ki temelji na specifikacijah tehničnega okvira, ali drugače pridobiti storitev podpisovanja.

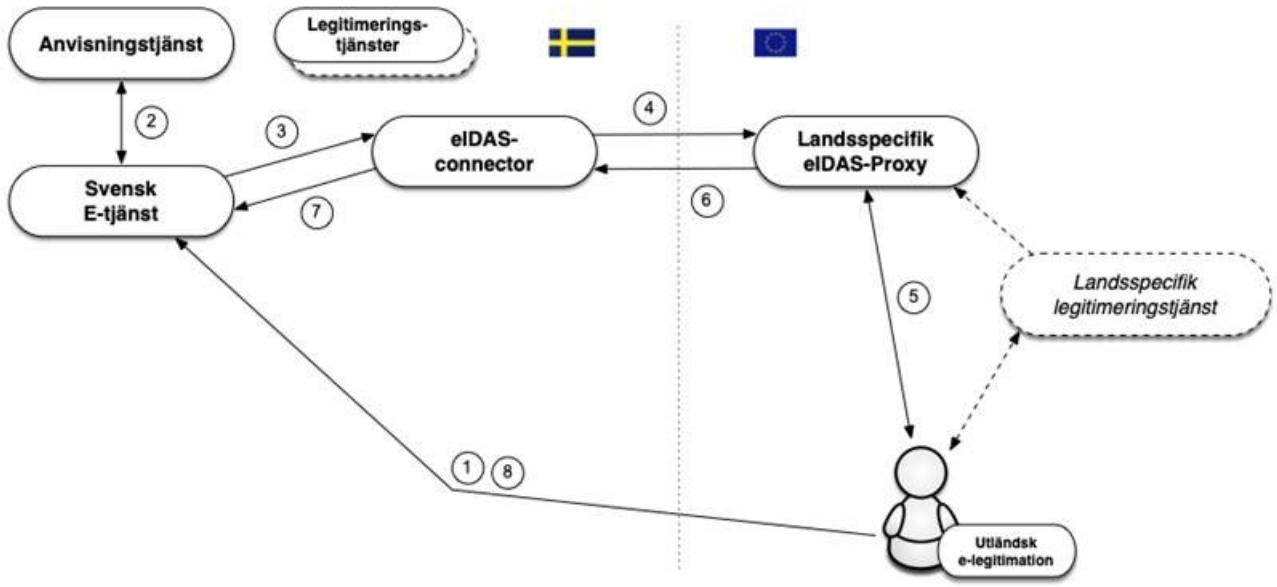
[2]: Poudariti je treba, da je izjemno pomembno, da uporabnik ta proces dojema kot podpis dokumenta. Zato je treba za elektronske identifikacije, ki to podpirajo, v povezavi z „avtentikacijo za podpis“ uporabiti tok podpisov.

1.7 Tehnični okvir in eIDAS

V skladu z Uredbo (EU) št. 910/2014 o elektronski identifikaciji in storitvah zaupanja (uredba eIDAS) se od švedskih javnih organov zahteva, da priznajo elektronske identifikacije, ki so jih priglasile druge države eIDAS. To pomeni, da mora biti švedska javna elektronska storitev na podlagi določenih pravil zmožna sprejeti prijavo, opravljeno z uporabo elektronske identifikacije, izdane v drugi državi.

1.7.1 Avtentikacija s tujimi elektronskimi identifikacijami

Tehnične specifikacije za eIDAS temeljijo, tako kot tehnični okvir, na standardih SAML, kljub številnim podobnostim pa v teh specifikacijah obstajajo tudi razlike. Vendar se švedska elektronska storitev ne sme neposredno nanašati na tehnične specifikacije za eIDAS. Spodnja slika prikazuje, kako švedsko vozlišče eIDAS (*eIDAS-connector*) deluje kot most med drugimi državami in švedsko zvezo, kadar se oseba avtenticira s tujo elektronsko identifikacijo v švedski elektronski storitvi. Švedsko vozlišče eIDAS je skladno s tehničnim okvirom.



Anvisningstjänst	Storitev iskanja
Legitimeringstjänster	Storitve avtentikacije

Svensk E-tjänst	Švedska elektronska storitev
EiDAS-connector	eIDAS-connector
Landsspecifik Eidas Proxy	Posredniška storitev eIDAS za posamezno državo
Landsspecifik legitimeringstjänst	Storitev avtentikacije za posamezno državo
utländsk e-legitimation	tuja elektronska identifikacija

Tok je naslednji:

1. uporabnik s tujo elektronsko identifikacijo zahteva dostop do švedske elektronske storitve (tj. prijava);

2. elektronska storitev uporabniku omogoča izbiro načina prijave z uporabo storitve iskanja. Prikaže se možnost „Tuja eID“, ki jo uporabnik izbere v zadevi eIDAS;

3. elektronska storitev ustvari zahtevo za avtentikacijo v skladu s tem tehničnim okvirom in uporabnika usmeri na švedsko vozlišče eIDAS (eIDAS-*connector*), za katerega je odgovorna agencija DIGG. Vozlišče eIDAS deluje kot storitev avtentikacije (*Identity Provider*) znotraj zveze v zvezi s švedskimi zanašajočimi se strankami, kar pomeni, da komunikacija s to storitvijo poteka na enak način kot z drugimi storitvami avtentikacije znotraj zvez, ki so skladne s tehničnim okvirom;

4. prejeta zahteva se obdela, vozlišče eIDAS pa prikaže stran za izbor, na kateri uporabnik izbere „svojo državo“[1]. Švedsko vozlišče eIDAS zdaj pretvori prejeto zahtevo za avtentikacijo v zahtevo za avtentikacijo eIDAS in uporabnika usmeri na posredniško storitev eIDAS izbrane države;

5. ko posredniška storitev eIDAS za izbrano državo prejme zahtevo za avtentikacijo, delo prevzame tehnologija te države za avtentikacijo. Vse države eIDAS ne uporabljajo SAML za avtentikacijo, če pa bi bilo tako v našem primeru, bi bil uporabnik preusmerjen na storitev avtentikacije (*Identity Provider*), pred tem pa morda tudi storitev iskanja za izbiro storitve avtentikacije;

6. ko je avtentikacija opravljena, se potrdilo (*Assertion*) ustvari v skladu s specifikacijami eIDAS. To potrdilo vključuje atribute, specifične za eIDAS, ki identificirajo uporabnika. To potrdilo se zdaj posreduje švedskemu vozlišču eIDAS;

7. vozlišče prejme potrdilo in preveri njegovo točnost. To potrdilo se iz formata eIDAS pretvori v potrdilo, oblikovano v skladu s tehničnim okvirom, in se pošlje elektronski storitvi;

8. zanašajoča se stranka doda morebitne dodatne informacije in odloči, ali naj se uporabniku odobri dostop do storitve.

Švedske elektronske storitve morajo zato podpirati le tehnični okvir za obravnavo avtentikacije, izvedene z uporabo evropske elektronske identifikacije, vendar mora biti elektronska storitev zmožna obravnavati predloženo identiteto, ki ni nujno osebna identifikacijska številka. Tako se lahko zgodi, da elektronska storitev opravi avtentikacijo

uporabnika prek okvira eIDAS, vendar predstavljene identitete uporabnika ni mogoče uporabiti v elektronski storitvi. Več o tem v poglavju 1.7.3 spodaj.

> [1]: Uporabnik dejansko izbere posredniško storitev eIDAS, na katero je treba posredovati zahtevo. To je odvisno od države, kateri pripada izdajatelj elektronske identifikacije uporabnika.

1.7.2 Podpisi s tujimi elektronskimi identifikacijami

Kot je bilo že opisano, se v tem tehničnem okviru uporablja model za elektronski podpis, imenovan zvezni podpis. Strežniška storitev podpisovanja je povezana z elektronsko storitvijo, ki nato zahteva podpis. Ko uporabnik podpiše dokument, elektronska storitev pošlje zahtevo za podpis storitvi podpisovanja. Storitev podpisovanja nato zahteva avtentikacijo uporabnika. V zvezi z avtentikacijo uporabnik odobri podpis. Storitev podpisovanja pošlje podatke nazaj elektronski storitvi, nato pa se shranijo podatki o podpisu, povezani z dokumentom, ki je bil podpisan.

Ta postopek omogoča podpisovanje tudi s tujo elektronsko identifikacijo, saj se lahko storitev podpisovanja odloči za avtentikacijo uporabnika s tujo elektronsko identifikacijo v skladu s postopkom, opisanim v zgornjem oddelku 1.7.1.

Pri podpisu je v tem primeru švedsko vozlišče eIDAS odgovorno za obveščanje uporabnika, da je namen avtentikacije podpis dokumenta, kdo je zahteval podpis, in vse informacije o tem, kaj se podpisuje. Potrdilo o identiteti se izda šele, ko se uporabnik avtenticira (za podpis), in se pošlje storitvi podpisovanja, ki nato ustvari podpis.

1.7.3 Upravljanje identitet

Potrdila o identiteti iz drugih držav so skladna s tehničnimi specifikacijami na ravni EU, razvitimi v okviru uredbe eIDAS. Atributi, ki jih mora vsaka država vedno vključiti za fizične osebe in organizacije („Minimum Dataset“, MDS), so določeni v tej uredbi. Vsaka država mora vključiti edinstveni identifikator za vsako elektronsko identifikacijo, ki predstavlja samo eno fizično osebo. V nekaterih državah bodo ti identifikatorji edinstveni in obstojni na osebo na enak način kot na primer švedske osebne identifikacijske številke, vendar imajo lahko ti identifikatorji zelo različne sestave in značilnosti. Ena od značilnosti, ki se lahko razlikuje, je, kako obstojen je tak identifikator, tj. ali tak identifikator v času življenja osebe ostane nespremenjen ali se spremeni, če se na primer oseba preseli v drugo regijo, spremeni svoje ime ali preprosto spremeni svojo elektronsko identifikacijo. V nekaterih državah (npr. v Združenem kraljestvu) se identifikator razlikuje glede na to, katero elektronsko identifikacijo države trenutno izbere uporabnik.

Da bi poenostavili upravljanje uporabnikov v švedskih elektronskih storitvah, švedsko vozlišče eIDAS ustvari standardiziran atribut ID za uporabnike, ki so bili avtenticirani s tujo elektronsko identifikacijo, t. i. *začasno identifikacijsko oznako* (skrajšano PRID). Poleg tega se ustvari povezan atribut, ki določa pričakovano obstojnost ali življenjsko dobo tega atributa ID. Atribut PRID se ustvari na podlagi vrednosti atributov, pridobljenih s tujo avtentikacijo v skladu z določenimi metodami za zadevno državo. Vsaka kombinacija države in metode je kategorizirana glede na pričakovano obstojnost, tj. kako verjetno je, da se bo identiteta iste osebe čez čas spremenila. To omogoča švedskim elektronskim storitvam, da prilagodijo komunikacijo z uporabnikom in proaktivno zagotovijo funkcije, ki uporabniku, čigar

identiteta se je spremenila, olajšajo ponovni prevzem nadzora nad svojimi informacijami v elektronski storitvi.

V nekaterih primerih ima lahko oseba, ki je avtenticirana s tujo elektronsko identifikacijo, tudi švedsko osebno identifikacijsko številko. To je lahko na primer švedski državljan, ki se je preselil v tujino in pridobil tujo elektronsko identifikacijo, ali tuji državljan, ki je prijavljen na Švedskem in mu je bila dodeljena osebna identifikacijska številka.

Dejstvo, da ima oseba s tujo elektronsko identifikacijo švedsko osebno identifikacijsko številko, tuji storitvi avtentikacije običajno ni znano, zato te informacije niso vključene v potrdilo o identiteti iz države, v kateri je oseba avtenticirana. Švedsko vozlišče pa lahko po drugi strani opravi poizvedbo pri storitvi atributov na Švedskem[1], ali za avtenticirano osebo obstaja registrirana osebna identifikacijska številka, in lahko v tem primeru takšne informacije vključi v potrdilo o identiteti, poslano elektronski storitvi.

> [1]: V času pisanja ni storitve atributov, ki bi povezovala identitete eIDAS in švedske osebne identifikacijske številke.

1.7.4 Švedske elektronske identifikacije v tujih elektronskih storitvah

Švedska je priglasila švedske elektronske identifikacije na srednji in visoki ravni zanesljivosti v skladu z eIDAS.

Zahteva za avtentikacijo iz tuje elektronske storitve se pošlje švedskemu vozlišču eIDAS (posredniška storitev) prek vozlišča eIDAS (eIDAS-connector) v državi elektronske storitve. V švedskem vozlišču eIDAS uporabnik izbere, s katero švedsko elektronsko identifikacijo želi opraviti avtentikacijo, nato pa se storitvi za avtentikacijo pošlje zahteva za avtentikacijo (*Identitety Provider*), ki obravnava izbrano elektronsko identifikacijo. Ta zahteva je oblikovana v skladu s tehničnim okvirom, kar pomeni, da švedska storitev avtentikacije ni dolžna izpolnjevati tehničnih specifikacij eIDAS.

Uporabnika avtenticira švedska storitev za avtentikacijo in izda se potrdilo o identiteti (v skladu s tehničnim okvirom). To potrdilo prejme švedska posredniška storitev eIDAS in potrdilo se pretvori v potrdilo v skladu s specifikacijami eIDAS, preden se posreduje tujemu vozlišču eIDAS (eIDAS-connector) in nato klicni e-storitvi (*Service Provider*).

2. Tehnične specifikacije

To poglavje vsebuje specifikacije in profile za identitetne zveze, ki so skladne s tehničnim okvirom Sweden Connect, ter nekatere povezane storitve. Če ni drugače navedeno, so ti dokumenti predpisani za zagotavljanje storitev znotraj identitetnih zvez, ki izvajajo tehnični okvir.

2.1 Profili in specifikacije za SAML

Identitetne zveze, ki so skladne s tehničnim okvirom Sweden Connect, temeljijo na profilu uvedbe za švedski okvir elektronske identifikacije („Deployment Profile for the Swedish eID Framework“) (SAML.Profile). Na ta profil vpliva profil uvedbe SAML V2.0 za zvezno interoperabilnost („SAML V2.0 Deployment Profile for Federation Interoperability“)

[SAML2Int], vendar normativno ni odvisen od njega. [SAML.Profil] vsebuje tudi posebna pravila in smernice za tehnični okvir Sweden Connect.

2.1.1 Profil uvedbe za švedski okvir za elektronsko identifikacijo

Profil uvedbe za švedski okvir za elektronsko identifikacijo („Deployment Profile for the Swedish eID Framework“), [SAML.Profile], je glavni dokument tehničnega okvira in med drugim določa:

- kako se sestavijo in razlagajo metapodatki SAML;
- način oblikovanja zahteve za avtentikacijo;
- kako se obravnava zahteva za avtentikacijo in kako se oblikuje, preverja in obravnava potrdilo o identiteti;
- varnostne zahteve;
- posebne zahteve SAML za storitve podpisovanja in „avtentikacijo za podpis“.

2.1.2 Švedski okvir za elektronsko identifikacijo – register identifikatorjev

Za izvajanje infrastrukture za švedsko elektronsko identifikacijo so potrebne različne oblike identifikatorjev za predstavitev objektov v podatkovnih strukturah. Dokument „Sweden Connect – Registry for identifiers“, [SC.Registry], določa strukturo identifikatorjev, dodeljenih v skladu s tehničnim okvirom, in register opredeljenih identifikatorjev.

2.1.3 Specifikacija atributov za švedski okvir elektronske identifikacije

Specifikacija atributov za švedski okvir elektronske identifikacije („Attribute Specification for the Swedish eID Framework“), [SAML.Attributes], določa profile atributov SAML, ki se uporabljajo znotraj identitetnih zvez, ki izpolnjujejo tehnični okvir, vključno s tistimi, ki se povezujejo z eIDAS prek švedskega vozlišča eIDAS.

2.1.4 Kategorije subjektov za švedski okvir elektronske identifikacije

Kategorije subjektov se znotraj zveze uporabljajo za več različnih namenov:

- kategorije storitvenih subjektov (Service Entity Categories) – uporabljajo se v metapodatkih za prikaz zahtev elektronskih storitev glede ravni zanesljivosti in zahtevanih atributov ter izpolnjevanja ravni zanesljivosti storitev za avtentikacijo in zagotavljanja atributov;
- kategorije lastnosti storitev (Service Property Categories) – uporabljajo se za predstavitev posebne značilnosti storitve;
- kategorije subjektov glede na vrste storitev (Service Type Entity Categories) – uporablja se za predstavitev različnih vrst storitev znotraj zveze;

- kategorije subjektov s pogodbo o storitvah (Service Contract Entity Categories) – uporabljajo jih storitve za objavo obrazcev pogodb in podobno.

- splošne kategorije subjektov (General Entity Categories) – kategorije subjektov, ki ne spadajo v nobeno od zgornjih vrst.

Specifikacija kategorij subjektov za švedski okvir elektronske identifikacije („Entity Categories for the Swedish eID Framework“) [SAML.EntCat] določa kategorije subjektov, opredeljene s tehničnim okvirom, in opisuje njihov pomen.

2.1.5 Specifikacija izdelanih atributov eIDAS za švedski okvir elektronske identifikacije

Specifikacija izdelanih atributov eIDAS za švedski okvir elektronske identifikacije („eIDAS Constructed Attributes Specification for the Swedish eID Framework“), [SC.eIDAS.Attrs], določa procese in pravila za izdelavo atributov ID na podlagi atributov, prejetih med avtentikacijo v eIDAS.

2.1.6 Profil izvajanja za ponudnike identitete BankID v švedskem okviru elektronske identifikacije

Specifikacija profila izvajanja za ponudnike identitete BankID v švedskem okviru elektronske identifikacije („Implementation Profile for BankID Identity Providers within the Swedish eID Framework“), [SAML.BankID], določa pravila glede zasnove storitve za avtentikacijo, ki izvaja podporo za BankID.

> **Upoštevati je treba naslednje:** Ta specifikacija ne predpisuje skladnosti s tehničnim okvirom. Pomembna je le za storitve za avtentikacijo, ki izvajajo podporo za BankID in elektronske storitve, ki jih uporabljajo. Vendar pa morajo storitve za avtentikacijo, ki izvajajo podporo za BankID in se želijo povezati z zvezo Sweden Connect, izpolnjevati to specifikacijo.

2.1.7 Glavna izbira v zahtevah za avtentikacijo SAML

Specifikacija glavne izbire v zahtevah za avtentikacijo SAML („Principal Selection in SAML Authentication Requests“), [SAML.Principal], opredeljuje razširitev na SAML, ki zanašajoči se stranki omogoča, da obvesti storitev za avtentikacijo, katero identiteto želi avtenticirati.

2.1.8 Razširitev uporabniškega sporočila v zahtevah za avtentikacijo SAML

Specifikacija razširitve uporabniškega sporočila v zahtevah za avtentikacijo SAML („User Message Extension in SAML Authentication Requests“), [SAML.UMessage], opredeljuje razširitev na SAML, ki zanašajoči se stranki omogoča vključitev prikaznega sporočila v zahtevo za avtentikacijo, poslano storitvi za avtentikacijo. Storitev za avtentikacijo lahko nato prikaže to sporočilo uporabniku med korakom avtentikacije.

2.2 Profili in specifikacije za OpenID Connect

2.2.1 Profil OpenID Connect za Sweden Connect

Profil OpenID Connect za Sweden Connect („OpenID Connect Profile for Sweden Connect“), [OIDC.Profile], gradi na švedskem profilu OpenID Connect, ki je profil OpenID Connect, razvit s strani OIDC Sweden za spodbujanje interoperabilnosti in varnosti v švedskih rešitvah OIDC.

[OIDC.Profile] dodaja dodatne zahteve glede zveze Sweden Connect.

2.2.2 Specifikacija zahtev in obsega OpenID Connect za Sweden Connect

Specifikacija zahtev in obsega OpenID Connect za Sweden Connect („OpenID Connect Claims and Scopes Specification for Sweden Connect“), [OIDC.Claims], gradi na specifikaciji zahtev in obsega za švedski profil OpenID Connect („Claims and Scopes Specification for the Swedish OpenID Connect Profile“) OIDC Sweden.

2.3 Specifikacije za podpis

Ta oddelek vsebuje sklicevanja na dokumente, ki opredeljujejo storitve podpisovanja znotraj zvez, ki so skladne s tehničnim okvirom Sweden Connect.

2.3.1 Profil izvajanja za uporabo OASIS DSS v centralnih storitvah podpisovanja

Profil izvajanja za uporabo OASIS DSS v centralnih storitvah podpisovanja („Implementation Profile for Using OASIS DSS in Central Signing Services“), [Sign.DSS.Profile], določa profil za zahtevo za podpis in odgovor v skladu s standardom OASIS o osnovnih protokolih, elementih in vezavah za storitve digitalnega podpisa („Digital Signature Service Core Protocols, Elements, and Bindings“), [DSS].

2.3.2 Razširitev DSS za zvezne centralne storitve podpisovanja

Razširitev DSS za zvezne centralne storitve podpisovanja („DSS Extension for Federated Central Signing Services“), [Sign.DSS.Ext], je razširitev standarda OASIS o osnovnih protokolih, elementih in vezavah za storitve digitalnega podpisa („Digital Signature Service Core Protocols, Elements, and Bindings“), [DSS], ki določa opredelitve, potrebne za podpisovanje v tehničnem okviru.

2.3.3 Profil potrdila za potrdila, ki jih izdajo centralne storitve podpisovanja

Profil potrdila za potrdila, ki jih izdajo centralne storitve podpisovanja („Certificate profile for certificates issued by Central Signing services“), [Sign.Cert.Profile], določa vsebino potrdil za podpisovanje. Ta profil uporablja novo razširitev potrdila za podporo storitvam podpisovanja.

Ta profil se nanaša na razširitev potrdila za kontekst avtentikacije („Authentication Context Certificate Extension“), [AuthContext], ki opisuje, kako je kontekst avtentikacije („Authentication Context“) predstavljen v potrdilih X.509.

2.3.4 Protokol za aktiviranje podpisa za zvezno podpisovanje

V specifikaciji protokola za aktiviranje podpisa za zvezno podpisovanje („Signature Activation Protocol for Federated Signing“) (Sign.Activation) je opredeljen protokol za aktiviranje podpisa („Signature Activation Protocol“) (SAP) za izvajanje zagotavljanja izključnega nadzora na ravni 2 („Sole Control Assurance Level 2“) (SCAL2) v skladu s standardom EN 419241 Zaupanja vredni sistemi, ki podpirajo strežniško podpisovanje.

3. Referenčni seznam

3.1 DIGG

[Digg.Tillit]

Okvir zaupanja za švedsko elektronsko identifikacijo.

[SC.Registry]

Sweden Connect – Registry for identifiers.

[SAML.Profile]

Deployment Profile for the Swedish eID Framework.

[SAML.Attributes]

Attribute Specification for the Swedish eID Framework.

[SAML.EntCat]

Entity Categories for the Swedish eID Framework.

[SC.eIDAS.Attrs]

eIDAS Constructed Attributes Specification for the Swedish eID Framework.

[SAML.BankID]

Implementation Profile for BankID Identity Providers within the Swedish eID Framework.

[SAML.Principal]

Principal Selection in SAML Authentication Requests.

[SAML.UMessage]

User Message Extension in SAML Authentication Requests.

[OIDC.Profile]

OpenID Connect Profile for Sweden Connect.

[OIDC.Claims]

OpenID Connect Claims and Scopes Specification for Sweden Connect.

[Sign.DSS.Profile]

Implementation Profile for Using OASIS DSS in Central Signing Services.

[Sign.DSS.Ext]

DSS Extension for Federated Central Signing Services.

[Sign.Cert.Profile]

Certificate profile for certificates issued by Central Signing services.

[Sign.Activation]

Signature Activation Protocol for Federated Signing.

3.2 Druga sklicevanja

[SAML2Int]

SAML V2.0 Deployment Profile for Federation Interoperability.

[DSS]

OASIS Standard – Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0, April 11, 2007.

[AuthContext]

RFC-7773: Authentication Context Certificate Extension.