Sweden Connect

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Introductie tot het technische kader van Sweden Connect

2024-12-04

Referentienummer: **2019-267**

Inhoudsopgave

1. Inleiding

1.1. Overzicht

Het Technische kader van Sweden Connect is aangepast voor identiteitsfederaties op basis van SAML 2.0.

> In de laatste versie van het Technische kader zijn ook specificaties voor OpenID Connect geïntroduceerd. Op dit moment is er geen federatieondersteuning voor OpenID Connect. Dit zal in 2025 worden ingevoerd.

De overige delen van dit document beschrijven alleen de SAML-federatie. Zodra OpenID Connect volledig is geïntroduceerd, zal dit document ook betrekking hebben op deze technologie.

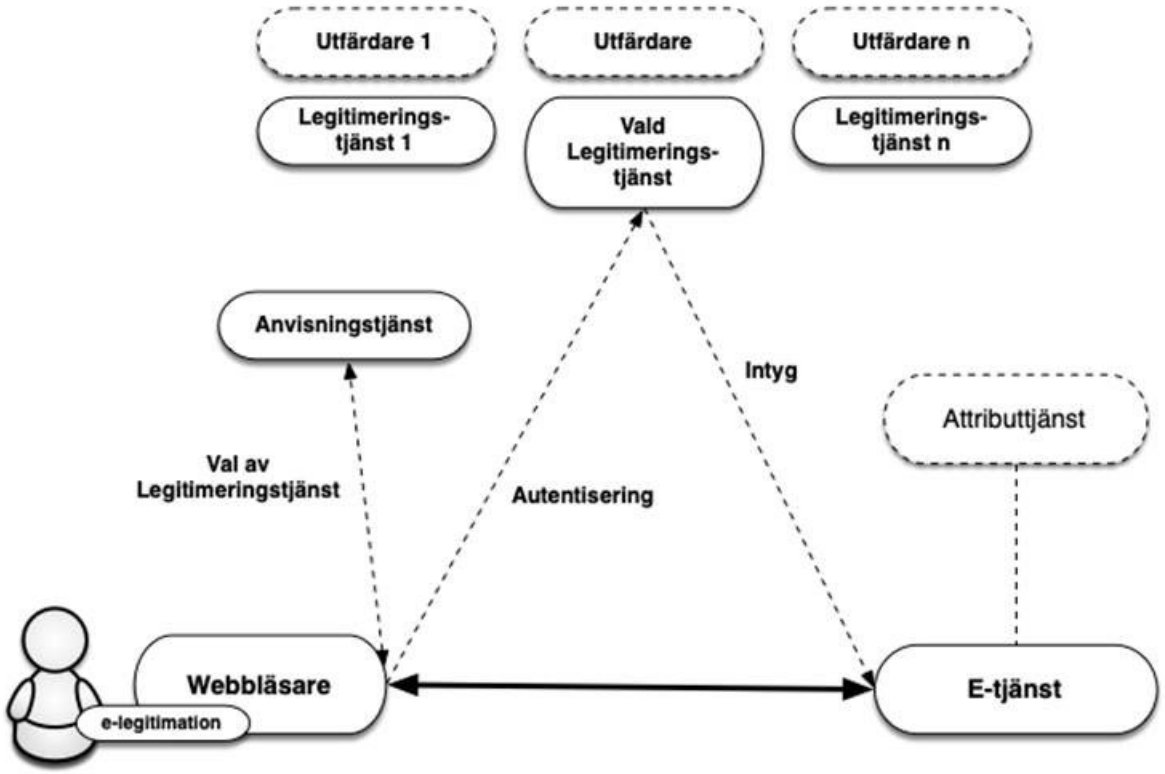
Betrouwbare partijen ontvangen identiteitscertificaten in een gestandaardiseerd formaat van een authenticatieservice[1].

E-services waarvoor een handtekening vereist is, hoeven niet te worden aangepast aan de eID's van verschillende gebruikers om elektronische handtekeningen aan te maken. In plaats daarvan delegeert de e-service dit uit aan een handtekeningservice, waarbij gebruikers door middel van authenticatie via een authenticatieservice de mogelijkheid krijgen om elektronische documenten te ondertekenen.

Binnen de federatie spelen e-services en bijbehorende betrouwbare partijen de rol van serviceprovider (SP) en authenticatieservices die identiteitscertificaten afgeven de rol van identiteitsprovider (IdP) en dus van diegene die de gebruiker authenticeert, ongeacht de e-service waarvoor de gebruiker wordt geauthenticeerd.

Voor die gevallen waarin de e-service meer informatie over de gebruiker nodig heeft, bijvoorbeeld informatie over rechtsbevoegdheid, kan een vraag worden gesteld aan een attributenservice binnen de federatie, Attributenautoriteit (AA), indien een dergelijke relevante attributenservice bestaat. Via een attributenaanvraag kan de e-service de nodige aanvullende informatie verkrijgen om de gebruiker te autoriseren en toegang te verlenen tot de e-service of een gelijkwaardige service.

Aangezien zowel persoonlijke identiteitsgegevens als andere kenmerken die aan gebruikers zijn gekoppeld, worden verstrekt via identiteitscertificaten en attributencertificaten, kunnen alle soorten eID's waarover betrouwbare partijen een overeenkomst hebben afgesloten en die deel uitmaken van de federatie, worden gebruikt voor authenticatie ten aanzien van een e-service waarvoor zowel een persoonlijk identiteitsnummer als aanvullende informatie vereist is, zelfs als de eID geen specifieke persoonsgegevens bevat (bv. programmacodes voor het genereren van eenmalige wachtwoorden).



Utfärdare 1	Uitgever 1
Utfärdare n	Uitgever n
Legitimeringstjänst 1	Authenticatieservice 1
Vald legitimeringstjänst	Geselecteerde authenticatieservice
Legitimeringstjänst n	Authenticatieservice n
Anvisningstjänst	Zoekdienst
Intyg	Certificaat
Val av legitimeringstjänst	Keuze van authenticatieservice
autentisering	Authenticatie
attributtjänst	Attributenservice
Webbläsare	Browser
E-tjänst	E-service

Afbeelding 1: *Illustratie van de communicatie tussen de verschillende services binnen een identiteitsfederatie.*

[1]: De authenticatieservice wordt in andere documentatie van Digg ook wel een identiteitsservice en een certificatieservice genoemd. In dit document wordt echter alleen de term “authenticatieservice” gebruikt.

1.2. Vertrouwenskader en beveiligingsniveaus

De basis voor het beveiligingsniveau dat dient te worden toegepast wanneer een gebruiker wordt geauthenticeerd is het zekerheidsniveau voor de door de e-service vereiste e-identificatie. Om ervoor te zorgen dat deze beveiligingsniveaus binnen het kader van de federatie vergelijkbaar zijn, zijn er vier zekerheidsniveaus (1-4) gedefinieerd in het

vertrouwenskader voor Zweedse e-identificatie [Digg.Tillit] en drie zekerheidsniveaus (laag, substantieel, hoog) in de eIDAS-verordening van de EU. Alle uitgevers van identiteitscertificaten dienen aan te tonen, dat het gehele proces dat ten grondslag ligt aan de afgifte van identiteitscertificaten voldoet aan de vereisten van het vereiste zekerheidsniveau, met inbegrip van:

- vereisten voor het opstellen van het identiteitscertificaat;
- vereisten voor elektronische identificatie (authenticatie);
- vereisten voor het afgifteproces;
- vereisten voor de eID zelf en het gebruik ervan;
- vereisten voor de eID-uitgever;
- vereiste voor het vaststellen van de identiteit van de eID-aanvrager.

1.3. Service voor het verzamelen, beheren en publiceren van metagegevens

Een SAML-federatie verstrekt informatie over de deelnemers van de federatie via SAML-metagegevens. Zowel entiteiten die authenticatie- en attributenservices in de federatie verlenen als betrouwbare partijen, d.w.z. entiteiten die deze services, bijvoorbeeld e-services, gebruiken, worden beschouwd als deelnemers aan een federatie.

Dankzij de metagegevens van de federatie kunnen deelnemers informatie verkrijgen over de services van andere deelnemers, met inbegrip van de gegevens die nodig zijn voor de veilige uitwisseling van informatie tussen deelnemers. Metagegevens dienen door elke partij up-to-date te worden gehouden en in overeenstemming te zijn met de contractuele voorwaarden.

Het belangrijkste doel van metagegevens is het verstrekken van de sleutels/certificaten die nodig zijn voor veilige communicatie en informatie-uitwisseling tussen services. Naast sleutels bevatten metagegevens ook andere informatie die belangrijk is voor de interactie tussen services, zoals adressen van vereiste functies, informatie over zekerheidsniveaus, servicecategorieën, gebruikersinterface-informatie, enz.

Een identiteitsfederatie wordt gedefinieerd door een register in XML-formaat dat is ondertekend met het certificaat van de federatiebeheerder. Het bestand bevat informatie over de leden van de identiteitsfederatie, inclusief hun certificaten. Aangezien het metagegevensbestand is ondertekend, volstaat het om een certificaat te vergelijken met zijn equivalent in metagegevens. Een infrastructuur op basis van een centraal federatieregister vereist dat het register voortdurend wordt bijgewerkt en dat de leden van de federatie altijd de nieuwste versie van het bestand gebruiken.

1.4. Zoekdienst

In een identiteitsfederatie is het mogelijk om een gedeelde zoekdienst aan te bieden en te gebruiken, waarin wordt vermeld uit welke authenticatieservices de gebruiker kan kiezen. Het doel van een dergelijke zoekdienst is om de individuele e-services die deel uitmaken van de identiteitsfederatie te ontlasten van het implementeren van ondersteuning voor de manier waarop gebruikers de authenticatieservice (of inlogmethode) kiezen.

Aangezien de zoekdienst beschikbaar is binnen de identiteitsfederatie kunnen e-services hun gebruikers daar naartoe verwijzen om de authenticatieservice te kiezen. De zoekdienst communiceert met de gebruiker die zijn keuze maakt en de gebruiker met zijn gemaakte keuze wordt teruggestuurd naar de e-service, die nu weet naar welke authenticatieservice de gebruiker dient te worden doorgestuurd voor authenticatie.

> Er is momenteel niet voorzien in een gedeelde zoekdienst voor de Sweden Connect-federatie.

1.5. Integratie bij de betrouwbare partij

Betrouwbare partijen, zoals e-services, integreren met authenticatieservices door middel van gestandaardiseerde berichten en gebruiken identiteitscertificaten die ook gestandaardiseerde formaten hebben.

Het technisch kader van Sweden Connect wordt beïnvloed door het interoperabiliteitsprofiel “SAML V2.0 Implementatieprofiel voor interoperabiliteit tussen federaties” [SAML2Int]. Het profiel wordt ondersteund door een aantal commerciële producten en open source-oplossingen, wat de integratie van e-services vergemakkelijkt.

Veel e-services maken gebruik van aparte authenticatieoplossingen, wat betekent dat het aanpassen van de integratie aan het technische kader een beperkte impact heeft op de e-service als zodanig.

1.6. Handtekening

Bij ondertekening maakt het technische kader van Sweden Connect het mogelijk om verschillende soorten eID te gebruiken, zelfs die welke niet op certificaten zijn gebaseerd, zonder dat er speciale aanpassingen in de e-service nodig zijn. Dit komt omdat het elektronisch afgegeven identiteitscertificaat (gebruikt voor de identificatie van gebruikers bij het ondertekenen) hetzelfde formaat heeft, ongeacht het type eID dat door de gebruiker wordt gebruikt.

Een handtekeningservice is bedoeld om binnen identiteitsfederaties handtekeningen te kunnen gebruiken die voldoen aan het technische kader, ondersteund door alle soorten eID die een voldoende mate van beveiliging bieden.

Door de inkoop[1] en introductie van een handtekeningservice kan een betrouwbare partij die deel uitmaakt van de federatie een gebruiker in staat stellen een elektronisch document te ondertekenen met de ondersteuning van de handtekeningservice. De elektronische handtekening van de gebruiker en het bijbehorende ondertekeningscertificaat worden aangemaakt door de handtekeningservice nadat de gebruiker ermee heeft ingestemd te ondertekenen door zich te authenticeren ten overstaan van de handtekeningservice[2].

> [1]: Het is ook mogelijk om een handtekeningservice te implementeren op basis van de specificaties van het technische kader, of anderszins een handtekeningservice te verwerven.
>
> [2]: Het is belangrijk op te merken dat het van het grootste belang is dat de gebruiker dit proces ziet als het ondertekenen van een document. Voor de eID’s

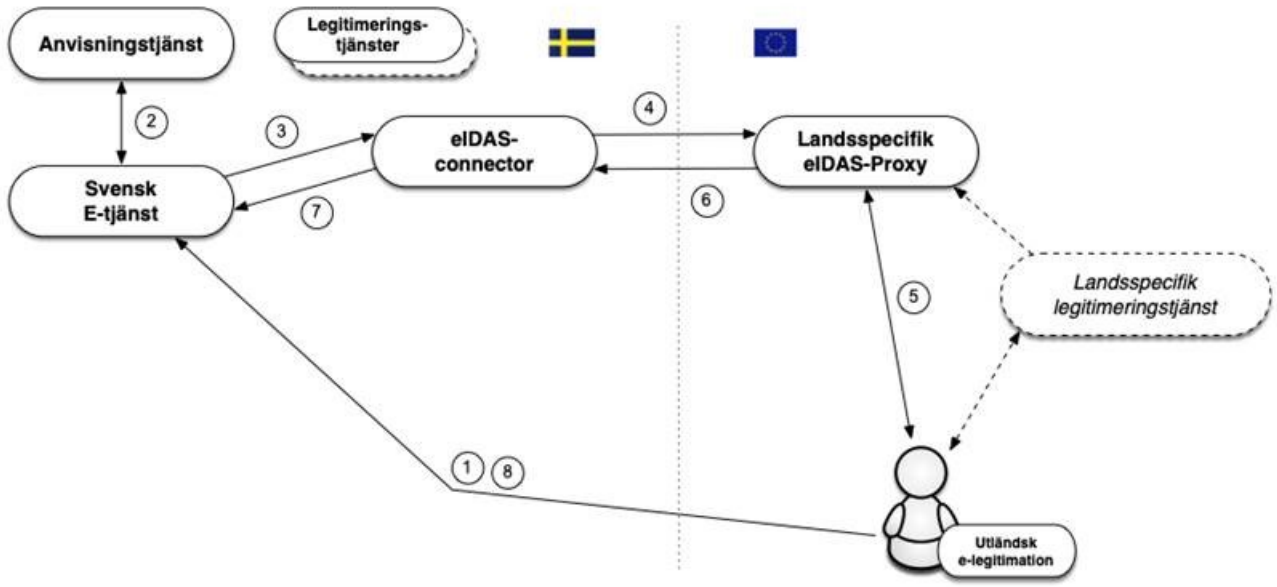
die dit ondersteunen dient daarom een handtekeningenstroom te worden gebruikt in verband met “authenticatie voor handtekening”.

1.7. Technisch kader en eIDAS

De EU-verordening (910/2014) betreffende elektronische identificatie en vertrouwensservices, eIDAS, verplicht Zweedse overheidsinstanties om de eID’s te erkennen die andere eIDAS-landen hebben aangemeld. Dit betekent dat een openbare Zweedse e-service op basis van bepaalde regels een login dient te kunnen accepteren die is uitgevoerd met een eID die in een ander land is uitgegeven.

1.7.1. Authenticatie met behulp van buitenlandse eID’s

De technische specificaties voor eIDAS zijn, net als het technische kader, gebaseerd op SAML-normen, en hoewel er veel overeenkomsten zijn, bestaan er ook verschillen in deze specificaties. Een Zweedse e-service mag echter niet rechtstreeks verband houden met de technische specificaties van eIDAS. De onderstaande afbeelding illustreert hoe het Zweedse eIDAS-knooppunt (*eIDAS-connector*) fungeert als brug tussen andere landen en de Zweedse federatie wanneer een persoon wordt geauthenticeerd met behulp van een buitenlandse eID in een Zweedse e-service. Het Zweedse eIDAS-knooppunt voldoet aan het technische kader.



Anvisningstjänst	Zoekdienst
Legitimeringstjänster	Authenticatieservices
Svensk E-tjänst	Zweedse e-service
EiDAS-connector	eiDAS-connector
Landsspecifik Eidas Proxy	Landspecifieke eIDAS-proxy
Landsspecifik legitimeringstjänst	Landspecifieke authenticatieservice
utländsk e-legitimation	Buitenlandse eID

De stroom is als volgt:

1. Een gebruiker met een buitenlandse eID vraagt toegang tot een Zweedse e-service (d.w.z. logt in).

2. Met de e-service kan de gebruiker de inlogmethode kiezen met behulp van een zoekdienst. Er wordt een optie “Buitenlandse eID” weergegeven, die door de gebruiker in het eIDAS-geval wordt geselecteerd.

3. De e-service maakt een authenticatieverzoek aan in overeenstemming met dit technische kader en stuurt de gebruiker naar het Zweedse eIDAS-knooppunt (*connector*) waarvoor DIGG verantwoordelijk is. Het eIDAS-knooppunt fungeert als authenticatieservice (*Identiteitsprovider*) in de federatie ten opzichte van Zweedse betrouwbare partijen, wat betekent dat de communicatie met deze service op dezelfde manier verloopt als met andere authenticatieservices binnen federaties die voldoen aan het technische kader.

4. Het ontvangen verzoek wordt verwerkt en het eIDAS-knooppunt toont een selectiepagina waarop de gebruiker “zijn land” selecteert[1]. Het Zweedse eIDAS-knooppunt zet nu het ontvangen authenticatieverzoek om in een eIDAS-authenticatieverzoek en stuurt de gebruiker naar de “eIDAS-proxyservice” van het geselecteerde land.

5. Wanneer het authenticatieverzoek wordt ontvangen door de eIDAS-proxyservice voor het geselecteerde land, neemt de authenticatietechnologie van dit land het over. Niet alle eIDAS-landen gebruiken SAML voor authenticatie, maar als dit het geval was in ons voorbeeld, zou de gebruiker worden doorgestuurd naar een authenticatieservice (*Identiteitsprovider*), en daarvoor misschien ook een zoekdienst voor de selectie van de authenticatieservice.

6. Nadat de authenticatie is uitgevoerd, wordt er een certificaat (*Verklaring*) aangemaakt volgens de eIDAS-specificaties. Dit certificaat bevat eIDAS-specifieke kenmerken die de gebruiker identificeren. Dit certificaat wordt nu doorgestuurd naar het Zweedse eIDAS-knooppunt.

7. Het knooppunt ontvangt het certificaat en valideert de juistheid ervan. Dit certificaat wordt omgezet van eIDAS-formaat in een certificaat dat is ingedeeld volgens het technische kader en wordt naar de e-service gemaild.

8. De betrouwbare partij voegt aanvullende informatie toe en bepaalt of de gebruiker toegang tot de service kan krijgen.

Zweedse e-services hoeven dus alleen het technische kader te ondersteunen om een authenticatie te verwerken die wordt uitgevoerd met behulp van een Europese eID. De e-service dient echter de gepresenteerde identiteit te kunnen verwerken, wat niet noodzakelijk een persoonlijk identiteitsnummer is. Er kunnen dus gevallen voorkomen waarin een e-service een gebruiker authenticeert via het eIDAS-kader, maar de gepresenteerde identiteit van de gebruiker niet kan worden gebruikt in de e-service. Meer hierover in hoofdstuk 1.7.3 hieronder.

[1]: In feite kiest de gebruiker de “eIDAS-proxyservice” waarnaar het verzoek dient te worden doorgestuurd. Dit is afhankelijk van het land waartoe de eID-uitgever van de gebruiker behoort.

1.7.2. Handtekeningen met behulp van buitenlandse eID's

Zoals reeds beschreven, wordt er een model voor elektronische handtekening toegepast binnen dit technische kader dat gefedereerde handtekening wordt genoemd. Er is een servergebaseerde handtekeningservice aan de e-service gekoppeld, die op zijn beurt een handtekening aanvraagt. Wanneer een gebruiker een document ondertekent, stuurt de e-service een handtekeningverzoek naar de handtekeningservice. De handtekeningservice vraagt de gebruiker vervolgens om zichzelf te authenticeren. In verband met de authenticatie keurt de gebruiker de handtekening goed. De handtekeningservice stuurt gegevens terug naar de e-service en vervolgens worden de handtekeninggegevens die zijn gekoppeld aan het ondertekende document, opgeslagen.

Deze procedure maakt het mogelijk om ook te ondertekenen met behulp van een buitenlandse eID, aangezien de handtekeningservice ervoor kan kiezen om de gebruiker te authenticeren met behulp van een buitenlandse eID in overeenstemming met de hierboven in punt 1.7.1 beschreven procedure.

Bij het ondertekenen is, in dit geval, het Zweedse eIDAS-knooppunt verantwoordelijk de gebruiker te informeren dat het doel van de authenticatie is een document te ondertekenen, wie de handtekening heeft aangevraagd en, indien van toepassing, wat er wordt ondertekend. Pas nadat de gebruiker zich (voor ondertekening) heeft geauthenticeerd wordt een identiteitscertificaat afgegeven dat naar de handtekeningservice wordt verzonden, die op zijn beurt de handtekening genereert.

1.7.3. Beheer van identiteiten

Identiteitscertificaten uit andere landen voldoen aan EU-brede technische specificaties die in het kader van de eIDAS-verordening zijn ontwikkeld. In deze verordening zijn de attributen vastgelegd die elk land altijd dient op te nemen voor natuurlijke personen en voor organisaties ("Minimale dataset", MDS). Elk land dient een unieke identificatiecode per eID op te nemen die slechts één natuurlijke persoon vertegenwoordigt. Identificatiecodes uit sommige landen zijn voor iedere persoon uniek en staan vast, op dezelfde manier als bijvoorbeeld Zweedse persoonlijke identiteitsnummers, maar deze identificatiecodes kunnen zeer verschillende samenstellingen en kenmerken hebben. Een kenmerk dat kan variëren is hoe permanent een dergelijke identificatie is, d.w.z. of een dergelijke identificatie tijdens het leven van een persoon ongewijzigd blijft of verandert als de persoon bijvoorbeeld naar een andere regio verhuist, zijn naam wijzigt of gewoon zijn eID wijzigt. De identificatiecode uit sommige landen (bv. het VK) kan variëren afhankelijk van welke van de in het land beschikbare eID's een gebruiker momenteel verkiest gebruik te maken.

Om het beheer van gebruikers in Zweedse e-services te vereenvoudigen genereert het Zweedse eIDAS-knooppunt een gestandaardiseerd ID-attribuut voor gebruikers die zijn geauthenticeerd met behulp van een buitenlandse eID, bekend als een *voorlopige ID* (afgekort als PRID). Daarnaast wordt er een geassocieerd attribuut gemaakt dat de verwachte persistentie of levensduur van dit ID-attribuut aangeeft. Het PRID-attribuut wordt gegenereerd op basis van de attributenwaarden die zijn verkregen uit de buitenlandse authenticatie volgens gespecificeerde methoden voor dat specifieke land. Elke combinatie van land en methode wordt gecategoriseerd voor wat betreft verwachte persistentie, d.w.z. hoe waarschijnlijk het is dat een identiteit voor dezelfde persoon in de loop van de tijd verandert. Dit stelt Zweedse e-services in staat om de communicatie met de gebruiker aan te passen en

proactief functies aan te bieden die het gemakkelijker maken voor een gebruiker wiens identiteit is veranderd om de controle over zijn informatie in de e-service terug te winnen.

In sommige gevallen kan een persoon die is geauthenticeerd met behulp van een buitenlandse eID ook in het bezit zijn van een Zweeds persoonlijk identiteitsnummer. Dit kan bijvoorbeeld een Zweedse burger zijn die naar het buitenland is verhuisd en een buitenlandse eID heeft verkregen, of een buitenlandse burger die in Zweden is geregistreerd en een persoonlijk identiteitsnummer heeft gekregen.

Het feit dat een persoon met een buitenlandse eID een Zweeds persoonlijk identiteitsnummer heeft, is normaal gesproken niet bekend bij de buitenlandse authenticatieservice en deze informatie is daarom niet opgenomen in het identiteitscertificaat van het land waar de persoon is geauthenticeerd. Het Zweedse knooppunt daarentegen heeft de mogelijkheid om een attributenservice in Zweden te raadplegen[1] om te kijken of er een geregistreerd persoonlijk identiteitsnummer bestaat voor de geauthenticeerde persoon en kan, indien dit het geval is, dergelijke informatie toevoegen aan het identiteitscertificaat dat naar de e-service wordt verzonden.

> [1]: Op het moment van schrijven bestaat er geen attributenservice die een verband legt tussen eIDAS-identiteiten en Zweedse persoonlijke identiteitsnummers.

1.7.4. Zweedse eID’s in buitenlandse e-services

Zweden heeft Zweedse eID’s aangemeld op de betrouwbaarheidsniveaus substantieel en hoog volgens eIDAS.

Een verzoek om authenticatie van een buitenlandse e-service wordt ingediend bij het Zweedse eIDAS-knooppunt (proxyservice) via een eIDAS-connector in het land van de e-service. In het Zweedse eIDAS-knooppunt kiest de gebruiker met welke Zweedse eID hij zich wil authenticeren, waarna er een authenticatieverzoek naar de authenticatieservice wordt gestuurd (*Identiteitsprovider*) die de geselecteerde eID afhandelt. Dit verzoek is geformatteerd volgens een technisch kader, wat betekent dat een Zweedse authenticatieservice niet hoeft te voldoen aan de technische specificaties van eIDAS.

De gebruiker wordt geauthenticeerd door de Zweedse authenticatieservice en er wordt een identiteitscertificaat afgegeven (volgens het technische kader). Dit certificaat wordt ontvangen door de Zweedse eIDAS-proxyservice en omgezet in een certificaat volgens eIDAS-specificaties voordat het wordt doorgestuurd naar de buitenlandse eIDAS-connector en vervolgens naar de oproepende e-service (*Serviceprovider*).

2. Technische specificaties

Dit hoofdstuk bevat specificaties en profielen voor identiteitsfederaties die voldoen aan het technische kader van Sweden Connect, en voor bepaalde gerelateerde services. Tenzij anders vermeld, zijn deze documenten bindend voor de levering van services binnen identiteitsfederaties die het technische kader implementeren.

2.1. Profielen en specificaties voor SAML

Identiteitsfederaties die voldoen aan het technische kader van Sweden Connect zijn opgebouwd rond het “Uitrolprofiel voor het Zweedse eID-kader”, [SAML.Profile]. Dit profiel wordt beïnvloed door, maar is niet op voorschrijvende wijze afhankelijk van het “SAML V2.0 Uitrolprofiel voor interoperabiliteit tussen federaties” [SAML2Int]. [SAML.Profile] bevat ook regels en richtsnoeren die specifiek zijn voor het technische kader van Sweden Connect.

2.1.1. Uitrolprofiel voor het Zweedse eID-kader

“Uitrolprofiel voor het Zweedse eID-kader”, [SAML.Profile], is het belangrijkste technische kaderdocument en specificeert onder meer:

- hoe SAML-metagegevens dienen te worden opgesteld en geïnterpreteerd;
- de wijze waarop het authenticatieverzoek wordt ingedeeld;
- hoe een authenticatieverzoek wordt behandeld en hoe een identiteitscertificaat wordt ontworpen, geverifieerd en behandeld;
- beveiligingsvereisten;
- specifieke SAML-vereisten voor handtekeningservices en “authenticatie voor handtekening”.

2.1.2. Zweeds eID-kader – register van identificatiemiddelen

De implementatie van een Zweedse eID-infrastructuur vereist verschillende vormen van identificatiemiddelen om objecten in gegevensstructuren weer te geven. Het document “Sweden Connect – Register van identificatiemiddelen”, [SC.Registry], definieert de structuur van de in het kader van het technische kader toegewezen identificatiemiddelen, alsook een register van gedefinieerde identificatiemiddelen.

2.1.3. Attributenspecificatie voor het Zweedse eID-kader

De specificatie “Attributenspecificatie voor het Zweedse eID-kader”, [SAML.Attributes], verklaart de SAML-attribuutprofielen die worden gebruikt binnen identiteitsfederaties die voldoen aan het technische kader, inclusief diegenen die verbinding maken met eIDAS via het Zweedse eIDAS-knooppunt.

2.1.4. Entiteitscategorieën voor het Zweedse eID-kader

Entiteitscategorieën worden binnen de federatie voor een aantal verschillende doeleinden gebruikt:

- Service-entiteitscategorieën – worden gebruikt in metagegevens om de vereisten van e-services voor zekerheidsniveaus en gevraagde attributen weer te geven, evenals de naleving van zekerheidsniveaus door authenticatieservices en de levering van attributen.
- Service-eigendomscategorieën – worden gebruikt om een specifiek kenmerk van een service weer te geven.

- Entiteitscategorieën van servicetype – worden gebruikt om verschillende servicetypes binnen de federatie weer te geven.

- Entiteitscategorieën van servicecontracten – worden gebruikt door services om formulieren voor overeenkomsten en dergelijke aan te kondigen.

- Algemene entiteitscategorieën — entiteitscategorieën die niet onder een van de bovengenoemde typen vallen.

De specificatie “Entiteitscategorieën voor het Zweedse eID-kader” [SAML.EntCat] specificeert de door het technische kader gedefinieerde entiteitscategorieën en beschrijft de betekenis ervan.

2.1.5. eIDAS-specificatie voor aangemaakte attributen van het Zweedse eID-kader

De specificatie “eIDAS-specificatie voor aangemaakte attributen van het Zweedse eID-kader”, [SC.eIDAS.Attrs], specificeert processen en regels voor hoe ID-attributen worden aangemaakt op basis van attributen die zijn ontvangen tijdens authenticatie in eIDAS.

2.1.6. Implementatieprofiel voor BankID-identiteitsproviders binnen het Zweedse eID-kader

De specificatie “Implementatieprofiel voor BankID-identiteitsproviders binnen het Zweedse eID-kader”, [SAML.BankID], definieert regels voor hoe een authenticatieservice die ondersteuning voor BankID implementeert, dient te worden ontworpen.

> **Let op het volgende:** Deze specificatie is niet voorschrijvend voor de naleving van een technisch kader. Het is alleen relevant voor authenticatieservices die ondersteuning implementeren voor BankID en e-services die deze gebruiken. Authenticatieservices die ondersteuning voor BankID implementeren en verbinding willen maken met de Sweden Connect-federatie, dienen echter aan deze specificatie te voldoen.

2.1.7. Hoofdselectie in SAML-authenticatieverzoeken

De specificatie “Hoofdselectie in SAML-authenticatieverzoeken”, [SAML.Principal], definieert een uitbreiding van SAML die een betrouwbare partij in staat stelt een authenticatieservice te informeren welke identiteit zij wenst te authenticeren.

2.1.8. Gebruikersberichtextensie in SAML-authenticatieverzoeken

De specificatie “Gebruikersberichtextensie in SAML-authenticatieverzoeken”, [SAML.UMessage], definieert een uitbreiding van SAML waarmee een betrouwbare partij een weergavebericht kan opnemen in het authenticatieverzoek dat naar de authenticatieservice wordt verzonden. De authenticatieservice kan dit bericht vervolgens tijdens de authenticatiestap aan de gebruiker tonen.

2.2. Profielen en specificaties voor OpenID Connect

2.2.1. OpenID Connect-profiel voor Sweden Connect

Het profiel “OpenID Connect-profiel voor Sweden Connect”, [OIDC.Profile], is gebaseerd op het Zweedse OpenID Connect-profiel, dat een OpenID Connect-profiel is dat is ontwikkeld door OIDC Sweden ter bevordering van interoperabiliteit en beveiliging binnen Zweedse OIDC-oplossingen.

[OIDC.Profile] voegt aanvullende vereisten toe met betrekking tot de Sweden Connect-federatie.

2.2.2. Specificatie van OpenID Connect-claims en toepassingsgebieden voor Sweden Connect

Het specificatiedocument “Specificatie van OpenID Connect-claims en toepassingsgebieden voor Sweden Connect”, [OIDC.Claims], is gebaseerd op de specificatie ‘Specificatie van claims en toepassingsgebieden voor het Zweedse OpenID Connect-profiel’ van OIDC Zweden.

2.3. Specificaties voor ondertekening

Dit gedeelte bevat verwijzingen naar de documenten die handtekeningservices binnen de federaties definiëren die aan het technische kader van Sweden Connect voldoen.

2.3.1. Implementatieprofiel voor het gebruik van OASIS DSS in centrale ondertekeningsservices

Het implementatieprofiel “Implementatieprofiel voor het gebruik van OASIS DSS in centrale ondertekeningsservices”, [Sign.DSS.Profile], specificeert een profiel voor het verzoek om ondertekening en het antwoord daarop overeenkomstig de OASIS-norm “Kernprotocollen, elementen en bindingen voor de digitale handtekeningservice”, [DSS].

2.3.2. DSS-uitbreiding voor gefedereerde centrale ondertekeningsservices

“DSS-uitbreiding voor gefedereerde centrale ondertekeningsservices”, [Sign.DSS.Ext], is een uitbreiding van de OASIS-norm “Kernprotocollen, elementen en bindingen voor de digitale handtekeningservice”, [DSS], waarin de definities zijn gespecificeerd die nodig zijn voor ondertekening binnen het technische kader.

2.3.3. Certificaatprofiel voor certificaten afgegeven door centrale ondertekeningsservices

Het certificaatprofiel “Certificaatprofiel voor door centrale ondertekenservices afgegeven certificaten”, [Sign.Cert.Profile], specificeert de inhoud van ondertekeningscertificaten. Dit profiel past een nieuwe certificaatuitbreiding toe ter ondersteuning van handtekeningservices.

Dit profiel verwijst naar de “Uitbreiding van het authenticatiecontextcertificaat”, [AuthContext], waarin wordt beschreven hoe de “Authenticatiecontext” wordt weergegeven in X.509-certificaten.

2.3.4. Handtekeningactiveringsprotocol voor gefedereerde ondertekening

De specificatie “Handtekeningactiveringsprotocol voor gefedereerde ondertekening”, [Sign.Activation], definieert een “Handtekeningactiveringsprotocol” (SAP) voor de implementatie van “Exclusief controlewaarborgingsniveau 2” (SCAL2) overeenkomstig de norm “prEN 419241 – Ondertekening op de ondersteunende server van betrouwenswaardige systemen”.

3. Referentielijst

3.1. DIGG

[Digg.Tillit]

Vertrouwenskader voor Zweedse e-identificatie.

[SC.Registry]

Sweden Connect – Register van identificatiemiddelen.

[SAML.Profiel]

Uitrolprofiel voor het Zweedse eID-kader.

[SAML.Attributen]

Attributenspecificatie voor het Zweedse eID-kader.

[SAML.EntCat]

Entiteitscategorieën voor het Zweedse eID-kader.

[SC.eIDAS.Attrs]

eIDAS-specificatie van aangemaakte attributen voor het Zweedse eID-kader.

[SAML.BankID]

Implementatieprofiel voor BankID-identiteitsproviders binnen het Zweedse eID-kader.

[SAML.Principal]

Hoofdselectie in SAML-authenticatieverzoeken.

[SAML.UMessage]

Gebruikersberichtextensie in SAML-authenticatieverzoeken.

[OIDC.Profile]

OpenID Connect-profiel voor Sweden Connect.

[OIDC.Claims]

Specificatie van OpenID Connect-claims en toepassingsgebieden voor Sweden Connect.

[Sign.DSS.Profile]

Implementatieprofiel voor het gebruik van OASIS DSS in centrale ondertekeningsservices.

[Teken.DSS.Ext]

DSS-uitbreiding voor gefedereerde centrale ondertekeningsservices.

[Sign.Cert.Profile]

Certificaatprofiel voor certificaten afgegeven door centrale ondertekeningsservices.

[Sign.Activation]

Handtekeningactiveringsprotocol voor gefedereerde ondertekening.

3.2. Overige referenties

[SAML2Int]

SAML V2.0 Implementatieprofiel voor interoperabiliteit tussen federaties.

[DSS]

OASIS-norm – Kernprotocollen, elementen en bindingen voor de digitale handtekeningservice, versie 1.0, 11 april 2007.

[AuthContext]

RFC-7773: Uitbreiding van verificatiecontextcertificaat.