Introduktion til de tekniske rammer for Sweden Connect

2024-12-04

NOR: **2019-267**

Indholdsfortegnelse

1. Indledning

1.1. Oversigt

De tekniske rammer for Sweden Connect er tilpasset identitetsføderationer baseret på SAML 2.0.

> I den seneste version af den tekniske ramme er der også indført specifikationer for OpenID Connect. I øjeblikket er der ingen føderationsunderstøttelse af OpenID Connect. Dette vil blive indført i 2025.
>
> De resterende dele af dette dokument beskriver kun SAML-føderationen. Når OpenID Connect er fuldt introduceret, vil dette dokument også dække denne teknologi.

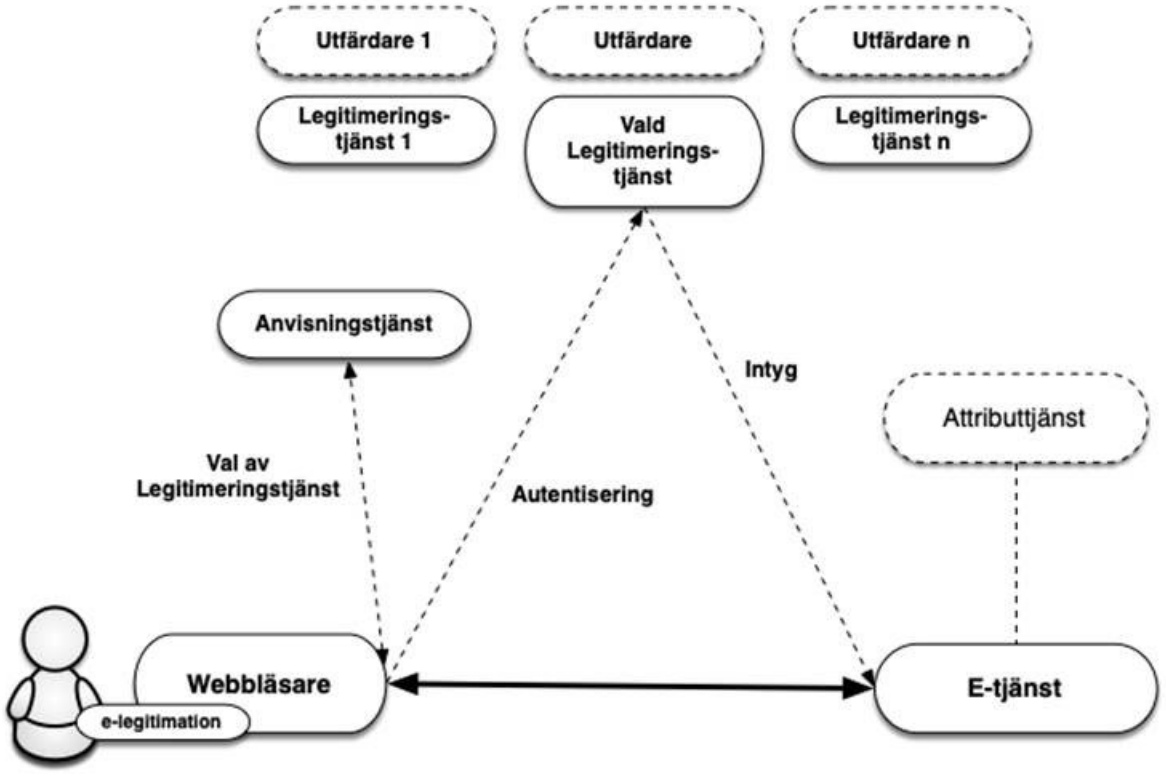
Modtagerparter modtager identitetscertifikater i et standardiseret format fra en autentifikationstjeneste[1].

E-tjenester, der kræver en signatur, behøver ikke at blive tilpasset forskellige brugeres eID'er for at kunne generere elektroniske signaturer. I stedet uddelegerer e-tjenesten dette til en signaturtjeneste, hvor brugerne, understøttet af autentifikation gennem en autentifikationstjeneste, får mulighed for at underskrive elektroniske dokumenter.

Inden for føderationen påtager e-tjenester og tilsvarende modtagerparter sig rollen som Service Provider (SP), mens autentifikationstjenester, der udsteder identitetscertifikater, påtager sig rollen som Identity Provider (IdP) og dermed autentifikator for brugeren, uanset hvilken e-tjeneste brugeren autentificeres for.

I de tilfælde, hvor e-tjenesten har brug for flere oplysninger om brugeren, f.eks. oplysninger om rets- og handleevne, kan der stilles et spørgsmål til en attributtjeneste, Attribute Authority (AA), inden for føderationen, hvis der findes en sådan relevant attributtjeneste. Via en attributanmodning kan e-tjenesten indhente de nødvendige yderligere oplysninger for at autorisere brugeren og give adgang til e-tjenesten eller tilsvarende.

Da både personoplysninger og andre attributter i forbindelse med brugere leveres gennem identitetscertifikater og attributcertifikater, kan alle typer eID'er, som modtagerparter har en aftale om, og som er en del af føderationen, anvendes til autentifikation i forbindelse med en e-tjeneste, der kræver både et personligt identitetsnummer og yderligere oplysninger, selv om eID'et ikke indeholder specifikke personoplysninger (f.eks. kodebokse til generering af engangsadgangskoder).



Utfärdare 1	Udsteder 1
Utfärdare n	Udsteder n

Legitimeringstjänst 1	Autentifikationstjeneste 1
Vald legitimeringstjänst	Valgt autentifikationstjeneste
Legitimeringstjänst n	Autentifikationstjeneste n
Anvisningstjänst	Opdagelsestjeneste
Intyg	Certifikat
Val av legitimeringstjänst	Valg af autentifikationstjeneste
autentisering	autentifikation
attributtjänst	attributtjeneste
Webbläsare	Browser
E-tjänst	E-tjeneste

Figur 1 *Illustration af kommunikationen mellem de forskellige tjenester inden for en identitetsføderation.*

> [1]: Autentifikationstjenesten omtales også i anden dokumentation fra Digg som en identitetstjeneste og en certificeringstjeneste. I dette dokument anvendes imidlertid kun udtrykket "autentifikationstjeneste".

1.2. Tillidsramme og sikkerhedsniveauer

Grundlaget for, hvilket sikkerhedsniveau der skal anvendes, når en bruger autentificerer sig, er tillidsniveauet for e-identifikationen, der kræves af e-tjenesten. For at disse sikkerhedsniveauer kan sammenlignes inden for føderationens rammer, er der defineret fire tillidsniveauer (1-4) i tillidsrammen for svensk e-identifikation [Digg.Tillit] og tre tillidsniveauer (lavt, betydeligt, højt) i EU's eIDAS-forordning. Alle identitetscertifikatudstedere skal påvise, at hele den proces, der ligger til grund for udstedelsen af identitetscertifikater, opfylder kravene til det krævede tillidsniveau, herunder:

- krav til oprettelse af identitetscertifikatet
- krav til elektronisk identifikation (autentifikation)
- krav til udstedelsesprocessen
- krav til selve eID'et og dets anvendelse
- krav til eID-udstederen
- krav til fastlæggelse af eID-ansøgerens identitet.

1.3. Tjeneste for indsamling, administration og offentliggørelse af metadata

En SAML-føderation giver oplysninger om føderationens deltagere gennem SAML-metadata. Både enheder, der leverer autentifikations- og attributtjenester i føderationen, og modtagerparter, dvs. enheder, der forbruger disse tjenester, f.eks. e-tjenester, anses for at være deltagere i en føderation.

Føderationens metadata giver deltagerne mulighed for at indhente oplysninger om andre deltageres tjenester, herunder de data, der er nødvendige for sikker udveksling af oplysninger

mellem deltagerne. Metadata skal holdes ajour af hver part og i overensstemmelse med kontraktbetingelserne.

Hovedformålet med metadata er at tilvejebringe de nøgler/certifikater, der er nødvendige for sikker kommunikation og udveksling af oplysninger mellem tjenester. Ud over nøgler indeholder metadata også andre oplysninger, der er vigtige for interaktionen mellem tjenester, såsom adresser på krævede funktioner, oplysninger om tillidsniveauer, tjenestekategorier, oplysninger om brugergrænseflader osv.

En identitetsføderation defineres af et register i XML-format, der er signeret med føderationsoperatørens certifikat. Filen indeholder oplysninger om medlemmerne af identitetsføderationen, herunder deres certifikater. Da metadatafilen er signeret, er det tilstrækkeligt at sammenligne et certifikat med dets metadata-modstykke. En infrastruktur, der er baseret på et centralt føderationsregister, kræver, at registret løbende opdateres, og at føderationens medlemmer altid bruger den seneste version af filen.

1.4. Opdagelsestjeneste

I en identitetsføderation er det muligt at tilbyde og forbruge en delt opdagelsestjeneste (Discovery Service), som viser de autentifikationstjenester, der er tilgængelige for brugeren at vælge imellem. Formålet med en sådan opdagelsestjeneste er at aflaste de enkelte e-tjenester, der er en del af identitetsføderationen, fra at implementere støtte med hensyn til, hvordan brugerne vælger autentifikationstjenesten (eller loginmetoden).

Da opdagelsestjenesten er tilgængelig inden for identitetsføderationen, kan e-tjenester dirigere deres brugere derhen for at vælge autentifikationstjenesten. Opdagelsestjenesten interagerer med den bruger, der foretager sit valg, og brugeren ledes sammen med brugerens valg tilbage til e-tjenesten, som nu ved, hvilken autentifikationstjeneste brugeren skal sendes til med henblik på autentifikation.

> Der er i øjeblikket ingen fælles opdagelsestjeneste for Sweden Connect-føderationen.

1.5. Integration hos modtagerparten

Modtagerparter, f.eks. e-tjenester, integrerer med autentifikationstjenester gennem standardiserede meddelelser og anvender identitetscertifikater, som også har standardiserede formater.

Sweden Connects tekniske ramme påvirkes af interoperabilitetsprofilen "SAML V2.0 Deployment Profile for Federation Interoperability" [SAML2Int]. Profilen understøttes af en række kommercielle produkter og Open Source-løsninger, som letter integrationen på e-tjenester.

Mange e-tjenester anvender selvstændige autentifikationsløsninger, hvilket betyder, at tilpasning af integrationen for at overholde den tekniske ramme har en begrænset indvirkning på e-tjenesten som sådan.

1.6. Signatur

Ved underskrivelse gør den tekniske ramme for Sweden Connect det muligt at anvende forskellige typer eID, selv dem, der ikke er certifikatbaserede, uden at der er behov for særlige tilpasninger i e-tjenesten. Dette skyldes, at det elektronisk udstedte identitetscertifikat (der anvendes til identifikation af brugere ved underskrivelse) har samme format, uanset hvilken type eID brugeren anvender.

En signaturtjeneste har til formål at muliggøre signaturer inden for identitetsføderationer, der overholder de tekniske rammer, understøttet af alle typer eID, der giver en tilstrækkelig grad af sikkerhed.

Ved anskaffelse[1] og indførelse af en signaturtjeneste kan en modtagerpart, der er en del af føderationen, give en bruger mulighed for at underskrive et elektronisk dokument med støtte fra signaturtjenesten. Brugerens elektroniske signatur og tilhørende signaturcertifikat oprettes af signaturtjenesten, efter at brugeren har accepteret at underskrive ved at autentificere sig over for signaturtjenesten[2].

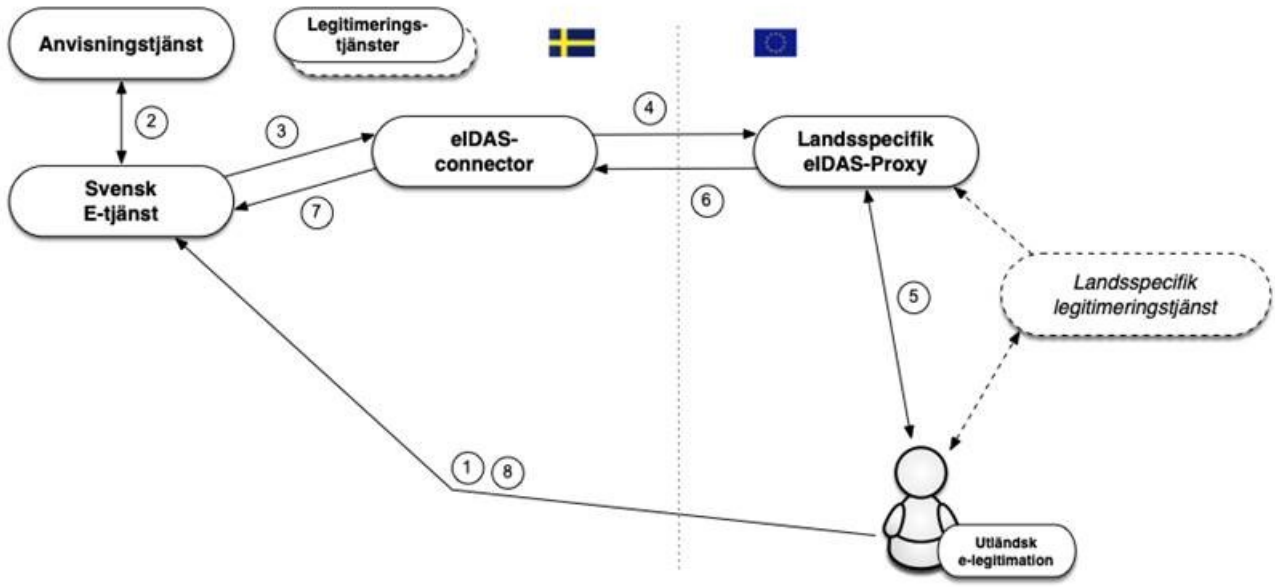
> [1]: Det er også muligt selv at implementere en signaturtjeneste baseret på specifikationerne i den tekniske ramme eller på anden måde erhverve en signaturtjeneste.
>
> [2]: Det er vigtigt at bemærke, at det er af allerstørste betydning, at brugeren opfatter denne proces som underskrivelse af et dokument. Der bør derfor anvendes et signaturflow til de eID'er, der understøtter dette i forbindelse med "autentifikation for signatur".

1.7. Teknisk ramme og eIDAS

I henhold til EU-forordning (910/2014) om elektronisk identifikation og tillidstjenester, eIDAS, skal svenske offentlige organer anerkende de eID'er, som andre eIDAS-lande har anmeldt. Det betyder, at en offentlig svensk e-tjeneste baseret på visse regler skal kunne acceptere et login udført ved hjælp af et eID udstedt i et andet land.

1.7.1. Autentifikation ved hjælp af udenlandske eID'er

De tekniske specifikationer for eIDAS er ligesom den tekniske ramme baseret på SAML-standarder, og selv om der er mange ligheder, er der også forskelle i disse specifikationer. En svensk e-tjeneste skal dog ikke forholde sig direkte til de tekniske specifikationer for eIDAS. Billedet nedenfor illustrerer, hvordan det svenske eIDAS-knudepunkt (*eIDAS-connector*) fungerer som bro mellem andre lande og den svenske føderation, når en person autentificeres ved hjælp af et udenlandsk eID mod en svensk e-tjeneste. Det svenske eIDAS-knudepunkt overholder de tekniske rammer.



Anvisningstjänst	Opdagelsestjeneste
Legitimeringstjänster	Autentifikationstjenester
Svensk E-tjänst	Svensk e-tjeneste
EiDAS-connector	eIDAS-connector
Landsspecifik Eidas Proxy	Landespecifik eIDAS-proxy
Landsspecifik legitimeringstjänst	Landespecifik autentifikationstjeneste
utländsk e-legitimation	udenlandsk eID

Flowet er som følger:

1. En bruger med et udenlandsk eID anmoder om adgang til en svensk e-tjeneste (dvs. logger ind).

2. E-tjenesten giver brugeren mulighed for at vælge loginmetoden ved hjælp af en opdagelsestjeneste. Der vises en mulighed for "udenlandsk eID", som vælges af brugeren i eIDAS-tilfældet.

3. E-tjenesten opretter en autentifikationsanmodning i overensstemmelse med denne tekniske ramme og dirigerer brugeren til det svenske eIDAS-knudepunkt (*connector*), som DIGG er ansvarlig for. eIDAS-knudepunktet fungerer som en autentifikationstjeneste (*Identity Provider*) i føderationen over for svenske modtagerparter, hvilket betyder, at kommunikationen med denne tjeneste foregår på samme måde som med andre autentifikationstjenester inden for føderationer, der overholder de tekniske rammer.

4. Den modtagne anmodning behandles, og eIDAS-knudepunktet viser en side med valgmuligheder, hvor brugeren vælger "sit land".[1] Det svenske eIDAS-knudepunkt konverterer nu den modtagne autentifikationsanmodning til en eIDAS-autentifikationsanmodning og dirigerer brugeren til det valgte lands "eIDAS-proxytjeneste".

5. Når autentifikationsanmodningen modtages af eIDAS-proxytjenesten for det valgte land, overtager dette lands autentifikationsteknologi processen. Ikke alle eIDAS-lande bruger SAML til autentifikation, men hvis dette var tilfældet i vores eksempel, ville brugeren blive omdirigeret til en autentifikationstjeneste (*Identity Provider*), og før det måske også en opdagelsestjeneste til valg af autentifikationstjenesten.

6. Når autentifikationen er udført, oprettes et certifikat (*Assertion*) i henhold til eIDAS-specifikationerne. Dette certifikat indeholder eIDAS-specifikke attributter, der identificerer brugeren. Dette certifikat sendes nu til det svenske eIDAS-knudepunkt.

7. Knudepunktet modtager certifikatet og validerer dets nøjagtighed. Dette certifikat omdannes fra eIDAS-format til et certifikat, der er formateret i overensstemmelse med den tekniske ramme, og sendes til e-tjenesten.

8. Modtagerparten tilføjer eventuelt yderligere oplysninger og afgør, om brugeren skal have adgang til tjenesten.

Svenske e-tjenester behøver således kun at understøtte den tekniske ramme for at kunne håndtere en autentifikation, der udføres ved hjælp af et europæisk eID. E-tjenesten skal dog kunne håndtere den præsenterede identitet, som ikke nødvendigvis er et personnummer. Der kan således være tilfælde, hvor en e-tjeneste autentificerer en bruger via eIDAS-rammen, men brugerens præsenterede identitet ikke kan anvendes i e-tjenesten. Mere om dette i kapitel 1.7.3 nedenfor.

> [1]: Faktisk vælger brugeren den "eIDAS-proxytjeneste", som anmodningen skal videresendes til. Dette afhænger af det land, som brugerens eID-udsteder tilhører.

1.7.2. Signaturer ved hjælp af udenlandske eID'er

Som allerede beskrevet anvendes en model for elektronisk signatur inden for denne tekniske ramme kaldet "fødereret signatur". En serverbaseret signaturtjeneste er knyttet til e-tjenesten, som igen anmoder om en signatur. Når en bruger underskriver et dokument, sender e-tjenesten en signaturanmodning til signaturtjenesten. Signaturtjenesten anmoder derefter brugeren om at autentificere sig selv. I forbindelse med autentifikationen godkender brugeren signaturen. Signaturtjenesten sender data tilbage til e-tjenesten, og derefter gemmes de signaturdata, der er knyttet til det underskrevne dokument.

Denne procedure gør det muligt også at underskrive ved hjælp af et udenlandsk eID, da signaturtjenesten kan vælge at autentificere brugeren ved hjælp af et udenlandsk eID i overensstemmelse med den procedure, der er beskrevet ovenfor i afsnit 1.7.1.

I forbindelse med signering er det svenske eIDAS-knudepunkt i dette tilfælde ansvarlig for at informere brugeren om, at formålet med autentifikationen er at signere et dokument, hvem der har anmodet om signaturen, og eventuelle oplysninger om, hvad der signeres. Et identitetscertifikat udstedes først, når brugeren har autentificeret sig selv (med henblik på signatur), og dette sendes til signaturtjenesten, som derefter genererer signaturen.

1.7.3. Forvaltning af identiteter

Identitetscertifikater fra andre lande overholder EU-dækkende tekniske specifikationer, der er udviklet inden for rammerne af eIDAS-forordningen. De attributter, som hvert land altid skal

medtage for fysiske personer og organisationer ("Minimum Dataset", MDS), er fastsat i denne forordning. Hvert land skal inkludere en unik identifikator pr. eID, der kun repræsenterer én fysisk person. Fra nogle lande vil disse identifikatorer være unikke og vedvarende pr. person på samme måde som f.eks. svenske personnumre, men disse identifikatorer kan have meget forskellige sammensætninger og karakteristika. En egenskab, der kan variere, er, hvor vedvarende en sådan identifikator er, dvs. om en sådan identifikator forbliver uændret i en persons levetid eller ændres, hvis personen f.eks. flytter til en anden region, ændrer sit navn eller blot ændrer sit eID. Fra nogle lande (f.eks. Storbritannien) vil identifikatoren variere afhængigt af, hvilket af landets eID'er en bruger i øjeblikket vælger at bruge.

For at forenkle forvaltningen af brugere i svenske e-tjenester genererer det svenske eIDAS-knudepunkt en standardiseret ID-attribut for brugere, der er blevet autentificeret ved hjælp af udenlandske eID'er, et såkaldt *provisional ID* (forkortet PRID). Desuden oprettes en tilknyttet attribut, der angiver den forventede persistens eller levetid for denne ID-attribut. PRID-attributten genereres på grundlag af attributværdierne fra den udenlandske autentifikation i henhold til bestemte metoder for det pågældende land. Hver kombination af land og metode kategoriseres efter forventet persistens, dvs. hvor sandsynligt det er, at en identitet ændrer sig over tid for den samme person. Dette gør det muligt for svenske e-tjenester at tilpasse kommunikationen med brugeren og proaktivt levere funktioner, der gør det lettere for en bruger, hvis identitet er ændret, at genvinde kontrollen over sine oplysninger i e-tjenesten.

I nogle tilfælde kan en person, der er autentificeret ved hjælp af et udenlandsk eID, også have et svensk personnummer. Det kan f.eks. være en svensk statsborger, der er flyttet til udlandet og har fået et udenlandsk eID, eller en udenlandsk statsborger, der er registreret i Sverige og har fået tildelt et personnummer.

Det forhold, at en person med et udenlandsk eID har et svensk personnummer, er normalt ikke kendt af den udenlandske autentifikationstjeneste, og denne information er derfor ikke medtaget i identitetcertifikatet fra det land, hvor personen autentificeres. Det svenske knudepunkt har på den anden side mulighed for at forespørge en attributtjeneste i Sverige[1] om, hvorvidt der findes et registreret personnummer for den autentificerede person, og kan, hvis dette er tilfældet, tilføje sådanne oplysninger til det identitetscertifikat, der sendes til e-tjenesten.

> [1]: I skrivende stund er der ingen attributtjeneste, der etablerer en forbindelse mellem eIDAS-identiteter og svenske personnumre.

1.7.4. Svenske eID'er i udenlandske e-tjenester

Sverige har anmeldt svenske eID'er på tillidsniveauerne betydeligt (substantial) og højt (high) i henhold til eIDAS.

En anmodning om autentifikation fra en udenlandsk e-tjeneste indgives til det svenske eIDAS-knudepunkt (proxytjeneste) via en eIDAS-connector i e-tjenestens land. I det svenske eIDAS-knudepunkt vælger brugeren, hvilket svensk eID vedkommende ønsker at autentificere sig med, hvorefter der sendes en autentifikationsanmodning til autentifikationstjenesten (*Identity Provider*), der håndterer det valgte eID. Denne anmodning er formateret i henhold til en teknisk ramme, hvilket betyder, at en svensk autentifikationstjeneste ikke behøver at overholde eIDAS' tekniske specifikationer.

Brugeren autentificeres af den svenske autentifikationstjeneste, og der udstedes et identitetscertifikat (i henhold til den tekniske ramme). Dette certifikat modtages af den svenske eIDAS-proxytjeneste og konverteres til et certifikat i henhold til eIDAS-specifikationerne, inden det videresendes til den udenlandske eIDAS-connector og derefter til den kaldende e-tjeneste (*Service Provider*).

2. Tekniske specifikationer

Dette kapitel indeholder specifikationer og profiler for identitetsføderationer, der overholder den tekniske ramme for Sweden Connect, og visse relaterede tjenester. Medmindre andet er angivet, er disse dokumenter præskriptive for levering af tjenester inden for identitetsføderationer, der implementerer den tekniske ramme.

2.1. Profiler og specifikationer for SAML

Identitetsføderationer, der overholder den tekniske ramme for Sweden Connect, er bygget op omkring "Deployment Profile for the Swedish eID Framework", [SAML.Profile]. Denne profil påvirkes af, men er ikke præskriptivt afhængig af, "SAML V2.0 Deployment Profile for Federation Interoperability" [SAML2Int]. [SAML.Profile] indeholder også regler og retningslinjer, der er specifikke for de tekniske rammer for Sweden Connect.

2.1.1. Deployment Profile for the Swedish eID Framework

"Deployment Profile for the Swedish eID Framework" [SAML.Profile] er det vigtigste tekniske rammedokument og præciserer bl.a.:

- hvordan SAML-metadata skal bygges op og fortolkes
- hvordan autentifikationsanmodningen skal formateres
- hvordan en anmodning om autentifikation skal håndteres, og hvordan et identitetscertifikat skal udformes, verificeres og håndteres
- sikkerhedskrav
- specifikke SAML-krav til signaturtjenester og "autentifikation for signatur".

2.1.2. Swedish eID Framework – Registry for identifiers

Gennemførelsen af en svensk eID-infrastruktur kræver forskellige former for identifikatorer for at repræsentere objekter i datastrukturer. Dokumentet "Sweden Connect - Registry for identifiers", [SC.Registry], definerer strukturen af de identifikatorer, der tildeles inden for den tekniske ramme, samt et register over definerede identifikatorer.

2.1.3. Attribute Specification for the Swedish eID Framework

Specifikationen "Attribute Specification for the Swedish eID Framework", [SAML.Attributes], erklærer de SAML-attributprofiler, der anvendes inden for

identitetsføderationer, som overholder den tekniske ramme, inklusive dem der forbinder til eIDAS via det svenske eIDAS-knudepunkt.

2.1.4. Entity Categories for the Swedish eID Framework

Enhedskategorier (Entity Categories) anvendes inden for føderationen til en række forskellige formål:

- Service Entity Categories — anvendes i metadata til at repræsentere e-tjenesters krav til tillidsniveauer og anmodede attributter samt autentifikationstjenesters opfyldelse af tillidsniveauer og levering af attributter.
- Service Property Categories — bruges til at repræsentere en specifik egenskab ved en tjeneste.
- Service Type Entity Categories — anvendes til at repræsentere forskellige tjenestetyper inden for føderationen.
- Service Contract Entity Categories — anvendes af tjenester til at annoncere aftaleformularer og lignende.
- General Entity Categories — enhedskategorier, der ikke falder ind under nogen af ovennævnte typer.

Specifikationen "Entity Categories for the Swedish eID Framework" [SAML.EntCat] specificerer de enhedskategorier, der er defineret af den tekniske ramme, og beskriver deres betydning.

2.1.5. eIDAS Constructed Attributes Specification for the Swedish eID Framework

Specifikationen "eIDAS Constructed Attributes Specification for the Swedish eID Framework", [SC.eIDAS.Attrs], angiver processer og regler for, hvordan ID-attributter konstrueres baseret på attributter modtaget under autentifikation i eIDAS.

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

Specifikationen "Implementation Profile for BankID Identity Providers within the Swedish eID Framework", [SAML.BankID], definerer regler for, hvordan en autentifikationstjeneste, der implementerer support for BankID, skal være udformet.

> **Bemærk venligst følgende:** Denne specifikation er ikke præskriptiv for opfyldelse af en teknisk ramme. Det er kun relevant for autentifikationstjenester, der implementerer støtte til BankID samt e-tjenester, der bruger disse. Autentifikationstjenester, der implementerer understøttelse af BankID og ønsker at tilslutte sig Sweden Connect-føderationen, skal dog opfylde denne specifikation.

2.1.7. Principal Selection in SAML Authentication Requests

Specifikationen "Principal Selection in SAML Authentication Requests", [SAML.Principal], definerer en udvidelse til SAML, der gør det muligt for en modtagerpart at informere en autentifikationstjeneste om, hvilken identitet den ønsker autentificeret.

2.1.8. User Message Extension in SAML Authentication Requests

Specifikationen "User Message Extension in SAML Authentication Requests", [SAML.UMessage], definerer en udvidelse til SAML, der gør det muligt for en modtagerpart at medtage en visningsmeddelelse i den autentifikationsanmodning, der sendes til autentifikationstjenesten. Autentifikationstjenesten kan derefter vise denne meddelelse til brugeren under autentifikationstrinnet.

2.2. Profiler og specifikationer for OpenID Connect

2.2.1. OpenID Connect Profile for Sweden Connect

Profilen "OpenID Connect Profile for Sweden Connect", [OIDC.Profile], bygger videre på The Swedish OpenID Connect Profile, som er en OpenID Connect-profil udviklet af OIDC Sweden for at fremme interoperabilitet og sikkerhed inden for svenske OIDC-løsninger.

[OIDC.Profile] tilføjer yderligere krav vedrørende Sweden Connect-føderationen.

2.2.2. OpenID Connect Claims and Scopes Specification for Sweden Connect

Specifikationen "OpenID Connect Claims and Scopes Specification for Sweden Connect", [OIDC.Claims], bygger videre på specifikationen Claims and Scopes Specification for the Swedish OpenID Connect Profile fra OIDC Sweden.

2.3. Specifikationer for signatur

Dette afsnit indeholder henvisninger til de dokumenter, der definerer signaturtjenester inden for føderationer, der overholder Sweden Connects tekniske rammer.

2.3.1. Implementation Profile for using OASIS DSS in Central Signing Services

Implementeringsprofilen "Implementation Profile for Using OASIS DSS in Central Signing Services", [Sign.DSS.Profile], specificerer en profil for signaturanmodningen og respons i henhold til OASIS-standarden "Digital Signature Service Core Protocols, Elements, and Bindings" [DSS].

2.3.2. DSS Extension for Federated Central Signing Services

"DSS Extension for Federated Central Signing Services", [Sign.DSS.Ext], er en udvidelse af OASIS-standarden "Digital Signature Service Core Protocols, Elements, and Bindings" [DSS], som specificerer definitioner, der er nødvendige for signering inden for den tekniske ramme.

2.3.3. Certificate Profile for Certificates Issued by Central Signing Services

Certifikatprofilen "Certificate profile for certificates issued by Central Signing services", [Sign.Cert.Profile], specificerer indholdet af signaturcertifikater. Denne profil anvender en ny certifikatudvidelse til at understøtte signaturtjenester.

Denne profil henviser til "Authentication Context Certificate Extension", [AuthContext], som beskriver, hvordan "Authentication Context" er repræsenteret i X.509-certifikater.

2.3.4. Signature Activation Protocol for Federated Signing

Specifikationen "Signature Activation Protocol for Federated Signing", [Sign.Activation], definerer en "Signature Activation Protocol" (SAP) til gennemførelse af "Sole Control Assurance Level 2" (SCAL2) i henhold til standarden "prEN 419241 – Trustworthy Systems Supporting Server Signing".

3. Referenceliste

3.1. DIGG

[Digg.Tillit]

Tillidsramme for svensk e-identifikation.

[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. Andre referencer

[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.