

Tekniskt ramverk för Svensk e-legitimation

ELN-0600-v1.5
Version: 1.5
2016-08-30

Utkast



1	INTRODUKTION	3
1.1	IDENTITETSFEDERATIONER FÖR SVENSK E-LEGITIMATION	3
1.2	TILLITSRAMVERK OCH SÄKERHETSNIVÅER	4
1.3	TJÄNST FÖR INSAMLING, ADMINISTRATION OCH PUBLICERING AV METADATA	4
1.3.1	TILLIT OCH METADATA	5
1.4	ANVISNINGSTJÄNST	5
1.5	UTFÄRDARE AV E-LEGITIMATION OCH UTFÄRDARE AV IDENTITETSINTYG	5
1.6	INTEGRATION I E-TJÄNSTER	5
1.7	UNDERSKRIFT	6
1.8	TEKNISKT RAMVERK OCH EIDAS	6
1.8.1	AUTENTISERINGAR MED UTLÄNDSKA E-LEGITIMATIONER	6
1.8.2	UNDERSKRIFTER MED UTLÄNDSKA E-LEGITIMATIONER	7
1.8.3	HANTERING AV IDENTITETER	8
1.8.4	SVENSKA E-LEGITIMATIONER ANVÄNDS I UTLÄNDSKA E-TJÄNSTER	8
2	TEKNISKA SPECIFIKATIONER	9
2.1	SAML-PROFILER	9
2.1.1	SPECIFIKATIONER FÖR ANVISNING (DISCOVERY)	9
2.2	SPECIFIKATIONER FÖR IDENTITETSFEDERATIONER FÖR SVENSK E-LEGITIMATION	9
2.2.1	REGISTER FÖR IDENTIFIERARE DEFINIERADE AV E-LEGITIMATIONSNÄMNDEN	9
2.2.2	ATTRIBUTSPECIFIKATION	9
2.2.3	SPECIFIKATIONER AV ENTITETSKATEGORIER	9
2.3	SPECIFIKATIONER FÖR UNDERSKRIFTSTJÄNST	10
3	REFERENSLISTA	11
3.1	E-LEGITIMATIONSNÄMNDEN	11
3.2	ÖVRIGA REFERENSER	11
4	ÄNDRINGAR MELLAN VERSIONER	12

1 Introduktion

1.1 Identitetsfederationer för Svensk e-legitimation

Det tekniska ramverket för Svensk e-legitimation är anpassat för särskilda s.k. identitetsfederationer som baseras på standardprotokollet SAML 2.0 och Svensk e-legitimation (identitetsfederationer för Svensk e-legitimation).

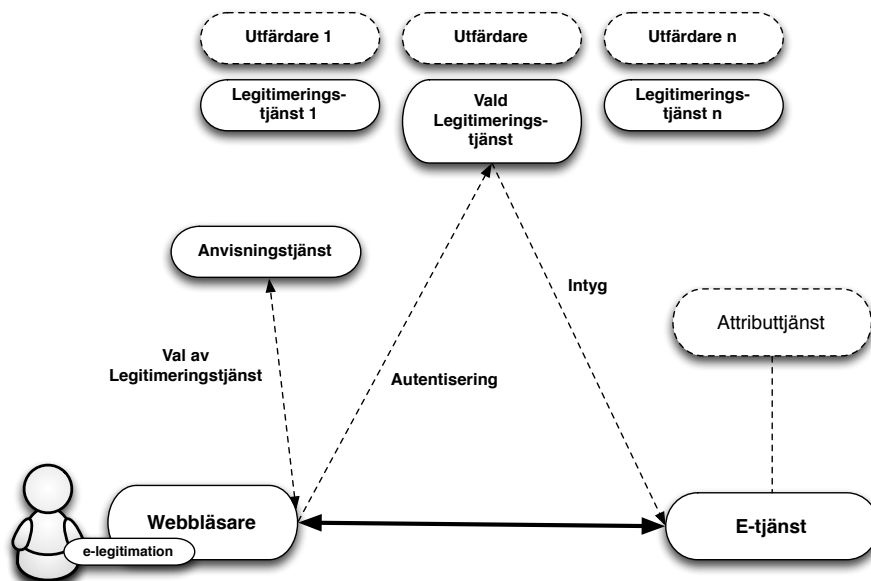
Den största skillnaden i förhållande till tidigare lösningar för elektronisk legitimering är att e-tjänster inte kommer i direkt kontakt med användarnas e-legitimationer utan istället får ett identitetsintyg i ett standardiserat format från en legitimeringstjänst. Legitimeringstjänsterna tillhandahålls av godkända leverantörer av eID-tjänster vars tjänster i sin tur bygger på godkända utfärdare av Svensk e-legitimation.

Det innebär att e-tjänster som kräver underskrift inte längre behöver anpassas efter olika användares e-legitimationer för att skapa elektroniska underskrifter. Istället kan e-tjänsten överlåta detta till en underskriftstjänst där användare med stöd av Svensk e-legitimation ges möjlighet att underteckna elektroniska handlingar.

Inom infrastrukturen för Svensk e-legitimation intar e-tjänster rollen som Service Provider (SP) medan legitimeringstjänster som utfärdar identitetsintyg intar rollen som Identity Provider (IdP) och därmed den som autentiserar användaren, oavsett mot vilken e-tjänst som användaren legitimerar sig. Anvisningstjänstens, Discovery Service (DS), uppgift är att avlasta de enskilda e-tjänsterna inom federationen från att själva implementera stöd för hur användaren väljer legitimeringstjänst.

För de fall där e-tjänsten behöver mer information om användaren t ex. uppgift om juridisk behörighet, kan en fråga ställas till en attributtjänst, Attribute Authority (AA). Genom en attributsförfrågan kan e-tjänsten erhålla nödvändig kompletterande information.

Då såväl identitetsuppgifter som andra attribut kopplat till användare tillhandahålls genom identitetsintyg och attributsintyg, kan alla typer av e-legitimationer som uppfyller kraven för Svensk e-legitimation användas för legitimering mot en e-tjänst som kräver såväl personnummer som ytterligare information om juridisk behörighet, även om e-legitimationen inte innehåller några specifika personuppgifter (t.ex. koddosor för generering av engångslösenord).



Figur 1: Illustration av kommunikationen mellan de olika tjänsterna inom en identitetsfederation för Svensk e-legitimation.

1.2 Tillitsramverk och säkerhetsnivåer

Grunden för vilken säkerhetsnivå som tillämpas när en användare legitimerar sig är den tillitsnivå som e-tjänsten kräver. För att dessa säkerhetsnivåer ska kunna vara jämförbara inom ramen för federationen definieras fyra tillitsnivåer i Tillitsramverket för Svensk e-legitimation [EidTillit]. Alla som utfärdar identitetsintyg måste visa att hela den process som ligger till grund för utfärdandet av identitetsintyg uppfyller kraven i den efterfrågade tillitsnivån, detta innefattar bl.a.

- Krav på skapandet av identitetsintyget.
- Krav på utfärdandeprocessen.
- Krav på själva e-legitimationen och dess användning.
- Krav på utfärdaren av e-legitimationen.
- Krav på fastställande av sökandens identitet.

1.3 Tjänst för insamling, administration och publicering av Metadata

En SAML 2.0-federation kan tillhandahålla information om federationens deltagare genom s.k. metadata. Som deltagare i en federation räknas såväl aktörer som levererar legitimerings- och attributtjänster i federationen som aktörer som konsumerar dessa tjänster t ex. e-tjänster.

Genom federationens metadata kan deltagare inhämta information om andra deltagares tjänster, inkl. de uppgifter som krävs för ett säkert informationsutbyte mellan deltagarna.

Metadata utgör en gemensam informationsmängd i en federation genom vilken deltagande aktörer kan erhålla efterfrågad information. Det viktigaste syftet med metadata är att tillhandahålla de nycklar som krävs för säker kommunikation och informationsutväxling mellan tjänster. Utöver nycklar innehåller metadata även annan information som är viktig för samverkan mellan tjänster t ex. Internetadresser till funktioner som krävs, information om tillitsnivåer, tjänstekategorier, användargränssnittsinformation mm.



1.3.1 Tillit och metadata

Identitetsfederationer för Svensk e-legitimation förutsätter att legitimeringstjänster och e-tjänster litar på varandra och därmed kan verifiera de signaturer som används i kommunikationen dem emellan. Rent tekniskt baseras denna tillit på att respektive aktörer litar på varandras signeringscertifikat.

En identitetsfederation definieras av ett register i XML-format som är signerat med federationsoperatörens certifikat. Filen innehåller information om identitetsfederationens medlemmar inklusive deras certifikat. Eftersom filen med metadata är signerad räcker det med att jämföra ett certifikat med dess motsvarighet i metadata. En infrastruktur baserad på ett centralt federationsregister förutsätter att registret uppdateras kontinuerligt samt att federationsmedlemmarna alltid använder den senaste versionen av filen.

1.4 Anvisningstjänst

En anvisningstjänst har som sitt syfte att avlasta de enskilda e-tjänsterna inom en identitetsfederation från att själva implementera stöd för hur användare väljer legitimeringstjänst.

Genom att anvisningstjänsten finns tillgänglig inom identitetsfederationen kan e-tjänster styra sina användare dit för val av legitimeringstjänst. Anvisningstjänsten interagerar med användaren som gör sitt val och användaren, tillsammans med dennes val, styrs tillbaka till e-tjänsten som nu vet till vilken legitimeringstjänst användaren ska skickas för legitimering.

Logik från anvisningstjänsten kan också integreras lokalt hos en e-tjänst för en tätare integration med e-tjänstens webbtjänst.

1.5 Utfärdare av e-legitimation och utfärdare av identitetsintyg

Varje typ av e-legitimation från en specifik utfärdare måste kopplas till ett namn på e-legitimationen som användaren känner igen och kan relatera till i det gränssnitt för val av e-legitimationer som skapas i samverkan med infrastrukturens anvisningstjänst. Detta namn återfinns även i identitetsfederationens metadata för respektive leverantör av eID-tjänst. Det är dessa metadata som utgör grunden för att såväl skapa gränssnitt för användare vid val som att koppla användarens val till en viss leverantör av eID-tjänst.

För att garantera att varje typ av e-legitimation representeras av ett för användaren begripligt namn och att detta endast kopplas samman med en leverantör av eID-tjänst, är utfärdaren av e-legitimationen ansvarig för definition av namn för dennes olika typer av e-legitimationer samt att specificera en och endast en godkänd leverantör av eID-tjänst för varje typ e-legitimation.

1.6 Integration i e-tjänster

E-tjänster integrerar mot legitimeringstjänster genom standardiserade meddelanden och konsumerar identitetsintyg vilka också har standardiserade format.

Ramverket för Svensk e-legitimation bygger på interoperabilitetsprofilen ” SAML2int profile – SAML 2.0 Interoperability Profile” [[SAML2int](#)]. Denna profil stöds av ett flertal kommersiella produkter och Open Source-lösningar, vilket underlättar integrationsarbetet hos e-tjänster.

Många e-tjänster har redan fristående autentiseringslösningar vilket innebär att en integration för att stödja Ramverket för Svensk e-legitimation påverkar en begränsad del av e-tjänstens IT-system.

1.7 Underskrift

Vid underskrift inom infrastrukturen för Svensk e-legitimation blir det möjligt att använda olika typer e-legitimationer dvs. även sådana e-legitimationer som inte är certifikatbaserade, utan speciella anpassningar i e-tjänsten. Detta därför att det inom infrastrukturen för Svensk e-legitimation är det elektroniskt utställda identitetsintyget som används för identifiering av användare vid underskrift och identitetsintyget har samma format oavsett vilken typ av e-legitimation som användaren använder.

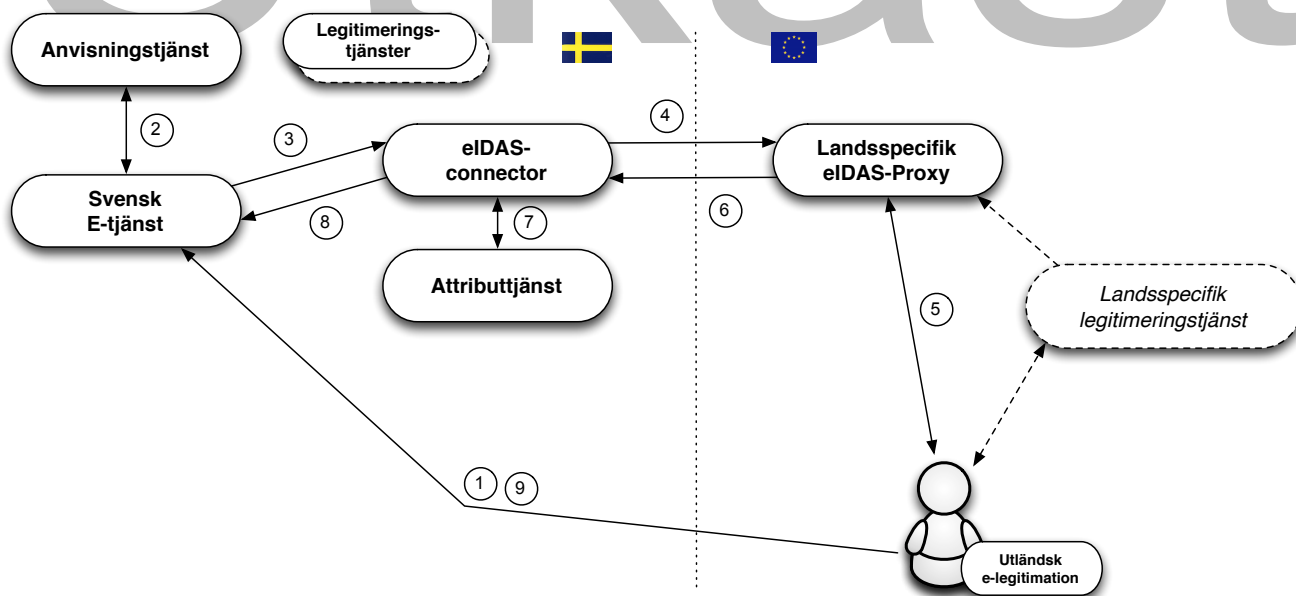
En underskriftstjänst har som syfte att möjliggöra underskrift inom identitetsfederationer för Svensk e-legitimation med stöd av alla typer av e-legitimationer som erbjuder tillräcklig grad av säkerhet. Genom att införa en underskriftstjänst som ansluts till e-tjänster som ingår i identitetsfederationen kan en e-tjänst låta en användare skriva under en elektronisk handling med stöd av underskriftstjänsten. Användarens elektroniska signatur och tillhörande signeringscertifikat skapas av underskriftstjänsten efter det att användaren accepterat att skriva under genom att legitimera sig mot underskriftstjänsten.

1.8 Tekniskt ramverk och eIDAS

EU-förordningen (910/2014) om elektronisk identifiering och betrodda tjänster, eIDAS, ställer krav på svenska offentliga organ att erkänna de e-legitimationer som andra eIDAS-länder har anmält. Detta innebär att en offentlig svensk e-tjänst skall kunna acceptera en inloggning som utförs med en e-legitimation utställd i ett annat europeiskt land.

1.8.1 Autentiseringar med utländska e-legitimationer

De tekniska specifikationerna för eIDAS bygger, såsom tekniskt ramverk för Svensk e-legitimation, på SAML-standarder, och även om likheterna är många finns även skillnader i dessa specifikationer. Dock behöver en svensk e-tjänst inte direkt förhålla sig till eIDAS tekniska specifikationer. Nedanstående bild illustrerar hur en s.k. eIDAS-connector agerar som en brygga mellan eIDAS-federationen och en svensk federation då en person autentiseras med en utländsk e-legitimation mot en svensk e-tjänst.



Flödet är enligt följande:

1. En användare med en utländsk e-legitimation begär åtkomst till en svensk e-tjänst (d.v.s., loggar in).



2. E-tjänsten utför anvisning (val av inloggningssätt), t.ex., genom att styra användaren till federationens anvisningstjänst. Ett val för "internationell inloggning" visas upp, vilket användaren i detta fall väljer.
3. E-tjänsten skapar en legitimeringsbegäran enligt tekniskt ramverk för Svensk e-legitimation och styr användaren till den svenska eIDAS-noden (connector). Denna "connector" uppträder som en legitimeringstjänst (Identity Provider) i federationen vilket innebär att kommunikation med denna tjänst utförs på samma sätt som mot övriga legitimeringstjänster inom federationen.
4. Den mottagna begäran behandlas och eIDAS-noden visar upp en valsida där användaren väljer "sitt land"¹. Den svenska eIDAS-noden omvandlar nu den mottagna legitimeringsbegäran till en legitimeringsbegäran enligt eIDAS och användaren styrs till det valda landets "eIDAS Proxy-tjänst".
5. Då legitimeringsbegäran mottas av den eIDAS-Proxy-tjänst för valt land tar detta lands teknik för autentisering över. Inte alla länder inom eIDAS använder SAML för autentisering, men om så var fallet i vårt exempel skulle användaren styras vidare till en legitimeringstjänst (Identity Provider), och innan dess kanske även en anvisningstjänst för val av legitimeringstjänst.
6. Då en autentisering utförts skapas ett intyg (Assertion) enligt eIDAS specifikationer. Detta intyg innehåller bl.a. eIDAS-specifika attribut som identifierar användaren.
7. Detta intyg styrs nu vidare till frågande part, som är den svenska eIDAS-noden. Denna nod tar emot intyget och validerar dess korrekthet. I samband med att intyget transformeras från eIDAS-format till ett intyg som uppfyller tekniskt ramverk för Svensk e-legitimation anropas också en attributtjänst för att, om möjligt, givet eIDAS-attribut erhålla attribut som stöds av den svenska e-tjänsten (t.ex. slå upp ett svenskt person- eller samordningsnummer givet ett eIDAS *PersonIdentifier*-attribut).
8. Slutligen postas ett intyg, på ett format som uppfyller tekniskt ramverk för Svensk e-legitimation, till e-tjänsten.
9. Användaren ges till åtkomst till tjänsten.

Svenska e-tjänster behöver således endast stödja tekniskt ramverk för Svensk e-legitimation för att kunna hantera en autentisering utförd med en europeisk e-legitimation. Dock måste e-tjänsten kunna hantera den identitet som presenteras, vilket inte nödvändigtvis är ett personnummer eller samordningsnummer. Det kan alltså hända att en e-tjänst autentiserar en användare via eIDAS-ramverket, men att användarens presenterade identitet inte går att använda hos e-tjänsten. Mer om detta i kapitlet 1.8.3 nedan.

1.8.2 Underskrifter med utländska e-legitimationer

Inom ramen för det tekniska ramverket för Svensk e-legitimation tillämpas en modell för elektronisk underskrift som kallas federerad underskrift. Denna modell utgörs av en serverbaserad underskriftstjänst som är knuten till e-tjänsten som begär underskrift. När en användare skriver under ett dokument så överförs användaren till underskriftstjänsten med en underskriftsbegäran utställd av e-tjänsten. Underskriftstjänsten begär därefter att användaren legitimerar sig samt i samband med detta godkänner underskriften.

Detta förfarande möjliggör att skriva under även med utländsk e-legitimation då underskriftstjänsten kan välja att legitimera användaren med utländsk e-legitimation i enlighet med förfarandet som beskrivs ovan i avsnitt 1.8.1.

Vid underskrift ansvarar den svenska eIDAS-noden för att användaren upplyses om att syftet med legitimeringen är att skriva under ett dokument, vem som begärt underskrift samt eventuell information om vad som undertecknas. Först när användaren accepterat att skriva under utfärdas ett identitetsintyg som skickas till underskriftstjänsten som genererar underskriften.

I likhet med legitimering med utländsk e-legitimation så innebär underskrift med utländsk e-legitimation att användarens identitet kan utgöras av andra attribut än de som tillhandahålls av en svensk legitimeringstjänst.

¹ Egentligen väljer användaren till vilken "eIDAS Proxy-tjänst" som begäran ska skickas vidare till. Detta är beroende landstillhörigheten för användarens e-legitimationsutfärdare.



1.8.3 Hantering av identiteter

Identitetsintyg från andra länders eIDAS-noder följer EU-gemensamma tekniska specifikationer framtagna inom ramen för eIDAS regleringen. Här specificeras de attribut som varje land alltid måste skicka med för fysiska personer såväl som för organisationer. Varje land måste skicka med en unik identifierare för fysiska personer men även om dessa är unika för varje användare inom respektive land så kan dessa identifierare ha vitt skilda sammansättningar och ha väldigt olika egenskaper. En egenskap som kan variera är hur persistent en sådan identifierare är, d.v.s, om en sådan identifierare är oförändrad under en persons livstid eller om den ändras om personen exempelvis flyttar till en annan region, byter namn eller bara byter e-legitimation.

För att förenkla hanteringen av användare i svenska e-tjänster så genererar den svenska eIDAS-noden ett standardiserat ID-attribut för användare som legitimerats med utländsk e-legitimation, ett s.k. *provisional ID* (förkortat PRID). Dessutom skapas ett tillhörande attribut som deklarerar vilken förväntad persistens, eller livslängd, detta ID-attribut har. PRID-attributet genereras utifrån de attributvärden som erhålls från den utländska legitimeringen enligt specificerade metoder för respektive land. Varje kombination av land och metod klassas med avseende på förväntad persistens, d.v.s, hur sannolikt det är att en identitet ändras över tiden för samma person. Detta gör det möjligt för svenska e-tjänster att anpassa kommunikationen med användaren och proaktivt tillhandahålla funktioner som underlättar för en användare vars identitet har ändrats, att återfå kontrollen över sin information i e-tjänsten.

I vissa fall kan en person som legitimeras med en utländsk e-legitimation även inneha ett svenskt personnummer eller ett styrkt svenskt samordningsnummer. Det kan till exempel röra sig om en svensk medborgare som flyttat utomlands och skaffat utländsk e-legitimation eller en utländsk medborgare som har sådan anknytning till svenska myndigheter att denne tilldelats ett styrkt samordningsnummer.

Det faktum att en person med utländsk e-legitimation innehar ett svenskt personnummer eller samordningsnummer är normalt sett inte känt för den utländska legitimeringstjänsten och denna information ingår därför inte i identitetsintyg från landet där personen legitimeras. Den svenska noden har däremot möjlighet att fråga en attributtjänst i Sverige om det finns ett registrerat personnummer eller samordningsnummer för den legitimerade personen och kan, om så är fallet, påföra sådan information i det identitetsintyg som skickas till e-tjänsten.

1.8.4 Svenska e-legitimationer används i utländska e-tjänster

Kommer att kompletteras.

2 Tekniska specifikationer

Detta kapitel innehåller specifikationer och profiler för identitetsfederationer för Svensk e-legitimation och vissa kringliggande tjänster. Där inget annat nämns är dessa dokument normativa för leverans av tjänster inom identitetsfederationen för Svensk e-legitimation.

2.1 SAML-profiler

Identitetsfederationer för Svensk e-legitimation är uppbyggda kring följande SAML-profiler:

- Implementationsprofil – "Kantara Initiative eGovernment Implementation Profile of SAML 2.0" [[eGov2](#)].
- Deploymentprofil – E-legitimationsnämndens "Deployment Profile for the Swedish eID Framework" [EidProfile]. Denna profil utgår från "SAML2int profile – SAML 2.0 Interoperability Profile" [[SAML2Int](#)].

2.1.1 Specifikationer för anvisning (Discovery)

Anvisning (Discovery) enligt "OASIS Committee Specification, Identity Provider Discovery Service Protocol and Profile" [[IdpDisco](#)] stöds av ramverket för Svensk e-legitimation. Denna specifikation utökas av [EidProfile].

Identitetsfederationer för Svensk e-legitimation stödjer också tekniker för lokalt integrerad anvisning vilket beskrivs i dokumentet "Discovery within the Swedish eID Framework" [EidDiscovery].

2.2 Specifikationer för identitetsfederationer för Svensk e-legitimation

2.2.1 Register för identifierare definierade av E-legitimationsnämnden

Implementering av en infrastruktur för Svensk e-legitimation kräver olika former av identifierare för att representera objekt i datastrukturer. Dokumentet "Registry for identifiers assigned by the Swedish e-identification board" [EidRegistry] definierar strukturen för identifierare som tilldelats av E-legitimationsnämnden, samt ett register över definierade identifierare.

2.2.2 Attributspecifikation

Dokumentet "Attribute Specification for the Swedish eID Framework" [EidAttributes] deklarerar de SAML attributprofiler som används inom identitetsfederationer för Svensk e-legitimation samt anslutande till eIDAS-federationen via svensk eIDAS-nod.

Dokumentet "eIDAS Constructed Attributes Specification for the Swedish eID Framework" [EidConstrAttributes] specificerar processer och regler för hur ID-attribut konstrueras baserat på attribut som tas emot vid legitimering mot eIDAS.

2.2.3 Specifikationer av entitetskategorier

Entitetskategorier (Entity Categories) används inom federationen för tre syften:

- Service Entity Categories – Används i federationens metadata för att representera e-tjänsters krav på tillitsnivåer och begärda attribut, samt legitimeringstjänsters uppfyllande av tillitsnivåer och leverans av attribut.
- Service Property Categories – Används för att representera en viss egenskap hos en tjänst.

- Service Type Entity Categories – Används för att representera olika tjänstetyper inom federationen.

Dokumentet "Entity Categories for the Swedish eID Framework" [EidEntCat] specificerar de entitetskategorier som definieras av E-legitimationsnämnden och beskriver dess betydelse.

2.3 Specifikationer för Underskriftstjänst

Detta stycke innehåller referenser till de dokument vilka definierar underskriftstjänster inom infrastrukturen för Svensk e-legitimation.

Implementationsprofilen "Implementation Profile for Using OASIS DSS in Central Signing Services" [EidDSSProfile] specificerar en profil för underskriftsbegäran och respons enligt OASIS standarden "Digital Signature Service Core Protocols, Elements, and Bindings" [DSS], och utökar denna med definitioner specificerade i "DSS Extension for Federated Central Signing Services" [EidDSSExt].

Vidare definieras en certifikatprofil "Certificate profile for certificates issued by Central Signing services" [EidCertProf] som specificerar innehåll i signeringscertifikat. Denna profil tillämpar en ny certifikatextension till stöd för signeringstjänsten, Authentication Context Certificate Extension [AuthContext], vilken beskriver hur "Authentication Context" representeras i X.509 certifikat.

Utkast

3 Referenslista

3.1 E-legitimationsnämnden

[EidTillit]

Tillitsramverk för Svensk E-legitimation.

[EidProfile]

Deployment Profile for the Swedish eID Framework.

[EidRegistry]

Registry for identifiers assigned by the Swedish e-identification board.

[EidAttributes]

Attribute Specification for the Swedish eID Framework.

[EidConstrAttributes]

eIDAS Constructed Attributes Specification for the Swedish eID Framework.

[EidEntCat]

Entity Categories for the Swedish eID Framework.

[EidDiscovery]

Discovery within the Swedish eID Framework.

[EidDSSProfile]

Implementation Profile for Using OASIS DSS in Central Signing Services.

[EidDSSExt]

DSS Extension for Federated Central Signing Services.

[EidCertProf]

Certificate profile for certificates issued by Central Signing services.

3.2 Övriga referenser

[eGov2]

[Kantara Initiative eGovernment Implementation Profile of SAML 2.0, Version 2.0, June 11, 2010.](#)

[SAML2Int]

[SAML2int profile v0.2.1 – SAML 2.0 Interoperability Profile.](#)

[IdpDisco]

[OASIS Committee Specification, Identity Provider Discovery Service Protocol and Profile, March 2008.](#)

[DSS]

[OASIS Standard – Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0, April 11, 2007.](#)

[AuthContext]

[Authentication Context Certificate Extension Draft 08, February 13, 2015.](#)

4 Ändringar mellan versioner

Ändringar mellan version 1.4 och version 1.5:

- Tillägg som beskriver Svensk e-legitimation och eIDAS (1.8).

Ändringar mellan version 1.3 och version 1.4:

- Tekniskt ramverk för Svensk e-legitimation bygger nu på en nyare version av "SAML2int Deployment Profile" (se <http://saml2int.org/profile/current/>).
- Specifikationen "Authentication Context Classes for Levels of Assurance for the Swedish eID Framework" är inte längre del av tekniskt ramverk för Svensk e-legitimation. Dess tidigare syfte har ersatts med användande av attribut (som definieras i [EidAttributes] och [EidProfile]). I detta dokument utgår det tidigare kapitlet 2.2.3, "Identifierare och schema för representation av tillitsnivåer".
- Specifikationen [EidDSSExt] vars tidigare namn var "Eid2 DSS Extension for SAML based Central Signing service" heter nu "DSS Extension for Federated Central Signing Services".

Ändringar mellan version 1.2 och version 1.3:

- Tagit bort avsnittet *Integrering med verksamhetsspecifika federationer* (flyttas till vägledningar).

Ändringar mellan version 1.1 och version 1.2:

- Genomgång av referenslistan. I övrigt inga förändringar.

Ändringar mellan version 1.0 och version 1.1:

- Förtydliganden kring användande av entitetskategorier.
- Tillägg av specifikationer för Underskriftstjänst.