Tekniskt ramverk för Svensk e-legitimation

ELN-0600-v1.4
Version: 1.4
2015-10-05

www.elegnamnden.se

Postadress	Besöksadress	Telefon växel	E-postadress
171 94 SOLNA	Korta gatan 10	010-574 21 00	kansliet@elegnamnden.se

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).

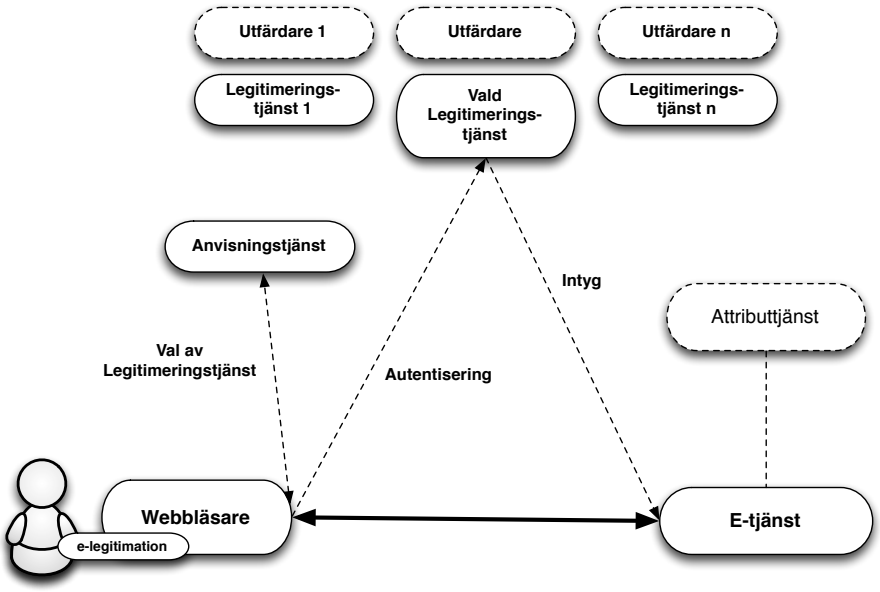
Den största skillnaden i förhållande till tidigare lösningar för elektronisk legitimering är att e-tjänster inte kommer i direkt kontakt med användarnas e-legitimationer utan istället får ett identitetsintyg i ett standardiserat format från en legitimeringstjänst. Legitimeringstjänsterna tillhandahålls 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 i 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-tjänstför 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.

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.

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.

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.

[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 1.3 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.