O introducere în cadrul tehnic Sweden Connect

4.12.2024

Număr de referință: **2019-267**

Cuprins

1. Introducere

1.1. Prezentare generală

Cadrul tehnic Sweden Connect este adaptat pentru federațiile de identitate bazate pe SAML 2.0.

În cea mai recentă versiune a cadrului tehnic, au fost introduse, de asemenea, specificații pentru OpenID Connect. În prezent, nu există suport federativ pentru OpenID Connect. Acesta va fi introdus în 2025.

> Celelalte părți ale acestui document descriu doar federația SAML. După introducerea completă a OpenID Connect, acest document va acoperi și această tehnologie.

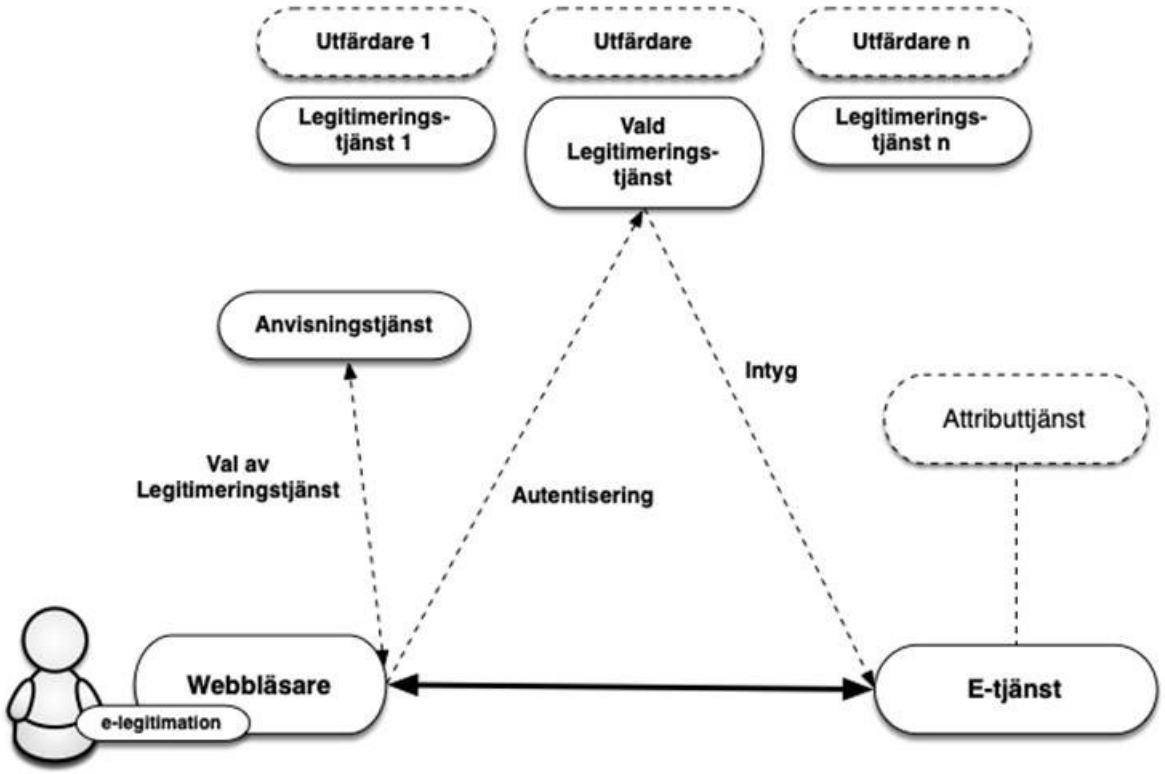
Beneficiarii primesc certificate de identitate într-un format standardizat de la un serviciu de autentificare[1].

Nu este necesar ca serviciile electronice care necesită o semnătură să fie adaptate la identificările electronice ale diferiților utilizatori pentru a crea semnături electronice. În schimb, serviciul electronic deleagă acest lucru unui serviciu de semnătură, în cadrul căruia utilizatorilor, care beneficiază de autentificare prin intermediul unui serviciu de autentificare, li se oferă posibilitatea de a semna documente electronice.

În cadrul federației, serviciile electronice și beneficiarii corespunzători își asumă rolul de furnizor de servicii (SP), în timp ce serviciile de autentificare care eliberează certificate de identitate își asumă rolul de furnizor de identitate (IdP) și, prin urmare, de autentificator al utilizatorului, indiferent de serviciul electronic pentru care utilizatorul este autentificat.

Pentru acele cazuri în care serviciul electronic are nevoie de mai multe informații despre utilizator, de exemplu informații despre capacitatea juridică, se poate adresa o întrebare unui serviciu de atribute, Autoritatea pentru atribute (AA), din cadrul federației, dacă există un astfel de serviciu de atribute relevant. Printr-o cerere de atribute, serviciul electronic poate obține informațiile suplimentare necesare pentru a autoriza utilizatorul și a oferi acces la serviciul electronic sau la un echivalent al acestuia.

Întrucât atât datele de identitate cu caracter personal, cât și alte atribute asociate utilizatorilor sunt furnizate prin intermediul certificatelor de identitate și al certificatelor de atribute, toate tipurile de identitate electronică asupra cărora părțile care se bazează au un acord și care fac parte din federație pot fi utilizate pentru autentificare în raport cu un serviciu electronic care necesită atât un număr de identitate personal, cât și informații suplimentare, chiar dacă identitatea electronică nu conține date cu caracter personal specifice (de exemplu, casete de cod pentru generarea de parole unice).



Utfärdare 1	Emitentul 1
Utfärdare n	Emitentul n
Legitimeringstjänst 1	Serviciul de autentificare 1
Vald legitimeringstjänst	Serviciu de autentificare selectat
Legitimeringstjänst n	Serviciul de autentificare n
Anvisningstjänst	Serviciul de căutare
Intyg	Certificat
Val av legitimeringstjänst	Alegerea serviciului de autentificare
autentisering	autentificare
attributtjänst	serviciu de atribute
Webbläsare	Browser
E-tjänst	Serviciu electronic

Figura 1: *Ilustrarea comunicării dintre diferitele servicii din cadrul unei federații de identitate.*

> [1]: Serviciul de autentificare este, de asemenea, menționat în alte documente de la Digg ca serviciu de identitate şi serviciu de certificare. Cu toate acestea, în prezentul document se utilizează numai termenul „serviciu de autentificare”.

1.2. Cadrul de încredere şi nivelurile de securitate

Baza pentru care se aplică nivelul de securitate atunci când un utilizator este autentificat este nivelul de asigurare pentru identificarea electronică cerut de serviciul electronic. Pentru ca aceste niveluri de securitate să fie comparabile în cadrul federației, patru niveluri de asigurare (1-4) sunt definite în cadrul de încredere pentru identificarea electronică suedeză [Digg.Tillit]

și trei niveluri de asigurare (scăzut, substanțial, ridicat) în Regulamentul eIDAS al UE. Toți emitenții de certificate de identitate trebuie să demonstreze că întregul proces care stă la baza eliberării certificatelor de identitate îndeplinește cerințele nivelului de asigurare necesar, inclusiv:

- cerințele pentru crearea certificatului de identitate;
- cerințe pentru identificarea electronică (autentificare);
- cerințele privind procesul de emitere;
- cerințele privind identificarea electronică propriu-zisă și utilizarea acesteia;
- cerințele pentru emitentul de identitate electronică;
- cerința de stabilire a identității solicitantului de identitate electronică.

1.3. Serviciul de colectare, administrare și publicare a metadatelor

O federație SAML furnizează informații cu privire la participanții federației prin intermediul metadatelor SAML. Atât entitățile care furnizează servicii de autentificare și de atribuire în cadrul federației, cât și beneficiarii, și anume entitățile care consumă aceste servicii, de exemplu serviciile electronice, sunt considerate a fi participanți la o federație.

Metadatele federației permit participanților să obțină informații cu privire la serviciile altor participanți, inclusiv datele necesare pentru schimbul securizat de informații între participanți. Metadatele trebuie să fie menținute la zi de fiecare parte și în conformitate cu condițiile contractuale.

Scopul principal al metadatelor este de a furniza cheile/certificatele necesare pentru comunicarea securizată și schimbul de informații între servicii. Pe lângă chei, metadatele conțin și alte informații importante pentru interacțiunea dintre servicii, cum ar fi adresele funcțiilor necesare, informații despre nivelurile de asigurare, categoriile de servicii, informațiile privind interfața cu utilizatorul etc.

O federație de identitate este definită de un registru în format XML care este semnat cu certificatul operatorului federației. Dosarul conține informații despre membrii federației de identitate, inclusiv certificatele acestora. Întrucât fișierul de metadate este semnat, este suficient să se compare un certificat cu omologul său de metadate. O infrastructură bazată pe un registru central al federației necesită ca registrul să fie actualizat în permanență și ca membrii federației să utilizeze întotdeauna cea mai recentă versiune a fișierului.

1.4. Serviciul de căutare

Într-o federație de identitate, este posibil să se ofere și să se consume un serviciu de căutare partajat, care enumeră serviciile de autentificare disponibile pentru utilizator pentru a alege. Scopul unui astfel de serviciu de căutare este de a scuti serviciile electronice individuale care fac parte din federația de identitate de la punerea în aplicare a sprijinului în ceea ce privește modul în care utilizatorii aleg serviciul de autentificare (sau metoda de conectare).

Întrucât serviciul de căutare este disponibil în cadrul federației de identitate, serviciile electronice își pot direcționa utilizatorii acolo pentru a alege serviciul de autentificare. Serviciul de căutare interacționează cu utilizatorul care face alegerea, iar utilizatorul, împreună cu alegerea sa, este direcționat înapoi către serviciul electronic, care știe acum la ce serviciu de autentificare ar trebui trimis utilizatorul pentru autentificare.

> În prezent, nu există un serviciu comun de căutare pentru federația Sweden Connect.

1.5. Integrarea la beneficiar

Beneficiarii, de exemplu serviciile electronice, se integrează cu serviciile de autentificare prin mesaje standardizate și consumă certificate de identitate care au, de asemenea, formate standardizate.

Cadrul tehnic Sweden Connect este influențat de profilul de interoperabilitate „Profilul de implementare pentru cadrul suedez de identificare electronică SAML V2.0” [SAML2Int]. Profilul este susținut de o serie de produse comerciale și soluții Open Source, care facilitează integrarea serviciilor electronice.

Multe servicii electronice utilizează soluții de autentificare de sine stătătoare, ceea ce înseamnă că adaptarea integrării pentru a respecta cadrul tehnic are un impact limitat asupra serviciului electronic ca atare.

1.6. Semnătura

La semnare, cadrul tehnic Sweden Connect face posibilă utilizarea diferitelor tipuri de identități electronice, chiar și a celor care nu se bazează pe certificate, fără a fi nevoie de adaptări speciale în cadrul serviciului electronic. Acest lucru se datorează faptului că certificatul de identitate emis electronic (utilizat pentru identificarea utilizatorilor la semnare) are același format, indiferent de tipul de identitate electronică utilizat de utilizator.

Un serviciu de semnătură urmărește să permită semnături în cadrul federațiilor de identitate care respectă cadrul tehnic, susținute de toate tipurile de identitate electronică care oferă un grad suficient de securitate.

Prin achiziționarea[1] și introducerea unui serviciu de semnătură, o parte care se bazează pe acesta și care face parte din federație poate permite unui utilizator să semneze un document electronic cu sprijinul serviciului de semnătură. Semnătura electronică a utilizatorului și certificatul de semnătură asociat sunt create de serviciul de semnătură după ce utilizatorul a fost de acord să semneze autentificându-se față de serviciul de semnătură[2].

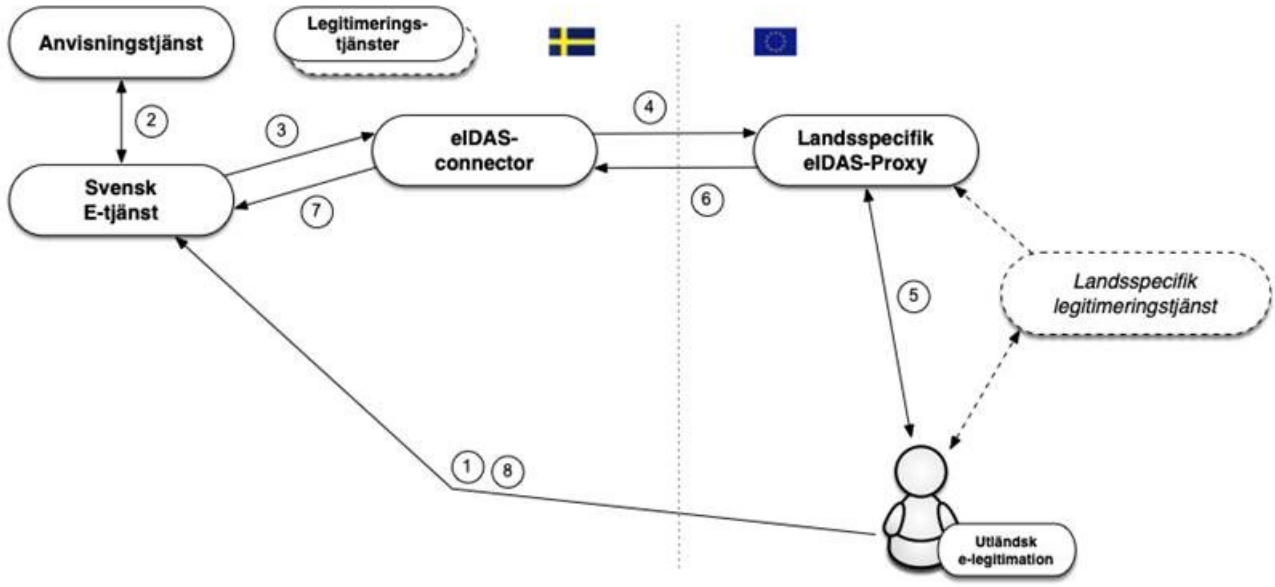
> [1]: De asemenea, este posibil să se pună în aplicare un serviciu de semnătură pe baza specificațiilor cadrului tehnic sau să se achiziționeze în alt mod un serviciu de semnătură.
>
> [2]: Este important de subliniat că este de cea mai mare importanță ca utilizatorul să perceapă acest proces ca semnarea unui document. Prin urmare, ar trebui utilizat un flux de semnături pentru identificările electronice care susțin acest lucru în legătură cu „autentificarea pentru semnătură”.

1.7. Cadrul tehnic şi eIDAS

Regulamentul UE (910/2014) privind identificarea electronică şi serviciile de încredere, eIDAS, impune organismelor publice suedeze să recunoască identificările electronice pe care alte ţări eIDAS le-au notificat. Aceasta înseamnă că un serviciu electronic public suedez bazat pe anumite norme trebuie să poată accepta o autentificare efectuată utilizând o identitate electronică emisă într-o altă ţară.

1.7.1. Autentificarea utilizând identităţi electronice străine

Specificaţiile tehnice pentru eIDAS se bazează, la fel ca şi cadrul tehnic, pe standardele SAML şi, deşi există multe asemănări, există, de asemenea, diferenţe între aceste specificaţii. Cu toate acestea, un serviciu electronic suedez nu ar trebui să se refere în mod direct la specificaţiile tehnice ale eIDAS. Imaginea de mai jos ilustrează modul în care nodul eIDAS suedez (*eIDAS-connector*) acţionează ca o punte între alte ţări şi federaţia suedeză atunci când o persoană este autentificată utilizând o carte de identitate electronică străină într-un serviciu electronic suedez. Nodul eIDAS suedez respectă cadrul tehnic.



Anvisningstjänst	Serviciul de căutare
Legitimeringstjänster	Servicii de autentificare
Svensk E-tjänst	Serviciu electronic suedez
EiDAS-connector	conectorul eiDAS
Landsspecifik Eidas Proxy	Substituent eIDAS specific pentru fiecare ţară
Landsspecifik legitimeringstjänst	Serviciu de autentificare specific ţării
utländsk e-legitimation	identitate electronică străină

Fluxul este următorul:

1. Un utilizator cu o identitate electronică străină solicită acces la un serviciu electronic suedez (și anume, se conectează).

2. Serviciul electronic permite utilizatorului să aleagă metoda de autentificare utilizând un serviciu de căutare. Se afișează o opțiune „Identificare electronică străină”, care este selectată de utilizator în cazul eIDAS.

3. Serviciul electronic creează o cerere de autentificare în conformitate cu acest cadru tehnic și direcționează utilizatorul către nodul eIDAS suedez (*connector*) pentru care DIGG este responsabil. Nodul eIDAS acționează ca un serviciu de autentificare (*Furnizor de identitate*) în cadrul federației față de beneficiarii suedezi, ceea ce înseamnă că comunicarea cu acest serviciu se efectuează în același mod ca și cu alte servicii de autentificare din cadrul federațiilor care respectă cadrul tehnic.

4. Cererea primită este prelucrată, iar nodul eIDAS afișează o pagină de selecție în care utilizatorul selectează „țara sa”[1]. Nodul eIDAS suedez transformă acum cererea de autentificare primită într-o cerere de autentificare eIDAS și direcționează utilizatorul către „serviciul proxy eIDAS” al țării selectate.

5. Atunci când cererea de autentificare este primită de serviciul proxy eIDAS pentru țara selectată, tehnologia de autentificare a țării respective preia controlul. Nu toate țările eIDAS utilizează SAML pentru autentificare, dar dacă acesta ar fi cazul în exemplul nostru, utilizatorul ar fi redirecționat către un serviciu de autentificare (*Furnizor de identitate*), iar înainte de aceasta poate și un serviciu de căutare pentru selectarea serviciului de autentificare.

6. Odată ce autentificarea a fost efectuată, un certificat (*afirmație categorică*) este creat în conformitate cu specificațiile eIDAS. Acest certificat include atribute specifice eIDAS care identifică utilizatorul. Acest certificat este acum transmis nodului suedez eIDAS.

7. Nodul primește certificatul și validează acuratețea acestuia. Acest certificat este transformat din format eIDAS într-un certificat formatat în conformitate cu cadrul tehnic și este transmis serviciului electronic.

8. Beneficiarul adaugă eventualele informații suplimentare și stabilește dacă utilizatorului ar trebui să i se acorde acces la serviciu.

Prin urmare, serviciile electronice suedeze trebuie doar să sprijine cadrul tehnic pentru a gestiona o autentificare efectuată utilizând o identificare electronică europeană. Cu toate acestea, serviciul electronic trebuie să fie în măsură să gestioneze identitatea prezentată, care nu este neapărat un număr personal de identificare. Astfel, pot exista cazuri în care un serviciu electronic autentifică un utilizator prin intermediul cadrului eIDAS, dar identitatea prezentată a utilizatorului nu poate fi utilizată în serviciul electronic. Mai multe despre acest subiect în capitolul 1.7.3 de mai jos.

[1]: De fapt, utilizatorul alege „serviciul proxy eIDAS” către care ar trebui transmisă cererea. Acest lucru depinde de țara de care aparține emitentul identității electronice a utilizatorului.

1.7.2. Semnături care utilizează identităţi electronice străine

După cum s-a descris deja, în acest cadru tehnic se aplică un model de semnătură electronică denumit semnătură federată. Un serviciu de semnătură bazat pe server este legat de serviciul electronic, care, la rândul său, solicită o semnătură. Atunci când un utilizator semnează un document, serviciul electronic trimite o cerere de semnătură serviciului de semnătură. Serviciul de semnătură solicită apoi utilizatorului să se autentifice. În legătură cu autentificarea, utilizatorul aprobă semnătura. Serviciul de semnătură trimite datele înapoi la serviciul electronic, iar apoi sunt stocate datele de semnătură asociate cu documentul care a fost semnat.

Această procedură face posibilă semnarea, de asemenea, utilizând o carte de identitate electronică străină, deoarece serviciul de semnătură poate alege să autentifice utilizatorul utilizând o carte de identitate electronică străină în conformitate cu procedura descrisă mai sus în secţiunea 1.7.1.

Atunci când semnează, în acest caz, nodul eIDAS suedez este responsabil pentru a informa utilizatorul că scopul autentificării este de a semna un document, cine a solicitat semnătura şi orice informaţii despre ceea ce se semnează. Un certificat de identitate este eliberat numai după ce utilizatorul s-a autentificat (pentru semnătură), iar acesta este trimis serviciului de semnătură, care, la rândul său, generează semnătura.

1.7.3. Gestionarea identităţilor

Certificatele de identitate din alte ţări respectă specificaţiile tehnice la nivelul UE elaborate în cadrul Regulamentului eIDAS. Atributele pe care fiecare ţară trebuie să le includă întotdeauna pentru persoanele fizice, precum şi pentru organizaţii („set minim de date”, SMD) sunt prevăzute în prezentul regulament. Fiecare ţară trebuie să includă un identificator unic pentru fiecare identitate electronică, reprezentând o singură persoană fizică. Din unele ţări, aceşti identificatori vor fi unici şi persistenţi pe persoană în acelaşi mod ca, de exemplu, numerele de identitate personale suedeze, dar aceşti identificatori pot avea compoziţii şi caracteristici foarte diferite. O caracteristică care poate varia este cât de persistent este un astfel de identificator, şi anume dacă un astfel de identificator rămâne neschimbat pe parcursul vieţii unei persoane sau se schimbă dacă, de exemplu, persoana se mută într-o altă regiune, îşi schimbă numele sau doar îşi schimbă identitatea electronică. Din unele ţări (de exemplu, Regatul Unit), identificatorul va varia în funcţie de identificarea electronică a ţării pe care un utilizator alege în prezent să o folosească.

Pentru a simplifica gestionarea utilizatorilor în serviciile electronice suedeze, nodul eIDAS suedez generează un atribut ID standardizat pentru utilizatorii care au fost autentificaţi utilizând o identitate electronică străină, cunoscut sub denumirea de *ID provizoriu* (prescurtat PRID). În plus, se creează un atribut asociat care declară persistenţa sau durata de viaţă aşteptată a acestui atribut ID. Atributul PRID este generat pe baza valorilor atributelor obţinute din autentificarea străină în conformitate cu metodele specificate pentru ţara respectivă. Fiecare combinaţie de ţară şi metodă este clasificată în funcţie de persistenţa preconizată, şi anume probabilitatea ca o identitate să se schimbe în timp pentru aceeaşi persoană. Acest lucru permite serviciilor electronice suedeze să adapteze comunicarea cu utilizatorul şi să ofere în mod proactiv caracteristici care să faciliteze redobândirea controlului asupra informaţiilor din serviciul electronic de către un utilizator a cărui identitate s-a schimbat.

În unele cazuri, o persoană care este autentificată utilizând o carte de identitate electronică străină poate deține, de asemenea, un număr personal de identitate suedez. Acesta poate fi, de exemplu, un cetățean suedez care s-a mutat în străinătate și a obținut o carte de identitate electronică străină sau un cetățean străin care este înregistrat în Suedia și căruia i s-a atribuit un număr personal de identificare.

Faptul că o persoană cu o identitate electronică străină are un număr de identitate personal suedez nu este cunoscut în mod normal serviciului de autentificare din străinătate și, prin urmare, aceste informații nu sunt incluse în certificatul de identitate din țara în care persoana este autentificată. Nodul suedez, pe de altă parte, are capacitatea de a interoga un serviciu de atribute în Suedia[1] cu privire la existența unui număr personal de identificare înregistrat pentru persoana autentificată și poate, în acest caz, să adauge astfel de informații la certificatul de identitate trimis serviciului electronic.

> [1]: La momentul redactării, nu există niciun serviciu de atribute care să stabilească o legătură între identitățile eIDAS și numerele de identitate personală suedeze.

1.7.4. Identificări electronice suedeze în serviciile electronice străine

Suedia a notificat identificări electronice suedeze la niveluri de asigurare substanțial și ridicat în conformitate cu eIDAS.

O cerere de autentificare din partea unui serviciu electronic străin este adresată nodului eIDAS suedez (serviciu proxy) prin intermediul unui conector eIDAS în țara serviciului electronic. În nodul eIDAS suedez, utilizatorul alege identitatea electronică suedeză cu care dorește să se autentifice, iar apoi o cerere de autentificare este trimisă serviciului de autentificare (*Furnizorul de identitate*) care gestionează identificarea electronică selectată. Această cerere este formatată în conformitate cu un cadru tehnic, ceea ce înseamnă că un serviciu suedez de autentificare nu trebuie să respecte specificațiile tehnice eIDAS.

Utilizatorul este autentificat de serviciul de autentificare suedez și se eliberează un certificat de identitate (în conformitate cu cadrul tehnic). Acest certificat este primit de serviciul proxy eIDAS suedez și transformat într-un certificat în conformitate cu specificațiile eIDAS înainte de a fi transmis către conectorul eIDAS străin și apoi către serviciul electronic apelant (*Furnizorul de servicii*).

2. Specificațiile tehnice

Acest capitol conține specificații și profiluri pentru federațiile de identitate care respectă cadrul tehnic Sweden Connect și anumite servicii conexe. Cu excepția cazului în care se prevede altfel, aceste documente sunt prescriptive pentru furnizarea de servicii în cadrul federațiilor de identitate care pun în aplicare cadrul tehnic.

2.1. Profiluri și specificații pentru SAML

Federațiile de identitate care respectă cadrul tehnic Sweden Connect sunt construite în jurul „Profilului de implementare pentru cadrul suedez de identificare electronică”, [SAML.Profile]. Acest profil este influențat, dar nu depinde în mod prescriptiv de „Profilul de

implementare SAML V2.0 pentru interoperabilitatea federației" [SAML2Int]. [SAML.Profile] conține, de asemenea, norme și orientări specifice cadrului tehnic Sweden Connect.

2.1.1. Profilul de implementare pentru cadrul suedez de identificare electronică

„Profilul de implementare pentru cadrul suedez de identificare electronică", [SAML.Profile], este principalul document-cadru tehnic și precizează, printre altele:

- modul în care se construiesc și se interpretează metadatele SAML;
- modul în care trebuie să fie formatată cererea de autentificare;
- modul în care se tratează o cerere de autentificare și modul în care se proiectează, se verifică și se gestionează un certificat de identitate;
- cerințele de securitate;
- cerințe SAML specifice pentru serviciile de semnătură și „autentificare pentru semnătură".

2.1.2. Cadrul suedez de identificare electronică – Registrul identificatorilor

Implementarea unei infrastructuri suedeze de identificare electronică necesită diferite forme de identificatori pentru a reprezenta obiecte în structurile de date. Documentul „Sweden Connect – Registry for identifiers" (Registrul identificatorilor), [SC.Registry], definește structura identificatorilor atribuiți în temeiul cadrului tehnic, precum și un registru al identificatorilor definiți.

2.1.3. Specificație de atribut pentru cadrul suedez de identificare electronică

Specificația „Attribute Specification for the Swedish eID Framework" (Specificație de atribut pentru cadrul suedez de identificare electronică, [SAML.Attributes], declară profilurile de atribute SAML care sunt utilizate în cadrul federațiilor de identitate care respectă cadrul tehnic inclusiv cele care se conectează la eIDAS prin nodul suedez eIDAS.

2.1.4. Categorii de entități pentru cadrul suedez de identificare electronică

Categoriile de entități sunt utilizate în cadrul federației pentru o serie de scopuri diferite:

- Categorii de entități de servicii – Utilizate în metadate pentru a reprezenta cerințele serviciilor electronice pentru nivelurile de asigurare și atributele solicitate, precum și îndeplinirea nivelurilor de asigurare și furnizarea atributelor de către serviciile de autentificare.
- Categorii de proprietăți ale serviciilor – utilizate pentru a reprezenta o caracteristică specifică a unui serviciu.
- Categorii de entități de tip serviciu – Utilizate pentru a reprezenta diferite tipuri de servicii în cadrul federației.

- Categorii de entități contractante de servicii – Utilizate de servicii pentru a anunța formulare de acord și altele asemenea.

- Categorii generale de entități – Categorii de entități care nu se încadrează în niciunul dintre tipurile de mai sus.

Specificația „Entity Categories for the Swedish eID Framework” (Categorii de entități pentru cadrul suedez de identificare electronică) [SAML.EntCat] precizează categoriile de entități definite de cadrul tehnic și descrie semnificația acestora.

2.1.5. Specificaţia atributelor construite eIDAS pentru cadrul suedez de identificare electronică

Caietul de sarcini „eIDAS Constructed Attributes Specification for the Swedish eID Framework” (Specificația atributelor construite eIDAS pentru cadrul suedez de identificare electronică), [SC.eIDAS.Attrs], specifică procesele și regulile pentru modul în care tributele ID sunt construite pe baza atributelor primite în timpul autentificării în eIDAS.

2.1.6. Profilul de implementare pentru furnizorii de identitate BankID în cadrul suedez de identificare electronică

Specificația „Implementation Profile for BankID Identity Providers within the Swedish eID Framework” (Profil de implementare pentru furnizorii de identitate BankID în cadrul suedez de identificare electronică), [SAML.BankID], definește reguli pentru modul în care un serviciu de autentificare care implementează suport pentru BankID trebuie să fie proiectat.

> **Vă rugăm să rețineți următoarele:** Această specificație nu este prescriptivă pentru conformitatea cu un cadru tehnic. Este relevant numai pentru serviciile de autentificare care implementează suport pentru BankID și pentru serviciile electronice care le utilizează. Cu toate acestea, serviciile de autentificare care implementează suport pentru BankID și doresc să se conecteze la federația Sweden Connect trebuie să respecte această specificație.

2.1.7. Selecţia principalului în cererile de autentificare SAML

Specificația „Principal Selection in SAML Authentication Requests” (Selecția principală în solicitările de autentificare SAML), [SAML.Principal], definește o extindere la SAML care permite unei părți care se bazează să informeze un serviciu de autentificare cu privire la identitatea pe care dorește să o autentifice.

2.1.8. Extensia mesajului utilizatorului în cererile de autentificare SAML

Specificația „User Message Extension in SAML Authentication Requests” (Extensia mesajelor utilizatorului în solicitările de autentificare SAML), [SAML.UMessage], definește o extensie la SAML care permite unei părți care se bazează să includă un mesaj de afișare în cererea de autentificare trimisă serviciului de autentificare. Serviciul de autentificare poate afișa apoi acest mesaj utilizatorului în timpul etapei de autentificare.

2.2. Profiluri şi specificaţii pentru OpenID Connect

2.2.1. Profilul OpenID Connect pentru Sweden Connect

Profilul „OpenID Connect Profile for Sweden Connect” (Profilul OpenID Connect pentru Sweden Connect), [OIDC.Profile], se bazează pe profilul suedez OpenID Connect care este un profil OpenID Connect dezvoltat de OIDC Suedia pentru a promova interoperabilitatea şi securitatea în cadrul soluţiilor OIDC suedeze.

[OIDC.Profile] adaugă cerinţe suplimentare privind federaţia Sweden Connect.

2.2.2. Revendicări şi specificaţii OpenID Connect privind domeniile de aplicare pentru Sweden Connect

Specificaţia „OpenID Connect Claims and Scopes Specification for Sweden Connect” (Revendicări şi specificaţii OpenID Connect privind domeniile de aplicare pentru Sweden Connect), [OIDC.Claims], se bazează pe specificaţia Claims and Scopes Specification for the Swedish OpenID Connect Profile din OIDC Sweden.

2.3. Specificaţii pentru semnătură

Această secţiune conţine trimiteri la documentele care definesc serviciile de semnătură din cadrul federaţiilor care respectă cadrul tehnic Sweden Connect.

2.3.1. Profil de implementare pentru utilizarea DSS OASIS în serviciile centrale de semnare

Profilul de implementare „Implementation Profile for Using OASIS DSS in Central Signing Services” (Profil de implementare pentru utilizarea DSS OASIS în serviciile centrale de semnătură), [Sign.DSS.Profile], specifică un profil pentru cererea de semnătură şi răspunsul la aceasta în conformitate cu standardul OASIS „Protocoale, elemente şi legături esenţiale ale serviciului de semnătură digitală”, [DSS].

2.3.2. Extensia DSS pentru serviciile federate de semnătură centrală

„DSS Extension for Federated Central Signing Services” (Extensia DSS pentru serviciile federate de semnătură centrală), [Sign.DSS.Ext], este o extensie a standardului OASIS „Protocoale, elemente şi legături esenţiale ale serviciului de semnătură digitală”, [DSS], care specifică definiţiile necesare pentru semnare în cadrul tehnic.

2.3.3. Profilul certificatului pentru certificatele emise de serviciile centrale de semnare

Profilul certificatului „Certificate Profile for Certificates Issued by Central Signing Services” (Profilul certificatului pentru certificatele eliberate de serviciile centrale de semnătură), [Sign.Cert.Profile], specifică conţinutul certificatelor de semnătură. Acest profil aplică o nouă extensie de certificat pentru a sprijini serviciile de semnătură.

Acest profil se referă la „Authentication Context Certificate Extension” (Extensie de certificat de context de autentificare), [AuthContext], care descrie modul în care „Authentication Context” este reprezentat în certificatele X.509.

2.3.4. Protocol de activare a semnăturii pentru semnare federată

Specificația „Signature Activation Protocol for Federated Signing” (Protocol de activare a semnăturii pentru semnare federată), [Sign.Activation], definește un „Signature Activation Protocol” (protocol de activare a semnăturii) (SAP) pentru punerea în aplicare a „Sole Control Assurance Level 2” (Nivelul de asigurare a controlului unic) (SCAL2) în conformitate cu standardul „prEN 419241 – Sisteme fiabile de susținere a semnăturii prin server”.

3. Listă de referințe

3.1. DIGG

[Digg.Tillit]

Cadrul de încredere pentru identificarea electronică suedeză.

[SC.Registry]

Sweden Connect – Registrul identificatorilor.

[SAML.Profile]

Profilul de implementare pentru cadrul suedez de identificare electronică.

[SAML.Attributes]

Specificație de atribut pentru cadrul suedez de identificare electronică.

[SAML.EntCat]

Categorii de entități pentru cadrul suedez de identificare electronică.

[SC.eIDAS.Attrs]

eIDAS Specificația atributelor construite pentru cadrul suedez de identificare electronică.

[SAML.BankID]

Profilul de implementare pentru furnizorii de identitate BankID din cadrul suedez de identificare electronică.

[SAML.Principal]

Selecția principală în cererile de autentificare SAML.

[SAML.UMessage]

Extensia mesajului utilizatorului în cererile de autentificare SAML.

[Profilul OIDC]

Profilul OpenID Connect pentru Sweden Connect.

[OIDC.Claims]

OpenID Connect Revendicări şi specificaţii privind domeniile pentru Sweden Connect.

[Sign.DSS.Profile]

Profil de implementare pentru utilizarea DSS OASIS în serviciile centrale de semnare.

[Sign.DSS.Ext]

Extensie DSS pentru serviciile federate de semnătură centrală.

[Sign.Cert.Profile]

Profilul certificatului pentru certificatele emise de serviciile centrale de semnare.

[Sign.Activation]

Protocol de activare a semnăturii pentru semnare federată.

3.2. Alte referinţe

[SAML2Int]

Profilul de implementare SAML V2.0 pentru interoperabilitatea federaţiei.

[DSS]

OASIS Standard – Digital Signature Service Core Protocols, Elements, and Bindings (Protocoale de bază ale serviciului de semnătură digitală, elemente şi legături) Versiunea 1.0, 11 aprilie 2007.

[AuthContext]

RFC-7773: Extensie de certificat pentru contextul de autentificare.