Introduction au cadre technique de Sweden Connect

4.12.2024

Numéro de référence: **2019-267**

Table des matières

1. Introduction

1.1. Aperçu général

Le cadre technique de Sweden Connect est adapté aux fédérations d’identité basées sur SAML 2.0.

> Dans la dernière version du cadre technique, des spécifications pour OpenID Connect ont également été introduites. Actuellement, il n’existe pas de prise en charge de fédération pour OpenID Connect. Cela sera introduit en 2025.

> Les autres parties de ce document ne décrivent que la fédération SAML. Une fois OpenID Connect entièrement introduit, ce document couvrira également cette technologie.

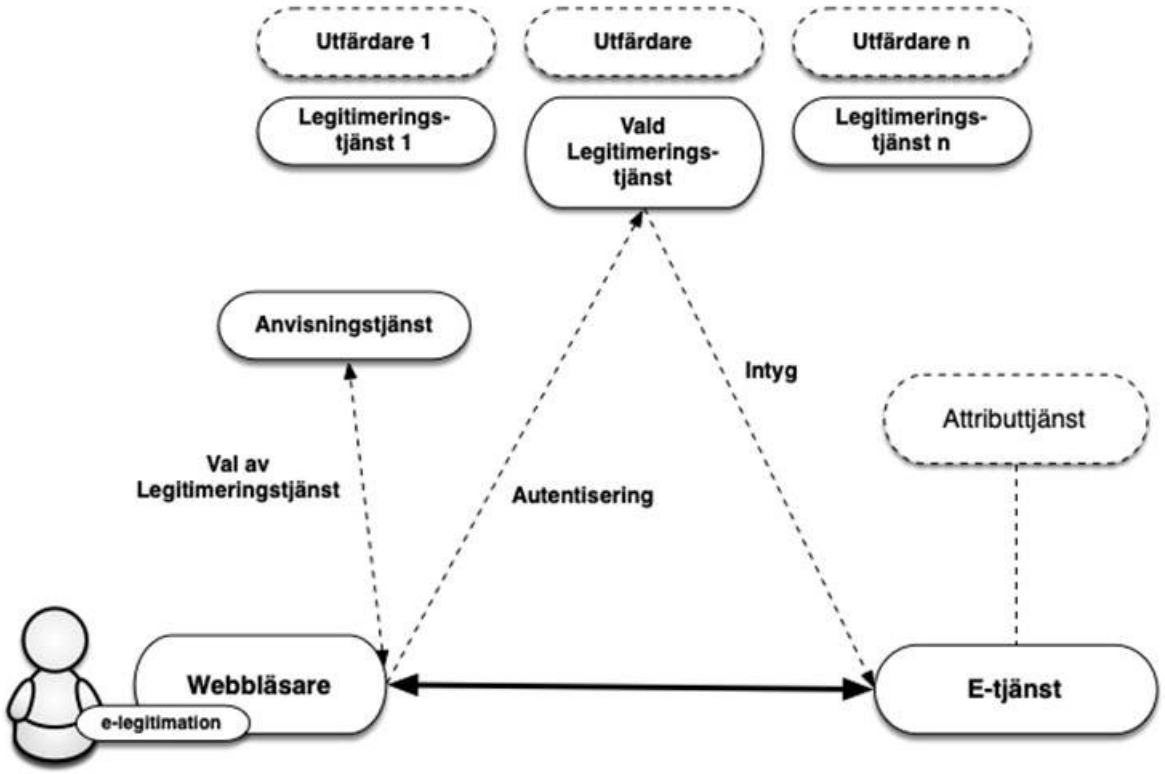
Les parties utilisatrices reçoivent des certificats d'identité dans un format standardisé d'un service d'authentification[1].

Les services électroniques qui nécessitent une signature n'ont pas besoin d'être adaptés aux eID des différents utilisateurs pour créer des signatures électroniques. Au lieu de cela, le service électronique délègue cela à un service de signature, où les utilisateurs, pris en charge par une authentification par le biais d'un service d'authentification, ont la possibilité de signer des documents électroniques.

Au sein de la fédération, les services électroniques et les parties utilisatrices correspondantes assument le rôle de prestataire de services (PS), tandis que les services d'authentification délivrant des certificats d'identité assument le rôle de fournisseur d'identité (FdI) et donc d'authentificateur de l'utilisateur, quel que soit le service électronique pour lequel l'utilisateur est authentifié.

Pour les cas où le service électronique a besoin de plus d'informations sur l'utilisateur, par exemple des informations sur la capacité juridique, une question peut être posée à un service d'attributs, l'autorité d'attributs (AA), au sein de la fédération, s'il existe un tel service d'attributs pertinent. Au moyen d'une requête d'attributs, le service électronique peut obtenir les informations supplémentaires nécessaires pour autoriser l'utilisateur et lui donner accès au service électronique ou équivalent.

Étant donné que les données d'identité personnelles et les autres attributs associés aux utilisateurs sont fournis au moyen de certificats d'identité et de certificats d'attributs, tous les types d'eID sur lesquels les parties utilisatrices ont conclu un accord et qui font partie de la fédération peuvent être utilisés pour l'authentification vis-à-vis d'un service électronique qui nécessite à la fois un numéro d'identité personnel et des informations supplémentaires, même si l'eID ne contient aucune donnée personnelle spécifique (par exemple, des boîtes de code pour la génération de mots de passe à usage unique).



Utfärdare 1	Émetteur 1
Utfärdare n	Émetteur n
Legitimeringstjänst 1	Service d'authentification 1
Vald legitimeringstjänst	Service d'authentification sélectionné
Legitimeringstjänst n	Service d'authentification n
Anvisningstjänst	Service de découverte
Intyg	Certificat
Val av legitimeringstjänst	Choix du service d'authentification
autentisering	Authentification
attributtjänst	Service d'attributs
Webbläsare	Navigateur
E-tjänst	Service électronique

Figure 1: *Illustration de la communication entre les différents services au sein d'une fédération d'identité.*

[1]: Le service d'authentification est également mentionné dans d'autres documents de la Digg comme un service d'identité et un service de certification. Toutefois, dans le présent document, seul le terme «service d'authentification» est utilisé.

1.2. Cadre de confiance et niveaux de sécurité

La base pour laquelle le niveau de sécurité doit être appliqué lors de l'authentification d'un utilisateur est le niveau d'assurance pour l'identification électronique requis par le service électronique. Afin que ces niveaux de sécurité soient comparables dans le cadre de la

fédération, quatre niveaux d'assurance (1-4) sont définis dans le cadre de confiance pour l'identification électronique suédoise [Digg.Tillit] et trois niveaux d'assurance (faible, substantiel, élevé) dans le règlement eIDAS de l'Union. Tous les émetteurs de certificats d'identité doivent démontrer que l'ensemble du processus qui sous-tend la délivrance des certificats d'identité satisfait aux exigences du niveau d'assurance requis, y compris:

- les exigences relatives à la création du certificat d'identité;
- les exigences en matière d'identification électronique (authentification);
- les exigences relatives au processus de délivrance;
- les exigences relatives à l'eID elle-même et à son utilisation;
- les exigences applicables à l'émetteur de l'eID;
- l'exigence d'établir l'identité du demandeur d'eID.

1.3. Service de collecte, d'administration et de publication de métadonnées

Une fédération SAML fournit des informations sur les participants de la fédération au moyen de métadonnées SAML. Les entités qui fournissent des services d'authentification et d'attributs dans la fédération ainsi que les parties utilisatrices, c'est-à-dire les entités qui consomment ces services, par exemple les services électroniques, sont considérées comme des participants à une fédération.

Les métadonnées de la fédération permettent aux participants d'obtenir des informations sur les services des autres participants, y compris les données nécessaires à l'échange sécurisé d'informations entre les participants. Les métadonnées doivent être tenues à jour par chaque partie et conformément aux conditions contractuelles.

L'objectif principal des métadonnées est de fournir les clés/certificats nécessaires à la communication sécurisée et à l'échange d'informations entre les services. Outre les clés, les métadonnées contiennent également d'autres informations importantes pour l'interaction entre les services, telles que les adresses des fonctions requises, des informations sur les niveaux d'assurance, les catégories de services, les informations sur l'interface utilisateur, etc.

Une fédération d'identité est définie par un registre au format XML qui est signé avec le certificat de l'opérateur de la fédération. Le fichier contient des informations sur les membres de la fédération d'identité, y compris leurs certificats. Étant donné que le fichier de métadonnées est signé, il suffit de comparer un certificat avec son homologue de métadonnées. Une infrastructure basée sur un registre central de fédération exige que le registre soit continuellement mis à jour et que les membres de la fédération utilisent toujours la dernière version du fichier.

1.4. Service de découverte

Dans une fédération d'identité, il est possible d'offrir et de consommer un service de découverte partagé, qui répertorie les services d'authentification disponibles pour l'utilisateur. Le but d'un tel service de découverte est de soulager les services électroniques individuels qui font partie de la fédération d'identité de la mise en œuvre de la prise en charge en ce qui

concerne la façon dont les utilisateurs choisissent le service d'authentification (ou la méthode de connexion).

Étant donné que le service de découverte est disponible au sein de la fédération d'identité, les services électroniques peuvent y diriger leurs utilisateurs afin de choisir le service d'authentification. Le service de découverte interagit avec l'utilisateur qui fait son choix, et l'utilisateur, ainsi que le choix de l'utilisateur, est redirigé vers le service électronique, qui sait désormais à quel service d'authentification l'utilisateur doit être envoyé pour authentification.

> Il n'existe actuellement aucun service de découverte partagé pour la fédération Sweden Connect.

1.5. Intégration au sein de la partie requérante

Les parties utilisatrices, par exemple les services électroniques, s'intègrent aux services d'authentification au moyen de messages normalisés et consomment des certificats d'identité qui ont également des formats normalisés.

Le cadre technique de Sweden Connect est influencé par le profil d'interopérabilité «profil de déploiement SAML V2.0 pour l'interopérabilité de fédération» [SAML2Int]. Le profil est pris en charge par un certain nombre de produits commerciaux et de solutions open source, ce qui facilite l'intégration aux services électroniques.

De nombreux services électroniques utilisent des solutions d'authentification autonomes, ce qui signifie que l'adaptation de l'intégration au cadre technique a un impact limité sur le service électronique en tant que tel.

1.6. Signature

Lors de la signature, le cadre technique de Sweden Connect permet d'utiliser différents types d'eID, même ceux qui ne sont pas basés sur des certificats, sans nécessiter d'adaptations spéciales dans le service électronique. En effet, le certificat d'identité délivré par voie électronique (utilisé pour l'identification des utilisateurs lors de la signature) a le même format, quel que soit le type d'eID utilisé par l'utilisateur.

Un service de signature vise à permettre des signatures au sein de fédérations d'identité conformes au cadre technique, prises en charge par tous les types d'eID offrant un degré de sécurité suffisant.

En se procurant[1] et en introduisant un service de signature, une partie utilisatrice qui fait partie de la fédération peut permettre à un utilisateur de signer un document électronique avec la prise en charge du service de signature. La signature électronique de l'utilisateur et le certificat de signature associé sont créés par le service de signature après que l'utilisateur a accepté de signer en s'authentifiant auprès du service de signature[2].

> [1]: Il est également possible de mettre en œuvre un service de signature basé sur les spécifications du cadre technique, ou d'acquérir un service de signature.
>
> [2]: Il est important de noter qu'il est de la plus haute importance que l'utilisateur perçoive ce processus comme la signature d'un document. Par conséquent, il

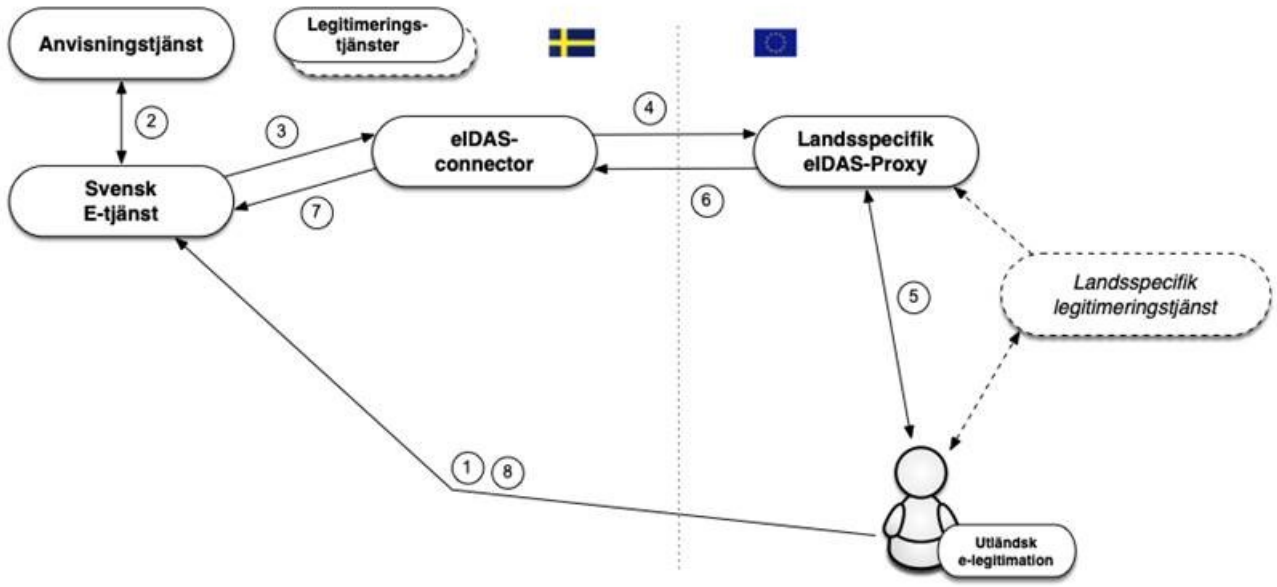
convient d’utiliser un flux de signature pour les eID qui le prennent en charge dans le cadre de l’«authentification pour signature».

1.7. Cadre technique et eIDAS

Le règlement UE (910/2014) sur l’identification électronique et les services de confiance, eIDAS, exige des organismes publics suédois qu’ils reconnaissent les eID que d’autres pays eIDAS ont notifiées. Cela signifie qu’un service électronique public suédois fondé sur certaines règles doit être en mesure d’accepter une connexion effectuée à l’aide d’une eID délivrée dans un autre pays.

1.7.1. Authentification à l’aide d’eID étrangères

Les spécifications techniques pour eIDAS sont basées, comme le cadre technique, sur les normes SAML, et bien qu’il existe de nombreuses similitudes, il existe également des différences dans ces spécifications. Toutefois, un service électronique suédois ne devrait pas être directement lié aux spécifications techniques d’eIDAS. L’image ci-dessous illustre comment le nœud suédois eIDAS (*eIDAS-connector*) sert de passerelle entre d’autres pays et la fédération suédoise lorsqu’une personne est authentifiée à l’aide d’une eID étrangère dans un service électronique suédois. Le nœud suédois eIDAS est conforme au cadre technique.



Anvisningstjänst	Service de découverte
Legitimeringstjänster	Services d’authentification
Svensk E-tjänst	Service électronique suédois
EiDAS-connector	Connecteur eIDAS
Landsspecifik Eidas Proxy	Proxy eIDAS spécifique au pays
Landsspecifik legitimeringstjänst	Service d’authentification spécifique au pays
utländsk e-legitimation	eID étrangère

Le débit est le suivant:

1. Un utilisateur avec une eID étrangère demande l'accès à un service électronique suédois (c'est-à-dire qu'il se connecte).

2. Le service électronique permet à l'utilisateur de choisir la méthode de connexion à l'aide d'un service de découverte. Une option «eID étrangère» est affichée, qui est sélectionnée par l'utilisateur dans le cas eIDAS.

3. Le service électronique crée une requête d'authentification conformément à ce cadre technique et dirige l'utilisateur vers le nœud eIDAS suédois (*connecteur*) dont la Digg est responsable. Le nœud eIDAS agit comme un service d'authentification (*fournisseur d'identité*) dans la fédération vis-à-vis des parties utilisatrices suédoises, ce qui signifie que la communication avec ce service est effectuée de la même manière qu'avec d'autres services d'authentification au sein de fédérations conformes au cadre technique.

4. La requête reçue est traitée et le nœud eIDAS affiche une page de sélection dans laquelle l'utilisateur sélectionne «son pays»[1]. Le nœud suédois eIDAS convertit désormais la requête d'authentification reçue en requête d'authentification eIDAS et dirige l'utilisateur vers le «service proxy eIDAS» du pays sélectionné.

5. Lorsque la requête d'authentification est reçue par le service proxy eIDAS pour le pays sélectionné, la technologie d'authentification de ce pays prend le relais. Tous les pays eIDAS n'utilisent pas SAML pour l'authentification, mais si c'était le cas dans notre exemple, l'utilisateur serait redirigé vers un service d'authentification (*fournisseur d'identité*), et avant cela peut-être aussi un service de découverte pour la sélection du service d'authentification.

6. Une fois l'authentification effectuée, un certificat (*assertion*) est créé selon les spécifications eIDAS. Ce certificat inclut des attributs spécifiques eIDAS qui identifient l'utilisateur. Ce certificat est maintenant transmis au nœud suédois eIDAS.

7. Le nœud reçoit le certificat et valide son exactitude. Ce certificat est transformé du format eIDAS en un certificat formaté selon le cadre technique et est envoyé au service électronique.

8. La partie utilisatrice ajoute des informations supplémentaires et détermine si l'utilisateur doit se voir accorder l'accès au service.

Les services électroniques suédois n'ont donc besoin de prendre en charge le cadre technique que pour gérer une authentification effectuée à l'aide d'une eID européenne. Toutefois, le service électronique doit être en mesure de gérer l'identité présentée, qui n'est pas nécessairement un numéro d'identité personnel. Ainsi, il peut y avoir des cas où un service électronique authentifie un utilisateur via le cadre eIDAS, mais où l'identité présentée par l'utilisateur ne peut pas être utilisée dans le service électronique. Pour en savoir plus à ce sujet, voir le point 1.7.3 ci-dessous.

[1]: En fait, l'utilisateur choisit le «service proxy eIDAS» auquel la requête doit être transmise. Cela dépend du pays auquel appartient l'émetteur de l'identification électronique de l'utilisateur.

1.7.2. Signatures à l'aide d'eID étrangères

Comme déjà décrit, un modèle de signature électronique est appliqué dans ce cadre technique appelé signature fédérée. Un service de signature basé sur un serveur est lié au service électronique, qui à son tour demande une signature. Lorsqu'un utilisateur signe un document, le service électronique envoie une requête de signature au service de signature. Le service de signature demande alors à l'utilisateur de s'authentifier. Dans le cadre de l'authentification, l'utilisateur approuve la signature. Le service de signature renvoie les données au service électronique, puis les données de signature associées au document signé sont stockées.

Cette procédure permet de signer également à l'aide d'une eID étrangère, étant donné que le service de signature peut choisir d'authentifier l'utilisateur à l'aide d'une eID étrangère conformément à la procédure décrite au point 1.7.1 ci-dessus.

Lors de la signature, dans ce cas, le nœud suédois eIDAS est responsable d'informer l'utilisateur que le but de l'authentification est de signer un document, qui a demandé la signature, et toute information sur ce qui est signé. Un certificat d'identité n'est délivré qu'une fois que l'utilisateur s'est authentifié (pour signature) et qu'il est envoyé au service de signature qui génère à son tour la signature.

1.7.3. Gestion des identités

Les certificats d'identité d'autres pays sont conformes aux spécifications techniques élaborées à l'échelle de l'Union dans le cadre du règlement eIDAS. Les attributs que chaque pays doit toujours inclure pour les personnes physiques ainsi que pour les organisations («ensemble de données minimal», EDM) sont définis dans le présent règlement. Chaque pays doit inclure un identifiant unique par eID représentant une seule personne physique. Dans certains pays, ces identifiants seront uniques et persistants par personne de la même manière que, par exemple, les numéros d'identité personnels suédois, mais ces identifiants peuvent avoir des compositions et des caractéristiques très différentes. Une caractéristique qui peut varier est la persistance d'un tel identifiant, c'est-à-dire si un tel identifiant reste inchangé au cours de la vie d'une personne ou change si, par exemple, la personne déménage dans une autre région, change de nom ou change simplement d'eID. Dans certains pays (par exemple, le Royaume-Uni), l'identifiant variera en fonction de l'eID du pays qu'un utilisateur choisit actuellement d'utiliser.

Afin de simplifier la gestion des utilisateurs dans les services électroniques suédois, le nœud eIDAS suédois génère un attribut d'identification normalisé pour les utilisateurs qui ont été authentifiés à l'aide d'une eID étrangère, connu sous le nom d'*ID provisoire* (en abrégé IDPR). En outre, un attribut associé est créé qui déclare la persistance attendue, ou la durée de vie, de cet attribut ID. L'attribut IDPR est généré sur la base des valeurs d'attribut obtenues à partir de l'authentification étrangère selon des méthodes spécifiées pour ce pays particulier. Chaque combinaison de pays et de méthode est classée en fonction de la persistance attendue, c'est-à-dire de la probabilité qu'une identité change au fil du temps pour la même personne. Cela permet aux services électroniques suédois d'adapter la communication avec l'utilisateur et de fournir de manière proactive des fonctionnalités qui permettent à un utilisateur dont l'identité a changé de reprendre le contrôle de ses informations dans le service électronique.

Dans certains cas, une personne authentifiée à l'aide d'une eID étrangère peut également détenir un numéro d'identité personnel suédois. Il peut s'agir, par exemple, d'un citoyen

suédois qui a déménagé à l'étranger et obtenu une eID étrangère ou d'un citoyen étranger qui est enregistré en Suède et qui s'est vu attribuer un numéro d'identité personnel.

Le fait qu'une personne possédant une eID étrangère dispose d'un numéro d'identité personnel suédois n'est normalement pas connu du service d'authentification étranger, et cette information n'est donc pas incluse dans le certificat d'identité du pays dans lequel la personne est authentifiée. Le nœud suédois, d'autre part, a la capacité d'interroger un service d'attributs en Suède[1] pour savoir s'il existe un numéro d'identité personnel enregistré pour la personne authentifiée et peut, le cas échéant, ajouter ces informations au certificat d'identité envoyé au service électronique.

> [1]: Au moment de la rédaction du présent document, aucun service d'attributs n'établit de lien entre les identités eIDAS et les numéros d'identité personnels suédois.

1.7.4. eID suédoise dans les services électroniques étrangers

La Suède a notifié des eID suédoises aux niveaux de garantie substantiel et élevé selon eIDAS.

Une requête d'authentification d'un service électronique étranger est adressée au nœud eIDAS suédois (service proxy) via un connecteur eIDAS dans le pays du service électronique. Dans le nœud eIDAS suédois, l'utilisateur choisit l'eID suédoise qu'il souhaite utiliser pour s'authentifier, puis une requête d'authentification est envoyée au service d'authentification (*fournisseur d'identité*) qui gère l'eID sélectionnée. Cette requête est formatée selon un cadre technique, ce qui signifie qu'un service d'authentification suédois n'a pas à se conformer aux spécifications techniques eIDAS.

L'utilisateur est authentifié par le service d'authentification suédois et un certificat d'identité est délivré (conformément au cadre technique). Ce certificat est reçu par le service proxy eIDAS suédois et converti en certificat selon les spécifications eIDAS avant d'être transmis au connecteur eIDAS étranger, puis au service électronique appelant (*prestataire de service*).

2. Spécifications techniques

Ce chapitre contient des spécifications et des profils pour les fédérations d'identité qui sont conformes au cadre technique de Sweden Connect, et certains services connexes. Sauf indication contraire, ces documents sont prescriptifs pour la prestation de services au sein des fédérations d'identité qui mettent en œuvre le cadre technique.

2.1. Profils et spécifications pour SAML

Les fédérations d'identité conformes au cadre technique de Sweden Connect s'articulent autour du «profil de déploiement pour le cadre d'eID suédoise», [SAML.Profile]. Ce profil est influencé par le «profil de déploiement SAML V2.0 pour l'interopérabilité de fédération» [SAML2Int], mais ne dépend pas de manière prescriptive de celui-ci. [SAML.Profile] contient également des règles et des lignes directrices spécifiques au cadre technique de Sweden Connect.

2.1.1. Profil de déploiement pour le cadre d'eID suédoise

Le «profil de déploiement pour le cadre d'eID suédoise», [SAML.Profile], est le principal document de cadre technique et précise, entre autres:

- comment les métadonnées SAML doivent être construites et interprétées;
- la manière dont la requête d'authentification doit être formatée;
- la manière dont une requête d'authentification est traitée et dont un certificat d'identité est conçu, vérifié et traité;
- les exigences en matière de sécurité;
- les exigences SAML spécifiques pour les services de signature et «authentification pour signature».

2.1.2. Cadre d'eID suédoise – Registre des identifiants

La mise en œuvre d'une infrastructure d'eID suédoise nécessite différentes formes d'identifiants pour représenter les objets dans les structures de données. Le document «Sweden Connect – Registre des identifiants», [SC.Registry], définit la structure des identifiants attribués dans le cadre technique, ainsi qu'un registre des identifiants définis.

2.1.3. Spécification d'attribut pour le cadre d'eID suédoise

La spécification «spécification d'attribut pour le cadre d'eID suédoise», [SAML.Attributes], déclare les profils d'attribut SAML qui sont utilisés au sein des fédérations d'identité qui se conforment au cadre technique y compris ceux qui se connectent à l'eIDAS via le nœud eIDAS suédois.

2.1.4. Catégories d'entités pour le cadre d'eID suédoise

Les catégories d'entités sont utilisées au sein de la fédération à différentes fins:

- Catégories d'entités de service – Utilisées dans les métadonnées pour représenter les exigences des services électroniques en matière de niveaux d'assurance et d'attributs demandés, ainsi que le respect des niveaux d'assurance et la fourniture d'attributs par les services d'authentification.
- Catégories de propriétés de service – Utilisées pour représenter une caractéristique spécifique d'un service.
- Catégories d'entités de type de service – Utilisées pour représenter différents types de services au sein de la fédération.
- Catégories d'entités de contrats de services – Utilisées par les services pour annoncer les formulaires d'accord et autres.

- Catégories générales d’entités – Catégories d’entités qui ne relèvent d’aucun des types ci-dessus.

La spécification «catégories d’entités pour le cadre d’eID suédoise» [SAML.EntCat] spécifie les catégories d’entités définies par le cadre technique et décrit leur signification.

2.1.5 Spécification des attributs construits eIDAS pour le cadre d’eID suédoise

La spécification «spécification des attributs construits eIDAS pour le cadre d’eID suédoise», [SC.eIDAS.Attrs], spécifie les processus et les règles pour la construction des attributs ID basée sur les attributs reçus lors de l’authentification dans eIDAS.

2.1.6. Profil de mise en œuvre pour les fournisseurs d’identité BankID dans le cadre d’eID suédoise

La spécification «profil de mise en œuvre pour les fournisseurs d’identité BankID dans le cadre d’eID suédoise», [SAML.BankID], définit les règles sur la manière dont un service d’authentification qui met en œuvre la prise en charge de BankID est conçu.

> **Veuillez noter ce qui suit:** Cette spécification n’est pas prescriptive pour la conformité avec un cadre technique. Il n’est pertinent que pour les services d’authentification qui mettent en œuvre la prise en charge de BankID et les services électroniques qui les utilisent. Cependant, les services d’authentification qui mettent en œuvre la prise en charge de BankID et qui souhaitent se connecter à la fédération Sweden Connect doivent se conformer à cette spécification.

2.1.7. Sélection du principal dans les requêtes d’authentification SAML

La spécification «sélection du principal dans les requêtes d’authentification SAML», [SAML.Principal], définit une extension de SAML qui permet à une partie utilisatrice d’informer un service d’authentification de l’identité qu’elle souhaite authentifier.

2.1.8. Extension de message utilisateur dans les requêtes d’authentification SAML

La spécification «extension de message utilisateur dans les requêtes d’authentification SAML», [SAML.UMessage], définit une extension de SAML qui permet à une partie utilisatrice d’inclure un message d’affichage dans la requête d’authentification envoyée au service d’authentification. Le service d’authentification peut ensuite afficher ce message à l’utilisateur lors de l’étape d’authentification.

2.2. Profils et spécifications pour OpenID Connect

2.2.1. Profil OpenID Connect pour Sweden Connect

Le profil «profil OpenID Connect pour Sweden Connect», [OIDC.Profile], s’appuie sur le profil OpenID Connect suédois qui est un profil OpenID Connect développé par OIDC Sweden pour promouvoir l’interopérabilité et la sécurité au sein des solutions OIDC suédoises.

[OIDC.Profile] ajoute des exigences supplémentaires concernant la fédération Sweden Connect.

2.2.2. Spécification des revendications et des portées d'OpenID Connect pour Sweden Connect

La spécification «spécification des revendications et des portées d'OpenID Connect pour Sweden Connect», [OIDC.Claims], s'appuie sur la spécification «spécification des revendications et des portées pour le profil OpenID Connect suédois d'OICD Sweden».

2.3. Spécifications pour signature

Cette section contient des références aux documents définissant les services de signature au sein des fédérations qui sont conformes au cadre technique Sweden Connect.

2.3.1. Profil de mise en œuvre pour l'utilisation du DSS OASIS dans les services de signature centraux

Le profil de mise en œuvre «profil de mise en œuvre pour l'utilisation du DSS OASIS dans les services de signature centraux», [Sign.DSS.Profile], spécifie un profil pour la requête de signature et la réponse conformément à la norme OASIS «protocoles de base, éléments et liaisons du service de signature numérique», [DSS].

2.3.2. Extension du DSS pour les services de signature centraux fédérés

«Extension du DSS pour les services de signature centraux fédérés», [Sign.DSS.Ext], est une extension de la norme OASIS «protocoles de base, éléments et liaisons du service de signature numérique», [DSS], qui spécifie les définitions nécessaires à la signature dans le cadre technique.

2.3.3. Profil de certificat pour les certificats délivrés par les services de signature centraux

Le profil de certificat «profil de certificat pour les certificats délivrés par les services de signature centraux», [Sign.Cert.Profile], spécifie le contenu des certificats de signature. Ce profil applique une nouvelle extension de certificat pour prendre en charge les services de signature.

Ce profil fait référence à l'«extension du certificat du contexte d'authentification», [AuthContext], qui décrit la manière dont le «contexte d'authentification» est représenté dans les certificats X.509.

2.3.4. Protocole d'activation de signature pour la signature fédérée

La spécification «protocole d'activation de signature pour la signature fédérée», [Sign.Activation], définit un «protocole d'activation de signature» (PAS) pour la mise en œuvre de l'«assurance de contrôle exclusif de niveau 2» (SCAL2) conformément à la norme «prEN 419241 – systèmes fiables de serveur de signature électronique».

3. Liste de référence

3.1. DIGG

[Digg.Tillit]

Cadre de confiance pour l’identification électronique suédoise.

[SC.Registry]

Sweden Connect – Registre des identifiants.

[SAML.Profile]

Profil de déploiement pour le cadre d’eID suédoise

[SAML.Attributes]

Spécification d’attribut pour le cadre d’eID suédoise.

[SAML.EntCat]

Catégories d’entités pour le cadre d’eID suédoise

[SC.eIDAS.Attrs]

Spécification des attributs construits eIDAS pour le cadre d’eID suédoise.

[SAML.BankID]

Profil de mise en œuvre pour les fournisseurs d’identité BankID dans le cadre d’eID suédoise.

[SAML.Principal]

Sélection du principal dans les requêtes d’authentification SAML.

[SAML.UMessage]

Extension de message utilisateur dans les requêtes d’authentification SAML.

[OIDC.Profile]

Profil OpenID Connect pour Sweden Connect.

[OIDC.Claims]

Spécification des revendications et des portées d’OpenID Connect pour Sweden Connect.

[Sign.DSS.Profile]

Profil de mise en œuvre pour l'utilisation du DSS OASIS dans les services de signature centraux.

[Sign.DSS.Ext]

Extension DSS pour les services de signature centraux fédérés.

[Sign.Cert.Profile]

Profil des certificats délivrés par les services de signature centraux.

[Sign.Activation]

Protocole d'activation de signature pour la signature fédérée.

3.2. Autres références

[SAML2Int]

Profil de déploiement SAML V2.0 pour l'interopérabilité de la fédération.

[DSS]

Norme OASIS – Protocoles de base, éléments et liaisons du service de signature numérique Version 1.0, 11 avril 2007.

[AuthContext]

RFC-7773: Extension de certificat de contexte d'authentification.