Eine Einführung in den Technischen Rahmen von Sweden Connect

2024-12-04

Referenznummer: **2019-267**

Inhaltsverzeichnis

1. Einleitung

1.1. Übersicht

Der Technische Rahmen Sweden Connect ist für föderierte Identitäten auf Basis von SAML 2.0 angepasst.

> In der neuesten Version des technischen Rahmens wurden auch Spezifikationen für OpenID Connect eingeführt. Derzeit gibt es keine Föderationsunterstützung für OpenID Connect. Diese wird 2025 eingeführt.
>
> Die übrigen Teile dieses Dokuments beschreiben nur die SAML-Föderation. Sobald OpenID Connect vollständig eingeführt wurde, wird dieses Dokument auch diese Technologie abdecken.

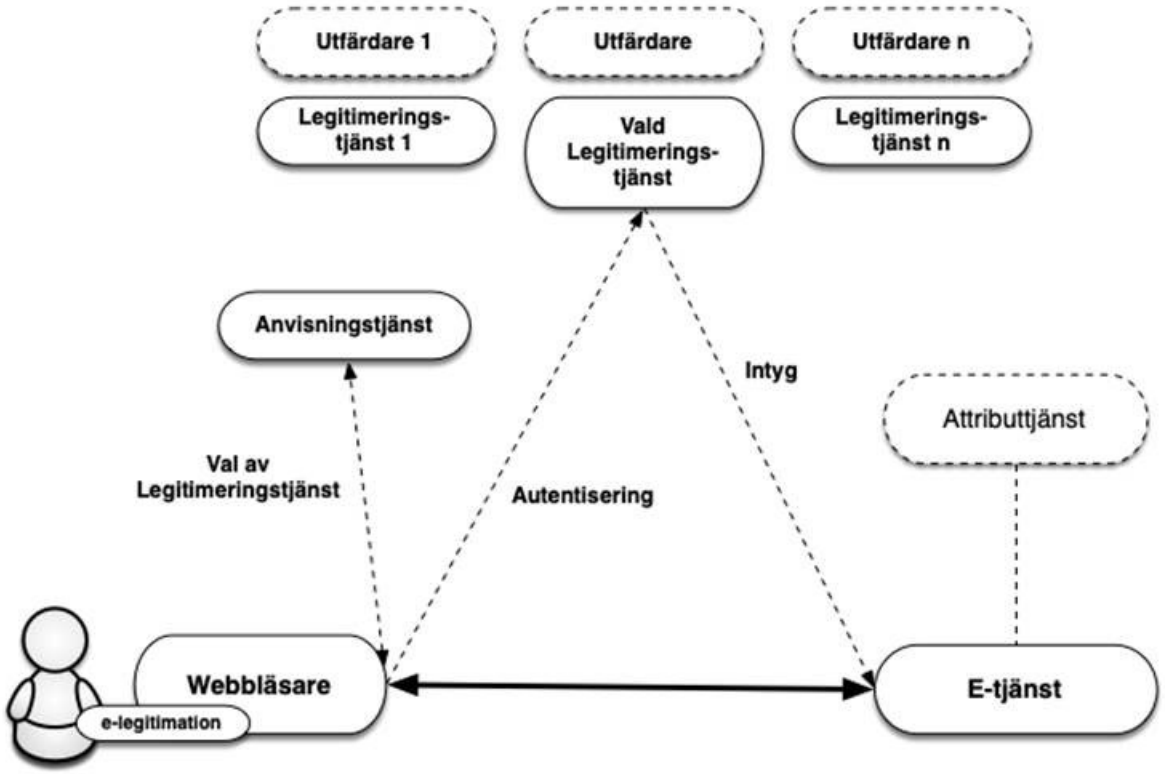
Vertrauende Parteien erhalten Identitätszertifikate in einem standardisierten Format von einem Authentifizierungsdienst[1].

E-Dienste, die eine Signatur erfordern, müssen nicht an die eID verschiedener Nutzer angepasst werden, um elektronische Signaturen zu erstellen. Stattdessen delegiert der E-Dienst dies an einen Signaturdienst, bei dem die Nutzer, unterstützt durch die Authentifizierung durch einen Authentifizierungsdienst, die Möglichkeit erhalten, elektronische Dokumente zu unterzeichnen.

Innerhalb der Föderation übernehmen E-Dienste und entsprechende vertrauende Parteien die Rolle des Service Provider (SP), während Authentifizierungsdienste, die Identitätszertifikate ausstellen, die Rolle des Identity Provider (IdP) und damit des Authentifizierers des Nutzers übernehmen, unabhängig davon, für welchen E-Dienst der Nutzer authentifiziert wird.

In den Fällen, in denen der elektronische Dienst mehr Informationen über den Nutzer benötigt, z. B. Informationen über die Rechtsfähigkeit, kann eine Frage an einen Attributdienst, die Attribute Authority (AA), innerhalb der Föderation gestellt werden, wenn ein solcher relevanter Attributdienst vorhanden ist. Durch eine Attributanfrage kann der elektronische Dienst die erforderlichen zusätzlichen Informationen erhalten, um den Nutzer zu autorisieren und Zugang zum elektronischen Dienst oder einem gleichwertigen Dienst zu gewähren.

Da sowohl personenbezogene Identitätsdaten als auch andere Attribute, die mit Nutzern verknüpft sind, über Identitätszertifikate und Attributzertifikate bereitgestellt werden, können alle Arten von eIDs, auf die sich vertrauende Parteien geeinigt haben und die Teil der Föderation sind, für die Authentifizierung gegenüber einem E-Dienst verwendet werden, der sowohl eine persönliche Identitätsnummer als auch zusätzliche Informationen erfordert, auch wenn die eID keine spezifischen personenbezogenen Daten enthält (z. B. Codeboxen für die Generierung von Einmalpasswörtern).



Utfärdare 1	Aussteller 1
Utfärdare n	Aussteller n
Legitimeringstjänst 1	Authentifizierungsdienst 1
Vald legitimeringstjänst	Ausgewählter Authentifizierungsdienst
Legitimeringstjänst n	Authentifizierungsdienst n
Anvisningstjänst	Erkennungsdienst
Intyg	Zertifikat
Val av legitimeringstjänst	Wahl des Authentifizierungsdienstes
autentisering	Authentifizierung
attributtjänst	Attributdienst
Webbläsare	Browser
E-tjänst	Elektronischer Dienst

Abbildung 1: *Darstellung der Kommunikation zwischen den verschiedenen Diensten innerhalb einer föderierten Identität.*

[1]: Der Authentifizierungsdienst wird auch in anderen Unterlagen von Digg als Identitätsdienst und Zertifizierungsdienst bezeichnet. In diesem Dokument wird jedoch nur der Begriff „Authentifizierungsdienst“ verwendet.

1.2. Vertrauensrahmen und Sicherheitsniveaus

Grundlage für die Anwendung der Sicherheitsstufe bei der Authentifizierung eines Nutzers ist das vom elektronischen Dienst geforderte Sicherheitsniveau für die elektronische Identifizierung. Damit diese Sicherheitsstufen im Rahmen der Föderation vergleichbar sind, sind im Sicherheitsrahmen für die schwedische elektronische Identifizierung [Digg.Tillit] vier

Sicherheitsniveaus (1-4) und in der eIDAS-Verordnung der EU drei Sicherheitsniveaus (niedrig, substanziell, hoch) festgelegt. Alle Aussteller von Identitätszertifikaten müssen nachweisen, dass der gesamte Prozess, der der Ausstellung von Identitätszertifikaten zugrunde liegt, die Anforderungen des erforderlichen Sicherheitsniveaus erfüllt, einschließlich:

- Anforderungen an die Erstellung des Identitätszertifikats;
- Anforderungen an die elektronische Identifizierung (Authentifizierung);
- Anforderungen an das Ausstellungsverfahren;
- Anforderungen an die eID selbst und ihre Verwendung;
- Anforderungen an den eID-Aussteller;
- Voraussetzung für die Feststellung der Identität des eID-Antragstellers.

1.3. Dienst für die Erfassung, Verwaltung und Veröffentlichung von Metadaten

Eine SAML-Föderation stellt über SAML-Metadaten Informationen über die Teilnehmer der Föderation bereit. Sowohl Entitäten, die Authentifizierungs- und Attributdienste in der Föderation erbringen, als auch vertrauende Parteien, d. h. Entitäten, die diese Dienste nutzen, z. B. E-Dienste, gelten als Teilnehmer an einer Föderation.

Die Metadaten der Föderation ermöglichen es den Teilnehmern, Informationen über die Dienste anderer Teilnehmer zu erhalten, einschließlich der Daten, die für den sicheren Informationsaustausch zwischen den Teilnehmern erforderlich sind. Metadaten müssen von jeder Partei und in Übereinstimmung mit den Vertragsbedingungen auf dem neuesten Stand gehalten werden.

Der Hauptzweck von Metadaten besteht darin, die Schlüssel/Zertifikate bereitzustellen, die für die sichere Kommunikation und den Informationsaustausch zwischen den Diensten erforderlich sind. Neben Schlüsseln enthalten Metadaten auch andere Informationen, die für die Interaktion zwischen Diensten wichtig sind, wie Adressen der erforderlichen Funktionen, Informationen über Sicherheitsniveaus, Dienstkategorien, Benutzeroberflächeninformationen usw.

Eine föderierte Identität wird durch ein Register im XML-Format definiert, das mit dem Zertifikat des Föderationsbetreibers signiert ist. Die Datei enthält Informationen über die Mitglieder der föderierten Identitäten, einschließlich ihrer Zertifikate. Da die Metadatendatei signiert ist, reicht es aus, ein Zertifikat mit seinem Metadaten-Gegenstück zu vergleichen. Eine Infrastruktur, die auf einem zentralen Föderationsregister basiert, erfordert, dass das Register kontinuierlich aktualisiert wird und dass die Föderationsmitglieder immer die neueste Version der Datei verwenden.

1.4. Erkennungsdienst

In einer föderierten Identität ist es möglich, einen gemeinsamen Erkennungsdienst anzubieten und zu nutzen, der die Authentifizierungsdienste auflistet, aus denen der Nutzer auswählen

kann. Der Zweck eines solchen Erkennungsdienstes besteht darin, die einzelnen E-Dienste, die Teil der föderierten Identität sind, von der Implementierung von Support in Bezug darauf zu entlasten, wie Nutzer den Authentifizierungsdienst (oder die Anmeldemethode) wählen.

Da der Erkennungsdienst innerhalb der föderierten Identität verfügbar ist, können E-Dienste ihre Nutzer dorthin leiten, um den Authentifizierungsdienst auszuwählen. Der Erkennungsdienst interagiert mit dem Nutzer, der seine Wahl trifft, und der Nutzer wird zusammen mit der Wahl des Nutzers zurück zum E-Dienst geleitet, der nun weiß, an welchen Authentifizierungsdienst der Nutzer zur Authentifizierung gesendet werden sollte.

> Derzeit gibt es keinen gemeinsamen Erkennungsdienst für die Sweden Connect-Föderation.

1.5. Integration bei der vertrauenden Partei

Vertrauensparteien, z. B. E-Dienste, integrieren sich über standardisierte Nachrichten in Authentifizierungsdienste und verwenden Identitätszertifikate, die ebenfalls standardisierte Formate haben.

Der Technische Rahmen Sweden Connect wird durch das Interoperabilitätsprofil „SAML V2.0 Deployment Profile for Federation Interoperability“ [SAML2Int] beeinflusst. Das Profil wird durch eine Reihe kommerzieller Produkte und Open-Source-Lösungen unterstützt, die die Integration bei E-Diensten erleichtern.

Viele elektronische Dienste verwenden eigenständige Authentifizierungslösungen, was bedeutet, dass die Anpassung der Integration an den technischen Rahmen nur begrenzte Auswirkungen auf den elektronischen Dienst als solchen hat.

1.6. Signatur

Bei der Unterzeichnung ermöglicht der Technische Rahmen Sweden Connect die Verwendung verschiedener Arten von eID, auch solcher, die nicht zertifikatsbasiert sind, ohne dass besondere Anpassungen im elektronischen Dienst erforderlich sind. Dies liegt daran, dass das elektronisch ausgestellte Identitätszertifikat (das zur Identifizierung von Nutzern bei der Unterzeichnung verwendet wird) unabhängig von der Art der vom Nutzer verwendeten eID das gleiche Format hat.

Ein Signaturdienst soll Signaturen innerhalb von föderierten Identitäten ermöglichen, die dem technischen Rahmen entsprechen, unterstützt durch alle Arten von eID, die ein ausreichendes Maß an Sicherheit bieten.

Durch die Beschaffung[1] und Einführung eines Signaturdienstes kann eine vertrauende Partei, die Teil der Föderation ist, es einem Nutzer ermöglichen, ein elektronisches Dokument mit Unterstützung des Signaturdienstes zu unterzeichnen. Die elektronische Signatur des Nutzers und das zugehörige Signaturzertifikat werden vom Signaturdienst erstellt, nachdem der Nutzer der Unterzeichnung zugestimmt hat, indem er sich gegenüber dem Signaturdienst authentifiziert[2].

[1]: Es ist auch möglich, einen Signaturdienst auf der Grundlage der Spezifikationen des technischen Rahmens zu implementieren oder anderweitig einen Signaturdienst zu erwerben.

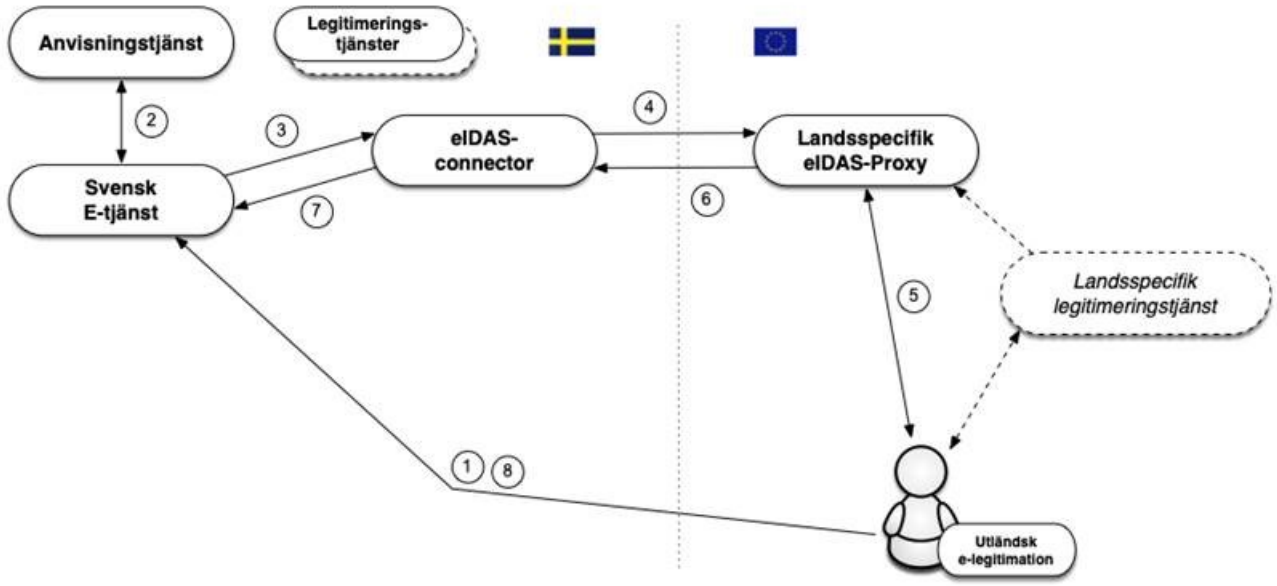
[2]: Es ist wichtig zu beachten, dass es von größter Bedeutung ist, dass der Nutzer diesen Prozess als Unterzeichnung eines Dokuments wahrnimmt. Daher sollte für die eIDs, die dies im Zusammenhang mit der „Authentifizierung zur Signatur“ unterstützen, ein Signaturfluss verwendet werden.

1.7. Technischer Rahmen und eIDAS

Die EU-Verordnung (910/2014) über elektronische Identifizierung und Vertrauensdienste, eIDAS, verpflichtet schwedische öffentliche Stellen, die von anderen eIDAS-Ländern gemeldeten eIDs anzuerkennen. Dies bedeutet, dass ein öffentlicher schwedischer elektronischer Dienst, der auf bestimmten Regeln basiert, in der Lage sein muss, ein Login zu akzeptieren, das mit einer in einem anderen Land ausgestellten eID durchgeführt wird.

1.7.1. Authentifizierung mit ausländischen eIDs

Die technischen Spezifikationen für eIDAS basieren wie der technische Rahmen auf SAML-Standards, und obwohl es viele Ähnlichkeiten gibt, gibt es auch Unterschiede in diesen Spezifikationen. Ein schwedischer elektronischer Dienst sollte sich jedoch nicht direkt auf die technischen Spezifikationen von eIDAS beziehen. Das Bild unten zeigt, wie der schwedische eIDAS-Knoten (*eIDAS-Connector*) als Brücke zwischen anderen Ländern und der schwedischen Föderation fungiert, wenn eine Person mit einer ausländischen eID in einem schwedischen E-Dienst authentifiziert wird. Der schwedische eIDAS-Knoten entspricht dem technischen Rahmen.



Anvisningstjänst	Erkennungsdienst
Legitimeringstjänster	Authentifizierungsdienste
Svensk E-tjänst	Schwedischer E-Dienst
EiDAS-connector	eIDAS-Connector

Landsspecifik Eidas Proxy	Länderspezifischer eIDAS-Proxy
Landsspecifik legitimeringstjänst	Länderspezifischer Authentifizierungsdienst
utländsk e-legitimation	Ausländische eID

Der Flow ist wie folgt:

1. Ein Nutzer mit einer ausländischen eID beantragt den Zugang zu einem schwedischen E-Dienst (d. h. er meldet sich an).

2. Der E-Dienst ermöglicht es dem Nutzer, die Anmeldemethode mithilfe eines Erkennungsdienstes auszuwählen. Es wird eine Option „Ausländische eID“ angezeigt, die vom Nutzer im eIDAS-Fall ausgewählt wird.

3. Der E-Dienst erstellt eine Authentifizierungsanforderung in Übereinstimmung mit diesem technischen Rahmen und leitet den Nutzer an den schwedischen eIDAS-Knoten (*Connector*), für den die DIGG verantwortlich ist. Der eIDAS-Knoten fungiert als Authentifizierungsdienst (*Identitätsanbieter*) in der Föderation gegenüber schwedischen vertrauenden Parteien, was bedeutet, dass die Kommunikation mit diesem Dienst auf die gleiche Weise erfolgt wie mit anderen Authentifizierungsdiensten innerhalb von Verbänden, die dem technischen Rahmen entsprechen.

4. Die eingegangene Anfrage wird bearbeitet, und der eIDAS-Knoten zeigt eine Auswahlseite an, auf der der Nutzer „sein Land“ [1] auswählt. Der schwedische eIDAS-Knoten wandelt nun die empfangene Authentifizierungsanforderung in eine eIDAS-Authentifizierungsanforderung um und leitet den Nutzer zum „eIDAS-Proxydienst“ des ausgewählten Landes weiter.

5. Geht die Authentifizierungsanforderung beim eIDAS-Proxydienst für das ausgewählte Land ein, übernimmt die Authentifizierungstechnologie dieses Landes. Nicht alle eIDAS-Länder verwenden SAML für die Authentifizierung, aber wenn dies in unserem Beispiel der Fall wäre, würde der Nutzer zu einem Authentifizierungsdienst weitergeleitet (*Identitätsanbieter*), und davor vielleicht auch zu einem Erkennungsdienst für die Auswahl des Authentifizierungsdienstes.

6. Sobald die Authentifizierung durchgeführt wurde, wird ein Zertifikat (*Assertion*) nach eIDAS-Spezifikationen erstellt. Dieses Zertifikat enthält eIDAS-spezifische Attribute, die den Nutzer identifizieren. Dieses Zertifikat wird nun an den schwedischen eIDAS-Knoten weitergeleitet.

7. Der Knoten erhält das Zertifikat und validiert dessen Richtigkeit. Dieses Zertifikat wird vom eIDAS-Format in ein nach dem technischen Rahmen formatiertes Zertifikat umgewandelt und an den E-Dienst gesendet.

8. Die vertrauende Partei fügt zusätzliche Informationen hinzu und legt fest, ob dem Nutzer Zugriff auf den Dienst gewährt werden soll.

Schwedische elektronische Dienste müssen daher nur den technischen Rahmen unterstützen, um eine mit einer europäischen eID durchgeführte Authentifizierung zu handhaben. Der

elektronische Dienst muss jedoch in der Lage sein, mit der vorgelegten Identität umzugehen, bei der es sich nicht unbedingt um eine persönliche Identitätsnummer handelt. So kann es Fälle geben, in denen ein elektronischer Dienst einen Nutzer über den eIDAS-Rahmen authentifiziert, die präsentierte Identität des Nutzers jedoch nicht im elektronischen Dienst verwendet werden kann. Mehr dazu in Kapitel 1.7.3 unten.

> [1]: Tatsächlich wählt der Nutzer den „eIDAS-Proxydienst“, an den die Anfrage weitergeleitet werden soll. Dies hängt von dem Land ab, dem der Aussteller der eID des Nutzers angehört.

1.7.2. Signaturen mit ausländischen eIDs

Wie bereits beschrieben, wird innerhalb dieses technischen Rahmens ein Modell für die elektronische Signatur angewendet, das als föderierte Signatur bezeichnet wird. Ein serverbasierter Signaturdienst ist mit dem E-Dienst verknüpft, der wiederum eine Signatur anfordert. Wenn ein Nutzer ein Dokument signiert, sendet der E-Dienst eine Signaturanfrage an den Signaturdienst. Der Signaturdienst fordert den Nutzer dann auf, sich zu authentifizieren. Im Zusammenhang mit der Authentifizierung genehmigt der Nutzer die Signatur. Der Signaturdienst sendet Daten an den E-Dienst zurück, und dann werden die Signaturdaten, die dem signierten Dokument zugeordnet sind, gespeichert.

Dieses Verfahren ermöglicht es, auch mit einer ausländischen eID zu signieren, da der Signaturdienst beschließen kann, den Nutzer mit einer ausländischen eID gemäß dem oben in Abschnitt 1.7.1 beschriebenen Verfahren zu authentifizieren.

Bei der Unterzeichnung ist in diesem Fall der schwedische eIDAS-Knoten dafür verantwortlich, den Nutzer darüber zu informieren, dass der Zweck der Authentifizierung darin besteht, ein Dokument zu unterzeichnen, wer die Signatur angefordert hat, und alle Informationen darüber, was signiert wird. Ein Identitätszertifikat wird erst ausgestellt, wenn sich der Nutzer authentifiziert hat (für die Signatur), und dieses wird an den Signaturdienst gesendet, der wiederum die Signatur generiert.

1.7.3. Verwaltung von Identitäten

Identitätszertifikate aus anderen Ländern entsprechen den EU-weiten technischen Spezifikationen, die im Rahmen der eIDAS-Verordnung entwickelt wurden. Die Attribute, die jedes Land sowohl für natürliche Personen als auch für Organisationen („Minimum Dataset“, MDS) stets enthalten muss, sind in dieser Verordnung festgelegt. Jedes Land muss eine eindeutige Kennung pro eID vorsehen, die nur eine natürliche Person repräsentiert. Aus einigen Ländern werden diese Kennungen eindeutig und dauerhaft pro Person sein, wie beispielsweise schwedische persönliche Identitätsnummern, aber diese Kennungen können sehr unterschiedliche Zusammensetzungen und Merkmale aufweisen. Ein Merkmal, das variieren kann, ist die Persistenz einer solchen Kennung, d. h. ob eine solche Kennung zu Lebzeiten einer Person unverändert bleibt oder sich ändert, wenn die Person beispielsweise in eine andere Region zieht, ihren Namen ändert oder nur ihre eID ändert. In einigen Ländern (z. B. im Vereinigten Königreich) hängt die Kennung davon ab, welche der eIDs des Landes ein Nutzer derzeit verwendet.

Um die Verwaltung von Nutzern in schwedischen E-Diensten zu vereinfachen, generiert der schwedische eIDAS-Knoten ein standardisiertes ID-Attribut für Nutzer, die mit einer

ausländischen eID authentifiziert wurden, bekannt als *provisional ID* (abgekürzt PRID). Darüber hinaus wird ein zugehöriges Attribut erstellt, das die erwartete Persistenz oder Lebensdauer dieses ID-Attributs angibt. Das PRID-Attribut wird auf der Grundlage der Attributwerte generiert, die aus der ausländischen Authentifizierung gemäß den für das jeweilige Land festgelegten Methoden erhalten wurden. Jede Kombination aus Land und Methode wird in Bezug auf die erwartete Persistenz kategorisiert, d. h. wie wahrscheinlich es ist, dass sich eine Identität im Laufe der Zeit für dieselbe Person ändert. Dies ermöglicht es schwedischen E-Diensten, die Kommunikation mit dem Nutzer anzupassen und proaktiv Funktionen bereitzustellen, die es einem Nutzer, dessen Identität sich geändert hat, erleichtern, die Kontrolle über seine Informationen im E-Dienst wiederzuerlangen.

In einigen Fällen kann eine Person, die mit einer ausländischen eID authentifiziert wurde, auch eine schwedische persönliche Identitätsnummer besitzen. Dies kann beispielsweise ein schwedischer Staatsbürger sein, der ins Ausland gezogen ist und eine ausländische eID erhalten hat, oder ein ausländischer Staatsbürger, der in Schweden registriert ist und eine persönliche Identitätsnummer erhalten hat.

Die Tatsache, dass eine Person mit einer ausländischen eID eine schwedische persönliche Identitätsnummer hat, ist dem ausländischen Authentifizierungsdienst normalerweise nicht bekannt, und diese Informationen sind daher nicht im Identitätszertifikat des Landes enthalten, in dem die Person authentifiziert ist. Der schwedische Knoten hingegen hat die Möglichkeit, einen Attributdienst in Schweden abzufragen[1], ob es eine registrierte persönliche Identitätsnummer für die authentifizierte Person gibt, und kann, wenn dies der Fall ist, diese Informationen dem Identitätszertifikat hinzufügen, die an den elektronischen Dienst gesendet wird.

> [1]: Zum Zeitpunkt des Schreibens gibt es keinen Attributdienst, der eine Verbindung zwischen eIDAS-Identitäten und schwedischen persönlichen Identitätsnummern herstellt.

1.7.4. Schwedische eIDs in ausländischen E-Diensten

Schweden hat schwedische eIDs auf den Sicherheitsniveaus „substanziell“ und „hoch“ gemäß eIDAS notifiziert.

Ein Antrag auf Authentifizierung von einem ausländischen E-Dienst wird über einen eIDAS-Connector im Land des E-Dienstes an den schwedischen eIDAS-Knoten (Proxy-Dienst) gestellt. Im schwedischen eIDAS-Knoten wählt der Nutzer aus, mit welcher schwedischen eID er sich authentifizieren möchte, und dann wird eine Authentifizierungsanforderung an den Authentifizierungsdienst (*Identity Provider*) gesendet, der die ausgewählte eID verarbeitet. Diese Anforderung ist nach einem technischen Rahmen formatiert, was bedeutet, dass ein schwedischer Authentifizierungsdienst die technischen Spezifikationen von eIDAS nicht erfüllen muss.

Der Nutzer wird vom schwedischen Authentifizierungsdienst authentifiziert und es wird ein Identitätszertifikat ausgestellt (gemäß dem technischen Rahmen). Dieses Zertifikat wird vom schwedischen eIDAS-Proxydienst empfangen und in ein Zertifikat nach eIDAS-Spezifikationen umgewandelt, bevor es an den ausländischen eIDAS-Connector und dann an den aufrufenden E-Dienst weitergeleitet wird (*Service Provider*).

2. Technische Spezifikationen

Dieses Kapitel enthält Spezifikationen und Profile für föderierte Identitäten, die dem Technischen Rahmen von Sweden Connect und bestimmten damit verbundenen Diensten entsprechen. Sofern nicht anders angegeben, sind diese Dokumente für die Erbringung von Dienstleistungen innerhalb von föderierten Identitäten, die den technischen Rahmen implementieren, verbindlich.

2.1. Profile und Spezifikationen für SAML

Föderierte Identitäten, die dem Technischen Rahmen von Sweden Connect entsprechen, basieren auf dem „Deployment Profile for the Swedish eID Framework“, [SAML.Profile]. Dieses Profil wird durch das „SAML V2.0 Deployment Profile for Federation Interoperability“ [SAML2Int] beeinflusst, ist aber nicht präskriptiv davon abhängig. [SAML.Profile] enthält auch spezifische Regeln und Leitlinien für den Technischen Rahmen von Sweden Connect.

2.1.1. Deployment Profile for the Swedish eID Framework

„Deployment Profile for the Swedish eID Framework“, [SAML.Profile], ist das wichtigste technische Rahmendokument und legt unter anderem Folgendes fest:

- wie SAML-Metadaten konstruiert und interpretiert werden;
- wie der Authentifizierungsantrag zu formatieren ist;
- wie mit einem Authentifizierungsantrag umzugehen ist und wie ein Identitätszertifikat zu gestalten, zu überprüfen und zu behandeln ist;
- Sicherheitsanforderungen;
- spezifische SAML-Anforderungen für Signaturdienste und „Authentifizierung für Signaturen“.

2.1.2. Swedish eID Framework – Registry for identifiers

Die Implementierung einer schwedischen eID-Infrastruktur erfordert verschiedene Formen von Kennungen, um Objekte in Datenstrukturen darzustellen. Das Dokument „Sweden Connect – Registry for identifiers“, [SC.Registry], definiert die Struktur der im technischen Rahmen zugewiesenen Kennungen sowie ein Register definierter Kennungen.

2.1.3. #Attribute Specification for the Swedish eID Framework

Die Spezifikation „Attribute Specification for the Swedish eID Framework“, [SAML.Attributes], deklariert die SAML-Attributprofile, die innerhalb von föderierten Identitäten verwendet werden, die dem technischen Rahmen entsprechen, einschließlich derjenigen, die über den schwedischen eIDAS-Knoten mit eIDAS verbunden sind.

2.1.4. Entity Categories for the Swedish eID Framework

Entitätskategorien (Entity Categories) werden innerhalb der Föderation für eine Reihe verschiedener Zwecke verwendet:

- Service Entity Categories – wird in Metadaten verwendet, um die Anforderungen elektronischer Dienste an Sicherheitsniveaus und angeforderte Attribute sowie die Erfüllung von Sicherheitsniveaus und die Bereitstellung von Attributen durch Authentifizierungsdienste darzustellen.

- Service Property Categories – wird verwendet, um ein spezifisches Merkmal einer Dienstleistung darzustellen.

- Service Type Entity Categories – wird verwendet, um verschiedene Diensttypen innerhalb der Föderation darzustellen.

- Service Contract Entity Categories – werden von Dienstleistungen verwendet, um Vertragsformulare und dergleichen anzukündigen.

- General Entity Categories – Entitätskategorien, die nicht unter eine der oben genannten Arten fallen.

Die Spezifikation „Entity Categories for the Swedish eID Framework“ [SAML.EntCat] spezifiziert die durch den technischen Rahmen definierten Entitätskategorien und beschreibt deren Bedeutung.

2.1.5. eIDAS Constructed Attributes Specification for the Swedish eID Framework

Die Spezifikation „eIDAS Constructed Attributes Specification for the Swedish eID Framework“, [SC.eIDAS.Attrs], spezifiziert Prozesse und Regeln für die Konstruktion von ID-Attributen basierend auf Attributen, die während der Authentifizierung in eIDAS erhalten werden.

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

Die Spezifikation „Implementation Profile for BankID Identity Providers within the Swedish eID Framework“, [SAML.BankID], definiert Regeln dafür, wie ein Authentifizierungsdienst, der Unterstützung für BankID implementiert, entworfen werden soll.

> **Bitte beachten Sie Folgendes:** Diese Spezifikation ist nicht präskriptiv für die Einhaltung eines technischen Rahmens. Sie ist nur für Authentifizierungsdienste relevant, die Unterstützung für BankID und E-Dienste implementieren, die diese nutzen. Authentifizierungsdienste, die Unterstützung für BankID implementieren und sich mit der Sweden Connect-Föderation verbinden möchten, müssen jedoch dieser Spezifikation entsprechen.

2.1.7. Principal Selection in SAML Authentication Requests

Die Spezifikation „Principal Selection in SAML Authentication Requests“, [SAML.Principal], definiert eine Erweiterung von SAML, die es einer vertrauenden Partei

ermöglicht, einem Authentifizierungsdienst mitzuteilen, welche Identität sie authentifizieren möchte.

2.1.8. User Message Extension in SAML Authentication Requests

Die Spezifikation „User Message Extension in SAML Authentication Requests“, [SAML.UMessage], definiert eine SAML-Erweiterung, die es einer vertrauenden Partei ermöglicht, eine Anzeigenachricht in die an den Authentifizierungsdienst gesendete Authentifizierungsanforderung aufzunehmen. Der Authentifizierungsdienst kann dem Nutzer diese Nachricht dann während des Authentifizierungsschritts anzeigen.

2.2. Profile und Spezifikationen für OpenID Connect

2.2.1. OpenID Connect Profile for Sweden Connect

Das Profil „OpenID Connect Profile for Sweden Connect“, [OIDC.Profil], baut auf The Swedish OpenID Connect Profile auf, das ein OpenID Connect-Profil ist, das von OIDC Schweden entwickelt wurde, um Interoperabilität und Sicherheit innerhalb schwedischer OIDC-Lösungen zu fördern.

[OIDC.Profile] fügt zusätzliche Anforderungen in Bezug auf die Föderation Sweden Connect hinzu.

2.2.2. OpenID Connect Claims and Scopes Specification for Sweden Connect

Die Spezifikation „OpenID Connect Claims and Scopes Specification for Sweden Connect“, [OIDC.Claims], baut auf der Spezifikation Claims and Scopes Specification for the Swedish OpenID Connect Profile von OIDC Schweden auf.

2.3. Spezifikationen für die Signatur

Dieser Abschnitt enthält Verweise auf die Dokumente, in denen Signaturdienste innerhalb von Föderationen definiert werden, die dem Technischen Rahmen von Sweden Connect entsprechen.

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

Das Umsetzungsprofil „Implementation Profile for using OASIS DSS in Central Signing Services“, [Sign.DSS.Profile], spezifiziert ein Profil für die Signaturanforderung und -antwort nach dem OASIS-Standard „Digital Signature Service Core Protocols, Elements, and Bindings“, [DSS].

2.3.2. DSS Extension for Federated Central Signing Services

„DSS Extension for Federated Central Signing Services“, [Sign.DSS.Ext], ist eine Erweiterung des OASIS-Standards „Digital Signature Service Core Protocols, Elements, and Bindings“, [DSS], der die für die Unterzeichnung innerhalb des technischen Rahmens erforderlichen Definitionen festlegt.

2.3.3. Certificate Profile for Certificates Issued by Central Signing Services

Das Zertifikatsprofil „Certificate profile for certificates issued by Central Signing services“, [Sign.Cert.Profile], spezifiziert den Inhalt von Signierzertifikaten. Dieses Profil wendet eine neue Zertifikaterweiterung an, um Signaturdienste zu unterstützen.

Dieses Profil bezieht sich auf die „Authentication Context Certificate Extension“, [AuthContext], die beschreibt, wie der „Authentication Context“ in X.509-Zertifikaten dargestellt wird.

2.3.4. Signature Activation Protocol for Federated Signing

Die Spezifikation „Signature Activation Protocol for Federated Signing“, [Sign.Activation], definiert ein „Signature Activation Protocol“ (SAP) für die Implementierung von „Sole Control Assurance Level 2“ (SCAL2) gemäß der Norm „prEN 419241 – Trustworthy Systems Supporting Server Signing“.

3. Referenzliste

3.1. DIGG

[Digg.Tillit]

Vertrauensrahmen für die schwedische elektronische Identifizierung.

[SC.Registry]

Sweden Connect – Registry for identifiers.

[SAML.Profile]

Deployment Profile for the Swedish eID Framework.

[SAML.Attributes]

Attribute Specification for the Swedish eID Framework.

[SAML.EntCat]

Entity Categories for the Swedish eID Framework.

[SC.eIDAS.Attrs]

eIDAS Constructed Attributes Specification for the Swedish eID Framework.

[SAML.BankID]

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

[SAML.Principal]

Principal Selection in SAML Authentication Requests.

[SAML.UMessage]

User Message Extension in SAML Authentication Requests.

[OIDC.Profile]

OpenID Connect Profile for Sweden Connect.

[OIDC.Claims]

OpenID Connect Claims and Scopes Specification for Sweden Connect.

[Sign.DSS.Profile]

Implementation Profile for Using OASIS DSS in Central Signing Services.

[Sign.DSS.Ext]

DSS Extension for Federated Central Signing Services.

[Sign.Cert.Profile]

Certificate profile for certificates issued by Central Signing services.

[Sign.Activation]

Signature Activation Protocol for Federated Signing.

3.2. Sonstige Referenzen

[SAML2Int]

SAML V2.0 Deployment Profile for Federation Interoperability.

[DSS]

OASIS Standard – Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0, 11. April 2007.

[AuthContext]

RFC-7773: Authentication Context Certificate Extension.