Una introducción al marco técnico Sweden Connect

04-12-2024

Número de referencia: **2019-267**

Índice

1. Introducción

1.1. Visión general

El marco técnico de Sweden Connect está adaptado para federaciones de identidad con base en la autenticación SAML 2.0.

> En la última versión del marco técnico, también se han introducido especificaciones para OpenID Connect. Actualmente, no hay soporte de federación para OpenID Connect. Esto se introducirá en 2025.
>
> Las partes restantes de este documento solo describen la federación de SAML. Una vez que OpenID Connect se haya introducido por completo, este documento también cubrirá esta tecnología.

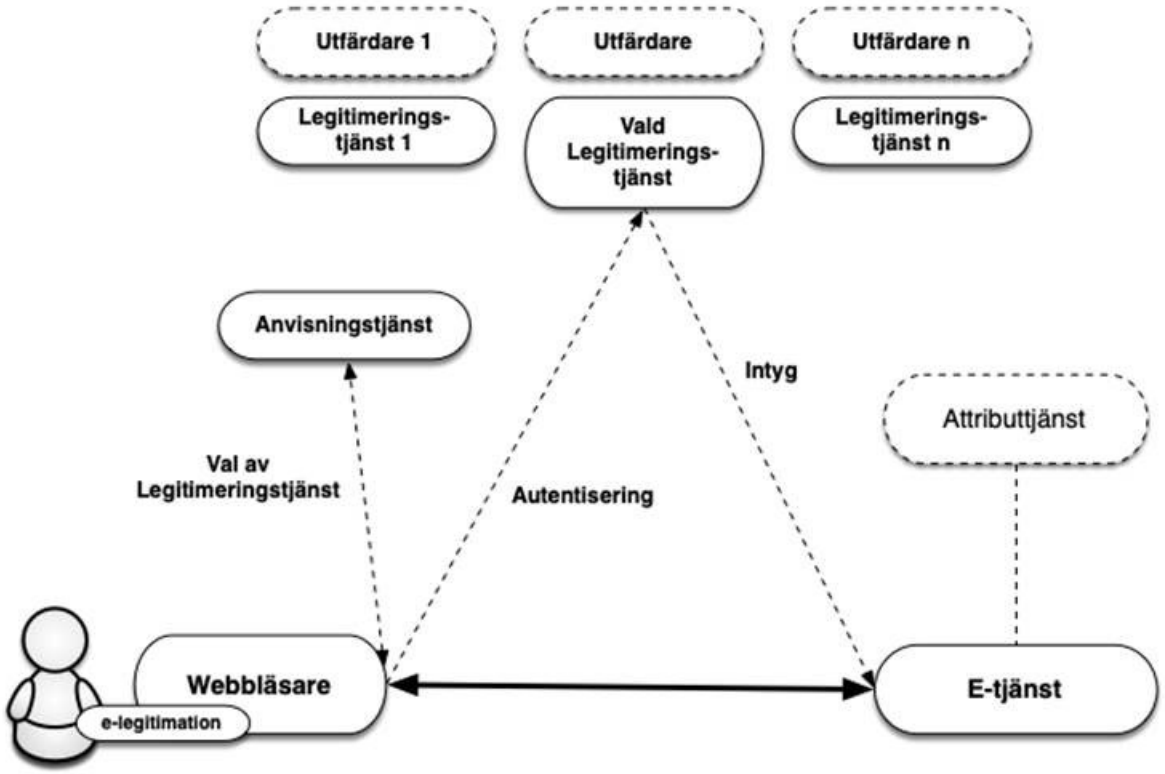
Las partes usuarias reciben certificados de identidad en un formato normalizado de un servicio de autenticación[1].

Los servicios electrónicos que requieren una firma no necesitan adaptarse a las distintas identificaciones electrónicas (eID) de los usuarios para crear firmas electrónicas. En cambio, el servicio electrónico delega esto en un servicio de firma, donde los usuarios, apoyados por la autenticación a través de un servicio de autenticación, tienen la oportunidad de firmar documentos electrónicos.

Dentro de la federación, los servicios electrónicos y las partes usuarias correspondientes asumen el papel de proveedor de servicios (*Service Provider*, SP, por su versión en inglés), mientras que los servicios de autenticación que emiten certificados de identidad asumen el papel de proveedor de identidad (*Identity Provider*, IdP, por su versión en inglés) y, por lo tanto, el autenticador del usuario, independientemente del servicio electrónico para el que se autentica el usuario.

En los casos en que el servicio electrónico necesite más información sobre el usuario, por ejemplo, información sobre la capacidad jurídica, puede formularse una pregunta a un servicio de atributos, la autoridad de atributos (*Attribute Authority*, AA, por su versión en inglés), dentro de la federación, si existe dicho servicio de atributos pertinente. A través de una solicitud de atributos, el servicio electrónico puede obtener la información adicional necesaria para autorizar al usuario y proporcionar acceso al servicio electrónico o equivalente.

Dado que tanto los datos de identidad personal como otros atributos asociados con los usuarios se proporcionan a través de certificados de identidad y certificados de atributos, todos los tipos de identificación electrónica (eID) con los que las partes usuarias tienen un acuerdo y que forman parte de la federación pueden utilizarse para la autenticación con respecto a un servicio electrónico que requiere tanto un número de identidad personal como información adicional, incluso si la identificación electrónica (eID) no contiene ningún dato personal específico (por ejemplo, casillas de código para la generación de contraseñas únicas).



Utfärdare 1	Emisor 1
Utfärdare n	Emisor n.º
Legitimeringstjänst 1	Servicio de autenticación 1
Vald legitimeringstjänst	Servicio de autenticación seleccionado
Legitimeringstjänst n	Servicio de autenticación n
Anvisningstjänst	Servicio de localización
Intyg	Certificado
Val av legitimeringstjänst	Elección del servicio de autenticación
autentisering	Autenticación
attributtjänst	Servicio de atributos
Webbläsare	Navegador
E-tjänst	Servicio electrónico

Figura 1 *Ilustración de la comunicación entre los diferentes servicios dentro de una federación de identidades.*

> [1]: El servicio de autenticación también se menciona en otra documentación de la Digg como un servicio de identidad y un servicio de certificación. En este documento, sin embargo, solo se utiliza el término «servicio de autenticación».

1.2. Marco de confianza y niveles de seguridad

La base para la aplicación del nivel de seguridad cuando se autentica a un usuario es el nivel de garantía de la identificación electrónica que exige el servicio electrónico. Para que estos niveles de seguridad sean comparables en el marco de la federación, se definen cuatro niveles de seguridad (1 a 4) en el marco de confianza para la identificación electrónica sueca

[Digg.Tillit] y tres niveles de seguridad (bajo, sustancial, alto) en el Reglamento eIDAS de la UE. Todos los emisores de certificados de identidad deben demostrar que todo el proceso en el que se basa la expedición de certificados de identidad cumple los requisitos del nivel de seguridad requerido, entre ellos:

- requisitos para la creación del certificado de identidad;
- requisitos para la identificación electrónica (autenticación);
- requisitos para el proceso de emisión;
- requisitos para la propia identificación electrónica (eID) y su uso;
- requisitos para el emisor de la identificación electrónica (eID);
- requisito para establecer la identidad del solicitante de la identificación electrónica (eID).

1.3. Servicio de recogida, administración y publicación de metadatos

Una federación de SAML proporciona información sobre los participantes de la federación a través de los metadatos de SAML. Tanto las entidades que proporcionan servicios de autenticación y atributos en la federación como las partes usuarias, es decir, las entidades que consumen estos servicios, por ejemplo, los servicios electrónicos, se consideran participantes de una federación.

Los metadatos de la federación permiten a los participantes obtener información sobre los servicios de otros participantes, incluidos los datos necesarios para el intercambio seguro de información entre los participantes. Los metadatos deben mantenerse actualizados por cada parte y de acuerdo con las condiciones contractuales.

El objetivo principal de los metadatos es proporcionar las claves o los certificados necesarios para la comunicación segura y el intercambio de información entre servicios. Además de las claves, los metadatos también contienen otra información que es importante para la interacción entre servicios, como direcciones de funciones requeridas, información sobre niveles de seguridad, categorías de servicios, información de interfaz de usuario, etc.

Una federación de identidades se define mediante un registro en formato XML firmado con el certificado del operador de la federación. El archivo contiene información sobre los miembros de la federación de identidades, incluidos sus certificados. Dado que el archivo de metadatos está firmado, es suficiente comparar un certificado con su contraparte de metadatos. Una infraestructura basada en un registro de federación central requiere que el registro se actualice continuamente y que los miembros de la federación siempre usen la última versión del archivo.

1.4. Servicio de localización

En una federación de identidades, es posible ofrecer y consumir un servicio de localización compartido, que enumera los servicios de autenticación disponibles para que el usuario elija. El propósito de tal servicio de localización es liberar los servicios electrónicos individuales

que forman parte de la federación de identidades de implementar soporte con respecto a cómo los usuarios eligen el servicio de autenticación (o método de inicio de sesión).

Dado que el servicio de localización está disponible dentro de la federación de identidades, los servicios electrónicos pueden dirigir a sus usuarios allí para elegir el servicio de autenticación. El servicio de localización interactúa con el usuario que hace su elección, y el usuario, junto con la elección del usuario, se dirige de nuevo al servicio electrónico, que a continuación sabe a qué servicio de autenticación debe enviarse al usuario para su autenticación.

> Actualmente no existe un servicio de localización compartido para la federación Sweden Connect.

1.5. Integración en la parte usuaria

Las partes usuarias, por ejemplo los servicios electrónicos, se integran con los servicios de autenticación a través de mensajes normalizados y consumen certificados de identidad que también tienen formatos normalizados.

El marco técnico Sweden Connect se ve influido por el perfil de interoperabilidad «SAML V2.0 Deployment Profile for Federation Interoperability» [SAML2Int] (Perfil de implementación para la interoperabilidad de la federación). El perfil está respaldado por una serie de productos comerciales y soluciones de código abierto, lo que facilita la integración en los servicios electrónicos.

Muchos servicios electrónicos utilizan soluciones de autenticación independientes, lo que significa que adaptar la integración para cumplir el marco técnico tiene un impacto limitado en el servicio electrónico como tal.

1.6. Firma

Al firmar, el marco técnico Sweden Connect permite utilizar diferentes tipos de identificación electrónica, incluso aquellos que no están basados en certificados, sin la necesidad de adaptaciones especiales en el servicio electrónico. Esto se debe a que el certificado de identidad emitido electrónicamente (utilizado para la identificación de los usuarios al firmar) tiene el mismo formato, independientemente del tipo de identificación electrónica utilizada por el usuario.

Un servicio de firma tiene como objetivo habilitar firmas dentro de federaciones de identidades que cumplan con el marco técnico, con el apoyo de todos los tipos de identificación electrónica que ofrecen un grado suficiente de seguridad.

Mediante la contratación[1] e introducción de un servicio de firma, una parte usuaria que forme parte de la federación puede permitir que un usuario firme un documento electrónico con el apoyo del servicio de firma. El servicio de firma crea la firma electrónica del usuario y el certificado de firma asociado después de que el usuario haya aceptado firmar autenticándose ante el servicio de firma[2].

> [1]: También es posible implementar un servicio de firma basado en las especificaciones del marco técnico, o adquirir de otro modo un servicio de firma.

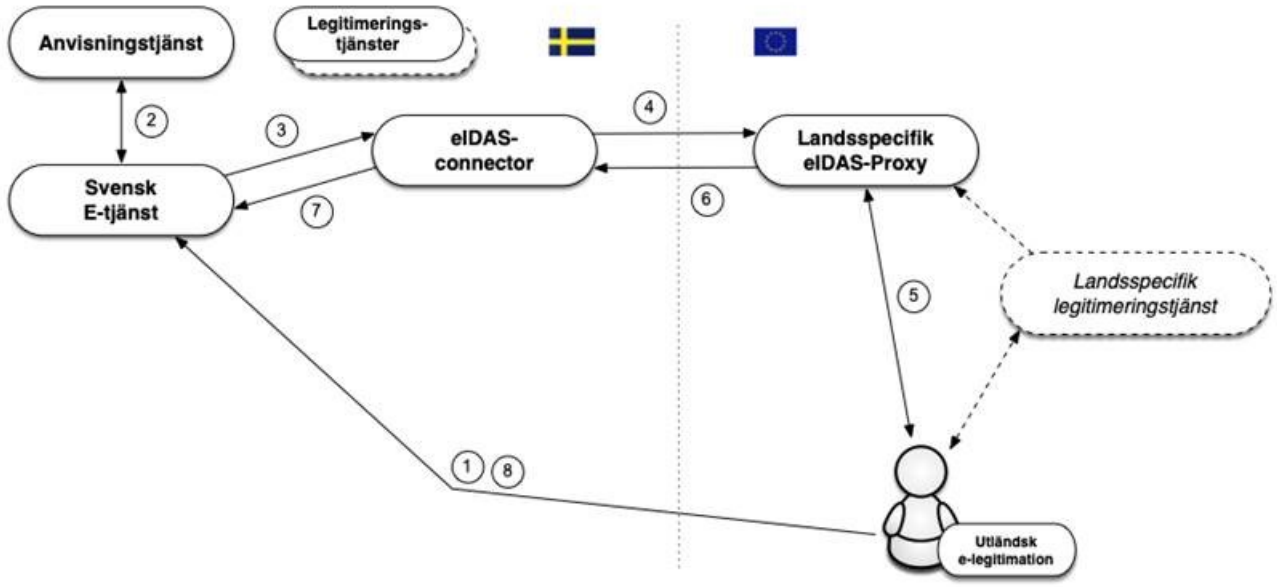
[2]: Es importante tener en cuenta que es de suma importancia que el usuario perciba este proceso como la firma de un documento. Por lo tanto, debe utilizarse un flujo de firma para las identificaciones electrónicas (eID) que lo admitan en relación con la «autenticación para la firma».

1.7. Marco técnico y eIDAS

El Reglamento (UE) n.º 910/2014 relativo a la identificación electrónica y los servicios de confianza, eIDAS, exige que los organismos públicos suecos reconozcan las identificaciones electrónicas (eID) que otros países eIDAS han notificado. Esto significa que un servicio electrónico público sueco basado en ciertas normas debe poder aceptar un inicio de sesión realizado utilizando una identificación electrónica emitida en otro país.

1.7.1. Autenticación mediante identificaciones electrónicas (eID) extranjeras

Las especificaciones técnicas para eIDAS se basan, al igual que el marco técnico, en normas de SAML, y aunque hay muchas similitudes, también hay diferencias en estas especificaciones. Sin embargo, un servicio electrónico sueco no debe estar directamente relacionado con las especificaciones técnicas eIDAS. La siguiente imagen ilustra cómo el nodo sueco eIDAS (*eIDAS-connector*) (conexión eIDAS, por su versión en inglés) actúa como puente entre otros países y la federación sueca cuando una persona está siendo autenticada utilizando una identificación electrónica extranjera en un servicio electrónico sueco. El nodo sueco eIDAS cumple el marco técnico.



Anvisningstjänst	Servicio de localización
Legitimeringstjänster	Servicios de autenticación
Svensk E-tjänst	Servicio electrónico sueco
EiDAS-connector	*eIDAS-connector*
Landsspecifik Eidas Proxy	*Proxy* eIDAS específico de cada país
Landsspecifik legitimeringstjänst	Servicio de autenticación específico del país
utländsk e-legitimation	Identificación electrónica (eID) extranjera

El flujo es el siguiente:

1. Un usuario con una identificación electrónica extranjera solicita acceso a un servicio electrónico sueco (es decir, inicia sesión).

2. El servicio electrónico permite al usuario elegir el método de inicio de sesión mediante un servicio de localización. Aparece una opción «*Foreign eID*» [identificación electrónica (eID) extranjera, por su versión en inglés], que es seleccionada por el usuario en el caso de eIDAS.

3. El servicio electrónico crea una solicitud de autenticación de conformidad con este marco técnico y dirige al usuario al nodo eIDAS sueco (*connector*) del que es responsable la DIGG. El nodo eIDAS actúa como un servicio de autenticación (*Identity Provider*) en la federación frente a las partes usuarias suecas, lo que significa que la comunicación con este servicio se lleva a cabo de la misma manera que con otros servicios de autenticación dentro de las federaciones que cumplen el marco técnico.

4. La solicitud recibida se procesa y el nodo eIDAS muestra una página de selección en la que el usuario selecciona «su país»[1]. El nodo eIDAS sueco convierte a continuación la solicitud de autenticación recibida en una solicitud de autenticación eIDAS y dirige al usuario al «servicio *proxy* eIDAS» del país seleccionado.

5. Cuando la solicitud de autenticación es recibida por el servicio *proxy* eIDAS para el país seleccionado, la tecnología de autenticación de este país se hace cargo. No todos los países eIDAS utilizan SAML para la autenticación, pero si este fuera el caso en nuestro ejemplo, el usuario sería redirigido a un servicio de autenticación (*Identity Provider*) y antes de eso tal vez también a un servicio de localización para la selección del servicio de autenticación.

6. Una vez realizada la autenticación, se crea un certificado (*Assertion*) (declaración de validación, por su versión en inglés) de acuerdo con las especificaciones eIDAS. Este certificado incluye atributos específicos eIDAS que identifican al usuario. Este certificado se envía a continuación al nodo eIDAS sueco.

7. El nodo recibe el certificado y valida su exactitud. Este certificado se transforma del formato eIDAS a un certificado formateado de acuerdo con el marco técnico y se envía por correo al servicio electrónico.

8. La parte usuaria añade cualquier información adicional y determina si el usuario debe tener acceso al servicio.

Por lo tanto, los servicios electrónicos suecos solo necesitan apoyar el marco técnico para gestionar una autenticación realizada mediante una identificación electrónica europea (eID). Sin embargo, el servicio electrónico debe ser capaz de manejar la identidad presentada, que no es necesariamente un número de identidad personal. Por lo tanto, puede haber casos en los que un servicio electrónico autentique a un usuario a través del marco eIDAS, pero la identidad presentada por el usuario no pueda utilizarse en el servicio electrónico. Véase más sobre esta cuestión en el capítulo 1.7.3 a continuación.

[1]: En realidad, el usuario elige el «servicio *proxy* eIDAS» al que debe remitirse la solicitud. Esto depende del país al que pertenezca el emisor de la identificación electrónica del usuario.

1.7.2. Firmas que utilizan identificaciones electrónicas (eID) extranjeras

Como ya se ha descrito, dentro de este marco técnico se aplica un modelo de firma electrónica denominado firma federada. Un servicio de firma basado en servidor está vinculado al servicio electrónico, que a su vez solicita una firma. Cuando un usuario firma un documento, el servicio electrónico envía una solicitud de firma al servicio de firma. A continuación, el servicio de firma solicita al usuario que se autentique. El usuario aprueba la firma en relación con la autenticación. El servicio de firma envía los datos de vuelta al servicio electrónico y, a continuación, se almacenan los datos de firma asociados con el documento que se ha firmado.

Este procedimiento permite firmar también utilizando una identificación electrónica (eID) extranjera, ya que el servicio de firma puede optar por autenticar al usuario utilizando una identificación electrónica (eID) extranjera de conformidad con el procedimiento descrito anteriormente en el apartado 1.7.1.

Al firmar, en este caso, el nodo eIDAS sueco es responsable de informar al usuario de que el propósito de la autenticación es firmar un documento, quién solicitó la firma y cualquier información sobre lo que se está firmando. Un certificado de identidad solo se emite una vez que el usuario se ha autenticado (para la firma) y esto se envía al servicio de firma, el cual a su vez genera la firma.

1.7.3. Gestión de identidades

Los certificados de identidad de otros países cumplen las especificaciones técnicas a escala de la UE desarrolladas en el marco del Reglamento eIDAS. Los atributos que cada país debe incluir siempre para las personas físicas, así como para las organizaciones (*Minimum Dataset*, MDS) (conjunto mínimo de datos, por su versión en inglés) se establecen en el presente Reglamento. Cada país debe incluir un identificador único por identificación electrónica que represente a una sola persona física. De algunos países, estos identificadores serán únicos y persistentes por persona de la misma manera que, por ejemplo, los números de identidad personal suecos, pero estos identificadores pueden tener composiciones y características muy diferentes. Una característica que puede variar es la persistencia de dicho identificador, es decir, si permanece inalterado durante la vida de una persona o cambia si, por ejemplo, la persona se traslada a otra región, cambia su nombre o simplemente cambia su identificación electrónica. En algunos países (por ejemplo, el Reino Unido), el identificador variará en función de cuál de las identificaciones electrónicas del país elija actualmente un usuario.

Con el fin de simplificar la gestión de los usuarios en los servicios electrónicos suecos, el nodo eIDAS sueco genera un atributo de identificación normalizado para los usuarios que han sido autenticados utilizando una identificación electrónica (eID) extranjera, conocida como *ID provisional* (abreviado como PRID) (identificación provisional, por su versión en inglés). Además, se crea un atributo asociado que declara la persistencia esperada, o vida útil, de este atributo de identificación. El atributo de identificación provisional se genera en función de los valores de atributo obtenidos de la autenticación extranjera de acuerdo con los métodos especificados para ese país en particular. Cada combinación de país y método se clasifica en términos de persistencia esperada, es decir, cómo de probable es que una identidad cambie

con el tiempo para la misma persona. Esto permite a los servicios electrónicos suecos adaptar la comunicación con el usuario y proporcionar de forma proactiva funciones que facilitan que un usuario cuya identidad ha cambiado recupere el control sobre su información en el servicio electrónico.

En algunos casos, una persona que está autenticada utilizando una identificación electrónica (eID) extranjera también puede tener un número de identidad personal sueco. Puede tratarse, por ejemplo, de un ciudadano sueco que se ha trasladado al extranjero y ha obtenido una identificación electrónica extranjera o de un ciudadano extranjero que está registrado en Suecia y al que se le ha asignado un número de identidad personal.

El hecho de que una persona con una identificación electrónica (eID) extranjera tenga un número de identidad personal sueco normalmente no es conocido por el servicio de autenticación extranjero y, por lo tanto, esta información no se incluye en el certificado de identidad del país en el que la persona está autenticada. El nodo sueco, por otro lado, tiene la capacidad de consultar un servicio de atributos en Suecia[1] en cuanto a si existe un número de identidad personal registrado para la persona autenticada y puede, si este es el caso, añadir dicha información al certificado de identidad enviado al servicio electrónico.

> [1]: En el momento de redactar este documento, no existe un servicio de atributos que establezca un vínculo entre las identidades eIDAS y los números de identidad personal suecos.

1.7.4. Identificaciones electrónicas (eID) suecas en servicios electrónicos extranjeros

Suecia ha notificado identificaciones electrónicas suecas con niveles de seguridad sustancial y alto según el Reglamento eIDAS.

Se realiza una solicitud de autenticación de un servicio electrónico extranjero al nodo eIDAS sueco (servicio *proxy*) a través de un conector eIDAS en el país del servicio electrónico. En el nodo eIDAS sueco, el usuario elige con qué identificación electrónica sueca desea autenticarse y, a continuación, se envía una solicitud de autenticación al servicio de autenticación (*Identity Provider*) que maneja la identificación electrónica seleccionada. Esta solicitud se formatea de acuerdo con un marco técnico, lo que significa que un servicio de autenticación sueco no tiene que cumplir las especificaciones técnicas eIDAS.

El usuario es autenticado por el servicio de autenticación sueco y se emite un certificado de identidad (de acuerdo con el marco técnico). Este certificado es recibido por el servicio *proxy* sueco eIDAS y convertido en un certificado de acuerdo con las especificaciones eIDAS antes de ser enviado al conector eIDAS extranjero y luego al servicio electrónico de llamada (*Proveedor de servicios*).

2. Especificaciones técnicas

Este capítulo contiene especificaciones y perfiles para federaciones de identidades que cumplen el marco técnico de Sweden Connect y determinados servicios relacionados. A menos que se indique lo contrario, estos documentos son preceptivos para la prestación de servicios dentro de las federaciones de identidades que implementan el marco técnico.

2.1. Perfiles y especificaciones para SAML

Las federaciones de identidad que cumplen el marco técnico Sweden Connect se basan en el perfil de implementación para el marco sueco de identificaciones electrónicas «Deployment Profile for the Swedish eID Framework», [SAML.Profile]. Este perfil está influido por el «SAML V2.0 Deployment Profile for Federation Interoperability» [SAML2Int], pero no depende prescriptivamente de él. [SAML.Profile] también contiene reglas y directrices específicas para el marco técnico Sweden Connect.

2.1.1. Perfil de implementación para el marco sueco de identificaciones electrónicas (eID)

«Deployment Profile for the Swedish eID Framework», [SAML.Profile], es el principal documento del marco técnico y especifica, entre otras cosas:

- cómo deben construirse e interpretarse los metadatos SAML;
- el formato de la solicitud de autenticación;
- cómo se tramitará una solicitud de autenticación y cómo se diseñará, verificará y tramitará un certificado de identidad;
- requisitos de seguridad;
- requisitos específicos de SAML para los servicios de firma y «autenticación para la firma».

2.1.2. Marco sueco de identificaciones electrónicas (eID) – Registro de identificadores

La implementación de una infraestructura de identificación electrónica sueca requiere diferentes formas de identificadores para representar objetos en estructuras de datos. El documento «Sweden Connect – Registry for identifiers», [SC.Registry], define la estructura de los identificadores asignados en el marco técnico, así como un registro de identificadores definidos.

2.1.3. Especificación de atributos para el marco sueco de identificaciones electrónicas (eID)

La especificación «Attribute Specification for the Swedish eID Framework», [SAML.Attributes], declara los perfiles de atributos SAML que se utilizan dentro de las federaciones de identidad que cumplen el marco técnico incluidos aquellos que se conectan a eIDAS a través del nodo eIDAS sueco.

2.1.4. Categorías de entidades para el marco sueco de identificaciones electrónicas (eID)

Las categorías de entidades se utilizan dentro de la federación para una serie de propósitos diferentes:

- *Service Entity Categories* (categorías de entidades de servicios): se utilizan en los metadatos para representar los requisitos de los servicios electrónicos para los niveles

de seguridad y los atributos solicitados, así como el cumplimiento de los niveles de seguridad y la entrega de atributos por parte de los servicios de autenticación.

- *Service Property Categories* (categorías de propiedades de servicio): se utilizan para representar una característica específica de un servicio.
- *Service Type Entity Categories* (categorías de entidades de tipo de servicio): se utilizan para representar diferentes tipos de servicios dentro de la federación.
- *Service Contract Entity Categories* (categorías de entidades de contratos de servicios): utilizadas por los servicios para anunciar formularios de acuerdos y similares.
- *General Entity Categories* (categorías de entidades generales): categorías de entidades que no entran en ninguno de los tipos anteriores.

La especificación «Entity Categories for the Swedish eID Framework» [SAML.EntCat] especifica las categorías de entidades definidas por el marco técnico y describe su significado.

2.1.5. Especificación de atributos construidos eIDAS para el marco sueco de identificación electrónica

La especificación «eIDAS Constructed Attributes Specification for the Swedish eID Framework», [SC.eIDAS.Attrs], especifica procesos y reglas para cómo los atributos de identificación se construyen sobre la base de atributos recibidos durante laautenticación en eIDAS.

2.1.6. Perfil de implementación para proveedores de identidad de BankID dentro del marco sueco de identificaciones electrónicas

La especificación «Implementation Profile for BankID Identity Providers within the Swedish eID Framework», [SAML.BankID], define reglas para cómo un servicio de autenticación que implementa soporte para BankID debe ser diseñado.

> **Debe tenerse en cuenta lo siguiente:** Esta especificación no es prescriptiva para el cumplimiento de un marco técnico. Solo es pertinente para los servicios de autenticación que implementan soporte para BankID y los servicios electrónicos que los utilizan. Sin embargo, los servicios de autenticación que implementan soporte para BankID y desean conectarse a la federación Sweden Connect deben cumplir esta especificación.

2.1.7. Selección principal en solicitudes de autenticación SAML

La especificación «Principal Selection in SAML Authentication Requests», [SAML.Principal], define una extensión de SAML que permite a una parte usuaria informar a un servicio de autenticación de la identidad que desea autenticar.

2.1.8. Extensión de mensajes de usuario en solicitudes de autenticación SAML

La especificación «User Message Extension in SAML Authentication Requests», [SAML.UMessage], define una extensión de SAML que permite a una parte usuaria incluir un

mensaje de visualización en la solicitud de autenticación enviada al servicio de autenticación. El servicio de autenticación puede mostrar este mensaje al usuario durante el paso de autenticación.

2.2. Perfiles y especificaciones para OpenID Connect

2.2.1. Perfil de OpenID Connect para Sweden Connect

El perfil «OpenID Connect Profile for Sweden Connect», [OIDC.Profile], se basa en el perfil sueco OpenID Connect que es un perfil de OpenID Connect desarrollado por OIDC Suecia para promover la interoperabilidad y la seguridad dentro de las soluciones OIDC suecas.

[OIDC.Profile] añade requisitos adicionales relativos a la federación Sweden Connect.

2.2.2. Especificación de declaraciones y ámbitos de OpenID Connect para Sweden Connect

La especificación «OpenID Connect Claims and Scopes Specification for Sweden Connect», [OIDC.Claims], se basa en la especificación «Claims and Scopes Specification for the Swedish OpenID Connect Profile» de OIDC Suecia.

2.3. Especificaciones para la firma

Este apartado contiene referencias a los documentos que definen los servicios de firma dentro de las federaciones que cumplen el marco técnico Sweden Connect.

2.3.1. Perfil de implementación para el uso de OASIS DSS en servicios centrales de firma

El perfil de implementación «Implementation Profile for Using OASIS DSS in Central Signing Services», [Sign.DSS.Perfil], especifica un perfil para la solicitud de firma y la respuesta de acuerdo con la norma OASIS «Digital Signature Service Core Protocols, Elements, and Bindings», [DSS].

2.3.2. Extensión DSS para servicios de firma central federados

«DSS Extension for Federated Central Signing Services», [Sign.DSS.Ext], es una extensión de la norma OASIS «Digital Signature Service Core Protocols, Elements, and Bindings», [DSS], que especifica las definiciones necesarias para la firma con arreglo al marco técnico.

2.3.3. Perfil de certificado para certificados emitidos por servicios centrales de firma

El perfil de certificado «Certificate profile for certificates issued by Central Signing services», [Sign.Cert.Profile], especifica el contenido de los certificados de firma. Este perfil aplica una nueva extensión de certificado para admitir servicios de firma.

Este perfil hace referencia a la «Authentication Context Certificate Extension», [AuthContext], que describe cómo se representa el «Authentication Context» en los certificados X.509.

2.3.4. Protocolo de activación de firma para las firmas federadas

La especificación «Signature Activation Protocol for Federated Signing», [Sign.Activation], define un protocolo de activación de firma «Signature Activation Protocol» (SAP) para la aplicación del «Sole Control Assurance Level 2» (SCAL2)» con arreglo a la norma «prEN 419241. Sistemas confiables que permiten firma de servidor».

3. Lista de referencia

3.1. DIGG

[Digg.Tillit]

Marco de confianza para la identificación electrónica sueca.

[SC.Registry]

Sweden Connect. Registro de identificadores.

[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.

[Firma.DSS.Perfil]

Implementation Profile for Using OASIS DSS in Central Signing Services.

[Sign.DSS.Ext]

DSS Extension for Federated Central Signing Services.

[Firma.Cert.Perfil]

Certificate profile for certificates issued by Central Signing services.

[Firma.Activación]

Signature Activation Protocol for Federated Signing.

3.2. Otras referencias

[SAML2Int]

SAML V2.0 Deployment Profile for Federation Interoperability.

[DSS]

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

[AuthContext]

RFC-7773 Authentication Context Certificate Extension.