Introdução ao Quadro Técnico Sweden Connect

2024-12-04

Número de referência: **2019-267**

Índice

1. Introdução

1.1. Descrição geral

O Quadro Técnico Sweden Connect está adaptado às federações de identidade com base no SAML 2.0.

> Na versão mais recente do Quadro Técnico, foram também introduzidas especificações para o OpenID Connect. Atualmente, não há suporte federado para o OpenID Connect. Esta medida será introduzida em 2025.

> As restantes partes deste documento apenas descrevem a federação SAML. Uma vez que o OpenID Connect tenha sido totalmente introduzido, este documento também abrangerá esta tecnologia.

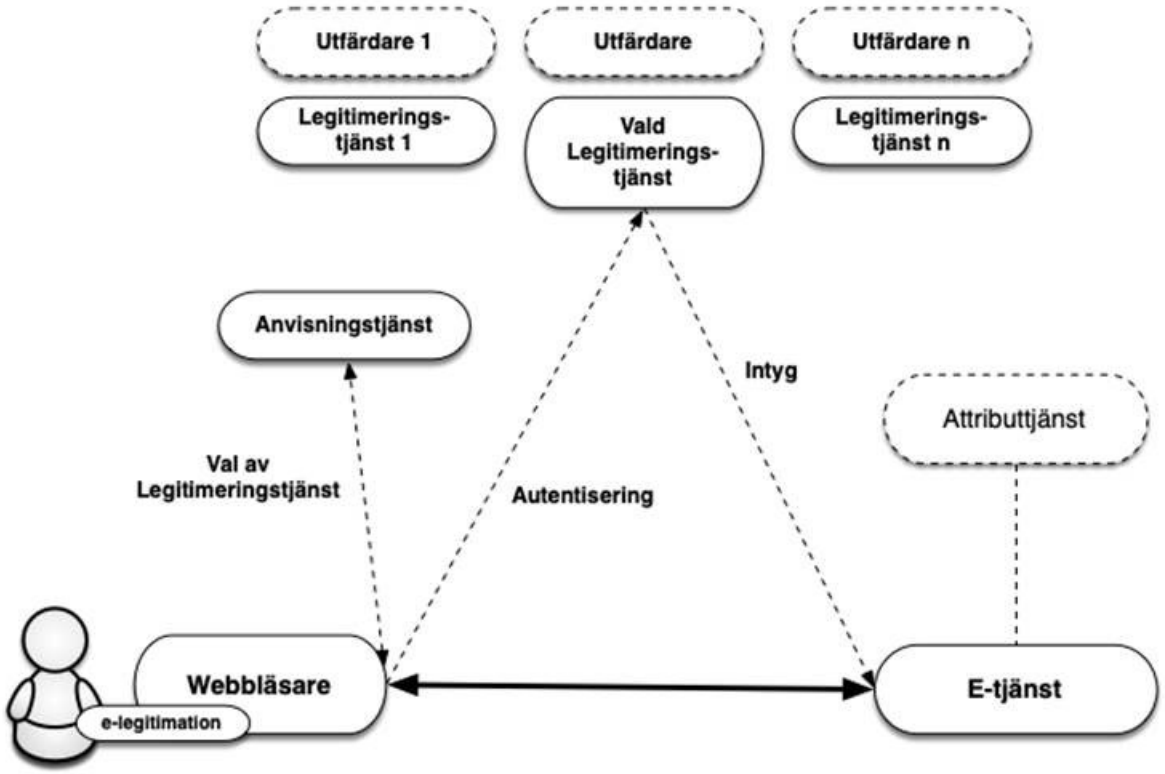
As partes utilizadoras recebem certificados de identidade num formato normalizado de um serviço de autenticação[1].

Os serviços eletrónicos que exigem uma assinatura não precisam de ser adaptados às identificações eletrónicas dos diferentes utilizadores para criar assinaturas eletrónicas. Em vez disso, o serviço eletrónico delega-o a um serviço de assinatura, em que os utilizadores, apoiados pela autenticação através de um serviço de autenticação, têm a oportunidade de assinar documentos eletrónicos.

No âmbito da federação, os serviços eletrónicos e as partes utilizadoras correspondentes assumem o papel de prestador de serviços (SP), ao passo que os serviços de autenticação que emitem certificados de identidade assumem o papel de fornecedor de identidade (IdP) e, por conseguinte, de autenticador do utilizador, independentemente do serviço eletrónico para o qual o utilizador está a ser autenticado.

Nos casos em que o serviço eletrónico necessite de mais informações sobre o utilizador, por exemplo, informações sobre a capacidade jurídica, pode ser colocada uma questão a um serviço de atributos, a Autoridade de Atributos (AA), dentro da federação, se esse serviço de atributos pertinente existir. Através de um pedido de atributo, o serviço eletrónico pode obter as informações adicionais necessárias para autorizar o utilizador e permitir o acesso ao serviço eletrónico ou equivalente.

Uma vez que os dados de identidade pessoal e outros atributos associados aos utilizadores são fornecidos através de certificados de identidade e certificados de atributos, todos os tipos de eID sobre os quais as partes utilizadoras tenham um acordo e que façam parte da federação podem ser utilizados para autenticação em relação a um serviço eletrónico que exija tanto um número de identidade pessoal como informações adicionais, mesmo que a eID não contenha quaisquer dados pessoais específicos (por exemplo, caixas de código para a geração de palavras-passe únicas).



Utfärdare 1	Emissor 1
Utfärdare n	Emissor n
Legitimeringstjänst 1	Serviço de autenticação 1
Vald legitimeringstjänst	Serviço de autenticação selecionado
Legitimeringstjänst n	Serviço de autenticação n
Anvisningstjänst	Serviço de pesquisa
Intyg	Certificado
Val av legitimeringstjänst	Escolha do serviço de autenticação
autentisering	Autenticação
attributtjänst	Serviço de atributo
Webbläsare	Navegador
E-tjänst	Serviço eletrónico

Figura 1 *Ilustração da comunicação entre os diferentes serviços no âmbito de uma federação de identidade.*

> [1]: O serviço de autenticação também é referido em outra documentação da Digg como um serviço de identidade e um serviço de certificação. No presente documento, no entanto, apenas é utilizado o termo «serviço de autenticação».

1.2. Quadro de confiança e níveis de segurança

A base para a aplicação do nível de segurança aquando da autenticação de um utilizador é o nível de garantia para a identificação eletrónica exigida pelo serviço eletrónico. Para que estes níveis de segurança sejam comparáveis no âmbito da federação, são definidos quatro níveis de garantia (1-4) no Quadro de Confiança para a Identificação Eletrónica Sueca [Digg.Tillit] e

três níveis de garantia (baixo, substancial, elevado) no Regulamento eIDAS da UE. Todos os emissores de certificados de identidade devem demonstrar que todo o processo subjacente à emissão de certificados de identidade cumpre os requisitos do nível de garantia exigido, incluindo:

- Requisitos para a criação do certificado de identidade;
- Requisitos para a identificação eletrónica (autenticação);
- Requisitos para o processo de emissão;
- Requisitos aplicáveis à própria identificação eletrónica e à sua utilização;
- Requisitos para o emissor de eID;
- requisito para estabelecer a identidade do requerente de eID.

1.3. Serviço de recolha, administração e publicação de metadados

Uma federação SAML fornece informações sobre os participantes da federação através dos metadados SAML. Tanto as entidades que prestam serviços de autenticação e atribuição na federação como as partes utilizadoras, ou seja, as entidades que consomem esses serviços, por exemplo, serviços eletrónicos, são consideradas participantes numa federação.

Os metadados da federação permitem aos participantes obter informações sobre os serviços de outros participantes, incluindo os dados necessários para a troca segura de informações entre os participantes. Os metadados devem ser mantidos atualizados por cada parte e de acordo com as condições contratuais.

O principal objetivo dos metadados é fornecer as chaves/certificados necessários para uma comunicação e um intercâmbio de informações seguros entre serviços. Além das chaves, os metadados também contêm outras informações importantes para a interação entre os serviços, tais como endereços das funções necessárias, informações sobre os níveis de garantia, categorias de serviços, informações sobre a interface do utilizador, etc.

Uma federação de identidade é definida por um registo em formato XML assinado com o certificado do operador da federação. O ficheiro contém informações sobre os membros da federação de identidade, incluindo os respetivos certificados. Uma vez que o ficheiro de metadados está assinado, é suficiente comparar um certificado com a sua contraparte de metadados. Uma infraestrutura baseada num registo central de federação exige que o registo seja continuamente atualizado e que os membros da federação utilizem sempre a versão mais recente do ficheiro.

1.4. Serviço de pesquisa

Numa federação de identidade, é possível oferecer e consumir um serviço de pesquisa partilhado, que lista os serviços de autenticação disponíveis para o utilizador escolher. O objetivo desse serviço de pesquisa é libertar os serviços eletrónicos individuais que fazem parte da federação de identidade da implementação de apoio no que diz respeito à forma como os utilizadores escolhem o serviço de autenticação (ou método de início de sessão).

Uma vez que o serviço de pesquisa está disponível na federação de identidade, os serviços eletrónicos podem direcionar os seus utilizadores para lá, a fim de escolher o serviço de autenticação. O serviço de pesquisa interage com o utilizador que faz a sua escolha e o utilizador, juntamente com a escolha do utilizador, é reencaminhado para o serviço eletrónico, que agora sabe para que serviço de autenticação o utilizador deve ser enviado para autenticação.

> Atualmente, não existe um serviço de pesquisa partilhado para a federação Sweden Connect.

1.5. Integração na entidade confiável

As partes utilizadoras, por exemplo, os serviços eletrónicos, integram-se nos serviços de autenticação através de mensagens normalizadas e consomem certificados de identidade que também têm formatos normalizados.

O quadro técnico Sweden Connect é influenciado pelo perfil de interoperabilidade «SAML V2.0 Deployment Profile for Federation Interoperability» [SAML2Int]. O perfil é suportado por uma série de produtos comerciais e soluções de código aberto, o que facilita a integração nos serviços eletrónicos.

Muitos serviços eletrónicos utilizam soluções de autenticação autónomas, o que significa que a adaptação da integração para cumprir o quadro técnico tem um impacto limitado no serviço eletrónico enquanto tal.

1.6. Assinatura

Ao assinar, o quadro técnico Sweden Connect permite utilizar diferentes tipos de identificação eletrónica, mesmo os que não se baseiam em certificados, sem necessidade de adaptações especiais no serviço eletrónico. Tal deve-se ao facto de o certificado de identidade emitido eletronicamente (utilizado para a identificação dos utilizadores aquando da assinatura) ter o mesmo formato, independentemente do tipo de identificação eletrónica utilizado pelo utilizador.

Um serviço de assinatura visa permitir assinaturas em federações de identidade que cumpram o quadro técnico, apoiadas por todos os tipos de identificação eletrónica que ofereçam um grau suficiente de segurança.

Ao adquirir[1] e introduzir um serviço de assinatura, uma parte utilizadora que faça parte da federação pode permitir que um utilizador assine um documento eletrónico com o apoio do serviço de assinatura. A assinatura eletrónica do utilizador e o certificado de assinatura associado são criados pelo serviço de assinatura após o utilizador ter concordado em assinar, autenticando-se perante o serviço de assinatura[2].

> [1]: Também é possível implementar um serviço de assinatura com base nas especificações do quadro técnico ou, alternativamente, adquirir um serviço de assinatura.
>
> [2]: É importante notar que é da maior importância que o utilizador perceba este processo como a assinatura de um documento. Por conseguinte, deve ser utilizado

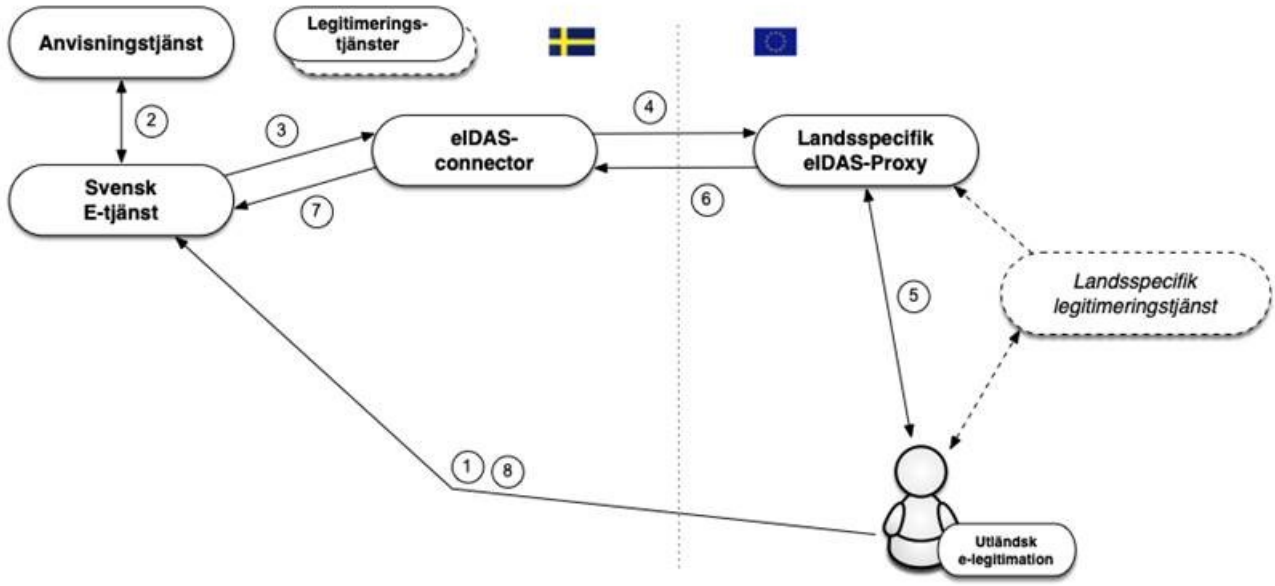
um fluxo de assinatura para os eID que o suportam no âmbito da «autenticação para assinatura».

1.7. Quadro técnico e eIDAS

O Regulamento (UE) n.º 910/2014 relativo à identificação eletrónica e aos serviços de confiança, eIDAS, exige que os organismos públicos suecos reconheçam as eID que outros países eIDAS notificaram. Isto significa que um serviço eletrónico público sueco baseado em determinadas regras deve poder aceitar um início de sessão efetuado utilizando uma identificação eletrónica emitida noutro país.

1.7.1. Autenticação com recurso a eIDs estrangeiras

As especificações técnicas das eIDAS baseiam-se, tal como o quadro técnico, nas normas SAML e, embora existam muitas semelhanças, existem também diferenças nestas especificações. No entanto, um serviço eletrónico sueco não deve estar diretamente relacionado com as especificações técnicas das eIDAS. A imagem abaixo ilustra como o nó sueco eIDAS (*eIDAS-connector*) funciona como ponte entre outros países e a federação sueca quando uma pessoa está a ser autenticada utilizando uma identificação eletrónica estrangeira num serviço eletrónico sueco. O nó sueco eIDAS está em conformidade com o quadro técnico.



Anvisningstjänst	Serviço de pesquisa
Legitimeringstjänster	Serviço de autenticação
Svensk E-tjänst	Serviço eletrónico sueco
EiDAS-connector	Conector eiDAS
Landsspecifik Eidas Proxy	Procuração específica eIDAS por país
Landsspecifik legitimeringstjänst	Serviço de autenticação específico do país
utländsk e-legitimation	Identificação eletrónica estrangeira

O fluxo é o seguinte:

1. Um utilizador com uma identificação eletrónica estrangeira solicita acesso a um serviço eletrónico sueco (ou seja, inicia sessão).

2. O serviço eletrónico permite ao utilizador escolher o método de início de sessão utilizando um serviço de pesquisa. É apresentada uma opção «Identificação eletrónica estrangeira», que é selecionada pelo utilizador no caso eIDAS.

3. O serviço eletrónico cria um pedido de autenticação em conformidade com este quadro técnico e encaminha o utilizador para o nó sueco eIDAS (*conector*) pelo qual a DIGG é responsável. O nó eIDAS funciona como um serviço de autenticação (*Fornecedor de Identidade*) na federação em relação às partes utilizadoras suecas, o que significa que a comunicação com este serviço é efetuada da mesma forma que com outros serviços de autenticação dentro das federações que cumprem o quadro técnico.

4. O pedido recebido é processado e o nó eIDAS apresenta uma página de seleção onde o utilizador seleciona «o seu país»[1]. O nó sueco eIDAS converte agora o pedido de autenticação recebido num pedido de autenticação eIDAS e encaminha o utilizador para o «serviço de proxy eIDAS» do país selecionado.

5. Quando o pedido de autenticação é recebido pelo serviço de proxy eIDAS para o país selecionado, a tecnologia de autenticação deste país assume o controlo. Nem todos os países eIDAS utilizam SAML para autenticação, mas se fosse este o caso no nosso exemplo, o utilizador seria redirecionado para um serviço de autenticação (*Fornecedor de Identidade*), e antes disso talvez também um serviço de deteção para a seleção do serviço de autenticação.

6. Uma vez efetuada a autenticação, um certificado (*Asserção*) é criado de acordo com as especificações eIDAS. Este certificado inclui atributos específicos do eIDAS que identificam o utilizador. Este certificado é agora reencaminhado para o nó sueco eIDAS.

7. O nó recebe o certificado e valida a sua precisão. Este certificado é transformado do formato eIDAS num certificado formatado de acordo com o quadro técnico e enviado para o serviço eletrónico.

8. A parte confiável acrescenta quaisquer informações adicionais e determina se o utilizador deve ter acesso ao serviço.

Por conseguinte, os serviços eletrónicos suecos só precisam de apoiar o quadro técnico para tratar uma autenticação realizada utilizando uma identificação eletrónica europeia. No entanto, o serviço eletrónico deve ser capaz de tratar a identidade apresentada, que não é necessariamente um número de identidade pessoal. Assim, pode haver casos em que um serviço eletrónico autentica um utilizador através do quadro eIDAS, mas a identidade apresentada pelo utilizador não pode ser utilizada no serviço eletrónico. Para mais informações, consultar o Capítulo 1.7.3 abaixo.

[1]: Na realidade, o utilizador escolhe o «serviço de proxy eIDAS» para o qual o pedido deve ser reencaminhado. Depende do país a que pertence o emissor de eID do utilizador.

1.7.2. Assinaturas que utilizam eIDs estrangeiras

Tal como já descrito, é aplicado um modelo de assinatura eletrónica no âmbito deste quadro técnico denominado assinatura federada. Um serviço de assinatura baseado no servidor está ligado ao serviço eletrónico, que, por sua vez, solicita uma assinatura. Quando um utilizador assina um documento, o serviço eletrónico envia um pedido de assinatura ao serviço de assinatura. O serviço de assinatura solicita então ao utilizador que se autentique. No âmbito da autenticação, o utilizador aprova a assinatura. O serviço de assinatura envia os dados de volta para o serviço eletrónico e, em seguida, os dados de assinatura associados ao documento que foi assinado são armazenados.

Este procedimento permite assinar também utilizando uma identificação eletrónica estrangeira, uma vez que o serviço de assinatura pode optar por autenticar o utilizador utilizando uma identificação eletrónica estrangeira em conformidade com o procedimento descrito no Artigo 1.7.1.

Ao assinar, neste caso, o nó sueco eIDAS é responsável por informar o utilizador de que o objetivo da autenticação é assinar um documento, quem solicitou a assinatura, e qualquer informação sobre o que está a ser assinado. Um certificado de identidade só é emitido depois de o utilizador se ter autenticado (para assinatura) e este é enviado para o serviço de assinatura, que, por sua vez, gera a assinatura.

1.7.3. Gestão de identidades

Os certificados de identidade de outros países cumprem as especificações técnicas à escala da UE elaboradas no âmbito do Regulamento eIDAS. Os atributos que cada país deve sempre incluir para as pessoas singulares, bem como para as organizações («conjunto mínimo de dados», MDS) são estabelecidos no presente regulamento. Cada país deve incluir um identificador único por identificação eletrónica que represente apenas uma pessoa singular. Em alguns países, estes identificadores serão únicos e persistentes por pessoa da mesma forma que, por exemplo, os números de identificação pessoal suecos, mas estes identificadores podem ter composições e características muito diferentes. Uma característica que pode variar é a persistência desse identificador, ou seja, se esse identificador permanece inalterado durante a vida de uma pessoa ou se muda se, por exemplo, a pessoa se mudar para outra região, alterar o seu nome ou simplesmente alterar a sua identificação eletrónica. Em alguns países (por exemplo, no Reino Unido), o identificador varia em função da identificação eletrónica do país que o utilizador opta atualmente por utilizar.

A fim de simplificar a gestão dos utilizadores nos serviços eletrónicos suecos, o nó eIDAS sueco gera um atributo de identificação normalizado para os utilizadores que tenham sido autenticados utilizando uma identificação eletrónica estrangeira, conhecido como *Identificação provisória* (abreviado como PRID). Além disso, é criado um atributo associado que declara a persistência esperada, ou tempo de vida, deste atributo ID. O atributo PRID é gerado com base nos valores dos atributos obtidos a partir da autenticação estrangeira de acordo com métodos especificados para esse país específico. Cada combinação de país e método é categorizada em termos de persistência esperada, ou seja, quão provável é que uma

identidade mude ao longo do tempo para a mesma pessoa. Tal permite que os serviços eletrónicos suecos adaptem a comunicação com o utilizador e disponibilizem proativamente funcionalidades que tornam mais fácil para um utilizador cuja identidade tenha sido alterada recuperar o controlo sobre as suas informações no serviço eletrónico.

Em alguns casos, uma pessoa autenticada através de uma identificação eletrónica estrangeira também pode possuir um número de identificação pessoal sueco. Pode tratar-se, por exemplo, de um cidadão sueco que se mudou para o estrangeiro e obteve uma identificação eletrónica estrangeira ou de um cidadão estrangeiro registado na Suécia ao qual tenha sido atribuído um número de identificação pessoal.

O facto de uma pessoa com uma identificação eletrónica estrangeira ter um número de identificação pessoal sueco não é normalmente conhecido do serviço de autenticação estrangeiro, pelo que esta informação não está incluída no certificado de identidade do país onde a pessoa está autenticada. O nó sueco, por outro lado, tem a capacidade de consultar um serviço de atributo na Suécia[1] se existe um número de identificação pessoal registado para a pessoa autenticada e pode, se for esse o caso, acrescentar essas informações ao certificado de identidade enviado para o serviço eletrónico.

> [1]: No momento da redação, não existe um serviço de atributos que estabeleça uma ligação entre as identidades eIDAS e os números de identificação pessoal suecos.

1.7.4. eIDs suecas em serviços eletrónicos estrangeiros

A Suécia notificou eID suecas nos níveis de garantia substancial e elevado, de acordo com as eIDAS.

Um pedido de autenticação de um serviço eletrónico estrangeiro é feito ao nó sueco eIDAS (serviço de procuração) através de um conector eIDAS no país do serviço eletrónico. No nó sueco eIDAS, o utilizador escolhe a identificação eletrónica sueca com a qual pretende autenticar-se e, em seguida, é enviado um pedido de autenticação ao serviço de autenticação (*Fornecedor de identidade*) que trata a identificação eletrónica selecionada. Este pedido é formatado de acordo com um quadro técnico, o que significa que um serviço de autenticação sueco não tem de cumprir as especificações técnicas do eIDAS.

O utilizador é autenticado pelo serviço de autenticação sueco e é emitido um certificado de identidade (de acordo com o quadro técnico). Este certificado é recebido pelo serviço de procuração eIDAS sueco e convertido num certificado de acordo com as especificações eIDAS antes de ser reencaminhado para o conector eIDAS estrangeiro e, em seguida, para o serviço eletrónico chamador (*Fornecedor de serviços*).

2. Especificações técnicas

Este capítulo contém especificações e perfis para federações de identidade que cumprem o quadro técnico Sweden Connect e determinados serviços conexos. Salvo indicação em contrário, estes documentos são prescritivos para a prestação de serviços dentro de federações de identidade que implementam o quadro técnico.

2.1. Perfis e especificações para SAML

As federações de identidade que cumprem o quadro técnico Sweden Connect são construídas em torno do «Perfil de Implantação do Quadro Sueco de Identificação Eletrónica», [SAML.Profile]. Este perfil é influenciado, mas não depende de forma prescritiva, do «SAML V2.0 Deployment Profile for Federation Interoperability» [SAML2Int]. [SAML.Profile] também contém regras e diretrizes específicas para o quadro técnico Sweden Connect.

2.1.1. Perfil de implantação para o quadro sueco de identificação eletrónica

O «Deployment Profile for the Swedish eID Framework» [SAML.Profile], é o principal documento do quadro técnico e especifica, nomeadamente:

- A forma como os metadados SAML devem ser construídos e interpretados;
- A forma como o pedido de autenticação deve ser formatado;
- A forma como um pedido de autenticação deve ser tratado e a forma como um certificado de identidade deve ser concebido, verificado e tratado;
- Requisitos de segurança;
- Requisitos SAML específicos para serviços de assinatura e «autenticação para assinatura».

2.1.2. Quadro sueco eID – Registo de identificadores

A implementação de uma infraestrutura sueca de identificação eletrónica exige diferentes formas de identificadores para representar objetos em estruturas de dados. O documento «Sweden Connect – Registry for identifiers», [SC.Registry], define a estrutura dos identificadores atribuídos no âmbito do quadro técnico, bem como um registo de identificadores definidos.

2.1.3. Especificação de atributos para o Quadro sueco eID

A especificação «Atributo Especificação para o Quadro sueco eID», [SAML.Atributos], declara os perfis de atributos SAML que são usados dentro das federações de identidade que cumprem com o quadro técnico incluindo aqueles que se ligam ao eIDAS através do nó sueco eIDAS.

2.1.4. Categorias de entidades para o quadro sueco eID

As categorias de entidades são utilizadas no âmbito da federação para vários fins diferentes:

- Categorias de entidades de serviços – Utilizadas em metadados para representar os requisitos dos serviços eletrónicos para os níveis de garantia e os atributos solicitados, bem como o cumprimento dos níveis de garantia e a entrega dos atributos pelos serviços de autenticação.

- Categorias de propriedades de serviços – Utilizadas para representar uma característica específica de um serviço.
- Categorias de entidades de tipo de serviço – Utilizadas para representar diferentes tipos de serviços dentro da federação.
- Categorias de entidades de contratos de serviços – Utilizadas pelos serviços para anunciar formulários de acordo e similares.
- Categorias gerais de entidades – Categorias de entidades que não se enquadram em nenhum dos tipos acima referidos.

A especificação «Categorias de entidades para o Quadro Sueco eID» [SAML.EntCat] especifica as categorias de entidades definidas pelo quadro técnico e descreve o seu significado.

2.1.5. Especificação de Atributos Construídos eIDAS para o Quadro Sueco de Identificação Eletrónica

A especificação «eIDAS Constructed Attributes Specification for the Swedish eID Framework», [SC.eIDAS.Attrs], especifica processos e regras para como os ID-atributos são construídos com base em atributos recebidos durante a autenticação no eIDAS.

2.1.6. Perfil de implementação para os fornecedores de identidade BankID no âmbito do quadro sueco de identificação eletrónica

A especificação «Perfil de execução para BankID Fornecedores de Identidade no quadro do eID sueco», [SAML.BankID], define regras para como um serviço de autenticação que implementa suporte para BankID deve ser concebido.

> **Tenha em atenção o seguinte:** Esta especificação não é prescritiva para o cumprimento de um quadro técnico. Só é relevante para os serviços de autenticação que implementam o suporte ao BankID e aos serviços eletrónicos que os utilizam. No entanto, os serviços de autenticação que implementem suporte para o BankID e pretendam ligar-se à federação Sweden Connect devem cumprir esta especificação.

2.1.7. Seleção principal em pedidos de autenticação SAML

A especificação «Seleção principal em pedidos de autenticação SAML», [SAML.Principal], define uma extensão do SAML que permite a uma parte utilizadora informar um serviço de autenticação sobre a identidade que pretende autenticar.

2.1.8. Extensão de mensagem de utilizador em pedidos de autenticação SAML

A especificação «Extensão de mensagem de utilizador em pedidos de autenticação SAML», [SAML.UMessage], define uma extensão do SAML que permite a uma parte utilizadora incluir uma mensagem de visualização no pedido de autenticação enviado ao serviço de autenticação. O serviço de autenticação pode então mostrar esta mensagem ao utilizador durante a etapa de autenticação.

2.2. Perfis e especificações para OpenID Connect

2.2.1. Perfil OpenID Connect para Sweden Connect

O perfil '«OpenID Connect Profile for Sweden Connect», [OIDC.Profile], baseia-se no Perfil Sueco OpenID Connect que é um perfil OpenID Connect desenvolvido pela OIDC Sweden para promover a interoperabilidade e a segurança nas soluções suecas da OIDC.

[OIDC.Profile] acrescenta requisitos adicionais relativos à federação Sweden Connect.

2.2.2. Especificação de Declarações e Âmbitos do OpenID Connect para o Sweden Connect

A especificação «OpenID Connect Claims and Scopes Specification for Sweden Connect», [OIDC.Claims], baseia-se na especificação Claims and Scopes Specification for the Swedish OpenID Connect Profile de OIDC Sweden.

2.3. Especificações para a assinatura

Este artigo contém referências aos documentos que definem os serviços de assinatura dentro das federações que cumprem o quadro técnico Sweden Connect.

2.3.1. Perfil de implementação para a utilização do OASIS DSS nos Serviços Centrais de Assinatura

O perfil de execução «Execução Profile for Using OASIS DSS in Central Signing Services», [Assinar.DSS.Perfil], especifica um perfil para o pedido de assinatura e a resposta de acordo com a norma OASIS «Digital Signature Service Core Protocols, Elements, and Bindings», [DSS].

2.3.2. Extensão DSS para Serviços Federados Centrais de Assinatura

A «DSS Extension for Federated Central Signing Services», [Sign.DSS.Ext], é uma extensão da norma OASIS «Digital Signature Service Core Protocols, Elements, and Bindings», [DSS], que especifica as definições necessárias para a assinatura no âmbito do quadro técnico.

2.3.3. Perfil do certificado para os certificados emitidos pelos Serviços Centrais de Assinatura

O perfil do certificado «Perfil para os certificados emitidos pelos serviços de assinatura central», [Sign.Cert.Profile], especifica o conteúdo dos certificados de assinatura. Este perfil aplica uma nova extensão de certificado para apoiar os serviços de assinatura.

Este perfil refere-se à «Authentication Context Certificate Extension», [AuthContext], que descreve a forma como o «Authentication Context» é representado nos certificados X.509.

2.3.4. Protocolo de Ativação de Assinatura para Assinatura Federada

A especificação «Signature Activation Protocol for Federated Signing», [Sign.Activation], define um «Signature Activation Protocol» (SAP) para a implementação do «Sole Control Assurance Level 2» (SCAL2) de acordo com a norma «prEN 419241 – Trustworthy Systems Supporting Server Signing».

3. Lista de referência

3.1. DIGG

[Digg.Tillit]

Quadro de confiança para a identificação eletrónica sueca.

[SC.Registo]

Sweden Connect – Registo de identificadores.

[SAML.Perfil]

Perfil de implantação para o Quadro sueco eID.

[SAML.Atributos]

Especificação de atributos para o Quadro sueco eID.

[SAML.EntCat]

Categorias de entidades para o Quadro sueco eID.

[SC.eIDAS.Attrs]

eIDAS Especificação de Atributos Construídos para o Quadro sueco eID.

[SAML.BankID]

Perfil de implementação para BankID Provedores de Identidade no Quadro sueco eID.

[SAML.Principal]

Seleção Principal em Pedidos de Autenticação SAML.

[SAML.UMessage]

Extensão de Mensagem de Utilizador em Pedidos de Autenticação SAML.

[OIDC.Perfil]

OpenID Connect Profile for Sweden Connect.

[OIDC.Claims]

OpenID Connect Claims and Scopes Specification for Sweden Connect.

[Sign.DSS.Perfil]

Perfil de Implementação para a Utilização do OASIS DSS nos Serviços de Assinatura Central.

[Sign.DSS.Ext]

Extensão DSS para os Serviços Federados de Assinatura Central.

[Sign.Cert.Perfil]

Perfil do certificado para os certificados emitidos pelos serviços centrais de assinatura.

[Sign.Activation]

Protocolo de Ativação de Assinatura para Assinatura Federada.

3.2. Outras referências

[SAML2Int]

SAML V2.0 Perfil de Implementação para a Interoperabilidade da Federação.

[DSS]

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

[Contexto da aut]

RFC-7773: Extensão do Certificado de Contexto de Autenticação.