Introduzione al quadro tecnico Sweden Connect

04-12-2024

Numero di riferimento: **2019-267**

Indice

1. Introduzione

1.1. Panoramica

Il quadro tecnico Sweden Connect è adattato per le federazioni di identità basate su SAML 2.0.

> Nell’ultima versione del quadro tecnico, sono state introdotte anche le specifiche per OpenID Connect. Attualmente, non esiste alcun supporto federativo per OpenID Connect. Questo sarà introdotto nel 2025.
>
> Le restanti parti di questo documento descrivono solo la federazione SAML. Una volta che OpenID Connect è stato completamente introdotto, questo documento coprirà anche questa tecnologia.

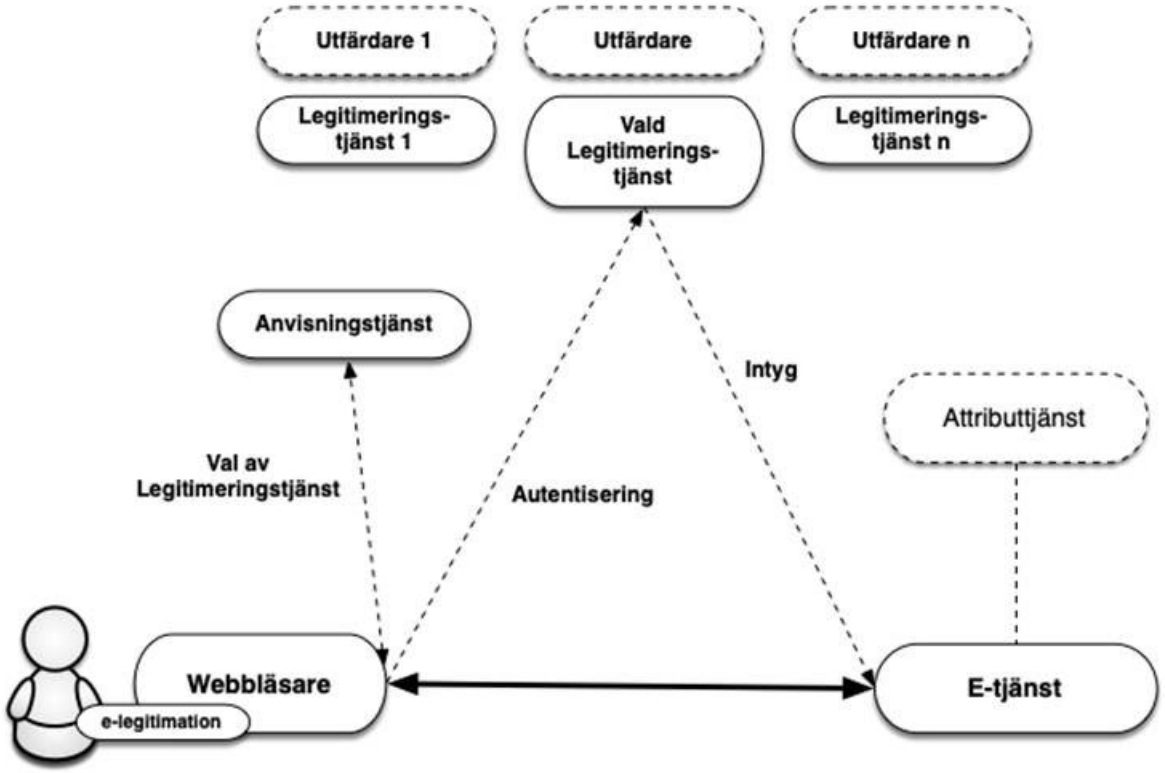
Le parti fiduciarie ricevono certificati di identità in un formato standardizzato da un servizio di autenticazione[1].

I servizi elettronici che richiedono una firma non devono essere adattati alle e-ID di utenti diversi al fine di creare firme elettroniche. Al contrario, il servizio elettronico delega questo compito a un servizio di firma, in cui gli utenti, supportati dall'autenticazione tramite un servizio di autenticazione, hanno la possibilità di firmare documenti elettronici.

All'interno della federazione, i servizi elettronici e le corrispondenti parti fiduciarie assumono il ruolo di Service Provider (SP, «fornitore di servizi»), mentre i servizi di autenticazione che rilasciano certificati di identità assumono il ruolo di Identity Provider (IdP, «fornitore di identità») e quindi di autenticatore dell'utente, indipendentemente dal servizio elettronico per il quale l'utente viene autenticato.

Per i casi in cui il servizio elettronico necessita di maggiori informazioni sull'utente, ad esempio informazioni sulla capacità giuridica, è possibile porre una domanda a un servizio di attributi, Attribute Authority (AA), all'interno della federazione, se esiste tale servizio di attributi pertinente. Attraverso una richiesta di attributi, il servizio elettronico può ottenere le informazioni supplementari necessarie per autorizzare l'utente e fornire l'accesso al servizio elettronico o a un servizio equivalente.

Poiché sia i dati di identità personale che gli altri attributi associati agli utenti sono forniti tramite certificati di identità e certificati di attributi, tutti i tipi di e-ID su cui le parti facenti affidamento sulla certificazione hanno un accordo e che fanno parte della federazione possono essere utilizzati per l'autenticazione nei confronti di un servizio elettronico che richiede sia un numero di identità personale che informazioni aggiuntive, anche se l'e-ID non contiene dati personali specifici (ad esempio caselle di codice per la generazione di password una tantum).



Utfärdare 1	Emittente 1
Utfärdare n	Emittente n
Legitimeringstjänst 1	Servizio di autenticazione 1
Vald legitimeringstjänst	Servizio di autenticazione selezionato
Legitimeringstjänst n	Servizio di autenticazione n
Anvisningstjänst	Servizio di orientamento
Intyg	Certificato
Val av legitimeringstjänst	Scelta del servizio di autenticazione
autentisering	autenticazione
attributtjänst	attributo di servizio
Webbläsare	Browser
E-tjänst	Servizio elettronico

Figura 1 *Illustrazione della comunicazione tra i diversi servizi all'interno di una federazione di identità.*

[1]: Il servizio di autenticazione è indicato anche in altra documentazione di Digg come servizio di identità e servizio di certificazione. Nel presente documento, tuttavia, viene utilizzato solo il termine «servizio di autenticazione».

1.2. Quadro di fiducia e livelli di sicurezza

La base per l'applicazione del livello di sicurezza all'atto dell'autenticazione di un utente è il livello di garanzia per l'identificazione elettronica richiesto dal servizio elettronico. Affinché tali livelli di sicurezza siano comparabili nel quadro della federazione, quattro livelli di garanzia (da 1 a 4) sono definiti nel quadro di fiducia per l'identificazione elettronica svedese [Digg.Tillit] e tre livelli di garanzia (basso, sostanziale, elevato) nel regolamento eIDAS dell'UE. Tutti gli emittenti di certificati di identità devono dimostrare che l'intero processo alla base del rilascio dei certificati di identità soddisfa i requisiti del livello di garanzia richiesto, tra cui:

- requisiti per la creazione del certificato di identità;
- requisiti per l'identificazione elettronica (autenticazione);
- requisiti per il processo di rilascio;
- requisiti per l'e-ID stessa e il suo utilizzo;
- requisiti per l'emittente dell'e-ID;
- obbligo di stabilire l'identità del richiedente l'e-ID.

1.3. Servizio per la raccolta, l'amministrazione e la pubblicazione dei metadati

Una federazione SAML fornisce informazioni sui partecipanti della federazione attraverso metadati SAML. Sia le entità che forniscono servizi di autenticazione e attributi nella

federazione sia le parti facenti affidamento, ossia le entità che consumano tali servizi, ad esempio i servizi elettronici, sono considerate partecipanti a una federazione.

I metadati della federazione consentono ai partecipanti di ottenere informazioni sui servizi di altri partecipanti, compresi i dati necessari per lo scambio sicuro di informazioni tra i partecipanti. I metadati devono essere tenuti aggiornati da ciascuna parte e in conformità con le condizioni contrattuali.

Lo scopo principale dei metadati è fornire le chiavi/i certificati necessari per la comunicazione sicura e lo scambio di informazioni tra i servizi. Oltre alle chiavi, i metadati contengono anche altre informazioni importanti per l'interazione tra i servizi, come gli indirizzi delle funzioni richieste, le informazioni sui livelli di affidabilità, le categorie di servizi, le informazioni sull'interfaccia utente, ecc.

Una federazione di identità è definita da un registro in formato XML firmato con il certificato dell'operatore della federazione. Il file contiene informazioni sui membri della federazione di identità, compresi i loro certificati. Poiché il file di metadati è firmato, è sufficiente confrontare un certificato con la sua controparte di metadati. Un'infrastruttura basata su un registro federativo centrale richiede che il registro sia continuamente aggiornato e che i membri della federazione utilizzino sempre l'ultima versione del file.

1.4. Servizio di orientamento

In una federazione di identità, è possibile offrire e utilizzare un servizio di orientamento condiviso, che elenca i servizi di autenticazione disponibili per l'utente tra cui scegliere. Lo scopo di tale servizio di orientamento è quello di sollevare i singoli servizi elettronici che fanno parte della federazione di identità dall'implementazione del supporto per quanto riguarda il modo in cui gli utenti scelgono il servizio di autenticazione (o il metodo di accesso).

Poiché il servizio di orientamento è disponibile all'interno della federazione delle identità, i servizi elettronici possono indirizzare i propri utenti al fine di scegliere il servizio di autenticazione. Il servizio di orientamento interagisce con l'utente che fa la sua scelta e l'utente, insieme alla scelta dell'utente, viene reindirizzato al servizio elettronico, che ora sa a quale servizio di autenticazione l'utente deve essere inviato per l'autenticazione.

> Attualmente non esiste un servizio di orientamento condiviso per la federazione Sweden Connect.

1.5. Integrazione presso la parte richiedente

Le parti facenti affidamento, ad esempio i servizi elettronici, si integrano con i servizi di autenticazione attraverso messaggi standardizzati e utilizzano certificati di identità che possiedono altresì formati standardizzati.

Il quadro tecnico Sweden Connect è influenzato dal profilo di interoperabilità «SAML V2.0 Deployment Profile for Federation Interoperability» [SAML2Int]. Il profilo è supportato da una serie di prodotti commerciali e soluzioni Open Source, che facilitano l'integrazione nei servizi elettronici.

Molti servizi elettronici utilizzano soluzioni di autenticazione autonome, il che significa che adattare l'integrazione per conformarsi al quadro tecnico ha un impatto limitato sul servizio elettronico in quanto tale.

1.6. Firma

Al momento della firma, il quadro tecnico Sweden Connect consente di utilizzare diversi tipi di e-ID, anche quelli che non sono basati su certificati, senza la necessità di adattamenti speciali nel servizio elettronico. Questo perché il certificato di identità rilasciato elettronicamente (utilizzato per l'identificazione degli utenti al momento della firma) ha lo stesso formato indipendentemente dal tipo di e-ID utilizzato dall'utente.

Un servizio di firma mira a consentire firme all'interno di federazioni di identità conformi al quadro tecnico, supportate da tutti i tipi di e-ID che offrono un grado sufficiente di sicurezza.

Appaltando[1] e introducendo un servizio di firma, una parte richiedente che fa parte della federazione può consentire a un utente di firmare un documento elettronico con il supporto del servizio di firma. La firma elettronica dell'utente e il relativo certificato di firma sono creati dal servizio di firma dopo che l'utente ha accettato di firmare autenticandosi nei confronti del servizio di firma[2].

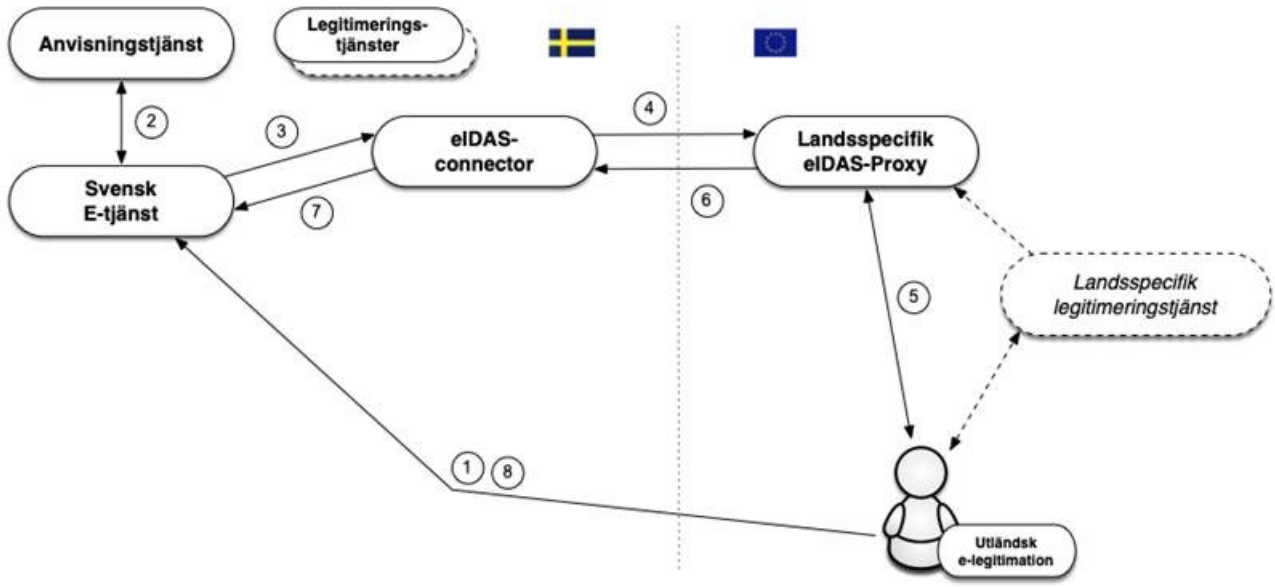
> [1]: È inoltre possibile implementare un servizio di firma basato sulle specifiche del quadro tecnico o acquisire in altro modo un servizio di firma.
>
> [2]: È importante notare che è fondamentale che l'utente abbia la sensazione di firmare un documento. È pertanto opportuno utilizzare un flusso di firma per le e-ID che lo supportano in relazione all'«autenticazione per la firma».

1.7. Quadro tecnico ed eIDAS

Il regolamento (UE) n. 910/2014 sull'identificazione elettronica e i servizi fiduciari, eIDAS, impone agli enti pubblici svedesi di riconoscere le e-ID notificate da altri paesi eIDAS. Ciò significa che un servizio elettronico pubblico svedese basato su determinate norme deve essere in grado di accettare un accesso effettuato utilizzando un'e-ID rilasciata in un altro paese.

1.7.1. Autenticazione mediante identificazione elettronica (e-ID) estera

Le specifiche tecniche per eIDAS si basano, come il quadro tecnico, sugli standard SAML e, sebbene vi siano molte somiglianze, vi sono anche differenze in tali specifiche. Tuttavia, un servizio elettronico svedese non dovrebbe riferirsi direttamente alle specifiche tecniche dell'eIDAS. L'immagine qui sotto illustra come il nodo svedese eIDAS (*eIDAS-connector*) funge da ponte tra altri paesi e la federazione svedese quando una persona viene autenticata utilizzando un'e-ID estera in un servizio elettronico svedese. Il nodo svedese eIDAS è conforme al quadro tecnico.



Anvisningstjänst	Servizio di orientamento
Legitimeringstjänster	Servizi di autenticazione
Svensk E-tjänst	Servizio elettronico svedese
EiDAS-connector	eiDAS-connector
Landsspecifik Eidas Proxy	Proxy eIDAS specifico per paese
Landsspecifik legitimeringstjänst	Servizio di autenticazione specifico per paese
utländsk e-legitimation	e-ID estera

Il flusso è il seguente:

1. Un utente con un'e-ID estera richiede l'accesso a un servizio elettronico svedese (ossia effettua l'accesso).

2. Il servizio elettronico consente all'utente di scegliere il metodo di login utilizzando un servizio di orientamento. Viene visualizzata l'opzione «e-ID estera», selezionata dall'utente nel caso eIDAS.

3. Il servizio elettronico crea una richiesta di autenticazione in conformità con questo quadro tecnico e indirizza l'utente al nodo svedese eIDAS (*connector*) di cui la DIGG è responsabile. Il nodo eIDAS funge da servizio di autenticazione (*Identity Provider*) nella federazione nei confronti delle parti svedesi facenti affidamento, il che significa che la comunicazione con questo servizio avviene allo stesso modo di altri servizi di autenticazione all'interno di federazioni conformi al quadro tecnico.

4. La richiesta ricevuta viene elaborata e il nodo eIDAS visualizza una pagina di selezione in cui l'utente seleziona «il proprio paese»[1]. Il nodo svedese eIDAS converte ora la richiesta di autenticazione ricevuta in una richiesta di autenticazione eIDAS e indirizza l'utente al «servizio proxy eIDAS» del paese selezionato.

5. Quando la richiesta di autenticazione è ricevuta dal servizio proxy eIDAS per il paese selezionato, subentra la tecnologia di autenticazione di tale paese. Non tutti i paesi eIDAS utilizzano SAML per l'autenticazione, ma se questo fosse il caso nel nostro esempio, l'utente verrebbe reindirizzato a un servizio di autenticazione (*Identity Provider*), e prima ancora forse anche a un servizio di orientamento per la selezione del servizio di autenticazione.

6. Una volta eseguita l'autenticazione, un certificato (*Assertion*) è creato secondo le specifiche eIDAS. Questo certificato include attributi specifici di eIDAS che identificano l'utente. Questo certificato viene ora inoltrato al nodo svedese eIDAS.

7. Il nodo riceve il certificato e ne convalida l'accuratezza. Questo certificato viene trasformato dal formato eIDAS in un certificato formattato secondo il quadro tecnico e inviato al servizio elettronico.

8. La parte richiedente aggiunge eventuali informazioni supplementari e determina se all'utente debba essere concesso l'accesso al servizio.

I servizi elettronici svedesi devono quindi solo supportare il quadro tecnico al fine di gestire un'autenticazione eseguita utilizzando un'e-ID europea. Tuttavia, il servizio elettronico deve essere in grado di gestire l'identità presentata, che non è necessariamente un numero di identità personale. Pertanto, vi possono essere casi in cui un servizio elettronico autentica un utente tramite il quadro eIDAS, ma l'identità presentata dall'utente non può essere utilizzata nel servizio elettronico. Ulteriori informazioni su questo argomento sono disponibili nel capitolo 1.7.3 di seguito.

> [1]: In realtà, l'utente sceglie il «servizio proxy eIDAS» a cui inoltrare la richiesta. Ciò dipende dal paese a cui appartiene l'emittente dell'e-ID dell'utente.

1.7.2. Firme che utilizzano e-ID estere

Come già descritto, all'interno del presente quadro tecnico viene applicato un modello di firma elettronica denominato firma federata. Un servizio di firma basato su server è collegato al servizio elettronico, che a sua volta richiede una firma. Quando un utente firma un documento, il servizio elettronico invia una richiesta di firma al servizio di firma. Il servizio di firma richiede quindi all'utente di autenticarsi. In relazione all'autenticazione, l'utente approva la firma. Il servizio di firma restituisce i dati al servizio elettronico e quindi vengono memorizzati i dati di firma associati al documento che è stato firmato.

Questa procedura consente di firmare anche utilizzando un'e-ID estera, in quanto il servizio di firma può scegliere di autenticare l'utente utilizzando un'e-ID estera conformemente alla procedura descritta nella sezione 1.7.1.

Al momento della firma, in questo caso, il nodo svedese eIDAS è responsabile di informare l'utente che lo scopo dell'autenticazione è quello di firmare un documento, chi ha richiesto la firma, e qualsiasi informazione su ciò che viene firmato. Un certificato di identità viene rilasciato solo dopo che l'utente si è autenticato (per la firma), che viene inviato al servizio di firma e che a sua volta genera la firma.

1.7.3. Gestione delle identità

I certificati di identità di altri paesi sono conformi alle specifiche tecniche a livello dell'UE sviluppate nell'ambito del regolamento eIDAS. Gli attributi che ciascun paese deve sempre includere per le persone fisiche e per le organizzazioni (Minimum Dataset, MDS) sono stabiliti nel presente regolamento. Ogni paese deve includere un identificativo univoco per e-ID che rappresenti una sola persona fisica. In alcuni paesi, tali identificativi saranno unici e persistenti per persona allo stesso modo, ad esempio, dei numeri di identità personale svedesi, anche se gli identificativi possono avere composizioni e caratteristiche molto diverse. Una caratteristica che può variare è la persistenza di tale identificativo, vale a dire se tale identificativo rimane invariato durante la vita di una persona o cambia se, ad esempio, la persona si trasferisce in un'altra regione, cambia il suo nome o semplicemente cambia la sua e-ID. In alcuni paesi (ad esempio il Regno Unito), l'identificativo varierà a seconda di quale delle e-ID del paese un utente sceglie attualmente di utilizzare.

Al fine di semplificare la gestione degli utenti nei servizi elettronici svedesi, il nodo svedese eIDAS genera un attributo ID standardizzato per gli utenti che sono stati autenticati utilizzando l'e-ID straniero, noto come *ID provvisorio* (abbreviato in PRID). Inoltre, viene creato un attributo associato che dichiara la persistenza prevista, o la durata, di questo attributo ID. L'attributo PRID viene generato in base ai valori degli attributi ottenuti dall'autenticazione estera secondo metodi specificati per quel particolare paese. Ogni combinazione di paese e metodo è classificata in termini di persistenza prevista, vale a dire quanto è probabile che un'identità cambi nel tempo per la stessa persona. Ciò consente ai servizi elettronici svedesi di adattare la comunicazione con l'utente e fornire in modo proattivo funzionalità che rendono più facile per un utente la cui identità è cambiata riprendere il controllo delle proprie informazioni nel servizio elettronico.

In alcuni casi, una persona autenticata con un'eID estera può altresì essere in possesso di un numero di identità personale svedese. Può trattarsi, ad esempio, di un cittadino svedese che si è trasferito all'estero e ha ottenuto un'e-ID estera o di un cittadino straniero registrato in Svezia al quale è stato assegnato un numero di identità personale.

Il fatto che una persona con un'e-ID estera abbia un numero di identità personale svedese non è normalmente noto al servizio di autenticazione straniero e tali informazioni non sono pertanto incluse nel certificato di identità del paese in cui la persona è autenticata. Il nodo svedese, d'altra parte, ha la capacità di interrogare un servizio di attributi in Svezia[1] per verificare se esiste un numero di identificazione personale registrato per la persona autenticata e può, in tal caso, aggiungere tali informazioni al certificato di identità inviato al servizio elettronico.

> [1]: Al momento in cui scriviamo, non esiste un servizio di attributi che stabilisca un collegamento tra le identità eIDAS e i numeri di identità personali svedesi.

1.7.4. Identificazione elettronica svedese nei servizi elettronici esteri

La Svezia ha notificato le e-ID svedesi ai livelli di garanzia sostanziale ed elevato secondo l'eIDAS.

Una richiesta di autenticazione da parte di un servizio elettronico estero viene effettuata al nodo svedese eIDAS (servizio proxy) tramite un connettore eIDAS nel paese del servizio

elettronico. Nel nodo svedese eIDAS, l'utente sceglie con quale e-ID svedese desidera autenticarsi, dopo di che viene inviata una richiesta di autenticazione al servizio di autenticazione (*Identity Provider*) che gestisce l'e-ID selezionata. Tale richiesta è formattata secondo un quadro tecnico, il che significa che un servizio di autenticazione svedese non deve essere conforme alle specifiche tecniche eIDAS.

L'utente viene autenticato dal servizio di autenticazione svedese ed è rilasciato un certificato di identità (secondo il quadro tecnico). Tale certificato viene ricevuto dal servizio proxy svedese eIDAS e convertito in un certificato secondo le specifiche eIDAS prima di essere inoltrato al connettore eIDAS straniero e quindi al servizio elettronico chiamante (*Service Provider*).

2. Specifiche tecniche

Questo capitolo contiene le specifiche e i profili per le federazioni di identità conformi al quadro tecnico Sweden Connect e ad alcuni servizi correlati. Salvo diversa indicazione, questi documenti sono prescrittivi per la fornitura di servizi all'interno di federazioni di identità che implementano il quadro tecnico.

2.1. Profili e specifiche per SAML

Le federazioni di identità conformi al quadro tecnico Sweden Connect sono costruite attorno al «Deployment Profile for the Swedish eID Framework», [SAML.Profile]. Questo profilo è influenzato dal «SAML V2.0 Deployment Profile for Federation Interoperability» [SAML2Int], ma non dipende da esso in modo prescrittivo. [SAML.Profile] contiene inoltre norme e linee guida specifiche per il quadro tecnico Sweden Connect.

2.1.1. Profilo di distribuzione per il quadro svedese di e-ID

«Deployment Profile for the Swedish eID Framework», [SAML.Profile], è il principale documento quadro tecnico e specifica, tra l'altro:

- come sono costruiti e interpretati i metadati SAML;
- le modalità di formattazione della richiesta di autenticazione;
- come è gestita una richiesta di autenticazione e come è progettato, verificato e gestito un certificato di identità;
- requisiti di sicurezza;
- requisiti SAML specifici per i servizi di firma e «autenticazione per firma».

2.1.2. Swedish e-ID Framework – Registry for identifiers

L'implementazione di un'infrastruttura di e-ID svedese richiede diverse forme di identificatori per rappresentare gli oggetti nelle strutture di dati. Il documento «Sweden Connect – Registry for identifiers», [SC.Registry], definisce la struttura degli identificativi assegnati nell'ambito del quadro tecnico, nonché un registro degli identificativi definiti.

2.1.3. Attribute Specification for the Swedish eID Framework

La specifica «Attribute Specification for the Swedish eID Framework», [SAML.Attributes], dichiara i profili degli attributi SAML che sono utilizzati all'interno delle federazioni di identità che rispettano il quadro tecnico, inclusi quelli che si connettono a eIDAS tramite il nodo eIDAS svedese.

2.1.4. Entity Categories for the Swedish eID Framework

Le categorie di entità (Entity Categories) sono utilizzate all'interno della federazione per scopi diversi:

- Service Entity Categories: utilizzate nei metadati per rappresentare i requisiti dei servizi elettronici per i livelli di affidabilità e gli attributi richiesti, nonché il soddisfacimento dei livelli di affidabilità e la fornitura di attributi da parte dei servizi di autenticazione.
- Service Property Categories: utilizzate per rappresentare una caratteristica specifica di un servizio.
- Service Type Entity Categories: utilizzate per rappresentare diversi tipi di servizi all'interno della federazione.
- Service Contract Entity Categories: utilizzate dai servizi per annunciare moduli di accordo e simili.
- General Entity Categories: categorie di entità che non rientrano in nessuno dei tipi di cui sopra.

La specifica «Entity Categories for the Swedish eID Framework» [SAML.EntCat] indica le categorie di entità definite dal quadro tecnico e ne descrive il significato.

2.1.5. eIDAS Constructed Attributes Specification for the Swedish eID Framework

La specifica «eIDAS Constructed Attributes Specification for the Swedish eID Framework», [SC.eIDAS.Attrs], definisce i processi e le regole su come gli ID-attributes sono costruiti sulla base degli attributi ricevuti durante l'autenticazione in eIDAS.

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

La specifica «Implementation Profile for BankID Identity Providers within the Swedish eID Framework», [SAML.BankID], definisce le regole su come un servizio di autenticazione che implementa il supporto per BankID debba essere progettato.

> **Si prega di notare quanto segue:** La presente specifica non è prescrittiva per la conformità a un quadro tecnico. È rilevante solo per i servizi di autenticazione che implementano il supporto per BankID e i servizi elettronici che li utilizzano. Tuttavia, i servizi di autenticazione che implementano il supporto per BankID e

desiderano connettersi alla federazione Sweden Connect devono essere conformi a questa specifica.

2.1.7. Principal Selection in SAML Authentication Requests

La specifica «Principal Selection in SAML Authentication Requests», [SAML.Principal], definisce un'estensione di SAML che consente a una parte richiedente di informare un servizio di autenticazione dell'identità che desidera autenticare.

2.1.8. User Message Extension in SAML Authentication Requests

La specifica «User Message Extension in SAML Authentication Requests», [SAML.UMessage], definisce un'estensione di SAML che consente a una parte richiedente di includere un messaggio di visualizzazione nella richiesta di autenticazione inviata al servizio di autenticazione. Il servizio di autenticazione può quindi mostrare questo messaggio all'utente durante la fase di autenticazione.

2.2. Profili e specifiche per OpenID Connect

2.2.1. OpenID Connect Profile for Sweden Connect

Il profilo «OpenID Connect Profile for Sweden Connect», [OIDC.Profile], si basa sul profilo svedese OpenID Connect che è un profilo OpenID Connect sviluppato da OIDC Sweden per promuovere l'interoperabilità e la sicurezza all'interno delle soluzioni OIDC svedesi.

[OIDC.Profile] aggiunge ulteriori requisiti relativi alla federazione Sweden Connect.

2.2.2. OpenID Connect Claims and Scopes Specification for Sweden Connect

La specifica «OpenID Connect Claims and Scopes Specification for Sweden Connect», [OIDC.Claims], si basa sulla specifica Claims and Scopes Specification for the Swedish OpenID Connect Profile di OIDC Sweden.

2.3. Specifiche per la firma

Questa sezione contiene riferimenti ai documenti che definiscono i servizi di firma all'interno delle federazioni conformi al quadro tecnico Sweden Connect.

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

Il profilo di attuazione «Implementation Profile for using OASIS DSS in Central Signing Services», [Sign.DSS.Profile], specifica un profilo per la richiesta di firma e la risposta secondo la norma OASIS «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], è un'estensione dello standard OASIS «Digital Signature Service Core Protocols, Elements, and Bindings», [DSS], che specifica le definizioni necessarie per la firma nell'ambito del quadro tecnico.

2.3.3. Certificate Profile for Certificates Issued by Central Signing Services

Il profilo del certificato «Certificate Profile for Certificates Issued by Central Signing Services», [Sign.Cert.Profile], specifica il contenuto dei certificati di firma. Questo profilo applica una nuova estensione del certificato per supportare i servizi di firma.

Questo profilo si riferisce alla «Authentication Context Certificate Extension», [AuthContext], che descrive il modo in cui l'«Authentication Context» è rappresentato nei certificati X.509.

2.3.4. Signature Activation Protocol for Federated Signing

La specifica «Signature Activation Protocol for Federated Signing», [Sign.Activation], definisce un «Signature Activation Protocol» (SAP) per l'attuazione del «Sole Control Assurance Level 2» (SCAL2) conformemente alla norma «prEN 419241 – Trustworthy Systems Supporting Server Signing».

3. Elenco di riferimento

3.1. DIGG

[Digg.Tillit]

Quadro di fiducia per l'identificazione elettronica svedese.

[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.

[Firma.Cert.Profilo]

Certificate profile for certificates issued by Central Signing services.

[Sign.Activation]

Signature Activation Protocol for Federated Signing.

3.2. Altri riferimenti

[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.