Úvod do technického rámce Sweden Connect

4. 12. 2024

Ref. číslo: **2019-267**

Copyright © Agentura pro digitální státní správu (Digg), 2015-2024.

Obsah

1. Úvod
   - 1.1. Přehled
   - 1.2. Rámec důvěry a úrovně zabezpečení
   - 1.3. Služba pro sběr, správu a zveřejňování metadat
   - 1.4. Vyhledávací služba
   - 1.5. Integrace na straně spoléhajícího se subjektu
   - 1.6. Podpis
   - 1.7. Technický rámec a eIDAS
   - 1.7.1. Ověřování pomocí zahraničních eID
   - 1.7.2. Podpisy s použitím zahraničních eID
   - 1.7.3. Správa identit
   - 1.7.4. Švédské elektronické identifikace v zahraničních elektronických službách
2. Technické podmínky
   - 2.1. Profily a specifikace pro SAML
   - 2.1.1. Deployment Profile for the Swedish eID Framework

2.1.2. Swedish eID Framework – Registry for identifiers

2.1.3. Attribute Specification for the Swedish eID Framework

2.1.4. Kategorie subjektů pro rámec švédské eID

2.1.5. eIDAS Constructed Attributes Specification for the Swedish eID Framework

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

2.1.7. Principal Selection in SAML Authentication Requests

2.1.8. User Message Extension in SAML Authentication Requests

2.2. Profily a specifikace pro OpenID Connect

2.2.1. OpenID Connect Profile for Sweden Connect

2.2.2. OpenID Connect Claims and Scopes Specification for Sweden Connect

2.3. Specifikace pro podpis

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

2.3.2. DSS Extension for Federated Central Signing Services

2.3.3. Certificate Profile for Certificates Issued by Central Signing Services

2.3.4. Signature Activation Protocol for Federated Signing

3. **Referenční seznam**

3.1. DIGG

3.2. Další odkazy

1. Úvod

1.1. Přehled

Technický rámec Sweden Connect je přizpůsoben pro federaci identit založené na SAML 2.0.

> V nejnovější verzi technického rámce byly také zavedeny specifikace pro OpenID Connect. V současné době není pro OpenID Connect k dispozici podpora sdružování. Ta bude zavedena v roce 2025.
>
> Zbývající části tohoto dokumentu popisují pouze federaci SAML. Po úplném zavedení technologie OpenID Connect se bude tento dokument zabývat i touto technologií.

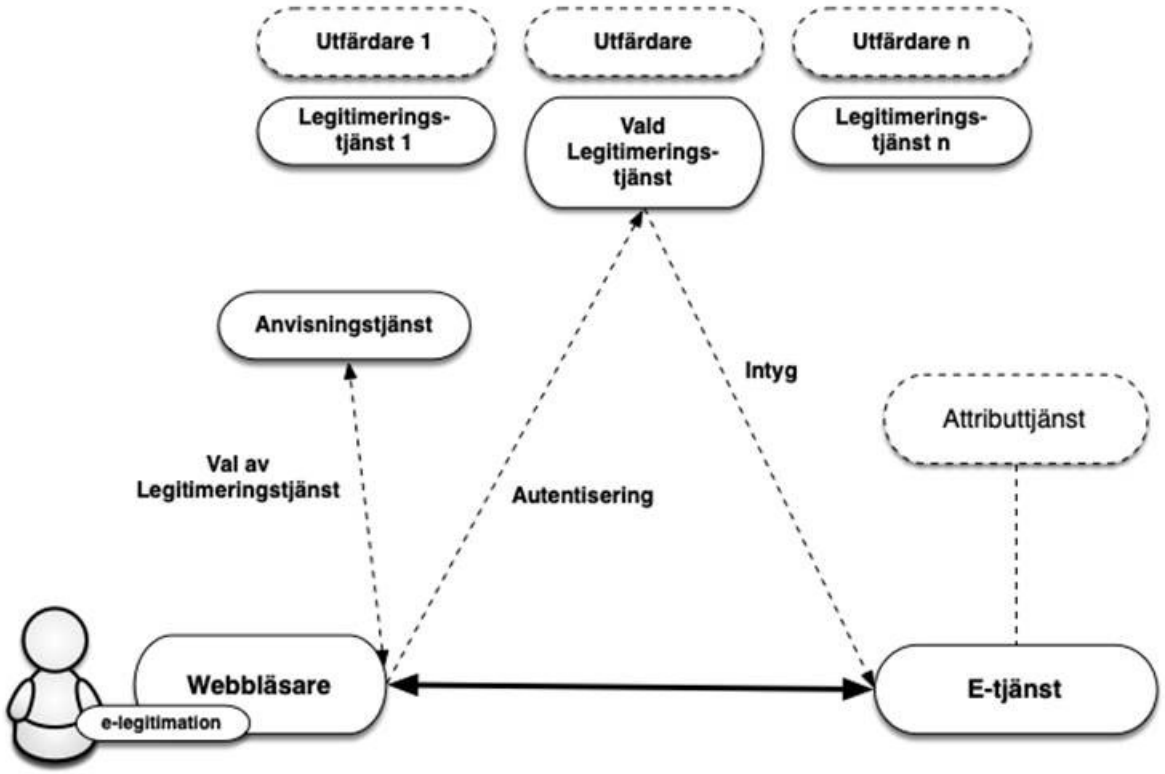
Spoléhající se subjekty obdrží od ověřovací služby[1] osvědčení totožnosti ve standardizovaném formátu.

Elektronické služby, které vyžadují podpis, není třeba přizpůsobovat různým eID uživatelů, aby bylo možné vytvářet elektronické podpisy. Místo toho elektronická služba deleguje tuto činnost na podpisovou službu, kde uživatelé, podpoření autentizací prostřednictvím ověřovací služby, mají možnost podepisovat elektronické dokumenty.

V rámci federace přebírají elektronické služby a odpovídající spoléhající se strany roli poskytovatele služeb („Service Provider“ – SP), zatímco ověřovací služby vydávající osvědčení totožnosti přebírají roli poskytovatele identit (IdP), a tedy ověřovatele uživatele, bez ohledu na to, pro jakou elektronickou službu je uživatel ověřován.

V případech, kdy elektronická služba potřebuje více informací o uživateli, např. informace o způsobilosti k právům a právním úkonům, lze položit otázku atributové službě, („Attribute Authority“, AA), v rámci federace, pokud taková relevantní atributová služba existuje. Prostřednictvím požadavku na atribut může elektronická služba získat další informace nezbytné k autorizaci uživatele a poskytnutí přístupu k elektronické službě nebo jejímu ekvivalentu.

Vzhledem k tomu, že osobní identifikační údaje i další atributy spojené s uživateli jsou poskytovány prostřednictvím osvědčení identity a atributových certifikátů, lze pro ověřování vůči elektronické službě, která vyžaduje jak osobní identifikační číslo, tak další informace, použít všechny typy eID, na kterých se spoléhající strany dohodly a které jsou součástí federace, a to i v případě, že eID neobsahuje žádné konkrétní osobní údaje (např. kódová pole pro generování jednorázových hesel).



Utfärdare 1	Vydavatel 1

Utfärdare n	Vydavatel n
Legitimeringstjänst 1	Ověřovací služba 1
Vald legitimeringstjänst	Vybraná ověřovací služba
Legitimeringstjänst n	Ověřovací služba n
Anvisningstjänst	Vyhledávací služba
Intyg	Osvědčení
Val av legitimeringstjänst	Volba ověřovací služby
autentisering	ověření
attributtjänst	atributová služba
Webbläsare	Prohlížeč
E-tjänst	Elektronická služba

Obrázek 1: *Ilustrace komunikace mezi různými službami v rámci federace identit.*

> [1]: Ověřovací služba je v další dokumentaci společnosti Digg označována také jako služba identit a certifikační služba. V tomto dokumentu se však používá pouze pojem „ověřovací služba“.

1.2. Rámec důvěry a úrovně zabezpečení

Základem pro to, která úroveň zabezpečení se má použít při ověřování uživatele, je úroveň důvěryhodnosti pro elektronickou identifikaci požadovanou elektronickou službou. K tomu, aby byly tyto úrovně zabezpečení v rámci federace srovnatelné, jsou v rámci důvěryhodnosti pro švédskou elektronickou identifikaci [Digg.Tillit] definovány čtyři úrovně důvěryhodnosti (1-4) a v nařízení EU o eIDAS tři úrovně zabezpečení (nízká, střední, vysoká). Všichni vydavatelé osvědčení totožnosti musí prokázat, že celý proces vydávání osvědčení totožnosti splňuje požadavky požadované úrovně důvěryhodnosti, včetně:

- požadavky na vytvoření osvědčení totožnosti;
- požadavky na elektronickou identifikaci (ověřování);
- požadavky na postup při vydávání;
- požadavky na samotnou eID a její použití;
- požadavky na vydavatele eID;
- požadavek na ověření totožnosti žadatele o elektronickou identifikaci (eID).

1.3. Služba pro sběr, správu a zveřejňování metadat

Federace SAML poskytuje informace o účastnících federace prostřednictvím metadat SAML. Za účastníky federace se považují jak subjekty, které poskytují autentizační a atributové služby ve federaci, tak spoléhající se subjekty, tj. subjekty, které tyto služby využívají, např. elektronické služby.

Metadata federace umožňují účastníkům získat informace o službách ostatních účastníků, včetně údajů nezbytných pro bezpečnou výměnu informací mezi účastníky. Metadata musí být aktualizována každou stranou a v souladu se smluvními podmínkami.

Hlavním účelem metadat je poskytovat klíče/certifikáty potřebné pro bezpečnou komunikaci a výměnu informací mezi službami. Kromě klíčů obsahují metadata také další informace důležité pro interakci mezi službami, jako jsou adresy požadovaných funkcí, informace o úrovních důvěryhodnosti, kategorie služeb, informace o uživatelském rozhraní atd.

Federace identit je definována registrem ve formátu XML, který je podepsán certifikátem provozovatele federace. Soubor obsahuje informace o členech federace identit včetně jejich certifikátů. Vzhledem k tomu, že soubor metadat je podepsaný, stačí porovnat certifikát s jeho protějškem v metadatech. Infrastruktura založená na centrálním registru federace vyžaduje, aby byl registr průběžně aktualizován a aby členové federace vždy používali nejnovější verzi souboru.

1.4. Vyhledávací služba

Ve federaci identit je možné nabízet a využívat sdílenou vyhledávací službu, která obsahuje seznam ověřovacích služeb, z nichž si uživatel může vybrat. Účelem takové vyhledávací služby je zbavit jednotlivé elektronické služby, které jsou součástí federace identit, povinnosti implementovat podporu s ohledem na to, jak si uživatelé zvolí ověřovací službu (nebo způsob přihlášení).

Jelikož je vyhledávací služba dostupná v rámci federace identit, mohou elektronické služby své uživatele nasměrovat tam, aby si vybrali ověřovací službu. Vyhledávací služba komunikuje s uživatelem, který provádí svou volbu, a uživatel je spolu se svou volbou nasměrován zpět k elektronické službě, která nyní ví, ke které ověřovací službě má být uživatel odeslán k ověření.

> V současné době neexistuje žádná sdílená vyhledávací služba pro federaci Sweden Connect.

1.5. Integrace na straně spoléhajícího se subjektu

Spoléhající se subjekty, např. elektronické služby, se integrují s ověřovacími službami prostřednictvím standardizovaných zpráv a využívají osvědčení totožnosti, které mají rovněž standardizované formáty.

Technický rámec Sweden Connect je ovlivněn profilem interoperability „SAML V2.0 Deployment Profile for Federation Interoperability“ [SAML2Int]. Tento profil je podporován řadou komerčních produktů a řešení s otevřeným zdrojovým kódem („open source“), což usnadňuje integraci u elektronických služeb.

Mnoho elektronických služeb používá samostatná řešení ověřování, což znamená, že přizpůsobení integrace tak, aby byla v souladu s technickým rámcem, má omezený dopad na elektronickou službu jako takovou.

1.6. Podpis

Technický rámec Sweden Connect umožňuje při podepisování používat různé typy eID, a to i ty, které nejsou založeny na osvědčení, aniž by bylo nutné provádět zvláštní úpravy v elektronické službě. Je tomu tak proto, že elektronicky vydané osvědčení totožnosti (používaný pro identifikaci uživatelů při podepisování) má stejný formát bez ohledu na typ eID používaný uživatelem.

Cílem podpisové služby je umožnit podepisování v rámci federací identit, které jsou v souladu s technickým rámcem, podporovaným všemi typy eID, které nabízejí dostatečný stupeň bezpečnosti.

Pořízením[1] a zavedením podpisové služby může spoléhající se strana, která je součástí federace, umožnit uživateli podepsat elektronický dokument s podporou podpisové služby. Elektronický podpis uživatele a související podpisový certifikát jsou vytvořeny podpisovou službou poté, co uživatel souhlasil s podpisem tím, že se ověřil prostřednictvím podpisové služby[2].

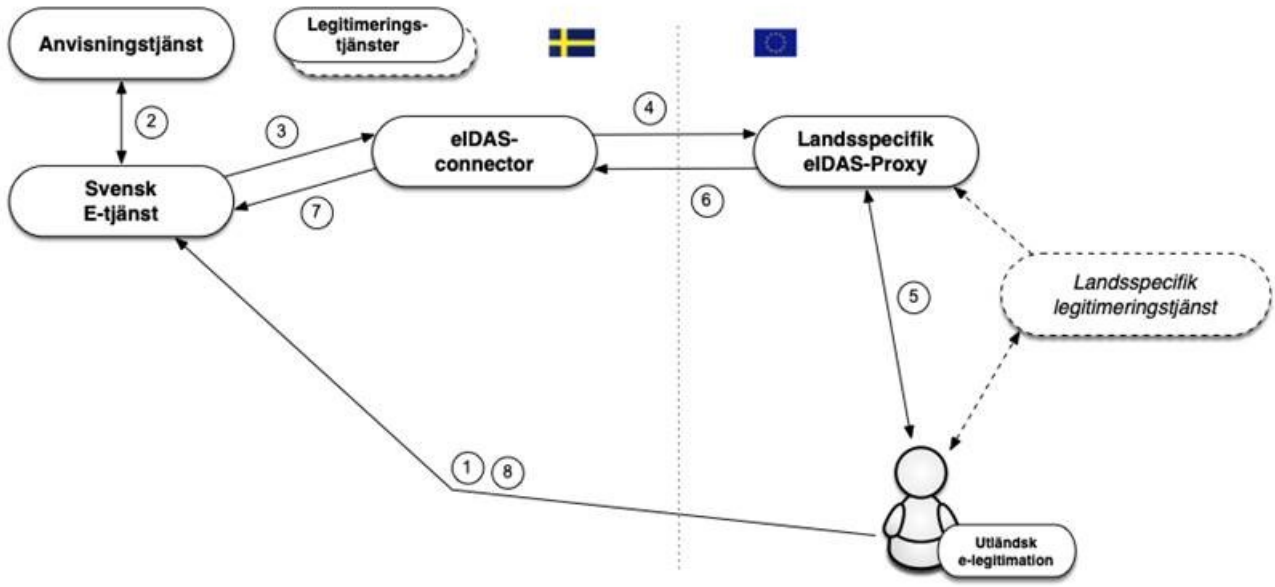
> [1]: Podpisovou službu je také možné implementovat na základě specifikací technického rámce nebo podpisovou službu získat jiným způsobem.
>
> [2]: Je důležité poznamenat, že je nanejvýš důležité, aby uživatel vnímal tento proces jako podepisování dokumentu. Proto by měl být pro eID, které to podporují, použit podpisový tok ve spojení s „ověřením pro podpis“.

1.7. Technický rámec a eIDAS

Nařízení EU (910/2014) o elektronické identifikaci a službách vytvářejících důvěru, eIDAS, vyžaduje, aby švédské veřejné orgány uznávaly eID, které oznámily jiné země eIDAS. To znamená, že švédská veřejná elektronická služba založená na určitých pravidlech musí být schopna přijmout přihlášení provedené pomocí eID vydaného v jiné zemi.

1.7.1. Ověřování pomocí zahraničních eID

Technické specifikace pro eIDAS vycházejí, stejně jako technický rámec, ze standardů SAML, a přestože existuje mnoho podobností, existují v těchto specifikacích i rozdíly. Švédská elektronická služba by se však neměla přímo vztahovat k technickým specifikacím eIDAS. Níže uvedený obrázek znázorňuje, jak švédský uzel eIDAS (*eIDAS-connector*) funguje jako most mezi jinými zeměmi a švédskou federací, když je osoba ověřována pomocí zahraničního eID ve švédské elektronické službě. Švédský uzel eIDAS je v souladu s technickým rámcem.



Anvisningstjänst	Vyhledávací služba
Legitimeringstjänster	Ověřovací služby
Svensk E-tjänst	Švédská elektronická služba
EiDAS-connector	eiDAS-connector
Landsspecifik Eidas Proxy	Proxy eIDAS pro jednotlivé státy
Landsspecifik legitimeringstjänst	Ověřovací služba pro jednotlivé státy
utländsk e-legitimation	Zahraniční eID

Průběh je následující:

1. Uživatel se zahraničním elektronickým průkazem totožnosti žádá o přístup ke švédské elektronické službě (tj. přihlásí se).

2. Elektronická služba umožňuje uživateli zvolit způsob přihlášení pomocí vyhledávací služby. Zobrazí se možnost „Zahraniční eID“, kterou uživatel zvolí v případě eIDAS.

3. Elektronická služba vytvoří žádost o ověření v souladu s tímto technickým rámcem a nasměruje uživatele do švédského uzlu eIDAS (*connector*), za který je DIGG odpovědná. Uzel eIDAS funguje jako ověřovací služba (*Identity Provider*) ve federaci vůči švédským spoléhajícím se stranám, což znamená, že komunikace s touto službou probíhá stejným způsobem jako s ostatními autentizačními službami v rámci federací, které splňují technický rámec.

4. Přijatý požadavek se zpracuje a uzel eIDAS zobrazí výběrovou stránku, kde si uživatel vybere „svou zemi“[1]. Švédský uzel eIDAS nyní převede přijatý požadavek na ověření na požadavek na ověření eIDAS a uživatel je přesměrován na službu „eIDAS Proxy Service“ vybrané země.

5. Po přijetí žádosti o ověření proxy službou eIDAS vybrané země převezme ověřování technologie této země. Ne všechny země eIDAS používají pro ověřování SAML, ale pokud by tomu tak bylo v našem příkladu, byl by uživatel přesměrován na ověřovací

službu (*Identity Provider*) a předtím možná také na instruktážní službu pro výběr poskytovatele identit.

6. Při ověřování je vytvořen certifikát (*Assertion*) podle specifikací eIDAS. Tento certifikát obsahuje atributy specifické pro eIDAS, které identifikují uživatele. Tento certifikát je nyní předán švédskému uzlu eIDAS.

7. Uzel obdrží certifikát a ověří jeho správnost. Tento certifikát je transformován z formátu eIDAS do certifikátu ve formátu podle technického rámce a je zaslán elektronické službě.

8. Spoléhající se strana doplní případné další informace a rozhodne, zda má být uživateli udělen přístup ke službě.

Švédské elektronické služby tedy musí podporovat pouze technický rámec, aby mohly zpracovat ověření provedené pomocí evropského eID. Elektronická služba však musí být schopna zpracovat předloženou identitu, která nemusí být nutně osobním identifikačním číslem. Mohou tedy nastat případy, kdy elektronická služba ověří uživatele prostřednictvím rámce eIDAS, ale předloženou identitu uživatele nelze v elektronické službě použít. Více o tom v kapitole 1.7.3 níže.

[1]: Uživatel si vlastně vybere „proxy službu eIDAS“, které má být požadavek předán. To závisí na zemi, do které patří vydavatel eID uživatele.

1.7.2. Podpisy s použitím zahraničních eID

Jak již bylo popsáno, v tomto technickém rámci se používá model elektronického podpisu, který se nazývá federovaný podpis. Podpisová služba založená na serveru je propojena s elektronickou službou, která následně požádá o podpis. Když uživatel podepíše dokument, elektronická služba odešle požadavek na podpis podpisové službě. Podpisová služba poté požádá uživatele o ověření totožnosti. V souvislosti s ověřením uživatel podpis schvaluje. Podpisová služba odešle data zpět elektronické službě a poté se uloží podpisová data spojená s podepsaným dokumentem.

Tento postup umožňuje podepisovat i pomocí zahraniční eID, neboť podpisová služba může zvolit ověření uživatele pomocí zahraniční eID v souladu s postupem popsaným výše v oddílu 1.7.1.

Při podepisování je v tomto případě švédský uzel eIDAS odpovědný za informování uživatele o tom, že účelem ověření je podepsání dokumentu, kdo o podpis požádal, a o všech informacích o tom, co se podepisuje. Certifikát totožnosti je vydán až poté, co se uživatel ověří (pro účely podpisu), což je zasláno podpisové službě a ta následně vygeneruje podpis.

1.7.3. Správa identit

Osvědčení totožnosti z jiných zemí splňují technické specifikace platné v celé EU, které byly vypracovány v rámci nařízení eIDAS. Atributy, které musí každá země vždy obsahovat pro fyzické osoby i organizace („Minimum Dataset“, MDS), jsou stanoveny v tomto nařízení. Každá země musí zahrnout jedinečný identifikátor pro každá eID, která představuje pouze jednu fyzickou osobu. Z některých zemí budou tyto identifikátory jedinečné a trvalé pro každou osobu stejně jako například švédská osobní identifikační čísla, ale tyto identifikátory

mohou mít velmi odlišné složení a vlastnosti. Jednou z charakteristik, která se může lišit, je to, jak je takový identifikátor trvalý, tj. zda zůstává během života osoby nezměněn, nebo se mění, pokud se například osoba přestěhuje do jiného regionu, změní své jméno nebo jen změní svou eID. V některých zemích (např. ve Spojeném království) se identifikátor liší podle toho, kterou z eID dané země se uživatel aktuálně rozhodne používat.

V zájmu zjednodušení správy uživatelů ve švédských elektronických službách generuje švédský uzel eIDAS pro uživatele, kteří byli ověřeni pomocí zahraničního eID, standardizovaný atribut ID, známý jako *provisional ID* (zkráceně PRID). Kromě toho je vytvořen přidružený atribut, který deklaruje očekávanou trvalost neboli životnost tohoto atributu ID. Atribut PRID je generován na základě hodnot atributů získaných ze zahraničního ověření podle stanovených metod pro danou zemi. Každá kombinace země a metody je kategorizována z hlediska očekávané perzistence, tj. jaká je pravděpodobnost, že se identita v průběhu času u téže osoby změní. To umožňuje švédským elektronickým službám přizpůsobit komunikaci s uživatelem a proaktivně poskytovat funkce, které uživateli, jehož identita se změnila, usnadní opětovné získání kontroly nad jeho informacemi v elektronické službě.

V některých případech může mít osoba, která je ověřena pomocí zahraničního elektronického osvědčení totožnosti, také švédské osobní identifikační číslo. Může se jednat například o švédského občana, který se přestěhoval do zahraničí a získal zahraniční eID, nebo o zahraničního občana, který je registrován ve Švédsku a bylo mu přiděleno osobní identifikační číslo.

Skutečnost, že osoba se zahraničním elektronickým průkazem totožnosti má švédské osobní identifikační číslo, není zahraniční ověřovací službě obvykle známa, a tato informace proto není uvedena v osvědčení totožnosti ze země, kde je osoba ověřena. Švédský uzel má naproti tomu možnost dotazovat se na atributovou službu ve Švédsku[1] ohledně toho, zda existuje registrované osobní identifikační číslo pro ověřenou osobu, a pokud ano, může tyto informace doplnit do osvědčení totožnosti zaslaného elektronické službě.

> [1]: V době vypracování tohoto dokumentu neexistuje žádná služba atributů, která by vytvářela spojení mezi identitami eIDAS a švédskými osobními identifikačními čísly.

1.7.4. Švédské elektronické identifikace v zahraničních elektronických službách

Švédsko oznámilo švédské elektronické identifikace na úrovních důvěryhodnosti značné a vysoké podle eIDAS.

Žádost o ověření ze strany zahraniční elektronické služby se podává švédskému uzlu eIDAS (proxy služba) prostřednictvím „eIDAS-connector“ v zemi elektronické služby. Ve švédském uzlu eIDAS si uživatel zvolí, kterou švédskou elektronickou identifikaci hodlá použít k ověřování, a poté je ověřovací službě (*Identity Provider*), která zpracovává vybranou elektronickou identifikaci, odeslána žádost o ověření. Tato žádost je formátována podle technického rámce, což znamená, že švédská ověřovací služba nemusí splňovat technické specifikace eIDAS.

Uživatel je ověřen švédskou ověřovací službou a je vydáno osvědčení totožnosti (podle technického rámce). Toto osvědčení obdrží švédská proxy služba eIDAS a převede jej na

osvědčení podle specifikací eIDAS, než je předán zahraničnímu zprostředkovateli „eIDAS-connector“ a poté volající elektronické službě (*Service Provider*).

2. Technické podmínky

Tato kapitola obsahuje specifikace a profily pro federace identit, které jsou v souladu s technickým rámcem Sweden Connect, a některé související služby. Není-li uvedeno jinak, jsou tyto dokumenty normativní pro poskytování služeb v rámci federací identit, které implementují technický rámec.

2.1. Profily a specifikace pro SAML

Identifikační federace, které jsou v souladu s technickým rámcem Sweden Connect, jsou založeny na „Deployment Profile for the Swedish eID Framework“ (Profil pro zavádění rámce pro švédskou elektronickou identifikaci), [SAML.Profile]. Tento profil je ovlivněn, ale není normativně závislý na „SAML V2.0 Deployment Profile for Federation Interoperability“ (Profil pro zavádění SAML V2.0 pro federační interoperabilitu) [SAML2Int]. [SAML.Profile] rovněž obsahuje pravidla a pokyny vztahující se na technický rámec Sweden Connect.

2.1.1. Deployment Profile for the Swedish eID Framework

„Deployment Profile for the Swedish eID Framework“ (Profil pro zavádění rámce švédské elektronické identifikace), [SAML.Profile], je hlavním dokumentem technického rámce a mimo jiné stanovuje:

- způsob, jakým mají být tvořena a interpretovana metadata SAML;
- způsob, jakým má být žádost o ověřování formátována;
- způsob, jakým má být vyřizována žádost o ověření a jak má být navrhována, ověřována a vyřizováno osvědčení totožnosti;
- bezpečnostní požadavky;
- zvláštní požadavky SAML na podpisové služby a „ověření pro podpis“.

2.1.2. Swedish eID Framework – Registry for identifiers

Zavedení infrastruktury pro švédskou elektronickou identifikaci vyžaduje různé formy identifikátorů pro reprezentaci objektů v datových strukturách. Dokument „Sweden Connect – Registry for identifiers“, [SC.Registry], definuje strukturu identifikátorů přidělených podle technického rámce, jakož i registr definovaných identifikátorů.

2.1.3. Attribute Specification for the Swedish eID Framework

Specifikace „Attribute Specification for the Swedish eID Framework“, [SAML.Attributes], deklaruje SAML profily atributů které jsou používány v rámci federací identit které jsou v souladu s technickým rámcem včetně těch které se připojují k eIDAS prostřednictvím švédského uzlu eIDAS.

2.1.4. Entity Categories for the Swedish eID Framework

Kategorie subjektů („Entity Categories“) se v rámci federace používají pro řadu různých účelů:

- Kategorie subjektů služeb („Service Entity Categorie“) – používají se v metadatech k reprezentaci požadavků elektronických služeb na úrovně důvěryhodnosti a požadované atributy, jakož i plnění úrovní důvěryhodnosti ze strany ověřovacích služeb a poskytování atributů.

- Kategorie vlastností služby („Service Property Categories“) – používají se k reprezentaci specifické vlastnosti služby.

- Kategorie subjektů typu služby („Service Type Entity Categories“) – používají se k reprezentaci různých typů služeb v rámci federace.

- Kategorie subjektů v rámci smlouvy o poskytování služeb („Service Contract Entity Categories“) – používají je služby k oznamování formulářů dohod a podobně.

- Obecné kategorie subjektů („General Entity Categories“) – kategorie subjektů, které nespadají do žádného z výše uvedených typů.

Specifikace „Entity Categories for the Swedish eID Framework“ (Kategorie subjektů pro rámec švédské elektronické identifikace) [SAML.EntCat] specifikuje kategorie subjektů definované technickým rámcem a popisuje jejich význam.

2.1.5. eIDAS Constructed Attributes Specification for the Swedish eID Framework

Specifikace „IDAS Constructed Attributes Specification for the Swedish eID Framework“, [SC.eIDAS.Attrs], stanoví postupy a pravidla pro to, jak atributy ID jsou konstruovány na základě atributů přijatých během ověřování v eIDAS.

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

Specifikace „Implementation Profile for BankID Identity Providers within the Swedish eID Framework“, [SAML.BankID], stanoví pravidla pro to, jak by měla být navržena ověřovací služba, která zavádí podporu pro BankID .

> **Vezměte prosím na vědomí následující:** Tato specifikace není normativní pro plnění technického rámce. Vztahuje se pouze na ověřovací služby, které implementují podporu BankID, a elektronické služby, které je využívají. Ověřovací služby, které implementují podporu pro BankID a chtějí se připojit k federaci Sweden Connect, však musí splňovat tuto specifikaci.

2.1.7. Principal Selection in SAML Authentication Requests

Specifikace „Principal Selection in SAML Authentication Requests“, [SAML.Principal], definuje rozšíření SAML, které umožňuje spoléhající se subjektu informovat ověřovací službu, kterou totožnost si přeje ověřit.

2.1.8. User Message Extension in SAML Authentication Requests

Specifikace „User Message Extension in SAML Authentication Requests“ (Rozšíření uživatelské zprávy v žádostech o ověření SAML), [SAML.UMessage], definuje rozšíření SAML, které umožňuje spoléhající se straně zahrnout zobrazovanou zprávu do žádosti o ověření odeslané ověřovací službě. Ověřovací služba pak může tuto zprávu zobrazit uživateli během kroku ověřování.

2.2. Profily a specifikace pro OpenID Connect

2.2.1. OpenID Connect Profile for Sweden Connect

Profil „OpenID Connect Profile for Sweden Connect“, [OIDC.Profil], je založen na švédském profilu OpenID Connect, což je profil OpenID Connect vyvinutý švédskou organizací OIDC na podporu interoperability a bezpečnosti v rámci švédských řešení OIDC.

[OIDC.Profile] přidává další požadavky týkající se federace Sweden Connect.

2.2.2. OpenID Connect Claims and Scopes Specification for Sweden Connect

Specifikace „OpenID Connect Claims and Scopes Specification for Sweden Connect“, [OIDC.Claims], navazuje na specifikaci „Claims and Scopes Specification for the Swedish OpenID Connect Profile“ od OIDC Sweden.

2.3. Specifikace pro podpis

Tento oddíl obsahuje odkazy na dokumenty definující podpisové služby v rámci federací, které jsou v souladu s technickým rámcem Sweden Connect.

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

Profil provádění „Implementation Profile for Using OASIS DSS in Central Signing Services“ (Profil pro používání OASIS DSS v centrálních podepisovacích službách), [Sign.DSS.Profile], stanoví profil pro žádost o podpis a odpověď podle normy 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], je rozšířením standardu OASIS „Digital Signature Service Core Protocols, Elements, and Bindings“, [DSS], který specifikuje definice nezbytné pro podepisování podle technického rámce.

2.3.3. Certificate Profile for Certificates Issued by Central Signing Services

Profil certifikátu „Certificate profil certifikátů vydaných službami centrálního podepisování“, [Znak.Cert.Profil], stanoví obsah podpisových certifikátů. Tento profil používá nové rozšíření certifikátu pro podporu podpisových služeb.

Tento profil odkazuje na „Authentication Context Certificate Extension“, [AuthContext], který popisuje, jak je „Authentication Context“ reprezentován v certifikátech X.509 certifikat.

2.3.4. Signature Activation Protocol for Federated Signing

Specifikace „Signature Activation Protocol for Federated Signing“, [Sign.Activation], definuje „Signature Activation Protocol“ (SAP) pro provádění „Sole Control Assurance Level 2“ (SCAL2) podle normy „prEN 419241 – Trustworthy Systems Supporting Server Signing“.

3. Referenční seznam

3.1. DIGG

[Digg.Tillit]

Trust framework for Swedish e-identification.

[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. Další odkazy

[SAML2Int]

SAML V2.0 Deployment Profile for Federation Interoperability.

[DSS]

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

[AuthContext]

RFC-7773: Authentication Context Certificate Extension.