Wprowadzenie do Ram Technicznych Sweden Connect

2024-12-04

Nr ref.: **2019-267**

Spis treści

1. Wprowadzenie

1.1. Przegląd

Ramy Techniczne Sweden Connect są dostosowane do federacji tożsamości opartych na SAML 2.0.

> W najnowszej wersji Ram Technicznych wprowadzono również specyfikacje OpenID Connect. Obecnie nie istnieje wsparcie federacyjne dla OpenID Connect. Zostanie ono wprowadzone w 2025 r.

> Pozostałe części niniejszego dokumentu opisują jedynie federację SAML. Po pełnym wprowadzeniu OpenID Connect dokument ten obejmie również tę technologię.

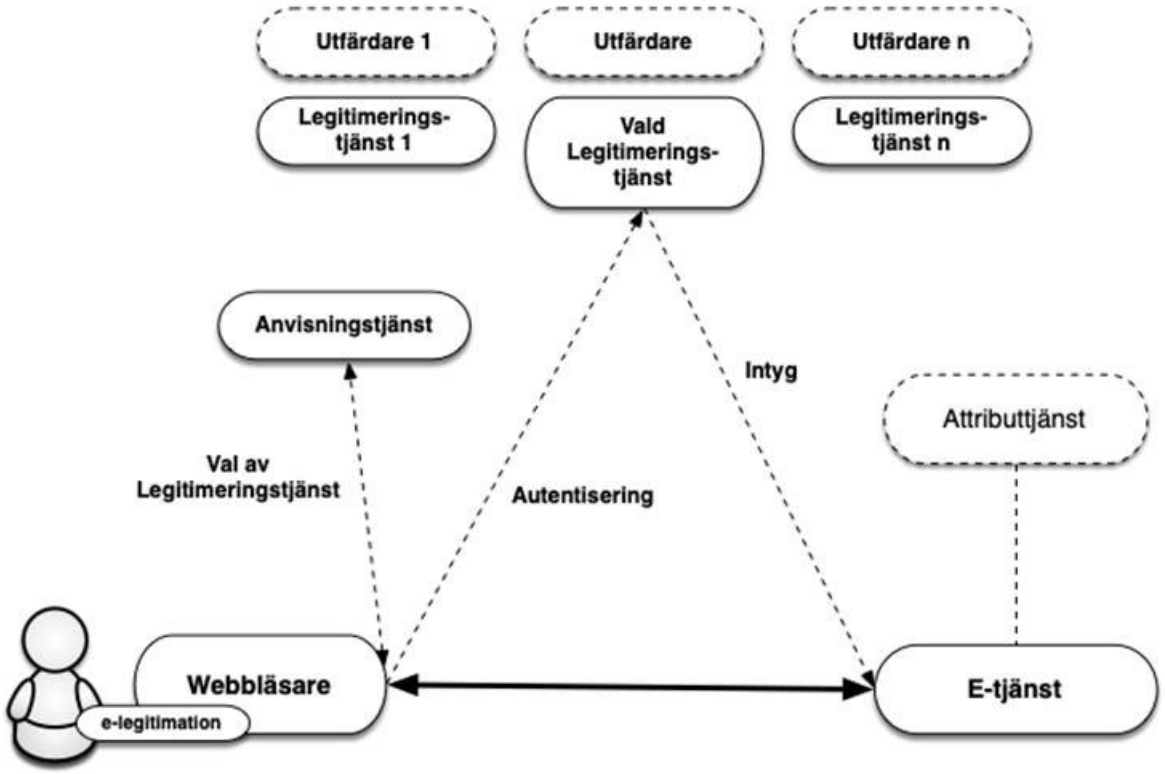
Strony ufające otrzymują certyfikaty tożsamości w znormalizowanym formacie z usługi uwierzytelniania[1].

Usługi elektroniczne wymagające podpisu nie muszą być dostosowywane do różnych identyfikatorów elektronicznych użytkowników w celu tworzenia podpisów elektronicznych. Zamiast tego usługa elektroniczna deleguje to zadanie do usługi podpisu, w ramach której użytkownicy, wspomagani uwierzytelnianiem za pośrednictwem usługi uwierzytelniania, mają możliwość podpisywania dokumentów elektronicznych.

W ramach federacji usługi elektroniczne i odpowiadające im strony ufające pełnią rolę Dostawcy Usług (SP), natomiast usługi uwierzytelniania wystawiające certyfikaty tożsamości pełnią rolę Dostawcy Tożsamości (IdP), a zatem są podmiotem uwierzytelniającym użytkownika, niezależnie od usługi elektronicznej, w której użytkownik jest uwierzytelniany.

W przypadkach, gdy usługa elektroniczna wymaga więcej informacji o użytkowniku, np. informacji o zdolności prawnej, można zadać pytanie usłudze atrybutów, Attribute Authority (AA), w ramach federacji, jeżeli taka odpowiednia usługa atrybutów istnieje. Poprzez żądanie atrybutu usługa elektroniczna może uzyskać niezbędne dodatkowe informacje w celu autoryzacji użytkownika i zapewnienia dostępu do usługi elektronicznej lub jej odpowiednika.

Ponieważ zarówno dane osobowe dotyczące tożsamości, jak i inne atrybuty związane z użytkownikami są dostarczane za pośrednictwem certyfikatów tożsamości i certyfikatów atrybutów, wszystkie rodzaje identyfikatorów elektronicznych, na które strony ufające mają zgodę i które są częścią federacji, mogą być wykorzystywane do uwierzytelniania w odniesieniu do usługi elektronicznej wymagającej zarówno osobistego numeru identyfikacyjnego, jak i dodatkowych informacji, nawet jeśli identyfikator elektroniczny nie zawiera żadnych konkretnych danych osobowych (np. pola kodowe do generowania haseł jednorazowych).



Utfärdare 1	Podmiot wydający 1
Utfärdare n	Podmiot wydający n
Legitimeringstjänst 1	Usługa uwierzytelniania 1
Vald legitimeringstjänst	Wybrana usługa uwierzytelniania
Legitimeringstjänst n	Usługa uwierzytelniania n
Anvisningstjänst	Usługa wyszukiwania
Intyg	Certyfikat
Val av legitimeringstjänst	Wybór usługi uwierzytelniania
autentisering	Uwierzytelnianie
attributtjänst	usługa atrybutu
Webbläsare	Przeglądarka
E-tjänst	Usługa elektroniczna

Rysunek 1 *Ilustracja komunikacji między poszczególnymi usługami w ramach federacji tożsamości.*

> [1]: Usługa uwierzytelniania jest również wymieniana w innej dokumentacji Digg jako usługa identyfikacji i usługa certyfikacji. W niniejszym dokumencie używa się jednak wyłącznie terminu „usługa uwierzytelniania”.

1.2. Ramy zaufania i poziomy bezpieczeństwa

Podstawą do określenia poziomu bezpieczeństwa stosowanego podczas uwierzytelniania użytkownika jest poziom zapewnienia bezpieczeństwa elektronicznej identyfikacji wymagany przez usługę elektroniczną. Aby te poziomy bezpieczeństwa były porównywalne w ramach federacji, w Ramach Zaufania dla szwedzkiej identyfikacji elektronicznej [Digg.Tillit]

zdefiniowano cztery poziomy pewności (1–4), a w unijnym rozporządzeniu eIDAS trzy poziomy pewności (niski, znaczny, wysoki). Wszyscy wystawcy certyfikatów tożsamości muszą wykazać, że cały proces leżący u podstaw wydawania certyfikatów tożsamości spełnia wymogi wymaganego poziomu pewności, w tym:

- wymogi dotyczące sporządzania certyfikatu tożsamości;
- wymogi dotyczące identyfikacji elektronicznej (uwierzytelniania);
- wymogi dotyczące procesu wydawania;
- wymogi dotyczące samej eID i jej użycia;
- wymogi dotyczące podmiotu wydającego eID;
- wymóg ustalenia tożsamości wnioskodawcy eID.

1.3. Usługa gromadzenia, administrowania i publikowania metadanych

Federacja SAML dostarcza informacji o uczestnikach federacji za pośrednictwem metadanych SAML. Zarówno podmioty świadczące usługi uwierzytelniania i atrybutów w federacji, jak i strony ufające, tj. podmioty korzystające z tych usług, np. usługi elektroniczne, uznaje się za uczestników federacji.

Metadane federacji umożliwiają uczestnikom uzyskanie informacji na temat usług innych uczestników, w tym danych niezbędnych do bezpiecznej wymiany informacji między uczestnikami. Metadane muszą być aktualizowane przez każdą ze stron i zgodnie z warunkami umownymi.

Głównym celem metadanych jest dostarczenie kluczy/certyfikatów wymaganych do bezpiecznej komunikacji i wymiany informacji między usługami. Oprócz kluczy metadane zawierają również inne informacje, które są ważne dla interakcji między usługami, takie jak adresy wymaganych funkcji, informacje o poziomach zapewnienia, kategorie usług, informacje o interfejsie użytkownika itp.

Federację tożsamości definiuje rejestr w formacie XML, który jest podpisany certyfikatem operatora federacji. Plik zawiera informacje o członkach federacji tożsamości, w tym o ich certyfikatach. Ponieważ plik metadanych jest podpisany, wystarczy porównać certyfikat z jego odpowiednikiem w metadanych. Infrastruktura oparta na centralnym rejestrze federacji wymaga, aby rejestr był stale aktualizowany, a członkowie federacji zawsze używali najnowszej wersji pliku.

1.4. Usługa wyszukiwania

W federacji tożsamości możliwe jest oferowanie i korzystanie ze wspólnej usługi wyszukiwania, która zawiera listę usług uwierzytelniania dostępnych dla użytkownika do wyboru. Celem takiej usługi wyszukiwania jest zwolnienie poszczególnych usług elektronicznych wchodzących w skład federacji tożsamości z konieczności wdrażania obsługi dotyczącej sposobu, w jaki użytkownicy wybierają usługę uwierzytelniania (lub metodę logowania).

Ponieważ usługa wyszukiwania jest dostępna w ramach federacji tożsamości, usługi elektroniczne mogą kierować tam swoich użytkowników w celu wyboru usługi uwierzytelniania. Usługa wyszukiwania wchodzi w interakcję z użytkownikiem, który dokonuje wyboru, zaś użytkownik wraz ze swoim wyborem zostaje przekierowany z powrotem do usługi elektronicznej, która teraz wie, do której usługi uwierzytelniania należy wysłać użytkownika w celu uwierzytelnienia.

Obecnie nie ma wspólnej usługi wyszukiwania dla federacji Sweden Connect.

1.5. Integracja u strony ufającej

Strony ufające, np. usługi elektroniczne, integrują się z usługami uwierzytelniania za pomocą znormalizowanych komunikatów i korzystają z certyfikatów tożsamości, które mają również znormalizowane formaty.

Na ramy techniczne Sweden Connect ma wpływ profil interoperacyjności „SAML V2.0 Deployment Profile for Federation Interoperability” [SAML2Int]. Profil wspierany jest przez szereg produktów komercyjnych oraz rozwiązań Open Source, co ułatwia integrację w usługach elektronicznych.

Wiele usług elektronicznych korzysta z samodzielnych rozwiązań w zakresie uwierzytelniania, co oznacza, że dostosowanie integracji do ram technicznych ma ograniczony wpływ na usługę elektroniczną jako taką.

1.6. Podpis

Ramy techniczne Sweden Connect umożliwiają korzystanie z różnych rodzajów identyfikacji elektronicznej, nawet tych, które nie są oparte na certyfikatach, bez konieczności specjalnych dostosowań w usłudze elektronicznej. Wynika to z faktu, że elektroniczny certyfikat tożsamości (używany do identyfikacji użytkowników podczas podpisywania) ma ten sam format, niezależnie od rodzaju identyfikacji elektronicznej stosowanej przez użytkownika.

Usługa podpisu ma na celu umożliwienie podpisów w federacjach tożsamości zgodnych z ramami technicznymi, wspieranych przez wszystkie rodzaje identyfikacji elektronicznej, które zapewniają wystarczający stopień bezpieczeństwa.

Dzięki pozyskaniu[1] i wprowadzeniu usługi podpisu cyfrowego strona ufająca, będąca częścią federacji, może zezwolić użytkownikowi na podpisanie dokumentu elektronicznego przy wsparciu usługi podpisu cyfrowego. Podpis elektroniczny użytkownika i związany z nim certyfikat podpisu są tworzone przez usługę podpisu po wyrażeniu przez użytkownika zgody na podpisanie poprzez uwierzytelnienie się w usłudze podpisu[2].

[1]: Możliwe jest również wdrożenie usługi podpisu w oparciu o specyfikacje ram technicznych lub w inny sposób nabycie usługi podpisu.

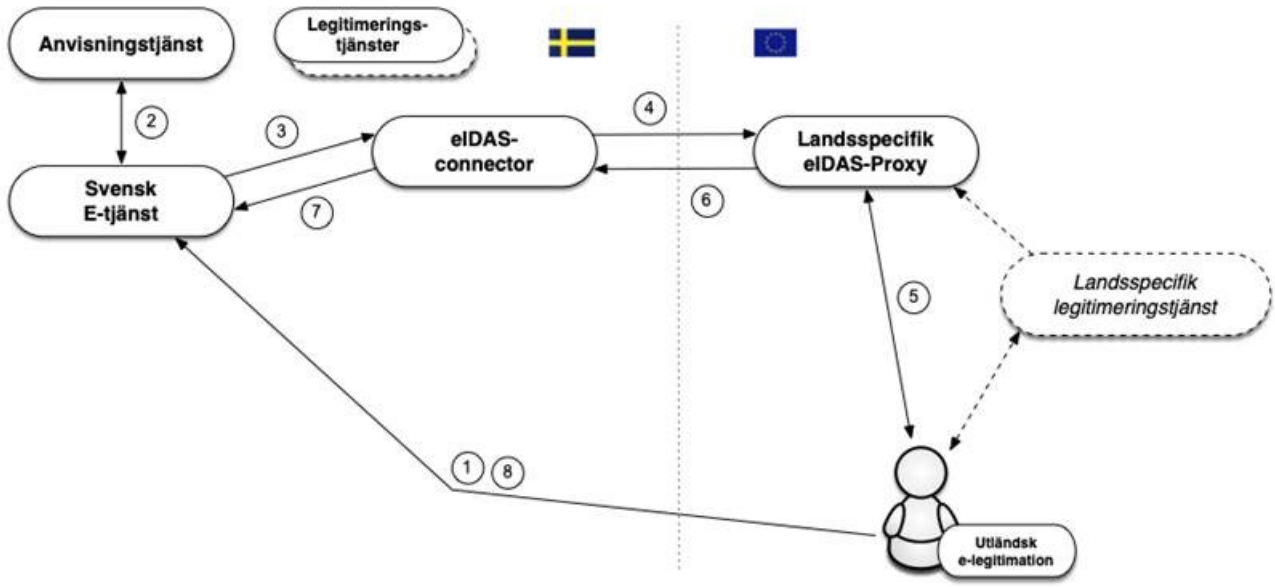
[2]: Należy zauważyć, że niezwykle istotne jest, aby użytkownik postrzegał ten proces jako podpisanie dokumentu. W związku z tym należy stosować przepływ podpisu w przypadku identyfikacji elektronicznych obsługujących tę funkcję w powiązaniu z „uwierzytelnianiem na potrzeby podpisu”.

1.7. Ramy techniczne i eIDAS

Rozporządzenie (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania, eIDAS, wymaga od szwedzkich organów publicznych uznawania identyfikacji elektronicznych zgłoszonych przez inne państwa eIDAS. Oznacza to, że publiczna szwedzka usługa elektroniczna oparta na określonych zasadach musi akceptować logowanie przy użyciu identyfikacji elektronicznej wydanej w innym kraju.

1.7.1. Uwierzytelnianie za pomocą zagranicznych identyfikacji elektronicznych

Specyfikacje techniczne eIDAS opierają się, podobnie jak ramy techniczne, na standardach SAML. Pomimo licznych podobieństw, specyfikacje te różnią się również między sobą. Szwedzka usługa elektroniczna nie powinna jednak odnosić się bezpośrednio do specyfikacji technicznych eIDAS. Poniższy rysunek przedstawia, w jaki sposób szwedzki węzeł eIDAS (*eIDAS-connector*) działa jako pomost między innymi krajami a federacją szwedzką, gdy dana osoba jest uwierzytelniana za pomocą zagranicznej identyfikacji elektronicznej w szwedzkiej usłudze elektronicznej. Szwedzki węzeł eIDAS jest zgodny z ramami technicznymi.



Anvisningstjänst	Usługa wyszukiwania
Legitimeringstjänster	Usługi uwierzytelniania
Svensk E-tjänst	Szwedzka usługa elektroniczna
EiDAS-connector	eiDAS-connector
Landsspecifik Eidas Proxy	Krajowy serwer pośredniczący eIDAS
Landsspecifik legitimeringstjänst	Usługa uwierzytelniania właściwa dla danego kraju
utländsk e-legitimation	zagraniczna identyfikacja elektroniczna

Przepływ jest następujący:

1. Użytkownik posiadający zagraniczną identyfikację elektroniczną składa wniosek o dostęp do szwedzkiej usługi elektronicznej (tj. loguje się).

2. Usługa elektroniczna pozwala użytkownikowi wybrać metodę logowania za pomocą usługi wyszukiwania. Wyświetla się opcja „Zagraniczna identyfikacja elektroniczna", którą użytkownik wybiera w przypadku eIDAS.

3. Usługa elektroniczna tworzy żądanie uwierzytelnienia zgodnie z tymi ramami technicznymi i kieruje użytkownika do szwedzkiego węzła eIDAS (*connector*), za który odpowiada DIGG. Węzeł eIDAS działa jako usługa uwierzytelniania (*Identity Provider*) w federacji wobec szwedzkich stron ufających, co oznacza, że komunikacja z tą usługą odbywa się w taki sam sposób jak z innymi usługami uwierzytelniania w ramach federacji, które są zgodne z ramami technicznymi.

4. Otrzymany wniosek jest przetwarzany, a węzeł eIDAS wyświetla stronę wyboru, na której użytkownik wybiera „swój kraj"[1]. Szwedzki węzeł eIDAS przekształca teraz otrzymane żądanie uwierzytelnienia w żądanie uwierzytelnienia eIDAS i kieruje użytkownika do „usługi proxy eIDAS" wybranego kraju.

5. Po otrzymaniu wniosku o uwierzytelnienie przez usługę proxy eIDAS dla wybranego kraju technologia uwierzytelniania tego kraju przejmuje kontrolę. Nie wszystkie kraje eIDAS używają SAML do uwierzytelniania, ale gdyby tak było w naszym przykładzie, użytkownik zostałby przekierowany do usługi uwierzytelniania (*Identity Provider*), a wcześniej być może również do usługi wyszukiwania służącej do wyboru usługi uwierzytelniania.

6. Po przeprowadzeniu uwierzytelnienia, certyfikat (*Assertion*) jest tworzony zgodnie ze specyfikacjami eIDAS. Certyfikat ten zawiera właściwe dla eIDAS atrybuty identyfikujące użytkownika. Certyfikat ten jest teraz przekazywany do szwedzkiego węzła eIDAS.

7. Węzeł otrzymuje certyfikat i weryfikuje jego dokładność. Certyfikat ten jest przekształcany z formatu eIDAS w certyfikat sformatowany zgodnie z ramami technicznymi i wysyłany do usługi elektronicznej.

8. Strona ufająca dodaje wszelkie dodatkowe informacje i określa, czy użytkownik powinien uzyskać dostęp do usługi.

Szwedzkie usługi elektroniczne muszą zatem jedynie wspierać ramy techniczne, aby móc obsługiwać uwierzytelnianie za pomocą europejskiej identyfikacji elektronicznej. Usługa elektroniczna musi jednak być w stanie obsługiwać przedstawioną tożsamość, która niekoniecznie jest osobistym numerem identyfikacyjnym. W związku z tym mogą wystąpić przypadki, w których usługa elektroniczna uwierzytelnia użytkownika za pośrednictwem ram eIDAS, ale przedstawionej tożsamości użytkownika nie można wykorzystać w usłudze elektronicznej. Więcej informacji na ten temat znajduje się w rozdziale 1.7.3 poniżej.

[1]: W rzeczywistości użytkownik wybiera „usługę pośredniczącą eIDAS", do której wniosek powinien zostać przekazany. Zależy to od kraju, do którego należy podmiot wydający identyfikację elektroniczną użytkownika.

1.7.2. Podpisywanie przy użyciu zagranicznych identyfikacji elektronicznych

Jak już opisano, w niniejszych ramach technicznych stosuje się model podpisu elektronicznego zwany podpisem federowanym. Usługa podpisu oparta na serwerze jest powiązana z usługą elektroniczną, która z kolei żąda podpisu. Gdy użytkownik podpisuje dokument, usługa elektroniczna wysyła żądanie złożenia podpisu do usługi składania podpisu. Usługa podpisu następnie prosi użytkownika o uwierzytelnienie się. W związku z uwierzytelnianiem użytkownik zatwierdza podpis. Usługa podpisu wysyła dane z powrotem do usługi elektronicznej, a następnie dane podpisu skojarzone z podpisanym dokumentem są przechowywane.

Procedura ta umożliwia podpisanie również za pomocą zagranicznej identyfikacji elektronicznej, ponieważ usługa składania podpisu może zdecydować się na uwierzytelnienie użytkownika za pomocą zagranicznej identyfikacji elektronicznej zgodnie z procedurą opisaną powyżej w sekcji 1.7.1.

Podczas podpisywania, w tym przypadku szwedzki węzeł eIDAS odpowiada za poinformowanie użytkownika, żecelem uwierzytelnienia jest podpisanie dokumentu, o osobie, która zażądała podpisu, a także o wszelkich informacjach na temat przedmiotu podpisu. Certyfikat tożsamości jest wydawany dopiero po uwierzytelnieniu się użytkownika (do podpisu) i wysłaniu go do usługi podpisu, która z kolei generuje podpis.

1.7.3. Zarządzanie tożsamościami

Certyfikaty tożsamości z innych państw są zgodne z ogólnounijnymi specyfikacjami technicznymi opracowanymi w ramach rozporządzenia eIDAS. Atrybuty, które każde państwo musi zawsze uwzględniać w odniesieniu do osób fizycznych, jak również organizacji („Minimum Dataset”, MDS), określono w tym rozporządzeniu. Każde państwo musi zawierać niepowtarzalny identyfikator dla każdej identyfikacji elektronicznej reprezentujący tylko jedną osobę fizyczną. W niektórych krajach identyfikatory te będą unikalne i trwałe dla każdej osoby, tak jak na przykład szwedzkie numery identyfikacyjne, ale identyfikatory te mogą mieć bardzo różny skład i cechy. Jedną z cech, która może się różnić, jest trwałość takiego identyfikatora, tj. to, czy taki identyfikator pozostaje niezmieniony przez cały okres życia danej osoby, czy też ulega zmianie, jeśli na przykład osoba przenosi się do innego regionu, zmienia imię i nazwisko lub po prostu zmienia identyfikację elektroniczną. W niektórych krajach (np. w Zjednoczonym Królestwie) identyfikator będzie się różnił w zależności od tego, z której identyfikacji elektronicznej danego kraju użytkownik zdecyduje się obecnie korzystać.

Aby uprościć zarządzanie użytkownikami szwedzkich usług elektronicznych, szwedzki węzeł eIDAS generuje znormalizowany atrybut identyfikacji dla użytkowników, którzy zostali uwierzytelnieni za pomocą zagranicznej identyfikacji elektronicznej, zwany *provisional ID* (w skrócie PRID). Ponadto tworzony jest powiązany atrybut, który deklaruje oczekiwaną trwałość lub okres istnienia tego atrybutu identyfikacji. Atrybut PRID jest generowany na podstawie wartości atrybutów uzyskanych z uwierzytelnienia zagranicznego zgodnie z określonymi metodami dla danego kraju. Każda kombinacja kraju i metody jest klasyfikowana pod względem oczekiwanej trwałości, tj. prawdopodobieństwa, że tożsamość zmieni się w czasie dla tej samej osoby. Umożliwia to szwedzkim usługom elektronicznym dostosowanie komunikacji z użytkownikiem i proaktywne dostarczanie funkcji ułatwiających

użytkownikowi, którego tożsamość uległa zmianie, odzyskanie kontroli nad swoimi informacjami w usłudze elektronicznej.

W niektórych przypadkach osoba uwierzytelniona za pomocą zagranicznej identyfikacji elektronicznej może również posiadać szwedzki osobisty numer identyfikacyjny. Może to być na przykład obywatel Szwecji, który przeprowadził się za granicę i uzyskał zagraniczną identyfikację elektroniczną, lub cudzoziemiec, który jest zarejestrowany w Szwecji i któremu przydzielono osobisty numer identyfikacyjny.

Fakt, że osoba posiadająca zagraniczną identyfikację elektroniczną posiada szwedzki osobisty numer identyfikacyjny, nie jest zwykle znany zagranicznym służbom uwierzytelniającym, a zatem informacje te nie są zawarte w certyfikacie tożsamości z państwa, w którym dana osoba została uwierzytelniona. Szwedzki węzeł ma z drugiej strony możliwość zapytania usługi atrybutów w Szwecji[1], czy istnieje zarejestrowany osobisty numer identyfikacyjny dla uwierzytelnionej osoby i może, jeśli tak jest, dodać takie informacje do certyfikatu tożsamości wysyłanego do usługi elektronicznej.

> [1]: Na moment opracowania niniejszego dokumentu nie istnieje usługa atrybutu, która ustanawiałaby powiązanie między tożsamościami eIDAS a szwedzkimi osobistymi numerami identyfikacyjnymi.

1.7.4. Szwedzkie identyfikacje elektroniczne w zagranicznych usługach elektronicznych

Szwecja zgłosiła szwedzkie identyfikacje elektroniczne na poziomach pewności znacznym i wysokim zgodnie z eIDAS.

Wniosek o uwierzytelnienie z zagranicznej usługi elektronicznej jest składany do szwedzkiego węzła eIDAS (usługa pośrednicząca) za pośrednictwem eIDAS connector w kraju usługi elektronicznej. W szwedzkim węźle eIDAS użytkownik wybiera, której szwedzkiej identyfikacji elektronicznej chce użyć do uwierzytelnienia, a następnie żądanie uwierzytelnienia jest wysyłane do usługi uwierzytelniania (*Identity Provider*) obsługującej wybraną identyfikację elektroniczną. Żądanie to jest sformatowane zgodnie z ramami technicznymi, co oznacza, że szwedzka usługa uwierzytelniania nie musi być zgodna ze specyfikacjami technicznymi eIDAS.

Użytkownik jest uwierzytelniany przez szwedzką usługę uwierzytelniania i wystawiany jest certyfikat tożsamości (zgodnie z ramami technicznymi). Certyfikat ten jest odbierany przez szwedzką usługę pośredniczącą eIDAS i przekształcany w certyfikat zgodnie ze specyfikacjami eIDAS przed przekazaniem go do zagranicznego eIDAS connector, a następnie do wywołującej usługi elektronicznej (*Service Provider*).

2. Specyfikacje techniczne

Ten rozdział zawiera specyfikacje i profile dla federacji tożsamości, które są zgodne z ramami technicznymi Sweden Connect, oraz niektóre powiązane usługi. O ile nie zaznaczono inaczej, dokumenty te mają charakter normatywny w zakresie świadczenia usług w ramach federacji tożsamości wdrażających ramy techniczne.

2.1. Profile i specyfikacje SAML

Federacje tożsamości, które są zgodne z ramami technicznymi Sweden Connect, opierają się na „Profilu wdrażania szwedzkich ram identyfikacji elektronicznej” [SAML.Profile]. Na profil ten ma wpływ „SAML V2.0 Deployment Profile for Federation Interoperability” [SAML2Int], ale nie jest on od niego zależny pod względem normatywnym. [SAML.Profil] zawiera również zasady i wytyczne specyficzne dla ram technicznych Sweden Connect.

2.1.1. Deployment Profile for the Swedish eID Framework

„Deployment Profile for the Swedish eID Framework” [SAML.Profile] jest głównym technicznym dokumentem ramowym i określa między innymi:

- sposób, w jaki metadane SAML powinny być konstruowane i interpretowane;
- sposób formatowania wniosku o uwierzytelnienie;
- sposób obsługi wniosku o uwierzytelnienie oraz sposób projektowania, weryfikacji i obsługi certyfikatu tożsamości;
- wymogi bezpieczeństwa;
- szczególne wymogi SAML dotyczące usług podpisu i „uwierzytelniania do podpisu”.

2.1.2. Swedish eID Framework – Registry for identifiers

Wdrożenie szwedzkiej infrastruktury identyfikacji elektronicznej wymaga różnych form identyfikatorów do reprezentowania obiektów w strukturach danych. Dokument „Sweden Connect – Registry for identifiers” [SC.Registry] definiuje strukturę identyfikatorów przydzielonych w ramach technicznych, a także rejestr zdefiniowanych identyfikatorów.

2.1.3. Attribute Specification for the Swedish eID Framework

Specyfikacja „Attribute Specification for the Swedish eID Framework”, [SAML.Attributes], określa profile atrybutów SAML, które są używane w federacjach tożsamości zgodnych z ramami technicznymi, w tym tych, które łączą się z eIDAS przez szwedzki węzeł eIDAS.

2.1.4. Entity Categories for the Swedish eID Framework

Kategorie podmiotów są wykorzystywane w ramach federacji do różnych celów:

- Kategorie podmiotów usługowych – wykorzystywane w metadanych do reprezentowania wymogów usług elektronicznych dotyczących poziomów pewności i wymaganych atrybutów, a także spełniania poziomów pewności i dostarczania atrybutów przez usługi uwierzytelniania.
- Kategorie właściwości usług – używane do reprezentowania określonej cechy charakterystycznej usługi.

- Kategorie podmiotów typu usługa – wykorzystywane do reprezentowania różnych rodzajów usług w ramach federacji.

- Kategorie podmiotów umowy o świadczenie usług – wykorzystywane przez usługi do ogłaszania formularzy umów i tym podobnych.

- Kategorie podmiotów ogólnych – kategorie podmiotów, które nie należą do żadnego z powyższych typów.

Specyfikacja „Entity Categories for the Swedish eID Framework" [SAML.EntCat] określa kategorie podmiotów zdefiniowane w ramach technicznych i opisuje ich znaczenie.

2.1.5. eIDAS Constructed Attributes Specification for the Swedish eID Framework

Specyfikacja „eIDAS Constructed Attributes Specification for the Swedish eID Framework", [SC.eIDAS.Attrs], określa procesy i zasady dotyczące sposobu, w jaki atrybuty identyfikacji są skonstruowane w oparciu o atrybuty otrzymane podczas uwierzytelniania w eIDAS.

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

Specyfikacja „Implementation Profile for BankID Identity Providers within the Swedish eID Framework", [SAML.BankID], określa zasady dotyczące tego, jak usługa uwierzytelniania, która wdraża wsparcie dla BankID, powinna zostać zaprojektowana.

> **Należy zwrócić uwagę na następujące kwestie:** Niniejsza specyfikacja nie jest normatywna w odniesieniu do zgodności z ramami technicznymi. Dotyczy tylko usług uwierzytelniania, które wdrażają wsparcie dla BankID i usług elektronicznych, które z nich korzystają. Jednak usługi uwierzytelniania, które wdrażają wsparcie dla BankID i chcą połączyć się z federacją Sweden Connect, muszą być zgodne z tą specyfikacją.

2.1.7. Principal Selection in SAML Authentication Requests

Specyfikacja „Principal Selection in SAML Authentication Requests", [SAML.Principal], określa rozszerzenie SAML, które umożliwia stronie ufającej poinformowanie usługi uwierzytelniania, którą tożsamość chce uwierzytelnić.

2.1.8. User Message Extension in SAML Authentication Requests

W specyfikacji „User Message Extension in SAML Authentication Requests", [SAML.UMessage], zdefiniowano rozszerzenie SAML, które umożliwia stronie ufającej włączenie komunikatu wyświetlanego w żądaniu uwierzytelnienia wysyłanym do usługi uwierzytelniania. Usługa uwierzytelniania może następnie wyświetlić tę wiadomość użytkownikowi podczas etapu uwierzytelniania.

2.2. Profile i specyfikacje OpenID Connect

2.2.1. OpenID Connect Profile for Sweden Connect

Profil „OpenID Connect Profile for Sweden Connect”, [OIDC.Profile], opiera się na szwedzkim profilu OpenID Connect, który jest profilem OpenID Connect opracowanym przez OIDC Sweden w celu promowania interoperacyjności i bezpieczeństwa w ramach szwedzkich rozwiązań OIDC.

[OIDC.Profile] dodaje dodatkowe wymagania dotyczące federacji Sweden Connect.

2.2.2. OpenID Connect Claims and Scopes Specification for Sweden Connect

Specyfikacja „OpenID Connect Claims and Scopes Specification for Sweden Connect”, [OIDC.Claims], opiera się na specyfikacji Claims and Scopes Specification for the Swedish OpenID Connect Profile OIDC Sweden.

2.3. Specyfikacje dotyczące podpisu

Ta sekcja zawiera odniesienia do dokumentów definiujących usługi podpisu w federacjach, które są zgodne z ramami technicznymi Sweden Connect.

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

Profil wdrożenia „Implementation Profile for Using OASIS DSS in Central Signing Services”, [Sign.DSS.Profile], określa profil dla żądania podpisu i odpowiedzi zgodnie ze standardem 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], jest rozszerzeniem standardu OASIS „Digital Signature Service Core Protocols, Elements, and Bindings”, [DSS], w którym określono definicje niezbędne do podpisywania zgodnie z ramami technicznymi.

2.3.3. Certificate Profile for Certificates Issued by Central Signing Services

Profil certyfikatu „Certificate profile for certificates issued by Central Signing services”, [Sign.Cert.Profile], określa treść certyfikatów podpisujących. Ten profil stosuje nowe rozszerzenie certyfikatu do obsługi usług podpisu.

Profil ten odnosi się do „Authentication Context Certificate Extension”, [AuthContext], który opisuje, w jaki sposób „Authentication Context” jest reprezentowany w certyfikatach X.509.

2.3.4. Signature Activation Protocol for Federated Signing

W specyfikacji „Signature Activation Protocol for Federated Signing”, [Sign.Activation], zdefiniowano „Signature Activation Protocol” (SAP) do celów wdrożenia „Sole Control Assurance Level 2” (SCAL2) zgodnie z normą „prEN 419241 – Trustworthy Systems Supporting Server Signing”.

3. Wykaz odniesień

3.1. DIGG

[Digg.Tillit]

Ramy zaufania dla szwedzkiej identyfikacji elektronicznej.

[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. Inne odnośniki

[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.