

Introduzzjoni għall-Qafas Tekniku Sweden Connect

2024-12-04

Numru ta' referenza: 2019-267

Copyright © Aġenzija għall-Gvern Diġitali (Digg), 2015-2024.

Werrej

1. [Introduzzjoni](#)
 - 1.1. Harsa ġenerali
 - 1.2. Qafas ta' fiduċja u livelli ta' sigurtà
 - 1.3. Servizz għall-ġbir, l-amministrazzjoni u l-pubblikazzjoni tal-metadati
 - 1.4. Servizz ta' skoperta
 - 1.5. Integrazzjoni fil-parti dipendenti
 - 1.6. Firma
 - 1.7. Qafas tekniku u eIDAS
 - 1.7.1. Awtentikazzjoni bl-użu ta' identifikazzjonijiet elettronici barranin
 - 1.7.2. Firem li jużaw identifikazzjonijiet elettronici barranin
 - 1.7.3. Ġestjoni tal-identitajiet
 - 1.7.4. Identifikazzjonijiet elettronici Żvedizi f'servizzi elettronici barranin
2. [Speċifikazzjonijiet tekniċi](#)
 - 2.1. Profili u speċifikazzjonijiet għall-SAML
 - 2.1.1. Profil tal-Varar għall-Qafas Żvediz tal-Identifikazzjoni Elettronika

- 2.1.2. Qafas Żvediż tal-Identifikazzjoni Elettronika – Reġistru għall-identifikaturi
- 2.1.3. Speċifikazzjoni tal-Attributi għall-Qafas Żvediż tal-Identifikazzjoni Elettronika
- 2.1.4. Kategoriji tal-Entità għall-Qafas Żvediż tal-Identifikazzjoni Elettronika
- 2.1.5. eIDAS Speċifikazzjoni tal-Attributi Mibnija għall-Qafas Żvediż tal-Identifikazzjoni Elettronika
- 2.1.6. Profil ta' Implimentazzjoni għal BankID Fornituri tal-Identità fi hdan il-Qafas Żvediż tal-Identifikazzjoni Elettronika
- 2.1.7. Għażla Prinċipali fit-Talbiet għall-Awtentikazzjoni tal-SAML
- 2.1.8. Estensjoni tal-Messaġġ tal-Utent fit-Talbiet ta' Awtentikazzjoni tal-SAML
- 2.2. Profili u speċifikazzjonijiet għal OpenID Connect
- 2.2.1. Profil ta' OpenID Connect għal Sweden Connect
- 2.2.2. Talbiet u Ambiti ta' OpenID Connect Speċifikazzjoni għal Sweden Connect
- 2.3. Speċifikazzjonijiet għal Firma
- 2.3.1. Profil ta' Implimentazzjoni għall-użu tad-DSS tal-OASIS fis-Servizzi Ċentrali tal-Iffirmar
- 2.3.2. Estensjoni tad-DSS għas-Servizzi Ċentrali Federati tal-Iffirmar
- 2.3.3. Profil taċ-Ċertifikat għaċ-Ċertifikati Maħruġa mis-Servizzi Ċentrali tal-Iffirmar
- 2.3.4. Protokoll ta' Attivazzjoni tal-Firma għall-Iffirmar Federat

3. [Lista ta' referenza](#)

- 3.1. DIGG
- 3.2. Referenzi oħra

1. Introduzzjoni

1.1. Harsa ġenerali

Il-Qafas Tekniku Sweden Connect huwa adattat għall-federazzjonijiet tal-identità abbażi tal-SAML 2.0.

Fl-aħħar verżjoni tal-Qafas Tekniku, ġew introdotti wkoll speċifikazzjonijiet għal OpenID Connect. Bhalissa, ma hemm l-ebda appoġġ tal-federazzjoni għal OpenID Connect. Dan se jiġi introdott fl-2025.

Il-partijiet li jifdal ta' dan id-dokument jiddeskrivu biss il-federazzjoni SAML. Ladarba OpenID Connect ikun ġie introdott bis-sħiħ, dan id-dokument se jkopri wkoll din it-teknoloġija.

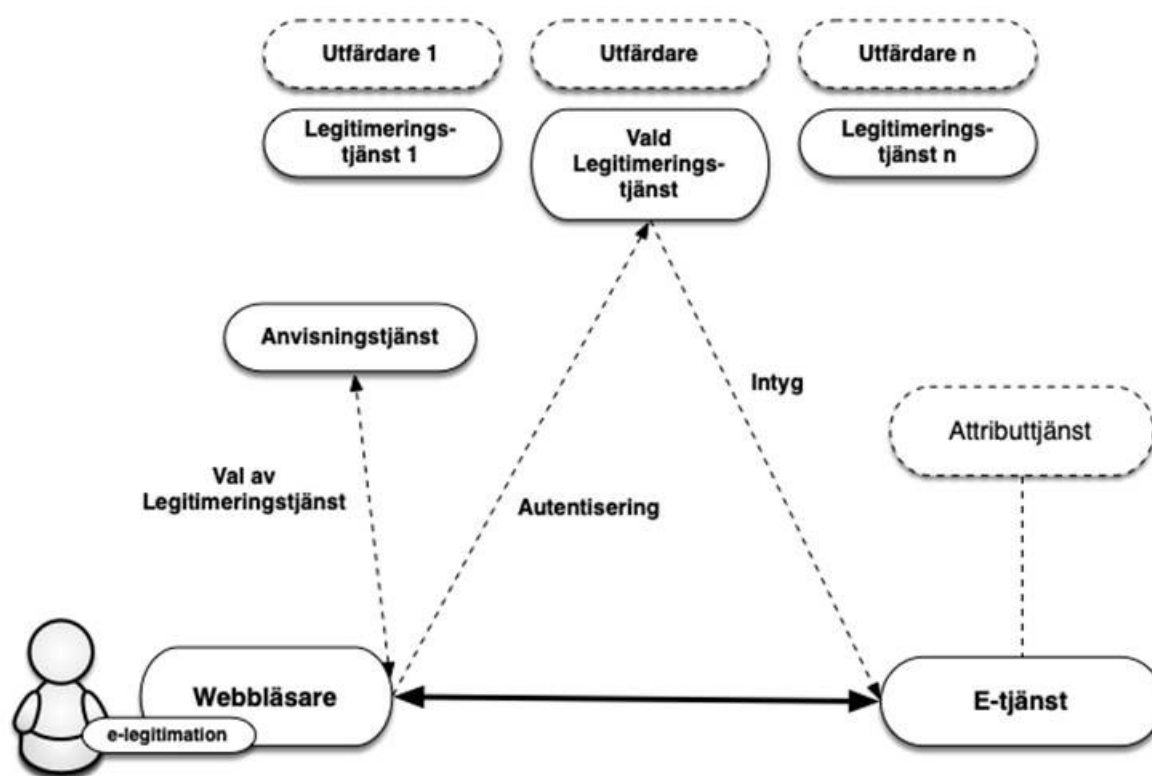
Il-partijiet dipendenti jirċievu ċertifikati tal-identità f'format standardizzat minn servizz ta' awtentikazzjoni¹.

Is-servizzi elettronici li jirrikjedu firma ma għandhomx bżonn jiġu adattati għall-identifikazzjonijiet elettronici tal-utenti differenti sabiex jinholqu firem elettronici. Minflok, is-servizz elettroniku jiddelega dan lil servizz ta' firma, fejn l-utenti, appoġġati minn awtentikazzjoni permezz ta' servizz ta' awtentikazzjoni, jingħataw l-opportunità li jiffirmaw dokumenti elettronici.

Fi hdan il-federazzjoni, is-servizzi elettronici u l-partijiet dipendenti korrispondenti jassumu r-rwol ta' Fornitur tas-Servizz (SP), filwaqt li s-servizzi ta' awtentikazzjoni li joħorġu ċertifikati tal-identità jassumu r-rwol ta' Fornitur tal-Identità (IdP) u b'hekk l-awtentikatur tal-utent, irrISPettivament mis-servizz elettroniku li għalih l-utent ikun qed jiġi awtentikat.

Għal dawk il-każijiet fejn is-servizz elettroniku jehtieg aktar informazzjoni dwar l-utent, eż. informazzjoni dwar il-kapaċità legali, tista' ssir mistoqsija lil servizz ta' attribut, Attribute Authority (AA), fi hdan il-federazzjoni, jekk ikun jeżisti tali servizz ta' attributi rilevanti. Permezz ta' talba għal attribut, is-servizz elettroniku jista' jikseb l-informazzjoni addizzjonali meħtieġa biex jawtorizza lill-utent u jipprovdi aċċess għas-servizz elettroniku jew ekwivalenti.

Peress li kemm id-data tal-identità personali kif ukoll attributi oħra assoċjati mal-utenti jiġu pprovduti permezz ta' ċertifikati tal-identità u ċertifikati tal-attributi, it-tipi kollha ta' identifikazzjonijiet elettronici li l-partijiet dipendenti għandhom ftehim dwarhom u li huma parti mill-federazzjoni jistgħu jintużaw għall-awtentikazzjoni vis-à-vis is-servizz elettroniku li jirrikjedi kemm numru tal-identità personali kif ukoll informazzjoni addizzjonali, anke jekk l-identifikazzjoni elektronika ma jkun fiha l-ebda data personali speċifika (eż. kaxxi tal-kodiċi għall-ġenerazzjoni ta' passwords ta' darba).



Utfärdare 1	Emittent 1
Utfärdare n	Emittent n
Legitimeringstjänst 1	Servizz ta' awtentikazzjoni 1
Vald legitimeringstjänst	Servizz ta' awtentikazzjoni magħżul
Legitimeringstjänst n	Servizz ta' awtentikazzjoni n
Anvisningstjänst	Servizz ta' skoperta
Intyg	Ċertifikat
Val av legitimeringstjänst	Għażla tas-servizz ta' awtentikazzjoni
autentisering	awtentikazzjoni
attributtjänst	servizz tal-attributi
Webbläsare	Brawżer
E-tjänst	Servizz elettroniku

Figura 1: *Illustrazzjoni tal-komunikazzjoni bejn is-servizzi differenti fi ħdan federazzjoni tal-identità.*

[1]: Is-servizz ta' awtentikazzjoni jissewma wkoll f' dokumentazzjoni oħra minn Digg bħala servizz tal-identità u servizz ta' ċertifikazzjoni. Madankollu, f'dan id-dokument, jintuża biss it-terminu "servizz ta' awtentikazzjoni".

1.2. Qafas ta' fiduċja u livelli ta' sigurtà

Il-bażi li għaliha għandu jiġi applikat il-livell ta' sigurtà meta utent ikun qed jiġi awtentikat hija l-livell ta' assigurazzjoni għall-identifikazzjoni elettronika meħtieġa mis-servizz elettroniku. Sabiex dawn il-livelli ta' sigurtà jkunu komparabbli fil-qafas tal-federazzjoni, erba' livelli ta' assigurazzjoni (1-4) huma definiti fil-Qafas ta' Fiducja għall-identifikazzjoni

elettronika Żvediża [Digg.Tillit] u tliet livelli ta' assigurazzjoni (baxx, sostanzjali, għoli) fir-Regolament eIDAS tal-UE. L-emittenti kollha taċ-ċertifikati tal-identità jeħtiġilhom juru li l-proċess kollu li jirfed il-ħruġ taċ-ċertifikati tal-identità jissodisfa r-rekwiżiti tal-livell ta' assigurazzjoni meħtieġ, inklużi:

- rekwiżiti għall-ħolqien taċ-ċertifikat tal-identità;
- rekwiżiti għall-identifikazzjoni elettronika (awtentikazzjoni);
- ir-rekwiżiti għall-proċess tal-ħruġ;
- ir-rekwiżiti għall-identifikazzjoni elettronika nnifisha u l-użu tagħha;
- rekwiżiti għall-emittent tal-identifikazzjoni elettronika;
- rekwiżit għall-istabbiliment tal-identità tal-applikant tal-identifikazzjoni elettronika.

1.3. Servizz għall-ġbir, l-amministrazzjoni u l-pubblikazzjoni tal-metadata

Federazzjoni tal-SAML tipprovdi informazzjoni dwar il-parteciċipanti tal-federazzjoni permezz tal-metadata tal-SAML. Iz-żewġ entitajiet li jipprovdu servizzi ta' awtentikazzjoni u attributi fil-federazzjoni kif ukoll il-partijiet dipendenti, jiġifieri entitajiet li jikkunsmaw dawn is-servizzi, eż. servizzi elettronici, jitqiesu bħala parteciċipanti f'federazzjoni.

Il-metadata tal-federazzjoni tippermetti lill-parteciċipanti jiksbu informazzjoni dwar is-servizzi ta' parteciċipanti oħra, inkluża d-data neċessarja għall-iskambju sigur ta' informazzjoni bejn il-parteciċipanti. Il-metadata trid tinżamm aġġornata minn kull parti u f'konformità mal-kundizzjonijiet kuntrattwali.

L-għan ewlieni tal-metadata huwa li tipprovdi l-kjavi/iċ-ċertifikati meħtieġa għall-komunikazzjoni sigura u l-iskambju ta' informazzjoni bejn is-servizzi. Minbarra l-kjavi, il-metadata fiha wkoll informazzjoni oħra li hija importanti għall-interazzjoni bejn is-servizzi, bħall-indirizzi tal-funzjonijiet meħtieġa, informazzjoni dwar il-livelli ta' assigurazzjoni, il-kategoriji tas-servizzi, l-informazzjoni dwar l-interfaċċa tal-utent, eċċ.

Federazzjoni tal-identità hija definita minn reġistru fil-format XML li huwa ffirmat biċ-ċertifikat tal-operatur tal-federazzjoni. Il-fajl fih informazzjoni dwar il-membri tal-federazzjoni tal-identità, inklużi ċ-ċertifikati tagħhom. Peress li l-fajl tal-metadata huwa ffirmat, huwa biżżejjed li jitqabbel ċertifikat mal-kontroparti tal-metadata tiegħu. Infrastruttura bbażata fuq reġistru ċentrali tal-federazzjoni tirrikjedi li r-reġistru jiġi aġġornat kontinwament u li l-membri tal-federazzjoni dejjem jużaw l-aħħar verżjoni tal-fajl.

1.4. Servizz ta' skoperta

F'federazzjoni tal-identità, huwa possibbli li jiġi offrut u kkunsmat servizz ta' skoperta kondiviż, li jelenka s-servizzi ta' awtentikazzjoni disponibbli għall-utent li jista' jagħżel minnhom. L-iskop ta' tali servizz ta' skoperta huwa li jehles lis-servizzi elettronici individwali li huma parti mill-federazzjoni tal-identità milli jimplimentaw appoġġ fir-rigward ta' kif l-utenti jagħżlu s-servizz ta' awtentikazzjoni (jew il-metodu ta' login).

Peress li s-servizz ta' skoperta huwa disponibbli fi hdan il-federazzjoni tal-identità, is-servizzi elettronici jistgħu jidderieġu lill-utenti tagħhom hemmhekk sabiex jagħzlu s-servizz ta' awtentikazzjoni. Is-servizz ta' skoperta jinteraġixxi mal-utent li jagħmel l-għażla tiegħu, u l-utent, flimkien mal-għażla tiegħu, jiġi dirett lura lejn is-servizz elettroniku, li issa jaf lil liema servizz ta' awtentikazzjoni għandu jintbagħat l-utent għall-awtentikazzjoni.

Bħalissa ma hemm l-ebda servizz ta' skoperta kondiviz għall-federazzjoni Sweden Connect.

1.5. Integrazzjoni fil-parti dipendenti

Il-partijiet dipendenti, eż. is-servizzi elettronici, jintegraw ma' servizzi ta' awtentikazzjoni permezz ta' messaġġi standardizzati u jikkunsmaw ċertifikati tal-identità li għandhom ukoll formati standardizzati.

Il-qafas tekniku Sweden Connect huwa influwenzat mill-profil tal-interoperabbiltà "Profil tal-Varar għall-Interoperabbiltà tal-Federazzjoni SAML V2.0" [SAML2Int]. Il-profil huwa appoġġat minn għadd ta' prodotti kummerċjali u soluzzjonijiet b'Sors Miftuħ, li jiffacilitaw l-integrazzjoni fis-servizzi elettronici.

Ħafna servizzi elettronici jużaw soluzzjonijiet ta' awtentikazzjoni awtonomi, li jfisser li l-adattament tal-integrazzjoni biex tintlaħaq konformità mal-qafas tekniku għandu impatt limitat fuq is-servizz elettroniku bħala tali.

1.6. Firma

Meta jsiru firem, il-qafas tekniku Sweden Connect jagħmilha possibbli li jintużaw tipi differenti ta' identifikazzjoni elettronika, anke dawk li mhumiex ibbażati fuq iċ-ċertifikati, mingħajr il-htieġa ta' adattamenti speċjali fis-servizz elettroniku. Dan għaliex iċ-ċertifikat tal-identità maħruġ elettronikament (użat għall-identifikazzjoni tal-utenti meta jiffirmaw) għandu l-istess format irrispettivament mit-tip ta' identifikazzjoni elettronika użat mill-utent.

Servizz ta' firma għandu l-għan li jippermetti firem fi hdan il-federazzjonijiet tal-identità li jikkonformaw mal-qafas tekniku, appoġġati mit-tipi kollha ta' identifikazzjoni elettronika li joffru livell suffiċjenti ta' sigurtà.

Permezz tal-akkwist¹ u l-introduzzjoni ta' servizz ta' firma, parti dipendenti li hija parti mill-federazzjoni tista' tippermetti lil utent jiffirma dokument elettroniku bl-appoġġ tas-servizz tal-firma. Il-firma elettronika tal-utent u ċ-ċertifikat ta' ffirmar assoċjat jinħolqu mis-servizz ta' firma wara li l-utent ikun qabel li jiffirma billi jawtentika lill-utent vis-à-vis is-servizz tal-firma².

[1]: Huwa possibbli wkoll li jiġi implimentat servizz ta' firma bbażat fuq l-ispeċifikazzjonijiet tal-qafas tekniku, jew inkella li jinkiseb servizz ta' firma.

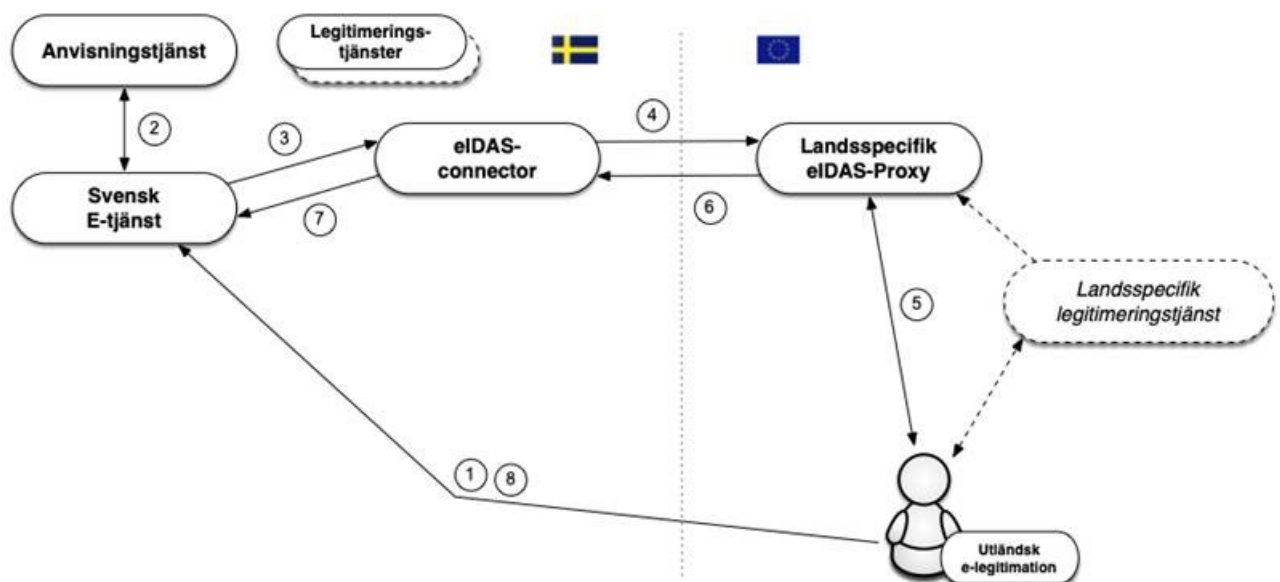
[2]: Huwa importanti li wiehded jinnota li huwa tal-akbar importanza li l-utent jipperċepixxi dan il-proċess bħala ffirmar ta' dokument. Għalhekk, għandu jintuża fluss ta' firem għall-identifikazzjonijiet elettronici li jappoġġaw dan b'raba mal-"awtentikazzjoni għall-firma".

1.7. Qafas tekniku u eIDAS

Ir-Regolament tal-UE (910/2014) dwar l-identifikazzjoni elettronika u s-servizzi ta' fiduċja, eIDAS, jirrikjedi li l-korpi pubbliċi Żvediżi jirrikonoxxu l-identifikazzjonijiet elettronici li pajjiżi oħra tal-eIDAS ikunu nnotifikaw. Dan ifisser li servizz elettroniku pubbliku Żvediż ibbażat fuq ċerti regoli għandu jkun jista' jaċċetta login imwettaq bl-użu ta' identifikazzjoni elettronika maħruġa f'pajjiż ieħor.

1.7.1. Awtentikazzjoni bl-użu ta' identifikazzjonijiet elettronici barranin

L-ispeċifikazzjonijiet tekniċi għall-eIDAS huma bbażati, bħall-qafas tekniku, fuq l-istandards tal-SAML, u għalkemm hemm ħafna similaritajiet, hemm ukoll differenzi f'dawn l-ispeċifikazzjonijiet. Madankollu, servizz elettroniku Żvediż ma għandux ikun relatat direttament mal-ispeċifikazzjonijiet tekniċi tal-eIDAS. L-istampa ta' hawn taħt turi kif in-nodu tal-eIDAS Żvediż (*konnnettur tal-eIDAS*) jaġixxi bħala pont bejn pajjiżi oħra u l-federazzjoni Żvediża meta persuna tkun qed tiġi awtentikata bl-użu ta' identifikazzjoni elettronika barranija f'servizz elettroniku Żvediż. In-nodu tal-eIDAS Żvediż jikkonforma mal-qafas tekniku.



Anvisningstjänst	Servizz ta' skoperta
Legitimeringstjänster	Servizzi ta' awtentikazzjoni
Svensk E-tjänst	Servizz elettroniku Żvediż
EiDAS-connector	Konnnettur tal-eiDAS
Landsspecifik Eidas Proxy	Proxy eIDAS speċifiku għall-pajjiż
Landsspecifik legitimeringstjänst	Servizz ta' awtentikazzjoni speċifiku għall-pajjiż
utländsk e-legitimation	Identifikazzjoni elettronika barranija

Il-fluss huwa kif ġej:

1. Utent b'identifikazzjoni elettronika barranija jitlob aċċess għal servizz elettroniku Żvediz (jiġifieri jilloggja).
2. Is-servizz elettroniku jippermetti lill-utent jagħzel il-metodu tal-login bl-użu ta' servizz ta' skoperta. Tintwera għażla ta' "Identifikazzjoni Elettronika Barranija", li tintgħażel mill-utent fil-każ tal-eIDAS.
3. Is-servizz elettroniku jgħid talba ta' awtentikazzjoni f'konformità ma' dan il-qafas tekniku u jiehu lill-utent fin-nodu tal-eIDAS Żvediz (*konnnettur*) li għalih hija responsabbli d-DIGG. In-nodu tal-eIDAS jaġixxi bħala servizz ta' awtentikazzjoni (*Fornitur tal-Identità*) fil-federazzjoni vis-à-vis il-partijiet dipendenti Żvedizi, li jfisser li l-komunikazzjoni ma' dan is-servizz issir bl-istess mod bħal ma jsir ma' servizzi oħra ta' awtentikazzjoni fi hdan il-federazzjonijiet li jikkonformaw mal-qafas tekniku.
4. It-talba riċevuta tiġi pproċessata u n-nodu tal-eIDAS juri paġna tal-għażla fejn l-utent jagħzel "pajjiżu"¹. In-nodu tal-eIDAS Żvediz issa jikkonverti t-talba ta' awtentikazzjoni riċevuta f'talba ta' awtentikazzjoni tal-eIDAS u jiehu lill-utent fis-"servizz proxy tal-eIDAS" tal-pajjiż magħżul.
5. Meta t-talba ta' awtentikazzjoni tasal għand is-servizz proxy tal-eIDAS għall-pajjiż magħżul, it-teknoloġija tal-awtentikazzjoni ta' dan il-pajjiż tiegħu kontroll. Mhux il-pajjiżi kollha tal-eIDAS jużaw l-SAML għall-awtentikazzjoni, iżda jekk dan ikun il-każ fl-eżempju tagħna, l-utent jittiehed fis-servizz ta' awtentikazzjoni (*Fornitur tal-Identità*), u qabel dan forsi wkoll servizz ta' skoperta għall-għażla tas-servizz ta' awtentikazzjoni.
6. Ladarba tkun twettqet l-awtentikazzjoni, jinholq ċertifikat (*Asserzjoni*) skont l-ispeċifikazzjonijiet tal-eIDAS. Dan iċ-ċertifikat jinkludi attributi speċifiċi għall-eIDAS li jidentifikaw l-utent. Dan iċ-ċertifikat issa qed jintbagħat lin-nodu Żvediz tal-eIDAS.
7. In-nodu jirċievi iċ-ċertifikat u jivvalida l-akkuratezza tiegħu. Dan iċ-ċertifikat jiġi ttrasformat minn format eIDAS għal ċertifikat ifformattjat skont il-qafas tekniku u jintbagħat lis-servizz elettroniku.
8. Il-parti dipendenti żżid kwalunkwe informazzjoni addizzjonali u tiddetermina jekk l-utent għandux jingħata aċċess għas-servizz.

Għalhekk, is-servizzi elettroniċi Żvedizi jehtiegu biss li jappoġġaw il-qafas tekniku sabiex jittrattaw awtentikazzjoni mwettqa bl-użu ta' identifikazzjoni elettronika Ewropea. Madankollu, is-servizz elettroniku jehtieglu jkun kapaċi jittratta l-identità ppreżentata, li mhux neċessarjament tkun numru tal-identità personali. Għalhekk, jista' jkun hemm każijiet li fihom servizz elettroniku jawtentika utent permezz tal-qafas eIDAS, iżda l-identità ppreżentata tal-utent ma tkunx tista' tintuża fis-servizz elettroniku. Aktar dwar dan fil-Kapitolu 1.7.3 hawn taht.

[1]: Fil-fatt, l-utent jagħzel is-"servizz proxy tal-eIDAS" li lilu għandha tintbagħat it-talba. Dan jiddependi mill-pajjiż li għalih jappartjeni l-emittent tal-identifikazzjoni elettronika tal-utent.

1.7.2. Firem li jużaw identifikazzjonijiet elettronici barranin

Kif diġà deskritt, mudell għall-firma elettronika huwa applikat fi hdan dan il-qafas tekniku msejjaħ firma federata. Servizz ta' firma bbażat fuq is-server huwa marbut mas-servizz elettroniku, li min-naħa tiegħu jitlob firma. Meta utent jiffirma dokument, is-servizz elettroniku jibgħat talba għal firma lis-servizz tal-firma. Is-servizz ta' firma mbagħad jitlob lill-utent biex jawtentika lill-utent. B'rabta mal-awtentikazzjoni, l-utent japprova l-firma. Is-servizz ta' firma jibgħat id-data lura lis-servizz elettroniku, u mbagħad tinħażen id-data tal-firma assoċjata mad-dokument li jkun ġie ffirmat.

Din il-proċedura tippermetti wkoll li jsir iffirmar bl-użu ta' identifikazzjoni elettronika barranija, peress li s-servizz ta' firma jista' jagħmel li jawtentika l-utent bl-użu ta' identifikazzjoni elettronika barranija f'konformità mal-proċedura deskritta hawn fuq fit-taqsim 1.7.1.

Meta jiffirma, f'dan il-każ, in-nodu tal-eIDAS Żvediż huwa responsabbli biex jinforma lill-utent li l-għan tal-awtentikazzjoni huwa li jiffirma dokument, min talab il-firma, u kwalunkwe informazzjoni dwar x'qed jiġi ffirmat. Ċertifikat tal-identità jinhareġ biss ladarba l-utent ikun awtentika lill-utent (għall-firma) u dan jintbagħat lis-servizz tal-firma li min-naħa tiegħu jiġġenera l-firma.

1.7.3. Ġestjoni tal-identità

Iċ-ċertifikati tal-identità minn pajjiżi oħra jikkonformaw mal-ispeċifikazzjonijiet tekniċi madwar l-UE kollha żviluppata fil-qafas tar-Regolament eIDAS. L-attributi li kull pajjiż jeħtieġu dejjem jinkludi għall-persuni fiżiċi kif ukoll għall-organizzazzjonijiet ("Sett Minim ta' Data", MDS) huma stabbiliti f'dan ir-Regolament. Kull pajjiż jeħtieġu jinkludi identifikatur uniku għal kull identifikazzjoni elettronika li jirrappreżenta persuna fiżika waħda biss. Minn xi pajjiżi, dawn l-identifikaturi se jkunu uniċi u persistenti għal kull persuna bl-istess mod bħal, pereżempju, in-numri tal-identità personali Żvediżi, iżda dawn l-identifikaturi jista' jkollhom kompożizzjonijiet u karatteristiċi differenti ħafna. Karatteristika waħda li tista' tvarja hija l-persistenza ta' tali identifikatur, jiġifieri jekk tali identifikatur jibqax l-istess matul il-ħajja ta' persuna jew jinbidel jekk, pereżempju, il-persuna tiċċaqlaq lejn reġjun ieħor, tibdel isimha, jew sempliċement tbiddel l-identifikazzjoni elettronika tagħha. Minn xi pajjiżi (eż. ir-Renju Unit), l-identifikatur se jvarja skont liema identifikazzjoni elettronika tal-pajjiż l-utent jagħmel li juża fil-preżent.

Sabiex tiġi ssimplifikata l-ġestjoni tal-utenti fis-servizzi elettronici Żvediżi, in-nodu tal-eIDAS Żvediż jiġġenera attribut tal-ID standardizzat għall-utenti li ġew awtentikati bl-użu ta' identifikazzjoni elettronika barranija, magħruf bħala *ID provvizorja* (imqassa bħala PRID). Barra minn hekk, jinholq attribut assoċjat li jiddikjara l-persistenza mistennija, jew it-tul tal-ħajja, ta' dan l-attribut tal-ID. L-attribut PRID jiġi ġġenerat abbażi tal-valuri tal-attributi miksuba mill-awtentikazzjoni barranija skont metodi speċifikati għal dak il-pajjiż partikolari. Kull kombinazzjoni ta' pajjiż u metodu hija kklassifikata f'termini ta' persistenza mistennija, jiġifieri kemm huwa probabbli li identità tinbidel maż-żmien għall-istess persuna. Dan jippermetti lis-servizzi elettronici Żvediżi jadattaw il-komunikazzjoni mal-utent u jipprovdu b'mod proattiv karatteristiċi li jagħmluha aktar faċli għal utent li l-identità tiegħu tkun inbidlet biex jerga' jikseb kontroll fuq l-informazzjoni tiegħu fis-servizz elettroniku.

F’xi każijiet, persuna li tiġi awtentikata bl-użu ta’ identifikazzjoni elettronika barranija jista’ jkollha wkoll numru tal-identità personali Żvediż. Dan jista’ jkun, pereżempju, ċittadin Żvediż li mar jgħix barra mill-pajjiż u kiseb identifikazzjoni elettronika barranija jew ċittadin barrani li huwa rreġistrat fl-Iżvezja u li ġie assenjat numru tal-identità personali.

Il-fatt li persuna b’identifikazzjoni elettronika barranija jkollha numru tal-identità personali Żvediż normalment ma jkunx magħruf mis-servizz ta’ awtentikazzjoni barrani, u għalhekk din l-informazzjoni ma tkunx inkluża fiċ-ċertifikat tal-identità mill-pajjiż fejn il-persuna tiġi awtentikata. In-nodu Żvediż, min-naħa l-oħra, għandu l-abbiltà li jistaqsi lil servizz ta’ attributi fl-Iżvezja¹ dwar jekk hemmx numru tal-identità personali rreġistrat għall-persuna awtentikata u jista’, jekk dan ikun il-każ, iżid tali informazzjoni maċ-ċertifikat tal-identità mibgħut lis-servizz elektroniku.

[1]: Fiż-żmien tal-kitba, ma hemm l-ebda servizz ta’ attributi li jistabbilixxi rabta bejn l-identitajiet tal-eIDAS u n-numri tal-identità personali Żvediżi.

1.7.4. Identifikazzjonijiet elettronici Żvediżi f’servizzi elettronici barranin

L-Iżvezja nnotifikat identifikazzjonijiet elettronici Żvediżi fil-livelli ta’ assigurazzjoni sostanzjali u għoljin skont l-eIDAS.

Talba ta’ awtentikazzjoni minn servizz elektroniku barrani lin-nodu tal-eIDAS Żvediż (servizz proxy) issir permezz ta’ konnettur eIDAS fil-pajjiż tas-servizz elektroniku. Fin-nodu Żvediż tal-eIDAS, l-utent jagħżel liema identifikazzjoni elettronika Żvediża jixtieq juża biex jawtentika, u mbagħad tintbagħat talba ta’ awtentikazzjoni lis-servizz ta’ awtentikazzjoni (*Fornitur tal-Identità*) li jittratta l-identifikazzjoni elettronika magħżula. Din it-talba hija fformattjata skont qafas tekniku, li jfisser li servizz ta’ awtentikazzjoni Żvediż ma għandux għalfejn jikkonforma mal-ispeċifikazzjonijiet tekniċi tal-eIDAS.

L-utent jiġi awtentikat mis-servizz ta’ awtentikazzjoni Żvediż u jinħareġ ċertifikat tal-identità (skont il-qafas tekniku). Dan iċ-ċertifikat jiġi riċevut mis-servizz proxy tal-eIDAS Żvediż u kkonvertit f’ċertifikat skont l-ispeċifikazzjonijiet tal-eIDAS qabel ma jintbagħat lill-konnettur tal-eIDAS barrani u mbagħad lis-servizz elektroniku li jagħmel is-sejha (*Fornitur tas-Servizz*).

2. Speċifikazzjonijiet tekniċi

Dan il-kapitolu fih speċifikazzjonijiet u profili għall-federazzjonijiet tal-identità li jikkonformaw mal-qafas tekniku Sweden Connect, u ċerti servizzi relatati. Sakemm ma jkunx iddikjarat mod ieħor, dawn id-dokumenti huma preskrittivi għall-ghoti ta’ servizzi fi hdan il-federazzjonijiet tal-identità li jimplementaw il-qafas tekniku.

2.1. Profili u speċifikazzjonijiet għall-SAML

Il-federazzjonijiet tal-identità li jikkonformaw mal-qafas tekniku Sweden Connect huma mibnija abbażi tal-“Profil ta’ Varar għall-Qafas Żvediż tal-Identifikazzjoni Elettronika”, [SAML.Profil]. Dan il-profil huwa influwenzat mill-“Profil tal-Varar għall-Interoperabbiltà tal-Federazzjoni SAML V2.0” [SAML2Int], iżda mhux dipendenti preskrittivament fuqu. [SAML.Profil] fih ukoll regoli u linji gwida speċifiċi għall-qafas tekniku Sweden Connect.

2.1.1. Profil tal-Varar għall-Qafas Żvediż tal-Identifikazzjoni Elettronika

Il-“Profil tal-Varar għall-Qafas Żvediż tal-Identifikazzjoni Elettronika”, [SAML.Profile], huwa d-dokument qafas tekniku ewlieni u jispeċifika, fost l-oħrajn:

- kif għandha tinbena u tiġi interpretata l-metadata tal-SAML;
- kif għandha tiġi fformattjata t-talba ta' awtentikazzjoni;
- kif għandha tiġi ttrattata talba ta' awtentikazzjoni, u kif għandu jiġi mfassal, vverifikat u ttrattat ċertifikat tal-identità;
- ir-rekwiziti ta' sigurtà;
- ir-rekwiziti SAML speċifiċi għal servizzi ta' firma u “awtentikazzjoni għall-firma”.

2.1.2. Qafas Żvediż tal-Identifikazzjoni Elettronika – Reġistru għall-identifikaturi

L-implimentazzjoni ta' infrastruttura Żvediża tal-identifikazzjoni elettronika tirrikjedi forum differenti ta' identifikaturi biex jirrappreżentaw oġġetti fl-istrutturi tad-data. Id-dokument “Sweden Connect – Registry for identifiers”, [SC.Registry], jiddefinixxi l-istruttura tal-identifikaturi assenjati skont il-qafas tekniku, kif ukoll reġistru ta' identifikaturi definiti.

2.1.3. Speċifikazzjoni tal-Attributi għall-Qafas Żvediż tal-Identifikazzjoni Elettronika

L-ispeċifikazzjoni “Speċifikazzjoni tal-Attributi għall-Qafas Żvediż tal-Identifikazzjoni Elettronika”, [SAML.Attributes], tiddikjara l-profil tal-attributi tal-SAML li jintużaw fi ħdan il-federazzjonijiet tal-identità li jikkonformaw mal-qafas tekniku inklużi dawk li jaqdbu mal-eIDAS permezz tan-nodu tal-eIDAS Żvediż.

2.1.4. Kategoriji ta' Entitajiet għall-Qafas Żvediż tal-Identifikazzjoni Elettronika

Il-Kategoriji ta' Entitajiet jintużaw fi ħdan il-federazzjoni għal għadd ta' skopijiet differenti:

- Kategoriji ta' Entitajiet ta' Servizz – Użati f'-metadata biex jirrappreżentaw ir-rekwiziti tas-servizzi elettronici għal-livelli ta' assigurazzjoni u l-attributi mitluba, kif ukoll l-issodisfar mis-servizzi ta' awtentikazzjoni tal-livelli ta' assigurazzjoni u l-forniment tal-attributi.
- Kategoriji tal-Proprietà tas-Servizz – Użati biex jirrappreżentaw karatteristika speċifika ta' servizz.
- Kategoriji ta' Entitajiet tat-Tip ta' Servizz – Użati biex jirrappreżentaw tipi differenti ta' servizz fi ħdan il-federazzjoni.
- Kategoriji ta' Entitajiet tal-Kuntratt ta' Servizz – Użati mis-servizzi biex jithabbru l-formoli tal-ftħim u affarijiet simili.
- Kategoriji ta' Entitajiet Ġenerali – Kategoriji tal-Entitajiet li ma jaqgħu taħt l-ebda wieħed mit-tipi ta' hawn fuq.

L-ispeċifikazzjoni “Kategoriji ta’ Entitajiet għall-Qafas Żvediz tal-Identifikazzjoni Elettronika” [SAML.EntCat] tispeċifika l-kategoriji ta’ entitajiet definiti mill-qafas tekniku u tiddekrivi t-tifsira tagħhom.

2.1.5. Speċifikazzjoni tal-Attributi Mibnija mill-eIDAS għall-Qafas Żvediz tal-Identifikazzjoni Elettronika

L-ispeċifikazzjoni “eIDAS Speċifikazzjoni tal-Attributi Mibnija għall-Qafas Żvediz tal-Identifikazzjoni Elettronika”, [SC.eIDAS.Attrs], tispeċifika l-proċessi u r-regoli għall-mod li bih jinbnew l-attributi tal-ID ibbażati fuq attributi riċevuti matul awtentikazzjoni fl-eIDAS.

2.1.6. Profil ta’ Implimentazzjoni għall-Fornituri tal-Identità ta’ BankID fi hdan il-Qafas Żvediz tal-Identifikazzjoni Elettronika

L-ispeċifikazzjoni “Profil ta’ Implimentazzjoni tal-Fornitur ta’ Identità ta’ BankID fil-Qafas Żvediz tal-Identifikazzjoni Elettronika”, [SAML.BankID], tiddefinixxi r-regoli għall-mod li bih servizz ta’ awtentikazzjoni li jimplimenta appoġġ għal BankID għandu jiġi ddisinjat.

Jekk jogħġbok innota dan li ġej: Din l-ispeċifikazzjoni mhijiex preskruttiva għall-konformità ma’ qafas tekniku. Hija rilevanti biss għas-servizzi ta’ awtentikazzjoni li jimplimentaw appoġġ għal BankID u għas-servizzi elettronici li jużawhom. Madankollu, is-servizzi ta’ awtentikazzjoni li jimplimentaw l-appoġġ għal BankID u li jridu jaqbd u mal-federazzjoni Sweden Connect jehtigilhom jikkonformaw ma’ din l-ispeċifikazzjoni.

2.1.7. Għażla Prinċipali fit-Talbiet għall-Awtentikazzjoni tal-SAML

L-ispeċifikazzjoni “Għażla Prinċipali fit-Talbiet għall-Awtentikazzjoni tal-SAML”, [SAML.Principal], tiddefinixxi estensjoni għall-SAML li tippermetti lil parti dipendenti tinforma lil servizz ta’ awtentikazzjoni liema identità tixtieq li tiġi awtentikata.

2.1.8. Estensjoni tal-Messaġġ tal-Utent fit-Talbiet ta’ Awtentikazzjoni tal-SAML

L-ispeċifikazzjoni “Estensjoni tal-Messaġġ tal-Utent fit-Talbiet ta’ Awtentikazzjoni tal-SAML”, [SAML.UMessage], tiddefinixxi estensjoni għall-SAML li tippermetti lil parti dipendenti tinkludi messaġġ tal-wiri fit-talba ta’ awtentikazzjoni mibgħuta lis-servizz ta’ awtentikazzjoni. Is-servizz ta’ awtentikazzjoni mbagħad jista’ juri dan il-messaġġ lill-utent matul il-pass tal-awtentikazzjoni.

2.2. Profili u speċifikazzjonijiet għal OpenID Connect

2.2.1. Profil ta’ OpenID Connect għal Sweden Connect

Il-profil “Profil ta’ OpenID Connect għal Sweden Connect”, [OIDC.Profile], jibni fuq il-Profil Żvediz OpenID Connectli huwa profil OpenID Connect żviluppat minn OIDC Sweden biex tippromwovi l-interoperabbiltà u s-sigurtà fi hdan is-soluzzjonijiet Żvedizi tal-OIDC.

[OIDC.Profile] iżżid rekwiżiti addizzjonali rigward il-federazzjoni Sweden Connect.

2.2.2. Talbiet u Ambiti ta' OpenID Connect Speċifikazzjoni għal Sweden Connect

L-ispeċifikazzjoni “Talbiet u Ambiti ta' OpenID Connect Speċifikazzjoni għal Sweden Connect”, [OIDC.Claims], tibni fuq l-ispeċifikazzjoni Talbiet u Ambiti Speċifikazzjoni għall-Profil Żevediż ta' OpenID Connect minn OIDC Sweden.

2.3. Speċifikazzjonijiet għall-Firma

Din it-taqsima fiha referenzi għad-dokumenti li jiddefinixxu s-servizzi tal-firma fi hdan il-federazzjonijiet li jikkonformaw mal-qafas tekniku Sweden Connect.

2.3.1. Profil ta' Implimentazzjoni għall-użu tad-DSS tal-OASIS fis-Servizzi Ċentrali tal-Iffirmar

Il-profil ta' implimentazzjoni “Profil ta' Implimentazzjoni għall-Użu tad-DSS tal-OASIS fis-Servizzi ta' Ffirmar Ċentrali”, [Sign.DSS.Profile], jispeċifika profil għat-talba ta' firma u rispons skont l-istandard OASIS “Protokoll, Elementi, u Rabtiet Ewlenin tas-Servizz tal-Firem Diġitali”, [DSS].

2.3.2. Estensjoni tad-DSS għas-Servizzi Ċentrali Federati tal-Iffirmar

“Estensjoni DSS għal Servizzi ta' Firma Ċentrali Federati”, [Sign.DSS.Ext], hija estensjoni tal-istandard tal-OASIS “Protokoll, Elementi, u Rabtiet Ewlenin tas-Servizz tal-Firem Diġitali”, [DSS], li tispeċifika d-definizzjonijiet meħtieġa għall-iffirmar skont il-qafas tekniku.

2.3.3. Profil taċ-Ċertifikat għaċ-Ċertifikati Mahruġa mis-Servizzi Ċentrali tal-Iffirmar

Il-profil taċ-ċertifikat “Profil taċ-ċertifikat għaċ-ċertifikati mahruġa mis-Servizzi Ċentrali tal-Iffirmar”, [Sign.Cert.Profile], jispeċifika il-kontenut taċ-ċertifikati tal-iffirmar. Dan il-profil japplika estensjoni ġdida taċ-ċertifikat biex jappoġġa s-servizzi tal-firma.

Dan il-profil jirreferi għall-“Estensjoni taċ-Ċertifikat tal-Kuntest tal-Awtentikazzjoni”, [AuthContext], li jiddeskrivi kif il-“Kuntest tal-Awtentikazzjoni” huwa rrappreżentat fiċ-ċertifikati X.509.

2.3.4. Protokoll ta' Attivazzjoni tal-Firma għall-Iffirmar Federat

L-ispeċifikazzjoni “Protokoll ta' Attivazzjoni tal-Firma għall-Iffirmar Federat”, [Sign.Activation], tiddefinixxi l-“Protokoll ta' Attivazzjoni tal-Firma” (SAP) għall-implimentazzjoni tal-“Assigurazzjoni ta' Kontroll Waħdieni Livell 2” (SCAL2) skont l-istandard “prEN 419241 – Sistemi Affidabbli li Jappoġġaw l-Iffirmar tas-Server”.

3. Lista ta' referenza

3.1. DIGG

[Digg.Tillit]

Qafas ta' fiduċja għall-identifikazzjoni elettronika Żvediza.

[SC.Registru]

Sweden Connect – Registru għall-identifikaturi.

[SAML.Profile]

Profil tal-Varar għall-Qafas Żvediz tal-Identifikazzjoni Elettronika.

[SAML.Attributi]

Speċifikazzjoni tal-Attributi għall-Qafas Żvediz tal-Identifikazzjoni Elettronika.

[SAML.EntCat]

Kategoriji ta' Entitajiet għall-Qafas Żvediz tal-Identifikazzjoni Elettronika.

[SC.eIDAS.Attrs]

eIDAS Speċifikazzjoni tal-Attributi Mibnija għall-Qafas Żvediz tal-Identifikazzjoni Elettronika.

[SAML.BankID]

Profil ta' Implimentazzjoni għal BankID Fornituri tal-Identità fi hdan il-Qafas Żvediz tal-Identifikazzjoni Elettronika.

[SAML.Principali]

Għażla Principali fit-Talbiet ta' Awtentikazzjoni tal-SAML.

[SAML.UMessage]

Estensjoni tal-Messaġġ tal-Utent fit-Talbiet ta' Awtentikazzjoni tal-SAML.

[OIDC.Profile]

Profil ta' OpenID Connect għal Sweden Connect.

[OIDC.Claims]

Talbiet u Ambiti ta' OpenID Connect Speċifikazzjoni għal Sweden Connect.

[Sign.DSS.Profile]

Profil ta' Implimentazzjoni għall-Użu tad-DSS tal-OASIS fis-Servizzi Ċentrali tal-Iffirmar.

[Sign.DSS.Ext]

Estensjoni tad-DSS għas-Servizzi Ċentrali Federati tal-Iffirmar.

[Sign.Cert.Profile]

Profil taċ-ċertifikat għaċ-ċertifikati maħruġa mis-servizzi tal-Iffirmar Ċentrali.

[Sinjal.Attivazzjoni]

Protokoll ta' Attivazzjoni tal-Firma għall-Iffirmar Federat.

3.2. Referenzi oħra**[SAML2Int]**

Profil ta' Varar għall-Interoperabbiltà tal-Federazzjoni SAML V2.0.

[DSS]

OASIS Standard – Protokollu Principali tas-Servizz tal-Firma Digitali, Elementi, u Verżjoni tal-Konnessjonijiet 1.0, 11 ta' April 2007.

[AuthContext]

RFC-7773: Estensjoni taċ-Ċertifikat tal-Kuntest tal-Awtentikazzjoni.