

Profilhantering

Dokumenthistorik

Version	Datum	Utförare	Kommentar
0.9	20 May 2021	Skarsgård, Grim	Upprättad
1.0	14 Jun 2021	UnSkowrsgår Use, Grim	Fastställd
2.0	07 Nov 2023	Stefan Eriksson	Uppdaterat med privata e-legitimationer och eIDAS
2..1	28 Nov 2023	Stefan Eriksson	Tagit bort vissa attribut
2.2	08 Dec 2023	Stefan Eriksson	Fotnot för eIDAS profilen
2.3	15 Dec 2023	Tomas Fransson	Godkänd

Innehållsförteckning

- [Underskriftsprofiler](#)
 - [Styrning av underskriftsprofil](#)
 - [Användarattribut](#)
- [Stödtjänstprofil](#)

1. Underskriftsprofiler

Underskriftsprofiler styr vilka användarattribut som ska ingå i det slutgiltiga underskriftscertifikatet .

Tillgängliggjorda underskriftsprofiler utgår ifrån Digitaliseringsmyndighetens attribute sets.

Underskriftsprofil	dn i underskriftscertifikat, exempel	DIGGs attributset som ligger till grund för underskriftsprofilen	Utgivande CA för underskriftscertifikat	Signaturalgorithm	Signaturtyp
eln_ap_pnr_01	cn=Elin Svensson serialNumber=199101192384 sn=Svensson givenName=Elin	ELN-AP-Pnr-01 - Natural Personal Identity with Civic Registration Number (Personnummer)	För LOA2: CGI Sverige AB Low DSS End User CA För LOA3: CGI Sverige AB Substantial DSS End User CA	ECDSA P256	XAdES-BASELINE-B, Enveloped PADES-BASELINE-B, Enveloped
digg_ap_hsaid_01	cn=Elin Svensson serialNumber= TST5565594230-12R7 sn=Svensson givenName=Elin	DIGG-AP-HSAid-01 - Natural Person Identity with HSA-ID			
eln_ap_orgperson_01	cn=Elin Svensson serialNumber= TST5565594230-12R7@5565594230 sn=Svensson givenName=Elin O=Inera AB	ELN-AP-OrgPerson-01 - Organizational Identity for Natural Persons			
eln_ap_pnr_01_orgid	cn=Elin Svensson serialNumber= 199101192384 sn=Svensson givenName=Elin 2.5.4.97=5590858584	Kombination av ELN-AP-Pnr-01 och ELN-AP-OrgPerson-01			
eln_ap_eidas_natper_01	cn=Elin Svensson serialNumber= xx:yy:199101192384 sn=Svensson givenName=Elin	ELN-AP-eIDAS-NatPer-01	För LOW: CGI Sverige AB Low DSS End User CA För SUB: CGI Sverige AB Substantial DSS End User CA För HIGH: CGI Sverige AB HIGH DSS End User CA	ECDSA P256	XAdES-BASELINE-B, Enveloped PADES-BASELINE-B, Enveloped

Namngivningen av dessa profiler är i praktiken ändringsbara per logisk instans (varje ansluten e-tjänst).

1.1. Styrning av underskriftsprofil

E-tjänsten anger i fältet `<csig:AuthnProfile>` i `SignRequest` vilken underskriftsprofil som önskas.

Styrande användarattribut inkommer i `SignRequest` från e-tjänsten till Underskriftstjänsten, i elementet `<csig:Signer>`. Underskriftstjänsten skickar dessa attribut vidare i `AuthnRequest` till IdP, i fältet `<psc:PrincipalSelection>`. IdP returnerar sedan användarattribut från autentiseringen i `SAMLResponse`, i fältet `<saml2:AttributeStatement>`. Dessa attributvärden valideras mot de som angavs i `SignRequest`, och används sedan för att skapa underskriftscertifikatet enligt önskad underskriftsprofil. Exempel-requests återfinns i [SAD - Underskriftstjänsten - Requests](#).

1.2. Användarattribut

Följande SAML-attribut från Ineras IdP används för att populera användarattributen i underskriftscertifikatet:

Fält i dn i underskriftscertifikatet	Attribut från IdP	Attribut från IdP för e-legitimationer som stödjer DIGG's SAML Profil
cn=Elin Svensson	urn:name	urn:oid:2.16.840.1.113730.3.1.241
givenName=Elin	http://sambi.se/attributes/1/givenName	urn:oid:2.5.4.42
sn=Svensson	http://sambi.se/attributes/1/surname	urn:oid:2.5.4.4
O=Inera AB	http://sambi.se/attributes/1/organizationName	urn:oid:2.5.4.10
2.5.4.97=5590858584	http://sambi.se/attributes/1/organizationIdentifier	urn:oid:2.5.4.97

serialNumber baseras på olika [attribut från IdP](#) beroende på underskriftsprofil:

Underskriftsprofil	serialNumber, exempel	Attribut från IdP (Inera's IdP)	Attribut från IdP för e-legitimationer som stödjer DIGG's SAML profil
eln_ap_pnr_01	serialNumber=199101192384	http://sambi.se/attributes/1/personalIdentityNumber	urn:oid:1.2.752.29.4.13
digg_ap_hsaid_01	serialNumber= TST5565594230-12R7	http://sambi.se/attributes/1/employeeHsaId	
eln_ap_orgperson_01	serialNumber= TST5565594230-12R7@5565594230	urn:orgAffiliation	
eln_ap_pnr_01_orgid	serialNumber= 199101192384	http://sambi.se/attributes/1/personalIdentityNumber	
eln_ap_eidas_natper_01	serialNumber= xx:yy:199101192384	N/A	urn:oid:1.2.752.201.3.4

Vid användning av IDP:er för t ex **BankID** eller **Freja eID+** så mappas attributen till X509 certifikatet baserat på DIGG's SAML profil: [ELN-AP-Pnr-01 - Natural Personal Identity with Civic Registration Number \(Personnummer\)](#) samt att det är den enda profilen som fungerar med dessa typer av e-legitimationer.

2. Stödtjänstprofil

Stödtjänsten kombinerar Underskriftstjänstens underskriftsprofiler och önskad tillitsnivå (LoA) i s.k. *stödtjänstprofiler*.

Underskriftsprofil	Godkänd tillitsnivå	Stödtjänstprofil
eln_ap_pnr_01	LoA 2 eller LoA 3	eln_ap_pnr_01_loa2_loa3
	LoA 3	eln_ap_pnr_01_loa3
digg_ap_hsaid_01	LoA 2 eller LoA 3	digg_ap_hsaid_01_loa2_loa3
	LoA 3	digg_ap_hsaid_01_loa3
eln_ap_orgperson_01	LoA 2 eller LoA 3	eln_ap_orgperson_01_loa2_loa3
	LoA 3	eln_ap_orgperson_01_loa3
eln_ap_pnr_01_orgid	LoA 2 eller LoA 3	eln_ap_pnr_01_orgid_loa2_loa3
	LoA 3	eln_ap_pnr_01_orgid_loa3
eln_ap_eidas_natper_01 ¹	eidas-sub eller eidas-high	eln_ap_eidas_natper_eidas_sub_eidas_high

¹ Profilen eln_ap_eidas_natper_01 för eIDAS stöds ej av Underskriftstjänsten - Bas.