Inledning

SAML Attributsprofil

2026W14

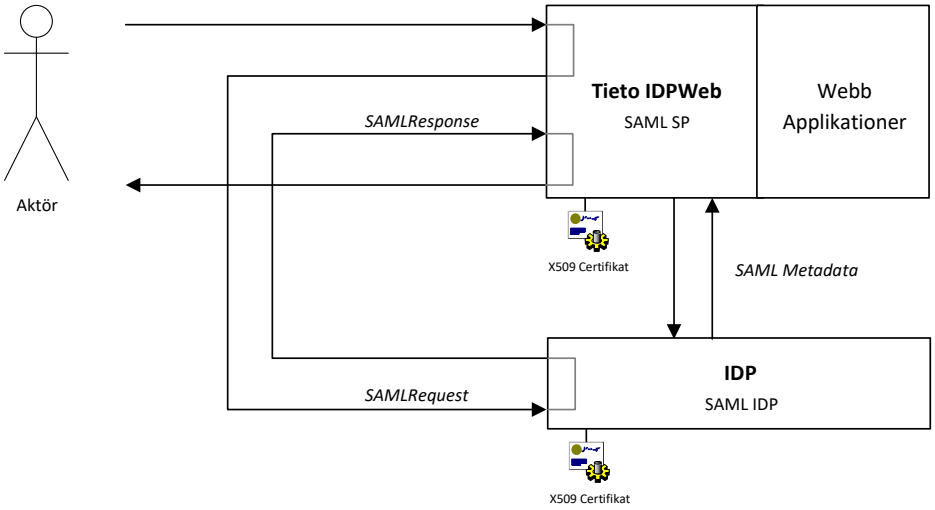
Innehållsförteckning

1 Inledning

Dokumentet beskriver den applikationsprofil som Tieto stödjer i produkter och tjänster inom vård och omsorg, familjeomsorg samt inom skola och barnomsorg. Applikationsprofilen är verifierad från säkerhetsplattformar från flera av våra stora Identity Providers.

2 SAML 2.0

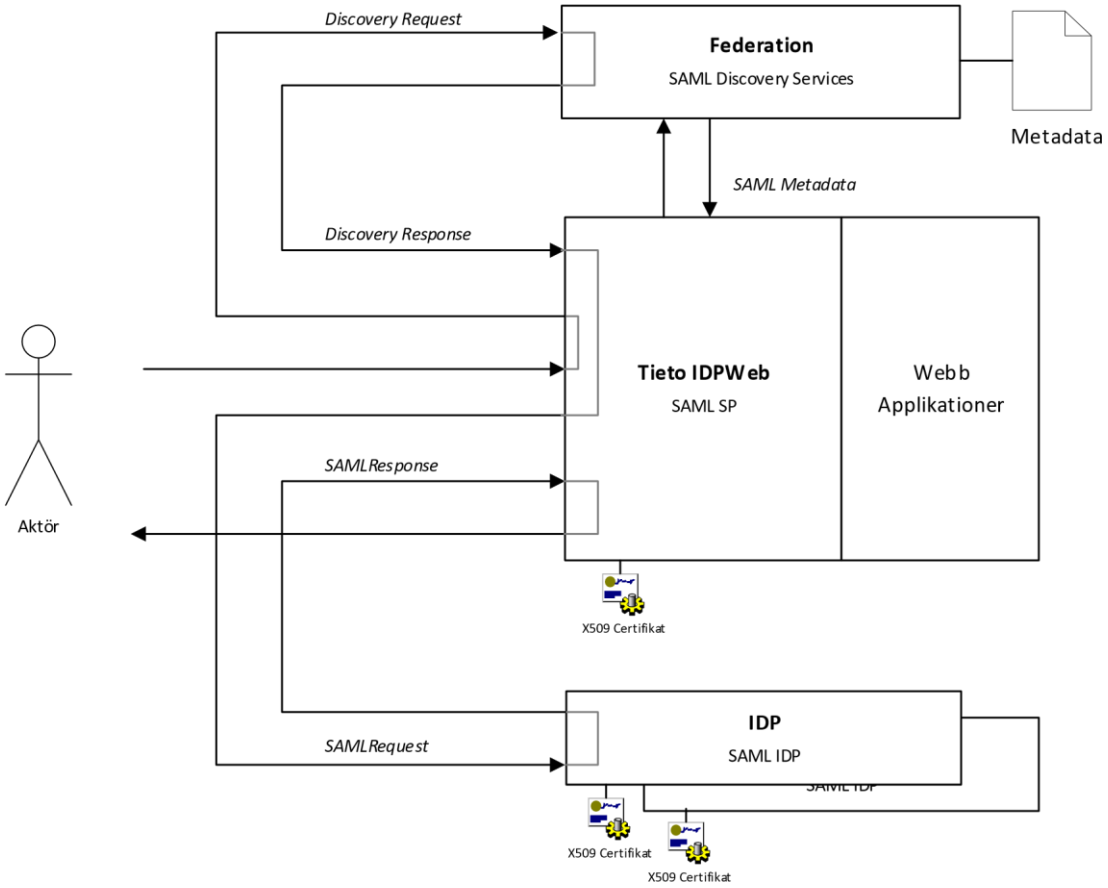
Protokollen som används idag är SAML 2.0 Web-Browser SSO Profile, SAML Metatdata och SAML Discovery Services där Tieto agerar som en SAML Service provider (SP). Användarna identifieras med personnummer och auktorisering utförs i verksamhetssystemen. För att identifiera Identity Provider (IdP) och SP används X509 certifikat.



2.1 SAML Identity Provider Discovery Service Protocol

SAML federationer använder SAML Identity Provider Discovery Service Protocol som anvisningstjänst för att presentera alla anslutna IdP'er i federationen av operatören.

Vid federationer kan SAML HTTP-Redirect bindning användas när IdP saknar SAML HTTP-POST i metadata. Kräver federationsoperatören en specifik bindning måste detta beskrivas i metadata för alla IdP'er som ingår i federationen.



2.2 SAML Web-Browser SSO Profile

Bindningen som skall användas är HTTP POST Binding där meddelandena är base64 kodade i ett HTML formulär. Enligt specifikationen skall SAMLRequest och SAMLResponse vara signerad med PKI och transporten skall ske med TLS 1.2 eller högre. IdP och SP autentiserar varandra med X509 certifikat enligt de riktlinjer som beskrivs i RFC 2459.

Attributen för att identifiera en användare i SAML Assertion förekommer i XML elementen Subject eller AttributeStatement.

2.2.1 Attribut för identifiering

Attribut	Format	Beskrivning	Förekomst
userid	Personnummer enligt formatet YYYYMMDDNNNN eller HSAID (bara för Welfare) eller epost arbete/skola (endast EDU)	Användarens personnummer eller HSAID Identitet på person i **VERSALER** eller epost arbete/skola	Skall
sn	Text	Användarens efternamn	Rekommenderas
givenname	Text	Användarens tilltalsnamn	Rekommenderas

2.3 SAML Metadata

SAML-protokollets Metadata används av IdP och SP för att underlätta konfigurationen för kunders verktyg och tjänster med elementet EntityDescriptorType. Metatdatat som genereras är unik för varje kund och därför bör den genereras vid installationen.

Exempel på adress till metadata: https://demo-lcsse.service.tieto.com/HCW.Welfare.Common.IdentityPortalWeb/WS/V1/MetaDataProvider.svc/EduSeSales01

2.3.1 SSO Service Provider

SP använder elementen SPSSODescription och Signature för att informera IdP.

2.3.2 SSO Identity Provider

IdP använder elementen SPSSODescription, Organization och Signature för att informera SP

2.3.3 Single Logout

Vid konfigurering av nya federationsprofiler skickar SP (Lifecare/Tieto Education) alltid en logout-begäran (SLO) till IdP när användaren väljer att logga ut för att försäkra sig om att användarens session i IdP:n avslutas. Av den anledningen är det viktigt att kundens IdP tillhandahåller information om aktuell SLO-adress i sitt metadata. Om denna information inte är definierad så kommer utloggningar från våra applikationer inte att bli fullständiga. Detta då den federerade IdP:n håller sessionen levande och följaktligen kommer nästa anrop mot någon av våra applikationer i den webbläsarsessionen att omfattas av en SSO upplevelse, dvs användaren är inte utloggad i IdP och vår session återetableras som om den aldrig hade varit utloggad.

Attribut för Single logout återfinns i metadatat enligt:

```
<SingleLogoutService Binding=
```

OBS! I det fall federation sker mot exempelvis Azure AD Connect (direkt eller indirekt via broker-funktion eller dylikt) faller ansvaret på kunden att hantera om SLO ej önskas pga. av oönskade sidoeffekter (exempelvis risk för utloggning i andra applikationer som ingår i samma federation).

2.3.4 Kontaktuppgifter (ContactPerson)

För att vid behov snabbt få kontakt med ansvarig för konfiguration och drift av er IdP önskar vi att ni anger korrekt information i metadata-sektionen ”ContactPerson”. E-post-adress kan även vara funktionsbrevlåda om så önskas.

Exempel:

```
<md:ContactPerson xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
 contactType="administrative">
    <md:GivenName>Lisa</md:GivenName>
    <md:SurName>Andersson</md:SurName>
    <md:EmailAddress>lisa.andersson@organisation.se</md:EmailAddress>
</md:ContactPerson>
```

2.3.5 LOA – Level of assurance

Vår identitetsweb kan nu hantera att våra applikationer sätter ett krav på en viss nivå av LOA för att användarna ska kunna logga in. Detta för att säkerställa att användarna loggar in med 2-faktorsinloggning vid er IdP. I dessa fall krävs det att er IdP skickar med AuthnContext-värde med en accepterad nivå, dvs nivå 2.

```
<saml:AuthnContext>
    <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes
    :MobileTwoFactorContract</saml:AuthnContextClassRef>
</saml:AuthnContext>
```

Vilka värden som i dagsläget motsvaras av nivå 2 i vår interna tabell kan ni se här:

- Kerberos
- MobileTwoFactorContract
- MobileTwoFactorUnregistered
- PGP
- Smartcard
- SmartcardPKI
- SoftwarePKI
- SPKI
- TLSClient
- X509
- XMLDSig

Värdena är hämtade från sektion 3.4 ur OASIS standard saml-authn-context-2.0-os.pdf (oasis-open.org)

OBS! Värdena kontrolleras case sensitive så värdet måste skickas från er IdP exakt enligt ovan.

3 Bilagor

3.1 SIS Skolfederation (enbart for Tieto Education)

Metadata finns på adressen:

fed.skolfederation.se/prod/md/skolfederation-3_1.xml

Man måste konfigurera OrganizationName, OrganizationDisplayName och OrganizationURI innan metadata kan publiceras för skolfederationen.

Validering av Service Provider metadata: https://validator.skolfederation.se/

För mer information se: https://www.skolfederation.se/teknisk-information/

3.1.1 Attribut

Namn	ID	Beskrivning
norEduPersonNIN	urn:oid:1.3.6.1.4.1.2428.90.1.5	Personnummer

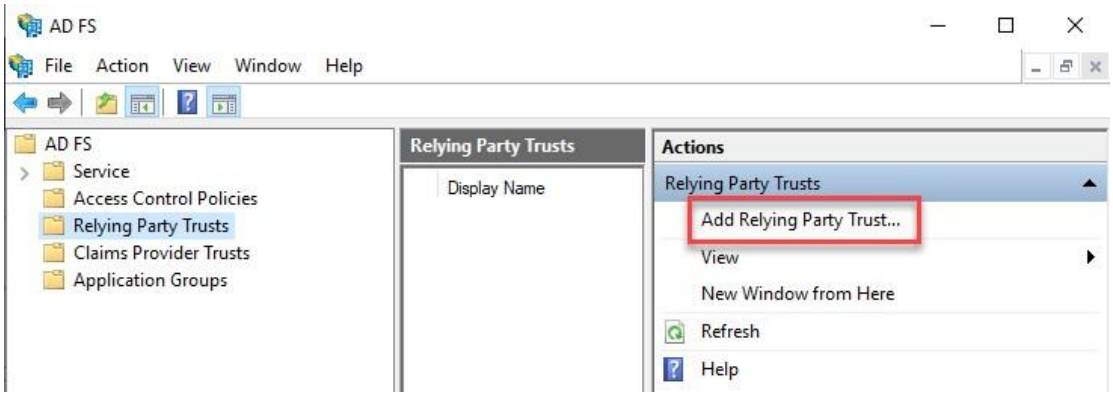
givenName	urn:oid:2.5.4.42	Förnamn
sn	urn:oid:2.5.4.4	Efternamn

3.2 Microsoft ADFS

För att integrationen skall fungera med våra produkter så måste en Relaying Part Trust skapas upp och lägga till en Claim Rules för attributen. Vid åtkomst från Internet bör endast kända utgivare av certifikat användas och brandvägg måste tillåta för trafik på TCP/443 från Internet till ADFS server.

3.2.1 Relaying Part Trust

Lägg till en ny Relaying Party Trust i AD FS Management



Gå igenom guiden och ange följande:

Welcome: Claims aware

Select Data source: Här kan man välja att göra konfigurationen manuell eller läsa in konfigurationen från en metadatalänk.

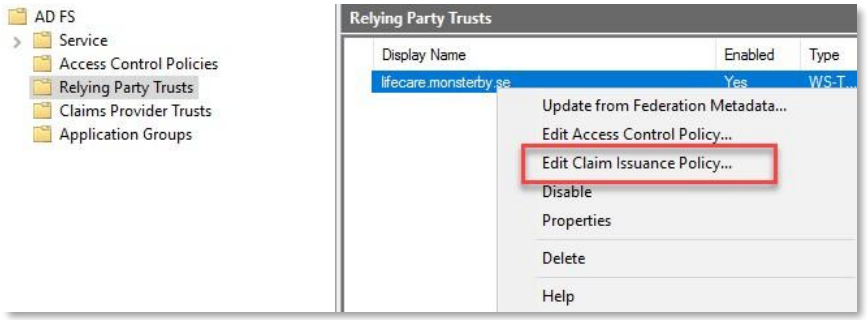
Vill man gör konfigurationen manuellt så väljer man *Enter data about relaying party manually*

För att importera data via metadatalänk så väljer man *Import Data av the relaying party*

Slutför sedan guiden och Relaying Party Trust är skapad.

3.2.2 Redigera Claims rules

Högerklicka på *Relaying Party Trusts* och välj *Edit Claim Issuance Policy*

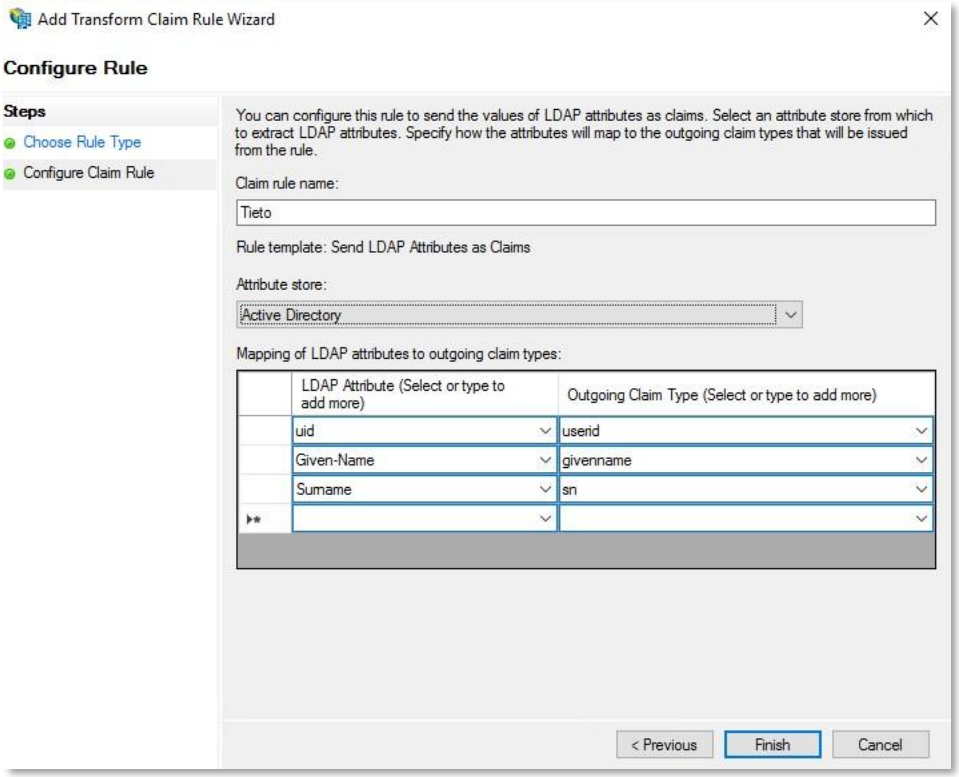


Välj mallen *Send LDAP Attributes as Claims*.

Ange ett passande namn för regeln.

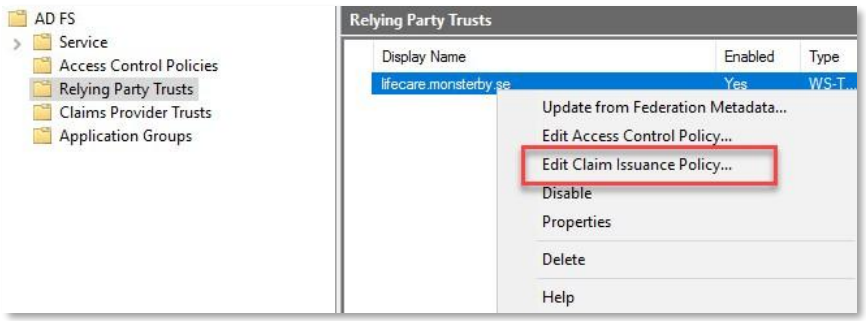
Kontrollera att ni har valt *Attribute Store*.

Mappa LDAP attributen som ska användas för identifiering.



3.2.3 Redigera Claim rules för Single Log out

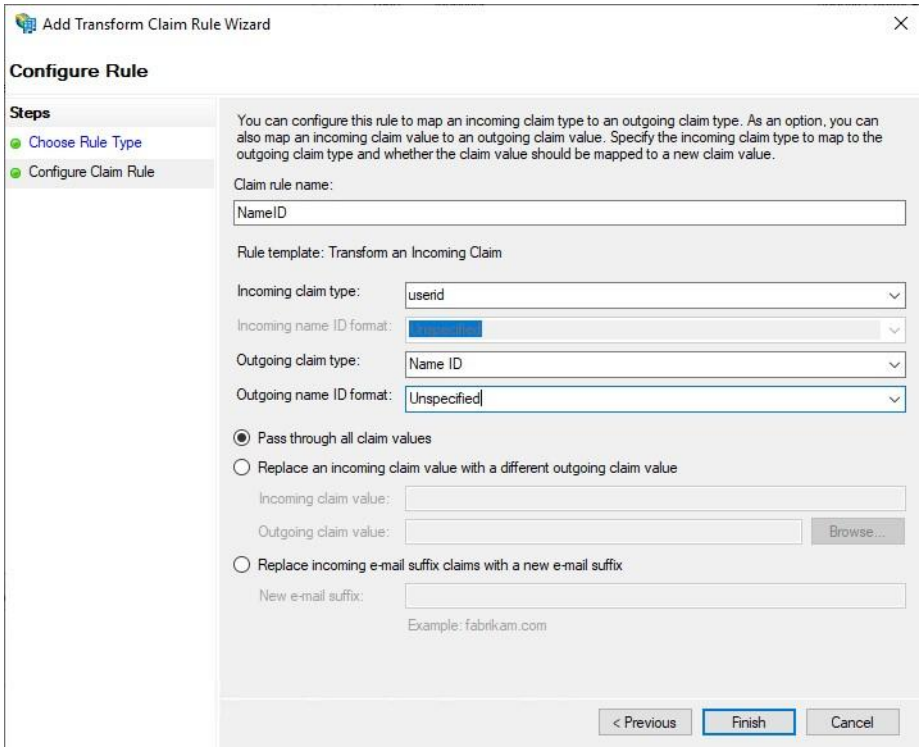
Högerklicka på *Relaying Party Trusts* och välj *Edit Claim Issuance Policy*.

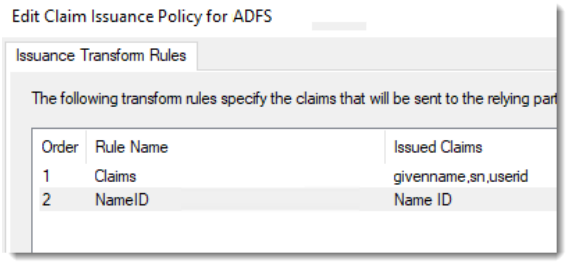


Välj att lägga till en ny regel och mallen ”*Transform an Incoming Claim*”.

Ange ett passande namn för regeln.

Välj de attibut ni vill skicka i NameID.





3.2.4 ADFS Metadata

Länk till ADFS metadata anges hos Service Provider. Information finner man i Endpoints under menyn Service i AD FS Management.

Exempel: https://www.kommun.se/FederationMetadata/2007-06/FederationMetadata.xml

3.3 Övrig information

Våra applikationer stödjer inte idp-initierad inloggning. För att undvika fel är det viktigt att distribuera rätt länk.

Distribuera alltså inte ut det som syns i adressfönstret efter redirect till IDP för inloggning, utan den rena länk mot applikationen som ni fått från Tieto. Exempel på korrekt länk:

```
https://kommun.se/WE.Flow3?domain=PROC&Actor=Actor_Professional&IDPMethod=saml
```

4 Ändringshistorik

Datum	Kapitel	Ändring
2026-03-31		Ny dokumentmall
2024-01-03	2.1.1	Lagt till epost som identifiering