

Individuella metadataströmmar



This information is aimed at Swedish readers. Development items put into production will be documented in English and published in the relevant place in this wiki.

Utvecklingsaktivitet

Kortfattad beskrivning	Individuella metadataströmmar baserade på valda filterkriterier
Status	UTVECKLING PÅGÅR



Nedanstående beskrivning syftar endast till att ge en översiktlig beskrivning av utvecklingsaktiviteten. Om du är intresserad av mer information, har synpunkter på lösningen eller vill bidra med idéer så kan du kontakta federationsoperatören på info@skolfederation.se eller info@sambi.se.

Bakgrund

SAML-federationer utgår vanligtvis från en metadataström som innehåller metadata från alla federationens medlemmar. Det är vanligt att strömmen delas upp i två strömmar där den ena strömmen innehåller alla IdP:er och den andra strömmen innehåller alla SP:ar. Strömmen kan även brytas på andra parametrar som tillitsnivå, kategori eller liknande.

De flesta parter som ingår i en federation har inte en relation till alla andra parter i federationen, utan behöver använda någon metod för att filtrera ut relevanta parter i federationen. Det kan realiseras genom flera olika mekanismer på olika nivåer i infrastrukturen eller i applikationslagret.

Om filtreringen sker direkt på metadata så förenklas efterföljande logik för SAML-instanser, applikationslager och stödfunktioner som anvisningstjänster och tjänsteportaler. En risk med filtrering på metadatanivå är att filtreringen utförs på ett sätt som innebär att förändrat metadata för en SP eller IdP filtreras bort oavsiktligt vilket leder till att användare inte längre har åtkomst till tjänsten.

En faktor som adderar ytterligare komplexitet är att en SAML-instans kan behöva läsa in metadata från flera olika strömmar, exempelvis i de fall instansen är ansluten till flera federationer.

Viss information i metadata kan användas för att underlätta eller automatisera konfiguration av den SAML-instans som läser in metadatat. Ett exempel på detta är "RequestedAttribute" som innebär att en SP kan signalera de attribut som krävs och där IdP:n kan använda den informationen för att släppa relevanta attribut utan manuell konfiguration. Vi avråder från denna typ av automatisering eftersom det innebär att användarorganisationen inte har kontroll på vilka attribut som släpps om en användare i det fall tjänsten uppdaterar efterfrågade attribut, om inte någon typ av logik finns på plats för att förhindra detta.

Anpassad metadataström per medlem

Genom att generera en anpassad metadataström per medlem (eller flera strömmar vid behov) så kan innehållet i strömmens innehåll konfigureras av medlemmen själv utifrån ett antal filtervillkor.

Detta möjliggör i sin tur versionering per ström så att automatiserad attributrelease kan nyttjas, möjlighet att nyttja samma infrastruktur till olika federativa kontexter (se [Federationskoncept](#)), möjlighet till anpassad JSON-feed (se [SSO-länkar](#)), samt förenklar administrationen av medlemsinstansen och öppnar upp för fler möjligheter till anpassade federationslösningar.

Lösningen bygger på att medlemmen konfigurerar sin egen ström utifrån ett antal filtervillkor i Federationsadmin och får då en egen URL där det anpassade metadatat kan läsas in. Vissa förändringar av metadata (exempelvis om en tjänst ändrar efterfrågade attribut) notifieras till medlemmen så att ändringen behöver godkännas innan den slår igenom i den anpassade metadataströmmen vilket ger medlemmen större kontroll över det metadata som konsumeras.

Individuella metadataströmmar

Aggregerad MD

Filter

Individuell MD

