Bilaga 6 - Tekniska krav för anslutning till Skolfederations provisioneringslösning

Inledning

Skolfederations provisioneringslösning kräver för god säkerhet och interoperabilitet att kraven i denna bilaga uppfylls av varje tekniskt ansluten Medlem i Skolfederations provisioneringslösning.

Aktörskrav

Producent

Med Producent avses den part (Användarorganisation) som levererar (producerar) information till en Konsument (Tjänsteleverantör). Producenten avgör, i enlighet med gällande lag och avtal, vilken information som lämnas ut till vilken Konsument. Producenten förutsätts ha tillgång till erforderliga register för att tillhandahålla den information som ska överföras.

Konsument

Med Konsument avses den part (Tjänsteleverantör) som mottager (konsumerar) information från en Producent. I Skolfederations provisioneringslösning kan det exempelvis handla om information om användare, undervisningsgrupper, och organisationsstrukturer som vanligen krävs för att kunna auktorisera en användares åtkomst till Konsumentens tjänster i samband med inloggning.

Federationsoperatör

En av Federationsoperatörens viktigaste uppgifter är att tillhandahålla ett aggregat av digitalt signerat Metadata, vilket kan anses vara Federationens tekniska kärna som knyter samman parterna. Federationsoperatören ansvarar för att annoteringar och utökningar i Metadata som registrerats direkt hos Skolfederation är korrekta och i den mån dessa påverkar beteende hos Producenter och Konsumenter också överensstämmer med federationens regelverk och gällande lag.

Teknik

Nyckelhantering

Säkerhetskrav på nycklar för signering och kryptering

Samtliga Medlemmar i Federationen **ska** skapa, hantera och förvara sina signerings- och krypteringsnycklar i enlighet med de krav som ställs i Skolfederations Tillitsramverk. Där annat inte angetts **ska** val av algoritmer och nyckellängder för autentisering, kryptering och signering följa NIST SP 800-131A eller ETSI TS 102 176-1 5 . I termer av algoritmval, kan kraven uppfyllas genom att använda SHA-256 och RSA med en nyckellängd (modulus) om minst 2048 bitar. Observera att krav på nyckellängder och val av algoritmer är föremål för ständig omvärdering, varför detta krav kan komma att förändras över tid.

Publicering av Federationsoperatörens publika nyckel

Federationsoperatörens publika nyckel används för verifiera signaturerna över publicerad Metadata. Aktuell nyckel publiceras under följande webbadress:

https://www.skolfederation.se/teknisk-information/kontosynk/

Verifiering av Federationsoperatörens publika nyckel

Vid uppdatering av Federationsoperatörens publika nyckel i en Medlems lokala konfiguration **ska** Medlemmen alltid verifiera dess äkthet mot minst två olika källor. Följande är sådana godtagbara verifieringskällor:

- hämtning av nyckel direkt från publiceringsplatsen (https://www.skolfederation.se/teknisk-information/kontosynk/), innefattande positiv verifiering av det HTTPS- certifikat som identifierar publiceringsplatsen (i enlighet med Web PKI),
- kontakt med Skolfederations kundtjänst, där nyckelns digitala fingeravtryck verifieras över telefon.

Byte av Federationsoperatörens publika nyckel

Vid planerat byte av Federationsoperatörens publika nyckel **ska** samtliga Federationens Medlemmar meddelas minst 30 dagar innan den nya nyckeln börjar användas för signering. För att minska risken för sammanblandning publiceras den nya nyckeln och tillhörande Metadata på en webbadress som skiljer sig från tidigare nycklar/Metadata med hjälp av versionsförändring av URL:en enligt ovan.

Metadata

För att Medlemmarna i Federationen ska kunna lita på varandras provisionerade information krävs ett utbyte av parternas publika nycklar. Utbytet sker genom att Medlemmarnas Metadata (MD), vilket beskriver deras egenskaper, förmågor och publika nycklar, aggregeras av Federationsoperatören. Federationsoperatören genomför rimlighetskontroller, varefter denne signerar och publicerar det aggregerade Metadatat. Det aggregerade och signerade Metadata som publiceras av Federationsoperatören är således den samlade bilden av Federationens samtliga aktörers egenskaper, förmågor och publika nycklar.

Publicering av Metadata

Federationens aggregerade och signerade Metadata publiceras under följande adress (VERSION ersätts med versionsnummer för aktuellt Metadata):

https://md.swefed.se/kontosynk/kontosynk-prod-VERSION.jws

Verifiering av signerad Metadata

Varje Medlem ska, med den av Federationsoperatören publicerade nyckeln, verifiera den elektroniska signatur som omsluter Metadatat vid varje uppdatering av den lokala kopian.

Utformning av Metadata

I specifikationen för Federated TLS Authentication[1] regleras hur utformning av Metadata sker. Samtliga ingående Medlemmar i Federationen som vill använda Skolfederations provisioneringslösning **ska** utforma sitt Metadata enligt denna specifikation. Utöver dessa krav **ska** Medlemmar även stödja eventuella profileringar av Metadata publicerade på skolfederation.se.

[1] https://github.com/kirei/tls-fed-auth

Uppdatering av Skolfederations Metadata

Skolfederations Metadata innehåller beskrivning av hur länge det får användas via attributet *exp* i Metadatats header. Medlemmar **ska inte** lita på federationens Metadata efter att tidsangivelsen i *exp* har passerats. Medlem **bör** uppdatera sin lokala kopia av federationens Metadata med en periodicitet på trettio minuter.

Revisionshistorik

Datum	Version	Författare	Kommentar
2019-11-22	1.0	Rasmus Larsson	Första utgåva av Bilaga 6