INTERNET STIFTELSEN

Tekniska krav för anslutning till Skolfederation Moa

Senast uppdaterad 2024-05-30

INTERNET STIFTELSEN

1 Inledning

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

2 Teknik

2.1 Nyckelhantering

2.1.1 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, alternativt SHA-256 med ECDSA med en nyckellängd om minst 224 bitar. Observera att krav på nyckellängder och val av algoritmer är föremål för ständig omvärdering, varför detta krav kan komma att förändras över tid.

2.1.2 Publicering av Federationsoperatörens publika nyckel

Federationsoperatörens publika nyckel används för att verifiera signaturerna över publicerad Metadata. Aktuell nyckel publiceras på federationens tekniska wiki.

2.1.3 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 federationens tekniska wiki, 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.

2.1.4 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.

2.2 Metadata

2.2.1 Publicering av Metadata

Federationens aggregerade och signerade Metadata publiceras på federationens tekniska wiki.

2.2.2 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.

2.2.3 Utformning av Metadata

Krav för hur utformning av Metadata ska ske i federationen finns reglerat i federationens tekniska profil, som är publicerat på federationens tekniska wiki.

2.2.4 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 i enlighet med den periodicitet som är angiven i attributet cache_ttl i Metadatats header.