Ny LoA-hantering för SITHS-kort 2021

Innehåll:

- Bakgrund
- Tidsplan för förändringen
- Vad behöver e-tjänsterna göra?
- SITHS-kort och eventuell ny LoA-nivå

Viktigt

Viktig information till alla e-tjänster anslutna till IdP

Bakgrund

All SITHS-kortinloggning med hjälp av både gamla och nya IdP:n har hittills efter dispens från Sambi setts som likvärdiga oavsett utgivningssätt. Sättet ett SITHS-kort är utgivet på styr vilken tillitsnivå det anses ha. Nivåerna kallas *Level of Assurance* (LoA) och kommer härefter kallas LoA-nivå.

Med lanseringen av SITHS e-id har LoA-nivån på SITHS-korten förtydligats genom att denna ingår i namnet på kortets certifikat. Till exempel är ett SITHS e-id-kort med certifikatet *SITHS e-id Person HSA-id **3** CA v1* är ett kort utgivet med högsta använda tillitsnivå LoA 3 medan *SITHS e-id Person HSA-id **2** CA v1* är utgivet med lägre tillitsnivå LoA 2 utgivet med rutiner för utlämnande av reserv- och crossborder-kort.

Hittills har alltså all lyckad SITHS-kortinloggning resulterat i en SAML-biljett med tillitsnivå LoA 3. Förändringen när dispensen löper ut betyder att IdP kommer att börja rapportera SITHS-kortets verkliga tillitsnivå i, bland annat, den utställda SAML-biljetten. Notera att gamla, ej uppgraderade SITHS-kort (inklusive eventuella s k "mjuka" certifikat av typen SITHS Type **3** CA v1 PP som ibland används i automatiska tester) kommer att betraktas som LoA 2.

Tidsplan för förändringen

Datum	Miljö
01 Oct 2020	**TEST/QA**
09 Nov 2020	**TEST/QA** Funktionscertifikat (för t ex autotester) utvärderas till LoA2
18 Jan 2021	**PRODUKTION**

Testkort

Notera att även testkort utgivna av SITHS Type 1 CA v1 PP kommer att bli LoA 2 fr.o.m 1:a oktober 2020.

Vad behöver e-tjänsterna göra?

Den första frågan förvaltningen av en e-tjänst måste reda ut är vilka krav på LoA-nivå som gäller för inloggning i den aktuella e-tjänsten. Får man logga in med reserv/crossborder-kort LoA 2 eller krävs den högsta använda LoA-nivån 3?

Den andra frågan är hur e-tjänsten vill kontrollera att inloggningen sker med ett SITHS-kort med tillräckligt hög tillitsnivå. Gör man det genom att evaluera utställd biljett och därmed sköta behörighetsstyrningen själv eller vill man att IdP:n ska rapportera misslyckad inloggning genom att i anropet till IdP:n (*Auth Request RequestedAuthnContext*) ange vilken/vilka LoA-nivåer som e-tjänsten kräver för en lyckad inloggning?

1. Varje förvaltning av en e-tjänst ansluten till IdP ombeds att se över ifall den anger LoA-nivå i sitt AuthRequest (eller motsvarande filtrering av claim/scope inom OIDC) och fundera på om detta fungerar med e-tjänstens krav på LoA-nivå när reservkort och gamla, ej uppgraderade, SITHS-kort börjar att rapporteras som LoA 2 enligt tabellen nedan.

Observera att ifall en SP till exempel accepterar både LoA 2 och LoA 3 och vill ange detta i sitt *AuthnRequest* så måste båda skickas med då IdP endast har stöd för *exakt* jämförelse av tillitsnivå (detta då SAMBI ställer det som tekniskt krav).

```
<samlp:AuthnRequest Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
    ...
    <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://sak.ost.se:4
    <samlp:RequestedAuthnContext Comparison="exact">
        <saml:AuthnContextClassRef>http://id.sambi.se/loa/loa2</saml:AuthnContextClassRef>
        <saml:AuthnContextClassRef>http://id.sambi.se/loa/loa3</saml:AuthnContextClassRef>
    </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Ett tillvägagångssätt att ta reda på en e-tjänsts AuthnRequest finns beskrivet i FAQ #28. Motsvarande för OIDC (jwt) i FAQ #29.

2. Varje förvaltning av en e-tjänst ansluten till IdP ombeds att se över ifall

> **a) den begär attributet (urn:sambi:names:attribute:levelOfAssurance eller acr i OIDC fallet) för LoA-nivå i sitt metadata och därmed i SAML/JWT-biljetten och**
>
> **b) fundera på om detta attribut evalueras av e-tjänsten och - i sådana fall om detta fungerar med e-tjänstens krav på LoA-nivå när reservkort och gamla, ej uppgraderade, SITHS-kort börjar att rapporteras som LoA 2 enligt tabellen nedan.**

Se även avsnittet om Tillitsnivå (LoA) i Anslutningsguide till IdP

SITHS-kort och eventuell ny LoA-nivå

Följande tabell visar på vilka typer av kort/certifikat IdP stödjer och vilken LoA-nivå som kommer att rapporteras i och med förändringen.

Utfärdare	LOA	OID-värde i Certifikatsprinciper	Kommentar
SITHS e-id Person HSA-id 3 CA v1 TEST SITHS e-id Person HSA-id 3 CA v1	3	1.2.752.74.8.502 1.2.752.74.8.503 1.2.752.74.8.506 1.2.752.74.8.507 1.2.752.74.8.509	502 - Ordinarie nyutgivet kort 503 - Reservkort LoA 3 506 - Distansuppgraderat kort 507 - Tilläggscertifikat 509 - Reservkort LoA 3, förlängt av användare via självservice.
SITHS e-id Person ID Mobile CA v1 TEST SITHS e-id Person ID Mobile CA v1	2 (3)	1.2.752.74.8.504	Certifikat för mobil autentisering. Hanteras som LoA 2 tills utfärdandeprocesssen har certifierats som LoA 3 av DIGG.
	2	1.2.752.74.8.510	Certifikat för mobil autentisering, temporär produktionsmiljö.
SITHS e-id Person HSA-id 2 CA v1 TEST SITHS e-id Person HSA-id 2 CA v1	2	1.2.752.74.8.501 1.2.752.74.8.508	501 - Reservkort LoA 2 508 - Reservkort "Crossborder"
SITHS CA Crossborder SITHS CA CrossBorder TEST v3	2	NA	Gamla SITHS "Crossborder"
SITHS Type 1 CA v1 SITHS Type 1 CA v1 PP	2	NA	Gamla, ej e-id-uppgraderade SITHS-kort oavsett utgivare (SIS, SITHS, lokalt utgivna, företagskort e.t.c). Kända typer och dess kortnummerserie: SITHS - SIS: 9752 XXXX 357 SITHS Reservkort: 9752 XXXX 957 SITHS VGR-utfärdade kort: 9752 XXXX 854 SITHS Skåne-utfärdade kort: 6280 8335 54 * Företagskort med eget utfärdarnummer: 9752 XXXX 857
SITHS Type 3 CA v1 PP	2	NA	Funktionscertifikat med kopplat testpersonpost i HSA Integrationsmiljö för bl a autotester

För frågor kontakta Ineras Support