2.4 Release notes - IdP

Revisionshistorik

Revisionshistorik

Version	Datum	Aktör	Förändring
0.1	06 Feb 2023	Nilsson, Bengt (OS Sweden AM)	Första utkast
0.2	23 Feb 2023	Ehlert, Stefan	Lagt till information om viktiga ändringar
0.3	10 Mar 2023	Christoffer Johansson	Förtydligat viss information och flyttat en del saker från viktiga till övriga ändringar.
0.4	13 Mar 2023	Christoffer Johansson	Ytterligare uppdateringar
0.9	17 Mar 2023	Christoffer Johansson	Inväntar svar om: • Utestående frågor och sista påsyn av CGI • Tider för release
0.95	17 Mar 2023	Christoffer Johansson	Kompletterad med svar på utestående frågor. Kvarstår att fastställa tidpunkter för release.
0.96	20 Mar 2023	Christoffer Johansson	Uppdaterat datum för release i olika miljöer
0.97	23 Mar 2023	Christoffer Johansson	Ändrade från Basefarm till Orange.
1.0	24 Mar 2023	Christoffer Johansson	Godkänd av förvaltning
1.01	30 Mar 2023	Christoffer Johansson	Tog bort information om SAML validatorn kontroll av felstavningar och icke-existerande attribut då den flyttades till senare release.
1.02	03 Apr 2023	Christoffer Johansson	Lade till information om att multipla subdomäner för SITHS-kort på denna enhet (mTLS) inte aktiveras förrän Q3-2023.

Innehållsförteckning

Innehållsförteckning

1. Datum i korthet

Miljö	Beräknade releasedatum
Systemtest CGI	24 Feb 2023
Acceptanstest Orange	16 Mar 2023
Acceptanstest Nogui	20 Mar 2023
QA Orange + Nogui	03 Apr 2023 till 14 Apr 2023
Prod Nogui	18 Apr 2023
Prod Orange	19 Apr 2023

2. Förändringar

2.1. Viktiga ändringar

Denna funktion aktiveras först under Q3-2023

I väntan på att den aktiveras får användaren bara **ett försök** att välja sitt klientcertifikat per webbläsarsession. Om SITHS-kortet inte sitter i läsaren, är för fel miljö eller om importen av certifikaten till operativsystemet inte fungerar måste användaren starta om webbläsaren för att kunna göra ett nytt försök att välja klientcertifikat. Detta beror på att det är den logiken som gäller för marknadens olika webbläsare.

Sammanfattning	Beskrivning	För lokal IdP
Förändringar för autentiseringsmetoden **SITHS-kort på denna enhet** (Mutual TLS) • Introduktion av flera subdomäner för legitimering med mTLS. • Möjlighet att göra ett nytt försök vid legitimering med mTLS.	Denna ändring påverkar endast autentiseringsmetoden **SITHS-kort på denna enhet.** **OM** webbläsaren har ett giltigt identitetsintyg uppnås som vanligt IdP SSO. Denna ändring påverkar endast beteendet när en användare måste göra en ny inloggning via IdP. **OM** webbläsaren **inte** har IdP SSO kommer hen att vid upprepade inloggningar kommer att behöva välja ett certifikat på nytt Ändringen fungerar så att IdP använder sig av flera subdomäner/endpoints som webbläsaren skickas mellan. Anledningen till att webbläsaren behöver slussas till nya domännamn är för att webbläsare "sparar" valt certifikat per domännamn. Genom att skicka webbläsaren vidare till olika domännamn kan IdP få upp användardialogen om att välja klientcertifikat för varje nytt domännamn. I praktiken innebär detta att användaren/webbläsaren, för metoden **SITHS-kort på denna enhet,** istället för att endast hamna på secure.idp.inera<miljö>.org/se kommer att hamna på någon av subdomänerna **secure0-secure24**.idp.inera<*miljö*>.org/se. Vilken subdomän webbläsaren hamnar på styrs av en lokalt lagrad sessions-cookie för webbläsaren. Totalt får webbläsaren **25 inloggningsförsök** innan den behöver startas om. Tidigare behövde webbläsaren startas om efter 1 försök. En följdeffekt av ovan är också att användaren får möjlighet att göra nya försök till legitimering om hen glömt stoppa in ett kort. Tidigare skickades användaren tillbaka till tjänsten där hen påbörjade sin inloggning.	Instruktioner kring hur detta kan konfigureras finns i **kapitel 9.4.3** i **SAD IdP**

2.2. Övriga ändringar

Sammanfattning	Beskrivning	För lokal Idp
Attributet för administrativa uppdrag ska kunna hämtas även via SAML	Attributet för administrativa uppdrag (authorizationScope) kan nu hämtas via SAML. Tidigare kunde det endast hämtas via OIDC	
Attributet at_hash levereras i scopet oidc	Attributet at_hash levereras nu som standard i scopet oidc. Tidigare var detta endast dokumenterat och ej implementerat.	
Förbättringar i IdP Public Tools SAML-validatorn	Användare har nu möjlighet att importera SAML metadata till IdP Public Tools SAML-validatorn utöver möjligheten att kunna klistra in metadata manuellt.	
Statistik per timme	Förvaltningen på Ineras och kunder med lokal IdP kan nu få ut statistik per timme. Statistiken innehåller information om antal in- och utloggningar per timme sammanlagt och per anslutning. Statistiken är uppdelad per protokoll och lyckade/misslyckade inloggningar. Den går också att ta ut per anslutning/klient.	Detaljerad information om detta finns under **rubrik 10.3** på sidan **Lokal IdP**

2.3. Visuella ändringar

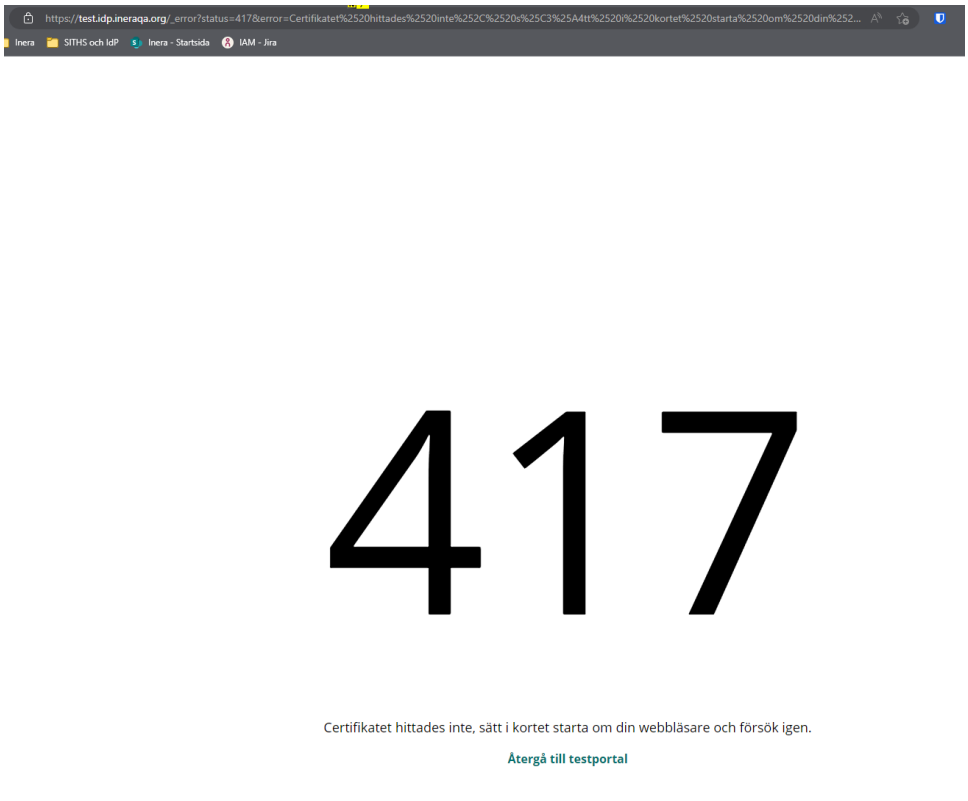
2.3.1. Nya vyer för autentiseringsmetoden SITHS-kort på denna enhet

Denna ändring påverkar endast autentiseringsmetoden **SITHS-kort på denna enhet**, dvs. när användaren autentiseras med Mutual TLS /Dubbelriktad TLS (mTLS).

2.3.1.1. För många inloggningsförsök via dubbelriktad TLS

Från och med denna version får användaren upp till 25 försök att logga in via IdP som driftas av Inera. När dessa försök är förbrukade i den pågående webbläsarsessionen (dvs. utan att alla flikar för webbläsaren stängs webbläsaren startas på nytt) fås följande meddelande.

Logiken med att användaren alltid får upp till **25 inloggningsförsök** är beroende av att användarens webbläsare **INTE** har inställningen för att öppna flikar från föregående session aktiverad. Mer information finns i **Anslutningsguide till IdP**

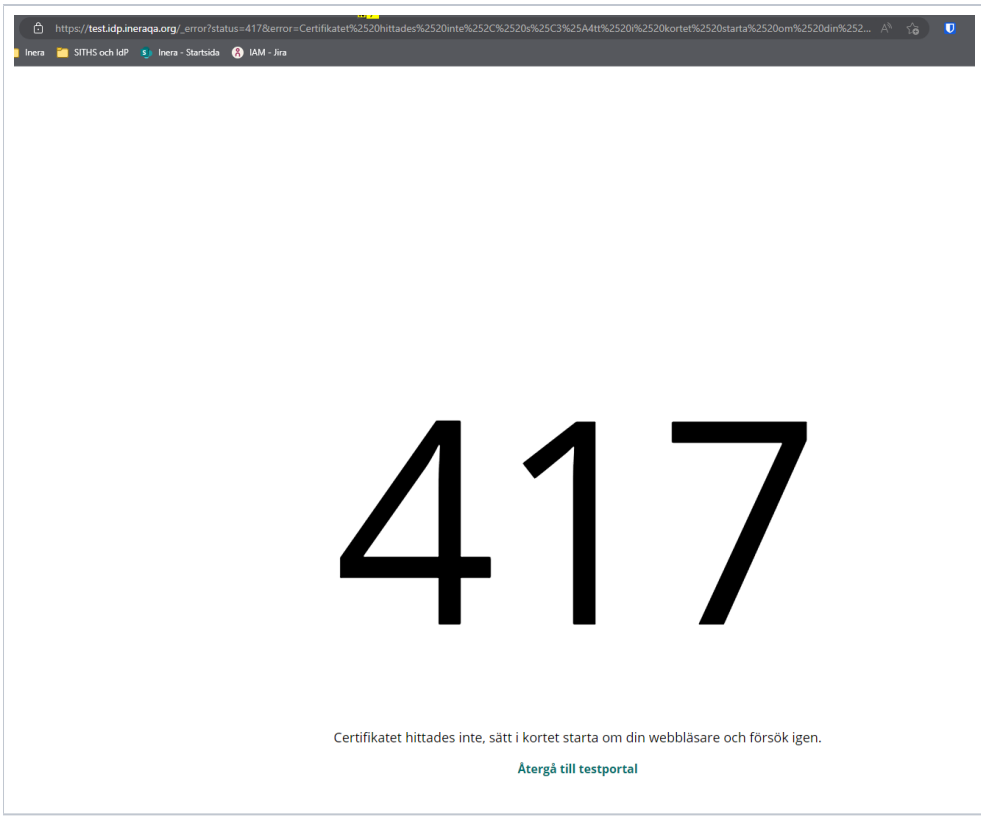
Innan IdP 2.4 - Endast en subdomän	IdP 2.4 eller senare - med flera sub
	

2.3.1.2. Inget certifikat användes

Detta kan uppstå om användaren:

- Glömmer sätta i sitt SITHS-kort
- Det är problem att importera certifikaten från kortet till datorn med Net iD eller SITHS eID-app för Windows **MD** (SAC minidriver)
- Användaren har satt i ett SITHS-kort avsett för en annan miljö en den där hen loggar in

Flera endpoints inaktivt (gamla lösningen)	Flera endpoints aktivt


https://test.idp.ineraqa.org/_error?status=417&error=Certifikatet%2520hittades%2520inte%252C%2520s%25C3%25A4tt%2520i%2520kortet%2520starta%2520om%2520din%252...
Inera
SITHS och IdP
Inera - Startsida
IAM - Jira
417
Certifikatet hittades inte, sätt i kortet starta om din webbläsare och försök igen.
Återgå till testportal


IdP - Inera
https://idp.dev.inera.test:8443/idp/no-cer
IdP
Inget certifikat användes vid inloggni

3. Påverkan på existerande funktionalitet

3.1. Nya användarattribut

- Inga nya användarattribut

3.2. Ändrade användarattribut

Namn	OIDC	SAML Friendly	SAML Name	Beskrivning	Ändring
authorizationScope	authorizationScope	authorizationScope	urn:authorizationScope	Möjliggör för anslutande tjänsten att få administrativa uppdrag för en person.	Attributet kan från och med denna release hämtas via SAML och inte bara via OIDC

4. Dokumentation

4.1. Uppdaterad dokumentation

Följande dokumentation är uppdaterad:

- 2.4.1 Patch Release - IdP
- 2.4 SAD - IdP
- 2.4 Lokal IdP
- 2.4 Anslutningsguide till IdP
- 2.4 Attributlista

4.2. Fullständig åtgärdslista

Åtkomst till informationen nedan kräver inloggning

Visa fullständig åtgärdslista

Unable to render {include} The included page could not be found.

4.3. 2.3 Testrapport (CGI) - IdP

Åtkomst till informationen nedan kräver inloggning

Visa testrapport

Unable to render {include} The included page could not be found.

4.4. 2.3 Testrapport (NMT) - IdP

Åtkomst till informationen nedan kräver inloggning

Visa testrapport

Unable to render {include} The included page could not be found.

5. Lokal IdP

Lokal IdP kommer att tillgängliggöras för nerladdning, för aktuella regioner.