Anslutningsguide till IdP

Innehållsförteckning

Revisionshistorik

Version	Datum	Författare	Kommentar
0.1	26 Oct 2023	Ehlert, Stefan	• Kopierat från IdP 2.4 • Lagt till modifierad information om förval av principalen
1.0	17 Nov 2023	Pietu Hammarström	Godkänt

1. Sammanfattning

Ineras IdP syftar till att erbjuda vårdgivare och dess vårdsystem en säker autentisering av aktörer/vårdpersonal för olika behov. Ineras IdP tillhandahåller s. k. single sign on (SSO) inom webbapplikationer enligt väl definierade standarder, så som SAML Web SSO Profile samt OpenID Connect. E-tjänst och system används synonymt i följande dokument.

Tjänsten tillhandahåller också funktion för att logga ut aktören och avsluta SSO-sessionen hos IdP.

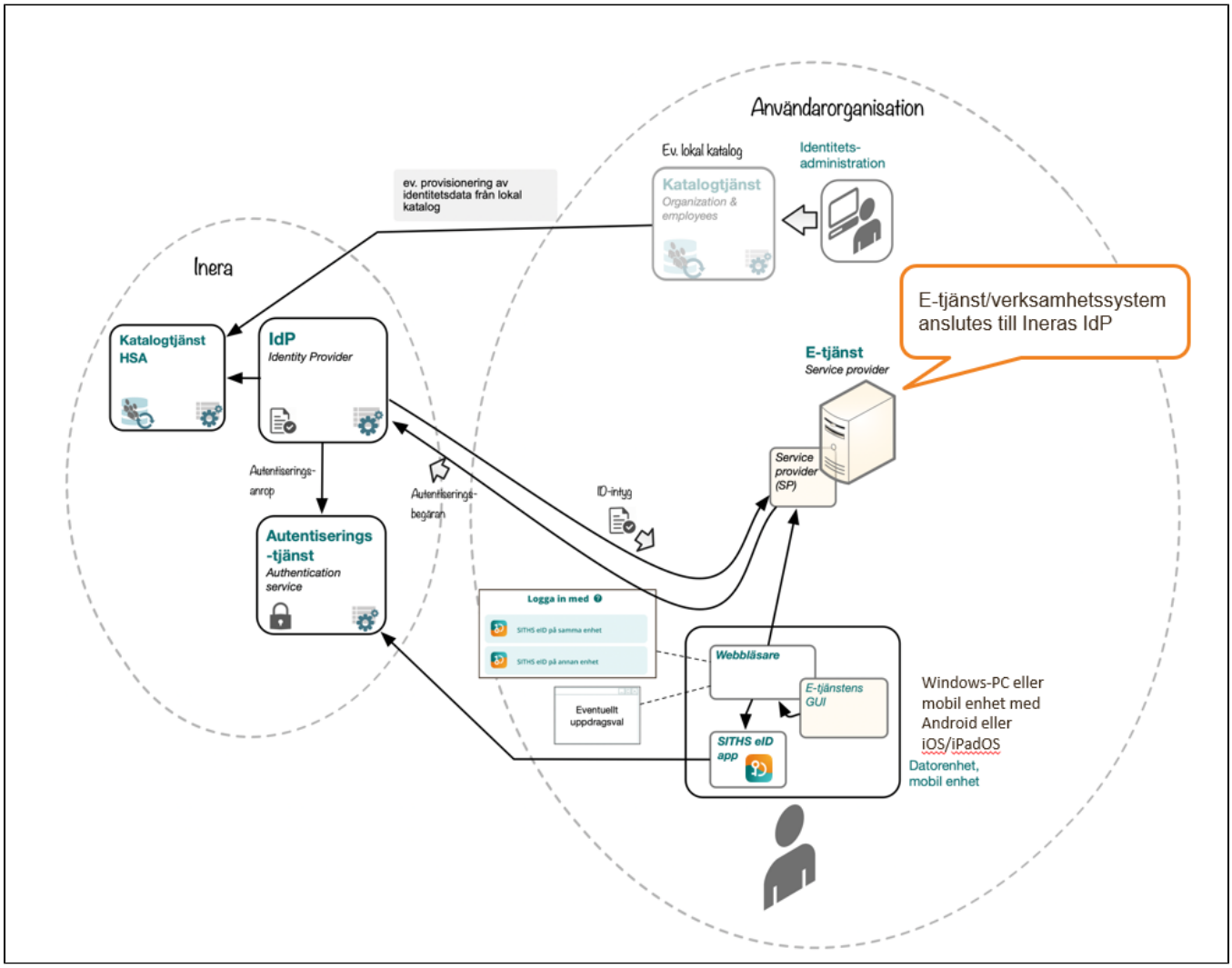
Vid en lyckad autentisering utfärdas ett identitetsintyg, (SAML-biljett, eller Id-token för OIDC) som innehåller information om autentiseringen samt eventuellt ytterligare användarattribut, som kan användas av ett ABAC (Attribute Based Access Control) behörighetssystem, d.v.s. behörighet på egenskapsnivå.

Anslutning till IdP kan ske direkt för en e-tjänst, men det går också att ansluta en lokal IdP som en proxy till Ineras IdP. För jämförelse mellan olika anslutningsmönster, se Att ansluta e-tjänster för autentisering med SITHS eID.

För att anslutande e-tjänst skall få ut ytterligare användarattribut måste slutanvändare som skall autentiseras existera i den nationella HSA-katalogen. Beroende på vilka attribut som efterfrågas för en aktör kan eventuella val behöva göras i inloggningsflödet. Exempel på detta är medarbetaruppdrag och /eller autentiseringsmetod.

De e-tjänster som vill nyttja elektronisk underskrift kan ansluta till Underskriftstjänsten. I och med denna anslutning möjliggörs *autentisering för underskrift via Ineras IdP,* se Underskriftstjänsten.

Exempel på e-tjänsts anslutning till Ineras IdP som Service Provider och med ny auteniseringsmetod och klient:



1.1. Tekniska förutsättningar för användning Inera IdP

Nedan följer information om de övergripande tekniska kraven och komponenterna för anslutning och användning

I dagsläget utfärdas identitetsintyget enligt två protokoll, SAML (Security Assertion Markup Language) och OIDC (OpenID Connect).

Anslutande e-tjänster väljer vilket av dessa båda protokoll som de vill nytta.

1.1.1. SAML

Ansluten e-tjänst registreras manuellt i Ineras IdP genom förmedling av metadata. Genom metadata kan man ex. specificera vilka attribut man önskar få från IdP:n och utbyta vilka nycklar som ska användas, adresser vid utloggning, o.s.v.
Se SAML-Profilen och Attributstyrning SAML för detaljer kring hur Inera IdP implementerar SAML-protokollet.

För åtkomst till IdP:s SAML-metadata, se Adresser och portar nedan.

1.1.1.1. Validering av SAML metadata

För att säkerställa att metadata uppfyller kraven för att kunna läsas in i IdP:n bör ett eller flera valideringsverktyg användas. Använd gärna verktygen i listan nedan för att säkerställa att metadatat valideras korrekt innan det förmedlas till förvaltningen för inläsning till IdP:n.

I de fallen då ADFS metadata är tänkt att läsas in ska inte Sambi Metadata validatorn användas. I de fallen bör endast IdP Public tools användas.

- IdP Public tools - IdP:ns egen metadata validator. Valideras metadatat korrekt i detta verktyg går det att läsa in i IdP:n.
- Sambi Metadata validator - Sambis egen SAML metadatavalidator
- Chilkat Online Tools - XML Digital Signature verification - Verktyg för att validera signerad XML. Går signaturen inte att verifiera kan metadatat inte läsas in i IdP:n.
- CSR Decoder and Certificate Decoder - Verktyg för att kontrollera giltigheten av certifikat

1.1.1.2. Förmedling av SAML metadata

Förmedlingen av metadata kan ske på flera olika sätt. Som del av den förstudie som skickas in när e-tjänsten ska registreras väljs vilket sätt som ska användas. De tvåmöjligheterna som erbjuds idag är som följer:

1.1.1.2.1. Skicka in metadata på fil för engångs-inläsning

Väljs detta alternativ skickas en .xml-fil innehållandes metadatat in som senare också ska bli inläst i IdP:n. Detta görs enklast genom att skicka in filen i samband med att förstudien skickas in för granskning. Metadatat kommer då att granskas i samma veva som förstudien granskas.

1.1.1.2.2. Skicka in metadata via en URL för engångs-inläsning

Vid detta alternativ anges en URL varifrån metadatat kan hämtas som ska bli inläst till IdP:n. Säkerställ gärna en extra gång att URL:en funkar och att metadatat som fås via URL:en är rätt metadata för anslutningen. Under förstudiegranskningen kommer samma metadata som hämtas från URL:en användas för granskning.

1.1.2. OIDC

Registrering av OIDC-klienter i Inera IdP sköts manuellt. Se OIDC-Profil och Attributstyrning OIDC för detaljer kring hur Inera IdP implementerar OIDC-protokollet.

För åtkomst till IdP:s OIDC-metadata, se Adresser och portar nedan.

1.1.3. Sjunet

Ineras IdP är tillgänglig från både internet och Sjunet med samma instans och domän (se Adresser och portar nedan).

Se Nätverksinställningar för tjänster inom identitet och åtkomst för gemensam nätverksteknisk information för alla IAM-tjänsterna (IdP, Autentiseringstjänsten, Utfärdandeportalen, etc.), inklusive information om Sjunet-routing.

1.1.4. Funktionscertifikat

1.1.4.1. Produktion

Anslutande systems signeringscertifikat (det certifikat som bifogas i t.ex. SAML metadata och som meddelanden signeras med) för produktionsmiljö kan ställas ut av valfri utfärdare men nyckelhanteringen förutsätts följa de instruktioner och rekommendationer som anges i "Instruktion, nyckelhantering för lagrade krypterade data".

Inera rekommenderar välrenommerade och robusta utfärdare med följsamhet mot principerna i ISO-27002 (wikipedia, riktlinjer till ISO-27001). Väljs "SITHS e-id Function CA v1" (utfärdare, SITHS e-id Root CA v2) kan mer information ges på SITHS på inera.se. Se SITHS CA repository för de utfärdande certifikaten.

1.1.4.2. Testmiljöer

Vilken utgivare som helst är godkänd för funktionscertifikaten som används i anslutningar till testmiljöerna.

1.1.5. Programvara som användaren behöver

En eller flera klientapplikationer/klientprogramvaror behöver vara tillgängliga för e-tjänstens slutanvändare, se avsnitt längre ner för testade versioner och länkar till klienter.

2. Livscykelhantering - förändring av existerande anslutningar

Anslutningen till IdP kan förändras t.ex. om e-tjänsten har nya kontaktuppgifter, har förnyat sitt funktionscertifikat, vill få tillgång till ytterligare användarattribut eller tillgängliggöra flera (eller andra) autentiseringsmetoder för sina slutanvändare.

Vid önskade förändringar i anslutningen följs följande principiella mönster:

1. Inkom med en uppdaterad förstudie för testmiljö(er) där ni fyller i relevanta ändringar och noterar i revisionstabellen vad som ändrats. Bifoga även eventuellt metadata
    a. Efter godkänd förstudie justeras anslutningen hos den aktuella test-IdP:n. Vid nekad förstudie kontaktas e-tjänstens förvaltning
2. Verifiera funktionen i testmiljö(erna) genom att
    a. Inkom med en motsvarande uppdaterad förstudie för produktionsmiljön.
    b. Bifoga testrapport från testmiljö.
    c. Ange eventuellt önskat datum och tidpunkt för aktivering av ny funktionalitet.
3. Vid godkänd förstudie justeras anslutningen i prod-IdP:n, direkt eller vid vald tidpunkt. Vid nekad förstudie kontaktas e-tjänstens förvaltning

3. Anslutningsmönster

3.1. Anslutning av e-tjänst till Ineras IdP

En e-tjänst kan ansluta till Ineras IdP som en SAML SP (Service Provider) eller OIDC RP (Relying Party).

- Vilka metoder som är tillgängliga för slutanvändarna konfigureras i IdP per e-tjänst, det går således att i förstudien att endast använda ett urval av de autentiseringsmetoder som Ineras IdP tillhandahåller.
- e-tjänsten anger i sitt metadata (om SAML) eller i autentiseringsanropet (om OIDC) vilka användarattribut som önskas. Se Attributstyrning SAML alternativt Attributstyrning OIDC.
- Inera IdP tillhandahåller begärda användarattribut som finns på certifikatet och eventuella attribut på personposten i den nationella HSA-katalogen samt presenterar uppdragsval för användaren.
- Inera IdP tolkar och förmedlar tillitsnivå (LoA) utifrån användarens certifikat.

3.2. Anslutning av lokal IdP till Ineras IdP (proxy-anslutning)

Lokala e-tjänster kan erhålla identitetsintyg från Ineras IdP via en lokal IdP genom anslutning som en OIDC RP eller SAML SP och agera som en "proxy-IdP". Anslutningen sker som en vanlig anslutning (som ovan) av en e-tjänst till Ineras IdP men skillnaderna består i stor sett av en förskjuten ansvarsfördelning från Ineras till den lokala IdPn.

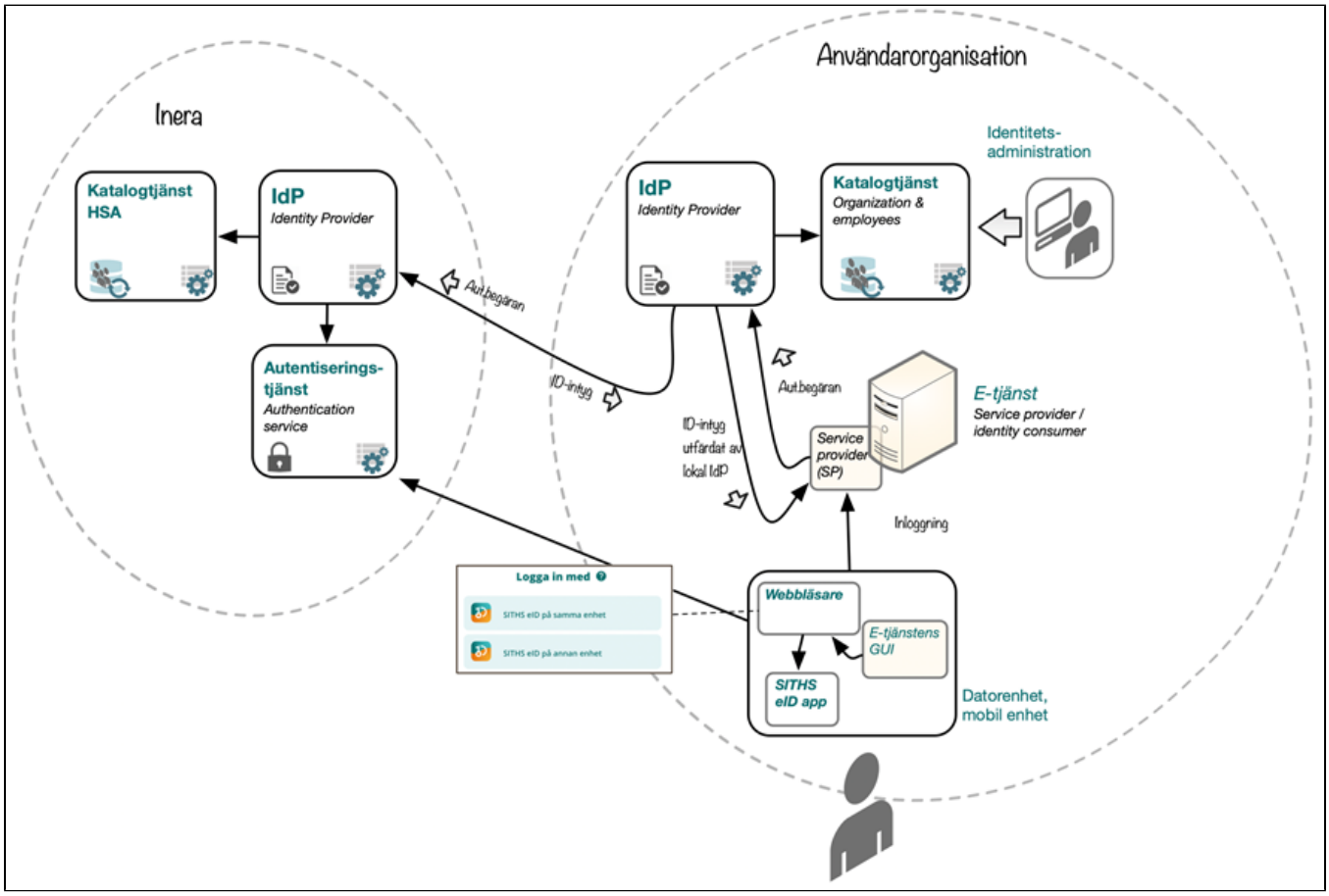
Inera IdP:

- tillhandahåller eventuellt autentiseringsmetod samt de attribut som rör autentisering av användaren, se nästa avsnitt för de idag rekommenderade
- revokeringskontroll

Lokal IdP:

- implementerar en SAML-SP eller en OIDC-RP som ansluts till Ineras IdP,
- väljer vilken eller vilka autentiseringsmetoder som Inera IdP skall exponera för slutanvändare,
- ansvarar för eventuellt uppdragsval,
- (valbart men starkt rekommenderat, revokeringskontroll)
- beräknar tillitsnivå (LoA) utifrån certifikatsattribut som Ineras IdP tillhandahåller
    - Se Tillitsnivå (LoA) för information om hur Ineras IdP tolkar tillitsnivåer för en rekommendation.
- hämtar eventuella övriga användarattribut från en lokal katalogtjänst

Observera att Ineras lokala IdP **inte** kan agera proxy IdP



3.2.1. Användning av iframes

System som har för avsikt att använda sig av iframes för att visa IdP:ns användargränssnitt för slutanvändaren blir inte godkända för att ansluta sig mot IdP:n. Detta med anledning av att vi inte kan lämna några garantier för att IdPn:s funktionalitet bibehålls när iframes används. Detta är ett hårt krav där inga undantag kommer göras. Vidare så avrekommenderar även DIGG emot användningen av iframes, se DIGGs artikel för mer information.

3.2.2. Rekommenderade attribut för en lokal IdP

Förutom attribut som alltid anges i SAML-biljetten eller OIDC-tokens per default (se Attributlista), så är följande attributlista för en rekommendation på en "maximal" lista för lokal IdP att begära från Inera IdP. Detta för att undvika att slutanvändare presenteras uppdragsvalsdialogen i Ineras IdP och förbättra mönstrets effektivitet.

SAML Attributnamn	OIDC Attributnamn
urn:sambi:names:attribute:authnMethod	amr
urn:sambi:names:attribute:x509IssuerName http://www.w3.org/2000/09/xmldsig#X509IssuerName	x509IssuerName
http://www.w3.org/2000/09/xmldsig#X509SubjectName	x509SubjectName
urn:sambi:names:attribute:levelOfAssurance	acr
urn:credential:givenName	credentialGivenName
urn:credential:surname	credentialSurname
urn:credential:personalIdentityNumber	credentialPersonalIdentityNumber
urn:credential:displayName	credentialDisplayName
urn:credential:organizationName	credentialOrganizationName
urn:credential:certificatePolicies	credentialCertificatePolicies

Vill man i den anslutande lokala IdP:n även få med HSA-id för användaren går det också bra, men om det finns flera HSA-id för samma användare så leder det till ett uppdragsval eller tjänsteidval. Vill man undivika det så kan man ta med alla HSA-id för användaren .

SAML Attributnamn	OIDC Attributnamn
http://sambi.se/attributes/1/employeeHsaId	employeeHsaId
urn:allEmployeeHsaIds	allEmployeeHsaIds

4. Dokumentation

Utöver denna guide finns följande dokumentation framtagen för tjänsten.

5. Adresser och portar

Se Nätverksinställningar för tjänster inom identitet och åtkomst för gemensam nätverksteknisk information för alla IAM-tjänsterna (IdP, Autentiseringstjänsten, Utfärdandeportalen, etc.) och övriga tjänster.

Följande adressmatris används för anslutning till Inera IdP och tydliggör i vilken HSA miljö som slutanvändare förväntas finnas. Dessa adresser och IP-adresser är samma för både Internet och Sjunet.
HSA adresserna anger både Sjunet respektive internetgränssnitten för administration.

Mlljö	Domäner	Anslutningsbar	IdP Metadata	OIDC .well-known	SITHS eID App	Ansluten till HSA miljö (se gärna även här (Riktlinjer för tester och testdata))
Produktion	idp.inera.se secure.idp.inera.se	Ja	https://idp.inera.se/saml	https://idp.inera.se/oidc/.well-known/openid-configuration	SITHS eID	https://hsa.inera.se/ https://hsahotell.carelink.sjunet.org/nordicedge/customer/hsa/jsp/login.jsp
QA	idp.ineraqa.org secure.idp.ineraqa.org	Ja	https://idp.ineraqa.org/saml	https://idp.ineraqa.org/oidc/.well-known/openid-configuration	QA SITHS eID	https://hsatest.inera.se/ https://testhotell2.carelink.sjunet.org/
Test	idp.ineratest.org secure.ineratest.org	Ja, främst Ineras e-tjänster	https://idp.ineratest.org/saml	https://idp.ineratest.org/oidc/.well-known/openid-configuration	TEST SITHS eID	https://hsatest.inera.se/ https://testhotell2.carelink.sjunet.org/

6. Tillitsnivå (LoA)

För hantering av tillitsnivå för olika typer av certifikat, se Tillitsnivå (LoA).

7. Autentiseringsmetoder

7.1. Aktivering av autentiseringsmetoder

Anslutna tjänster kan välja vilka inloggningsmetoder som skall vara aktiva och därmed valbara för användarna vid autentisering.

Tillgängliga metoder:

- SITHS eID på **annan** enhet
- SITHS eID på **denna** enhet
- SITHS-kort på **denna** enhet

> Om endast en metod är aktiv för given e-tjänst så ställs användaren inte inför något val av autentiseringsmetod.

> Om metoden **SITHS-kort på denna enhet** är vald, kommer metoden att synas på mobila enheter. Autentiseringslösningen baserar sig dock på dubbelriktad TLS (mTLS), vilket inte fungerar tillsammans med SITHS. Om man vill försäkra sig om att detta inte händer bör man definiera en egen SP-ingång som uteslutande visar SITHS eID-metoderna och som man hänvisar användare av Mobila enheter till.

Aktivering av ny autentiseringsmetod som använder SITHS eID-apparna görs vid ifyllande av förstudiemall version 3.x, både för nya anslutningar samt befintliga. Se den generella rutinen för livscykelhanteringen ovan

Förutom det formella anslutningsförfarandet tillkommer arbete kring att

1. ordna med brandväggsöppningar mot Autentiseringstjänsten (Nätverksinställningar för tjänster inom identitet och åtkomst),
2. säkerställa att slutanvändarna använder en webbläsare (för att anropa IdP) på ett sätt som möjliggör för autostart av SITHS eID-appen (se även nedan samt SITHS eID Appväxling - Exempel för inbäddade webbläsare),
3. informera och eventuellt utbilda slutanvändarna i användningen av appar/mobila enheter samt
4. distribuera appar, (inklusive att över tid säkerställa förmåga till robust testning och uppdatering)

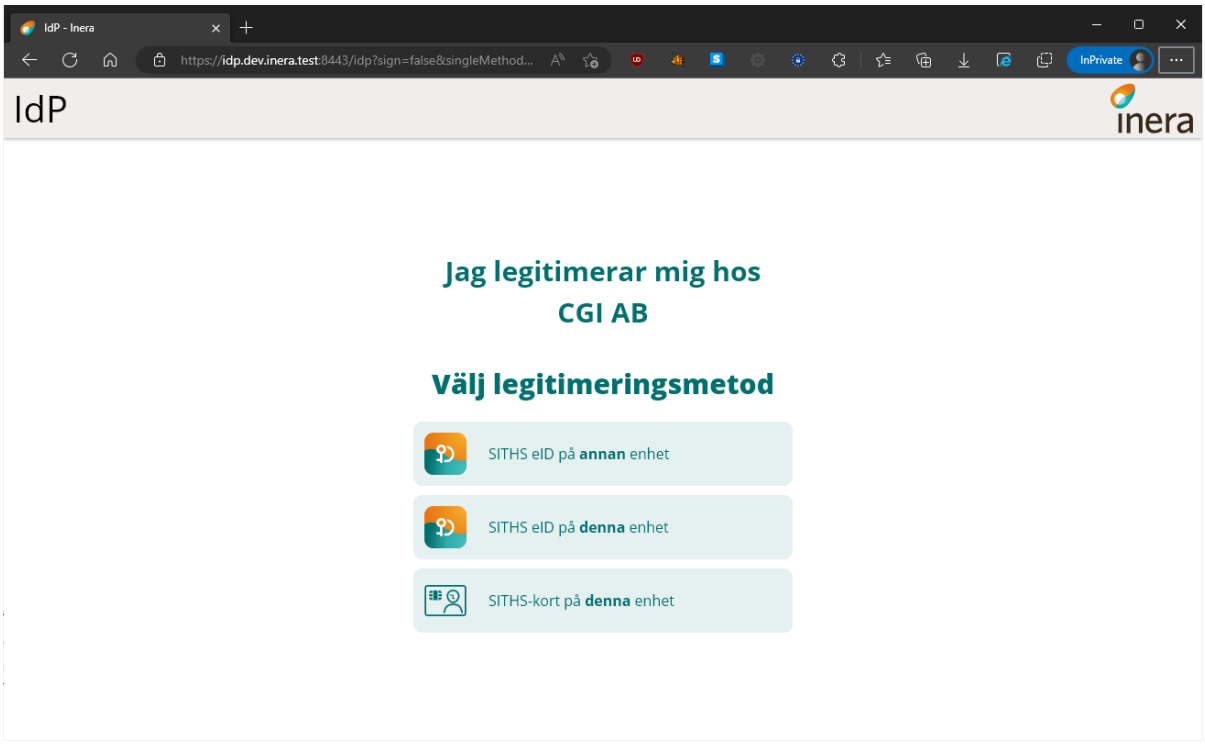
För mer detaljerad information om autentiseringsmetoderna för "SITHS eID på **denna** respektive **annan** enhet" och vilka krav som ställs på anslutande organisationer, se Anslutningsguide till Autentiseringstjänst SITHS.

7.2. Användarval av autentiseringsmetod

För de tjänster som aktiverar **fler än en** autentiseringsmetod så kommer användarna vid autentisering att mötas av en dialog där de får välja vilken metod de vill använda. Säkerställ att e-tjänstens slutanvändare har erforderlig klientprogramvara installerad, har fått lämpliga instruktioner i god tid före produktionsutrullning och inte överraskas över denna dialog (samt eventuellt, lämplig mobil enhet, tillgänglig).

För slutanvändaren kan valet av autentiseringsmetod påverka det senare uppdragsvalet om ett sådant krävs.

- SITHS-kort på denna enhet kommer alltid föredra HSA-id-certifikat
- SITHS eID på denna/annan enhet föredrar ett personnummer-certifikat om ett sådant finns. Beroende på vilka uppdrag som har kopplats i HSA för personnumret jämfört med vad som är kopplat till HSA-id:t kan SITHS eID på denna/annan enhet resultera i att användaren får fler valbara alternativ i tjänste-id- och uppdragsvalet.



7.2.1. SITHS-kort på denna enhet - Dubbelriktad TLS/Mutual TLS (mTLS)

Autentiseringslösningen baseras på teknik och standard för dubbelriktad TLS/Mutual TLS (mTLS). Webbläsaren utmanar användaren om att presentera ett giltigt klientcertifikat som servern litar på. Certifikaten importeras från SITHS-kortet till datorns operativsystem med hjälp av någon av klientprogramvarorna nedan. Integrationen sker alltså egentligen mot operativsystemet/webbläsaren snarare än mot klientprogramvaran.

Förutsätter att användaren har någon av klientprogramvarorna nedan och ett SITHS-kort:

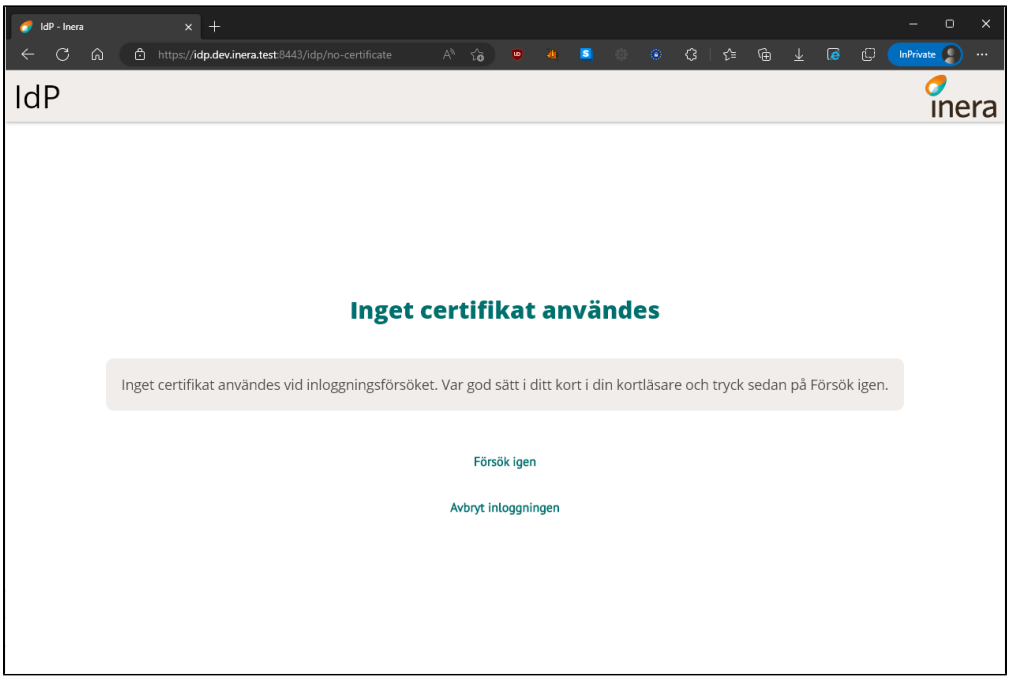
- SITHS eID-app för Windows **MD** (där SAC minidriver tekniskt sätt hanterar stödet för autentiseringsmetoden)
- Net iD Enterprise

7.2.1.1. Flera subdomäner ger användaren fler försök att välja certifikat

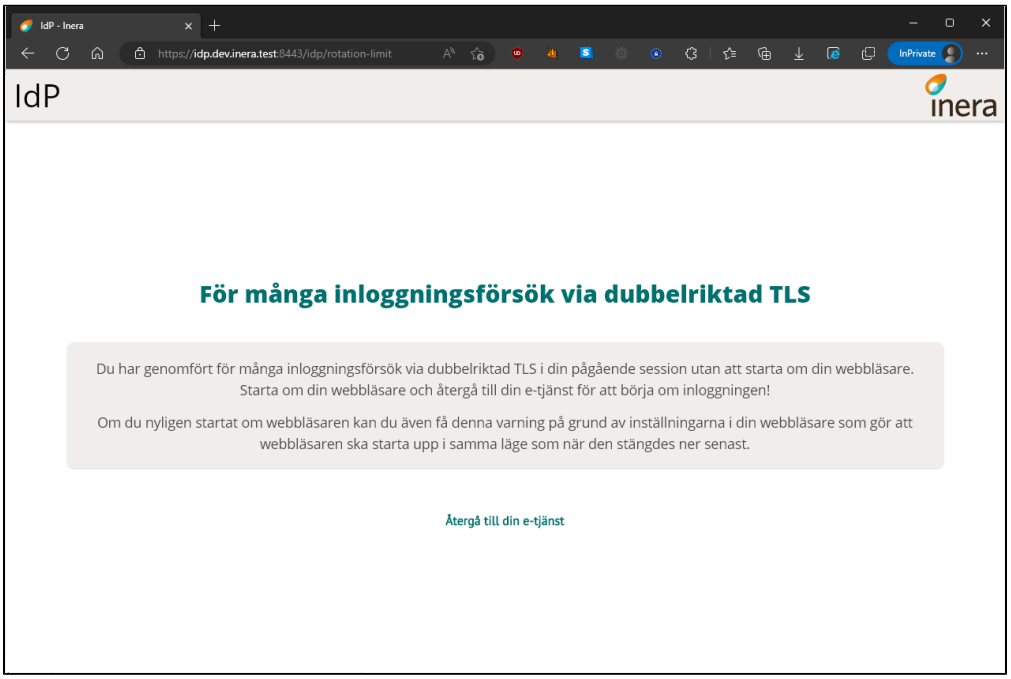
> **Denna funktion aktiveras först under Q3-2023**
>
> I väntan på att den aktiveras får användaren bara **ett försök** att välja sitt klientcertifikat per webbläsarsession. Om SITHS-kortet inte sitter i läsaren, är för fel miljö eller om importen av certifikaten till operativsystemet inte fungerar måste 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.

För att säkerställa att användaren måste välja ett certifikat när SITHS-kort på denna enhet används dirigerar IdP:n användaren om till olika subdomäner vid varje inloggningsförsök i den pågående webbläsarsessionen.

OM användaren inte valde något certifikat, t ex. inte hade sitt SITHS-kort i kortläsaren, visas denna dialog och användaren får ett nytt försök genom att välja **Försök igen.**



OM användaren har kommit till maxvärdet för antalet inloggningsförsök innan webbläsaren måste startas om *(i skrivande stund 25 försök för IdP som driftas av Inera)* visas denna dialog och användaren måste starta om webbläsaren för att starta om antalet försök.



OBS!

Logiken med att användaren alltid får **25 inloggningsförsök** är beroende av att användarens webbläsare **INTE** har inställningen för att öppna flikar från föregående session aktiverad *(se exempel nedan)*. Inställningen gör att räknaren i cookien för vilken endpoint/domännamn användaren ska hamna på inte nollställs korrekt. Användaren kommer således att fortsätta på det värde som webbläsaren senast hade och nollställas först när den når maxvärdet (25) och användaren då startar om webbläsaren. Rent praktiskt innebär det att användaren istället för 25st nya försök kommer ha färre försök på sig innan meddelandet ovan om *För många inloggningsförsök via dubbelriktad TLS* presenteras.

7.2.2. SITHS eID på denna/annan enhet - Out-of-band authentication (OOB)

Förutsätter att användaren har någon eller båda av:

- SITHS eID-app för Mobil och ett nedladdat Mobilt SITHS eller

- SITHS eID-app för Windows och ett SITHS-kort.

För detaljerad information kring de nya autentiseringsmetoderna och dess klientprogramvaror, dvs. apparna, fungerar se respektive Användarhandbok

- Användarhandbok - SITHS eID-app för Mobilt SITHS
- Användarhandbok - SITHS eID-app för Windows

7.3. Test av autentiseringsmetoder

På följande länkar kan samtliga autentiseringsmetoder testas för att försäkra sig om att autentisering mot IDP är möjlig

- PROD - https://test.idp.inera.se/
- TEST/QA - https://test.idp.ineratest.org/

8. Val av tjänste-id/medarbetaruppdrag

Under inloggningsflödet kan användaren bli presenterad med en vy där användaren behöver göra ett uppdragsval. Uppdragsvalet innebär att användaren specifikt måste välja med vilket tjänste-id och hos vilken vårdgivare/vårdenhet användaren avser att logga in hos. För att slutföra inloggningen måste ett val göras, annars misslyckas inloggningen.

Uppdragsvalet visas när den anslutande tjänsten (SP:n) begär attribut som endast kan uppfyllas av att ett tjänste-id och/eller uppdrag väljs, annars skippas det här steget helt. Se Attributlistan över vilka attribut som kan trigga uppdragsval.

Om uppdragsvalet presenteras för användaren så varierar de listade alternativen beroende på hur de enskilda användarna är konfigurerade i HSA samt vilken autentiseringsmetod som valts.

Autentiseringsmetodsvalet påverkar uppdragsvalet genom att:

- Inloggning med SITHS eID på denna/annan enhet föredrar personnummer-certifikat om ett sådant finns
    - En användares personnummer kan ha uppdrag kopplade till sig i HSA som inte också är kopplade på användarens HSA-id. Detta kan i sin tur resultera i att användaren får fler uppdragsval att välja mellan på för denna autentiseringsmetod.
- Inloggning med SITHS-kort på denna enhet alltid föredrar HSA-id-certifikat

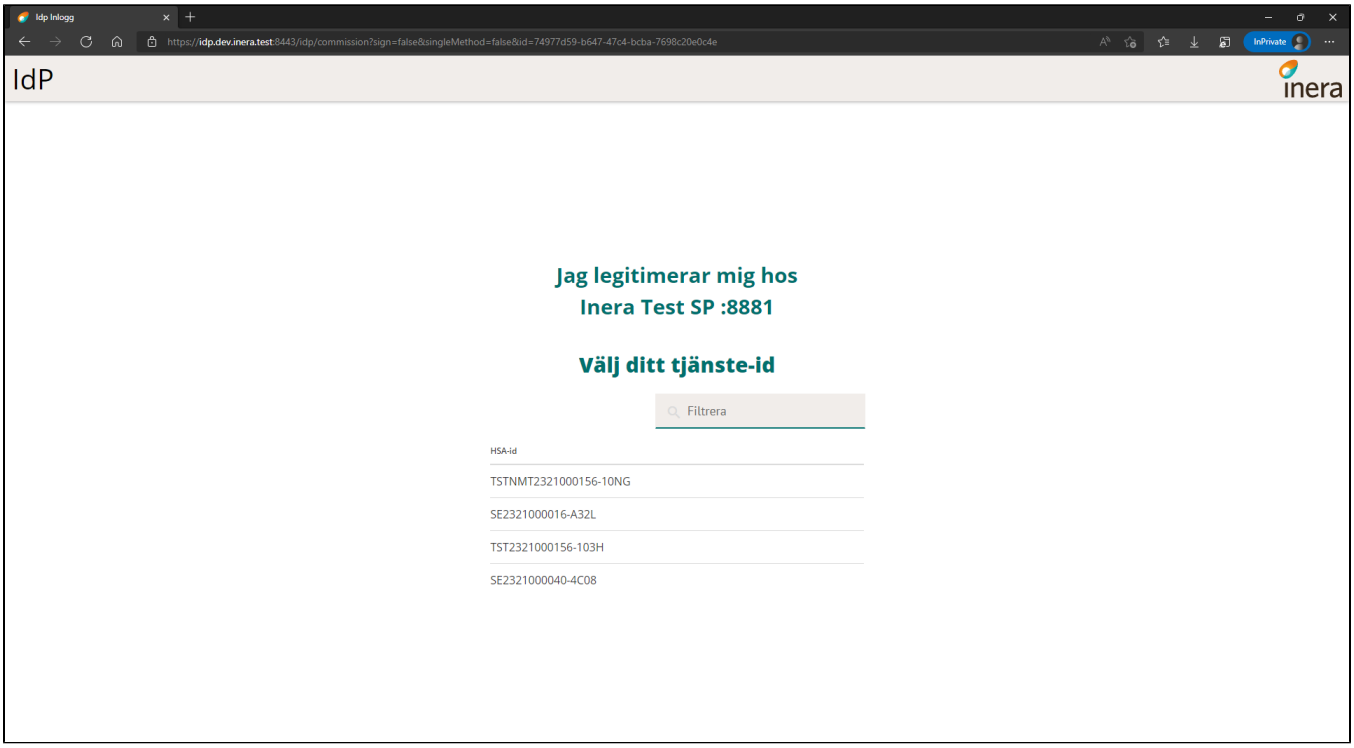
.När ett val behöver göras finns det ett flertal scenarion att förhålla sig till. Dessa finns specifierade här nedan.

8.1. Användaren har **ett** tjänste-id utan uppdrag

I detta fall kommer IdP:n automatiskt välja tjänste-id:t. I praktiken innebär det att användaren inte kommer bli presenterad med något val i webbläsaren.

8.2. Användaren har **flera** tjänste-id:n där **inget** tjänste-id har medarbetaruppdrag

I det här fallet har inget av användarens tjänste-id:n några uppdrag kopplade till sig. När detta inträffar får användaren en vy presenterad för sig där endast ett tjänste-id kan väljas.

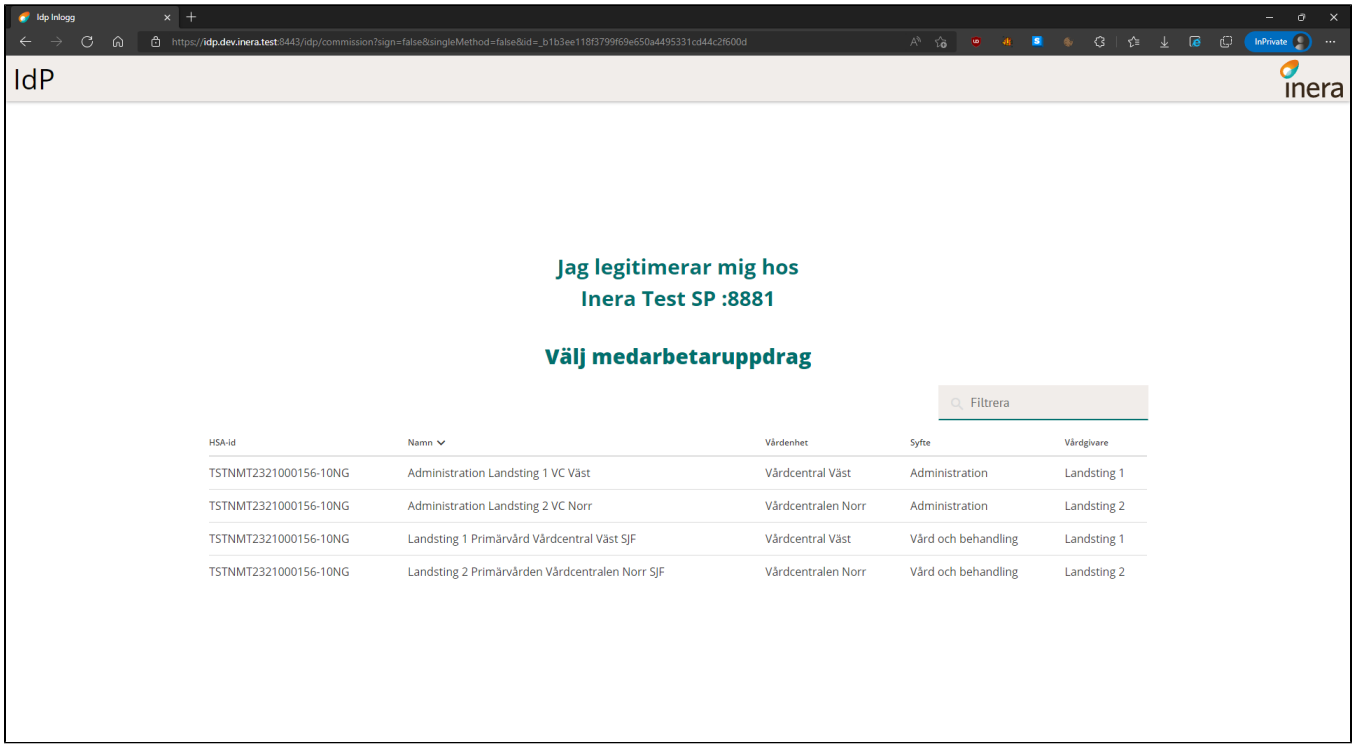


8.3. Användaren har **ett** tjänste-id med **ett** medarbetaruppdrag

När detta fall inträffar väljer IdP:n automatiskt tjänste-id:t och det tillhörande uppdraget. I praktiken innebär det att användaren inte kommer bli presenterad med något val i webbläsaren.

8.4. Användaren har **ett** tjänste-id med **flera** medarbetaruppdrag

I det här fallet kommer användaren få välja bland alla uppdrag som finns kopplade till användarens tjänste-id. Notera i bilden nedan hur HSA-id:t i kolumnen längst ut till höger är detsamma för alla uppdrag.



8.5. Förval av principalen

IdP stödjer förval av principalen (den inloggade användaren). Förvalet möjliggörs genom att tillåta SAML- och OIDC-anslutningar att skicka in värden som del av deras legitimerings- och signeringsbegäran. Dessa värden används sedan av IdP:n för att kunna göra ett val at tjänste-id och/eller medarbetaruppdraget utan användarinteraktion om möjligt. Alternativt om inte tillräckligt precisa värden skickats in kan IdP:n visa ett urval av valmöjligheter i tjänste-id- eller medarbetaruppdragsväljaren som på förhand har filtrerats med hjälp av de inskickade värdena.

Med denna mekanism har anslutande system möjlighet att på förhand välja vilket personnummer, tjänste-id, medarbetaruppdrag eller organisationsnummer användaren måste slutföra inloggningen med. Om något av de inskickade värden inte kan uppfyllas av användaren (antingen genom att fel kort använts eller uppgifter saknas i HSA) kommer inloggningen eller signeringen att misslyckas.

För respektive protokoll finns det väsentliga skillnader på hur dessa värden skickas in, samt vilka villkor som måste vara uppfyllda för att filtreringen och förvalet ska kunna genomföras. Läs mer om respektive implementation för OIDC och SAML här:

- Attributstyrning SAML
- Attributstyrning OIDC

9. Visningsnamn under legitimerings- och signeringsflödet

Under legitimerings- och signeringsflödet visar IdP:n ett namn på organisationen som användaren är på väg att logga in i eller utföra en signatur för. Samma namn visas också i SITHS eID-appen om en av SITHS eID autentiseringsmetoderna har valts.

Namnet som visas kan väljas själv av den anslutande organisationen och anges i förstudien. Gäller det en anslutning med SAML som protokoll ska namnet även finnas i SAML metadatat. Som del av förstudien ska både ett namn på systemet och ett namn på organisationen anges. I praktiken kommer dock endast namnet på organisationen visas för slutanvändaren.

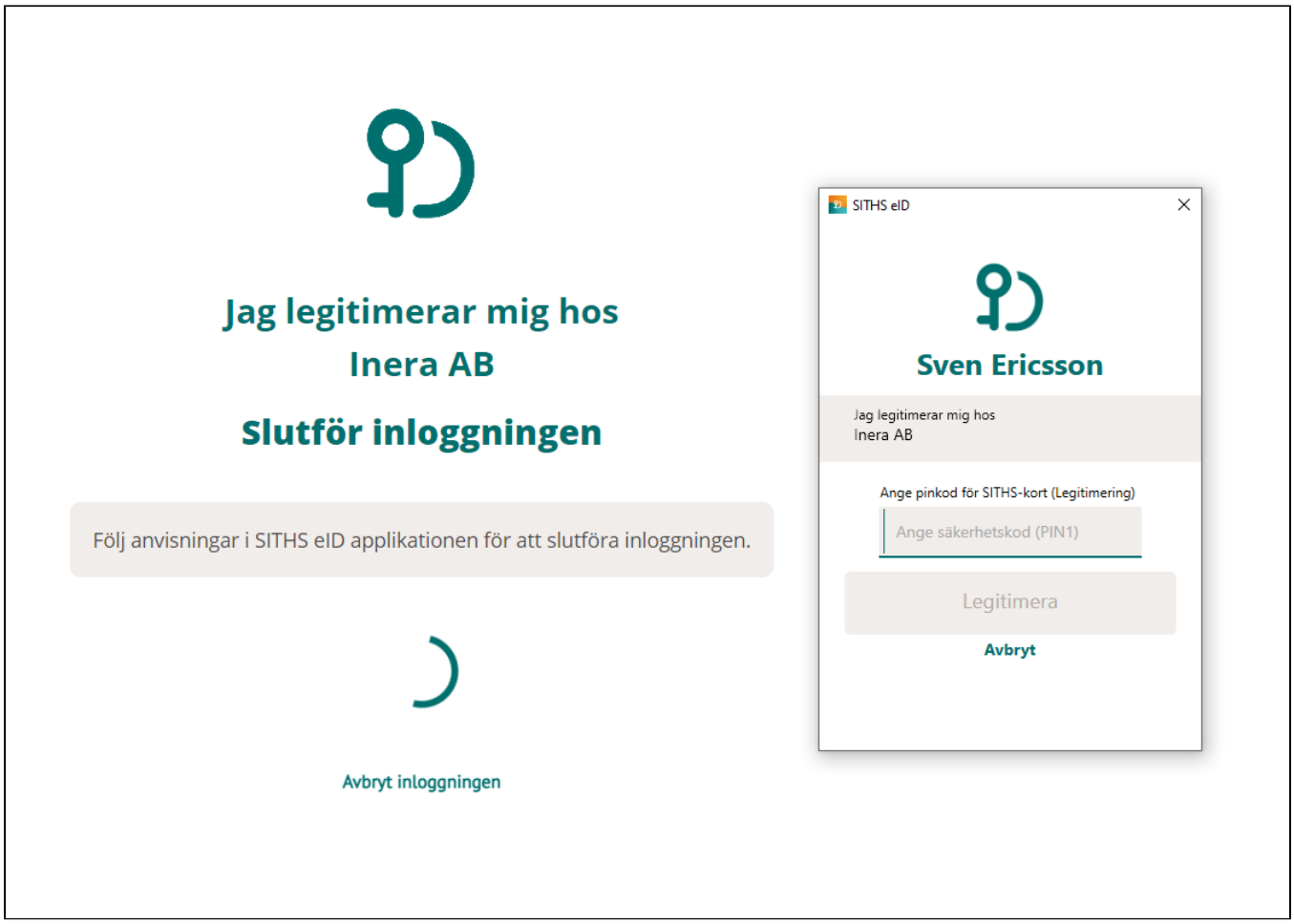
9.1. SAML

Vid anslutningsförfarandet hämtas organisationsnamnet som visas under legitimerings- och signeringsflödet från SAML metadatat. IdP:n letar efter ett OrganizationDisplayName under Organization-taggen (se SAML-Profil för konkreta exempel). Namnet som finns angetts under OrganizationDisplayName ska matcha med det som angetts i förstudien under Organisationens visningsnamn. Systemets visningsnamn ska inte vara definierat i SAML metadatat utom ska endast återfinnas i förstudien.

9.2. OIDC

Vid anslutningsförfarandet anges organisationens och systemets visningsnamn endast i förstudien. Dessa värden läses sedan in manuellt till IdP:n.

OBS! Vid uppgraderingen till IdP 2.3 är visningsnamnet för OIDC-anslutningarna initialt systemets visningsnamn. IdP saknar information kring vilken den anslutande organisationen är i tidigare versioner av IdP:n och kommer behöva kompletteras allt eftersom.



10. IdP SSO-sessionens giltighetstid

Efter slutanvändarna har lyckats med sin inloggning tilldelar IdP:n deras SSO-session en fast giltighetstid på 60 minuter oavsett om användaren under giltighetstiden har gjort en HTTP-slagning där giltighetstiden kontrolleras eller inte. Det exakta värdet för giltighetstiden kan komma att ändras i framtiden då detta konfigureras på IdP:ns sida.

Exempel: Användaren är inloggad i System A sen 59 minuter tillbaka och väljer att öppna System B i webbläsaren. Användaren blir inloggad i System B men SSO-sessionens giltighetstid utökas inte. När användaren öppnar System C i webbläsaren efter 61 minuter kommer användaren behöva logga in igen. När användaren väljer att logga ut eller stänger ner webbläsaren försvinner SSO-sessionen.

10.1. Cachning av PIN-kod (PIN-cache, PIN-SSO)

Cachning av pin-koden har historiskt också kallats för/använts som SSO. Detta är dock en form av SSO som hanteras nere på operativsystemet tillsammans med den mjukvara som används dom drivrutin för att läsa SITHS-kortet. Dvs Net iD Enterprise eller SITHS eID-appen för Windows **MD** (med SAC minidriver).

Därav kan användarupplevelsen variera beroende på hur appen är konfigurerad lokalt. Som standard är PIN-SSO aktiverad, vilket medför att användare vid en ny inloggning inte alltid behöver slå in PIN-koden efter att de valt sitt certifikat. Även om IdP:ns SSO-session har avslutats.

OM organisationen valt att inaktivera eller ställa in en kort tid för PIN-SSO kan användaren behöva uppge sin pin-kod vid varje inloggning.

PIN-SSO avslutas annars som regel när:

- Användaren avlägsnar sitt kort från kortläsaren eller
- Datorn startas om
- Timeout för PIN-SSO inträffar

10.2. Utloggning

För att fullständigt logga ut från en e-tjänst behöver följande ske

1. Användaren använder tjänstens egen funktion för utloggning
2. Att tjänsten vidareförmedlar utloggningsbegäran till IdP för att avsluta IdP-SSO
3. Användaren avlägsnar SITHS-kortet från kortläsaren för att avsluta PIN-SSO
4. Tjänsten bör komplettera med en egen inaktivitetstimeout för att avsluta applikations-sessioner från inaktiva användare

    a. Denna hjälper dock inte om användare glömmer att avlägsna sitt SITHS-kort.

11. Kompatibilitetsinformation

För att få tillgång till rättningar krävs att supporterad hårdvara och mjukvara enligt listorna nedan används.

11.1. IdP

Ineras IdP följer vedertagna standards för utfärdande av identitetsintyg (SAMLv2/OIDC). Användning av dessa standards medför att IdP fungerar på merparten av alla operativsystem och webbläsare. De e-legitimationer som stöds av Ineras IdP (SITHS) är dock beroende av Klientprogramvaror som har kompatibilitetskrav för den plattform och hårdvara de installeras och används på.

11.1.1. Windows - Operativsystemsversioner

Tester sker primärt utifrån kraven i eKlients kravbibliotek gällande vilka versioner av Windows som ska stödjas. När Microsoft släpper en ny release är målet att ha testat stödet för denna inom 6 månader.

OBS! Vi supporterar endast de versioner av Windows som Microsoft själva supporterar. Nedan följer länkar till Microsofts livscykelplaner för Windows:

- Windows 11 Home och Pro Lifecycle
- Windows 11 Enterprise och Education
- Windows 10 Home och Pro Lifecycle
- Windows 10 Enterprise och Education Lifecycle

Operativsystem (endast 64-bitar)	Autentiseringsmetod	
	SITHS eID på denna/annan enhet (out-of-band)	SITHS-kort på denna enhet (mTLS)
Windows 11 upp till 22H2	X	X
Windows 10 upp till 22H2	X	X

11.1.2. Windows - Webbläsare

Följande webbläsare supporteras så länge den version som används också supporteras av tillverkaren av respektive webbläsare:

- Chrome
- Edge
- Inbäddad Internet Explorer 11 och Internet Explorer 11-läge i Microsoft Edge **(EOL)**
- Firefox

Stödet för Internet Explorer 11 är under avveckling.

Stödet blir allt svårare att vidmakthålla och risken för upptäckt av allvarliga säkerhetsbrister gör att vi kan behöva avveckla stödet med kort varsel.

Microsoft slutade supportera fristående Internet Explorer 11 i maj 2022.

Uthoppslösningar

Kompatibilitet för e-tjänster med s k uthoppslösningar kan behöva verifiera att inställningar för "Trusted Zones" på den tekniska stödsidan IdP med Edge och IE 11 och Trusted sites.

Inbäddade webbläsare

Inbäddade webbläsare samt ev. andra webbläsare kan behöva anpassningar för att stödja anpassade browser-scheman som används för att autostarta appen. För SITHS eID-appen används **siths://**.

Se mer information här: SITHS eID Appväxling - Exempel för inbäddade webbläsare

11.2. Klientprogramvaror

11.2.1. SITHS eID-app för Windows

Laddas ner via **Ladda ner SITHS eID-app för Windows**

2.0.8481 Användarhandbok - SITHS eID-app för Windows

Under detta avsnitt listas:

- supporterade versioner SITHS eID-appen för Windows
- samt versioner för den plattform och hårdvara på vilken appen ska fungera.

För att få tillgång till rättningar krävs att supporterad hårdvara och mjukvara enligt listorna nedan används.

11.2.2. Versioner av SITHS eID-appen för Windows

Inera supporterar den:

- senaste versionen av SITHS eID-appen för Windows
- näst senaste versionen av SITHS eID-appen för Windows i **6 månader efter release av en nyare version**

Vid felanmälan kan Inera komma att kräva att felet återskapas i någon av följande versioner:

Version av SITHS eID-appen	Utgivningsdatum	Sista datum för support
2..0.8481	04 Apr 2023	Ej planerat
2.0.8325	04 Oct 2022	4 oktober 2023

11.2.3. Hårdvara

11.2.3.1. SITHS-kort

Följande SITHS-kort supporteras:

Kortnamn	Produktnummer
IDClassic 410	4XX 9XX
IDPrime SIS 840	5XX
IDPrime 940 SIS	6XX 7XX

11.2.3.2. Kortläsare

Vi rekommenderar att ni alltid använder senaste drivrutinerna från tillverkaren av respektive kortläsare.

För att använda appen tillsammans med SITHS eID på kort krävs en smartkortläsare. Merparten av alla kortläsare på marknaden och som som **endast** ansluts till en dator åt gången bör fungera. Nedan återfinns en lista över smartkortläsare som supporteras.

11.2.3.2.1. Kortläsare som läser kortet chip

- Gemalto IDBridge K30
- Gemalto IDBridge K50
- Gemalto IDBridge CT30
- Gemalto IDBridge CT40
- OMNIKEY 5422
- OMNIKEY Cardman 5422
- OMNIKEY 3121
- IDBridge CL3000 (EOS)

11.2.3.2.2. Kortläsare som läser kortets chip och har extern pin-pad

- Gemalto IDBridge CT700

För kortläsare med extern pin-pad fungerar inmatning av pin-kod på den externa pin-paden endast:

- för autentiseringslösningar baserade på mTLS-teknik. Dvs. med SITHS eID-app för Windows **MD** (SAC minidriver)
- för SITHS 940-kort (dvs. kortprodukterna 6XX, 7XX)
  - 410- och 840-kort stöds **INTE** i dagsläget

11.2.4. Mjukvara

11.2.4.1. Operativsystem

Vi ämnar följa rekommendationerna i eKlients kravbibliotek gällande vilka versioner av Windows som ska stödjas. När Microsoft släpper en ny release är målet att ha testat stödet för denna inom 6 månader.

OBS! Vi supporterar endast de versioner av Windows som Microsoft själva supporterar. Nedan följer länkar till Microsofts livscykelplaner för Windows:

- Windows 11 Home och Pro Lifecycle
- Windows 11 Enterprise och Education
- Windows 10 Home och Pro Lifecycle
- Windows 10 Enterprise och Education Lifecycle

Autentiseringslösning: Applikation	**Out-of-band: SITHS eID-appen**	**Dubbelriktad TLS (mTLS): SAC minidriver som installeras via paketen för SITHS eID-app för Windows MD**
Operativsystem (endast 64-bitar)		
Klient		
Windows 11 upp till 22H2	X	X
Windows 10 upp till 22H2	X	X*
Server		
Windows Server 2022		X
Windows Server 2019		X
Windows Server 2016		X
Windows Server 2012 och 2012R2		X**

** - SAC minidriver släpptes innan Windows releasen tillgängliggjordes. Support ges, men ev. behov av rättningar som beror på version av Windows kommer först släppas i en senare version av SAC*

*** - SAC supporteras på Windows Server 2012 and 2012R2 enligt Thales release notes, men då det saknas en certifiering för SITHS äldre kortprodukter fungerar inte installationen så som den ser ut inom SITHS eID-app för Windows utan användare accepterar insallation av ej signerade drivrutiner. Detta påverkar möjligheten att installera SITHS eID-app för Windows i MD-paketering på Windows Server 2012 och 2012R2 som tyst installation.*

11.2.4.2. Webbläsare

Följande webbläsare supporteras så länge den version som används också supporteras av tillverkaren av respektive webbläsare:

- Chrome
- Edge
- Firefox

Inbäddade webbläsare samt ev. andra webbläsare kan behöva anpassningar för att stödja anpassade browser-scheman som används för att autostarta appen. För SITHS eID-appen används **siths://**.

Se mer information här: SITHS eID Appväxling - Exempel för inbäddade webbläsare

11.2.5. SITHS eID-app för Mobila enheter

Laddas ner via App Store eller Google Play.

För att hämta Mobilt SITHS kan du antingen använda ett befintligt Mobilt SITHS eller så måste du använda SITHS eID-app för Windows, läs mer på SITHS eID-app för Windows.

2.2.5 Användarhandbok - SITHS eID-app för Mobilt SITHS

Under detta avsnitt listas:

- supporterade versioner SITHS eID-appen för mobila enheter
- samt versioner för den plattform och hårdvara på vilken appen ska fungera.

För att få tillgång till rättningar krävs att supporterad hårdvara och mjukvara enligt listorna nedan används. Om det hittas enheter som ej fungerar trots att de täcks av rubriken **Hårdvara och operativsystem för mobila enheter** förbehåller sig Inera komplettera listan med Ej kompatibla enheter.

11.2.6. Versioner av SITHS eID-appen för mobila enheter

Inera supporterar den **senaste** versionen av SITHS eID-appen för mobila enheter

Vid felanmälan kan Inera komma att kräva att felet återskapas i någon av följande versioner:

Appversion	Operativsystem	Utgivningsdatum	Sista datum för support
2.2.5	Android	2022-08-31	Ej planerat
2.2.5	iOS	2022-08-31	Ej planerat

11.2.7. Hårdvara och operativsystem för mobila enheter

Appen fungerar endast på vissa kombinationer av hårdvara och mobila operativsystem.

11.2.7.1. Apple

Lägsta hårdvarukrav	Lägsta supporterade hårdvara	Lägsta OS-version	Lägsta supporterade OS-version	Webbläsare
Enheten behöver ha Secure Enclave hårdvarukryptering Modeller: • iPhone 6s eller senare • iPad mini gen5 (A2133) • iPad gen5 (A1823)	Samma som lägsta hårdvarukrav	iOS 12	iOS 12	Safari rekommenderas för bästa användarupplevelse, men även andra webbläsare ska fungera

11.2.7.2. Apple - Biometri

Lägsta hårdvarukrav	Lägsta supporterade hårdvara	Lägsta supporterade OS-version	Högsta supporterade OS-version	Biometri som stöds
Enheten ska stödja skapande av en asymmetrisk kryptonyckel i enhetens säkra hårdvaruutrymme (Secure Enclave) med krav på biometrisk autentisering för dess användande. Modeller: • iPhone 6s eller senare • iPad mini gen5 (A2133) • iPad gen5 (A1823)	Samma som lägsta hårdvarukrav	iOS 12	Ingen högsta version definierad	Face ID eller Touch ID beroende på vad som finns tillgängligt på enheten.

11.2.7.3. Android

Lägsta hårdvarukrav	Lägsta supporterade hårdvara	Lägsta OS-version	Lägsta supporterade OS-version	Högsta supporterade OS-version	Webbläsare
Enheten behöver ha CPU (Qualcomm) med Trust Zone (motsvarar TPM) Keystore Trusted Execution Environment (TEE)	Enheten behöver finnas med på någon av följande listor • Google Enterprise Recommended ◦ Sök efter enheter som är kompatibla • Samsung Enterprise Edition	Android 7.1.1	Android 9	Android 11 **From. 1 november 2023 går denna version av appen inte längre gå att installera på nyare versioner än Android 11.** **OBS! Redan existerande installationer av appen påverkas inte.**	Vi rekommenderar användning av enhetens standardwebbläsare för bäst användarupplevelse, men även andra webbläsare ska fungera.

11.2.7.4. Android - Biometri

Lägsta hårdvarukrav	Lägsta supporterade hårdvara	Lägsta supporterade OS-version	Högsta supporterade OS-version	Biometri som stöds
Vid aktivering av biometri skapas en asymmetrisk kryptonyckel i enhetens säkra hårdvaruutrymme (TEE) med krav på biometrisk autentisering uppfyllande “Class 3” (tidigare benämnd “Strong”)	Samma som lägsta hårdvarukrav	Android 9 (API-nivå 28)	Android 10 (API-nivå 29)	Endast fingeravtrycksläsare
		Android 11 (API-nivå 30)	Ingen högsta version definierad	Alla biometriska läsare som uppfyller "Class 3" enligt Androids API för kontroll av biometrisk hårdvara.

11.2.7.5. Ej kompatibla enheter

Lista över enheter som inte fungerar trots att de matchar ovan plattformskrav

Operativsystem	Enhetsmodell (Tillverkare - modellnamn)	OS-version
Inga kända för närvarande		

11.2.7.6. Ej kompatibla enheter - Biometri

Operativsystem	Enhetsmodell (Tillverkare - modellnamn)	OS-version
Inga kända för närvarande		

11.2.8. Webbläsare

Beroende på om inloggningen sker på den mobila enheten eller om Mobilt SITHS används för att logga in i en applikation på en dator finns olika förutsättningar.

För inloggning med Mobilt SITHS på en dator fungerar de flesta förekommande webbläsare som också supporteras av respektive operativsystem

För inloggning med Mobilt SITHS på den mobila enheten gäller att webbläsaren som används ska vara markerad som **standardwebbläsare** OCH att webbläsaren också supporteras av tillverkaren av respektive webbläsare.

Följande webbläsare supporteras på **Android**

- Chrome
- Edge
- Samsung Internet

Följande webbläsare supporteras på **iOS**

- Chrome
- Safari

> Inbäddade webbläsare samt ev. andra webbläsare kan behöva anpassningar för att stödja anpassade browser-scheman som används för att autostarta appen. För SITHS eID-appen används **siths://**.
>
> Se mer information här: SITHS eID Appväxling - Exempel för inbäddade webbläsare

11.2.9. Net iD Enterprise

Information om kompatibilitet och support för Net iD Enterprise finns på sidan Programvaror och tillbehör för SITHS.