2.3 Anslutningsguide till IdP

Version	Datum	Författare	Kommentar
1.0	18 Sep 2022	Christoffer Johansson	Godkänd av förvaltning

Reservkort och LoA-nivåer

Från och med 18 Jan 2021 rapporteras Ineras IdP:er LoA 2 för reservkort istället för LoA 3. Detta kan kräva anpassning av SP.

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.

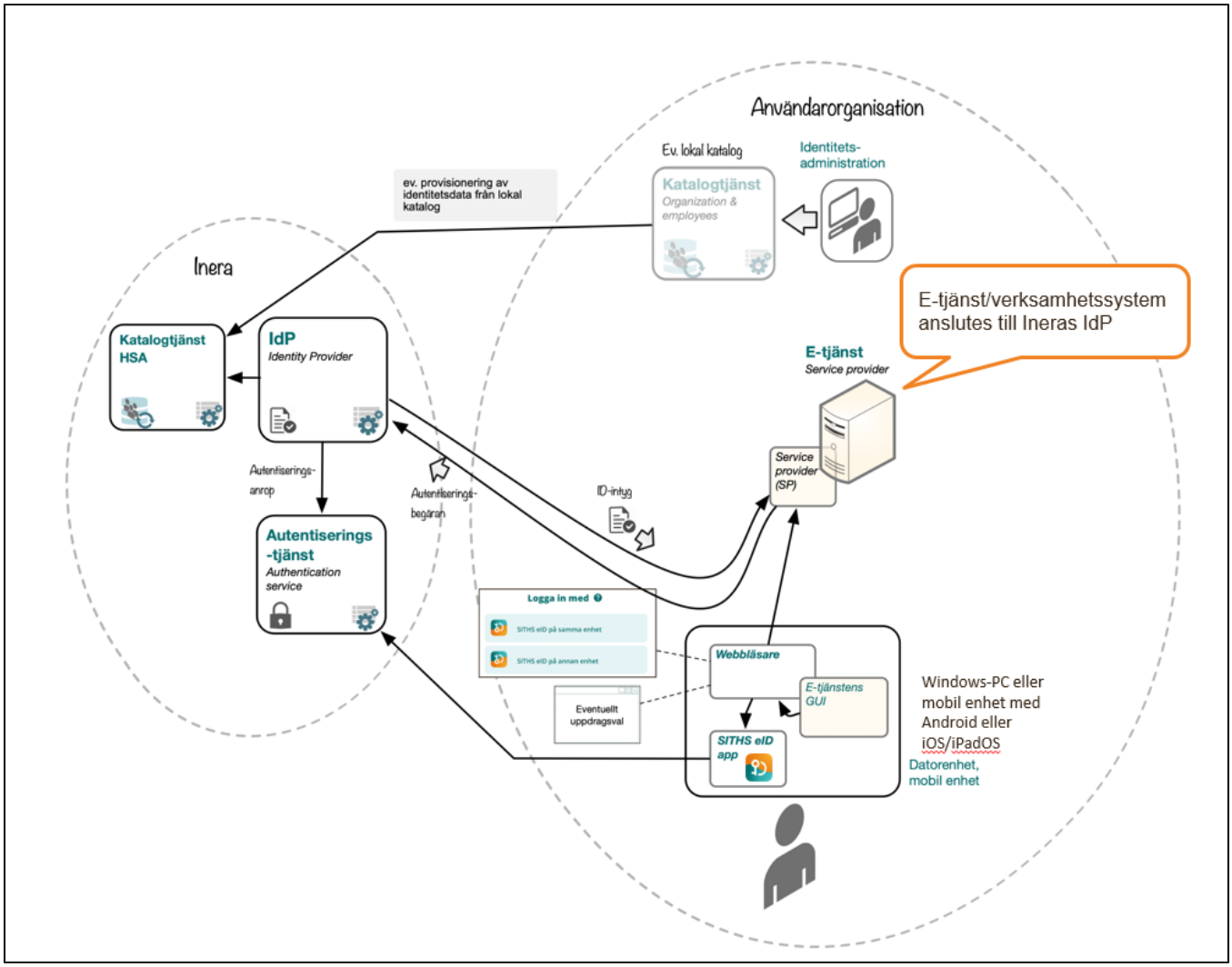
Vid en lyckad autentisering utfärdas ett identitetsintyg, (SAML-biljett, eller Id-token för OIDC) som innehåller information om autentiseringen samt eventuellt ytterligare användarattribut, som kan användas av ett ABAC (Attribute Based Access Control) behörighetssystem, d.v.s. behörighet på egenskapsnivå.

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 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 måste metadata valideras med Sambi Metadata validator. 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 sker tillsammans med förstudie som skickas in när e-tjänsten ska registreras väljs vilket sätt som ska användas. De två möjligheterna 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.

1.1.1.3. Metdata fil exempel

- SP Metadata exempel

> Observera att attributet för personnummer http://sambi.se/attributes/1/personalIdentityNumber ger ett kataloguppslag. urn:credential: personalIdentityNumber hämtas från e-legitimationen. Normalt är att e-tjänsten väljer ett av attributen, inte bägge och att metadata följaktligen innehåller ett av attributen.

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 IAM-tjänster 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. Slutanvändarklienter

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

1.1.6. Testkort

För tillgång till SITHS eID på kort för test, vänd er till www.inera.se/siths.

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.

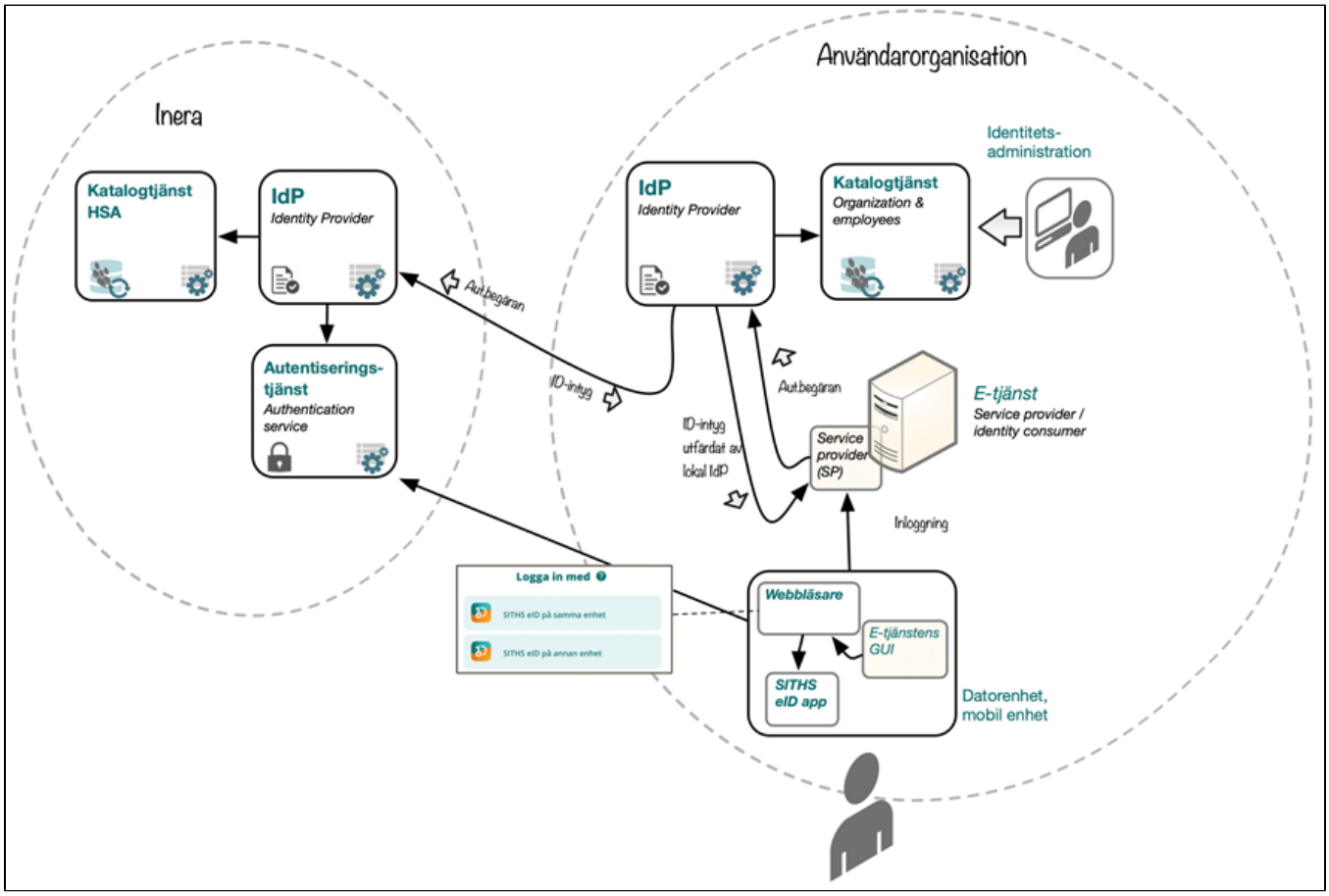
Inera IdP:

- 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

Observera att attributet för personnummer http://sambi.se/attributes/1/personalIdentityNumber ger ett kataloguppslag. Därför rekommenderar vi att använda urn:credential:personalIdentityNumber, attributet hämtas från e-legitimationen.

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 undvika 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 IAM-tjänster 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.

Miljö	**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

I dagsläget har alla anslutna tjänster endast en autentiseringsmetod tillgänglig, SITHS eID på denna enhet - via dubbelriktad TLS.

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

Tillgängliga metoder:

- SITHS eID på **annan** enhet - via SITHS eID-appen
- SITHS eID på **denna** enhet - via SITHS eID-appen
- 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, det kommer dock inte att fungera. Om man vill försäkra sig om att det inte händer bör man definiera en egen SP-ingång som uteslutande visar SITHS eID-metoderna, dvs out-of-band.

Aktivering av ny autentiseringsmetod som använder SITHS eID-klienterna 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

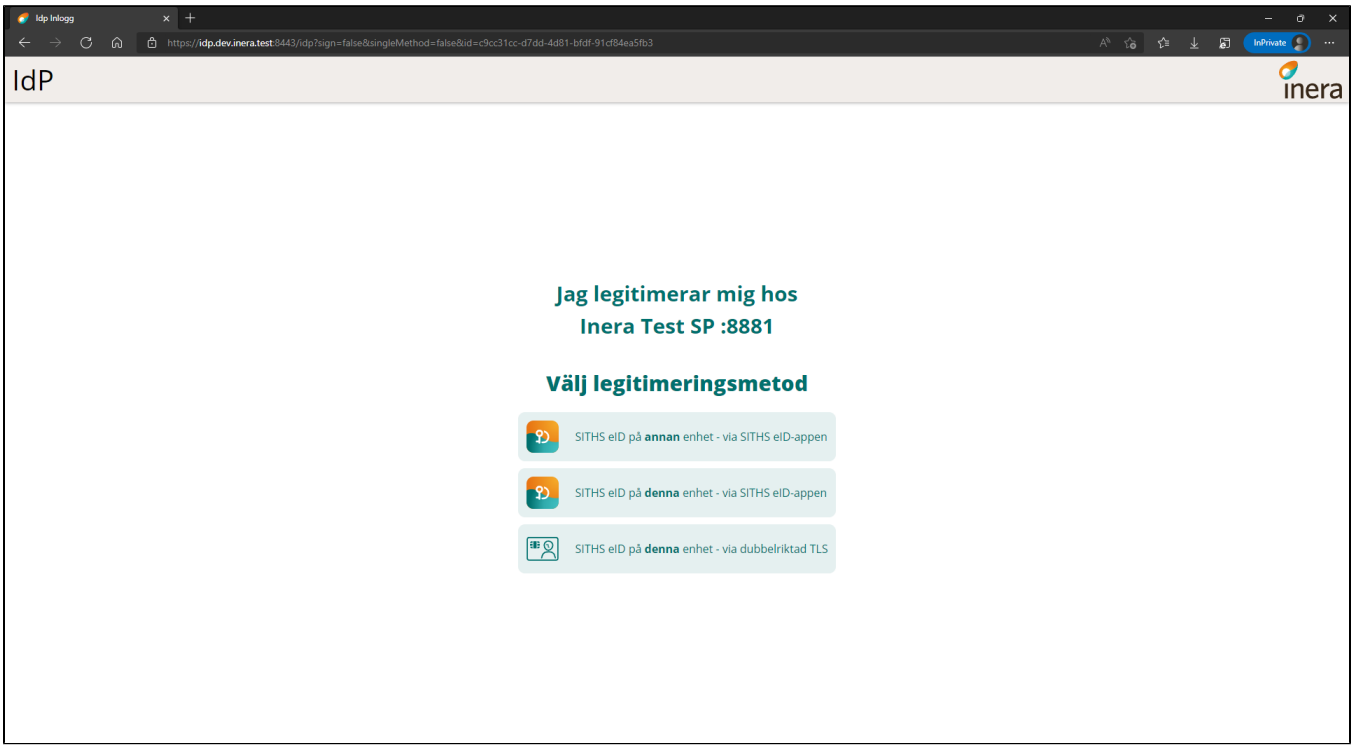
1. ordna med brandväggsöppningar mot Autentiseringstjänsten (Nätverksinställningar för IAM-tjänster),
2. säkerställa att slutanvändarna använder en webbläsare (för att anropa IdP) på ett sätt som möjliggör för autostart av SITHS eID-klienten (se även nedan samt SITHS eID Appväxling - Exempel för inbäddade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

För mer detaljerad information om de nya autentiseringsmetoderna och vilka krav som ställs på anslutande organisationer, se Anslutningsguide till Autentiseringstjänsten.

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 klient 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 eID på denna enhet - via dubbelriktad TLS kommer alltid föredra HSA-id-certifikat medans SITHS eID på denna/annan enhet - via SITHS eID-appen föredrar ett personnummer-certifikat om ett sådant finns. Beroende på vilka uppdrag som har kopplats i HSA för personnumret och HSA-id:t respektive kan SITHS eID på denna/annan enhet - via SITHS eID-appen resultera i att användaren får fler valbara alternativ i tjänste-id- och uppdragsvalet.



7.3. Nya autentiseringsmetoder

För detaljerad information kring de nya autentiseringsmetoderna och hur de fungerar i klienterna, se respektive användarhandbok

- Användarhandbok - SITHS eID Mobilklient
- Användarhandbok - SITHS eID Windowsklient

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 - via SITHS eID föredrar personnummer-certifikat om ett sådant finns medans inloggning med SITHS eID på denna enhet - via dubbelriktad TLS alltid föredrar HSA-id-certifkat. 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 när SITHS eID på denna/annan enhet - via SITHS eID-appen används istället för SITHS eID på denna enhet - via dubbelriktad TLS.

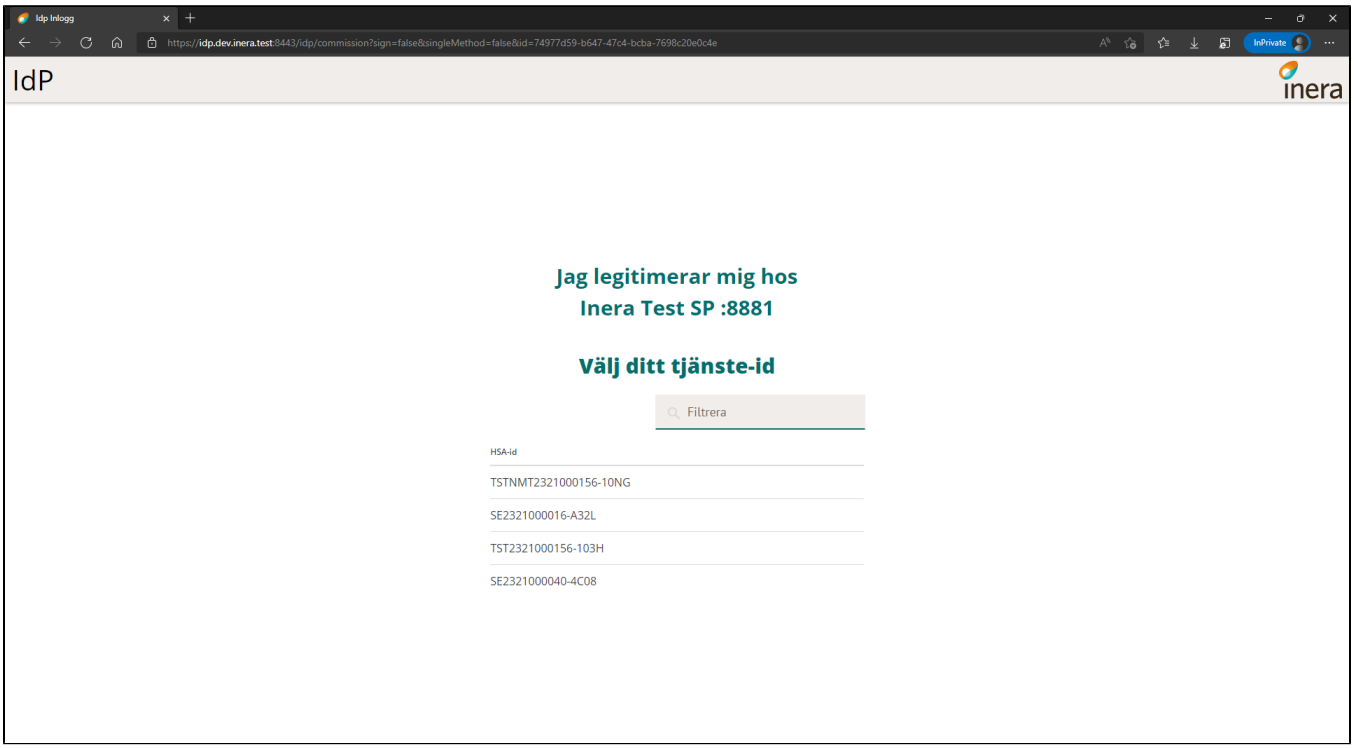
När ett val behöver göras finns det ett flertal scenarion att förhålla sig till. Dessa finns specifierade här nedan.

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.

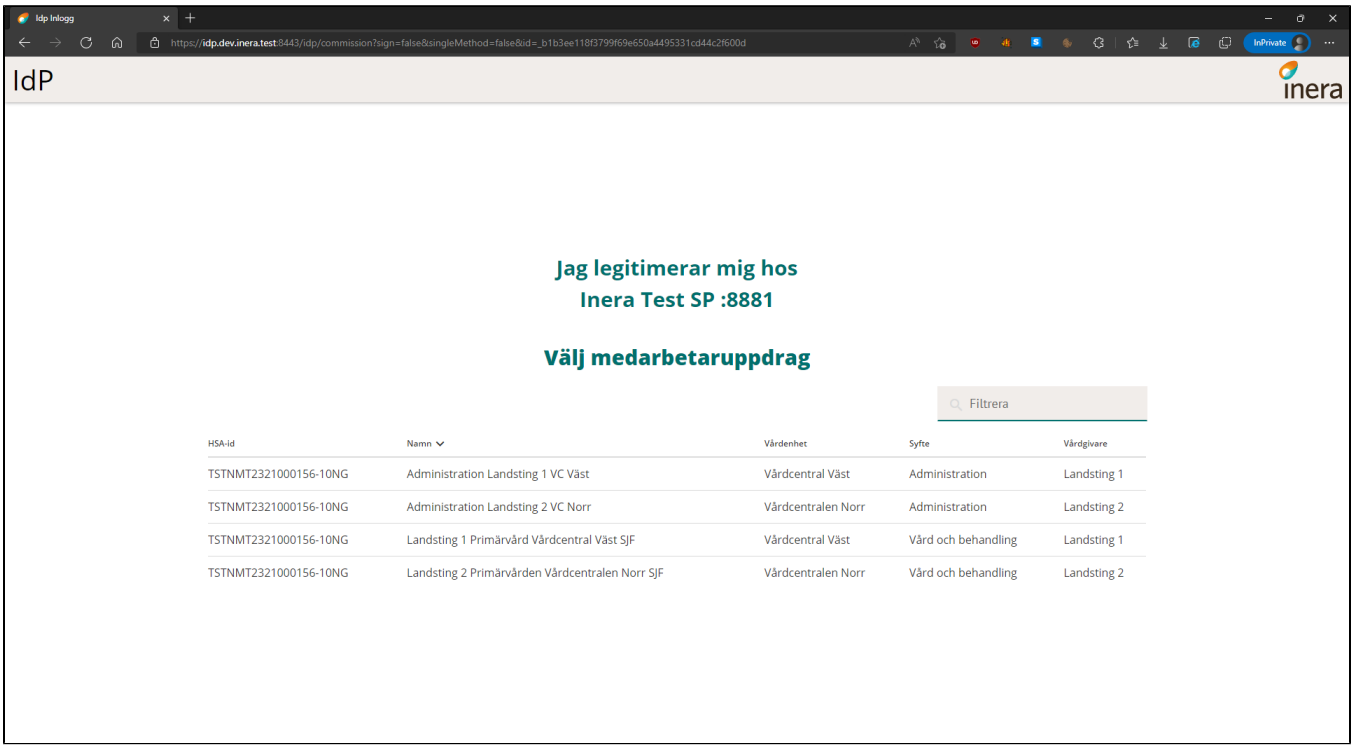


8.3. Användaren har ett tjänste-id med ett medarbetaruppdrag

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.

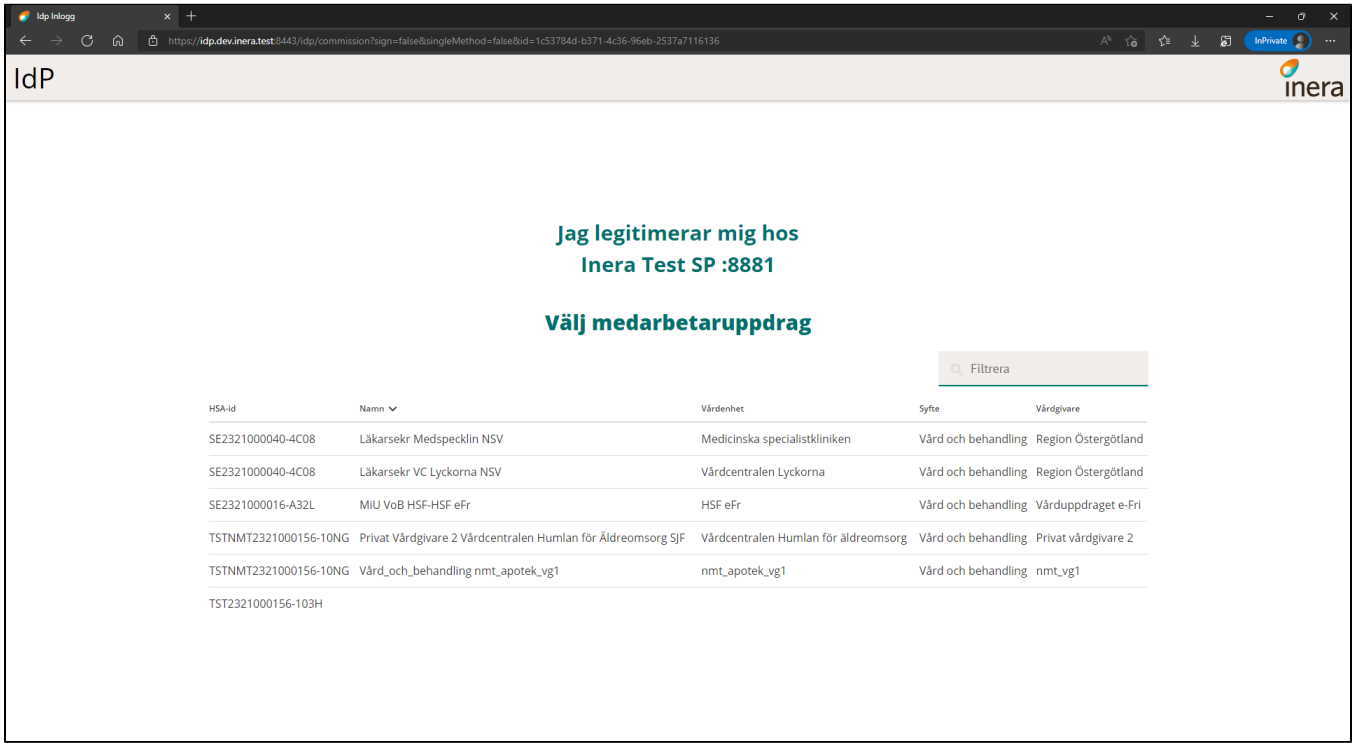
8.4. Användaren har ett tjänste-id med flera medarbetaruppdrag

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. Användaren har flera tjänste-id:n med flera medarbetaruppdrag

I detta fall kan användaren välja både mellan uppdrag och enskilda tjänsteid:n. Notera i bilden nedan hur det finns fyra olika tjänste-id:n att välja mellan där tjänste-id:n ...**-10NG** och ...**-10NX** har uppdrag medans ...**-10NY** och ...**-10NZ** saknar uppdrag.



8.6. Filtrering av personnummer, HSA-id och organisationsnummer

IdP:n stödjer filtrering av attributen personalIdentityNumber, employeeHsaId samt organisationIdentifier. Denna funktionalitet är baseras på PrincipalSelection som främst nyttjas för signerings-syften för SAML. För IdP:n har funktionaliteten utökats att även stödja filtrering av dessa attribut för autentisering både för SAML och OIDC.

Med denna filtrering har anslutande system möjlighet att förhandsvälja exempelvis en användares HSA-id om denne har flera HSA-id:n att välja mellan så att valet av tjänste-id hoppas över. Liknande filtrering kan göras genom att ange filtrera ut ett specifikt organisationsnummer om en användare arbetar mot flera olika organisationer. Filtrering av personnummer är endast användbart för signering. Observera att idag stödjs endast dessa tre attribut för att göra filtreringar.

8.6.1. SAML

För att kunna tillämpa denna filtrering med SAML används PrincipalSelection. Se dokumentationen hos DIGG över hur PrincipalSelection fungerar och hur det används. Mer läsvärd information hittas under artikeln för Attributstyrning SAML.

8.6.2. OIDC

När denna filtrering ska användas för OIDC görs det genom att ange de önskade värden i de claims som den anslutande tjänsten begär från IdP:n. Hur detta funkar i praktiken går att se under artikeln för 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 klienterna för Windows, Android och iOS 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.

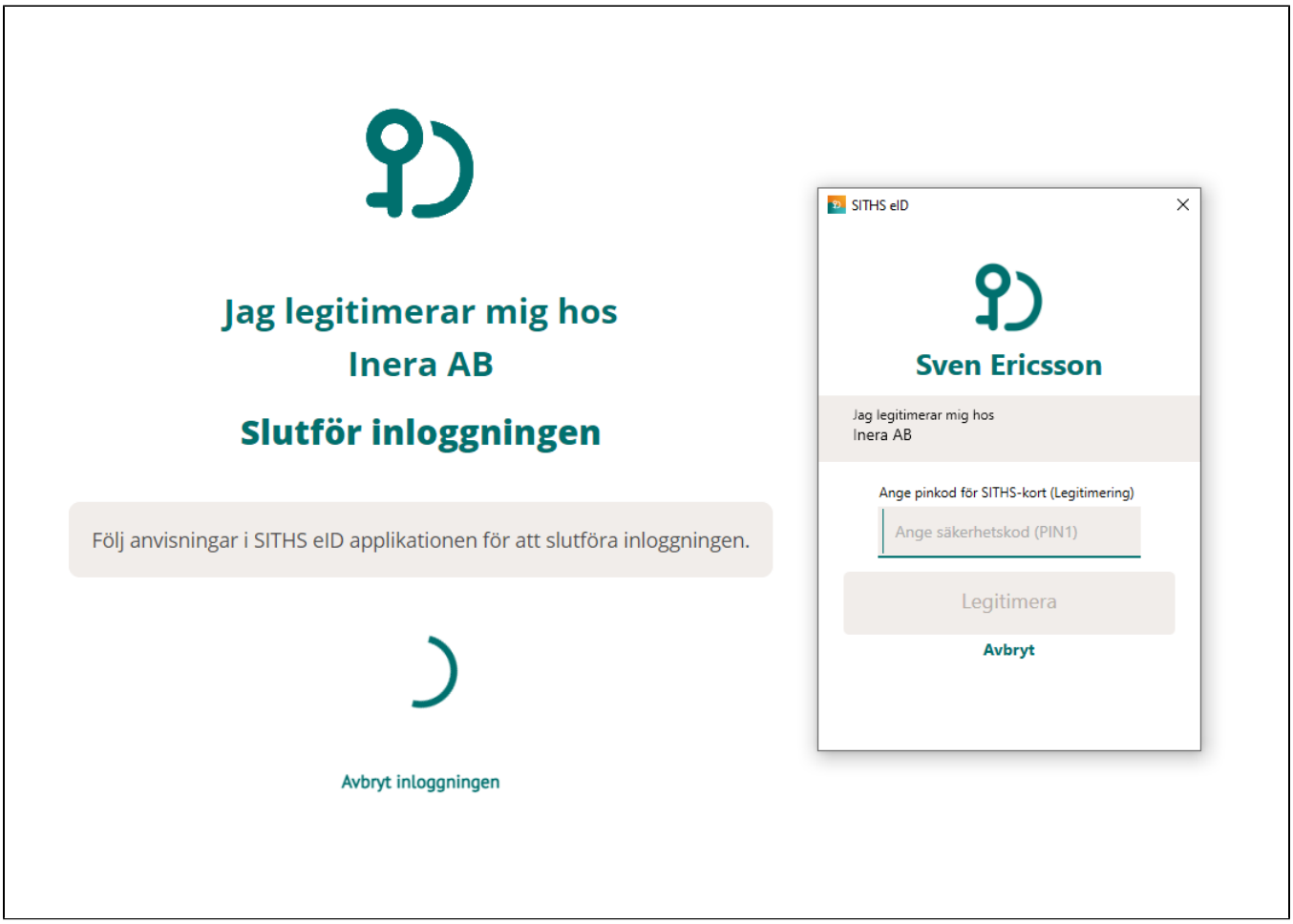
9.1. SAML

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 sakner information kring vilken den anslutande organisationen är i tidigare versioner av IdP:n och kommer behöva kompletteras allt eftersom.



10. 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.

11. Användarklienter

11.1. SITHS eID-klienter

Mobilklienterna laddas ner via App Store eller Google Play. Windowsklienten tillgängliggörs under SITHS eID-app för Windows och organisationer kan välja att distribuera den själva eller att dela länken med sina användare.

Se nedan för länkar till specifik information kring respektive applikation.

Windowsklienten

Mobilklienterna

11.2. Net iD Enterprise (inloggning via dubbelriktad TLS)

Övergripande information kring Net iD-klienten finns också på Ineras SITHS confluence space.

Tabellen nedan visar på verifierade kombinationer av komponenter.

Operativsystem	Webbläsare				Net iD Enterprise
Windows 7+8	Chrome	Internet Explorer 11	Edge Chromium		✓ 6.8.0.22 SITHS 1301, 1311 ✓ 6.8.1.31 SITHS 1301, 1311 ✓ 6.8.2.38 SITHS 1301, 1311 ✓ 6.8.3.21 SITHS 1301, 1311
Windows 10	Chrome	Internet Explorer	Edge	Edge Chromium	✓ 6.8.0.22 SITHS 1301, 1311 ✓ 6.8.1.31 SITHS 1301, 1311 ✓ 6.8.2.38 SITHS 1301, 1311 ✓ 6.8.0.22 SITHS 1301, 1311

Alla Net iD-versioner tidigare än 6.7 anses vara icke fungerande då en allvarlig sårbarhet upptäcktes relaterad till cache-tiden för PIN-koden.

Version 6.7 av Net iD Enterprise finns inte i Ineras paketering eller tillgänglig att ladda ner på Secmakers hemsida.

Vid problem med Net iD Enterprise kan SecMakers supportsida konsulteras för att se vilka versioner som det har rapporterats problem. Idp förvaltningen har inte alltid senaste information kring vilka versioner av Net iD som slutat stödjas även om vi uppdaterar detta dokument i samband med nya Idp releaser.

Från SecMakers Windows 10 sida: https://service.secmaker.com/w10.aspx Uppdaterad senast 2020-09-23.

Funktion	Status	Kommentar
Logga in i Windows 10 med smart kort utan Net iD Credential Provider	👍	I det här fallet blir det förstås utan Net iDs trevliga grafiska representation av certifikaten
Logga in i Windows 10 med smart kort med Net iD Credential Provider	👍	Fungerar, men för att promptningen ska lira optimalt krävs att Net iDs Credential Provider konfigureras för "full mode" istället för "pass-through-mode".
Dubbelriktad TLS med Internet Explorer 11	👍	Inga problem, lirar lika fint som vanligt! T.ex. med paketen SITHS1301, 1311 och 1901
Ladda Net iDs plugin i Internet Explorer 11	👍	Fungerar utmärkt! Men ladda inte pluginen via egna script, använd alltid SecMakers Javascript Tools om du vill kunna få bra support.
Dubbelriktad TLS med nya Edge	👍	Fungerar utmärkt!
Ladda Net iDs plugin i nya Edge	👍	Fungerar endast om man konfigurerar Edge att ladda sajten i "IE mode"

11.3. Cachning av PIN-kod

Användarupplevelsen med Net iD Enterprise kan variera beroende på hur klienten är konfigurerad lokalt. Det är bra att känna till att beteendet för cachning av PIN-koden påverkas av detta. Vid en ny inloggning kan vissa användare inte behöva slå in PIN-koden efter att de valt sitt certifikat även om det har gått lång tid sedan en tidigare inloggning. I andra fall kan PIN-koden dock krävas vid varje inloggning i de fallen där konfigurationen resulterar i en kort cachningstid.

12. Systemkrav

✅ = Säkerställt	⚠️ = Fungerar delvis	❌ = Stöds ej

12.1. IdP kompatibilitet

Operativsystem	IE11	Chrome	Edge	Edge Chromium	Firefox
Windows 7 + 8	⚠ *, **, ***, **** Slutar supportas Juni 2022	⚠ ***, ****	⚠ **, ***, ****	⚠ ***	⚠ (ej mTLS)
Windows 10	⚠ *, ** Slutar supportas Juni 2022	✓	⚠ **	✓	⚠ (ej mTLS)
Android	Se Användarhandbok - SITHS eID Mobilklient#Plattformskrav för kompabilitet och kända begränsningar				
iOS					

Tabell över olika webbläsares kompatibilitet med IdP 2.0 (januari 2021)

**) Kompatibilitet för e-tjänster med s k uthoppslösningar kan behöva verifiera att inställningar för IE "Trusted Zones" på den tekniska stödsidan IdP med Edge och IE 11 och Trusted sites.*
***) I och med att Microsoft har avslutat sitt stöd för och uppdateringar av IE11 samt legacy Edge är det svårare att få dessa webbläsare att fungera att fungera fullt ut, i alla tjänster, i alla användningsfall och konfigurationer på ett robust sätt. Uppdateras Microsoft OS och IE11/Edge med en ny och oprövad systemuppdatering garanteras det inte att det kommer att fungera initialt med alla kombinationer.*
****) I och med att Microsoft har avslutat sitt stöd för och uppdateringar av äldre Windowsversioner ges begränsad support för dessa.*

*****) Full funktionalitet kan ej garanteras med SITHS eID (OOB) klienter, se Användarhandbok - SITHS eID Windowsklient#Plattformskrav.*