2.0 Anslutningsguide till IdP

Visa Revisionshistorik

Version	Datum	Författare	Kommentar
0.1	13 Jun 2018	Daniel Petersson	Upprättad
1.0	14 Jan 2019	Grim Skarsgård	Fastställd
1.1	24 Sep 2019	Unknown User (lexhagenm)	Lagt till information om SITHS e-id samt Skånes kortnummer
1.2	16 Dec 2019	Unknown User (lexhagenm)	Lagt till information om dispens för reservkort och dess LoA-nivå i utställd biljett.
1.3	14 Feb 2020	Unknown User (lexhagenm)	Lagt till information om LoA-nivå i AuthnRequest
1.4	24 Mar 2020	Niclas Hedlund	Godkända certifikatutgivare för system, IE11 Trusted Zones
1.5	01 Apr 2020	Unknown User (lexhagenm)	LoA-nivå-förändring uppskjuten till oktober 2020
1.6	04 Jun 2020	Niclas Hedlund	LoA-nivå-förändring uppskjuten till december 2020
1.7	29 Sep 2020	Unknown User (lexhagenm)	Info om och hänvisningar till kommande LoA-nivå-förändring
1.8	02 Nov 2020	Skarsgård, Grim	Uppdaterat länk till DNS-information för Sjunet
1.9	08 Dec 2020	Skarsgård, Grim	Uppdaterat datum för LoA-förändring
1.91	18 Dec 2020	Skarsgård, Grim	Länkat till gemensam anslutningsinformation
1.92	13 Jan 2021	Skarsgård, Grim	Information om val av autentiseringsmetoder
1.93	25 Jan 2021	Niclas Hedlund Skarsgård, Grim	Förtydliganden, flytta duplicerad information. Mer, tydligare information om olika anslutningsmönster.
2.0	08 Feb 2021	Niclas Hedlund	Kompabilitet och klienter
2.1	16 Apr 2021	Unknown User (erikssonkr)	Uppdaterat Kap. 8.2 Net iD Enterprise samt kap 9.1 Idp kompatibilitet.
2.1.1	01 Jul 2021	Niclas Hedlund	1.1.4: Borttag av krav på SITHS som utgivare för signeringscertifikat i produktionsmiljö, tillägg nyckelhanteringsintruktion

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.

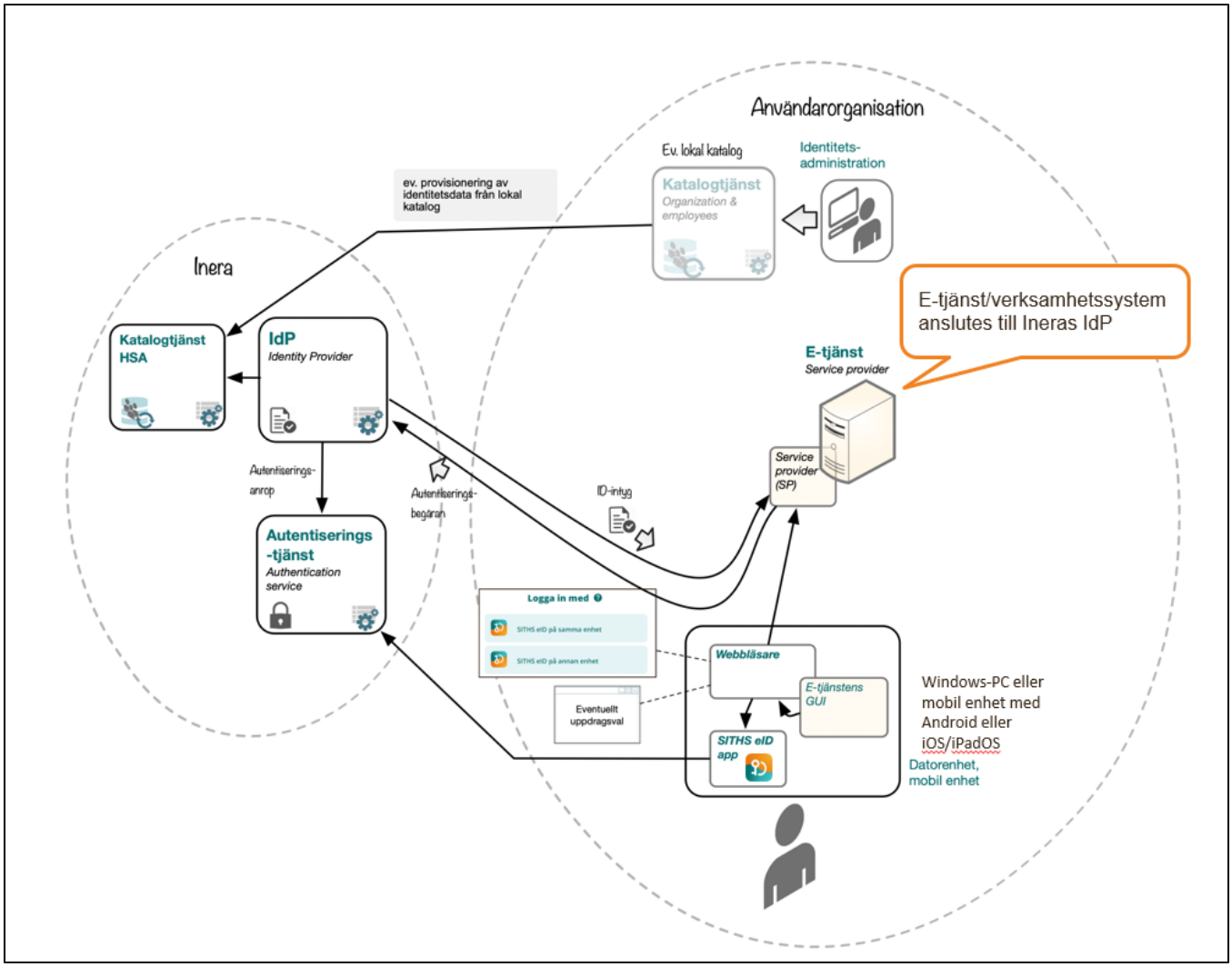
Vid en lyckad autentisering utfärdas ett identitetsintyg, (SAML-biljett, eller Id-token för OIDC) som innehåller information om autentiseringen samt eventuellt ytterligare användarattribut, som kan användas av ett ABAC (Attribute Based Access Control) behörighetssystem, d.v.s. behörighet på egenskapsnivå.

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.

1.1.2. 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.

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)

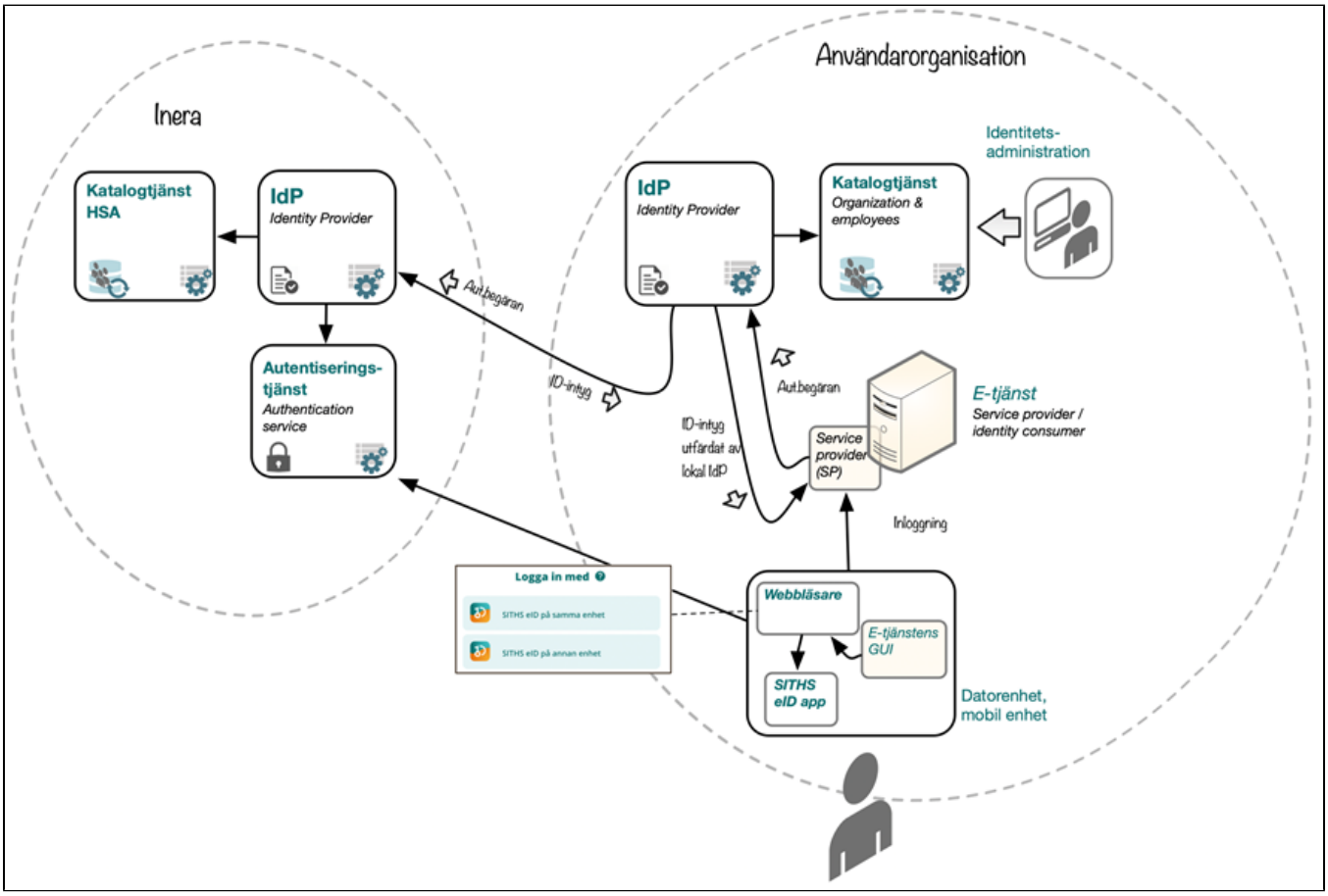
Lokala e-tjänster kan erhålla identitetsintyg från Ineras IdP via en lokal IdP genom anslutning som en OIDC RP eller SAML SP och agera som en "proxy-IdP". Anslutningen sker som en vanlig anslutning (som ovan) av en e-tjänst till Ineras IdP men skillnaderna består i stor sett av en förskjuten ansvarsfördelning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



3.2.1. 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

4. Dokumentation

Utöver denna guide finns följande dokumentation framtagen för tjänsten.

The root page IdP could not be found in space Inera - Identitet och åtkomst.

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, mTLS med Net iD Enterprise.

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

Tillgängliga metoder:

- SITHS eID på samma enhet
- SITHS eID på annan enhet
- mTLS med Net iD Enterprise

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

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

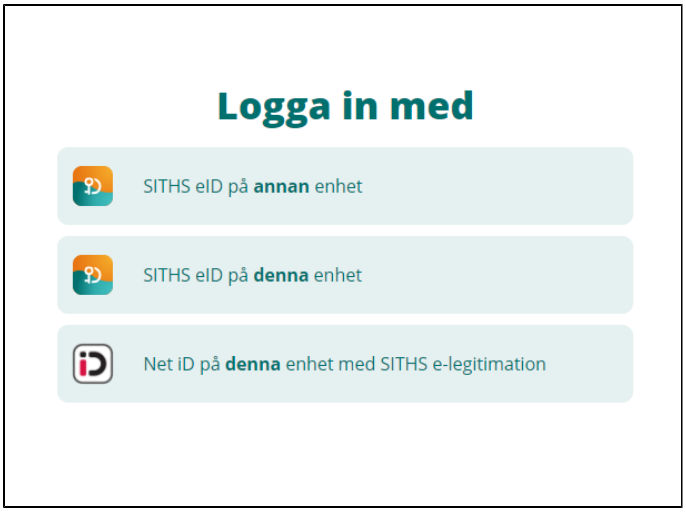
Förutom det formella anslutningsförfarandet tillkommer arbete kring att

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).



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. Användarklienter

8.1. 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

8.2. Net iD Enterprise (mTLS-inloggning)

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"

9. Systemkrav

✅ = Säkerställt	⚠️ = Fungerar delvis	❌ = Stöds ej

9.1. IdP kompatibilitet

Operativsystem	IE11	Chrome	Edge	Edge Chromium	Firefox
Windows 7 + 8	⚠ *, **, ***, ****	⚠ ***, ****	⚠ **, ***, ****	⚠ ***	⚠ (ej mTLS)
Windows 10	⚠ *, **	✓	⚠ **	✓	⚠ (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.*