Att ansluta e-tjänster för autentisering med SITHS eID

Inledning

Denna sida beskriver översiktligt olika varianter på hur din organisations e-tjänster kan nyttja autentiseringsmetoderna som baseras på SITHS eID. Längst ner på sidan hittar du en sammanställning av för- och nackdelar med respektive variant samt vilka som just nu finns tillgängliga för dig som kund.

Inera rekommenderar i första hand att ansluta e-tjänsten till Ineras IdP som Service Provider, i andra hand att ansluta den egna IdP:n som IdP-Proxy mot Ineras IdP. Detaljerad information om respektive anslutningssätt hittar du under Referenser längst ner på denna sida.

Gemensamt för alla varianter är att Inera tillhandahåller komplett klient- och serverprogramvara utan beroende till tredje part. Dock går det att kombinera t ex kundens lokala IdP med flera av anslutningsalternativen.

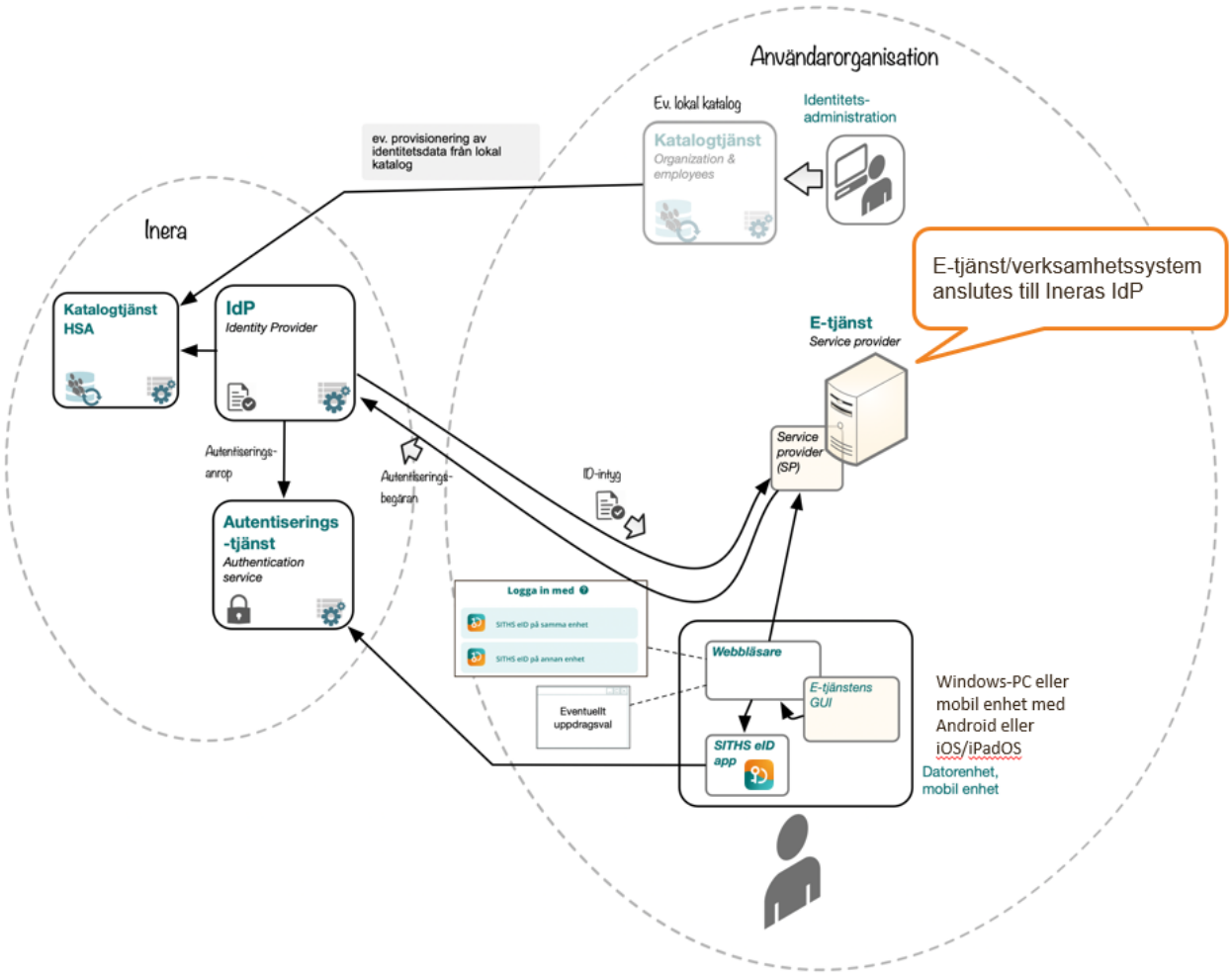
En funktion som i många fall är önskvärd är SSO (Single Sign On). I kapitlet Referenser hittar du en *fördjupad beskrivning på hur SSO fungerar* i olika scenarior.

Bland referenserna finns också en länk till en artikel om hantering av personidentitet vid autentisering för den som vill veta mer om hur det går till i Ineras lösning.

Anslut e-tjänst till Ineras IdP

Detta innebär att ansluta e-tjänsten som en Service Provider till Ineras IdP. Denna komponent har ett antal förmågor:

- Standardiserade protokoll i form av SAML2 eller OIDC som e-tjänsten använder i integrationen med IdP:n.
- Slutanvändaren väljer autentiseringsmetod i en dialog som IdP:n tillhandahåller. **Detta inkluderar möjligheten att låta e-tjänsten nyttja mTLS som autentiseringsmetod**.
- Resultatet av en gjord autentisering levereras till e-tjänsten i form av en biljett (identitetsintyg).
- E-tjänsten begär, eller får, en viss tillitsnivå (LoA, Level of Assurance) i biljetten men behöver inte ha någon kunskap om vilken autentiseringsmetod som används och får dessutom information om användarens behörighet i biljetten, om så önskas.
- Du som kund kan välja vilka autentiseringsmetoder som ska gälla per e-tjänst.
- Användarinformationen hämtar IdP:n från den centrala HSA-katalogen men informationen adminstreras lokalt i den egna organisationen.



Kundens e-tjänst ansluter till Ineras IdP som Service Provider

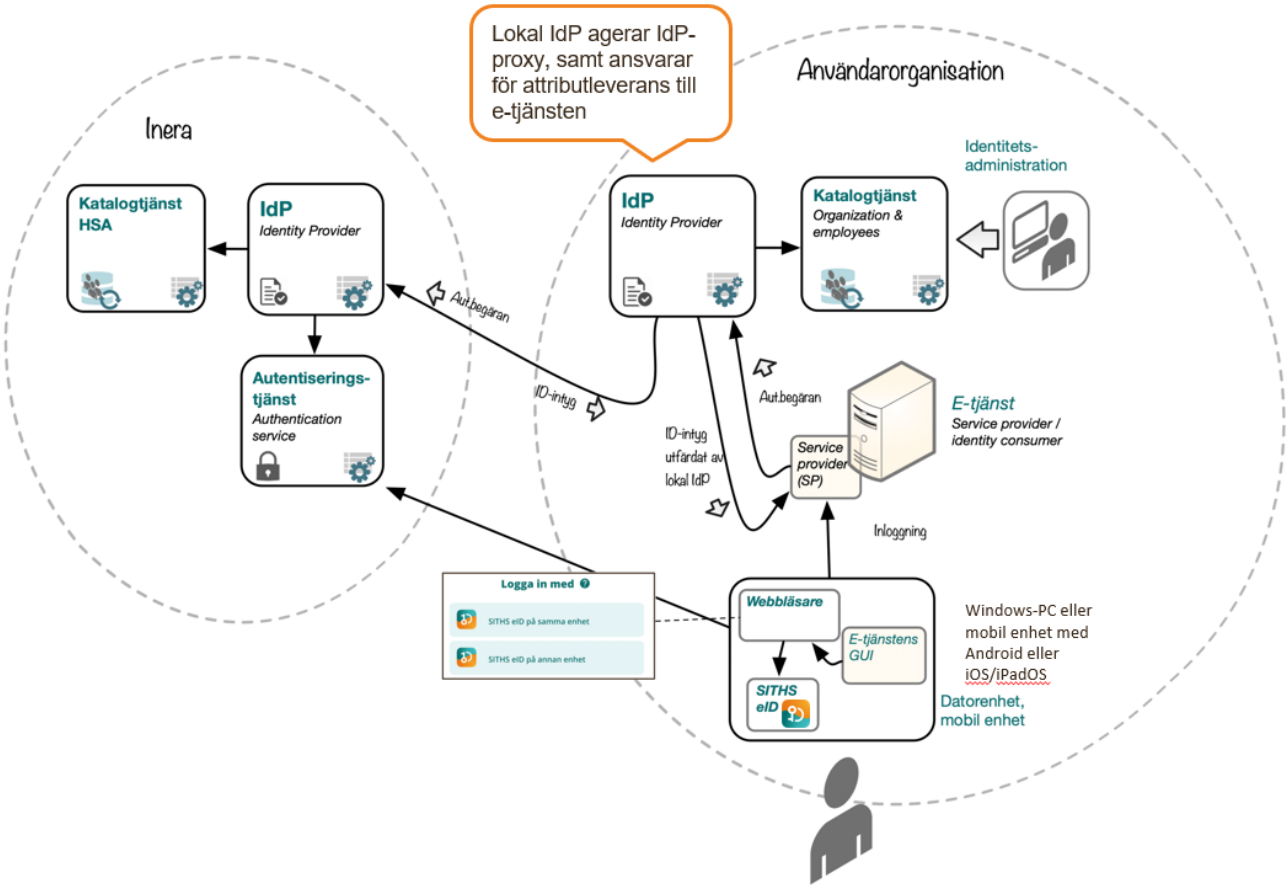
Anslut kundens IdP som IdP-proxy mot Ineras IdP

Kunden ansluter sin IdP som en Service Provder till Ineras IdP. På så sätt kan man ha en egen IdP, anpassad för specifika lokala behov men ändå ansluta till Ineras lösning via standardiserade gränssnitt. Kunden slipper de nackdelar och kostnader som det medför att utveckla och underhålla IdP-funktionalitet som redan finns i Ineras IdP men måste agera IdP-proxy. Med det menas att gentemot Ineras IdP uppträder den som en Service Provider men mot de anslutna e-tjänsterna agerar den IdP. Kunden behöver utveckla den lokala IdP:n så att den stödjer denna förmåga.

Om kunden använder den egna IdP:n för andra e-tjänster så kommer användarna att kunna få SSO, Single Sign-On. Du som användare behöver bara autentisera sig en gång för åtkomst till alla e-tjänster som är anslutna till samma IdP. Se även *Fördjupning om SSO* bland Referenser i denna artikel.

Teoretiskt kunde kundens IdP få behörighetsstyrande information (attribut) om användaren via det identitetsintyg (biljett) som levereras från Ineras IdP men tanken är att den informationen ska hämtas från den lokala katalogtjänsten. Ineras IdP svarar i huvudsak för e-legitimeringen. Kundens IdP ansvarar för att tillverka ett nytt identitetsintyg, med attribut, baserat på biljettinformation från Ineras IdP och den lokala katalogtjänsten. I *Anslutningsguide till IdP* finns rekommendationer för vilka attribut som är lämpliga.

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



Kundens IdP ansluter till Ineras IdP som Service Provider och uppträder som IdP mot de anslutna e-tjänsterna, dsv som IdP-proxy.

Anslut kundens IdP till Autentiseringstjänst SITHS från Inera

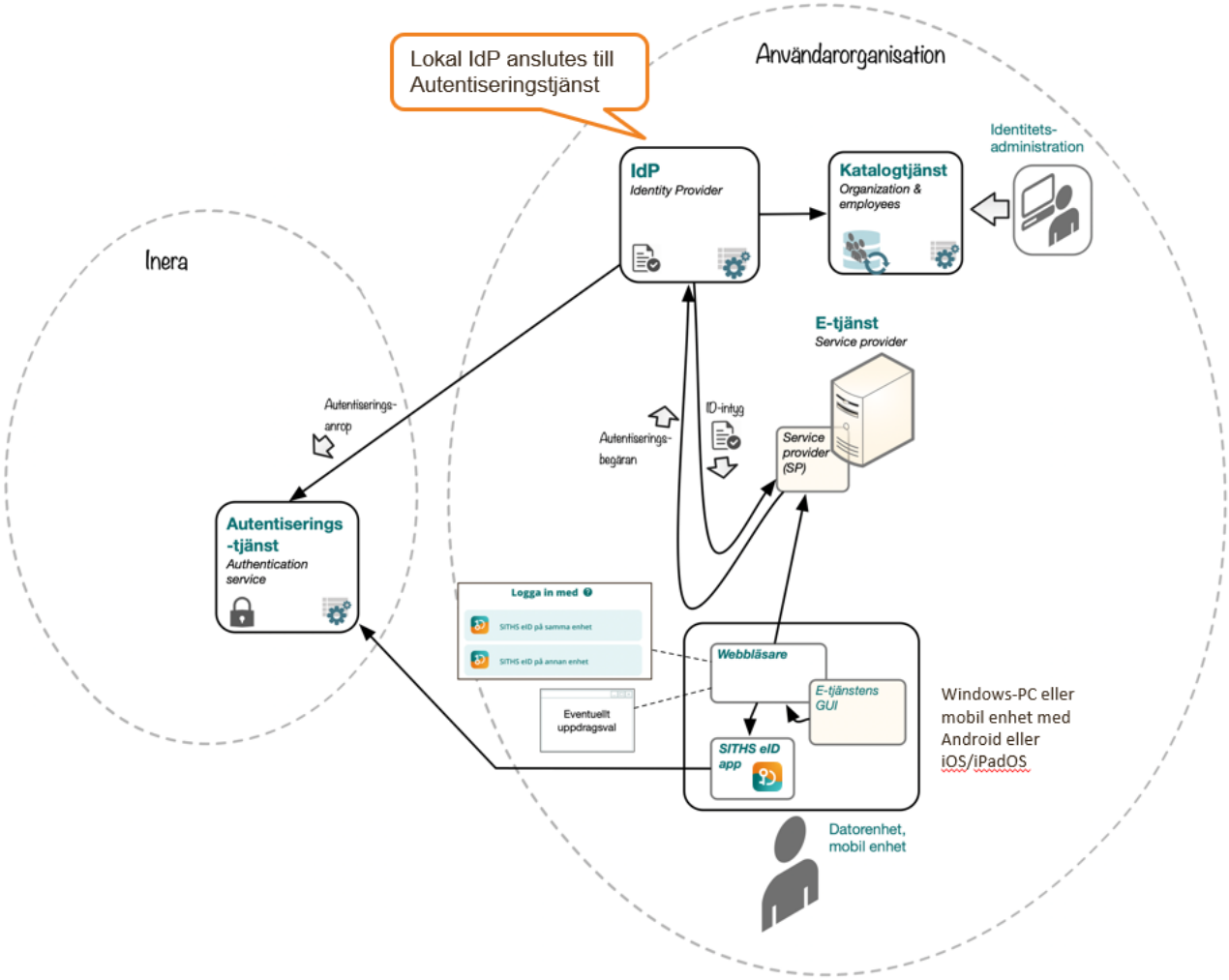
I det här fallet så kan kunden ansluta sin egen IdP till Autentiseringstjänst SITHS från Inera via det proprietära protokoll som Inera har utvecklat. Kundens e-tjänster måste då ansluta till kundens egna IdP för att via denna väg få tillgång till de autentiseringsmetoder som finns för SITHS eID. **Kunden måste själ v utveckla** motsvarande funktionalitet i sin IdP som återfinns i Ineras IdP. T ex

- Integration mot Ineras Autentiseringstjänst SITHS med presentation av användarens val av autentiseringsmetod
- QR-kodhantering för säkrad autentisering
- Tolkning av tillitsnivå (LoA)
- Integration mot katalogtjänsten
- App-växling
- Uppdragsval

Mer information om hur man ansluter till Autentiseringstjänst SITHS finns i *Anslutningsguide till Autentiseringstjänst SITHS*, se kapitlet Referenser.

> Observera att Ineras lokala IdP **kan** ansluta till Autentiseringstjänst SITHS från Inera, på så sätt slipper kunden utveckla motsvarande funktionalitet. Se *Lokal IdP från Inera* bland Referenser.

.



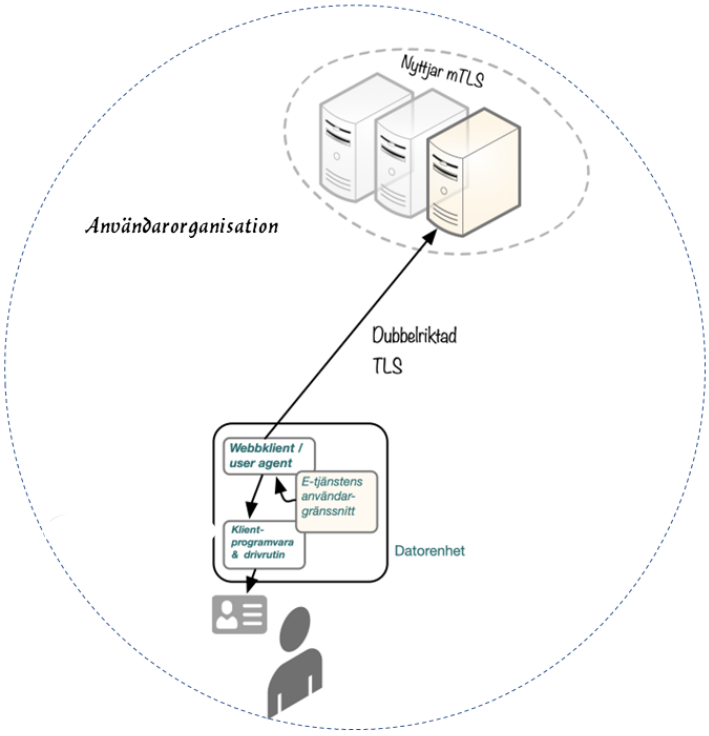
Kundens IdP ansluter till Autentiseringstjänsten

Dubbelriktad TLS (Mutual TLS, mTLS)

mTLS är en autentiseringsteknik där tilliten mellan klient och server bygger på ömsesidig utmaning av varandras certifikat. För att det ska fungera fullt ut, behöver e-legitimationen stödja tekniken, vilket SITHS eID gör.

Till skillnad från andra autentiseringstekniker beskrivna här, är inte användarorganisationen beroende av Ineras tjänster vid autentiseringen. Inera levererar dock all nödvändig programvara i form av klientprogramvara och drivrutin för att realisera detta. Det går också att använda mTLS via Ineras IdP men i exemplet nedan har användarorganisationen valt att realisera autentisering via mTLS helt i egen regi. Skälet till det kan vara att det är snabbare att gå över till att använda SITHS eID när användarorganisationen vill bli av med beroendet till tredje parts programvaror.

En annan viktig principiell skillnad är att mTLS är en *in-band* teknik, där informationskanal och säkerhetskanal alltid är densamma. Mobilt SITHS eID är en *out-of-band* teknik där kanalerna kan vara separata.



För- och nackdelar med de olika anslutningssätten

Varje anslutningssätt har sina möjligheter och begränsningar. Här är en sammanställning.

Förmåga/Anslutningssätt	**E-tjänst till Ineras IdP**	**Kundens IdP som IdP-proxy**	**Kundens IdP till Autentiseringstjänst SITHS** **Kan vara Ineras Lokala IdP**	**Dubbelriktad TLS (Mutual TLS, mTLS)**
Enbart standardiserade API:er	JA	JA	NEJ	JA
Hantering av LoA, m h a av komponenter i Ineras miljö	JA	JA	NEJ	NEJ
Utforma användardialogen för metodval enligt kundens UX-standard	NEJ	NEJ	JA	JA
Välja vilka autentiseringsmetoder som gäller per e-tjänst	JA	NEJ	JA	Beroende på hur det är uppsatt
Tolkning av LoA kan vara en annan än Ineras	NEJ	JA	JA	JA
Kunden kan välja katalog för användarinformation	NEJ	JA	JA	JA
Ingå i valfri federation	NEJ	JA	JA	JA
Använda andra e-legitimationer än SITHS eID	NEJ	JA (om kundens IdP har stöd för detta)	JA (om kundens IdP har stöd för detta)	NEJ
Tillgång till mTLS	JA	JA	NEJ, inte via Autentiseringstjänst SITHS men om den lokala IdP:n har stöd för detta går det att använda mTLS Ineras lokala IdP har stöd för mTLS.	Integrationen görs i verksamhetssystemet
SSO för alla e-tjänster, lokala och Ineras	JA (om alla e-tjänster ansluts till Ineras IdP)	NEJ	NEJ	Nej
SSO för lokala e-tjänster	JA (om alla e-tjänster ansluts till Ineras IdP)	JA (om alla e-tjänster ansluts till den lokala IdP:n)	JA (om alla e-tjänster ansluts till den lokala IdP:n)	Beroende på hur det är uppsatt

Referenser

- Anslutningsguide till Autentiseringstjänst SITHS
- Anslutningsguide till IdP
- Autentisering via SITHS eID övergripande presentation
- Autentiseringstjänst SITHS
- Filmer
- Fördjupning om SSO
- Gemensam anslutningsinformation
- Hantering av personidentifierare vid autentisering
- IdP från Inera (central)
- Lokal IdP från Inera
- OIDC
- Programvaror och tillbehör för SITHS
- SAML
- SSO
- Tolkning av tillitsnivå
- Utgivning och användning av SITHS e-legitimation