1.3 Anslutningsguide till Autentiseringstjänsten

Version	Datum	Författare	Kommentar
0.1	22 Mar 2022	Unknown User (erikssonkr)	Kopierat från Anslutningsguide för Autentiseringstjänst version 1.2
0.2			

Introduktion

Autentiseringstjänsten tillhandahåller autentisering för legitimering och underskrift via SITHS eID Windowsklient och SITHS eID Mobilklient (SITHS eID-klienterna) för användare som har e-legitimation från Identifieringstjänst SITHS.

Denna guide har som syfte att stötta organisationer som avser att ansluta en lokal IdP till Inera Autentiseringstjänst (mönster 3 nedan).

Integrationsmönster

Läs Att ansluta e-tjänster för en övergripande beskrivning av tillgängliga integrationsmönster och hjälp med att välja integrationsmönster.

De tre integrationsmönstren som erbjuds vid autentisering av e-tjänsters användare via Autentiseringstjänsten och SITHS eID-klienterna.

1. Anslutning av en eller flera lokal e-tjänster till Ineras IdP
2. Anslutning av lokal IdP till Ineras IdP (proxy-anslutning)
3. Anslutning av lokal IdP till Autentiseringstjänsten (direktanslutning)

Detta dokument innehåller framförallt information om direktanslutning till Autentiseringstjänsten (fall 3 ovan). Anslutningsguide till IdP beskriver motsvarande för de två första mönstren.

Övergripande information

Oavsett val av integrationsmönster så finns det hänsynstaganden som behöver hanteras av alla organisationer som avser att använda sig av Autentiseringstjänsten för legitimering och signering, dessa hänsynstaganden följer nedan.

Generellt anslutningsflöde

1. Anmäl intresse, teckna avtal med Inera för valt anslutningsmönster och därmed tjänst:
2. Beställ tjänsten för information om hur en beställning av IdP/Autentiseringstjänst-anslutning går till
3. Fakturering påbörjas.
4. Fyll i förstudiemall Autentiseringstjänst / Förstudie vid anslutning till IdP för testanslutning och skicka in för granskning via etjanster.inera.se /DokumentGranskning.
5. När förstudien är godkänd kan anslutning upprättas mellan den lokala tjänstens testmiljö och testmiljö hos Ineras tjänst (IdP eller Autentiseringstjänsten).
6. Testa anslutningen och funktionen i test.
7. Fyll i **separat** förstudie för produktionsanslutning, bifoga testrapport som visar att integrationen fungerar som tänkt för de tänkta nyttjandescenarierna.
8. När förstudien mot produktion är godkänd kan anslutning ske mellan produktionsmiljöerna.

Förutsättningar

Utöver de angivna generella förutsättningarna i Gemensam anslutningsinformation behöver följande förutsättningar vara på plats;

Anslutande lokal IdP SKALL;

1. **initalt förmedla HSA-id** för inläsning i Autentiseringstjänsten
    a. Relying party API:et skyddas av bl a mTLS. För att kunna anropa detta API behöver IdP:n presentera sig med ett SITHS funktionscertifikat (utgivet av SITHS e-id Function CA v1) vars subject matchar tjänstens HSA-id som läses in i Autentiseringstjänsten vid anslutningstillfället.
2. **vara en central IdP** för den anslutande organisationen. Varje kund tillåts ha en ansluten IdP, med eventuellt undantag för de största regionerna.
    a. Denna begränsning ämnar dels till att möjliggöra följsamhet mot referensarkitekturen, som specificerar att autentisering skall centraliseras till en specialiserad tjänst.
    b. Att hålla nere antalet anslutna tjänster är också avgörande för att kunna säkerställa att anslutna system håller sina anslutningar uppdaterade i takt med att Autentiseringstjänsten förändras.
3. **inom 6 månader kunna anpassa sig** till nya versioner av API:et hos Autentiseringstjänsten.
    a. När nya versioner av API:erna släpps så kommer de gamla API-versionerna att ligga aktiva parallellt med de nya under en övergångsperiod på 6 månader under vilken den anslutande IdP:n måste anpassas för att använda den nya versionen av API:erna.
4. **stödja appväxling.** IdP:n behöver kunna anropa det externa protokollet "siths://" för att kunna autostarta SITHS eID-klienterna vid inloggning "på samma enhet".
5. **hantera**
    a. QR kod,
    b. tolkning av tillitsnivå (LoA) och
    c. medarbetaruppdragsval
6. **eventuellt hantera**
    a. val av autentiseringsmetod och
    b. integration mot lokal katalogtjänst

Anslutande organisation SKALL;

1. upprätthålla kontaktvägar mot Inera:
    a. Minst en funktionsbrevlåda anges som kontaktpunkt i produktionsmiljö.
    b. Testanslutningar tillåts ha personkopplad epostadress
    c. prenumerara på nyhetsbrev från Inera och Säkerhetstjänster

Konnektivitet och nätverk

Se Nätverksinställningar för IAM-tjänster för mer detaljerad information.

SITHS eID-klienterna

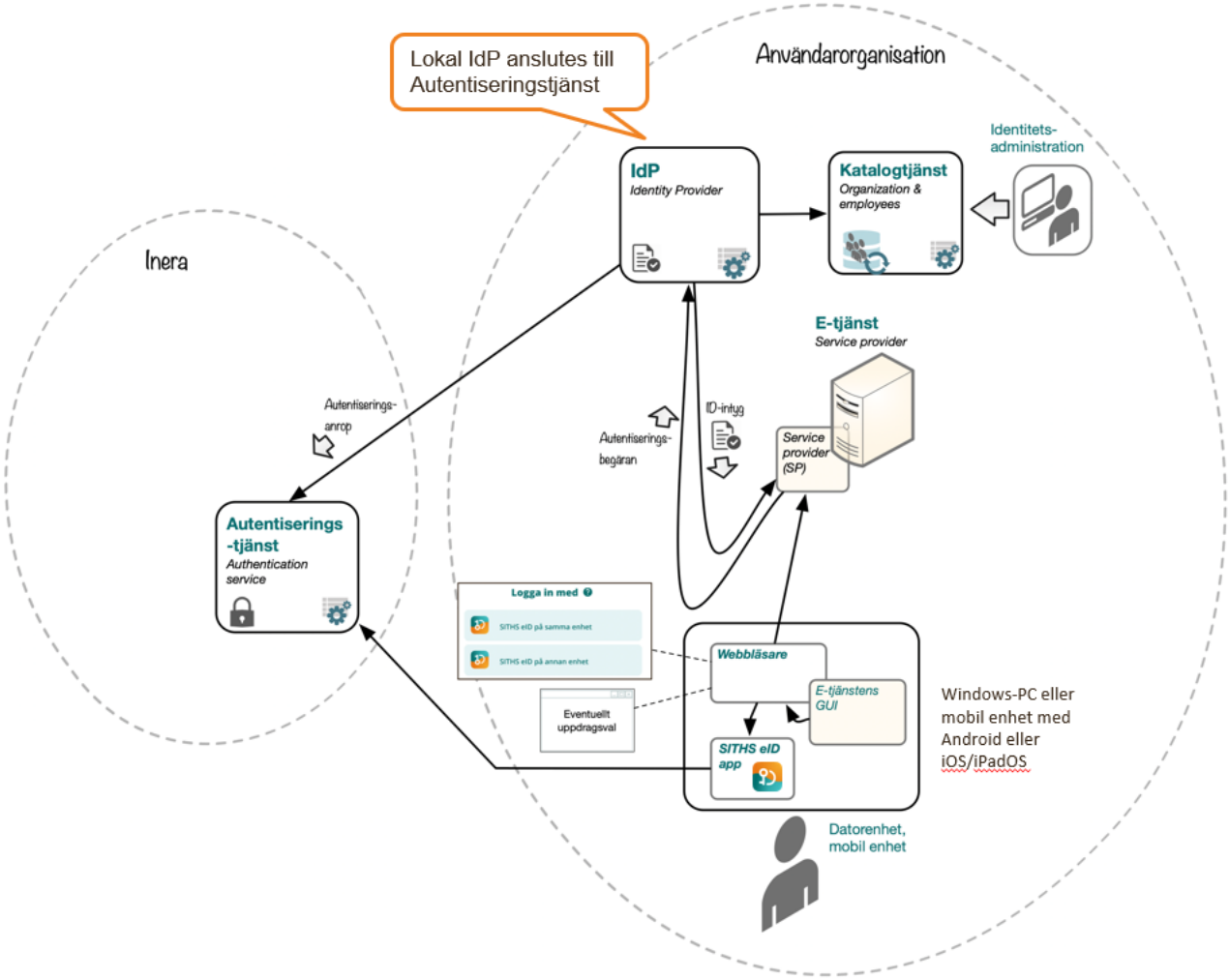
Mobilklienterna laddas ner via App Store eller Google Play. Windowsklienten tillgängliggörs i detta confluence-space och organisationer kan välja att distribuera den själva eller att dela länken med sina användare.

Se SITHS eID-app (Autentiseringsklienter) för mer information.

Anslutning av lokal IdP till Autentiseringstjänsten (direktanslutning)

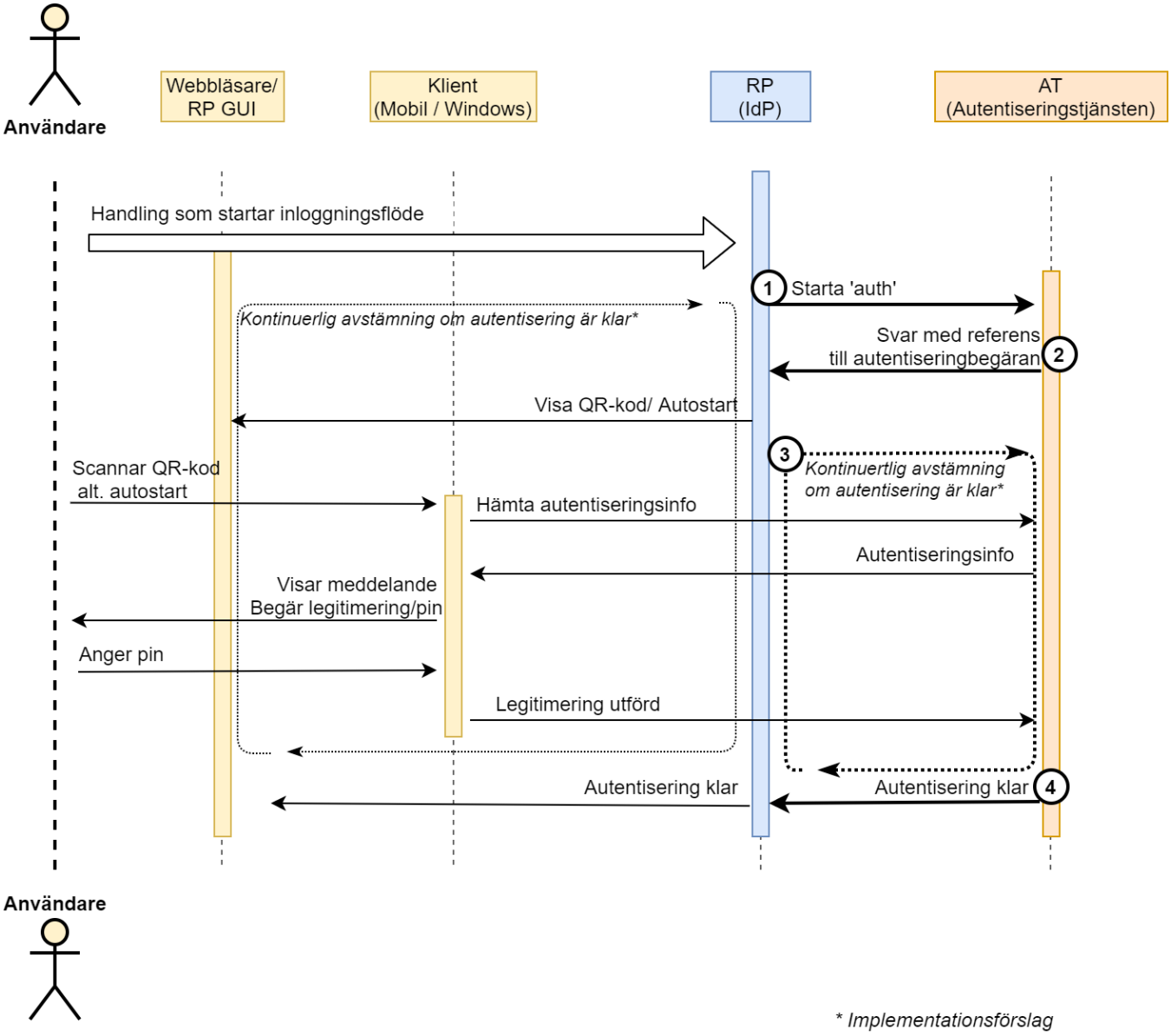
En lokal IdP kan anslutas direkt till Autentiseringstjänsten via Ineras proprietära API.

- Lokal IdP ansvarar för eventuellt val av inloggningsmetod
- Lokal IdP förmedlar autostarttoken till SITHS eID-klienterna
  - Se SITHS eID Appväxling - Exempel för inbäddade webbläsare ifall er IdP använder sig av en inbäddad webbläsare.
- Lokal IdP ansvarar för att tolka och förmedla tillitsnivå, utifrån information från användarcertifikatet som levereras från Autentiseringstjänsten.
  - Se Tillitsnivå (LoA) för information om hur Ineras IdP tolkar tillitsnivåer.



Teknisk Information

Flödesbeskrivning



1. Anslutande tjänst (RP) startar flödet med AT genom att skicka en förfrågan till "auth" med information om bland annat subject och autentiseringsförfrågans organisationstillhörighet.
2. AT svarar på förfrågan till "auth" genom att skicka tillbaka en "orderRef" (referens till utfärdad autentiseringsförfrågan) samt en "autoStartToken". RP förmedlar denna autostarttoken till SITHS eID-klienten m.h.a. appväxling eller QR-kod.
3. RP kollar (förslagsvis kontinuerligt m.h.a pollning) mot "collect" hos AT för att se om AT fått autentiseringen legitimerad av subject. Till "collect" skickas tidigare mottagna "orderRef" som är kopplad till en autentiseringsförfrågan.
4. AT svarar på förfrågan till "collect" genom att skicka tillbaka en status och tillhörande data om huruvida kopplad autentiseringsförfrågan blivit legitimerad, om den blivit legitimerad är autentiseringsflödet nu avklarat.
    a. alternativt kan subject välja att avbryta ("cancel") en legitimering och då avslutas autentiseringsflödet och detta meddelas som svar på "collect".

Se ex. SAD IdP för information om hur Ineras IdP realiserar autentiseringsflödet med hjälp av Autentiseringstjänsten.

Använding 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.

Autentiseringstjänstens API

Autentiseringstjänstens API är indelat i tre delar:

1. **Relying Party API:** API för att RP ska kunna starta och konsumera autentiserings- och signerings-förfrågningar. (../rp)
2. **Client API:** API för att en klient ska kunna resolvera autentiserings- och signerings-förfrågningar. (../auth)
3. **Registration Authority:** API för att registrera och aktivera certifikat. (../ra)

Anslutande IdP:er kommunicerar via **Relying Party API.**

Anrop där förmedling av certifikat krävs ska ske mot adresser som är prefixade med "secure". T.ex. för test: https://secure-authservice.mobiltsiths.ineratest.org/.

Swaggerdokumentation

Autentiseringstjänstens API-dokumentation tillgängliggörs via swagger på Autentiseringstjänsten med följande sökväg: "/openapi/swagger-ui/index.html?configUrl=/v3/api-docs/swagger-config".

Exempel för Testmiljön:

Dokumentation: https://authservice.test.siths.se/openapi/swagger-ui/index.html?configUrl=/v3/api-docs/swagger-config

URL för anslutning: https://secure-authservice.mobiltsiths.ineratest.org/

Hänsynstaganden vid anrop mot /auth

Parametern *"checkRevocation"* anger huruvida Autentiseringstjänsten skall utföra revokeringskontroll på användarcertifikatet och bör sättas till "*true"*. Det är fullt möjligt att utföra revokeringskontrollen i IdP efter autentiseringen är utförd, men det rekommenderas att delegera detta till Autentiseringstjänsten för att eventuella fel i autentiseringen skall upptäckas så tidigt som möjligt i flödet.

Parametern *"enhancedAuthentication"* **måste** sättas till *"true".* Den var initialt menad att kunna ange huruvida autostarttoken krävdes eller inte, men klienterna stödjer inte längre flödet utan autostarttoken. Parametern lär försvinna helt i framtida versioner.

Svarsfälten "*qrStartToken"* och "*qrStartSecret"* används till att beräkna animerade QR kod värden.

Hänsynstaganden vid anrop mot /collect

Pollning mot autentiseringstjänsten ska göras från servern. Det vill säga en användare ska inte kunna påverka hur ofta pollningen mot autentiseringstjänsten sker (annat än att påbörja sin inloggning).
Rekommenderat tidsinterval för pollning är 2 sekunder.

Starta klienten och förmedla autostarttoken

Kopplingen till klienten skapas genom att klienten från IdP får en autostarttoken (som IdP från från Autentiseringstjänsten i svaret ifrån anropet till /auth) som klienten sedan använder i sitt anrop mot Autentiseringstjänsten. Förmedligen av autostarttoken till klienten kan ske på två sätt:

1. Autostart via appväxling m.h.a. custom-protokollet <siths://> (om autentisering på samma enhet)
2. QR-kod som scannas in med Mobilklienten (om autentisering på annan enhet)

Formatet för custom-protokollet är följande:

```
siths://?autostarttoken=<autostarttoken>
```

Vid inloggning med annan enhet (mobil eller platta) ska en QR kod genereras och exponeras av IdP:n och skannas av med hjälp av Mobilklienten.
QR koden ska innehålla värdet <autostarttoken> eller den RP genererade animerade QR koden.

QR koder

Statisk QR

Statiska QR koder skall innehålla värdet av <autostarttoken> från auth/sign svaret.

Animerad QR

Svarsfälten "*qrStartToken"* och "*qrStartSecret"* används till att beräkna animerade QR kod värden. "*qrStartSecret"* skall endast vara en secret mellan RP och AT.

Animerade QR koder skall beräknas enlig prefix.qrStartToken.tid.hmacSHA256(qrStartSecret, tid)

Fält	Beskrivning
prefix	Fast värde för närvarande, skall sättas till "auth"
qrStartToken	UUID som mottages från auth/sign svaret
tid	Tid i sekunder sedan svaret från auth/sign mottogs
hmac	Hash som beräknas enligt HMACSHA256(qrStartSecret, tid) Formatteras som en 64 tecken hexadecimal unsigned integer med ledande nollor Java formatering String.format("%064x", new BigInteger(1/*unsigned*/, HMACSHA256(qrStartSecret, tid)));

Exempelsekvens:

tid=0

auth.db65306e-63ab-48ba-a2c5-fbadab3aa20e.0.bc81b15eb62e07283694433e5b95ae176dfea54096e9601a6bf8e808801779ad

tid=1

auth.db65306e-63ab-48ba-a2c5-fbadab3aa20e.1.71c30896ad541cd0a8794f3cdf9f305085c60a794b860fb8d2b47f14b6bca742

tid=2

auth.db65306e-63ab-48ba-a2c5-fbadab3aa20e.2.fb2d2343e7901f65f9d0aec2fb77bd4bc7dd5103b1b19977a841dfa3659d2037