SAD IdP

Innehållsförteckning

Revisionshistorik

Version	Datum	Utförare	Kommentar
0.1	23 Feb 2023	Ehlert, Stefan	▪ Kopierat från IdP 2.4
0.2	30 Oct 2023	Ehlert, Stefan	▪ Brutit ut information kring LoA Administration till egen dokumentstruktur
1.0	17 Nov 2023	Pietu Hammarström	Efter dokumentationsmötet 16/11 godkänns detta dokument

1. Inledning

1.1. Nomenklatur

Begrepp	Definition
Autentisering	Kontroll av uppgiven identitet, t.ex. vid inloggning, vid kommunikation mellan två system eller vid utväxling av meddelande mellan användare
Auktorisation / Behörighetskontroll	Kontroll av att en Autentiserad entitet (person eller system) är behörig att komma åt en begärd resurs.
e-legitimation, e-identitet, e-id	Elektronisk legitimation. Används för att identifiera en person eller ett system. T.ex. ett användarcertifikat på ett smartkort.
SITHS	Identifieringstjänst SITHS, en säkerhetslösning som används för att utfärda elektroniska identitetshandlingar (e-identiteter) till både personer och system.
SITHS eID	Den nya generationen SITHS e-identiteter, kan finnas både på smartkort och på mobila enheter.
Mobilt SITHS eID	SITHS eID på mobila enheter.
SITHS eID-klienter	SITHS eID Windowsklient och SITHS eID Mobilklient. Användarklienter på dator repektive mobila enheter som låter användare använda SITHS eID på kort eller i en mobil enhet för legitimation och underskrift.
CA (Certification Authority)	Certifikatutfärdare. System som utfärdar certifikat för användare och system.
OCSP/CRL	Protokoll för revokeringskontroll av certifikat.
LoA, Tillitsnivå	Level of Assurance. Grad av säkerhet och tillförlitlighet för en given e-legitimation. Ju högre tillitsnivå en e-legitimation har desto säkrare är den, både när det gäller teknisk och administrativ säkerhet.
SAML	Security Assertion Markup Language – XML-baserat ramverk för skapande och utfärdande av autentiserings- och attribut-information mellan between betrodda system över internet.
OIDC	OpenID Connect – internetcentrerat, federerat identitets- och autentiseringsprotokoll utökandes behörighetsramverket OAuth2.0 och det kryptografiskt systemet 'JSON Object Signing and Encryption' (JOSE)
E-tjänst	System som erbjuder en funktionalitet för användare eller andra system.
IdP (Identity Provider)	Komponent i infrastrukturen som efter godkänd autentisering av en användare, tillhandahåller elektroniska intyg (SAML biljett alternativt "ID token" inom OIDC) med identitet och attribut tillhörande användaren och/eller hens organisation. Syftar i detta dokument även på OpenID Provider (OP) för OIDC.
SP (Service Provider)	E-tjänst som begär och erhåller elektroniska intyg för en användare från en IdP. Oftast en e-tjänst som tillhandahåller funktionalitet och information till användare. Syftar i detta dokument även på Relying Party (RP) för OIDC.
OP (OpenID Provider)	OIDC-term. Se IdP.
RP (Relying Party)	OIDC-term. Se SP.
Katalogtjänst HSA	Användarkatalog. Datakälla för information om vårdpersonal, inklusive behörighetsinformation.
Autentiseringstjänsten	Infrastrukturkomponent som förmedlar autentiseringsbegäran mellan IdP och SITHS eID-klienter, samt förmedlar begäran om certifikatsutfärdande mellan SITHS eID Mobilklient och Utfärdandeportalen.
Utfärdandeportalen	Infrastrukturkomponent som låter användare utfärda Mobilt SITHS eID, och som förmedlar certifikatsbegäran och certifikat till och från CA.
Underskriftstjänsten	Infrastrukturkomponent som tillhandahåller underskrift för e-tjänster, via IdP, Autentiseringstjänsten och användarnas SITHS eID-klienter.
Claim	OIDC-term. Ett användar- eller autentisreingsattribut som RP efterfrågar i sin autentiseringsbegäran till OP.
Scope	OIDC-term. Omfång eller omfattning av ett eller flera claims.
JWT	JSON Web Token, datatyp innehållandes nycklar:värdepar för roll- eller attributbaserade säkerhetsmodeller.

1.2. Syfte

IdP:n syftar till stödja e-tjänster/applikationers behov av s k stark autentisering och behörighetshantering.

- Att tillhandahålla en implementation av en s k Identity Provider, IdP, enligt referensarkitekturen för identitet och åtkomst [S1].
- Att tillhandahålla en nationell tjänst som ger ett gemensamt sätt att utföra autentisering och tillhandahålla underlag för behörighetsstyrning för e-tjänster.
- Att tillhandahålla en tjänst till regionala och lokala intressenter som vill installera och drifta en egen instans av tjänsten.
- Att på ett enhetligt, och distribuerat sätt, via HSA, kunna administrera behörighetsstyrande attribut.

1.3. Målgrupp

De huvudsakliga målgrupperna för detta dokument är: systemägare, systemförvaltare, systemarkitekter och utvecklingsteam samt Inera Arkitektur.

1.4. Referenser

1.4.1. Nyttjade plattformsfunktioner

Ref	Dokument ID	Dokument inom kategori
P1	HSA	https://www.inera.se/hsa HSA används i lösningen för att tillhanda kvalitetssäkrade uppgifter om personer och funktioner/system. Grundläggande rättighetshetstilldelning utgår från HSA.
P2	SITHS	https://www.inera.se/siths SITHS-kort används för säker inloggning, ger stöd för stark autentisering av användare.
P3	Autentiseringstjänsten	Autentiseringstjänst SITHS
P4	Underskriftstjänsten	Underskriftstjänsten
P5	LoA administration	LoA administration

1.4.2. Nyttjade tjänstekontrakt

Ref	Dokument ID	Dokument inom kategori
T1	HSA TK	Nationella tjänstekontrakt (TK) för integration med HSA-katalogen: **infrastructure:directory:authorizationmanagement** • GetAdminCredentialsForPersonIncludingProtectedPerson • GetCredentialsForPersonIncludingProtectedPerson **infrastructure:directory:employee** • GetEmployeeIncludingProtectedPerson
T2	Autentiseringstjänstens Relying Party API	Autentiseringstjänstens API-dokumentation (swagger)

1.4.3. Styrande dokument

Ref	Dokument ID	Dokument länk
S1	ARK_0046	Referensarkitektur - Identitet och åtkomst
S2	ARK_0019	Referensarkitektur för vård och omsorg - T-boken Rev. B
S4	ARK_0060	Referensarkitektur för elektronisk underskrift och stämpel
S5	SAML2	• SAML2Int • SAML2Core • SAML2Prof • SAML2Bind • SAML2Conf • SAML2Meta • eGov
S6	OIDC	• OpenID Connect Core 1.0 • OpenId Connect Specifications • Heart OpenID Connect • Heart Oauth2

S7	SAMBI	https://www.sambi.se/teknik/
S8	SAML-profil	SAML-Profil
S9	OASIS	https://www.oasis-open.org/
S10	SwedenConnect	https://swedenconnect.se/tekniskt-ramverk.html
S11	Sweden Connect Deployment Profile (2019-308)	Deployment Profile for the Swedish eID Framework

1.4.4. Stödjande dokumentation

Ref	Dokument ID	Dokument/länk
R1	RIV-TA	http://rivta.se/documents.html

2. Arkitekturell översikt

Tjänsten är baserad på två standarder, SAML2.0 samt OpenID Connect (OIDC). Dessa kan båda tillgodose tjänstens syfte, men gör så med två olika tekniska ramverk. SAML är den äldre av dessa två och har använts under en längre tid inom vården och de nationella tjänsterna. OIDC är en nyare teknik som bygger på OAuth2 standarden.

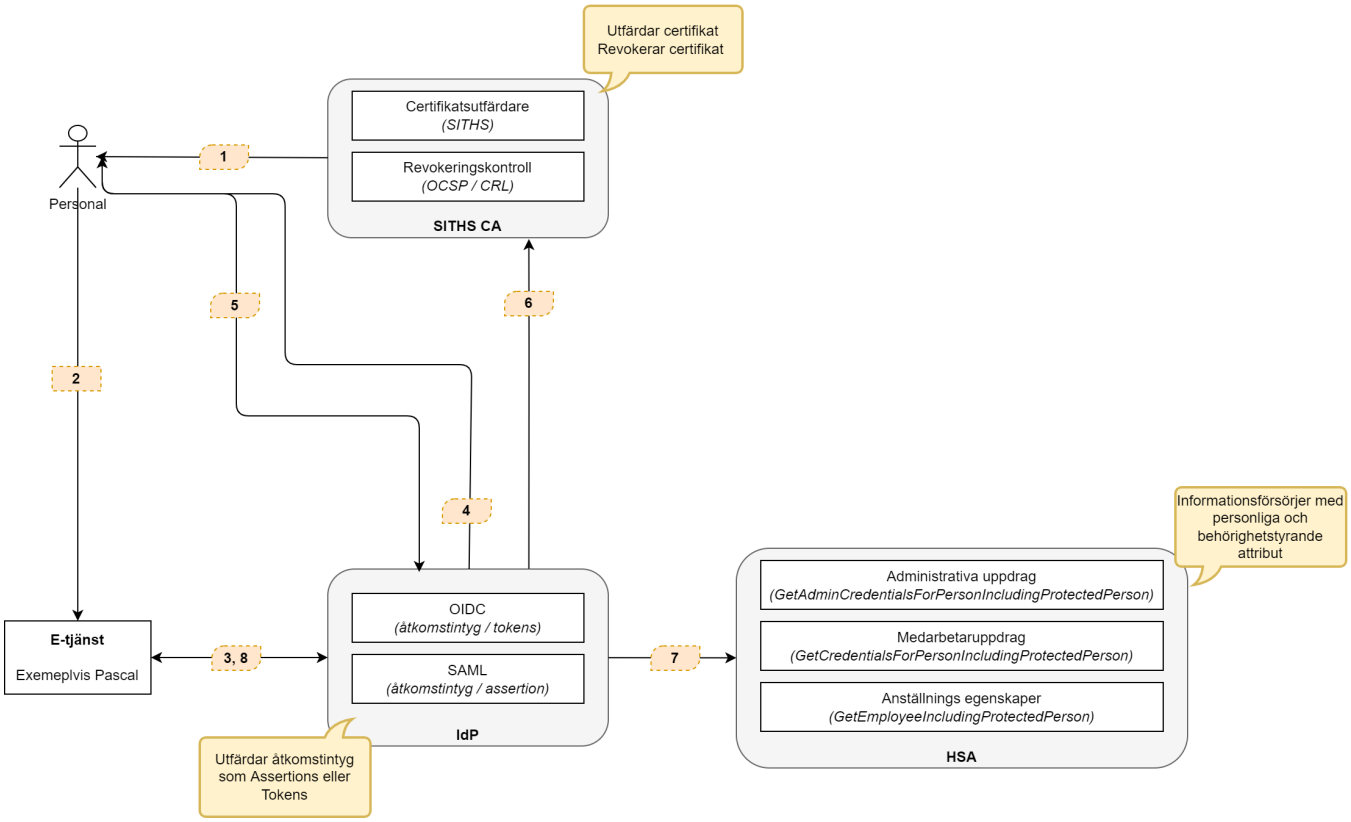
En användare som vill autentisera sig via tjänsten gör detta genom att presentera ett personligt eID. Detta kan exempelvis vara ett SITHS-certifikat. Aktörens e-id kan förmedlas med olika protokoll avsedda för autentisering (mTLS, WebAuthn eller dylikt). Aktörens attribut inhämtas från HSA-katalogen (nationell eller lokal beroende på installation). Identitetsbärare kan vara ett fysiskt kort.

Vid lyckad autentisering erhåller den e-tjänst som begärde autentiseringen att giltigt intyg enligt önskad standard (SAML2.0 eller OIDC).

Övergripande flöde

Personal vill nyttja en e-tjänst som kräver autentisering och behörighet.

1. Aktören måste vid ett tidigare tillfälle ha erhållit ett personligt eID, av en för IdP:n pålitlig utfärdare.
2. Aktören försöker ansluta till e-tjänsten.
3. E-tjänsten kräver autentisering av aktören via IdP.
4. IdP kräver att aktören autentiserar sig genom någon av de tillgängliga autentiseringsmetoderna.
5. Aktören identifierar sig med sitt e-id genom att ange tillhörande legitimeringskod eller liknande (t.ex. fingeravtryck eller annan biometri) i sin autentiseringsklient..
6. IdP:n säkerställer att certifikatet är giltigt.
7. Personliga och behörighetsstyrande attribut inhämtas via HSA-katalogen (genom RIV-TA tjänster).
8. Intyg i form av SAML-assertion eller ID-token förmedlas till e-tjänsten som behörighetskontrollerar och avgör access till aktören.

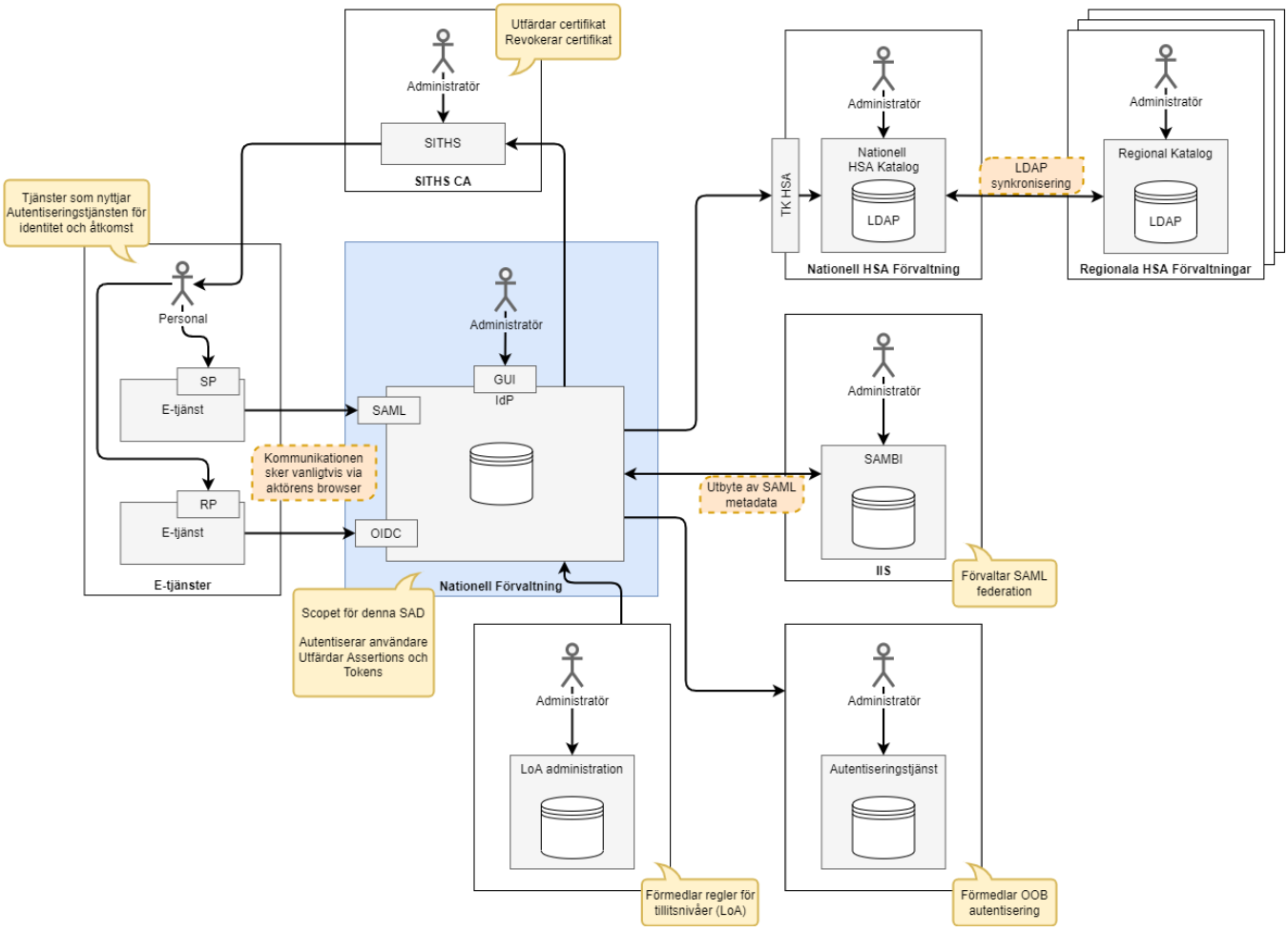


Bilden illustrerar ett typiskt autentiseringsflöde med tillhörande tjänsteintegrationer.

Arkitekturen är baserad på standarderna SAML2.0 samt OIDC. E-tjänsterna kopplar sitt säkerhetslager (SP/RP) mot IdP via något av dessa protokoll. Själva IdP:n är dock bara en liten del av hela infrastrukturen för att utföra en autentisering och erhålla behörighetsstyrande attribut. **Scopet för denna SAD är enbart IdP**, men följande delar ingår i infrastrukturen för identitet och åtkomst.

E-tjänster	De tjänster/system som vill använda IdP för att autentisera sina användare

Certifikatsutfärdare	Utfärdar certifikat till användare. Hanterar även revokering av dessa.
Regional HSA Förvaltning	Förvaltar lokal HSA-katalog. Replikering till Nationell HSA.
Nationell HSA Förvaltning	Förvaltar nationell HSA-katalog. Det är gentemot denna som IdP hämtar användares attribut.
Internetstiftelsen i Sverige (IIS)	Ansvarar för federationen SAMBI. IdP kan hämta ner federerat metadata härifrån.
Autentiseringstjänst	Förmedlar autentisering med SITHS eID
Utfärdandeportal	Utfärdar mobila certifikat för SITHS eID



Bilden illustrerar de parter som är en del av Identitets och åtkomst integrationerna för IdP.

IdP tillhandahåller (vid lyckad autentisering) en SAML-Assertion eller ID-token (beroende på den standard som används av e-tjänsten) innehållande attribut från HSA-katalogen. Detta kan vara attribut kopplade till personen, ett medarbetaruppdrag, eller administrativa uppdrag. E-tjänsten använder sedan dessa attribut för att utföra behörighetskontroll och hantera användarinformation vid exempelvis presentation i dess tjänst eller vid audit-loggning.

Detaljerad information för SAML och OIDC är definierade i:

- SAML-Profil
- OIDC-Profil

Förutom funktion för SAML och OIDC så tillhandahåller IdP ett GUI för administration av tjänsten. Se "Administrationsgränssnitt" senare i dokumentet.

2.1. Arkitekturella mål

2.1.1. Mål

- Följsamhet mot "Referensarkitektur för identitet & åtkomst" [S1]
- Följsamhet mot Nationella IT-strategin, enligt T-Boken [S2]
- Följsamhet mot de OASIS standarder som berörs [S7]
- Följsamhet mot ”SAMBI SAML Profil” [S6]
- Följsamhet mot SAMBI:s tekniska ramverk [S5]
- Följsamhet mot OpenID Connect [S4]
- Följsamhet mot HEART profile for OpenID Connect [S4]

2.1.2. Planerade avsteg

Frånsteg från ovan givna mål kan behöva göras för att tillgodose kravställning från Inera, eller i de fall två profiler är motstridiga i sina uppgifter.

2.2. Prioriterade områden

- Skapa en tjänst baserad på etablerade ramverk och tekniker. Detta för att minska långsiktiga förvaltningskostnader och underlätta utvecklingsarbetet.
- Basera tjänsten på standardprotokoll och följa specifikationer med så få avsteg som möjligt.
- Utveckla tjänsten för att fungera i en moduliserad driftmiljö - Paas. Detta för att minimera kostnader, underlätta deploy, möjliggöra anpassad skalning m.m.
- Ej bygga in "onödig" funktionalitet i tjänsten, utan nyttja externa tjänster där de lämpar sig bäst. Exempelvis för övervakning av metrics och logginsamling/sökning. Detta för att minska utvecklings och förvaltningskostnader, samt att externa tjänster oftast har mycket bättre funktionalitet än vad som kan byggas in i applikationen för rimlig kostnad.
- Undvika proprietära lösningar som kan försvåra flytt av förvaltning.

3. Följsamhet till T-boken

3.1. Följsamhet mot T-bokens styrande principer

3.1.1. IT2: Informationssäkerhet

Förutsättningar att uppfylla	*Uppfyllnad*
Verksamhetskritiskt IT-stöd designas för att möta verksamhetens krav på tillgänglighet vid frånfall av ett externt beroende. Ju fler beroenden till andra komponenters tillgänglighet, desto lägre egen tillgänglighet.	Applikationen är utvecklad för att fungera i PaaS miljö (containerbaserad) för att skapa maximal flexibilitet gällande tillgänglighet. Applikationen tillämpar lös koppling för att integrera komponenter. • Tjänsten själv (OIDC, SAML, REST) • Attributkälla (RIV-TA) Då applikationen i sig har till uppgift att förmedla identifierande/behörighetsstyrande attribut innebär ett bortfall av externa tjänster att applikationens uppgift inte kan uppfyllas.
Verksamhetskritiska gemensamma stödtjänster (t.ex. tillgång till behörighetsstyrande information) erbjuder möjlighet till lokala instanser som med tillräcklig aktualitet hålls uppdaterade med gemensam master.	Applikationen är en identifierings- och auktoriseringstjänst. • Lokala instanser kan skapas genom att använda samma paketerade tjänst (container i PaaS miljö, eller anpassad installation av binär)
Krav mellan integrerade parter måste regleras, informationsägaren ska godkänna att ett visst system får agera mot informationen genom ett visst tjänstekontrakt. *Exempelvis skall enligt integrationsprocessen för den gemensamma tjänsteplattformen ett överenskommelsesnummer för en integrationsöverenskommelse registreras i samband med att man "öppnar dörren" för en viss tjänstekonsument mot en viss kombination av informationsägare och tjänstekontrakt.*	Applikationen informationsförsörjs via nationella RIV-TA tjänstekontrakt. Anslutningsprocess för HSA RIV-TA sker via informationsägaren. Anslutning för e-tjänst gentemot applikationen sker via anslutningsavtal genom Inera.
Arkitekturen måste möjliggöra tillräcklig tillgänglighet vid flera samverkande system.	Applikationen är utformad för en hög tillgänglighet med horisontell skalning i PaaS miljö. Respektive tjänsteproducent av tjänstekontrakt skall leverera enligt SLA.
En sammantagen tolkning av tillämpliga lagar och förordningars konsekvenser för teknisk realisering av informationsfångst, utbyte och lagring.	Tjänsten hanterar personuppgifter. • GDPR tillämpas
Förutsättningar för spårbarhet etableras i form av loggningsregler för komponenter som deltar i säkert informationsutbyte.	Se kapitel: Spårbarhet.
Interoperabla, internationellt beprövade och för leverantörer tillgängliga standarder tillämpas för kommunikation mellan parter som har upprättat tillit.	Applikationen tillämpar standardprotokoll. • HTTPS/TLS • SAMLv2 • OIDC 1.0 • RIV-TA • SOAP-WS

3.1.2. IT3: Nationell funktionell skalbarhet

Förutsättningar att uppfylla	*Uppfyllnad*
Nationella tjänstekontrakt definieras med nationell täckning som funktionell omfattning. Det är möjligt för ett centraliserat verksamhetssystem som användas av alla verksamheter i Sverige att realisera varje standardiserat tjänstekontrakt. Det får inte finnas underförstådda funktionella avgränsningar till regioner, kommuner, landsting eller andra organisatoriska avgränsningar i nationella tjänstekontrakt.	Applikationen informationsförsörjs via nationella tjänstekontrakt (HSA) med SOAP-WS.
SLA ska definieras för varje tjänstekontrakt. Detta SLA ska ta hänsyn till framtida kapacitet för tjänstekontraktet med avseende på transaktionsvolym, variationer i användningsmönster och krav på tillgänglighet, i kombination med förmåga till kontinuerlig förändring.	SLA definieras i TKB som nyttjas. Övriga SLA'er för Applikationen hantera s av systemförvaltare.

Integration ska ske över en integrationsinfrastruktur (t.ex. virtualiseringsplattform) som möjliggör uppföljning av tjänsteproducenters fullföljande av SLA.	Nationella tjänsteplattformen kan används för informationsförsörjning (HSA).
System och e-tjänster som upphandlas kan utökas med fler organisationer som kunder utan krav på infrastrukturella ingrepp (jämför s.k. SaaS)	Applikationen är utvecklad för att tillgängliggöras nationellt i form av PaaS. Lokalt erhålls applikationen som binär (jar-fil). Denna kan köras som den är eller paketeras till exempelvis Docker image för installation i lokal Paas-miljö.

3.1.3. IT4: Lös koppling

Förutsättningar att uppfylla	***Uppfyllnad***
Meddelandeutbyte baseras på att kommunikation etableras utgående från vem som äger informationen som ska konsumeras eller berikas, inte vilket system, plattform, datalager eller tekniskt gränssnitt som informationsägaren för stunden använder för att hantera informationen. Genom centralt administrerad förmedlingstjänst skapas lös koppling mellan informationskonsument och informationsägarens tekniska lösning.	Lös koppling tillämpas alltid. Där möjligt används: • Nationella tjänsteplattformen • Nationella tjänstekontrakt
En arkitektur som skapar lös koppling mellan konsumenter och producenter, avseende adressering och standarder för kommunikation.	Följer vedertagna standards. Se kapitel: "Standarder"
En nationell integrationspunkt ska kunna erbjudas för varje nationellt standardiserat tjänstekontrakt, som en fasad mot bakomliggande brokiga systemlandskap.	N/A Inga tjänstekontrakt tillhandahålls av tjänsten.
Nationella tjänstekontrakt förvaltas i en nationellt koordinerad förvaltning.	N/A Inga tjänstekontrakt tillhandahålls av tjänsten.
För en process inom vård och omsorg kan flera tjänstekontrakt ingå. Därför är det viktigt att alla tjänstekontrakt baseras på en gemensam referensmodell för informationsstruktur.	Inga tjänstekontrakt tillhandahålls av tjänsten. SAML, Oauth2 samt OIDC standard följs.
Parter som samverkar i enlighet med arkitekturen integrerar med system hos parter som lyder under annan styrning (t.ex. myndigheter, kunder och leverantörer). Det kan leda till att vård- och omsorgsgivare antingen: • *Nationellt bryggar informationen (semantisk översättning) eller* • *Nationellt införlivar externt förvaltat tjänstekontrakt som standard.* *Observera att semantisk bryggning av information till vårdens referensmodell förutsätter en nationell förvaltning av bryggningstjänster.* *För att införliva ett externt förvaltat tjänstekontrakt förutsätts en transparent, robust och uthållig tjänstekontraktsförvaltning hos den externa parten.*	N/A Inga tjänstekontrakt tillhandahålls av tjänsten.

Befintliga system behöver anpassas till nationella tjänstekontrakt. Detta kan göras av leverantörer direkt i produkten, eller genom fristående integrationskomponenter (”anslutningar”). En anslutning bör ligga nära (logiskt vara en del av) det system som ansluts, oavsett om det är i rollen som konsument eller producent för anslutningen som genomförs.	N/A Inga tjänstekontrakt tillhandahålls av tjänsten.
Interoperabla standarder för meddelandeutbyte tillämpas, så att integration med till exempel en Web Service kan utföras utan att anropande system behöver tillföras en för tjänsteproducenten specialskriven integrationsmodul (s.k. agent).	Internationella standarder används. Se kapitel: "Standarder"

3.1.4. IT5: Lokalt driven e-tjänsteförsörjning

Förutsättningar att uppfylla	***Uppfyllnad***
När utveckling av källkod är en del av en tjänsteleverans skall följande beaktas: • *Alla leveranser tillgängliggörs under öppen källkodslicens. Valet av licensformer samordnas nationellt genom rekommendationer.* • *Utvecklingen bedrivs från start i en allmänt tillgänglig (över öppna nätverk) projektinfrastruktur där förvaltningsorganisation kan förändras över tiden inom ramen för en kontinuerligt tillgänglig projektinfrastruktur (analogi: ”Projektplatsen för e-tjänsteutveckling”).* • *Det innebär full insyn och åtkomst för utvecklare till källkod, versionshantering, ärendehantering, stödforum och andra element i en projektinfrastruktur under projektets och förvaltningens hela livscykel.* • *Upphandlade e-tjänster fungerar på de vanligaste plattformarna hos vårdgivarna och hos nationella driftspartners (Windows, Linux, Unix) t.ex. genom att vara byggda för att exekvera på en s.k. Java virtuell maskin.* • *Gemensam referensmodell för e-tjänsters interna uppbyggnad stimulerar och förenklar återanvändning och överföring av förvaltningsansvar mellan organisationer.*	All dokumentation och källkod tillhörande applikationen återfinns i leverantörens Atlassian Suite. Förvaltnings organisationen har full tillgång till dessa system, och externa parter bereds tillgång vid efterfrågan. Samtliga leverabler kan flyttas över till förvaltningsorganisation då egen infrastruktur är framtagen. Applikationen är utvecklad i Java och tillhandahålls lokalt i form av en jar binär. Denna kan paketeras till en Docker Image för lokal installation, eller körs direkt som den är. Docker kan exekvera på både Linux och Windows, eller i dedikerad PaaS (ex. OpenShift, Kubernetes osv).
Minsta möjliga – men tillräcklig – mängd standarder och stödjande gemensamma grundbultar för nationella e-tjänstekanaler säkerställer att även utvecklingsenheter i mindre organisationer kan bidra med e-tjänster för en integrerad användarupplevelse och att en gemensam back-office för anslutning av huvudmän till e-tjänster finns etablerad. I den mån etablerade standarder med bred tillämpning i kommersiella e-tjänster finns (t.ex. för single-sign-on), bör de användas i syfte att möjliggöra upphandling av hyllprodukter.	Se kapitel: "Standarder" samt "Teknik och Ramverk"
Utveckling sker mot globalt dominerande portabilitetsstandarder i de fall mellanvara (applikationsservrar) tillämpas. Det är möjliggöraren för nyttjande av free-ware och lågkostnadsverktyg i organisationer som inte orkar bära tunga licenskostnader för komplexa utvecklingsverktyg och driftsplattformar.	Se kapitel: "Standarder" samt "Teknik och Ramverk" För lokala installationer nyttjas Docker.
Nationell (eller regional – beroende på sammanhang vård/omsorg) förvaltning är etablerad (t. ex. s.k. Portal Governance), med effektiva processer för att införliva lokalt utvecklade e-tjänster i nationella e-tjänstekanaler. Systematisk och effektiv allokering av resurser för drift är en viktig grundförutsättning.	Applikationen förvaltas av Inera/CGI. Driften hanteras av Orange och NoGUI.
Genom lokal governance och tillämpning av det nationella regelverket får lokala projekt den stöttning som behövs för att från början bygga in förutsättningar för integration i samordnade (t. ex. nationella) e-tjänstekanaler.	Följande regelverk tillämpas: • Nationell referensarkitektur tillämpas • RIV-TA • Referensarkitektur för identitet och åtkomst

3.1.5. IT6: Samverkan i federation

Förutsättningar	***Uppfyllnad***
Att gemensamma gränssnitt i alla federativa utbyten finns framtagna och beskrivna, vilket möjliggör kostnadseffektiva och leverantörsneutrala lösningar.	Attributhantering utgår från SAMBI profil.
Det behövs organ och processer för att godkänna utgivare av elektroniska identitetsintyg och certifikat som är giltiga i federationen.	Användare registreras i regionala kataloger (tillgängliggörs via HSA) SITHS används.

Aktörer i olika nät, inklusive öppna nät ska vara välkomna i elektronisk samverkan genom att samverkande komponenter är säkra.	Infrastrukturen är ansluten till internet och sjunet.
Att Ingående parter i federationen är överens om ett antal gemensamma ståndpunkter: • *att stark autentisering likställs med 2-faktors autentisering* • *att vid samverkan acceptera följande metoder för stark autentisering; eID, PKI med lagring av nyckelpar på SmartCard eller motsvarande och metoder baserade på engångslösenord, antingen genererade i en fysisk enhet eller säkert distribuerad till fysisk enhet* • *att tillämpa en gemensam certifikat- och utfärdarpolicy, likvärdig med SITHS, som ett minimikrav för egen eller annans PKI* • *att sträva mot en autentiseringslösning, framför flera olika, för att realisera stark autentisering i den egna organisationen och i federation* • *att enbart acceptera SAMLv2, eller senare version, vid identitetsfederering samt tydliggöra att det i förekommande fall är det enda sättet att logga in och säkerställa det inte finns någon bakväg in* • *att tillämpa ett gemensamt ramverk för att ingå i en federation* • *att tillämpa en gemensam katalogpolicy, med utgångspunkt från HSA policy, som ett minimikrav för egna kataloger* • *att sträva mot att all gränsöverskridande kommunikation skall vara möjlig både över Sjunet och Internet. Det är den egna organisationen som beslutar vilken tillgänglighet som är tillräcklig för anslutningen* • *att sträva efter att möjliggöra kontroll av trafik till och från den egna infrastrukturen i en eller få kontrollpunkter* • *Att utgå från att kommunikation över Internet och Sjunet har ett likvärdigt skyddsbehov*	Applikationen är en IdP / OP. Se kapitel: "Standarder"

4. Användningsfall

Här beskrivs systemet ur ett funktionellt perspektiv i form av en användningsfallsmodell i syfte att lyfta fram de funktionella krav som är drivande för arkitekturen.

4.1. Användningsfall - Översikt

Ref	Användningsfall
AF1	Administrera tjänsten
AF2	Autentisera aktör
AF3	Logga ut aktör
AF4	Revokera tokens
AF5	Biljettväxling
AF6	Elektronisk underskrift

Schematisk användningsfallsöversikt.

4.2. Aktörsinformation

Aktör	Beskrivning
Personal	Användaren som använder en e-tjänst.
E-tjänst	E-tjänsten använder IdP för att autentisera och auktorisera personal.
Katalogtjänst (HSA)	Informationskälla för personliga och behörighetsgrundande egenskaper (behörighetsroller).
Systemförvaltare	Person som administrerar IdP. Aktiverar e-tjänster som skall använda IdP.

4.3. Autentiseringsmetoder

Idp:n har flera olika autentiseringsmetoder som kan användas. Dessa konfigureras per SP. Om det enbart finns 1 metod görs valet implicit och flödet fortsätter automatiskt.

Följande autentiseringsmetoder är för närvarande aktuella i IdP:

- SITHS eID på **annan** enhet (SITHS_EID_OTHER_DEVICE)
- SITHS eID på **denna** enhet (SITHS_EID_SAME_DEVICE)
- SITHS-kort på **denna** enhet (MTLS)

Nedan beskrivningar av Autentiseringsmetoderna gäller bara:

- **OM** IdP **INTE** har en giltig SSO-session
- Eller för autentisering via Autentiseringstjänsten (OOB) om SP/IdP begär en:
    - Förnyad autentisering eller
    - Legitimering för Underskrift (ForceAuthn)

Se Anslutningsguide till IdP för mer information om de olika autentiseringsmetoderna. Eventuella skillnader i autentiseringsflödena illustreras i användningsfallen nedan.

4.3.1. Dubbelriktad TLS (mTLS)

> ⚠ **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.

Användarens certifikat förmedlas via webbläsaren integration mot operativsystemet. En klient på användarens dator läser kortet och publicerar certet till operativsystemet/webbläsaren som använder det för att skapa en mTLS-anslutning till servern via webbläsaren. Finns det flera certifikat som accepteras av servern erbjuder webbläsaren en certifikatvalsdialog som ligger utanför serverns kontroll.

Användaren kommer vid varje nytt inloggningsförsök bli omdirigerad till en annan subdomän för att undvika att certifikatet som valdes vid förra inloggningsförsöket väljs igen av webbläsaren. Rent praktiskt kommer användaren bli omdirigerad till subdomäner som börjar med **secure0**.idp.inera.se och sedan inkrementera det numeriska värdet ända tills den högsta tillåtna subdomänen nås som IdP:n är konfigurerad till att omdirigera användare till, exempelvis **secure24**.idp.inera.se. Efter att användaren har förbrukat subdomänen med det högsta numeriska värdet blir användaren ombedd att starta om sin webbläsare för att rensa certifikatsvalen som webbläsaren kommit ihåg. Efter omstarten kommer användaren få börja om med **secure0**.idp.inera.se som första subdomän.

Användaren får dessutom möjlighet att göra nya inloggningsförsök ifall inget certifikat har förmedlats till IdP:n, exempelvis genom att inget kort har suttit i kortläsaren eller om användaren råkat trycka på Avbryt när certifikatsväljaren har presenterats i webbläsaren. I dessa fall kommer användaren hamna på en felsida som berättar att ett certifikat saknas för att slutföra inloggningen. Här har dock användaren möjlighet att trycka på kanppen Försök igen som dirigerar om användaren till nästa subdomän i kedjan. Väl där får användaren en ny chans att välja ett certifikat som förmedlas till IdP:n.

En detalj att känna till här är webbläsarnas omförmåga att rensa sessionskakor när en särskild inställning i webbläsaren används. Inställningen handlar om i vilket läge webbläsaren ska starta upp i. I fallet då användaren har valt att webbläsaren ska starta om med samma flikar och session som när webbläsaren stängdes ner senast kommer denna funktionalitet ha en negativ konsekvens i form av att användaren kan behöva starta om webbläsaren oftare än vad som skulle vara nödvändigt. Ett sådant scenario kan se ut såhär. Användaren har gjort 23 inloggningar med dubbelriktad TLS i den pågående webbläsarsessionen och väljer att stänga ner sin webbläsare. Senare startar användaren upp sin webbläsare igen. Då webbläsaren inte har rensat sessionskakorna kommer nästa inloggning med dubbelriktad TLS leda till att användaren autentiserar sig på subdomänen **secure24**.idp.inera.se. Vid nästa inloggningsförsök får användaren varningen att webbläsaren behöver startas om då för många inloggning gjorts i den pågående webbläsarsessionen även fast användaren bara gjort ett inloggningsförsök sedan senaste omstart.

4.3.2. Autentiseringstjänst (OOB - out-of-band)

Autentisering baserad på OOB-teknik (Out Of Band) sker via Autentiseringstjänsten [P3]. Två typer av Autentiseringsmetoder för OOB exponeras via IdP:n, autentisering med samma enhet och autentisering med annan enhet. Skillnaden mellan de två är enbart i hur IdP:n exponerar autostart-token för SITHS eID-appen.

- SITHS eID på **denna** enhet - IdP:n triggar uppstart av klientapplikation via webbläsaren och custom-protokollet "siths://" tillsammans med autostart-token i anropet.
- SITHS eID på **annan** enhet - IdP:n visar en QR-kod och användaren får själv starta sin applikation för att skanna QR-koden med kameran på den mobila enheten.

Se dokumentationen för Autentiseringstjänsten [P3] för mer detaljer.

4.4. Logisk realisering av signifikanta användningsfall

4.4.1. AF1 - Administrera tjänsten

4.4.1.1. Textuell beskrivning

IdP har en tillhörande administrativ komponent. Komponenten och sina funktioner beskrivs utförligt i Användarhandboken. Nedan sammanfattas de administrativa möjligheter som tillhandahålls.

- Administrera behöriga SAML-klienter
- Administrera behöriga OIDC-klienter
- Administrera pålitliga Certifikatsutfärdare
- Administrera tjänstens Certifikat / Privata Nycklar
- Administrera behörigheter för administratörer av GUI
- Konfigurera kontaktuppgifter för tjänsten

4.4.1.2. Realisering

En aktör med behörighet vill administrera IdP.

1. Aktören loggar in i tjänsten, och en förutsättning är att aktören har behörighet genom sina attribut i HSA-katalogen.
2. Aktören är inloggad och utför den tilltänkta administrationen.
3. Aktören loggar ut ur tjänsten.

4.4.2. AF2 - Autentisera aktör

4.4.2.1. Textuell beskrivning

Användningsfallet beskriver hur en användare autentiseras i flödet.

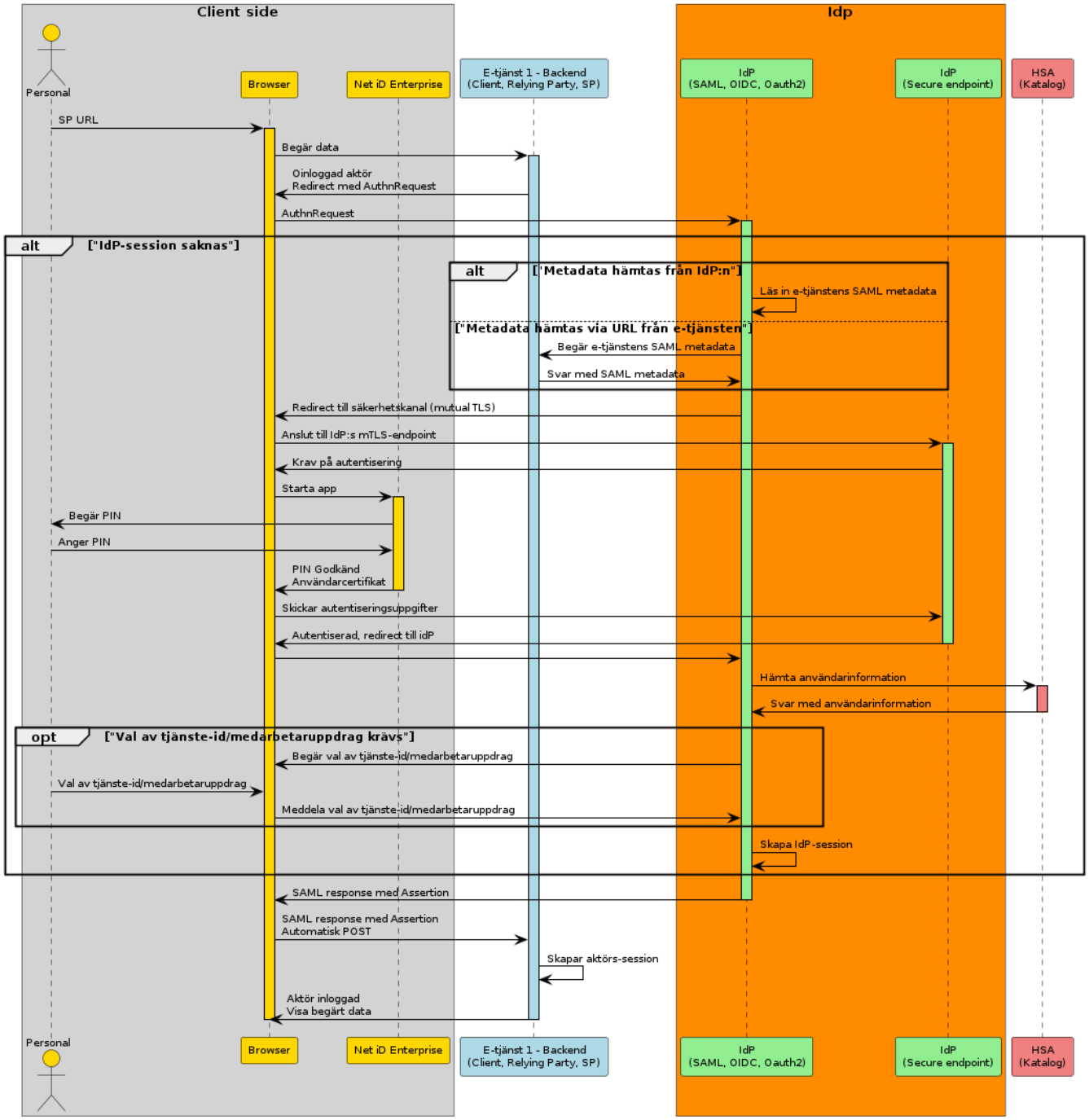
Se Inledning för beskrivning av detta användningsfall.

4.4.2.2. Realisering

4.4.2.2.1. SAML

Flödet visar en Autentisering med SAML. Flödet är inte uttömmande utan visar enbart ett av många alternativ som kan ske under en autentisering. Exempelvis att aktören i detta fall måste välja ett tjänste-id/medarbetaruppdrag i enlighet med begäran från SP, samt att aktören har mer än ett uppdrag att välja. Likaså att inget tjänste-id, organisationsnummer, personnummer eller orgAffiliation har pekats ut med hjälp av PrincipalSelection för att förenkla inloggningsflödet för en användare.

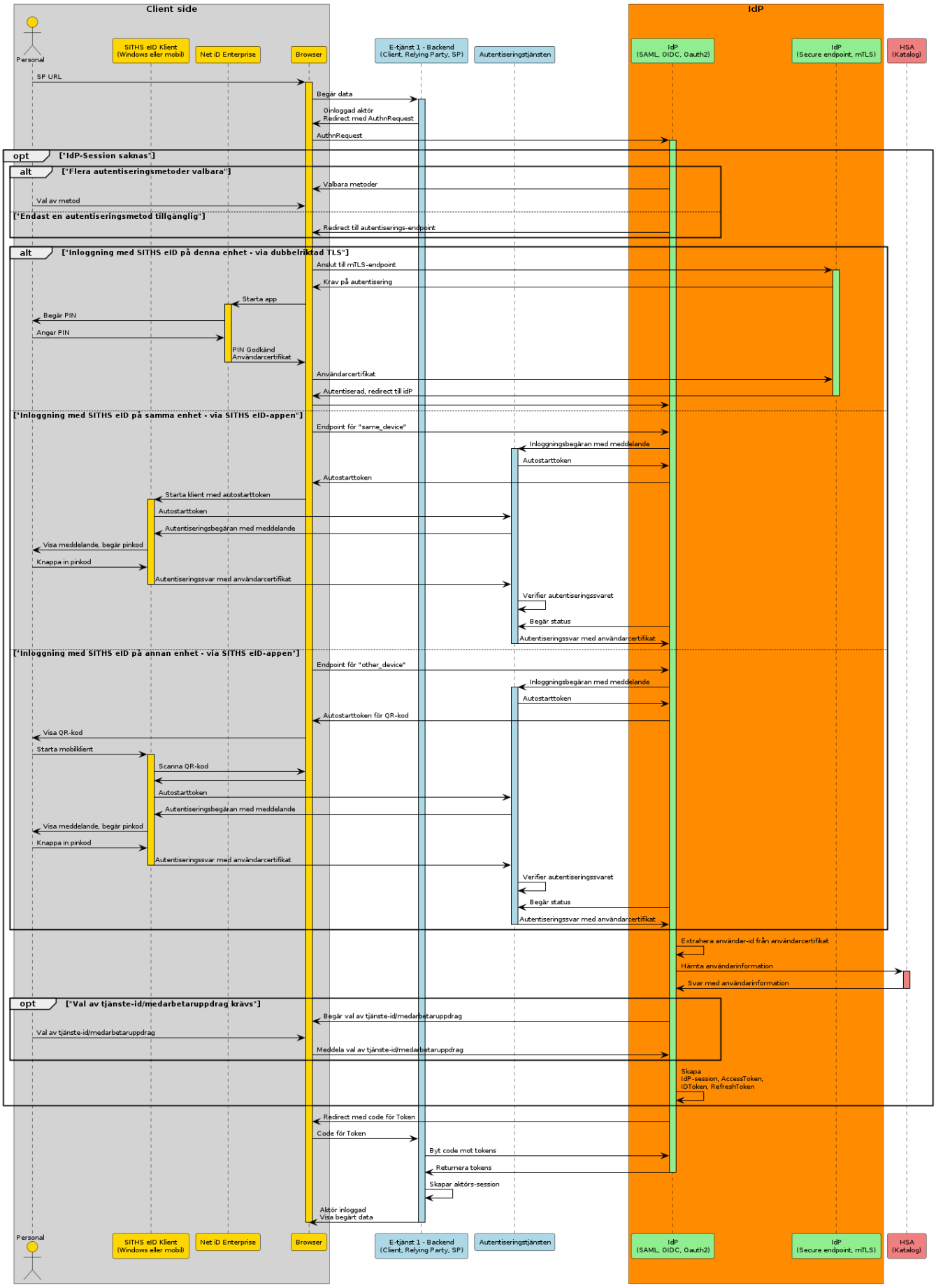
Likaså är flödet förenklat och visar exempelvis inte revokeringskontroll av certifikat.



4.4.2.2.2. OIDC

Flödet visar en Autentisering med OIDC. Kommentarer för SAML-flödet är applicerbart även i detta flöde.

Nämnvärt i det här fallet är att möjligheten till filtrering (likvärdigt PrincipalSelection för SAML) av tjänste-id, organisationsnummer, personnummer eller orgAffiliation inte synliggjorts i flödet.


Client side
IdP
Personal
SITHS eID Klient (Windows eller mobil)
Net iD Enterprise
Browser
E-tjänst 1 - Backend (Client, Relying Party, SP)
Autentiseringstjänsten
IdP (SAML, OIDC, Oauth2)
IdP (Secure endpoint, mTLS)
HSA (Katalog)
SP URL
Begär data
Oinloggad aktör
Redirect med AuthnRequest
AuthnRequest
opt
["IdP-Session saknas"]
alt
["Flera autentiseringsmetoder valbara"]
Valbara metoder
Val av metod
["Endast en autentiseringsmetod tillgänglig"]
Redirect till autentiserings-endpoint
alt
["Inloggning med SITHS eID på denna enhet - via dubbelriktad TLS"]
Anslut till mTLS-endpoint
Krav på autentisering
Starta app
Begär PIN
Anger PIN
PIN Godkänd
Användarcertifikat
Användarcertifikat
Autentiserad, redirect till idP
["Inloggning med SITHS eID på samma enhet - via SITHS eID-appen"]
Endpoint för "same_device"
Inloggningsbegäran med meddelande
Autostarttoken
Autostarttoken
Starta klient med autostarttoken
Autostarttoken
Autentiseringsbegäran med meddelande
Visa meddelande, begär pinkod
Knappa in pinkod
Autentiseringssvar med användarcertifikat
Verifier autentiseringssvaret
Begär status
Autentiseringssvar med användarcertifikat
["Inloggning med SITHS eID på annan enhet - via SITHS eID-appen"]
Endpoint för "other_device"
Inloggningsbegäran med meddelande
Autostarttoken
Autostarttoken för QR-kod
Visa QR-kod
Starta mobilklient
Scanna QR-kod
Autostarttoken
Autentiseringsbegäran med meddelande
Visa meddelande, begär pinkod
Knappa in pinkod
Autentiseringssvar med användarcertifikat
Verifier autentiseringssvaret
Begär status
Autentiseringssvar med användarcertifikat
Extrahera användar-id från användarcertifikat
Hämta användarinformation
Svar med användarinformation
opt
["Val av tjänste-id/medarbetaruppdrag krävs"]
Begär val av tjänste-id/medarbetaruppdrag
Val av tjänste-id/medarbetaruppdrag
Meddela val av tjänste-id/medarbetaruppdrag
Skapa IdP-session, AccessToken, IDToken, RefreshToken
Redirect med code för Token
Code för Token
Byt code mot tokens
Returnera tokens
Skapar aktörs-session
Aktör inloggad
Visa begärt data

4.4.3. AF3 - Logga ut aktör

4.4.3.1. Textuell beskrivning

Användningsfallet beskriver hur en utloggning går till inom tjänsten. Användningsfallet består av 2 alternativ.

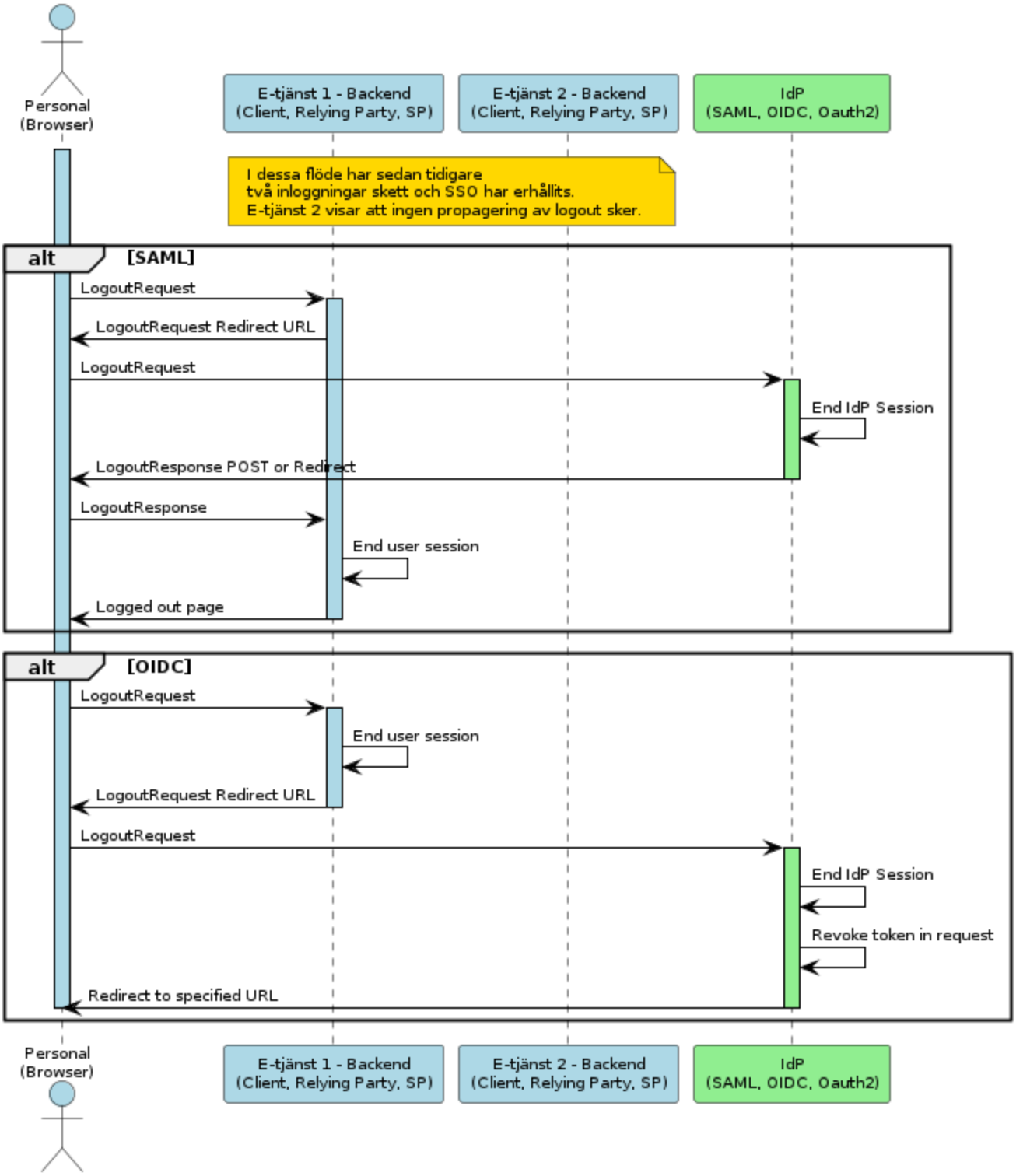
1. SAML
    a. En inloggad SP skickar ett LogoutRequest (via användarens user-agent) till IdP'n. **Detta LogoutRequest måste vara signerat.**
    b. Vid ett giltigt request avslutar IdP'n den eventuella IdP-sessionen. **Ingen propagering till andra SP/RP i samma IdP session sker.**
    c. SSO för tidigare IdP-session är nu avslutad och ny AuthnRequest kommer resulterar i ny inloggning, och ny IdP-session.
    d. LogoutResponse returneras till SP i enlighet med efterfrågad binding.
    e. SP ansvarar för att avsluta den egna sessionen med användaren.
2. OIDC Logout
    a. En inloggad RP gör en Logout begäran (via användarens user-agent) till IdP'n. I detta anrop skickas idtoken med. Detta anrop görs efter det att aktören loggat ut från RP i enlighet med standard.
    b. Vid en giltig begäran avslutar IdP'n den eventuella IdP-sessionen, samt revokerar id-token, access-token, samt refresh-token som hör till det token som skickades in. Tokens utfärdade till andra RP revokeras ej. **Ingen propagering till andra RP/SP i samma IdP session sker.**
    c. SSO för tidigare IdP-session är nu avslutad
    d. Eventuellt redirectas användaren till en av RP angiven URL, URL:en måste finnas registrerad på servern för att redirekten ska tillåtas.

Dessa två flöden kan sammanfattas med följande:

- Vid en logoutbegäran inom antingen SAML eller OIDC så kommer IdP'n att avsluta IdP-sessionen och förhindra fortsatt SSO. Tokens utfärdade till andra RP fortsätter vara giltiga.

4.4.3.2.

Flöden nedan representerar de olika scenarion för utloggning som anges ovan.



4.4.4. AF4 - Revokera tokens

4.4.4.1. Textuell beskrivning

Användningsfallet beskriver hur en revokering av token går till inom tjänsten..

1. Token revokering
    a. En RP som har tillgång till en Access Token eller Refresh Token vill revokera denna. En revokeringsbegäran för denna token skickas till IdP'n.
    b. Vid giltig begäran revokerar idP'n det token som ingick i begäran samt eventuella tillhörande tokens (ID Token, Access Token, Refresh Token som utfärdades samtidigt).
    c. Ingen inverkan på den IdP-session som token utfärdades inom sker. Om IdP-sessionen fortfarande är giltig kan SSO fortsatt erhållas.

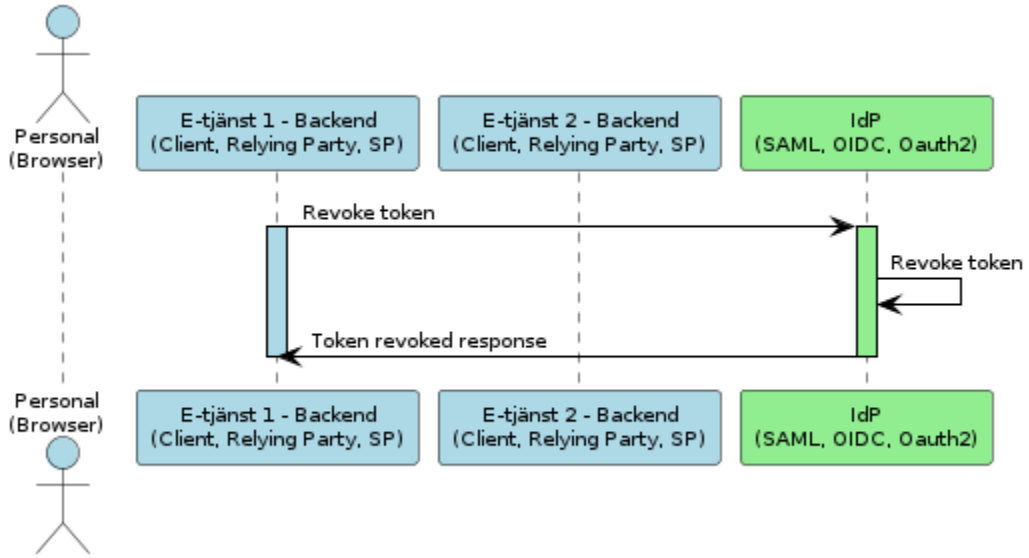
d. IdP skickar svar på begäran med statuskod.

Detta flöde kan sammanfattas med följande:

- Vid revokeringsbegäran kommer enbart den/de tokens som hör till begäran att revokeras. Ingen inverkan på användaren IdP-session kommer att ske, och vid giltig IdP-session fortsätter användaren erhålla SSO.

4.4.4.2. Realisering

Flöden nedan representerar de olika scenarion för revokering som anges ovan.



4.4.5. AF5 - Biljettväxling

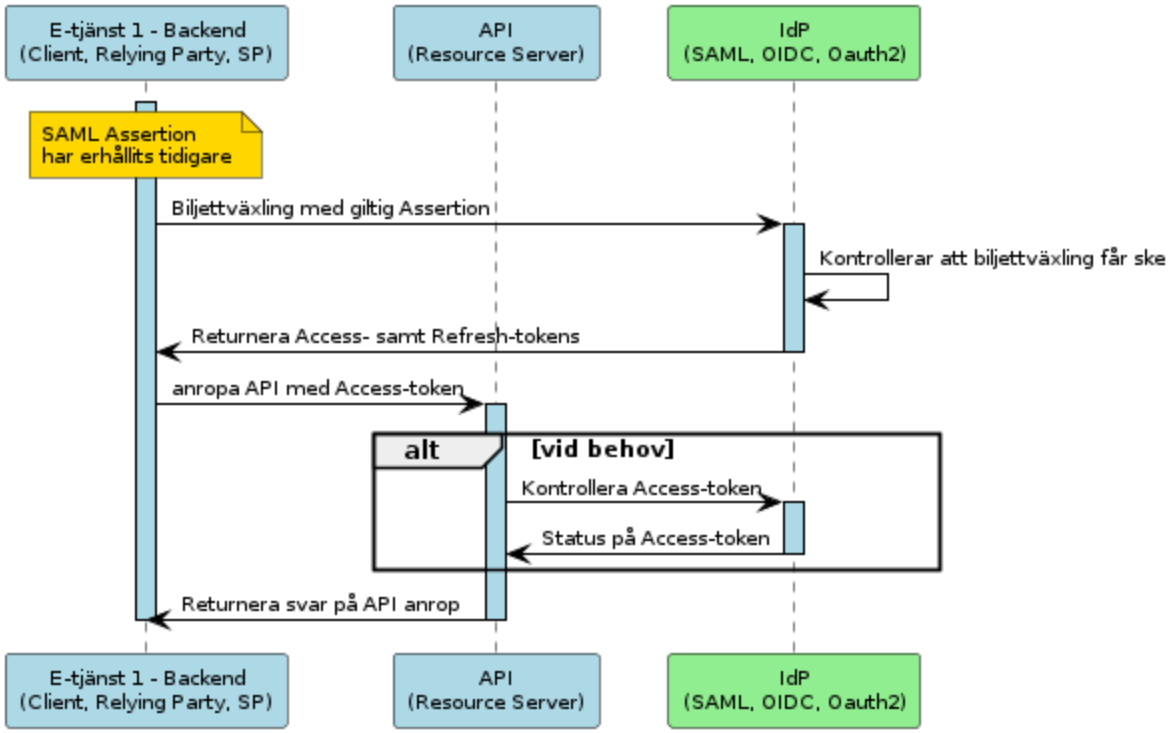
4.4.5.1. Textuell beskrivning

Biljettväxling beskrivs i RFC7522 och innebär att en E-tjänst med tillgång till en giltig SAML Assertion, kan använda denna för ett erhålla en AccessToken med motsvarande innehåll.

1. En e-tjänst har erhållit en giltig SAML Assertion, men behöver ett åtkomstintyg i form av en access-token för anrop till ett skyddat API.
2. e-tjänsten använder denna Assertion i ett anrop mot IdP:ns biljettväxlings-endpoint.
3. IdP säkerställer att biljettväxling får ske.
4. IdP tillhandahåller en access, samt refresh-token tillbaka till e-tjänsten
5. e-tjänsten använder access-token gentemot det skyddade API't.
    a. Tjänsten med API't kan eventuellt vilja kontrollera den använda access-token gentemot IdP.
    b. API-tjänsten returnerar ett svar

4.4.5.2. Realisering

Flödet nedan representerar en biljettväxling för en e-tjänst.



4.4.6. AF6 - Elektronisk underskrift

4.4.6.1. Introduktion

IdP:n har stöd för anslutning till Underskriftstjänst [P4] som följer SwedenConnects SAML-profil för underskrift [S11]. Detta innebär att kunder kan ansluta mot integrerande Underskriftstjänst och utnyttja IdP:n för autentisering mot denna.
Underskrifter kan endast ske via autentiseringsmetoderna som nyttjar SITHS eID via Autentiseringstjänsten [P3].

4.4.6.2. Relevanta skillnader mot inloggningsflödet

Flödet för underskrift är i stort identiskt med flödet för Autentisering med SITHS eID. Följande listar relevanta skillnader:

- Enbart SAML stöds vid underskrift.
- Underskriftsfunktionaliteten förlitar sig på Autentiseringstjänsten och SITHS eID-klienterna, och fungerar alltså inte med mTLS-autentisering.
- Metadata för underskriftsintegration publiceras separat och innehåller en delmängd av attributen som IdP:n kan producera.
- Underskrift följer standarden för Sweden Connect [S10] istället för Sambi [S7] .
- Det publiceras flera endpoints för underskrifts SAML-anrop, en för varje autentiseringsmetod. Detta för att kunna välja autentiseringsmetod redan vid anropet då det inte är önskvärt att användaren får val vid just underskrift.
- Vid anropet till IdP skickas en personidentifierare med som måste matcha identiteten som sedan autentiseras. Denna identifierare skickas i enskilda fall vidare till Autentiseringstjänsten (se här) och efter autentisering valideras den i IdP.
- Vid anropet skickas ett meddelande om vad som ska undertecknas med, detta MÅSTE visas upp för användaren. Meddelandet skickas vidare till Autentiseringstjänsten för vidare förmedling till autentiseringsklienterna.

4.4.6.3. Anvisning om vilken individ som skall utföra underskriften, via PrincipalSelection

Vid anrop till IdP kan filtrering av data skickas med i enlighet med SwedenConnects SAML-profil för underskrift [S11]. Detta sker i fältet <PrincipalSelection> i Autentiseringsbegäran.
Dessa attribut används för att redan i autentiseringsbegäran specificera vilken tjänsteidentitet som skall användas för autentiseringen, för att undvika användarinteraktioner i underskriftsflödet.

De attribut som avläses i IdP:n för PrincipalSelection är:

Attribut	Används för
http://sambi.se/attributes/1/personalIdentityNumber	Personidentifierare
http://sambi.se/attributes/1/employeeHsaId	Personidentifierare
urn:orgAffiliation	Filtrering av Medarbetaruppdrag
http://sambi.se/attributes/1/organizationIdentifier	Filtrering av Medarbetaruppdrag

Övriga attribut kommer att ignoreras.

Attributet *SAML Subject* kan användas för att förmedla Personidentifierare med samma påföljder som om PrincipalSelection används.

Endas ETT sätt ska användas för att förmedla Personidentifierare.
Endast ETT sätt ska användas för att förmedla OrganisationsIdentifierare.

4.4.6.4. Underskrift med flera kort

IdP stödjer signering med flera kort, exempelvis för att kvittera tillhandahållande av ett nytt SITHS-kort till en användare via SITHS eID Portal. För att hantera det här specialfallet görs ytterligare steg som skiljer sig från det normala signeringsflödet:

1. IdP skickar den tillhandahållna personidentifieraren som ska utföra signaturen till Autentiseringstjänsten.
2. IdP skickar en extra flagga vid autostarten av autentiseringsklienten för Windows för att signalera att samtliga kortens certifikat ska skickas till Autentiseringstjänsten. Det kompletta anropet för autostarten ser då ut som följer: siths://?autostarttoken=<uuid>**&multicard=true**. I normalfallet skickas endast certifikaten från kortet som sitter i den primära kortläsaren till Autentiseringstjänsten.
3. Autentiseringstjänsten tar senare emot samtliga istoppade kortens certifikat. Autentiseringstjänsten väljer då med hjälp av personidentifieraren som tillhandahållits av IdP:n ut vilket av korten och därmed vilket certifikat som signaturen ska slutföras med. I sitt svar till autentiseringsklienten för Windows skickar Autentiseringstjänsten med informationen om vilket certifikat som valts ut.

Möjligheten till att få nyttja underskrift flera kort konfigureras per SAML-anslutning och görs via IdP:ns administrationsgränssnitt.

4.4.6.5. Funktioner som inte stöds

Saml2 Scoping stöds inte.

```
<saml2p:Scoping>
        <saml2p:RequesterID>http://www.origsp.com/sp</saml2:RequesterID>
</saml2p:Scoping>
```

4.4.6.6. SignMessage

Attributet SignMessage kommer visas för användaren. Ingen formatering av meddelandet stöds, enbart plain text.

4.4.6.7. authenticationMessage

> Ska endast användas vid kritiska inloggningsmoment. Exempelvis när en användare eller ID-administratör gör en förnyad autentisering i samband med utfärdande av SITHS eID i SITHS eID Portal.

Attributet authenticationMessage kommer att visas för användaren i SITHS eID-appen. Ingen formatering av meddelandet stöd, enbart plain text.

Till skillnad från en signeringsbegäran kan authenticationMessage skickas in även när protokollet OIDC används. I dessa fall förmedlas meddelandet med claimet authenticationMessage.

När protokollet SAML används förmedlas meddelandet på samma sätt som vid en signeringsbegäran. Det vill säga med ett SignMessage extension.

5. Icke-funktionella krav

Denna information är låst och behörighetsstyrd. Åtkomst sker genom att expandera fältet nedan efter inloggning om du är behörig

Unable to render {include} The included page could not be found.

6. Teknisk lösning

Denna information är låst och behörighetsstyrd. Åtkomst sker genom att expandera fältet nedan efter inloggning om du är behörig

Unable to render {include} The included page could not be found.

7. Säkerhet

Denna information är låst och behörighetsstyrd. Åtkomst sker genom att expandera fältet nedan efter inloggning om du är behörig

Unable to render {include} The included page could not be found.

8. LoA administration

Denna information är låst och behörighetsstyrd. Åtkomst sker genom att expandera fältet nedan efter inloggning om du är behörig

SAD - LoA Administration

9. Informationshantering

9.1. Domäninformationsmodell

IdP har ingen egen domäninformationstabell.

9.2. Informationens ursprung

9.2.1. Information som konsumeras

Information om egenskaper som förmedlas via IdP hämtas från nationell eller regional kataloger. Informationen hämtas från HSA via definerade tjänstekontrakt se 1.4.2.

Information om identitet som förmedlas via IdP hämtas antingen från Katalogtjänst HSA eller från certifikat utfärdat av betrodd certifikatsutfärdare, såsom SITHS CA.

9.2.2. Information som skapas

Ingen information skapas utan paketeras enbart utifrån ovan nämnda källor.

10. Driftaspekter

Denna information är låst och behörighetsstyrd. Åtkomst sker genom att expandera fältet nedan efter inloggning om du är behörig

Unable to render {include} The included page could not be found.