1.3 SAD - Autentiseringstjänsten

Version	Datum	Författare	Kommentar
0.1	22 Mar 2022	Okänd användare (erikssonkr)	Kopierat SAD från version 1.2
0.2	03 May 2022	Ehlert, Stefan	Uppdaterat arkitekturdiagram
0.3	03 May 2022	Christoffer Johansson	Granskat och lämnat en kommentar i dokumentationsjiran ang. 5.2.2. Konfigurationsstyrning och om beskrivningen av hur vi kan styra biometri verkligen är fullständig.
1.0	05 May 2022	Christoffer Johansson	Godkänd av SITHS Förvaltning
2.0	17 May 2022	Ehlert, Stefan	Tillägg av beskrivningar för aktivering och autentisering med biometri som komplement till legitimeringskod
2.1	30 May 2022	Christoffer Johansson	Lade till detaljerade flöden för "Utfärdande samt kontroll av Legitimeringskod respektive biometri vid användning av Mobilt SITHS"
2.15	07 Jun 2022	Ehlert, Stefan	Tillägg av beskrivningar kring blockeringsmöjligheter för användning av biometri från backend.
2.2	05 Jul 2022	Christoffer Johansson	Tillägg för biometri godkänt av projekt och förvaltning.

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.
PKCS#11	Kryptografisk standard som definierar ett gränssnitt för hantering av kryptografiska nycklar.
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.
E-tjänst	System som erbjuder en funktionalitet för användare eller andra system.
IdP (Identity Provider)	Infrastrukturkomponent som använder olika metoder för att autentisera användare och förmedla ett identitetsintyg till e-tjänster som använder IdP för autentisering av användare. Ur Autentiseringstjänstens perspektiv agerar IdP en RP.
RP (Relying Party)	Ett system som förlitar sig på ett annat system för någon funktionalitet. Som exempel så kan en e-tjänst agera RP mot en IdP om e-tjänsten använder sig av IdP för autentisering av användare. Men IdP:n kan också i sin tur agera RP mot Autentiseringstjänsten.
SP (Service Provider)	Se begreppet e-tjänst ovan.
AT (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.
Katalogtjänst HSA	Användarkatalog. Datakälla för information om vårdpersonal, inklusive behörighetsinformation.

1.2. Syfte

Autentiseringstjänstens syfte är att möta e-tjänsters behov av att autentisera användare över multipla plattformar och operativsystem. Autentisering av användare kan nyttjas för såväl säker inloggning som för elektronisk underskrift.

Autentiseringstjänsten används tillsammans med en IdP och SITHS eID apparna för att förmedla en begäran om inloggning via en Säkerhetskanal som är separerad från informationskanalen, även kallat Out-of-band authentication.

Denna teknik ger ett mer enhetligt inloggningsförfarande över olika plattformar och möjliggöra också lagring av och inloggning med SITHS eID som lagras i Mobila enheter.

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	SITHS	https://www.inera.se/siths
P2	SITHS eID apparna	https://confluence.cgiostersund.se/x/MlYgDQ

1.4.2. Nyttjade tjänstekontrakt

Detta kapitel refererar till de tjänstekontrakt (API:er) som publiceras eller konsumeras av detta system. Autentiseringstjänsten använder enbart api:er som tillhandahålls av Utfärdandeportalen för Mobilt SITHS

Utfärdandeportal för Mobilt SITHS

För fullständig API-dokumentation, se: https://mobiltsiths.test.siths.se/openapi/swagger-ui/index.html?url=/v3/api-docs/

Dessa API:er används:

- internal-registration-controller

1.4.3. Styrande dokument

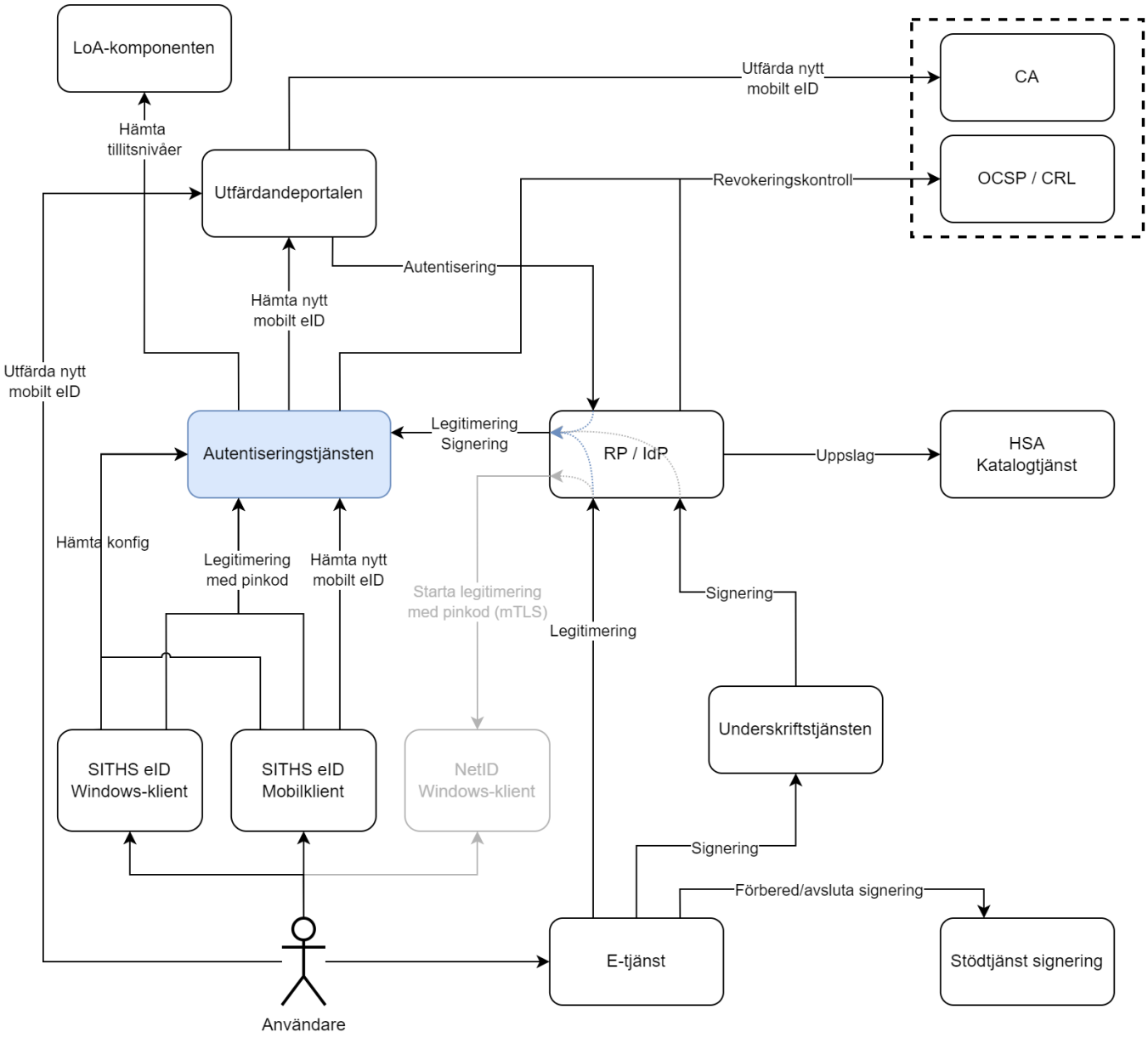
Ref	Dokument ID	Dokumentlänk
S1	Webauthn	https://w3c.github.io/webauthn/
S2	FIDO	https://fidoalliance.org/overview/
S3	W3C	https://www.w3.org/
S4	webauthn4j	https://github.com/webauthn4j/webauthn4j
S5	Registrering	https://developers.yubico.com/WebAuthn/WebAuthn_Developer_Guide/WebAuthn_Client_Registration.html
S6	Autentisering	https://developers.yubico.com/WebAuthn/WebAuthn_Developer_Guide/WebAuthn_Client_Authentication.html
S7	ARK_0046	Referensarkitektur - Identitet och åtkomst

1.4.4. Stödjande dokumentation

Ref	Dokument ID	Dokumentlänk
R1	RIV-TA	http://rivta.se/documents.html
R2	swagger	https://swagger.io/

2. Arkitekturell översikt

Bilden nedan visar en översikt över den del av infrastrukturen för Identitet och Åtkomst som är relevant för användning av Autentiseringstjänsten.



Autentiseringstjänsten använder sig av FIDO2 WebAuthn för att säkra att kommunikation mellan klient och server.
Vid en lyckad autentisering returneras användarens certifikat och metadata om inloggningen till anropande tjänst, typiskt en IdP.

IdP används för att:

- Starta inloggnings- och underskriftsuppdrag. IdP agerar här i rollen RP (Relying Party) mot Autentiseringstjänsten.
- Kommunicera med SITHS eID-klienterna för att koppla ihop sessionen mellan klient och AT med sessionen mellan IdP och AT. Detta sker antingen genom appväxling eller uppmaning till användaren om att skanna en QR-kod.

Utfärdandeportalen används för att:

- Skapa certifikatsbegäran vid utfärdande av nytt Mobilt SITHS eID
- Förmedla denna begäran till CA
- Leverera det nya certifikatet för vidare förmedling ner till SITHS eID Mobilklient via Autentiseringstjänsten.

SITHS eID klienterna används för att:

- Förmedla inloggnings- och underskriftsbegäran till användare

- Låta användaren signera inloggnings- eller underskriftsbegäran genom att låsa upp användarcertifikat med pinkod
- Leverera denna signerade begäran tillbaka till AT för vidare förmedling till IdP

SITHS eID Mobilklient används dessutom för att:

- Begära utfärdande av nytt Mobilt SITHS eID

OCSP- och CRL-tjänster hos certifikatsutfärdaren används för att:

- Utföra revokeringskontroller på användarcertifikat

2.1. Arkitekturella mål

- Säker och effektiv autentisering över flera olika plattformar, inklusive mobila enheter, som ett alternativ till Mutual TLS
- Följsamhet mot FIDO2 WebAuthn.
- Följsamhet mot Ineras Referensarkitektur.

2.2. Prioriterade områden

- Använda etablerade ramverk och tekniker.
- Använda standarder i största möjliga utsträckning.
- Stödja modulariserad driftmiljö(Paas).
- Undvika proprietära lösningar.

3. Följsamhet till T-boken

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 (REST) • Certifikatförmedlare (REST) Vid bortfall av externa system kan inte certifikat utfärdas men autentisering kommer fortfarande vara möjlig.
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 autentiseringstjänst. • 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.*	Anslutning för RP (IdP) 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.
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 • FIDO2 Webauthn

3.1.2. IT3: Nationell funktionell skalbarhet

Förutsättningar att uppfylla	***Uppfyllnad***
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.
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 Ineras driftsleverantör.
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: • Referensarkitektur för identitet och åtkomst [S7]

4. Användningsfall

4.1. Användningsfall - Översikt

AF	Dokument
AF1	Administrera Autentiseringstjänsten
AF2	Utfärda nytt mobilt SITHS eID
AF3	Registrera SITHS eID i Autentiseringstjänsten
AF4	Legitimering
AF5	Underskrift

4.2. Aktörsinformation

Ej sammanställt

4.3. Logisk realisering av signifikanta användningsfall

4.3.1. AF1 – Administrera Autentiseringstjänsten

4.3.1.1. Textuell beskrivning

Autentiseringstjänsten har en tillhörande administrativ komponent. Exmpelvis kan man i denna konfigurera vilka Relying Partys/IdP:er som tillåts använda Autentiseringstjänsten.

4.3.1.2. Realisering

En aktör med behörighet vill administrera Autentiseringstjänsten.

1. Aktören loggar in i tjänsten, och en förutsättning är att aktören på förhand är registrerad som behörig med sitt Person-ID
2. Aktören är inloggad och utför den tilltänkta administrationen.
3. Aktören loggar ut ur tjänsten.

4.3.2. AF2 – Utfärda nytt mobilt SITHS eID

4.3.2.1. Textuell beskrivning

En användare vill utfärda (beställa och ladda ner) ett Mobilt SITHS eID till sin mobila enhet.

4.3.2.2. Realisering

Se SAD - Utfärdandeportalen, SAD - SITHS eID-app för Windows och Användarhandbok - SITHS eID Mobilklient för information om detta användningsfall.

4.3.3. AF3 – Registrera SITHS eID i Autentiseringstjänsten

4.3.3.1. Textuell beskrivning

Innan SITHS e-legitimation på kort kan användas för att utföra legitimering eller underskrift mot Autentiseringstjänsten behöver certifikaten registreras. Denna process sker automatiskt för Mobilt SITHS i samband med utfärdandet eller vid användning om certifikatet av någon anledning skulle ha fallit bort ur databasen.

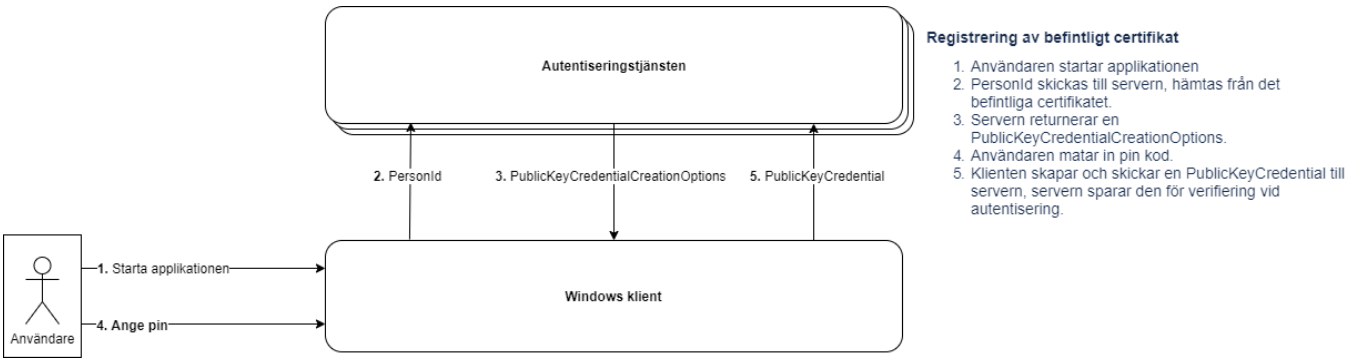
4.3.3.2. Realisering

1. Användaren startar klienten eller laddar om huvudsidan.
2. Klienten hämtar och validerar signerad konfiguration ifrån Autentiseringstjänsten.
    a. Om det rör sig om SITHS e-legitimation på kort måst Användaren till se att det smarta kortet sitter i kortläsaren.
3. Klienten kontrollerar sitt/sina Credential IDs mot Autentiseringstjänsten.
4. Om Autentiseringstjänsten saknar ett eller flera SITHS eID och därmed kräver registrering, uppmanas användaren att mata in legitimeringskod för att utföra registreringen.
5. Klienten använder de upplåsta certifikaten för att utföra registrering mot Autentiseringstjänsten.

Diagrammet nedan visar registreringsflödet:

- Kommunikationen mellan klienten och Autentiseringstjänsten i punkt 3 och 5 följer FIDO2 WebAuthn Client Registration. Dessa resulterar i att klienten levererar en PublicKeyCredential som Autentiseringstjänsten sparar. PublicKeyCredential innehåller bland annat användarens certifikat samt ett unikt credentialId som är härlett utifrån certifikatet.

Anropen i steg 3 och 5 i figuren nedan följer och



4.3.4. AF4 - Legitimering

4.3.4.1. Textuell beskrivning

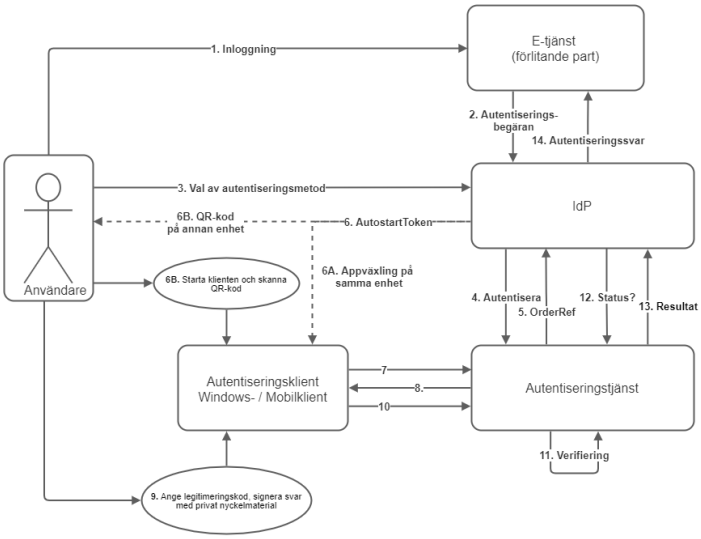
Användaren vill autentisera sig med eID som är registrerat hos Autentiseringstjänsten enligt ovan.

4.3.4.2. Realisering

1. Användaren efterfrågar tillgång till en Tjänst (t.ex. klickar på webblänk).
2. Användaren blir omdirigerad mot IdP/RP
3. Beroende på hur Tjänsten konfigurerats får antingen Användaren välja eller så väljer IdP:n automatiskt mellan inloggning med SITHS eID på **samma** eller **annan** enhet
    a. Samma enhet - autostart-token förmedlas via appväxling.
        i. **OBS!** För SITHS eID Windowsklient fungerar endast denna metod
    b. Annan enhet - autostart-token förmedlas via inskanning av QR-kod
4. Efter valet startar IdP/RP ett uppdrag mot Autentiseringstjänsten som i sin tur returnerar en OrderRef som kan användas för att begära status på begär legitimering/underskrift och en autostart-token som måste inkomma i anropet från SITHS eID-app till autentiseringstjänsten för att öka sannolikheten att det är samma användare som startat legitimerigen som också genomför den.
5. Klienten måste öppnas, vilket kan ske olika beroende på vilken metod som väljs
    a. Samma enhet - Automatisk via appväxling
        i. Om flera kort finns anslutna till datorn vid användning av SITHS eID Windowsklient väljs ett av dessa som aktivt, annars används det kort som är valt sedan tidigare - användaren kan själv välja aktivt SITHS eID
    b. Annan enhet - Manuellt av Användaren
6. Användaren uppmanas att ange sin legitimeringskod för att låsa upp certifikatet när:
    a. klienten är startad
    b. har en autostart-token dvs. en begäran om legitimering/underskrift som hämtats från Autentiseringstjänsten,
    c. har ett godkänt och giltigt certifikat för aktuell autostart-token. Begäran via autostart-token kan filtreras på:
        i. Godkända certifikatsutfärdare för att styra accepterad tilltsnivå
        ii. Person-ID
        iii. Valet av godkänt certifikat görs av Autentiseringstjänsten
7. Användaren matar in legitimeringskod och klienten utför legitimering.
8. Legitimeringsflödet fortsätter via IdP som utfärdar ett Identitetsintyg
9. Identitetsintyget för medlas tillbaka till Tjänsten där användaren efterfrågade tillgång
10. Tjänsten avgör om användaren beviljas eller nekas tillgång till Tjänsten.
11. Användningsfallet avslutas

Diagrammet nedan visar flödet vid Legitimering:

- Klientens del i flödet startar i steg 6 när IdP förmedlar en autostarttoken till klienten, antingen via appväxling eller via en QR-kod.
- För Windowsklienten sker förmedling av autostarttoken alltid m.h.a. appväxling (steg 6A).
- Kommunikationen mellan klienten och Autentiseringstjänsten i steg 8 och 10 följer FIDO2 WebAuthn Client Authentication.



1. Användaren väljer att logga in i E-tjänst. E-tjänsten är sedan tidigare kopplad till legitimeringstjänsten IdP för autentisering av användare via SAML2 eller OpenID Connect.

2. En autentiseringsbegäran på viss tillitsnivå skickas till IdP (Anropet går över användarens user agent).

3. Användaren väljer bland de autentiseringsmetoder som konfigurerats för e-tjänsten. För SITHS eID kan autentiseringen ske antingen på samma enhet som användaren har för kommunikation med e-tjänsten, eller en annan (mobil) enhet.

4-5. IdP skickar en autentiseringsbegäran till Autentiseringstjänsten inkl. krav på certifikatsutfärdare (tolkat utifrån begärd tillitsnivå), samt eventuellt krav på användaridentifierare (t.ex. personnummer). Autentiseringstjänsten returnerar en slumpmässig referens (OrderRef) till autentiseringbegäran samt en slumpmässig AutostartToken.

6. IdP förmedlar AutostartToken till Autentiseringsklienten, antingen via appväxling på samma enhet (6A) eller via inskanning av QR-kod på annan enhet (6B).

7. Autentiseringsklienten initierar ett autentiseringsflöde och skickar med AutostartToken till Autentiseringstjänsten, tillsammans med en lista över tillgängliga certifikat, identifierade med credentialId
    Autentiseringstjänsten verifierar att AutostartToken kan knytas till en aktiv autentiseringsbegäran.
    Autentiseringstjänsten väljer ett av de tillgängliga certifikaten att använda för autentisering. Listan från klienten filtreras utifrån den lista av certifikatsutfärdare samt eventuell användaridentifierare som IdP förmedlade i den initiala autentiseringsbegäran. Är ingen användaridentifierare angiven från IdP väljs certifikat utifrån typ av användaridentifierare på certifikatet, med prioriteringen: personnummer > samordningsnummer > HSA-id. Finns sedan flera certifikat med samma identifierare så väljs det första av dessa.

8-10 Autentiseringsförfarande enligt FIDO2 Web Authentication API (webauthnAPI) med SITHS-certifikat och svar signerat med användarens privata nyckel.
    8. Autentiseringstjänsten returnerar en slumpmässig utmaning till Autentiseringsklienten att signera med användarens privata nyckelmaterial (FIDO2 publicKeyCredentialRequestOptions-objekt), tillsammans med credentialId för det certifikat som skall användas.
    9. Användaren uppmanas att ange sin legitimeringskod i Autentiseringsklienten. Autentiseringsklienten skapar ett svar på utmaning och signerar med det privata nyckelmaterialet (FIDO2 publicKeyCredential-objekt)
    10. Signerat svar skickas till Autentiseringstjänsten (FIDO2 publicKeyCredential-objekt)

11. Autentiseringstjänsten verifierar det signerade svaret (FIDO2 publicKeyCredential-objekt) och kontrollerar mot tidigare registrerat data. Autentiseringstjänsten kontrollerar certifikatets giltighet, att utfärdaren är betrodd och att det inte är spärrat (OCSP).

12. IdP pollar status för autentiseringbegäran hos Autentiseringstjänsten med hjälp av OrderRef

13. När autentiseringen är slutförd returneras användarens certifikat till IdP

14. IdP kontrollerar certifikatets giltighet, att utfärdaren är betrodd och att det inte är spärrat (OCSP), samt att det uppfyller begärd tillitsnivå.

15. Vid lyckad autentisering returnerar IdP ett autentiseringssvar till E-tjänsten innehållande ett signerat ID-intyg. Vilka attribut som intyget innehåller avgörs av vad e-tjänsten har konfigurerats för och vad som är tillgängligt i den till IdP kopplade attributkällan (ej medtagen i detta flöde).

4.3.5. AF5 - Underskrift (Legitimering för Underskrift)

4.3.5.1. Textuell beskrivning

Användaren ska kunna använda SITHS e-legitimation för att elelktroniskt underteckna information (ex. dokument) via Underskriftstjänsten

4.3.5.2. Realisering

Anropsflödet är i stort sett identiskt för Underskrift och Legitimering, se diagrammet i **AF4 - Legitimering** ovan.

Det som skiljer dessa två användningsfall är att i samband med angivelse av legitimeringskoden kommer appen förutom att visa upp vilken tjänst som begär underskrift även visa ett Underskriftsmeddelande, som talar om vilken information Användaren skriver under. Detta görs som en bekräftelse till Användaren för att undvika tveksamheter om vad man skriver under.

Meddelandet kommer från IdP / RP i steg 4 ovan, och förmedlas till klienten i steg 8.

5. Icke-funktionella krav

Denna information är låst åtkomst sker via länken nedan som kräver inloggning.

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

6. Teknisk Lösning

Denna information är låst åtkomst sker via länken nedan som kräver inloggning.

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

7. Säkerhet

Denna information är låst åtkomst sker via länken nedan som kräver inloggning.

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

8. Informationshantering

8.1. Domäninformationsmodell

Autentiseringstjänsten har ingen egen domäninformationsmodell

8.2. Informationens ursprung

8.2.1. Information som konsumeras

All information som behandlas i systemet kommer ifrån användarcertifikatet förmedlat av anslutna klienter, samt via autentiseringsanrop från IdP/RP för legitimering och underskrift.

8.2.2. Information som skapas

Ingen information skapas i systemet.

9. Driftaspekter

Denna information är låst åtkomst sker via länken nedan som kräver inloggning.

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