Utredning
Framtida SITHS eID-bärare

Publik version

240308 -241231

inera
Ett företag inom SKR

Innehållsförteckning

1 Bakgrund & syfte

1.1 Bakgrund till utredningen

Inera har infört en ny tjänst för eID-utfärdande vilken ersatt den tidigare tjänsten SITHS omfattande nya lösningar för SITHS-komponenterna autentisering, CA/spärr, eID-administrationsportal och eID-bärare (kortproduktion).

Då dagens SITHS eID-bärare har funnits med i stort sett samma funktion sedan 2005 har det i samband med detta arbete utretts hur bärarutbudet kan vidareutvecklas. Resultatet av utredningen presenteras i denna rapport.

1.2 Syfte, omfattning och avgränsningar

Genomförandet av utredning avseende framtida bärare som förberedelse inför kommande upphandling av eID-bärare har utförts under perioden februari 2024 till december 2024.

Beslutsunderlaget skulle enligt uppdragsdirektivet omfatta:

1. Genomförande av kartläggning och prioritering av kundernas behov avseende framtida eID-bärare. Kravanalys sammanställd samt förankrad med referensgrupp samt andra relevanta forum (exempelvis regionernas och kommunernas arkitekturråd)
2. Utvärdering av alternativa standarder samt tekniska lösningar vilka kan realisera kravbilden i samverkan med marknadsaktörer (RFI) samt kunder.
3. Prioritering samt sammanställning av rekommendation avseende möjliga lösningar. Viktigt att säkerställa bred uppslutning då dessa löningar kommer leva under lång tid och ska möta huvuddelen av kundernas behov
4. Framtagning av förslag på övergripande färdplan samt möjlig införandeplan. Förankras med referensgruppen samt i andra relevanta forum.
5. Förslag på möjlig omfattning avseende framtida leveransavtal för produktion av framtida bärare samt därtill hörande tekniska lösningar utgående från kravställning.
6. Underlag för beslut avseende sourcinginriktning för leveransavtal för framtida bärare och relaterade tekniska lösningar. Omfattar förslag på:
    - Prioriterade utvecklingsbehov relaterat till bärare
    - Lösningsförslag som realiserar prioriterade behov
    - Förslag på färdplan för införande av rekommenderade lösningar
    - Sourcingstrategi och möjligt upplägg för kommande upphandling
    - Beslutsunderlag till styrgrupp

Resultatet har redovisats för SITHS-styrgrupp 241213 och resultatet överlämnats till SITHS tjänsteförvaltning.

1.3 Avgränsningar

Följande avgränsningar gäller:

1. Utredningen omfattar ej framtagande av komplett upphandlingsunderlag utan är avsett att vara ett planeringsunderlag.
2. Utredningen omfattar ej genomförande av upphandling. Detta beslutas och finansieras i ett senare läge.
3. Beslutsprocess avseende fortsatt arbete hanteras av SITHS tjänsteförvaltning.

1.4 Förankring av resultat

Löpande förankring av resultaten har skett mot ett antal grupperingar. Utöver den externa arbetsgruppen, bland annat kan nämnas: Projektets styrgrupp, SITHS PA-grupp, Referensgruppen för Ny Lösning SITHS-projekten, kommunernas och regionernas arkitekturråd, Klas Nilsson på SKR (arbetar med digitaliseringsfrågor mot regioner och kommuner) samt slutligen SITHS-dagen november 2024.

1.5 Rekommendationer

Rekommendationen medan beskriver vilka bärare och lösningar som föreslås införas samt hur detta kan ske.

1.5.1 Rekommenderade bärare och lösningar

Utredningen rekommenderar att utöka SITHS-tjänsten med följande bärare:

1. Ett **nytt smartkort** som är en vidareutveckling av befintligt SITHS-kort.
   Smartkortet förses med stöd för:
   - Kontaktlös tvåfaktorsautentisering via FIDO2 [R2] över NFC [R3].
   - Certifikatsbaserad autentisering (PKI) med dagens kortprofil för kontaktbaserad tvåfaktorsautentisering, inklusive autentisering via dubbelriktad TLS.
   - MIFARE DESFire för fysisk åtkomst [R10]
     - Kortet förses med en basprofil för MIFARE DESFire vid dess personalisering i fabriken, inklusive applikation, tillhörande filer och nyckeluppsättning.
     - Möjlighet att organisationen vid behov kan lägga till egna och leverantörspecifika applikationer och nycklar.
     - Det rekommenderas även att utvärdera möjligheten att lägga på emulerad MIFARE Classic via DESFire EV3C-teknik. MIFARE Classic skall då vara kodad på samma sätt som dagens SITHS-kort och möjliggöra bakåtkompatibilitet.
2. En **säkerhetsnyckel** med stöd för:
   - Kontaktlös och kontaktbaserad tvåfaktorsautentisering via FIDO2 över NFC respektive USB-C.

De nya bärartyperna införs primärt för att möjliggöra e-legitimering och e-underskrift med SITHS eID i applikationer vid användning av:

- **Delade mobila enheter** som har inbyggd NFC-läsare (smartkort eller säkerhetsnyckel) alternativt USB-kontakt (säkerhetsnyckel)

- **Delade datorer** som har NFC-läsare (smartkort eller säkerhetsnyckel) eller USB-kontakt (säkerhetsnyckel)
- **Personlig dator** som har USB-kontakt (säkerhetsnyckel) alternativt NFC-läsare (smartkort eller säkerhetsnyckel)

För att ge stöd för de nya bärarna i SITHS-tjänsten rekommenderas att implementera följande funktioner:

1. **Stöd för nytt smartkort i beställningsflödena** för SITHS ordinarie kort, reservkort och testkort
2. **Stöd för beställning av säkerhetsnycklar i bunt** med leverans till utgivningskontor
3. **Artikelhantering och fakturering för de nya bärarna** i SITHS eID Portal samt Kundportalen
4. **Anpassning av gränssnitten i SITHS eID Portal och Mina Sidor** för de nya bärarna
5. **Stöd för att aktivera FIDO2-delen för en SITHS-bärare på distans**. Utformningen av aktiveringen behöver ta hänsyn till de nya planerade flöden för utgivning av SITHS eID inom ramen för initiativet Förenklad utgivning av SITHS eID
6. **Stöd för externa FIDO2-bärare i SITHS eID-apparna och Autentiseringstjänst SITHS**, kontaktlöst respektive kontaktbaserat
7. **Hantering av spärr och upplåsning av FIDO2-bärare**
8. **Automatiserad hantering av nycklar för MIFARE DESFire**. Funktion i SITHS eID Portal för ansvariga utgivare för att på ett säkert sätt kunna hämta nödvändiga nycklar för MIFARE DESFire

Utredningen rekommenderar vidare att utreda möjligheten att införa följande bärare och funktioner i SITHS-tjänsten:

- Användning av **mobilen för fysisk åtkomst**, dvs. för inpassage, upplåsning, follow-me-print-lösningar och liknande.
    - Realiseras förslagsvis som en självservicefunktion i SITHS Mina sidor som medger utfärdande av ett personaliserat virtuellt kort för MIFARE DESFire.
    - I ett sådant arbete bör även bevakas utvecklingen och kommande stöd för standarden Aliro [R6] som alternativ teknik till MIFARE DESFire.
- Bärare med **inbyggd biometrisk autentisering**
    - Utreda möjligheten att anskaffa bärare med inbyggd fingeravtryckssensor. Detta kan avse säkerhetsnyckeln och/eller smartkortet enligt ovan.
    - Utreda kostnader, juridiska aspekter och tillgänglighet för bärare med inbyggd biometrisk autentisering som också möter övriga krav i SITHS.
    - SITHS eID-apparna behöver förses med stöd för att kunna registrera och nyttja biometri för autentisering som alternativ till legitimeringskoden.

1.5.2 Förslag på färdplan

Utredningen rekommenderar att genomföra följande steg för realisering av föreslagna bärare och funktioner:

1. **Inled beslutsprocess** om införande av rekommenderade bärartyper inklusive anpassning av berörda tjänster samt appar. Utred även erforderlig **finansiering** (Inera bekostar alternativt intresseanmälan).
2. **Fatta inriktningsbeslut vad gäller vidareutveckling av SITHS bärare:**
    - Fastställ långsiktig målbild
    - Besluta på vilket sätt som arbetet framöver ska bedrivas
    - Se över kostnadsberäkningar
3. **Etablera organisation för genomförande samt säkerställ resurser**
4. **Genomför "Proof of Concept" av nytt smartkort** i samverkan med kunder.
5. **Planera genomförandet** samt ta fram beslutsunderlag omfattande projektplan
6. **Besluta att införa nytt smartkort med stöd för PKI samt kontaktlöst DESFire och FIDO2-teknik**. Beslut fattas baserat på resultat av POC.
7. **Besluta om införande av säkerhetsnyckel** med stöd för kontaktlös samt kontaktbaserad tvåfaktorsautentisering med stöd i SITHS eID-appen.
8. **Genomför upphandling avseende produktion av bärare**.
9. **Besluta om införande av stöd för FIDO2 i SITHS eID-appar** Omfattar e-legitimering samt e-underskrift på följande enheter**:**
    - **personlig dator** med USB alternativt NFC-läsare
    - **delade datorer** med USB alternativt NFC-läsare
    - **delade mobila enheter** med USB eller inbyggd NFC-läsare
10. **Genomför översyn av prissättning för att ta hänsyn till nya funktioner.**

1.5.3 Fortsatt arbete, övriga åtgärder

Förutsatt att beslut fattats om inriktning och fortsatt genomförande av arbete avseende nya bärare, rekommenderar arbetsgruppen att följande övriga åtgärder genomförs:

1. **Genomför fortsatt förankring** av rekommenderad inriktning (ledningsnivå samt fördjupad), arkitekturråd, PA-gruppen, SLIT
2. **Genomför fältstudie i samverkan med utvalda kunder avseende ny korttyp** som utöver dagens funktioner även omfattar beröringsfri teknik (FIDO2) samt MIFARE DESFire. Dialog har förts med leverantören av dagens bärare och det bedöms vara möjligt att inom ramarna för nuvarande kortavtal leverera smartkort för teständamål.
3. **Genomför juridisk utredning inom följande områden:**
    - Användning och lagring av biometri vid autentisering. Genomförs av Inera, eventuellt i samverkan med SKR avseende användning och lagring av biometri vid autentisering för ett antal utvalda användningsfall som är intressanta för regioner och kommuner, exempelvis vid användning av Windows Hello och ansiktsigenkänning vid inloggning till Windows.
    - Sammanställ Ineras riktlinjer för hur biometri kan hanteras inom SITHS-tjänsten.

4. **Ta referenser på ny teknik och lösningar** som beslutas vara prioriterade att gå vidare och implementera inom ramarna för SITHS-tjänsten.
5. **Fastställ slutdatum för tillhandahållande av MIFARE Classic teknik i SITHS bärare** samt kommunicera vid lämpligt tillfälle.
6. **Genomför kompletterande sourcinganalys inför start av upphandling** givet de förutsättningar som råder vid tidpunkten.
7. **När pågående utredningar avseende RPA är avslutade,** utred om föreslagna bärare och lösningar påverkas.
8. **Utred lämplig kravställning av kvantsäkra kryptoalgoritmer** (*Post-Quantum Cryptography*) som Inera borde tillämpa på lösningar och avtal framöver.
9. **Bevaka utveckling av Digital plånbok** och samverkan med SITHS bärare.

1.6 Behov som ej bedöms möjliga att realisera

Följande behov samt funktioner har utretts men ej bedöms vara möjliga att realisera under de närmaste åren. Detta beror dels på att de bäst löses i andra delar av infrastrukturen, alternativt ej ännu är allmänt tillgängliga på marknaden.

Inom följande områden bedöms ej en lösning baserad på bärare går att införa i närtid:

- Närvaroavkänning för låsning av session
- Personlig dator med TPM som eID-bärare för SITHS eID-app (Windows & Mac)
- Användning av SITHS eID inom ramen för Windows Hello för Business
- Säkerhetsnyckel med stöd för inpassering via SITHS eID PKI
- SITHS eID PKI stödjs på säkerhetsnyckel
- Använda bäraren för RPA, separat utredning pågår

Inom följande område är lösningen ej relaterad till bäraren:

- SSO-upplevelse, flera olika krav
- Logga in i **mobilens operativsystem**. Säker ”Blipp” med tvåfaktorsautentisering (kod) mot den mobila enheten för att logga in i enheten (operativsysteminloggning)

1.7 Referenser

[R1]	Referensarkitektur för Identitet och åtkomst https://www.rivta.se/documents/ARK_0046/
[R2]	FIDO2 (Fast Identity Online) Standard för säker autentisering på internet baserad på publika nycklar och asymmetrisk kryptering. https://fidoalliance.org/fido2/
[R3]	Närfältskommunikation, NFC https://sv.wikipedia.org/wiki/Närfältskommunikation

[R4]	X.509-certifikat https://en.wikipedia.org/wiki/X.509
[R5]	Biometriska uppgifter i arbetslivet, https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/arbetsliv/biometri/
[R6]	Connectivity Standards Association https://csa-iot.org
[R7]	European Digital Identity Framework, eIDAS https://www.eid.as
[R8]	European Telecommunications Standards Institute, ETSI https://www.etsi.org/
[R9]	MIFARE https://www.mifare.net

1.8 Terminologi

Term	Beskrivning
BTV	För varje tjänst som omfattas av ett kundavtal för en tjänst finns ett dokument som beskriver de villkor som är specifika för just den tjänsten. Dokumentet heter Beskrivning och tjänstespecifika villkor och förkortas ofta BTV
Digg	Myndigheten för digital förvaltning
ITU	Inera Test och Utveckling
Legitimeringstjänst, IdP	Tjänst i IT-infrastrukturen som utför identifiering och autentisering av användare på begäran av en e-tjänst. Legitimeringstjänsten utfärdar vid godkänd legitimering ett identitetsintyg till e-tjänsten med begärda uppgifter om en autentiserad användare.
MIFARE	Kontaktlös autentiseringsteknik för primärt fysisk åtkomst såsom till exempel inpassering. Det finns flera varianter av MIFARE-tekniken som ”Classic”, ”DESFire” osv.
PKCS	Public Key Cryptography Standards En svit av standarder kring kryptografi baserat på publika nycklar.
PKI	Public Key Infrastructure En infrastruktur baserat på publika kryptonycklar. Oftast avses tillämpning med certifikat och certifikatsutfärdare.

Postkvantkryptografi	Post-quantum cryptography, PQC. Kvantsäkra kryptografiska algoritmer som anses vara säkra mot en kryptoanalytisk attack av en kvantdator.
RPA	Robotic process automation handlar om att automatisera (robotisera) vissa arbetsflöden, typiskt sådant som är repetitivt.
Single Sign-on (SSO)	Singelinloggning - en användare behöver endast logga in en gång för att nå de system som är anpassade till funktionen.
SITHS	Identifieringstjänst SITHS är en elektronisk identitetshandling som används för säker identifiering av både personer och system inom regioner, kommuner, privata vårdgivare och statliga myndigheter.
SITHS eID	SITHS e-legitimation vilken är godkänd enligt det statliga kvalitetsmärket Svensk e-legitimation på tillitsnivå 3 (se Myndigheten för digital förvaltning).
SITHS eID Portal	Administrativ portal för utgivning av SITHS eID och tillhörande bärare.
SITHS Mina sidor	Webbgränssnitt för SITHS självservice-funktioner för medarbetare.
Tillitsnivå	(här) Gradering av säkerhet när det gäller teknisk och administrativ säkerhet och hur tillförlitlig en e-legitimation är utifrån den aktuella nivån. Tillitsnivå förkortas ofta LoA (Level of Assurance).
Virtualiseringsplattform	Plattform som hanterar åtkomst till virtuella skrivbord (VDI) och/eller publicerade appar.

2 Behovsanalys

Utredningen inleddes med genomförande av en behovsanalys i samverkan med den externa arbetsgruppen.

2.1 Regioner

2.1.1 Vidmakthålla befintlig funktionalitet

Vid analys av behov kring framtida bärare för SITHS eID, är det inte minst viktigt att lyfta fram befintlig funktionalitet inom SITHS som behöver vidmakthållas även med nya eller vidareutvecklade bärartyper.
De viktigaste befintliga funktionerna som lyfts i analysen är:

- E-legitimering genom tvåfaktorsautentisering upp till tillitsnivå 3 enligt tillitsramverket för Svensk e-legitimation.
- E-underskrift genom tvåfaktorsautentisering upp till tillitsnivå 3 enligt Digg's specifikation för e-underskrift.
- Inpassage till fastigheter med kontaktlös teknik. Idag kan SITHS-kortet fungera som en autentiseringsfaktor kopplad till kortinnehavaren. Ytterligare faktorer, som till exempel en personlig kod, kan efter behov läggas till i lokala system.
- Öppnande av lås, med samma teknik som för inpassage (1-faktors autentisering från bäraren).
- Säkra utskrifter (follow-me-print), med samma teknik som för inpassage (1-faktors autentisering från bäraren).
- Multifunktionella bärare. Medarbetare ska kunna använda en och samma bärare för e-legitimering, e-underskrift och inpassage/upplåsning/säkra utskrifter. Detta behöver stödjas av minst en bärartyp för SITHS.
- Bärare för SITHS ska kunna användas för lokalt utfärdande av SITHS eID till medarbetare med kort varsel, till exempel till medarbetare som förlorat eller inte har med sig sin ordinarie SITHS-bärare. Idag används primärt SITHS reservkort för detta.
- Möjlighet till fysisk legitimering i tjänsten med foto och namn. Detta behöver stödjas av minst en bärartyp för SITHS.
- Säker inloggning till datorer med SITHS eID (operativsysteminloggning). Idag stöds detta genom certifikatsbaserad inloggning med SITHS-kort. De organisationer som nyttjar detta idag använder det främst på datorer med Windows.
- Kunna rengöra och desinficera bäraren för SITHS eID så att det blir möjligt att medföra bäraren till miljöer med höga krav på hygien. Detta gäller primärt användning inom vård- och omsorg, men då gränsdragningar kan vara svåra, har arbetsgruppen sett detta som ett skallkrav på bärarna.

2.1.2 Kontaktlös tvåfaktorsautentisering

Att kunna använda kontaktlös (även kallad beröringsfri) tvåfaktorsautentisering för SITHS eID har lyfts fram som ett högt prioriterat behov, framför allt för att stödja säker delning av enheter (datorer, mobiler osv) mellan medarbetare.

Två olika primära användningsfall har lyfts fram där kontaktlös tvåfaktorsautentisering för SITHS skulle ge ökad verksamhetsnytta:

- Medarbetare som använder flera olika gemensamma datorer/terminaler under sitt arbetspass, och loggar in, låser session och loggar ut många gånger per dag.
- Medarbetare som använder mobila enheter som är delade mellan användare.

2.1.3 Kontaktlös autentisering vid delade datorer

I detta användningsfall används typiskt en stationär datormiljö där klientdatorn används i s.k. kioskläge, dvs. användaren behöver inte logga in i klientens operativsystem. Medarbetaren använder en valfri enhet och autentiserar sig mot en virtualiserad miljö, för att få åtkomst till hens virtuella skrivbord och/eller publicerade appar.

Behovet är här fokuserat på att göra det smidigare och snabbare för medarbetarna att med bibehållen säkerhetsnivå (tillitsnivå 3) autentisera sig med SITHS eID. Målbilden är att medarbetaren ska kunna blippa bäraren mot en kontaktlös läsare och ange sin personliga legitimeringskod för snabb autentisering på valfri enhet. Medarbetare behöver här kunna legitimera sig i samband med att en ny session etableras, men även för att återansluta till en låst session.

Även e-underskrifter behöver kunna stödjas kontaktlöst i de tillämpningar där det förekommer.

2.1.4 Kontaktlös autentisering vid delade mobila enheter

I detta användningsfall används typiskt icke personliga mobiler eller läsplattor som tillhandahålls av arbetsgivaren. Dagens lösning för Mobilt SITHS är mest lämpad för personliga enheter då utfärdandet binder enheten och det SITHS eID den lagrar till medarbetaren. Att hämta ett nytt SITHS eID för en annan medarbetare som ska ta över enheten från den första är relativt tidskrävande, och rutinen bedöms svår att väsentligen förenkla med bibehållen tillitsnivå.

Medarbetaren behöver hämta ut en enhet i början av hens arbetspass, eventuellt flera gånger under en arbetsdag, för att sedan lämna tillbaka enheten så att någon annan kan använda den.

Behovet är här fokuserat på att möjliggöra en säker autentisering med SITHS eID på tillitnivå 3, trots att den mobila enheten är delad och icke personlig. Målbilden är att medarbetaren ska kunna blippa bäraren mot enheten och ange sin personliga legitimeringskod för autentisering med SITHS eID mot mobila nativa och webbaserade appar.

2.1.5 Logga in i mobilens operativsystem

Det finns även önskemål att kunna använda SITHS eID för säker inloggning till den mobila enheten, dvs. inloggning i mobilens operativsystem. Särskilt vid delade enheter vore det önskvärt att helt kunna separera användarprofiler med en säker inloggning med SITHS eID.

2.1.6 Låsning av session

Vid användning av delade datorer finns behov att på ett enkelt och intuitivt sätt kunna lämna en klientdator i låst läge och vara trygg med att inte någon annan kan ta över hens session. Ju mer intuitivt och enkelt det är att låsa, desto större sannolikhet att användarna faktiskt låser sessionen när de lämnar datorn.

2.1.7 Närvaroavkänning

I analysen lyftes även ett önskemål om bärare som ger stöd för automatisk närvaroavkänning, där klientdatorn automatiskt låses när användaren (egentligen bäraren) avlägsnar sig tillräckligt långt från datorn.

2.1.8 Bärare med standard USB-kontakt

En bärare för SITHS eID med USB-kontakt, är främst kopplat till följande behov:

- Kunna använda SITHS eID med delade läsplattor som vare sig har kortläsare eller kontaktlös teknik (NFC). Detta skulle ge större flexibilitet och potentiella kostnadsbesparingar i anskaffning av läsplattor. Kortläsare på mobila enheter är inget realistiskt alternativ på mobila enheter då det kräver dyra tredjepartslösningar.
- Kunna använda SITHS eID med datorer som varken har inbyggd kortläsare eller kontaktlös teknik (NFC). Detta kan ge större flexibilitet och potentiella kostnadsbesparingar i anskaffning av datorer och tillbehör. Bärartypen skulle till exempel kunna passa bra för administrativ personal som har personliga datorer. Det finns även kategorier av medarbetare som behöver använda flera SITHS eID-bärare samtidigt som skulle ha särskild nytta av denna typ av bärare.

2.1.9 Personlig dator som bärare

För organisationer som har ett stort antal personliga datorer har uttryckts önskan att kunna använda själva datorn som bärare för SITHS eID. Detta kan jämföras med Mobilt SITHS där den mobila enheten också utgör bärare av medarbetarens eID. Som medarbetare behöver jag ingenting annat än min arbetsdator för att med SITHS eID logga in i applikationer, göra e-underskrifter osv. Fokus är på användarvänlighet, enkelhet och snabbare autentisering.

2.1.10 Biometrisk autentisering

Ett annat önskemål är att kunna nyttja biometriska egenskaper för autentisering, för att medarbetarna ska slippa hantera och minnas koder. Även här är fokus på användarvänlighet, enkelhet och snabbare autentisering.

Idag finns möjlighet till biometrisk autentisering enbart för Mobilt SITHS (fingeravtryck eller ansikte), men inte för SITHS-kortet. Det ska tilläggas att biometrin i detta sammanhang snarare är ett alternativ till användarens personliga kod och inte en hel ersättning. Vid behov kan en medarbetare som aktiverat biometri via ett val, i stället använda sin kod när behov av det föreligger. Vi kan förutsätta att samma behov finns även för andra bärare som ska stödja biometri som en alternativ andra faktor vid e-legitimeringen.

Inom detta område har även lyfts önskemål om att kunna använda datorns inbyggda kamera och/eller fingeravtrycksläsare för att verifiera användarens biometri i samband med autentiseringen med SITHS eID. Tekniken används bland annat i Microsofts plattformslösning Windows Hello, men även i Apples plattformar.

2.1.11 Single Sign-on

Att för användaren undvika på varandra upprepade legitimeringar med SITHS eID under arbetspasset, dvs. en SSO-upplevelse, har lyfts som mycket efterfrågat. Målbilden är att användaren gör en legitimering vid öppnande av sessionen, och kan sedan starta och använda övriga applikationer utan upprepad legitimering under (del av) arbetspasset. Även lokal AD-inloggning önskas ingå i detta.

2.1.12 Modern och säker teknik för fysisk åtkomst

Ett starkt efterfrågat behov är att ersätta den nuvarande underliggande tekniken för fysisk åtkomst, dvs. inpassage till fastigheter, upplåsning av olika typer av lås och säkra utskrifter. Dagens SITHS-kort använder ett chip för kontaktlös autentisering med protokollet MIFARE Classic [R10], vilket behöver bytas ut till ett modernare och säkrare protokoll. Kan noteras att SITHS-kortet utgör här endast en autentiseringsfaktor knuten till innehavarens identitet. Denna faktor kompletteras där det finns utökat skyddsbehov med ytterligare faktorer i det lokala systemet, vanligast en personlig kod.

2.1.13 Mobil enhet för fysisk åtkomst

Inom området fysisk åtkomst efterfrågas även att kunna använda mobiltelefonen för beröringsfri blipp för inpassage, upplåsning och säker utskrift. Detta skulle vara ett steg mot att medarbetare endast behöver ha mobilen med sig för såväl e-legitimering som säker inpassage till lokaler osv. Idag behöver personalen som regel ett kort för inpassage, även om behovet av e-legitimering skulle kunna täckas med Mobilt SITHS.

2.1.14 Hantera övergången till ny teknik

En aspekt som alltid behöver beaktas vid införande av ny teknik är hur övergången kan hanteras och hur lång transitionsperioden förväntas bli.

Det finns flera utmaningar i övergången till ny teknik för fysisk åtkomst. De befintliga systemen för åtkomst till fastigheter, låsta skåp osv. har ofta långa livscykler och inte alltid möjlighet till uppgradering av dess programvara för att stödja andra protokoll. Det är därför viktigt att beakta:

- Befintliga system som inte i närtid kommer att kunna uppgraderas till ny teknik.
- En lång transitionsperiod kommer att vara nödvändig för många organisationer, för att helt gå över till en ny teknik för alla berörda fastigheter och system.

Det har även framhållits att det är viktigt att tidigt kommunicera vilken teknik som SITHS kommer att använda framöver för fysisk åtkomst. Detta för att kunna börja planera för och förbereda lokala system i samverkan med aktuella leverantörer.

När det gäller användning av SITHS eID på kort för legitimering behöver också beaktas att ett införande av en ny kontaktlös teknik behöver kunna göras successivt och tänkbart riktat till kategorier av medarbetare där det gör mest nytta. Det innebär också att det behöver finnas kvar möjligheten att använda kortet i kortläsare under överskådlig tid.

2.1.15 Stöd för RPA

Under denna utredning har även lyfts behov att kunna nyttja SITHS eID i lösningar för RPA (*Robotic Process Automation*). Utredningen har avgränsat sig från detta då förutsättningar och lösningar för RPA primärt hanteras i andra utredningar. Det är dock viktigt att ha med denna aspekt i kommande anskaffning av bärare för SITHS, så att inte bärartypen som sådan hindrar att användas i RPA-lösningar.

2.1.16 Icke funktionella krav

Förutom behov kring ny funktionalitet för SITHS, behöver tas hänsyn till ett antal icke funktionella krav, såväl kvalitativa som tekniska, i kommande anskaffningar av bärare. Några av dessa områden är

- Bäraren kan uppfylla alla säkerhetskrav för tillitsnivå 3. Det avser bland annat skyddet av nyckelmaterial, säkerhetsalgoritmer och säkra kommunikationsprotokoll.
  I kommande upphandling bör även tas ställning till kvantsäkra kryptoalgoritmer (*Post-Quantum Cryptography*) för att framtidssäkra skyddsnivån.
- Bäraren och dess tekniska förutsättningar ska kunna implementeras med rimlig insats i befintliga autentiseringslösningar för SITHS.
- De tekniska lösningarna för bäraren ska samverka i en arkitektur som följer Ineras Referensarkitektur för Identitet och åtkomst.
- Bäraren och dess autentiseringsteknik ska orsaka så liten fördröjning som möjligt för användaren.
- Bäraren kan användas i känsliga miljöer, såsom lokaler med medicinteknisk utrustning, och även vara tillräckligt tåliga för att kunna användas i miljöer som alstrar störningar.
- Bäraren ger möjlighet till autentisering lokalt vid avbrott till centrala tjänster (kan kräva lokala åtgärder).
- Bäraren kan användas på klientplattformarna som stöds av SITHS eID-apparna.
  Dessa är vid tidpunkten för denna rapports färdigställande: Windows, macOS, Android, iOS/iPadOS, Linux samt prioriterade plattformar för virtuella skrivbord och appar.

2.2 Kommuner

2.2.1 Inledning

SITHS har hittills spelat en avsevärt mindre roll i kommunal verksamhet än hos regionerna. Det har förstås sin naturliga förklaring i historiken med fokus på hälso- och sjukvård. Bara 3 procent av den kommunala verksamheten är hälso- och sjukvård. De stora sektorerna i kommunal verksamhet är skola och socialtjänst.

Ändå finns det kommuner som breddinfört SITHS. Intresset för SITHS ökar också efterhand som SVOD (Sammanhållen vård- och omsorgsdokumentation) och andra liknande initiativ möjliggör informationsutbyte mellan Hälso- och sjukvård och kommunal omsorg. Det finns även ett fåtal kommuner som har infört SITHS i skolförvaltningen. Det finns mycket att vinna på att använda samma infrastruktur över sådana sektorsgränser.

En annan viktig aspekt är att kommunerna i allmänhet har en mycket kärv ekonomi, ännu mer än vad som gäller för regionerna. Kommunernas storlek är starkt bidragande till det.

2.2.2 Delade enheter

Ett starkt behov för kommunerna är att underlätta för personal med delade enheter, inte minst inom hemtjänsten. Att kunna byta användare snabbt för en mobil enhet när ett nytt pass startar, och att kunna ha SSO så långt det är möjligt, är viktiga önskemål. Det löser man inte med valet av bärartyp, men tekniker som stöds och som underlättar denna hantering av delade enheter är viktiga för kommunerna.

2.2.3 Inpassering

Behoven av SITHS för inpassering är blandade när det gäller kommunal verksamhet. Man har väldigt många olika verksamheter och fastigheter med olika inpasseringssystem, som man anser är i princip omöjligt att samordna. Man har heller inte samma andel inpasseringar med hög säkerhet som regionerna (sjukvården) har.

Med det sagt så använder ändå några av de större kommunerna SITHS för inpassering. Där finns samma utmaningar med gammal teknik, dvs MIFARE Classic, som vi ser hos regionerna.

Även om kommunerna har färre andel inpasseringar med hög säkerhet, så finns de. Exempelvis har man produktion av dricksvatten och ibland infrastruktur såsom telekommunikation/fiber samt åtkomst till serverhallar.

2.2.4 Förenklad utgivning

Förenklad utgivning av SITHS eID lyfts ofta. Det ingår dock inte i det här projektet utan hanteras i ett annat projekt.

2.2.5 Teknikval

NFC är en möjlighet som kommunerna ser som intressant, även om man inte har en klar bild över möjliga användningsfall utöver delade mobila enheter i framför allt hemtjänsten, som nämnts ovan.

FIDO2 är en teknik som används alltmer i kommunsektorn och som man över lag ser som en teknik att satsa på framöver.

2.2.6 Kostnadsläget

Kommunerna är som bekant av väldigt varierande storlek. För att SITHS ska kunna bli en viktig del av kommunernas infrastruktur så är det avgörande att administrationen är rimligt hög och att prisbilden är gynnsam i förhållande till andra lösningar som inte bygger på SITHS. Helst vill man ha förutsägbara kostnader, dvs undvika modeller som bygger på tickkostnad.

2.2.7 Prioriterade användningsfall

Sammanfattningsvis är följande användningsfall de högst prioriterade ur ett kommunperspektiv:

- Kontaktfri autentisering vid delade mobila enheter
- Logga in i mobilens operativsystem
- Single Sign-on

3 RFI samt utvärdering av standarder och tekniska lösningar

3.1 Deltagare och genomförande

De större aktörerna verksamma i Sverige inom de områden som utredningen fokuserar har kontaktats för deltagande vid RFI. Leverantörerna har vid dialogmöten beretts möjlighet att informera om lösningar relaterade till behovsbilden. Som underlag har Inera tillhandahållit en sammanställning av identifierade behov kompletterat med ett antal specifika frågeställningar (samma för alla) vi önskade svar på.

Samtliga leverantörer erbjöds ett initialt möte om 2 timmar. I de fall behov förelåg bokades endera ytterligare ett möte för genomgång av resterande frågeställningar alternativt fördes skriftlig dialog avseende kompletteringar av de svar som lämnades vid dialogmötet.

Samtliga leverantörer har lämnat svar på de frågor som Inera ställt med undantag för frågor avseende lösningar som leverantören i fråga ej tillhandahåller.

Vid dialogmötena deltog den interna arbetsgruppen från Inera.

3.2 Analys av standarder och lösningar

3.2.1 Autentiseringsteknik för SITHS eID

Autentiseringsteknik för SITHS eID avser de tekniska protokoll samt tillhörande säkerhetsteknik som själva bäraren av eID stödjer. I e-legitimationssammanhang är det centralt att tekniken är asymmetrisk, dvs. att det finns en privat nyckel som aldrig lämnar bäraren, samt en publik nyckel som knyts till användaren i de tjänster som behöver autentisera användaren. I just denna analys är specifikt kontaktlös autentisering med SITHS eID i fokus för att möta prioriterade behov.

I dialogen med leverantörerna är det två globala öppna standarder för säker användarautentisering som särskilt framhålls: *FIDO2* (*Fast Identity Online [R2]*) och *certifikatsbaserad autentisering* (*PKI*, *Public Key Infrastructure*).
Både dessa tekniker är rekommenderade för användarautentisering i Ineras Referensarkitektur för Identitet och åtkomst [R1], och används i olika grad i dagens SITHS. Båda teknikerna kan användas för att personalisera bäraren (knytas till person) centralt i fabrik eller på distans med hjälp av annat eID eller en fysisk id-handling.

3.2.1.1 FIDO2

FIDO2 är en standard förvaltad av *FIDO Alliance* och *World Wide Web Consortium* [R2] med mycket god interoperabilitet och brett stöd på marknaden. Dess specifikationer hanterar kommunikation mellan klient och eID-bärare (*Client to Authenticator Protocol, CTAP*), och klient och verifierande system (*W3C Web Authentication, webauthn*).

En stark drivfaktor för FIDO2-tekniken är att kunna ersätta lösenordsbaserade lösningar (*passwordless*) med säkrare teknik. Nyckelmaterialet som används kallas även för *passkeys*. Stöd för FIDO2-tekniken har implementerats relativt brett i datorer/operativsystem, mobila enheter, webbläsare och IAM-infrastruktur.

Sammantaget bör detta främja en god förvaltningsbarhet över tid. Vidare har FIDO2-tekniken följande fördelaktiga egenskaper relativt behovsbilden:

- Utformad för att fungera bra även kontaktlöst över radioteknik genom ett säkert meddelandeutbyte med bäraren.
- Kräver normalt ingen mellanprogramvara (*middleware*) på klientenheten. Bra inbyggt stöd i operativsystem och webbläsare för FIDO2, även för mobila operativsystem. Stöd för bärare kan byggas in i app via standardiserade API:er.
- Förberett för att kunna registrera och använda biometrisk autentisering via standardiserat gränssnitt.
- Standardiserad hantering av godkända bärartyper (*FIDO attestations*).

Hantering av legitimeringskoden (PIN) och låsning/upplåsning av FIDO2-baserade bärare skiljer sig en del mot motsvarande PKI-baserade. FIDO2-bärare implementerar vanligtvis både en temporär låsning efter ett fåtal felaktiga försök, och en permanent låsning efter relativt många felaktiga försök. Vid temporär låsning kan användaren försöka igen genom att till exempel ta ur och sätta tillbaka bäraren. Vid permanent låsning är däremot nycklarna på bäraren förbrukade och bäraren kan endast användas igen genom att utföra en ny personalisering och aktivering. Noteras här att inga upplåsningskoder (puk) förekommer för FIDO2-bärare.

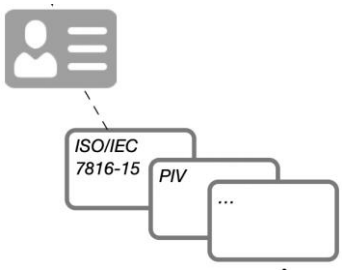
För att använda FIDO2-baserade bärare i SITHS behöver följande ges stöd för i SITHS infrastruktur:

- Personalisering inkluderande utfärdande av användarcertifikat för att knyta bäraren och nyckelmaterialet till en användare.
- Spärr av SITHS eID på FIDO2-bärare.
- Registrering/ändring av legitimeringskoden, samordna med ev. PKI-del.
- Upplåsning (återaktivering) av FIDO2-bärare

3.2.1.2 Certifikatsbaserad autentisering (PKI)

Certifikatsbaserad användarautentisering med X.509-certifikat [R4] är relativt brett implementerat, men framför allt inom organisationer med höga säkerhetskrav, och är det som används för SITHS-korten idag. För enkelhet skull benämner vi i denna rapport bärare som stödjer denna teknik *PKI-bärare*.

Det finns flera olika profiler för PKI-bärare på marknaden. PIV-profilen (FIPS 201) togs ursprungligen fram av myndigheter i USA för att standardisera de PKI-bärare som deras förvaltningarna skulle använda, och har sedan blivit en allmänt tillgänglig standard. Inom Europa har andra kortprofiler oftast använts som möter krav från eIDAS [R7] och ETSI [R8].



Smartkortet kortprofil specificerar dess interna layout för nyckel- och certifikatsbehållare mm.

Detta medför att mellanprogramvaran på klientenheterna för bärare kan behöva stödja flera olika bärarprofiler, alternativt att flera mellanprogramvaror läggs på klientenheterna.
Det finns förvisso inbyggt stöd för PIV-profilen i många plattformar, men för certifikatskrivning och annan bäraradministration som krävs för SITHS behövs ändå en specifik mellanprogramvara. Standardisering finns på API-nivån ovan PKI-profilen i form av PKCS#11, men det förutsätter ändå att bärarprofilen stöds av mellanprogramvaran.

En fördel med certifikatsbaserad autentisering är att spärrhanteringen är standardiserad och en del av en PKI-implementation. Certifikatsbaserad autentisering är också från början anpassat till storskaliga företagsimplementationer.

3.2.2 Hårdvarubaserade bärare

Bärare för e-id kan grovt delas in i hårdvarubaserade respektive plattformsbaserade. Hårdvarubaserade bärare består av en dedikerad hårdvara som enbart används som bärare, medan plattformsbaserade bärare är implementerade i en enhet som också kan användas för andra applikationer, till exempel en mobil enhet eller en dator med säkerhetschip.

När det gäller hårdvarubaserade bärare är de två typer som lyfts fram i utredningen som lämpliga för SITHS eID med hänsyn till stöd för kontaktlös teknik:

- Smartkort med kontakt (”guldkontakt”) och kontaktlöst via NFC-teknik (Near Field Communication, [R3]).
- Säkerhetsnyckel med USB och kontaktlöst via NFC-teknik.

Båda typerna finns också med fingeravtrycksläsare, men kan begränsa utbudet, speciellt i kombination med övriga krav inom SITHS och behovsbilden som framkommit i denna utredning.

3.2.2.1 Smartkort

Smartkort kan förses med både den klassiska guldkontakten och NFC för kontaktlös teknik. När kortets chip kan kommunicera över båda teknikerna kallas det även för "*dual interface*".

Smartkortet har med dess formfaktor flera specifika fördelar relativt behoven inom SITHS:

- Möjliggör god antennverkan för att ge hög tillförlitlighet vid fysisk åtkomst, till exempel vid inpassering genom dörrar och öppnande av lås.
- Lämpligt för grafisk utformning och tryck av personuppgifter för fysisk legitimering.

3.2.2.2 Säkerhetsnyckel

Säkerhetsnycklar finns i flera kombinationer och formatfaktorer med olika typer av USB-kontakt och kontaktlöst via NFC eller BLE (*Bluetooth Low Energy*).
För USB går produkter och lösningar successivt över mot den förbättrade och mer framtidssäkra USB-C, samt att det finns adaptrar till andra förekommande varianter som USB-A.
För kontaktlöst passar NFC-tekniken generellt bäst för säker blipp med eID-bärare då den har mycket kort räckvidd, i kombination med att kunna arbeta passivt, dvs. inte kräva batteri i bäraren.

Fördelar som kan lyftas fram för säkerhetsnycklarna är:

- Mycket tåligt format. Jämfört med plastkort kan säkerhetsnycklar göras betydligt tåligare och därmed ha längre förväntad livslängd.
- Standard USB-kontakt, kräver ingen smartkort-läsare.
- Möjliga att desinficera.
- Kan innehålla signerade data om tillverkare och bärarmodell för att kunna godkänna anslutning som tillbehör till datorer och användning för SITHS.

Samtidigt finns det också begränsningar och nackdelar med säkerhetsnycklar att ta hänsyn såsom

- Saknas stöd för fysisk åtkomst med MIFARE-teknik – svårt att finna produkt på marknaden med dagens de facto teknik för inpassering.
- Begränsade möjligheter till grafisk utformning
- Ej lämpade för tryck av personuppgifter för fysisk legitimering
- Inköpspris per bärare är generellt sätt högre jämfört med smartkortet, vilket dock kan kompenseras med längre livslängd och återanvändbarhet.

3.2.3 Plattformsbaserade bärare

När det gäller plattformsbaserade bärare för e-id finns det primärt två huvudtyper:

- Mobil enhet med säkerhetschip
- Dator med säkerhetschip

Nyckelmaterial för e-id behöver för dessa kunna lagras i ett säkerhetschip, även kallade TPM-chip (*Trusted Processing Module / Secure Enclave*).

En fördel med plattformsbaserade bärare är potentialen att kunna använda enhetens biometriska sensorer (kamera/fingeravtrycksensor) i stället för legitimeringskod.

Mobil enhet som bärare finns redan i SITHS i form av Mobilt SITHS. I behovsanalysen lyftes önskemål att utöka detta med personlig dator som bärare.

3.2.3.1 Dator med säkerhetschip

För att kunna använda en personlig dator som bärare av SITHS eID krävs en tillräckligt säker utfärdandeprocess och ett tillräckligt skydd av e-legitimationen i sig, för att möta kraven i tillitsramverket för Svensk e-legitimation.

En utfärdandeprocess skulle kunna baseras på id-växling från annat eID, alternativt en digital id-kontroll med fysisk legitimation. Noteras ska också att det inte räcker att lagra nycklarna i säkerhetschip, det behöver också säkerställas att nyckeln inte kan användas av någon programvara på datorn, utan att den rättmätiga innehavaraaren har tillfört något denne vet (legitimeringskod) eller är (biometri).

Utredningen bedömer att det förvisso är tekniskt möjligt att realisera en lösning för detta, men att lösningen är komplex och förhållandevis kostsam. Detta ska ställas mot att nyttan är starkt beroende på andelen personliga datorer i organisationen.

3.2.4 Delade datorer

För situationer där medarbetare behöver använda flera olika delade datorer, och loggar in och ut många gånger per arbetspass, är det brukligt att använda klientdatorer i s.k. ”kioskläge”, dvs. användaren behöver inte logga in i datorns operativsystem. Användaren behöver i stället kunna använda e-legitimering med SITHS eID för åtkomst till applikationsresurser. Typiskt används också en virtualiseringsplattform för att ge åtkomst till virtuella skrivbord eller appar med stöd för sessionsförflyttning till valfri klientdator.
I en sådan miljö är det fokus på att hantera säker identitet i applikationslagret, något som också rekommenderas från de leverantörer som bidragit i utredningen.

De tekniska lösningarna för e-legitimering kan här grovt delas in i följande kategorier

- IdP-baserad autentisering
- Använd en anpassad autentiseringsmodul på klienten

3.2.4.1 IdP-baserad autentisering

IdP-baserad autentisering innebär att applikationerna ansluts till en legitimeringstjänst (IdP), som ansvarar för all användarautentisering. Det gör att ny teknik som till exempel kontaktlös säker blipp via FIDO2 kan realiseras i autentiseringstjänster kopplad till legitimeringstjänsten, frikopplat från applikationerna. Även autentisering på annan enhet kan stödjas, till exempel Mobilt SITHS för autentisering på dator.

Används en virtualiseringsplattform är det denna som ansluts till legitimeringstjänsten. Single Sign-On kan uppnås via legitimeringstjänstens sessionshantering, samt inbyggda funktioner i virtualiseringsplattformen.

IdP-baserad autentisering är den rekommenderade metoden enligt Ineras Referensarkitektur för Identitet och åtkomst [R1], och rekommenderas som första val även från plattformsleverantörerna i genomförd RFI.
Som exempel kan tekniken tillämpas i Windows-miljöer genom att integrera autentisering med

SITHS eID som en *External Authentication Method (EAM)* i Microsofts IdP Entra ID. Idag stöds det som en kompletterande autentiseringsfaktor.

3.2.4.2 Anpassad autentiseringsmodul på klienten

Ett annat alternativ är att utveckla eller anskaffa en anpassad autentiseringsmodul (*custom authentication provider*) som integreras i operativsystemet på klientdatorerna och tar över inloggningen. Modulen implementerar autentiseringstekniken till exempel kontaktlös säker blipp via FIDO2, typiskt med stöd av en autentiseringstjänst.

Med denna teknik kan även inloggning till datorns operativsystem hanteras, men nackdelen är att lösningen inte är standardiserad utan blir djupt integrerad i varje teknisk plattform, och behöver följa med ändringar i dessa. Detta kan medföra en hög förvaltningskostnad över tid, och kan därför inte rekommenderas som ett förstahandsalternativ.

3.2.5 Delade mobila enheter

Vid användning av gemensamma (delade) mobila enheter behöver säkerställas att föregående användares SITHS eID inte är tillgänglig för nästa användare. Ett sätt att åstadkomma det är att lägga SITHS eID på en extern personlig bärare som används tillsammans med den delade enheten, och att eID-appen på enheten inte har någon personbunden information.

Kommunikationen med eID-bäraren kan antingen vara kontaktlös, där främst NFC rekommenderas för säker blipp, eller kontaktbaserad med USB. Då många läsplattor på marknaden saknar NFC, kan det vara viktigt att ha USB som ett alternativ.

Som nämnts ovan finns det önskemål att kunna använda SITHS eID för säker inloggning till mobilens operativsystem, för att helt skilja på användarsessioner lokalt i enheten. I de dominerande mobila operativsystemen saknas det dock inbyggt stöd för sådan separation av användare genom en inloggning. Det går att nyttja administrativa verktyg (MDM) eller så kallade *custom launchers* (enbart i Android), för att reglera vad som är tillgängligt för respektive användare, men det saknas standardlösningar för att använda en autentiseringslösning som SITHS eID för detta.

Rekommendationen från plattformsleverantörerna är att hantera säker identitet i applikationslagret i stället, dvs. autentisering mot nativa och webbaserade appar, eventuellt med stöd av en virtualiseringsplattform. Genom autentisering via en IdP-tjänst och en så kallad *broker* på enheten (till exempel standardwebbläsaren) kan också Single Sign-on (SSO) realiseras.

För delning av mobila enheter, mobiltelefoner eller läsplattor, rekommenderas sammanfattningsvis:

- Använd externa personliga bärare för SITHS eID med stöd för NFC och/eller USB.
- Hantera säker identitet i applikationslagret genom autentisering med SITHS eID mot appar.
- Nyttja IdP-baserad legitimering enligt [R1] för att integrera med autentiseringstekniken, och realisera Single Sign-on (SSO) via IdP-tjänsten.

- Hantera vid behov rensning/återställning av enheten mellan användare med separat verktyg.

För kontaktlös autentisering rekommenderas även att begränsa vilka modeller av mobiler som används/stöds, då funktionalitet och handhavande (som var NFC-läsaren sitter) kan skilja ganska stort mellan tillverkare.

3.2.6 Inloggning i datorer

En ny eller vidareutvecklad bärarteknik för SITHS behöver kunna fortsätta stödja säker inloggning till datorer med SITHS eID (operativsysteminloggning). Idag stöds detta genom certifikatsbaserad inloggning (PKI) med SITHS-kort.

Utgående från de föreslagna autentiseringsteknikerna, certifikatsbaserat (PKI) och FIDO2, har utredningen undersökt nuvarande möjligheter till säker inloggning i prioriterade plattformar.

3.2.6.1 Datorinloggning med FIDO2

Datorinloggning med extern FIDO2-bärare stöds i Windows, macOS och Linux. Dock krävs att det först görs en separat registrering av bäraren lokalt i organisationen mot aktuell målmiljö (domän, tenant eller liknande). Vid registreringen skapas ett extra nyckelpar på bäraren.
En möjlighet är här att nyttja SITHS eID för att legitimera användaren i en lokal självservice-funktion för registreringen, detta är dock något som organisationen själv får hantera.

Förutsättningar i plattformarna för FIDO2-baserad inloggning är översiktligt:

- För Windows krävs att
  - FIDO2-bäraren registreras i MS Entra ID. Microsoft tillhandahåller användargränssnitt och API för att utföra registreringen.
  - Datorerna ska vara anslutna till MS Entra ID (Entra ID-joined) eller till lokal AD-miljö (Hybrid-joined). I det senare fallet krävs också en registrering av datorn mot MS Entra ID.
- För macOS stöds FIDO2-baserad inloggning från version *Sonoma*. Det krävs dock att användaren har två bärare av redundansskäl, och det stöds enbart över USB idag.
- För Linux finns stöd för FIDO2-baserad inloggning i de större distributionerna.

3.2.6.2 Datorinloggning med certifikatsbaserad autentisering (PKI)

Datorinloggning med extern PKI-bärare stöds i Windows, macOS och Linux. Bärarens certifikatsinformation behöver först registreras i målmiljön, och det krävs en mellanprogramvara på klienterna med stöd för PKI-bäraren, alternativt en bärare med PIV-profil.

Förutsättningar i plattformarna för certifikatsbaserad inloggning är översiktligt:

- För Windows stöds certifikatsbaserad inloggning i MS Entra ID och i lokal AD-miljö.
- För macOS stöds certifikatsbaserad inloggning i inbyggda *Crypto Token Kit* (CTK).

- För Linux stöd certifikatsbaserad inloggning genom en mellanprogramvara för PKCS11 för bäraren i fråga, alternativt en bärare med PIV-profil i de större distributionerna.

3.2.7 Biometrisk autentisering

Vid all behandling av medarbetares biometriska uppgifter i arbetslivet behöver tillses att lösningen för och användningen av biometri har rättslig grund och uppfyller regelverken för dataskydd av känsliga personuppgifter, se [R5]. Utredningen rekommenderar att dessa rättsliga förutsättningar utreds vidare innan en lösning för biometrisk autentisering realiseras i nya bärartyper för SITHS.

Utredningen bedömer dock att några av förutsättningarna för att en lösning ska kunna godkännas är att

- Biometriska uppgifter sparas och hanteras enbart skyddat på den personliga bäraren. Detta är i linje med styrande princip i Referensarkitektur för Identitet och åtkomst [R1]: "*Vid användning av biometri för autentisering bör biometriska data hållas nära användaren själv, helst endast inom användarens personliga bärare för e-id. Biometri bör inte användas som den enda faktorn i en autentiseringslösning.*"
- De biometriska uppgifterna kan endast användas i syfte att autentisera användaren i kombination med innehav av den personliga bäraren.
- Det är inte möjligt att återskapa de biometriska uppgifterna för att användas i något annat sammanhang.
- Medarbetaren avgör själv om hen vill nyttja biometrisk autentisering (opt-in). Det ska alltid vara möjligt att i stället använda en legitimeringskod, om medarbetaren föredrar det.

För att uppfylla ovan förutsättningar konstaterar utredningen att ett grundläggande krav är att den personliga bäraren för SITHS eID har inbyggd sensor för verifiering av biometri. Bäraren ska vidare ha starkt hårdvaru- och programvaruskydd för biometriska uppgifter. Tänkbara tillgängliga bärartyper för detta är hårdvarubaserade respektive plattformsbaserade.

3.2.7.1 Hårdvarubaserade bärare med inbyggd biometrisk sensor.

Det finns säkerhetsnycklar och smartkort med inbyggd fingeravtrycksläsare på marknaden som bör kunna möta de tekniska säkerhetskraven kring biometrisk autentisering. För användaren kan handhavandet bli mycket smidigt då hen bara behöver hålla ett finger på bäraren vid autentisering, i stället för att slå in en kod.

En nackdel kan dock vara att bäraren blir känsligare för slitage, till exempel på grund av desinficering eller mekanisk nötning.

Då bäraren förutom biometristödet också ska möta övriga tekniska krav i SITHS, inklusive kontaktlös autentisering, fysisk åtkomst osv. kan utbudet på marknaden av sådana bärare bli

begränsat. Inför ett beslut att införa bärare med fingeravtryckläsare bör även kostnaden för per bärare undersökas och vägas in.

En teknisk lösning i SITHS för säkerhetsnycklar och smartkort med inbyggd fingeravtryckläsare beror till stor del på vald autentiseringsteknik.

FIDO2-standarden är som nämnts förberett för att kunna registrera och använda biometrisk autentisering via ett standardiserat gränssnitt. Det finns till exempel inbyggt stöd för detta i Windows och i webbläsare som stödjer FIDO2-protokollen. Det gör också att det är möjligt att bygga in stöd för biometrihantering i SITHS eID-app som fungerar med bärare som följer FIDO2. Det kan också nämnas att fingeravtrycket i sig inte lagras på en FIDO2-bärare, endast en hash av fingeravtrycket lagras skyddat i bärarens chip.

För certifikatsbaserad autentisering (PKI) saknas standardisering för registrering och användning av biometri på bäraren. En lösning kräver som regel tillgång till ett SDK, en mellanprogramvara eller motsvarande från bärarleverantören. Detta sammantaget talar för att använda bärare med FIDO2-stöd för att lägga en bra grund för en realisering av biometrisk autentisering.

3.2.7.2 Biometri med plattformsbaserade bärare.

Ett annat alternativ är att nyttja biometristöd i den plattform (enhet) som användaren använder, för att verifiera användaren i samband med autentiseringen med SITHS eID. Denna teknik används idag i Mobilt SITHS med stöd för fingeravtryck och ansiktsmatchning.

Tekniken används också i alla större plattformsleverantörers operativsystem, såväl i Microsofts Windows Hello som i Apples TouchID och FaceID.

Gemensamt för dessa tekniska lösningar är att de är anpassade efter att nyckelmaterialet finns lagrat i säkerhetschip i enheten själv och inte i en extern bärare. Därför är det primärt användbart i de fall också SITHS eID lagras på enheten, som i fallet Mobilt SITHS.

3.2.8 Single Sign-on

En stark rekommendationen från flera leverantörer som ingått i RFI är att hantera Single Sign-on (SSO) via standardiserade gränssnitt till legitimeringstjänster (IdP:er), och inte i bäraren för e-id. Detta är också i linje med styrande principer i Referensarkitektur för Identitet och åtkomst [R1]. Utredningen rekommenderar att utforma applikationsarkitekturen så långt som möjligt utifrån denna princip för att erhålla en bra SSO-upplevelse för användarna.

När en virtualiseringsplattform används rekommenderas också att nyttja plattformens inbyggda stöd för SSO in till själva miljön, för åtkomst till en VDI eller publicerad app.

3.2.9 Låsning av session

Om en funktion för låsning av användarsession/klientdator skulle realiseras för SITHS, vore det en fördel om funktionen kan användas så generellt som möjligt, dvs. för

- olika typer av SITHS eID, såväl kontaktbaserade som kontaktlösa.

- prioriterade datormiljöer för delade datorer, såsom Citrix- och vmware- plattformarna.

Eftersom en låsfunktion behöver fungera tillsammans med kontaktlös autentisering via en blipp, går det inte att trigga låsningen på att bäraren för SITHS eID avlägsnas.

Ett annat alternativ som lyfts är att blippa med bäraren även för att låsa. En lösning skulle då behöva känna av att samma användare har en autentiserad session och då låsa sessionen. Å andra sidan ska inte sessionen låsas om blippen avser en förnyad autentisering för samma användare inom sessionen, eller en påföljande autentisering mot en annan tjänst för samma användare. Dessutom behöver en lösning kunna styra funktioner i de aktuella tekniska miljöerna, till exempel begära frånkoppling av sessionen i den virtuella miljön.

Sammantaget är en preliminär bedömning att det är relativt komplext att ta fram en låsfunktion baserad på blipp med SITHS bärare som fungerar stabilt och tillräckligt generellt. Det bör ställas mot den verksamhetsnytta en sådan funktion kan tillföra, jämfört med att använda inbyggda stöd för låsning som finns i operativsystemen och virtualiseringsplattformarna, till exempel via en knapptryckning.

3.2.10 Närvaroavkänning

Det finns lösningar för närvaroavkänning baserade på framför allt Bluetooth Low Energy (BLE). Lösningarna kan vara baserade på en mobil app alternativt en säkerhetsnyckel med inbyggt batteri som kommunicerar med en programvara på datorn.

Erfarenheterna från dessa är dock att det är svårt att i praktiken få dem tillräckligt tillförlitliga och användarvänliga. Bärare med inbyggt batteri medför också behov att kunna ladda upp bäraren, vilket kan ses som en stor nackdel jämfört med dagens bärare för SITHS.

3.2.11 Autentiseringsteknik för fysisk åtkomst

När det gäller val av nästa autentiseringsteknik för kontaktlös fysisk åtkomst, såsom inpassage till fastigheter, är det främst två tekniker som idag kan övervägas: MIFARE DESFire och certifikatsbaserad autentisering (X.509-certifikat med PKI).

3.2.11.1 MIFARE DESFire

MIFARE DESFire är framtagen av NXP Semiconductors för att ersätta den äldre MIFARE Classic med bland annat säkrare krypteringsteknik i form av AES (*Advanced Encryption Standard*) och stöd för längre kryptonycklar. MIFARE DESFire använder symmetrisk kryptering och NFC som kommunikationsteknik.

Genom det stora genomslag tekniken fått i produkter på marknaden och i installerad bas av inpassagesystem, kan MIFARE DESFire idag anses vara en de facto standard för autentiseringsteknik för fysisk åtkomst. MIFARE DESFire EV3 är den version av tekniken som gäller idag, kompatibel bakåt mot tidigare versioner (EV1 och EV2).

Som bärare av MIFARE DESFire är smartkortet överlägset vanligast. Smartkortet har en bra formfaktor för god antennverkan och rimligt läsavstånd, vilket är viktigt i en lösning där bäraren är elektriskt passiv dvs. strömsätts via läsarsystemet. Det är idag svårt att hitta andra bärartyper på marknaden med stöd för MIFARE DESFire.

3.2.11.2 Certifikatsbaserad autentisering (PKI)

Ett alternativ till MIFARE-tekniken är certifikatsbaserad autentisering. I praktiken är det PKI-bärare med PIV-profil som kan hittas stöd för i produkter och i viss mån i installerad bas.
Tekniken som sådan har som nämnts ovan flera goda säkerhetsrelaterade egenskaper, framför allt att den bygger på kryptering med publika nycklar, vilket medger en säker nyckelhantering och god skalbarhet.

Inom området fysisk åtkomst har certifikatsbaserad autentisering dock inte fått samma genomslag, och har främst tillämpats i s.k. högsäkerhetslösningar.
Den största nackdelen med tekniken är därför svagt stöd i befintlig installerad bas av låssystem för inpassage, skåp och utskriftslösningar. Utredningens samlade bedömning är att en övergång på bredden är svår och kostsam att genomföra, då det kan innebära byte av en stor mängd hårdvara/läsare, och att läsarna ofta är dyrare än motsvarande för MIFARE.

Sammantaget och utifrån dialogmötena med leverantörerna är utredningens slutsats att MIFARE DESFire är den mest lämpade tekniken att ersätta MIFARE Classic på SITHS-kortet.

3.2.12 Hantera övergången från MIFARE Classic

Utredningen har analyserat två olika strategier att hantera övergången från MIFARE Classic till MIFARE DESFire:

1. Inför ett nytt kort med MIFARE DESFire EV3, dvs. utan stöd för MIFARE Classic.
2. Inför ett nytt kort med MIFARE DESFire EV3C, vilket är bakåt kompatibelt genom att även emulera MIFARE Classic.

3.2.12.1 MIFARE DESFire EV3 (utan Classic)

Potentiella fördelar med ett ”rent” DESFire-kort skulle kunna vara ett tekniskt något enklare kort, samt möjligen ett större incitament att gå över till den nya tekniken för att få de andra fördelarna med det nya kortet.

Dock har framhållits i analysen att det skulle vara hindrande för en övergång till ett nytt kort om det saknade kompatibilitet bakåt med Classic-tekniken, eftersom en del befintliga system inte kan uppgraderas. Detta skulle kunna innebära en längre transitionsperiod och mindre nyttoeffekt i verksamheten.

En konsekvens av detta alternativ är att flertalet system skulle behöva konfigureras för att klara två olika läsarprofiler (DESFire respektive Classic) så länge de gamla korten är i omlopp. Med tanke på att giltighetstiden för ordinarie kort är fem år, samt att det gamla kortet kan vara svårt att helt avveckla, skulle detta stöd för två tekniker parallellt behöva gälla under lång tid.

Dessutom klarar inte alla system att hantera dubbla profiler. För dessa kan följande nödlösningar behöva tillämpas för att klara båda korttyperna:

- Äldre system som enbart stödjer MIFARE Classic kan ställas om till läsning av UID (Unique Identifier), dvs. MIFARE-chippets unika identifierare. UID är inte krypterat och säkerhetsnivån är inte särskilt hög. Det behöver även hanteras att UID för de gamla korten är 4 bytes långa, medan det är 7 bytes för MIFARE DESFire-kort.
- System som har stöd för DESFire, men enbart klarar en samtidig profil, kan ställas in för MIFARE DESFire, eventuellt i kombination med läsning av UID för Classic-korten.

3.2.12.2 MIFARE DESFire EV3C med emulerad MIFARE Classic

MIFARE DESFire EV3C är speciellt framtagen för att hantera kompatibilitet med Classic. Kortet presenterar sig för läsaren som endera DESFire eller Classic, beroende på vad den initiala handskakningen mellan kortet och läsaren resulterar i.
Korten kodas enbart med appar för MIFARE DESFire, men ett emuleringslager översätter informationen i dessa appar till MIFARE Classics protokoll med sektorer och block. Genom att använda samma data och konfiguration som i de nuvarande korten, kan ett nytt kort presentera sig på samma sätt som de gamla.

I teorin löser detta alternativ kompatibilitetsproblemen; system som enbart klarar MIFARE Classic presenteras med ett Classic-kort, system som stödjer MIFARE DESFire presenteras med ett DESFire-kort. När i framtiden Classic-tekniken inte längre behöver stödjas kan denna del stängas på befintliga kort i efterhand genom att skicka speciella kommandon till kortet.

En del system och läsare kan dock få problem att stödja EV3C. I vissa fall kan detta lösas med programuppgraderingar av läsarna och/eller det centrala systemet. Om inte detta är möjligt kan det bli nödvändigt att för undantagsfallen utfärda kort med enbart en MIFARE-teknik.

Sammantaget är utredningens bedömning att MIFARE DESFire EV3C med emulerad Classic-del borde ge de bästa förutsättningarna för att hantera övergången från MIFARE Classic. Samtidigt rekommenderas att genomföra tidiga verifieringar av tekniken i befintliga produktionssystem inför ett beslut om införande av korttypen.

3.2.13 Använda mobilen för fysisk åtkomst

Det sker mycket teknikutveckling och standardiseringsarbeten inom säkerhetslösningar baserade på mobila plattformar. Detta gäller inte minst teknik för att ersätta fysiska och andra former av nycklar med nyckel i mobilen.

Förutom en mängd leverantörsspecifika lösningar finns det idag möjligheter att använda de facto-standarden MIFARE DESFire även från en mobil enhet. En tjänst kan sättas upp där en användare kan autentisera sig för att kunna erhålla ett personaliserat virtuellt kort i mobilens digitala plånbok (wallet). Det virtuella kortet kan sedan agera som ett MIFARE DESFire-kort mot till exempel inpassagesystem eller andra digitala lås. Den operatör som agerar utfärdare behöver bli godkänd och ansluten till plattformsleverantörens tjänst.

Tekniken med MIFARE DESFire i mobilen är relativt ny och kräver typiskt de senaste operativsystemversionerna. Stöd finns i dag i Apples och Samsungs mobiler, och Google arbetar för närvarande på en lösning för Android. Apples virtuella kort kräver även att läsarsystemen stödjer tilläggsprotokollet *Enhanced Contactless Polling* (*ECP*), för att förbättra användarupplevelsen och minska felsituationer.

Noteras kan att tekniken primärt agerar som enfaktorsautentisering avsedd för personliga mobiler.

3.2.14 Framtida standarder för fysisk åtkomst

Det pågår även framtagning av en ny standard för digitala nycklar kallad *Aliro*. Arbetet bedrivs inom *Connectivity Standards Association* (CSA) [R6] och har fått ett starkt branschstöd: de stora plattformsleverantörerna och en stor mängd andra leverantörer inom området driver respektive backar upp initiativet.

Aliro har potentialen att få lösningar från olika leverantörer att fungera tillsammans via en öppen standard. Målet är att ge stöd för flera bärartyper såsom mobilappar, wearables, smartkort och säkerhetsnycklar, över kommunikationstekniker som NFC, BLE och UWB (*Ultra Wide Band*). Tekniskt bygger Aliro på asymmetrisk kryptering och publika nycklar, vilket borgar för en säker och skalbar nyckelhantering.

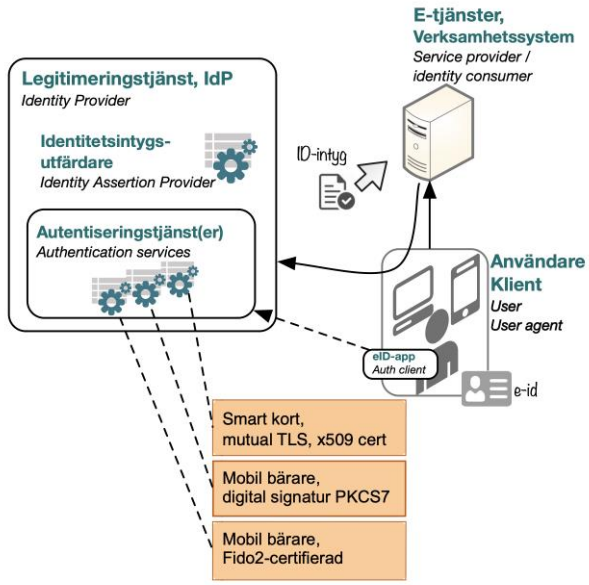
Bedömningen är att Aliro kan få stor påverkan på sikt, men att specifikationerna inte är färdigställda och stöd i produkter, inte minst i installerad bas av system, lär vänta. Troligen får standarden först påverkan på konsumentmarknaden för att senare komma in på företagssidan.

4 Arkitektur & lösning

4.1 Arkitektur

4.1.1 Referens- och lösningsarkitektur för SITHS

Framtida bärare för SITHS och tillhörande tekniska lösningar behöver passa in i lösningsarkitekturen för SITHS. Lösningsarkitekturen är i sin tur utformad enligt principerna i Ineras Referensarkitektur för Identitet och åtkomst [R1].



Denna arkitektur bygger på att e-legitimering hanteras av en legitimeringstjänst (IdP) med stöd av autentiseringstjänst(er), vilket innebär att verksamhetssystemet inte behöver känna till de tekniska detaljerna hur autentisering går till för olika bärartyper. E-tjänsten erhåller oavsett autentiseringsteknik ett id-intyg från legitimeringstjänsten enligt standardiserade protokoll som OIDC och SAML2.

En eID-bärare kommunicerar via en autentiseringsklient (SITHS eID-app) med en autentiseringstjänst som är anpassad för det specifika autentiseringsprotokollet, till exempel FIDO2. Detta betyder att en ny bärartyp med ett nytt autentiseringsprotokoll kan implementeras i autentiseringsklient och -tjänst, utan att påverka anslutna e-tjänster. Även legitimeringstjänsten behöver typiskt anpassas när nya bärartyper introduceras, bland annat för att hantera användarens val av bärartyp.

En styrande princip i referensarkitekturen är att autentisering ska kunna utföras i en separat säkerhetskanal (*out-of-band authentication*). Detta skapar ytterligare lös koppling och minskat beroende till vilka andra klientprogramvaror som används, till exempel webbläsare.

Som tidigare nämnts tillhandahåller legitimeringstjänsten stöd för Single Sign-on (SSO). Legitimeringstjänsten ska även erbjuda möjlighet till tvingande e-legitimering (*forced*

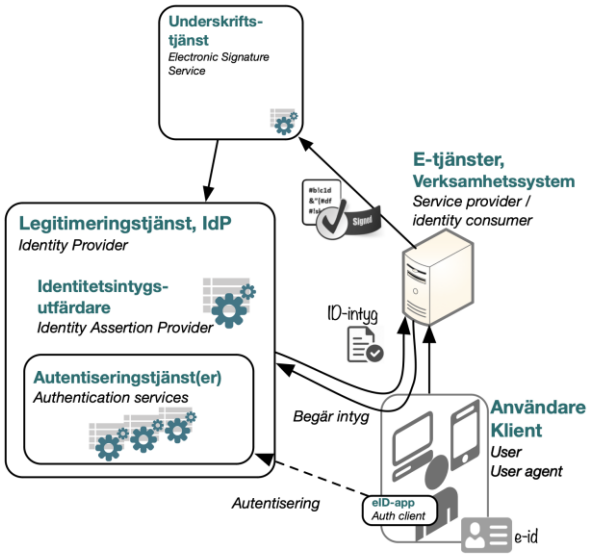
authentication), inte minst viktigt vid underskrift. Detta gör att eID-bäraren måste ha stöd för att på begäran initiera en ny tvåfaktorsautentisering oavsett om en SSO-session är aktiv eller ej.

FIDO2 som autentiseringsteknik passar väl in i denna lösningsarkitektur. I Autentiseringstjänst SITHS används idag också FIDO2-teknik för autentisering.

4.1.2 Ett enhetligt användargränssnitt

En annan arkitekturellt viktig aspekt är att SITHS tillhandahåller ett enhetligt och sammanhållet användargränssnitt, vilket primärt tillhandahålls via SITHS eID-app. Gränssnittet används vid såväl legitimering, underskrift och hantering av legitimeringskoden, vilket skapar igenkänning oavsett om en stationär eller mobil enhet används. För att upprätthålla detta behöver även nya bärartyper hanteras via SITHS eID-appen.

4.1.3 E-underskrifter



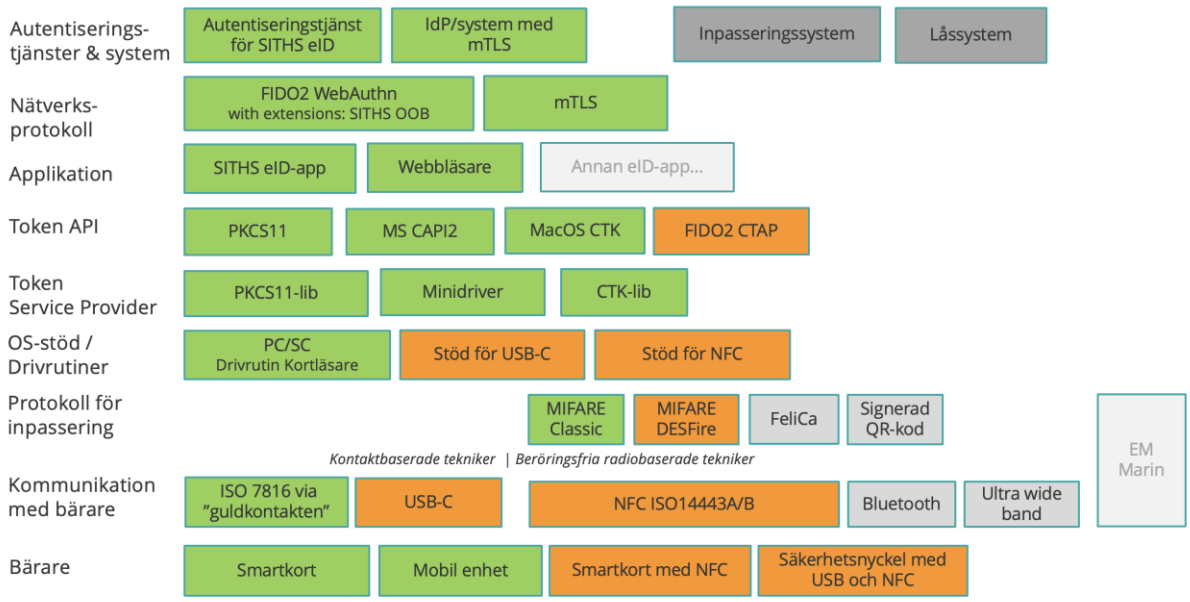
Även lösningen för e-underskrift med SITHS eID följer Ineras referensarkitekturer och baseras tekniskt på e-legitimering för underskrift med stöd av en fristående Underskriftstjänst. Samma infrastrukturtjänster för legitimering och autentisering används även här, vilket gör att om eID-bäraren fungerar för e-legitimering, fungerar den i princip även för e-underskrift.

4.1.4 Standarder och plattformsneutralitet

Ytterligare en styrande princip i referensarkitekturen är att IT-infrastruktur för identitet och åtkomst ska bygga på en plattformsneutral grund. Genom att välja standarder som har brett stöd i prioriterade plattformar, förbättras förvaltningsbarheten och utvecklingskostnader kan hållas nere.

Särskilt viktigt är här att hålla samman och minimera specifik programvara som behöver installeras på användarnas klientenheter. Varje protokoll, drivrutin osv. som införs bör noga övervägas om och hur de passar in i den övergripande klientarkitekturen. Nedan ”teknikstack”

kan vara ett sätt av att visualisera de olika arkitekturella delarna som behövs stöd för och hur de beror av underliggande delar.



Visualisering av teknikstack för SITHS eID med befintligt (grönt) och förslag på utökning (orange).

4.2 Lösningar

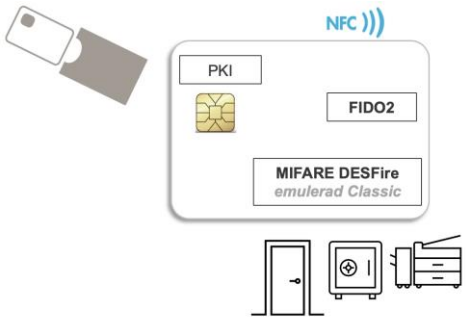
4.2.1 Rekommenderade bärartyper och teknik för SITHS

Utredningens rekommendation utifrån analysen och dialogen med leverantörerna är att två nya bärartyper införs i SITHS:

1. Ett **smartkort** med **FIDO2 över NFC** för **kontaktlös tvåfaktorsautentisering** (blipp) för SITHS eID, samt **MIFARE DESFire** för fysisk åtkomst.
   Kortet görs bakåt kompatibelt med nuvarande kort genom stöd för PKI över smartkortkontakten för att underlätta införandet.
2. En **säkerhetsnyckel** med **FIDO2 över NFC och USB** för **kontaktlös och kontaktbaserad tvåfaktorsautentisering** med SITHS eID.

För kontaktlös tvåfaktorsautentisering rekommenderas FIDO2 över NFC för båda bärartyperna. Tungt vägande skäl är nivån av standardisering som FIDO2 innebär, vilket främjar en god förvaltningsbarhet över tid, goda möjligheter till konkurrensutsättning och minskat behov av leverantörs- eller produktspecifik mellanprogramvara.

4.2.1.1 Smartkort utökat med FIDO2 över NFC



Det vidareutvecklade smartkortet tas fram för att möta behovet av kontaktlös tvåfaktorsautentisering (”säker blipp”) med SITHS eID. De primära användningsfallen är här kontaktlös e-legitimering och e-underskrift i applikationer vid användning av delade mobila enheter (med inbyggd NFC) eller delade datorer (primärt med extern NFC-läsare), även om tekniken i sig även fungerar för personliga enheter.

Används en virtualiseringsplattform för åtkomst till skrivbord och/eller publicerade appar, behöver den anslutas till en legitimeringstjänst med stöd för SITHS eID enligt principerna i [R1], för att kunna nyttja SITHS-kortet för säker inloggning och återanslutning till sessionen.

Smartkortet rekommenderas även ha fortsatt stöd för certifikatsbaserad autentisering (PKI) över smartkortkontakten med nuvarande SITHS kortprofil, inklusive autentisering via dubbelriktad TLS. På detta sätt kan kortet direkt ersätta dagens kort i med samma lokala tekniska förutsättningar, vilket underlättar en övergång. Endast där verksamheten ser nytta med att införa kontaktlös autentisering behöver det också förberedas i lokal utrustning.

Rent tekniskt skulle även kortet kunna stödja PKI över NFC, men detta ger funktionellt överlapp med FIDO2 över NFC samt ökar komplexiteten och risk för eventuella störningar, varför utredningen avråder detta.

För fysisk åtkomst med enfaktorsautentisering rekommenderas att kortet förses med MIFARE DESFire för säkrare enfaktorsautentisering för fysisk åtkomst. I första hand rekommenderas välja versionen EV3C med en emulerad MIFARE Classic för bakåtkompatibilitet med nuvarande kort. Som nämnts ovan bör dock tekniken verifieras praktiskt innan beslut om version tas, eftersom det finns vissa tekniska skillnader mot ett rent Classic-kort.

Vidare rekommenderas att i fabrik lägga på en basprofil för MIFARE DESFire, vilket direkt kan appliceras i lokala system genom distribution av läsnycklar. Detta motsvarar ungefär hanteringen för MIFARE Classic för nuvarande SITHS-kort. Basprofilen innehåller krypterade DESFire-applikationer med tillhörande datafiler och dess åtkomstregler.
Förutom basprofilen har utredningen identifierat att lokala system kan behöva specifik konfiguration för MIFARE DESFire. Därför föreslår utredningen att det skapas möjlighet för organisationen att vid behov lägga till egna och eventuellt leverantörspecifika applikationer och nycklar på kortet.

För mer detaljer kring hur konfigurationen för DESFire skulle kunna utformas se "*Konfiguration och nyckelhantering för fysisk åtkomst*".

4.2.1.2 Säkerhetsnyckel med FIDO2 över NFC och USB-C

Det finns fall där kontaktlös autentisering över NFC inte är möjlig eller praktisk:

- Mobila enheter som saknar inbyggd NFC-läsare. Flertalet modeller av läsplattor på marknaden saknar NFC-stöd, antingen rent hårdvarumässigt eller att stödet inte är tillgängligt för apputvecklare.
- Datorer som saknar användbart stöd för NFC.

Avsaknaden av stöd för NFC kan bero på att hårdvaran saknas, att stödet inte är tillgängligt för apputvecklare, eller att NFC-läsaren är placerad på ett sätt som gör användningen opraktisk. För mobila enheter är heller inte smartkortläsare ett realistiskt alternativ (mycket kostsamma lösningar), och även för personliga datorer finns fördelar om inbyggda standardkontakter kan användas.

Av ovan skäl rekommenderas att införa en säkerhetsnyckel med stöd både för kontaktbaserad och kontaktlös tvåfaktorsautentisering via FIDO2. För kontaktbaserad rekommenderas standard USB-C för bästa kompatibilitet med tillgänglig och framtida hårdvara. För kontaktlös autentisering rekommenderas NFC precis som för smartkortet.

Säkerhetsnyckeln kan således användas med kontakten utan krav på NFC eller smartkortläsare, men även kontaktlöst över NFC, vilket ger en stor flexibilitet i val av lokal utrustning.

Som nämnts i analysen ovan saknas det stöd för MIFARE-tekniken i säkerhetsnycklar på marknaden, varför säkerhetsnyckeln inte för närvarande bedöms kunna ersätta smartkortet för fysisk åtkomst till fastigheter och liknande.

I utredningen analyserades om säkerhetsnyckeln även borde förses med en PKI-del, i syfte att stödja samma protokoll som dagens SITHS-kort. Även om det finns produkter som har det tekniska stödet, finns det tydliga nackdelar med att stödja dubbla protokoll. Som nämndes tidigare i analysen skulle PKI-delen kräva en specifik mellanprogramvara på klienterna, vilket skulle öka den totala komplexiteten och tänkbart skapa en extra inlåsningseffekt. Rekommendationen är därför att i första hand implementera säkerhetsnyckeln som en ren FIDO2-bärare. För att använda säkerhetsnyckeln för datorinloggning se avsnitt 3.2.6.1.

Säkerhetsnyckeln kommer utan PKI-del inte stödja dubbelriktad TLS för autentisering lokalt vid avbrott mot centrala nätverkstjänster (”katastroflägen”). För autentisering i sådana situationer behöver säkerhetsnyckeln ha registrerats som FIDO2-nyckel mot en lokal legitimeringstjänst.

4.2.1.3 Stöd för FIDO2-baserade bärare i SITHS infrastruktur

För att nyttja FIDO2-baserade bärare för SITHS eID behöver ett antal delar implementeras i SITHS infrastruktur:

- Personalisering av FIDO2-delen av bäraren, inklusive aktivering, vilket lämpligen utformas som en självservice-funktion som kan utföras på distans i SITHS Mina sidor.
  Även stöd för upplåsning (återaktivering) av låst bärare behöver finnas.
- Utfärdande av användarcertifikat, lämpligen från en särskild utfärdande CA, för att knyta bäraren och nyckelmaterialet till en användare, och ge stöd för att implementera spärrfunktionalitet.
- Funktionalitet i SITHS eID-apparna där användaren kan registrera och ändra legitimeringskod för FIDO2-delen, samordna med PKI-delen för korten.
- Funktionalitet i SITHS eID Portal för att spärra SITHS eID på FIDO2-bärare, samt publicera spärrinformation.

4.2.1.4 Bärare med inbyggd biometrisk autentisering

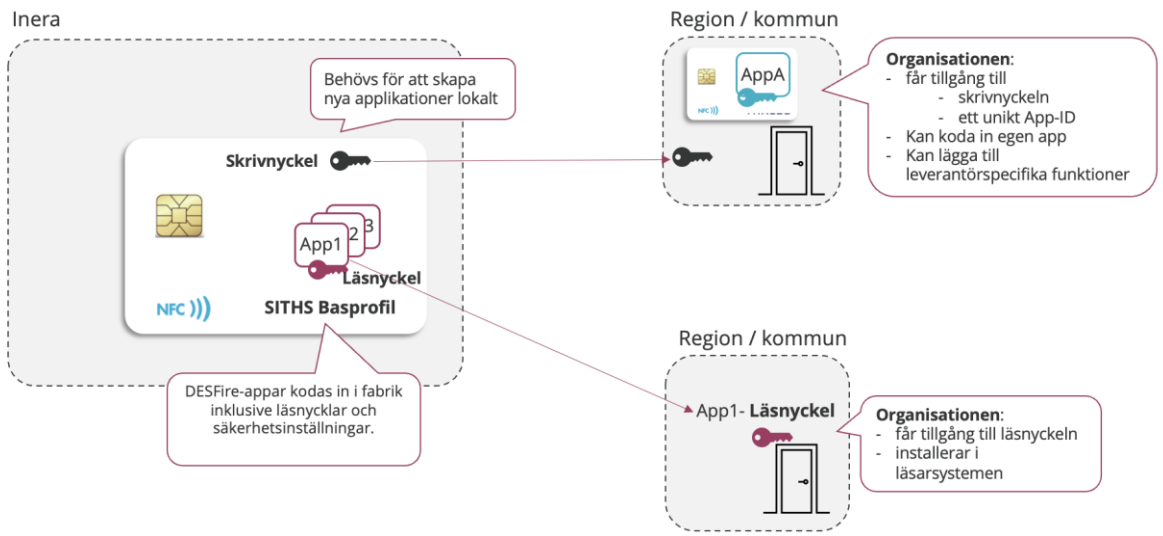
Både smartkortet och säkerhetsnyckeln skulle kunna ha inbyggd fingeravtrycksläsare för att användaren ska slippa hantera koder, ett av de högre värderade behoven i analysen. Som nämnts tidigare i rapporten finns dock flera aspekter att ta hänsyn till, och det rekommenderas att först utreda kostnader, juridiska aspekter och tillgänglighet för sådana bärare som också möter de övriga kraven i SITHS.

Följande funktioner skulle behöva läggas till i SITHS eID-apparna för att få stöd för bärare med biometrisk autentisering:

- Användaren kan initiera en registrering av en biometrisk profil på bäraren
- Användaren kan nyttja biometri för autentisering som alternativ till legitimeringskoden.
- Användaren kan falla tillbaka på att använda legitimeringskoden om biometrifunktionen inte fungerar (till exempel vid användning av handskar). Detta kan jämföras med hur biometristödet fungerar i Mobilt SITHS.

4.2.2 Konfiguration och nyckelhantering för fysisk åtkomst

I dialog med leverantörer inom området fysisk åtkomst har nedan principiella modell för konfiguration av MIFARE DESFire tagits fram.



Översikt modell för konfiguration av MIFARE DESFire

Modellen bygger på en gemensam leverantörsoberoende SITHS basprofil som kodas in på korten i fabrik i samband med personaliseringen av kortet, samt att det skapas möjligheter att lägga till lokal anpassning efter behov.

4.2.2.1 SITHS basprofil för fysisk åtkomst

Basprofilen för MIFARE DESFire kan förslagsvis bestå av följande applikationer:

- (1) En app för online-läsning som följer DESFire EV1 för bästa kompatibilitet. Denna ger stöd även för läsarsystem som inte har stöd för utökad funktion enligt EV2/EV3.
- (2) En app för online-läsning med extra EV2/EV3 säkerhetsfunktioner för läsarsystem som stödjer dessa.
- (3) En app för offline-läsning, där läsarsystemet kan ges skrivrättigheter för att skriva ner rättigheter och loggposter för åtkomst som sker via läsare utan kontakt med centralt system (offline). För denna app reserveras extra lagringsutrymme.

Varje app har en nyckel (krypteringsnyckel som medger läsning och för offline även skrivning) som behöver distribueras på ett säkert sätt till behörig hos organisationen för att installera i lokala system. Manuella rutiner för säker nyckeldistribution kan ofta bli både tidskrävande och krångliga, varför utredningen rekommenderar att lägga till en funktion i SITHS eID Portal där förslagsvis SITHS ansvariga utgivare kan logga in och på ett säkert sätt hämta nödvändiga nycklar.

För att möjliggöra att i framtiden rulla nycklar på ett kontrollerat sätt, kan extra kopior av apparna läggas på med andra uppsättningar nycklar. Dessa är vilande tills de används, och övergången till ny nyckel kan göras lokalt genom konfiguration. Övergången behöver inte synkroniseras mellan organisationer/system eftersom nycklarna kan fungera samtidigt.

Apparna i SITHS basprofil kodas med motsvarande uppgifter som idag kodas för MIFARE Classic, såsom kortserienummer och kortinnehavens HSA-id. För EV3C-kort konfigureras också en mappning till MIFARE Classic med samma kodning i sektorer och block som dagens SITHS-kort för kompatibilitet bakåt så långt det är möjligt.

En specifikation över SITHS basprofil bör göras tillgänglig tidigt för SITHS organisationer och aktuella leverantörer för att kunna förbereda lokala system och rutiner. SITHS basprofil kan även verka pådrivande på marknaden att använda en gemensam specifikation i stället för leverantörsspecifika varianter.

4.2.2.2 Lokal konfiguration för fysisk åtkomst

I de fall den gemensamma basprofilen inte är möjlig att använda, till exempel på grund av specifika lokala krav, kan organisationen ombesörja lokal tilläggskonfiguration på korten med egna DESFire-appar, eventuellt i samverkan med systemleverantör.

För detta behöver Inera kunna distribuera masterskrivnyckeln för MIFARE DESFire-delen till organisationen, där med fördel ovan nämnd funktion i SITHS eID Portal nyttjas. Masterskrivnyckeln medger endast att lägga till DESFire-applikationer på korten samt att formatera/rensa DESFire-delen. Den kan således inte användas för läsning eller ändring av andra applikationer på kortet.

Alla läs- och skrivnycklar för appar som läggs på lokalt hanteras sedan av organisationen själv. För varje app behövs även ett unikt app-id. För att säkerställa att detta alltid är unikt på SITHS-korten, föreslås att Inera förvaltar en förteckning över alla använda app-id.

4.2.3 Hantera övergången till ny teknik

4.2.3.1 Övergång till ny autentiseringsteknik för SITHS eID

Det vidareutvecklade SITHS-kortet med FIDO2-stöd bör kunna införas stegvis genom att göra kortet beställningsbart och till en början använda kortet som idag genom PKI över smartkortkontakten.

När stödet för FIDO2-bärare implementerats i SITHS, kan organisationerna införa ny kontaktlös autentisering successivt, till exempel för delade enheter och kategorier av medarbetare där det gör mest nytta. I samband med sådant införande kommer FIDO2-delen på bäraren att behöva aktiveras; här rekommenderas att detta löses genom en funktion för distansaktivering i SITHS Mina sidor.
Förutsatt att FIDO2-stödet även verifierats för säkerhetsnycklarna kan dessa göras beställningsbara och införas. För dessa finns inget arv att ta hänsyn till på samma sätt som för korten.

4.2.3.2 Övergång till MIFARE DESFire

Som nämnts ovan kan en övergång till MIFARE DESFire underlättas om kortet kan emulera MIFARE Classic för bakåtkompatibilitet med dagens kort.

Det finns också andra viktiga delar som rekommenderas vid en övergång:

- Tillämpa ett stegvist införande med möjlighet att testköra den nya tekniken i befintliga system.
- Inventera organisationens läsarsystem för fysisk åtkomst (dörrar, lås, utskrifter osv), dokumentera vilket tekniskt stöd som finns, och följ upp vilka åtgärder som behöver göras per system.
- Förbered läsarsystemen för att hantera dubbla profiler - Classic resp. DESFire.
- Se över behov att uppgradera programvara för läsarsystemen. Notera att detta kan underlättas betydligt om läsarsystemet har central programvara och inte i respektive läsare.
- Utvärdera lämplig nödlösning när inget av ovan fungerar för ett läsarsystem:
    - Om säkerheten bedöms acceptabel, använd UID-läsning för DESFire-kortet, dvs. läsning av MIFARE-chippets unika identifierare, företrädesvis i kombination med PIN-kod i läsarsystemet.
    - Utfärda MIFARE Classic-kort för de fall som inte kan anpassas.

5 Nyttoanalys och prioritering

I samverkan med den externa arbetsgruppen har nyttor i relation till insats för införande utvärderats. Syftet med nyttoanalysen har varit att ge ett stöd vid prioritering av vad som bör vidareutvecklas. *Nytta* för att införa en viss funktion har vägts mot *komplexiteten att införa* i kundernas verksamhet respektive *realiseringskomplexiteten* för Inera. Sammantaget har detta lett till en rangordning av behov respektive lösningar vilken ger en god vägledning avseende vad som är mest prioriterat att implementera.

5.1 Genomförande av nyttoanalys

Genomförandet av nyttoanalysen har skett tillsammans med arbetsgruppen och med fokus på följande värderingsområden:

- Verksamhetsnytta
- Införande i verksamhet
- Realisering och förvaltning

Verksamhetsnytta för de funktioner som föreslås implementeras. Kan vara en mängd olika saker som exempelvis:

- Uppfyllnad av organisationens strategiska inriktning såsom effektmål, KPI'er eller relevanta nyckeltal
- Resultatpåverkande (besparingar i tid, kostnader, resursbehov eller liknande)
- Kvalitativa (exempelvis bättre kvalitet vid utförande av vårdinsatser och ökat värdeskapande)
- Bättre upplevelse för patienter, brukare och medarbetare (ökad tillgänglighet och minskade väntetider för behandling, ger positiva effekter på vård- och omsorgsprocesser)
- Effektivisering av processer (tidsvinst vid autentisering, kan använda ett mobila applikationer med höga säkerhetskrav vilket ökar produktiviteten)
- Andra svårvärderade nyttor (exempelvis indirekta nyttor vilka nya bärare kan skapa förutsättningar för)

Införande i verksamhet. Vidare har komplexiteten att införa föreslagna nya lösningar i kundernas verksamheter analyserats. Exempel på komplexitet vid införande i lokala organisationer kan vara:

- Nödvändiga lokala tekniska anpassningar som förutsättning för införandet
- Insatser för att nå bestående förändring (förändringsledning, utbildning, kommunikation, etc.)
- Konsekvenser på organisationen under samt efter införandet
- Tid för att fullfölja införandet
- Risker i samband med införande
- Kostnadsnivå bedömning

Ursprungligen var ambitionen att i så stor utsträckning som möjligt kvantifiera de faktiska nyttorna för att på ett bra sätt kunna ställa olika behov emot varandra. Dock visade det sig under arbetets gång att representanterna från kundgruppen hade svårt att ta fram kalkylunderlag så det är endast i några få fall som nytta och införande har kunnat kvantifieras i värdet av besparingar, effektiviseringar, resursinsatser eller motsvarande.

På grund av detta har vi i de flesta fall baserat nytta respektive komplexitet på en samlad bedömning vilken graderats på en skala.

Realisering & förvaltning. Slutligen har en bedömning av realisering och komplexitet genomförts av Inera. Vid denna analys har vi tittat på ett antal faktorer som exempelvis:

- Standardiseringsgrad (baseras på standardiserade tekniker)
- Sourcingmöjligheter (möjligt att konkurrensutsätta, undvika inlåsningseffekter, mm.)
- Komplexitet vid realisering och löpande förvaltning
- Kostnadsnivå vid implementation (licenser, support, förvaltning, vidareutveckling, etc.)

Inera har fört dialog med utvecklingsteam samt leverantörer för att få en bild av arbetsinsats för realisering av de prioriterade funktionerna. I vissa fall väntar vi fortfarande på svar i samband med att rapporten färdigställs, i dessa fall får den informationen kompletteras vid ett senare tillfälle.

Skala för värdering	1 ->	5
Verksamhetsnytta	Låg	Hög
Införandekomplexitet	Hög	Låg
Realisering & förvaltning	Hög	Låg

5.2 Prioritering samt rekommendation

Ovanstående analyser är sammanställda i tabellen nedan. Kolumnen ”Nytto VÄRDE” är en summering av värderingarna för de tre kategorierna, ju högre värde desto större bedömd kostnadseffektivitet. Högst VÄRDE får således de funktioner som är *enkla att implementera*, *enkla att införa* samtidigt som de ge *störst verksamhetsnytta*.

Kolumnen ”Rekommendation” anger vilka användningsfall som arbetsgruppen anser vara mest prioriterade och bör fokuseras (de som är markerade ”Ja”).

Användningsfall	Verksam-hetsnytta (1-5)	Kund-införande (1-5)	Realisering & förvaltning (1-5)	Nytto VÄRDE	Rekom-menda-tion
eID-bärare som kan kopplas till personlig dator med **standardkontakt (USB-C)**	4	5	3	12	Ja
Kunna använda tillhörande **utrustning i steril miljö**	2	5	5	12	Ja
Inloggning på datorn med SITHS eID	3	4	4	11	Ja
Användaren kan ”blippa” säkert med tvåfaktorsautentisering (kod) mot den mobila enheten för att logga in i **applikationer**	5	4	2	11	Ja
eID-bärare som kan kopplas till delad mobil enhet med **standardkontakt (USB-C)** FIDO2 över USB-C - viktigt för mobila OS för att stödja läsplattor (iPadOS / Android).	5	4	2	11	Ja
Hantera övergång från MIFARE Classic. Åtkomst till lokaler vars passersystem stödjer äldre resp. andra med ny teknik under lång övergångsperiod. Samexistens med MIFARE Classic. Två alternativ: separata kort för DESFire och Classic, eller ett kombinerat kort med DESFire och Classic (EV3C). Se separat beskrivning	5	1	5	11	Ja
E-legitimering med blipp. Som användare vill jag kunna **”blippa” säkert** med [bäraren] och ange min … pin på en ”blipp”-kortläsare ansluten till en tunn klient (Sessionsdator) för att logga in i till min VDI eller till en publicerad applikation. FIDO2	5	3	2	10	Ja

Säker återanslutning: ” …kunna ”blippa” säkert med mitt SITHS kort och *ange min pin på en ”blipp”*-läsare ansluten till en tunn klient (Sessionsdator) för att återansluta min pågående VDI”	5	3	2	10	Ja
Som användare vill jag slippa ange en kod och i stället nyttja **biometri** för autentisering	5	3	2	10	Eventuellt
Modern och säker teknik för **fysisk åtkomst med smartkort**. Stöds via MIFARE DESFIRE i senaste versionen.	5	1	3	9	Ja
Låsning av session: När jag lämnar datorn vill jag kunna ”blippa” och sessionen kopplas ifrån / Windows låses	3	3	3	9	Nej
Stöd för **Windows Hello for Business** via bäraren för SITHS eID Notera att externa bärare inte stöds i konceptet WHB vid nyttjande av biometri, nyckelmaterialet skyddas i TPM.	3	4	1	8	Nej
Mobilen för fysisk åtkomst. Mobilen bärare för ”säker beröringsfri blipp” för inpassering	5	2	1	8	Nej
Mobilen för säker utskrift. Mobilen bärare för ”säker beröringsfri blipp” för utskrift	5	2	1	8	Nej
Kunna använda bäraren för **autentisering lokalt vid avbrott** till centrala tjänster	3	1	3	7	Eventuellt
Personlig dator, **TPM som eID-bärare** för SITHS eID-app (Windows & Mac)	2	4	n/a	6	Nej
SSO upplevelse. Väl inne i VDI´n vill jag sedan … kunna starta samtliga system även de som kräver 2-faktor… utan att	4	1	Denna funktion realiseras ej via bäraren. Ingår i implementation av IdP	5	Nej

behöva ”blippa” [bäraren] på nytt eller ange mina (AD-) inloggningsuppgifter under hela mitt arbetspass.					
Som användare önskar jag i inloggat läge kunna starta samtliga appar, även de som kräver 2-faktor utan att behöva "blippa" kortet på nytt, eller ange inloggningsuppgifter. En SSO upplevelse.	4	1	Denna funktion realiseras ej via bäraren. Ingår i implementation av IdP	5	Nej
Närvaroavkänning: ”När jag lämnar datorn skall sessionen kopplas ifrån / Windows låses automatiskt.”	1	3	Har ej hittat relevant teknisk lösning	4	Nej
Användaren kan ”blippa” säkert med tvåfaktorsautentisering (kod) mot den mobila enheten för att logga in i enheten (**operativsysteminloggning**)	2	1	Hanteras via operativsystem	3	Nej