inera
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

Referensarkitektur för Identitet och Åtkomst

Utformning av IT-stöd för säkerställd identitet och åtkomst till rätt information vid rätt tillfälle

Version 1.0 PA2

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

Innehåll

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

1 Dokumentinformation

1.1 Revisionsinformation

Version	Datum	Beskrivning	Författare
0.1	2016-10-12	Utkast 1, huvudstruktur	Per M
0.8	2016-10-31	Utkast för intern granskning i arbetsgruppen.	Per M
0.9	2016-11-06	Justeringar efter intern granskning i arbetsgruppen. Viss omstrukturering. Större revidering/komplettering av Kap 6.	Per M
0.97	2016-11-14	Revidering för slutgranskning arbetsgruppen.	Per M
1.0 PA1	2016-11-15	Version 1 för leverans och vidare förankring. Not: Planeras för en ytterligare version i dec-2016, där viss komplettering/justering kan bli aktuell, såsom fördjupning kring kap. 5.11, 5.12.	Per M
1.0 PA2	2016-11-22	Mindre redaktionella justeringar	Per M

1.2 Referenser[1]

Id	Referens/dokument
SIS-TR50:2015	SIS-TR 50:2015 Terminologi för informationssäkerhet, http://www.sis.se
Socialstyrelsens termbank	http://termbank.socialstyrelsen.se
RIVTA	Regelverk för interoperabilitet inom vård och omsorg, Tekniska anvisningar http://rivta.se
T-boken	VIT(S)-bokens tekniska arkitektur. Styrande principer, vägledande exempel och teknisk referensarkitektur för vård och omsorg. http://rivta.se/documents/ARK_0019/

[1] Övriga referenser anges primärt som fotnot i löpande text.

1.3 Grundläggande begrepp och termer

Identitets- och åtkomsthantering (Identity and Access Management, IAM) – sammanfattande benämning på det område som hanterar användares e-identiteter och behörighetsstyrande egenskaper, åtkomst till information i IT-system och regelverken som styr åtkomsten.

Singelinloggning (Single sign-on, SSO) – en användare behöver endast logga in en gång för att nå de system som är anpassade till tjänsten. SSO är ett ganska vitt begrepp och det finns flera ”undervarianter” som alla kan kombineras: användaren återkommer till samma system inom en viss tid och slipper logga in igen; användaren går in i flera system med en gemensam inloggning; användaren kan använda samma inloggningsfunktion för flera olika system. Det senare kan även ses som en *samordnad* inloggning.

Singelutloggning (Single sign-off / Single Logout , SLO) – en användare kan med en åtgärd logga ut sig ur flera system som hen är inloggad i.

Regulatoriskt regelverk – sammanhållande term för lagar, förordningar, informationssäkerhetspolicys etc. som är styrande för hur lösningarna utformas.

Egenskaper/attribut – i detta sammanhang synonyma begrepp för egenskaper för medarbetare/användare, organisationsenheter och IT-systemresurser. T.ex. yrkeslegitimation för personal.

PKI-infrastruktur (Public Key Infrastructure, PKI) – en IT-infrastruktur där asymmetrisk kryptering med långa publika och privata nycklar används för att t.ex. åstadkomma autentisering med hög tillit mot IT-system.

Identifiering – en process där en aktörs identitet fastställs, oftast med krav på *autentisering*.

Autentisering – kontroll av uppgiven identitet[2]. Kontrollen sker mot något slags ”äkthetsbevis” som styrker identitetens riktighet. Autentisering i IT-system baseras normalt på något man vet, något man har eller någon egenskap hos användaren (biometri). Autentiseringen kan baseras på en eller flera av sådana faktorer, t.ex. enbart ett hemligt lösenord (*enfaktorautentisering*) eller både ett tumavtryck och innehav av personlig smart mobil (*tvåfaktorautentisering*) osv.
Inom svensk författning används även begreppet ***stark autentisering*** – ”autentisering som innebär att identiteten kontrolleras på två olika sätt” [3]. För att räknas som ”stark” i detta sammanhang ska autentiseringen alltså baseras på (minst) två faktorer, men man

[2] Socialstyrelsens termbank

[3] SoSFS2008:14

bör även lägga till krav på att personens identitet har säkerställts på ett tillräckligt säkert sätt i samband med utfärdande av dennes e-identitet.

Certifikatsbaserad inloggning, även kallad ***PKI-baserad inloggning***. Denna typ av inloggning innebär att certifikat och asymmetrisk kryptografi används för autentisering, genom att på ett säkert sätt fastställa att ett certifikats uppgifter avser just den användare som just nu försöker logga in. Exempel på teknik som stödjer detta är x509-certifikat lagrade på smarta kort, s.k. ”hårda certifikat” (t.ex. SITHS-kort).

Utfärdande av e-identitet – en process för att en person får tillgång till en e-identitet att använda för åtkomst till e-tjänster. Utfärdandet kan t.ex. innebära att en säkerhetsdosa registreras kopplat till ett användarkonto eller att personen får en e-legitimation för kommunikation med myndigheter. En person kan ha flera e-identiteter, men som alla unikt identifierar personen.
Ofta används även begreppet ***Enrollment*** för registrerings- och utfärdandeprocesser som användaren själv hanterar, t.ex. när personens biometriska data registreras i mobilen så att personen senare kan logga in med t.ex. fingeravtrycket.

e-identitet, e-ID – elektronisk identitetshandling för legitimering mot IT-system.

e-identitetsutfärdare – tillhandahåller e-identitet till användare.

e-identitetsbärare – bärare/media där e-identiteten förvaras. Kan t.ex. vara en fil på USB-sticka, ett smart kort eller ett utrymme på en smart mobil.

Ärvd legitimering – process för att skapa en ny elektronisk identitet med en annan som underlag. Ex. kan en mobil elektronisk identitet skapas med hjälp av att användare loggar in med en elektronisk identitet i en tjänst för självadministration.

Identifieringstjänst (Identity Provider, IdP) – Tjänst i IT-infrastrukturen som utför autentisering av användare på begäran, och via en ***Identitetsintygsutfärdare*** vidarebefordrar ***identitetsintyg*** till e-tjänst med uppgifter om en identifierad användare. Identifieringstjänst ingår i flera säkerhetsarkitekturer med lite olika benämningar. Typiskt är att uppgifterna paketeras i s.k. ***intyg*** även kallade ***biljetter*** och ***tokens***.

e-tjänst – en IT-tillämpning/applikation som tillhandahålls till slutanvändare över nätet.
Service Provider (SP) – e-tjänst som tar emot intygade uppgifter om vem användaren är och dennes egenskaper och i syfte att kunna logga in användaren i e-tjänsten. Även kallad ***Relying party (RP)*** och ***Identity Consumer***.

Åtkomstintygsutfärdare – Tjänst i IT-infrastrukturen som utfärdar ***åtkomstintyg*** för åtkomst till skyddade integrationsgränssnitt. Även kallad ***Tokentjänst*** eller ***(Security) Token Service***.

Auktorisation – (här) en process för att avgöra om en aktör (användare eller system) har rättighet till viss information och/eller funktion. Det regelverk som sätts för detta kallas ***auktorisationsregler***.

Provisionering av identitetsdata – *(här)* process för att tillhandahålla kvalitetssäkrad information om identiteter och tillhörande egenskaper, t.ex. i syfte att skapa användarprofiler i identitetsdatalager och e-tjänster.

Federation – en överenskommelse mellan parter där man inom federationen har överenskomna gemensamma regler och att parterna litar på varandra att upprätthålla dessa regler. Inom identitets- och åtkomsthantering avses oftast en ***identitets- och behörighetsfederation***.

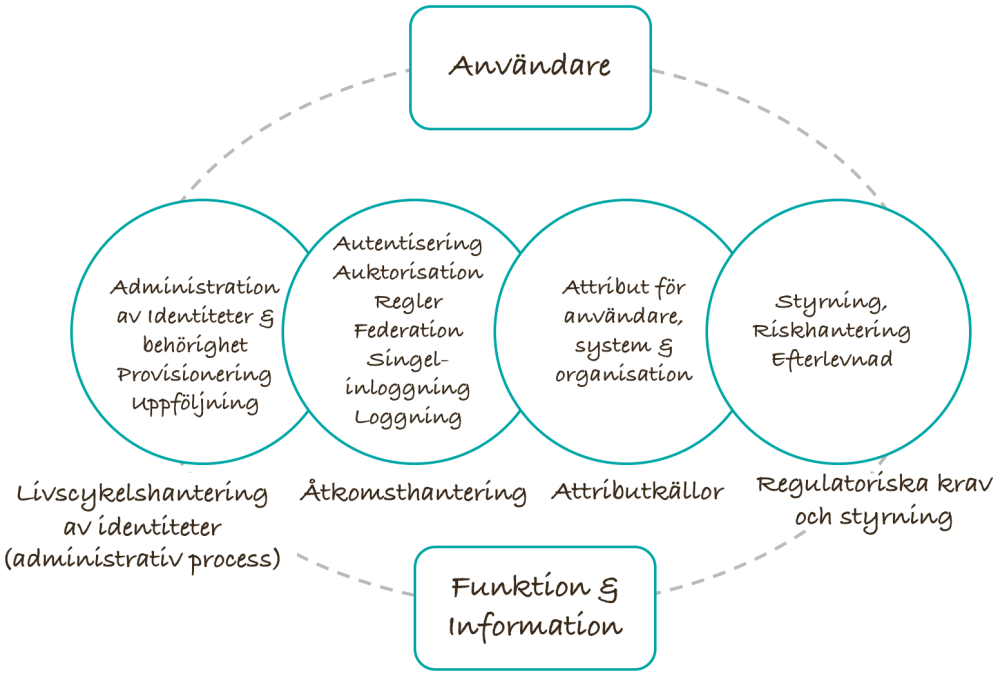
Klientdator – begrepp som refererar till datorer, mobila enheter och andra fysiska enheter som användare kan använda för att nå sitt IT-stöd. Se även *eKlient i samverkans* standard ”klassificering av klienter”.[4]

Klient (user agent) – den programvara som exekverar på klientdator och agerar användarens gränssnitt.

[4] http://www.inera.se/Documents/TJANSTER_PROJEKT/eKlient

2 Området Identitets- och åtkomsthantering

Det övergripande området som referensarkitekturen för Identitet och åtkomst ska stödja brukar kallas *Identitets- och åtkomsthantering*, på engelska *Identity & Access Management*, eller kort *IAM*.



Figur 1. Området Identitets- och åtkomsthantering

Området innehåller många olika delar som tillsammans syftar till att ge användare rätt tillgång till funktioner och information vid rätt tillfälle. Det användaren upplever som *singelinloggning*, *SSO*, är ofta ett resultat av en god samverkande arkitektur för identitet och åtkomst, med flera olika tjänster som levererar ”sin” del.

Styrande för vilken säkerhetsnivå som ska sättas är i huvudsak de regulatoriska kraven (lagar, föreskrifter etc.), informationens skyddsvärde samt verksamhetens riskbedömningar.

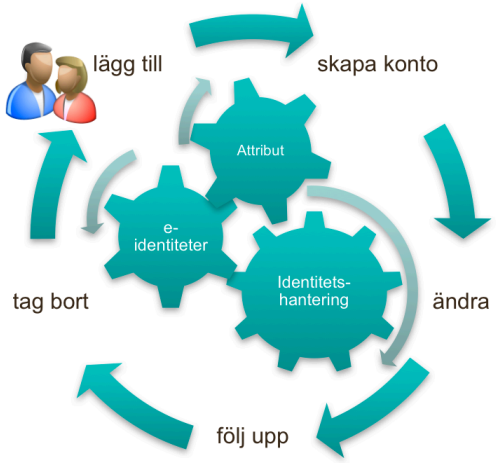
Referensarkitekturen för Identitet och åtkomst syftar till att kunna stödja de olika regelverk som gäller för respektive sektor/verksamhetsområde, t.ex. hälso- och sjukvård, omsorg, skola, samhällsbyggnad osv.

Till exempel läggs grunden till säkerhetskraven inom hälso- och sjukvården i *Patientdatalagen*[5] och *SOSFS 2008:14*[6] föreskrifter och handbok.

Organisationens riktlinjer för informationssäkerhet konkretiserar kravbilden ytterligare, t.ex. autentiseringskrav för åtkomst till olika typer av uppgifter, krav på behörighetstilldelning baserat på anställning och tilldelade arbetsuppgifter, krav på uppföljning av åtkomst till uppgifter osv.

En grundförutsättning för att säkerställa rätt åtkomst till rätt individ är kvalitetssäkrade uppgifter om användare (medarbetare), organisationer och tillhörande egenskaper/attribut. Dessa uppgifter hanteras ofta i olika slags katalogtjänster – *attributkällor* – för att utgöra grund för användarkonton, utgivning av e-identiteter, rätt koppling till organisation, uppdrag, behörigheter osv.

I organisationen behöver normalt olika källor som HR-system, personal- och organisationskatalog och IT-systemens kataloger synkroniseras och datakvaliteten säkerställas, rättigheter tas bort när personal slutar osv. Kort sagt behövs en *livcykelhantering av e-identiteter* och tillhörande egenskaper.



Figur 2: Livcykelhantering av e-identiteter

När väl en användare loggar in i sitt IT-stöd för att få tillgång till information, behöver ett antal funktioner vara på plats för att säkerställa identitet och rättigheter, såsom autentisering och auktorisation av användaren.

[5] SFS 2008:355, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/patientdatalag-2008355_sfs-2008-355

[6] http://www.socialstyrelsen.se/sosfs/2008-14

Referensarkitekturen syftar i stort till att beskriva en modell för hur dessa funktioner kan realiseras i IT-stödet och vilka krav som ställs på e-tjänster respektive IT-infrastruktur.

3 Styrande principer

Vad är styrande för utformning av referensarkitekturen och varför?

3.1 Generella styrande principer

Från *Teknisk referensarkitektur för vård och omsorg* [T-boken] har hämtats ett antal generella styrande principer med syfte att säkerställa spårbarhet, skalbarhet, flexibilitet och interoperabilitet i IT-system. Flertalet av dessa applicerar även direkt på området Identitet och åtkomst. Vi sammanfattar dessa här:

- Informationssäkerhet (IT2)
  - Tillgänglighet, sekretess, riktighet och spårbarhet ska säkerställas vid all samverkan.
- Skalbarhet (IT3)
  - Skalbarhet från lokalt till nationellt och vice versa. Lösningarna behöver kunna appliceras såväl på det lokala planet som det nationella. Arkitekturen ska inte begränsa dess användning i detta avseende.
- Lös koppling & interoperabilitet (IT4)
  - Innebär bl.a. att en komponent i en lösning kan bytas ut oberoende av andra.
  - Uppnås genom en tjänstebaserad arkitektur med kommunikation genom gemensamma, standardiserade gränsytor mellan komponenter.
  - Interoperabla, internationellt beprövade och för leverantörer tillgängliga (öppna) standarder tillämpas för meddelandeutbyte mellan system.
- Samverkan i federation (IT6)
  - Samverkan över organisationsgränser sker genom federation, såsom exempelvis identitetsfederering.
  - Federation bygger på gemensamma överenskomna regelverk, t.ex. kring krav på autentisering av användare i IT-system, tekniska regelverk osv.

3.2 Styrande principer för Identitet och åtkomst

Inom området Identitet och åtkomst definierar referensarkitekturen följande kompletterande och fördjupande styrande principer:

- **#IA1:** e-tjänsterna respektive IT-infrastrukturen för identitet och åtkomst separeras genom standardiserade gränssnitt.

  Motiv: Ger en lös och standardiserad koppling mellan e-tjänsterna och de generella funktionerna för identitet och åtkomst. Produktanpassningar blir applicerbara på en global marknad, och bättre förutsättningar för att marknadens produkter kommer anslutningsklara från början. Skapar även grundförutsättningar för en samlad administrationspunkt, federativa lösningar och återanvändning av investeringar i säkerhetsteknik. Minskar inlåsningseffekterna mot viss hårdvara och mjukvara.

- **#IA2**: Inloggning till IT-stödet sker i gemensam inloggningstjänst i IT-infrastrukturen.

  Motiv: Underlättar att skapa en samordnad användarinloggning med hög igenkänningsfaktor och hög tillit. Ökar flexibiliteten och möjliggör att lägga till nya inloggningsmetoder som är anpassade för verksamheten utan att påverka anslutna e-tjänster.

- **#IA3**: e-tjänster ansluts till IT-infrastrukturen för inloggning i första hand via standardiserad s.k. biljettbaserad teknik som levererar identitetsdata och grundläggande behörighetsgrundande information (attribut).

  Motiv: Gränssnittet mot e-tjänsten blir stabilare över tid då det inte påverkas av nya användarkrav på inloggningsfunktionen eller den senaste autentiseringstekniken, vilket ger ökad förvaltningsbarhet och minskade kostnader för IT-säkerhetslösningar. E-tjänsten kan i första hand fokusera på den verksamhetsfunktion den ska leverera.

- **#IA4**: e-tjänster använder federerad identitetsdata och behörighetsgrundande information i utgivet identitetsintyg som bas för en behörighetsprofil i e-tjänsten. Vid behov kompletterar e-tjänsten med ytterligare uppgifter kopplat till användaren för att avgöra de rättigheter användaren ska ha till information och funktioner i e-tjänsten.

  Motiv: en gemensam bas för identitet och behörighet skapar förutsättning för god skalbarhet och minskad administrativ börda i verksamheterna. Identitets- och behörighetsadministration kan konsolideras till en funktion där en användare samlat kan ges grundläggande rättigheter att arbeta med de IT-system och den information som hens arbete kräver. Även borttag av rättigheterna (t.ex. när medarbetare slutar anställning) underlättas.

- **#IA5**: IT-infrastruktur för identitet och åtkomst byggs i grunden plattformsneutral. Eventuella plattformsspecifika delar läggs till som anpassningar ovanpå grundstrukturen.

  Motiv: IT-infrastruktur för identitet och åtkomst (såsom inloggningsfunktionalitet) behöver kunna nyttjas för alla de olika typer av e-tjänster och enheter som ingår i verksamhetens IT-stöd: webb, tunna och feta klienter, mobila plattformar osv. Alternativet är att bygga, förvalta och administrera parallell IT-infrastruktur, vilket är resurs- och kostnadsdrivande.

- **#IA6**: Tillit till andra organisationers IT-lösningar för identitet och åtkomst skapas via öppna gemensamma regelverk, s.k. *tillitsramverk*. I första hand används standardiserade tillitsramverk när sådana finns att tillgå.

  Motiv: Genom öppna beskrivna tillitsramverk som kan delas av de parter som behöver kommunicera, kan man undvika att behöva skapa många bilaterala överenskommelser, som även riskerar att divergera och skapa suboptimerade lösningar.

- **#IA7**: Flerfaktorautentisering (två eller flera oberoende faktorer), samt en tillräckligt säker utgivningsprocess för e-identiteten, ger förutsättning för s.k. *stark autentisering*. För att kunna jämföra styrkan i olika autentiseringslösningar bestäms autentiseringslösningens *tillitsnivå* relativt ett överenskommet tillitsramverk.

  Motiv: Gemensam syn på vad som är tillräckligt för stark autentisering är en viktig förutsättning för samverkan mellan organisationerna. Genom kopplingen till tillitsramverk blir olika autentiseringslösningar jämförbara med varandra.

- **#IA8:** Arkitekturen för identitet och åtkomst behöver kunna stödja flera *alternativa e-identitetsbärare* för stark flerfaktorautentisering.

  Motiv: Ger en flexibilitet som bättre kan stödja olika verksamhetsbehov och därmed minska trösklarna för att införa säkra autentiseringslösningar i verksamheterna. Med anpassade lösningar för identifiering för det IT-stöd som används, ökar möjligheterna till en upplevd snabb inloggning. Ger även ökade möjligheter till säker inloggning i mobila plattformar.

- **#IA9:** Arkitekturen för identitet och åtkomst ska vid behov tillåta autentisering i separat *säkerhetskanal* skild ifrån *informationskanalen* (där användaren arbetar med informationssystemet), även kallad *out-of-band authentication*.

  Motiv: autentisering i separat kanal medför minskat beroende till vilken hårdvara som kan användas som kanal för informationssystemet, t.ex. en läsplatta, en digital whiteboard i korridoren, en kapslad tryckskärm i en operationsavdelning osv. Alternativet, att alltid endast använda samma kanal för både information och

autentisering, lägger starka tekniska krav och begränsningar på den utrustning som kan användas i IT-stödet.

- **#IA10:** Vid användning av biometri för autentisering bör biometrisk data hållas nära användaren själv, helst endast inom användarens personliga e-identitetsbärare. Biometri bör inte användas som den enda faktorn i en autentiseringslösning.

  Motiv: Biometriska data är integritetskänslig information. Det kan finnas fall då biometrisk data har ett värde att hanteras och lagras i ett centralt register, men detta bör alltså undvikas främst pga. integritetsskäl. Biometri rekommenderas inte i enfaktorslösningar, eftersom det inte går att återkalla (*”revokera*)” en persons biometriska data.

4 Verksamhetsvy – behov, förmågor och flöden

Verksamhetsvyn beskriver referensarkitekturen utifrån verksamhetens behov, och lyfter fram de förmågor inom området Identitet och åtkomst som behövs för att stödja behovet. Huvudsakliga flöden beskrivs.

4.1 Verksamhetsbehov och drivkrafter kopplat till identitet och åtkomst

Referensarkitekturen syftar bland annat till att möta följande behov i verksamheterna:

- Uppfylla regulatoriska krav och behov av informationsskydd, t.ex. krav på stark autentisering och möjlighet att följa upp åtkomst till information.
- Samordnad, enkel och säker singelinloggning (SSO) för medarbetarna till lokalt, regionalt och nationellt IT-stöd (e-tjänster).
- Möjliggöra flexibla inloggningssätt anpassade både till verksamheten och informationssäkerhetskrav.
- Möjliggöra mobila arbetssätt, både vad gäller medarbetarnas rörlighet och användning av mobila plattformar för informationsåtkomst.
- En samlad och kvalitetssäkrad hantering av användaridentiteter och behörigheter i IT-stödet, utan onödig administration.
    - En samordnad administrativ vy inom organisationen, där systemövergripande grundläggande användarprofiler kan sättas utifrån säkrade masterdata och beslut om behörighetstilldelning.
    - Smidiga och säkra sätt att förse användare med säkra e-identiteter för inloggning.
- Flexibla säkerhetslösningar till rimlig kostnad och hanterbar förvaltning
    - Utveckling av proprietär säkerhetsteknik i e-tjänsterna är inte kostnadseffektivt och skapar inlåsningseffekter.
    - Anslutning till säkerhetstekniken behöver vara standardiserad, så att kostnaderna kan hållas nere, förändringstakten kan ökas i informationssystemen, samt en stabil förvaltning kan upprätthållas.
- Minskat teknikberoende - kunna använda olika tekniska verktyg (mobila plattor, tryckkänsliga tavlor, smartmobiler, terminaler osv.) för att nå information på olika

sätt anpassade till verksamhetens behov, utan teknisk låsning till vald säkerhetsteknik.

- Säker åtkomst till information inte bara genom ett system, utan via vyer till flera bakomliggande informationstjänster, utan extra inloggningar.
- Kunna samverka kring IT-lösningar över organisationsgränser, utan att säkerhet och identitet- och behörighetshantering blir ett hinder, t.ex.
  - Samverkan via nationella och regionala e-tjänster.
  - Gemensamma verksamhetsstöd över organisationsgränser.
  - Samverkan med myndigheter – t.ex. krav på federativ anslutning för att nå myndigheters informationstjänster.
  - Nyttja molntjänster hos extern tjänsteleverantör via egen befintlig IT-infrastruktur och identitetshantering baserat på överenskommelse.

Behoven styr referensarkitekturen i en riktning mot

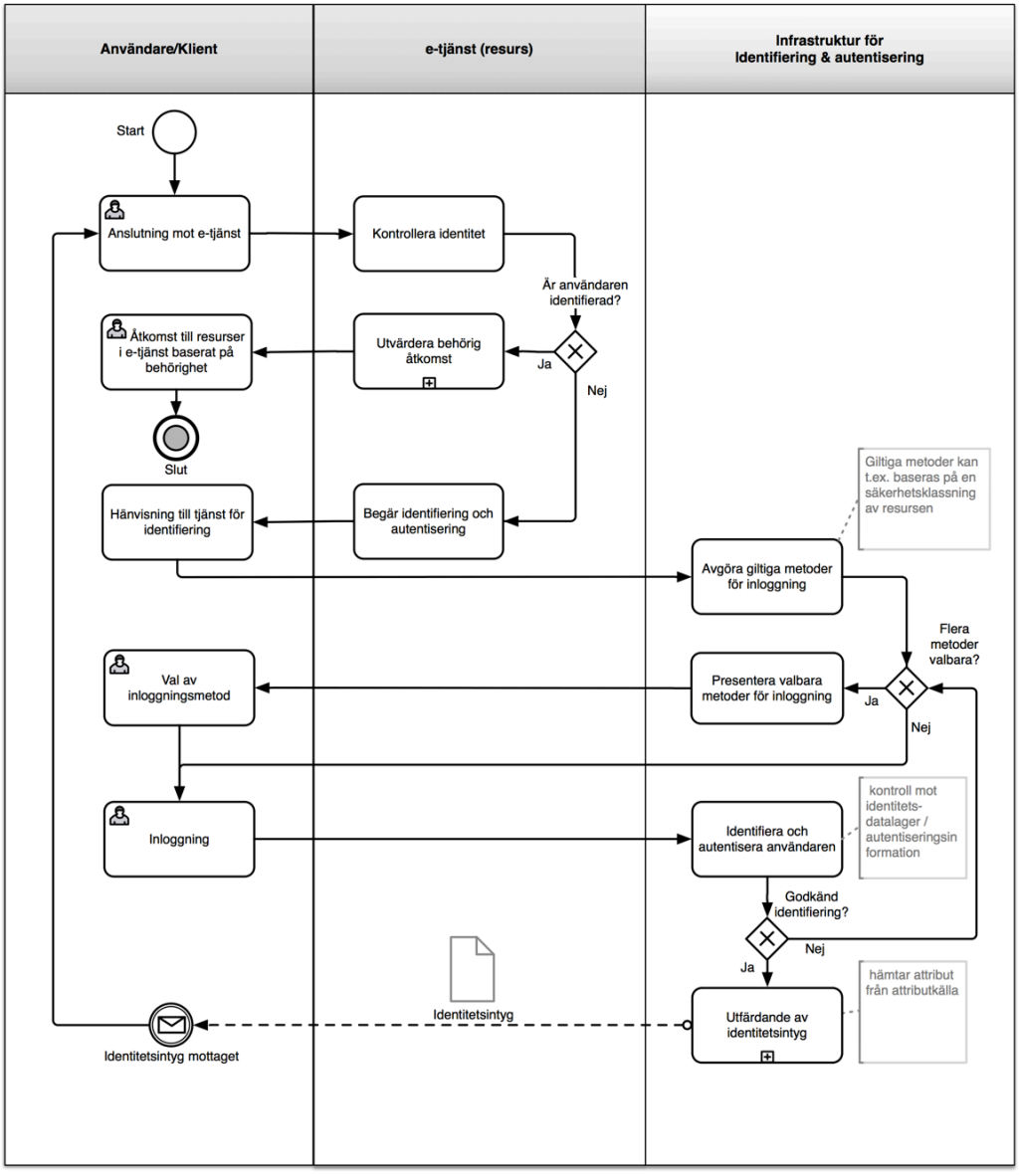
- Standardisering av säkerhetstekniken och gränsytorna mot övrigt IT-stöd.
- Separation av förmågor där respektive delsystem fokuserar på det den är ämnad för, t.ex. att tydligt skilja på att hantera säker inloggning respektive hantera verksamhetsinformation.
- Plattformsneutrala gemensamma lösningar som medger flexibilitet i teknikval.

I de följande kapitlen kommer några huvudsakliga flöden gås igenom som behövs för att hantera säker identifiering och ge rätt åtkomst till information (resurser) utifrån en samlad identitetshantering. I Informationssystemsvyn kommer dessa flöden och förmågor sedan omsättas i samverkande tjänster.

4.2 Inloggning - identifiering och autentisering

Följande flöde beskriver inloggning i en e-tjänst. Flödet stöder singelinloggning, dvs. ifall användaren redan är inloggad, behöver hen inte upprepa inloggningssteget.

Flödet omfattar identifiering och autentisering av användaren, där dessa förmågor hanteras av en separat betrodd IT-infrastruktur skild ifrån e-tjänsten (princip IA2). ”Beviset” på att identiteten verifierats kommuniceras till e-tjänsten i form av ett identitetsintyg som utfärdats av den betrodda tjänsten (princip IA3).



Figur 3. Flöde för inloggning i e-tjänst inklusive identifiering och autentisering

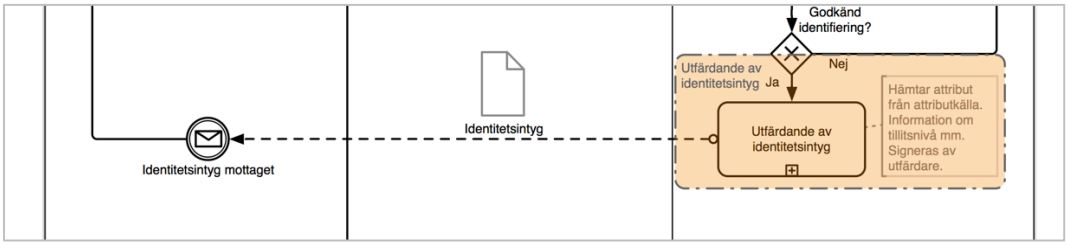
Tjänsten för inloggning ska ge stöd för att tillhandahålla flera möjliga inloggningsmetoder som är anpassade för verksamhetens behov och situation, t.ex. mobila arbetssätt (enligt princip IA2).

För att hantera detta i verksamhetens IT-stöd behövs följande förmågor etableras i IT-infrastrukturen:

- Identifiering och autentisering (*Identifieringstjänst*)
- Val av inloggningsmetod (*Inloggningstjänst*)
- Stöd för olika inloggningsmetoder, eller mer precist autentiseringsmetoder (*Autentiseringstjänster*)
- Utfärdande av identitetsintyg (*Identitetsintygsutfärdare*), vilket skapar en säker men lös teknisk koppling mellan e-tjänsterna och säkerhetslösningarna i IT-infrastrukturen.

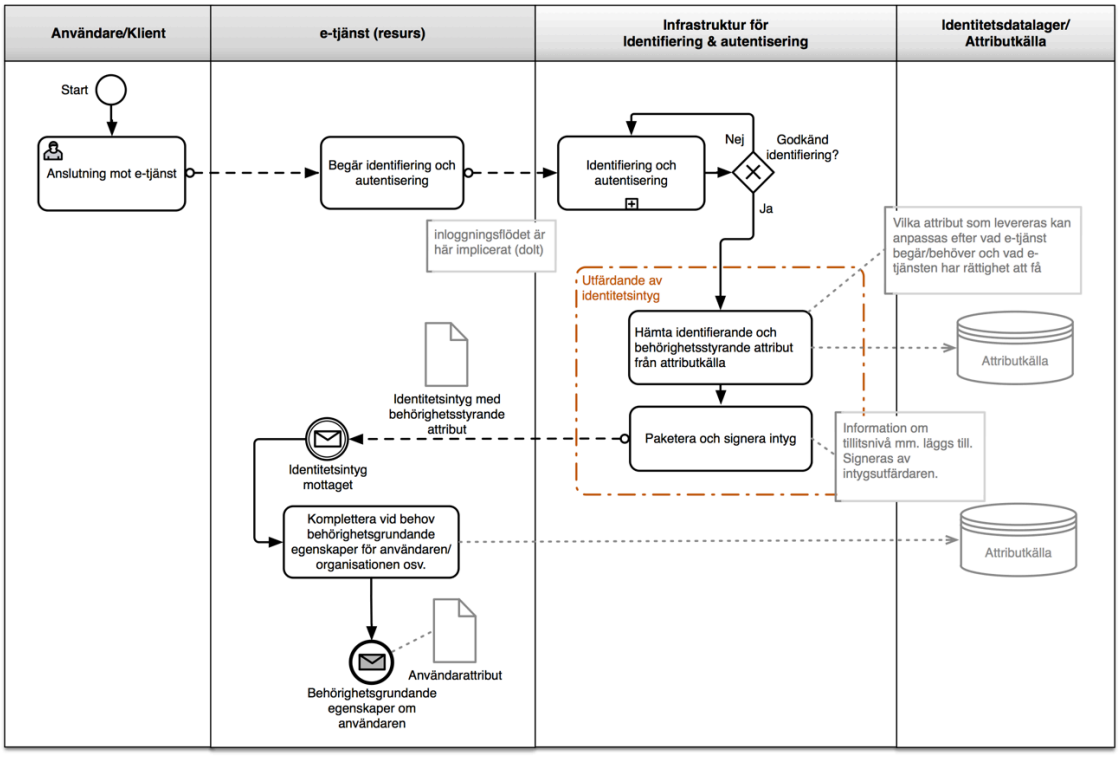
4.3 Utfärdande av identitetsintyg

I flödet för inloggning i e-tjänst ovan ingick ”utfärdande av identitetsintyg”.



Figur 4. Utfärdande av identitetsintyg, som del av identifieringsprocessen

I det följande tittar vi närmare på vad som krävs för detta delflöde. Vi döljer här för enkelhets skull själva inloggningsflödet, och förutsätter att användaren identifierats på ett godkänt sätt. Den betrodda *Identitetsintygsutfärdaren* utfärdar därefter ett identitetsintyg där uppgifter om användaren hämtas från en betrodd attributkälla. Intyget signeras med utfärdarens privata nyckel och levereras till e-tjänsten.



Figur 5. Utfärdande av identitetsintyg.

Av intyget behöver framgå bland annat

- Identifierande attribut.
- Behörighetsgrundande attribut.

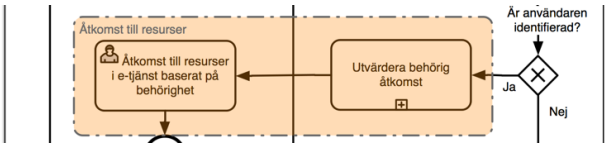
- Uppgift om använd autentiseringsmetods styrka (den tillit som metoden att verifiera användarens identitet har).
- Vem som utfärdat och signerat intyget.

Utgående från identitetsintyget kan e-tjänsten behöva kompletterande uppgifter för att fullt ut kunna avgöra användarens rättigheter till resurser i e-tjänsten, t.ex. ytterligare information om användarens organisation osv. Dessa hämtas vid behov från i första hand betrodda masterdatakällor, i figuren angiven som en ytterligare attributkälla.

Ovan uppgifter kallas här med en sammanhållande term *Användarattribut*, vilka utgör underlag för både identifiering av användaren samt en del av utvärderingen av behörig åtkomst, vilket vi kommer till i nästa avsnitt.

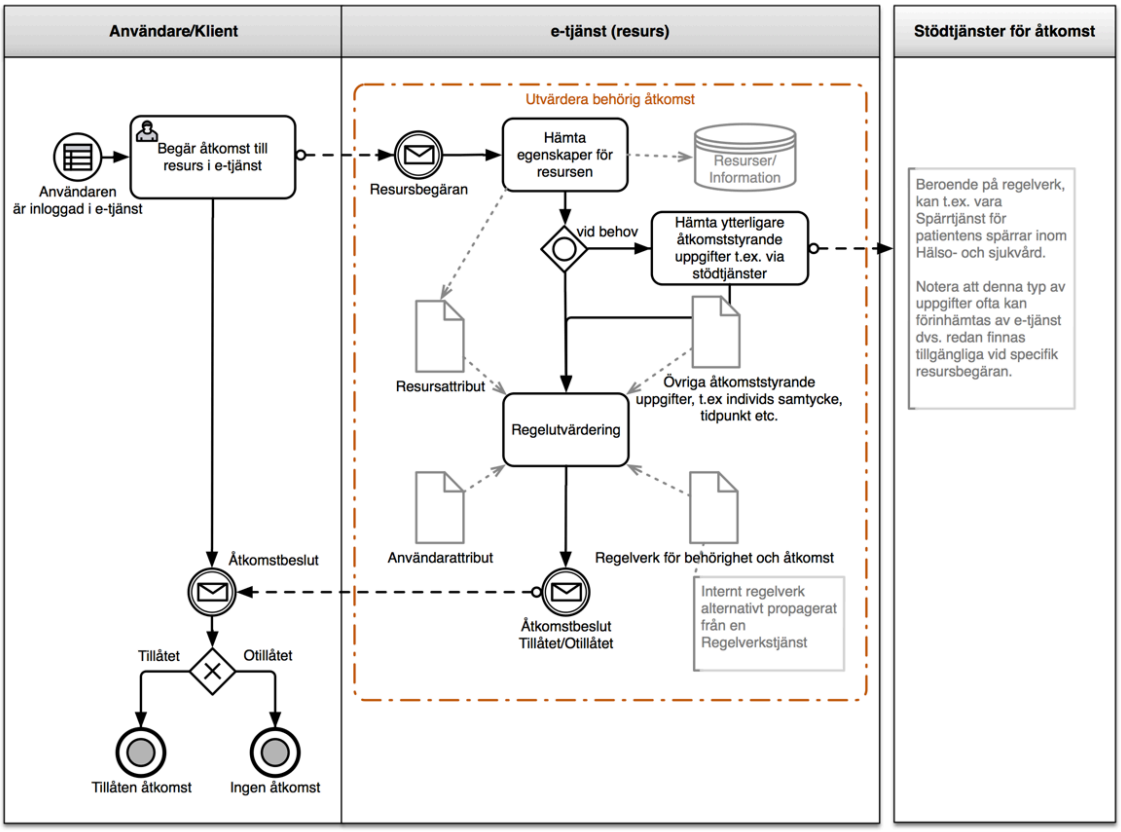
4.4 Åtkomst till resurser

Som en del av flödet för inloggning till e-tjänst ingår även ”åtkomst till resurser” enligt nedan, vilket i sin tur bygger på en utvärdering av behörig åtkomst till resurserna.



Figur 6. Åtkomst till resurser, som del av inloggningsflödet till e-tjänst

Referensarkitekturen ger (enligt princip IA4) stöd för ett skalbart sätt att hantera utvärdering av behörig åtkomst baserat på inhämtade attribut, s.k. *attributsbaserad* (även *egenskapsbaserad*) *behörighetsstyrning*. Genom att använda attribut från separata betrodda attributkällor för identiteter och behörigheter, kan åtkomst och behörighet administreras samlat och åtskilt ifrån e-tjänsterna. Detta ger stöd för att realisera en sammanhållen administrationsvy för att hantera identiteter och behörigheter i verksamheten.



Figur 7. Åtkomst till resurser inklusive utvärdering av behörig åtkomst

E-tjänsten får en resursbegäran från användaren och ansvarar för att utvärdera om åtkomst ska tillåtas eller inte. Med resurser avses här både funktioner (åtgärder) och information.

E-tjänsten ansvarar för en utvärdering av det gällande regelverket mot det underlag som finns och därefter fatta ett åtkomstbeslut. Denna förmåga brukar även kallas *Policy Decision Point (PDP)*.
Notera att e-tjänsten kan delegera regelutvärdering till någon extern komponent (ofta kallad *regelmotor*) som e-tjänsten litar på om så önskas, men det är inget krav; regelutvärderingen kan även vara en helt intern funktionalitet inom e-tjänsten.

E-tjänsten tar sedan och effektuerar åtkomstbeslutet och ger (något förenklat) antingen tillgång eller inte tillgång till efterfrågad resurs. Denna förmåga brukar även kallas *Policy Enforcement Point* (*PEP*). Självklart kan även resultatet vara en filtrerad tillgång till uppgifter baserat på åtkomstbesluten.

Underlaget för regelutvärderingen består generellt av följande delar:

- *Regelverk för behörighet och åtkomst* till resurser som hanteras inom e-tjänsten.
- *Användarattribut* – egenskaper hos användaren (aktören), primärt förmedlad via identitetsintyget, men kan även vara kompletterande uppgifter från andra masterdatakällor. Till användarattribut räknas även egenskaper kopplade till dennes organisation, uppdrag, och uppgift om aktuell användarautentisering etc.
- *Resursattribut* – egenskaper hos resursen, t.ex. vem som skapat informationen, informationsägare, begärd åtgärd, t.ex. läsa, signera, registrera, handlägga ärende etc.
- *Andra åtkomststyrande uppgifter*, t.ex. uppgift om individs samtycke till att ta del av hens uppgifter i systemet, tidpunkten på dygnet osv.

Notera att ovan underlag dels kan komma ifrån identitetsintyget och andra externa masterdatakällor, men även internt ifrån e-tjänsten, beroende på e-tjänstens förutsättningar. E-tjänster som konsekvent tillämpar principerna i referensarkitekturen, hämtar uppgifterna ifrån gemensamt identitetsdatalager och externa masterdatakällor där tillämpligt, så att verksamheten ges möjligheter till en fullt ut sammanhållen identitets- och behörighetsadministration.

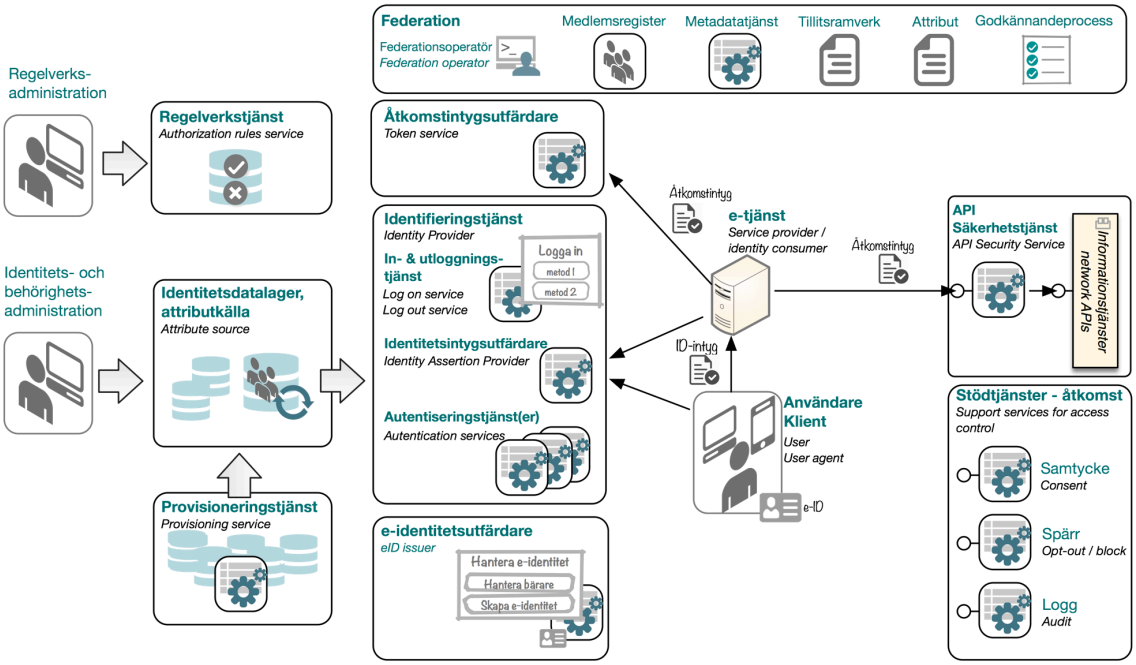
Regelverket för behörighet och åtkomst kan vara (och är oftast) internt inom e-tjänsten, då det är nära förknippat med verksamhetsreglerna för just denna e-tjänst. Referensarkitekturen ger dock även möjligheter där så är lämpligt att nyttja en extern *Regelverkstjänst* där regelverket administreras och sedan förs över till e-tjänsten på ett maskinläsbart format. Denna ger dock mest skalfördelar när behov finns att hantera gemensamma regler i ett stort antal informationstjänster.

5 Informationssystemvy – uppdelning i tjänster

Informationssystemvyn beskriver en referensarkitektur för hur samverkan och funktion uppstår via tjänster i IT-stödet. Vilka infrastrukturtjänster behöver vi för att realisera/besitta beskrivna förmågor?

5.1 Referensarkitektur för Identitet och åtkomst – en översikt

Referensarkitekturen för Identitet och åtkomst innehåller ett antal IT-infrastrukturtjänster som realiserar de förmågor som behövs, och som tillsammans syftar till att tillhandahålla ett användarvänligt, säkert, kostnadseffektivt och skalbart stöd för att ge användare tillgång till funktionalitet och information som användaren behöver och har behörighet till.



Figur 8 Referensarkitektur Identitet och åtkomst – översikt

En användare får tillgång till funktion och information via en *e-tjänst*, som kan vara någon typ av informationssystem: portal, vårdinformationssystem, administrativt system, mobil app, gemensam nationell e-tjänst eller dylikt.

Federerad inloggning via stödtjänster

E-tjänsten får hjälp av stödtjänster att säkerställa användarens identitet enligt ett federativt mönster, även kallat *federerad inloggning*. Man kan säga att e-tjänsten har ”outsourcat” inloggning och autentisering av användaren till en betrodd IT-infrastruktur med samlingsnamnet *Identifieringstjänst*.
Via en gemensam *in- och utloggningstjänst* kan användaren bli säkert autentiserad med någon vald metod via en *autentiseringstjänst*. *Identitetsintygsutfärdaren* levererar vid lyckat resultat ett *identitetsintyg* till e-tjänsten. E-tjänsten kan med hjälp av identitetsintyget ge användaren tillgång till e-tjänsten.

Singelinloggning

Identitetsintygstutfärdaren kan även etablera en säker session med användarens klient (t.ex. en webbläsare) för s.k. *singelinloggning* (*SSO*). Så länge den säkra sessionen gäller kan identitetsintygsutfärdaren acceptera nya begäran om intyg utan att avkräva att användaren autentiserar sig igen.

Underlag för auktorisation

Intyget ger även en grundläggande profil (egenskaper) för användaren, som kan ligga till grund för behörighetsbeslut (*auktorisation*) inom e-tjänsten. E-tjänsten kan behöva komplettera den grundläggande profilen med ytterligare information, använda internt definierad behörighetsstyrning, samt använda ytterligare *stödtjänster för åtkomst*, för att hantera det slutliga behörighetsbeslutet.

Identitetsdatalager och provisionering

Ett betrott intygsutfärdande kräver en kvalitetssäkrad bakomliggande information om användaren, hanterad i *identitetsdatalagret*, även kallad *attributkällan*. Delar av informationen i attributkällan kan härröra från processer i verksamheten, t.ex. personaladministrationen som sätter grundläggande egenskaper för en anställd medarbetare, t.ex. befattning. Andra delar kan hämtas från externa källor, t.ex. uppgift om legitimation i Socialstyrelsens HOSP-register. För att skapa en enhetlig vy av användarens profil i attributkällan, kan en *provisioneringstjänst* hjälpa till att automatisera denna sammanställning.

Identitets- och behörighetsadministration

I *identitets- och behörighetsadministrationen* läggs sedan vid behov ytterligare egenskaper och behörighetsstyrande attribut på användaren i attributkällan, vilka inte kunde fångas med automatik från andra processer. Det kan vara att verksamhetschefen delegerat ett särskilt ansvar till en medarbetare, t.ex. att göra viss uppföljning av verksamheten, hantera ekonomi etc.

Utfärdande av e-identiteter

Autentiseringen av användaren kräver att användaren elektroniskt kan bevisa för autentiseringstjänsten vem hen är. För detta utfärdas en s.k. *e-identitet* till användaren,

på någon form av bärare, t.ex. ett smart kort, en säkerhetsdosa, en skyddad del av en mobil enhet eller dylikt. E-identiteten har unika egenskaper (t.ex. en unik hemlig nyckel) som gör att det går att säkerställa att det är just den e-identiteten som används vid inloggningen.

Granulär åtkomst till information via integrationstjänster

Referensarkitekturen kan även ge stöd för att ge användaren granulär och säker åtkomst till information via *integrationstjänster* (api:er), genom samverkan mellan en *åtkomstintygsutfärdare* och en *API Säkerhetstjänst*. Åtkomstintygsutfärdaren kan utfärda intyg avseende viss åtkomst (inom visst ”scope”), som sedan kan användas för att anropa integrationstjänster som skyddas av *API Säkerhetstjänst*. Åtkomsträttigheter kan även *delegeras* från användaren till den e-tjänst som behöver hämta information.

Regelverkstjänst

Att ge tillgång till resurser, e-tjänster och information, handlar i grunden om att sätta och tillämpa ett antal regler för åtkomst (*authorization rules*). Regelverket kan ofta vara ”på papper” som sedan implementeras (programmeras) i respektive e-tjänst, informationstjänst osv.
Om det är många tjänster som ska skyddas, och/eller behovet att styra informationsåtkomsten är fingranulärt, behövs ett mer skalbart sätt att hantera att regelverket faktiskt tillämpas i tjänsterna. För detta behov finns en *regelverkstjänst* definierad i referensarkitekturen. I regelverkstjänsten administreras reglerna och beskrivs på ett maskinläsbart sätt som entydigt kan tolkas av de tjänster som behöver utföra auktorisation.

Identitets- och behörighetsfederation

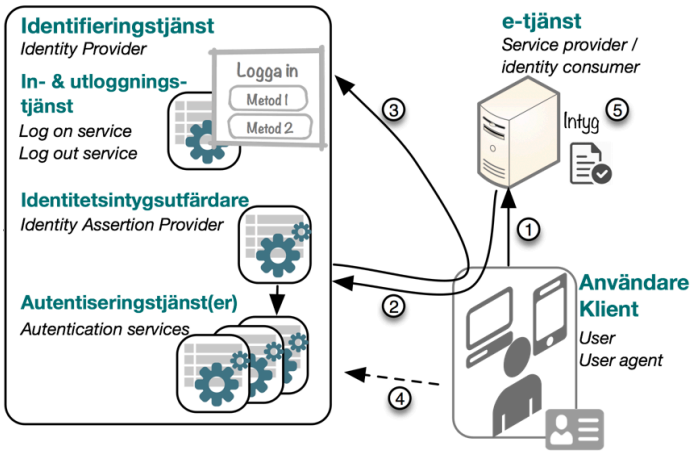
Referensarkitekturen stödjer vidare ett federativt sätt att bygga upp och knyta samman IT-infrastrukturer för identitet och åtkomst hos olika organisationer, t.ex. landsting – kommun, region – nationell samverkansorganisation, landsting – privat utförare av vård, kommun - myndighet osv. *Federationen* bygger på ett förlitande (*trust*) mellan organisationerna, vilket gör att man kan acceptera utfärdade identitetsintyg från annan part, och därigenom ge åtkomst till skyddade resurser utan att själv behöva administrera den andra partens medarbetares e-identiteter.
Federationens grundpelare är medlemmarna *(medlemsregistret)*, säker information om vilka tjänster som är anslutna *(metadatatjänst)*, ett *tillitsramverk* som definierar de krav som ställs, ett överenskommet innehåll *(attribut),* samt processer för att bli och vara ansluten *(godkännandeprocess)*.

5.2 Flöde för inloggning i e-tjänst

Nedan flöden beskriver principen för samspelet vid inloggning till en e-tjänst, där samverkan sker mellan

- Användaren
- Användarens klient
- Den e-tjänst som användaren loggar in till
- Inloggningstjänsten
- Identitetsintygsutfärdaren
- Autentiseringstjänsten

5.2.1 Basflöde för inloggning



Figur 9. Basflöde vid inloggning i e-tjänst

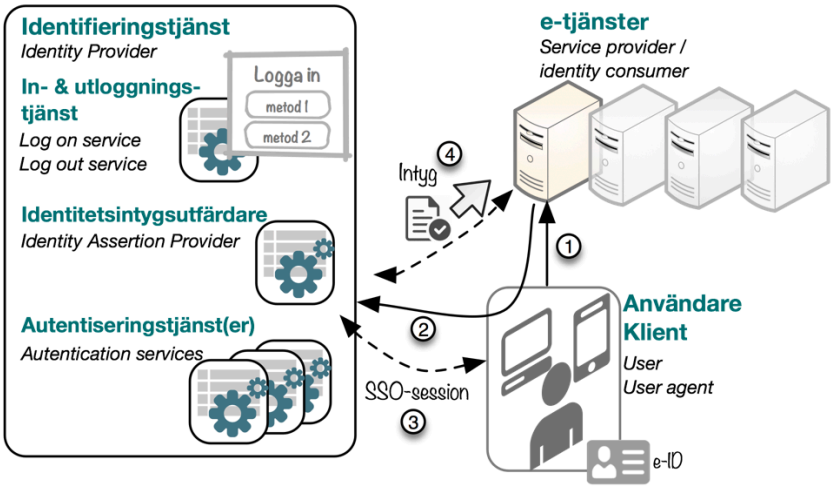
Basflödet, där vi antar att det inte finns en SSO-session etablerad sedan tidigare, kan beskrivas enligt följande:

1. Användaren väljer att logga in i en e-tjänst (session saknas)
2. E-tjänsten kräver en autentiserad användare och skickar en autentiseringsbegäran till *identitetsintygsutfärdaren*.
3. Identitetsintygsutfärdaren har ingen tidigare säkrad session med denna klient (ingen SSO-session), och styr därför om användaren till *inloggningstjänst*.

Här kan presenteras för användaren vilka metoder som erbjuds att logga in med och som motsvarar den tillitsnivå som e-tjänsten kräver.[7]

4. Användaren avkrävs autentisering med vald metod.
5. Identitetsutfärdaren utfärdar vid lyckad autentisering ett intyg som förmedlas till e-tjänsten.[8] E-tjänsten verifierar intygets giltighet, och om användaren är behörig att använda e-tjänsten blir användaren inloggad.

5.2.2 Flöde för singelinloggning - SSO



Figur 10. Flöde vid singelinloggning - SSO

Vid singelinloggning (SSO) påverkas flödet på så sätt att användaren inte aktivt behöver logga in igen i tjänsten, genom att en säker SSO-session har etablerats med användarens klient vid tidigare inloggning:

1. Användaren väljer att logga in i en e-tjänst (session saknas)
2. E-tjänsten kräver en autentiserad användare och skickar en autentiseringsbegäran till *identitetsintygsutfärdaren*.
3. Identitetsintygsutfärdaren har en giltig *SSO-session* med denna klient. Ingen ny autentisering krävs.

[7] Notera att detta steg kan hoppas över om valet är givet redan i e-tjänsten. Då hanterar e-tjänsten gränssnittet mot användaren. E-tjänsten kan även styra vilken tillitsnivå den kräver för autentiseringsmetoden.

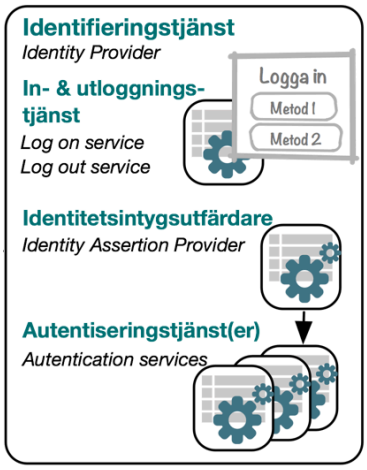
[8] Exakt hur detta går till beror på valt protokoll, men vi återkommer till vilka principiella metoder som används.

4. Identitetsutfärdaren utfärdar ett intyg som förmedlas till e-tjänsten. E-tjänsten verifierar intygets giltighet, och om användaren är behörig att använda e-tjänsten blir användaren inloggad.

Förfarandet kan upprepas för ytterligare anslutna e-tjänster (antydda i Figur 10); så länge det finns en giltig SSO-session, där sessionstiden ställs utifrån aktuella krav, kan användaren logga in i e-tjänsterna utan upprepad autentisering.

5.3 Identifieringstjänst

Referensarkitekturen bygger på en separation av inloggningsfunktionaliteten (inkl. autentisering) från e-tjänsten. Detta benämns även som *federerad inloggning*, där e-tjänsten litar på en infrastrukturtjänst – *Identifieringstjänst* – att hantera säkerställande av identitet.



Figur 11. Identifieringstjänst

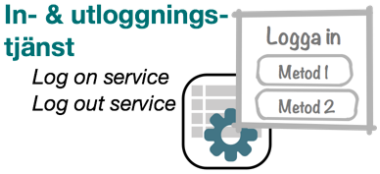
Identifieringstjänsten kan ses som ”navet” i IT-infratrukturen för identitet- och åtkomst, som sammanför de olika tekniska plattformarna (webb, mobilt, rika klienter osv.) som behöver stödjas i ett sammanhållet koncept.

Det leder till behovet av att på ett plattformsneutralt sätt

- Hantera olika metoder att logga in en användare (*Inloggningstjänst*).
- Att säkerställa (verifiera) identiteter (*Autentiseringstjänst*).
- Att förmedla den säkerställda identiteten (och även tillhörande egenskaper) till e-tjänster på ett säkert sätt (*Identitetsintygsutfärdare*).

5.4 In- och utloggningstjänst

In- och utloggningstjänsten är en stödtjänst i infrastrukturen som tillhandahåller en gemensam inloggningsfunktionalitet för federerad inloggning och ett gränssnitt emot användaren.



Figur 12. In- och utloggningstjänst

Notera att gränssnittet mot användaren för att logga in (t.ex. ”Logga in”, ”välj metod” osv.) även kan hanteras av e-tjänsten själv. Detta förutsätter dock att inloggningstjänsten erbjuder respektive metod som separata ändpunkter (*endpoints*) som e-tjänsten kan anropa. Basflödet i kap. 5.2.1 blir alltså detsamma förutom att steg 3 hoppas över.

Kopplat till tjänsten kan det även finnas en *utloggningstjänst* som loggar ut användaren ur en gemensam SSO-session. Viktigt är här att notera att det är e-tjänsten som har huvudansvaret att tillhandahålla användaren en tydlig utloggningsfunktionalitet, och det är e-tjänsten som ska säkerställa att användarens session i e-tjänsten avslutas. Den gemensamma utloggningstjänsten kan däremot tillföra en möjlighet att tvinga fram en ny inloggning om användaren försöker nå samma eller annan e-tjänst igen, dvs. att SSO-sessionen avslutas.

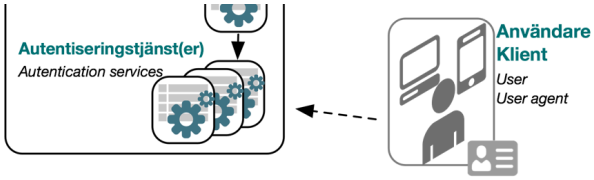
Utloggning kan även ske händelsestyrt, typiskt baserat på att en inaktivitetstid löpt ut. Detta kan gälla både sessionen i e-tjänsten samt SSO-sessionen i förekommande fall. Notera dock att detta i så fall måste kunna anpassas till aktuella säkerhets- och verksamhetskrav, samt vilka andra funktioner för sessions- och klientlåsning som används. Används t.ex. automatisk låsning av klient samt klientsessionsförflyttning (användaren kan återuppta hela klientsessionen på annan enhet), bör sessionstiderna för e-tjänsterna kunna anpassas, t.ex. till arbetspassens längd.

5.4.1 Specifika krav

- E-tjänsten ansvarar för att begära inloggning av användare av inloggningstjänst.
- E-tjänsten kan tillhandahålla användargränssnittet för inloggning, alternativt delegera detta till en inloggningstjänst.
- E-tjänsten ansvarar för att det finns en för användaren tydlig funktion för utloggning i e-tjänsten. Funktionen ska säkerställa att användarens session i e-tjänsten avslutas.
- Om e-tjänsten nyttjar en gemensam SSO-session hos inloggningstjänst, bör e-tjänsten vid behov kunna signalera utloggning ur SSO-sessionen, dvs. tvinga fram en ny inloggning vid nästa försök att nå e-tjänst.
- Funktion i e-tjänsten för automatisk utloggning vid inaktivitet ska kunna anpassas efter aktuella behov samt informationssäkerhetskrav.

5.5 Autentiseringstjänst

En *Autentiseringstjänst* ansvarar för att med viss autentiseringsmetod autentisera användaren, dvs. säkerställa användarens identitet, vilket är en grundläggande del av skyddet mot obehörig åtkomst.



Figur 13. Autentiseringstjänst(er)

5.5.1 Grundläggande principer för autentisering

I praktiken kan autentiseringssteget omfatta både att *identifiera* användaren (finna en användaridentitet, t.ex. hsa-id eller personnummer) och att *verifiera* identiteten (med stöd av något sorts ”äkthetsbevis”).

Autentisering av en aktör (både användare och system) inbegriper typiskt två principiella delar:

- Aktören tillhandahåller en eller flera *autentiseringsfaktorer* (”äkthetsbevis”), för att styrka e-identitetens riktighet, dvs. att aktören faktiskt är den som denne utger sig för att vara.
- Ett *autentiseringsprotokoll* som reglerar kommunikationen mellan aktören/klienten och en autentiseringstjänst, vars uppgift är att på ett säkert sätt överföra information som säkerställer aktörens identitet.

För autentisering av användare kan autentiseringsfaktorerna delas in i

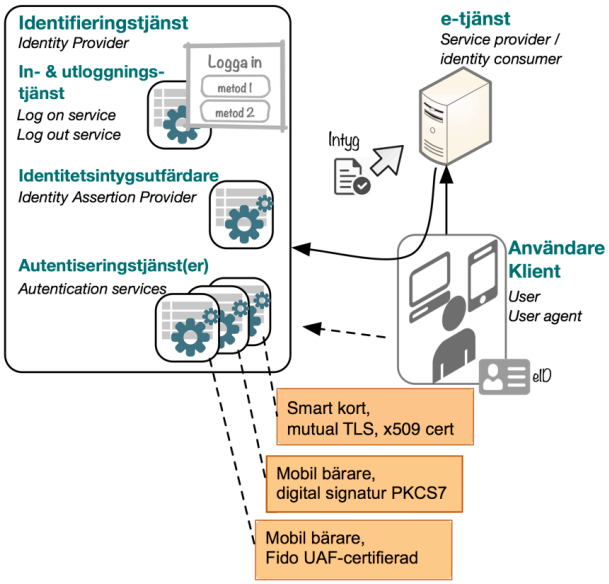
- Något (just denna) användaren vet,
- Något (just denna) användaren har
- Något (just denna) användaren är, dvs. någon egenskap hos användaren, även kallad *biometrisk* faktor.

Autentiseringen kan baseras på en eller flera av sådana faktorer, t.ex. enbart ett hemligt lösenord (*enfaktorautentisering*), både ett tumavtryck och innehav av en säkrad enhet (*tvåfaktorautentisering*) osv.

5.5.2 Stöd för multipla autentiseringsmetoder

Det kan finnas flera autentiseringstjänster inom ramen för samma infrastruktur som hanterar olika sätt att autentisera sig på. Autentiseringstjänsterna agerar som stödtjänster

till intygsutfärdaren, på så sätt att intygsutfärdaren begär autentisering av användaren av autentiseringstjänsten, och att autentiseringstjänsten rapporterar tillbaka resultatet (normalt om autentisering gick bra eller ej samt fastställd identitet) till intygsutfärdaren.



Figur 14. Multipla autentiseringsmetoder kan "pluggas in" inom en Identifieringstjänst

Referensarkitekturen ger på så sätt stöd för att införa nya autentiseringsmetoder i verksamheterna för att

- Möta informationssäkerhetskrav, t.ex. krav på tvåfaktorsautentisering med hög tillit pga. informationens skyddsvärde.
- Möta verksamhetens krav, t.ex. det ska gå snabbt att logga in, åtkomst mobilt osv.
- Kunna ta till sig och nyttja ny teknik inom området.

Den nya autentiseringsmetoden kan dessutom läggas till utan att e-tjänsternas anslutning till Identifieringstjänsten behöver förändras.

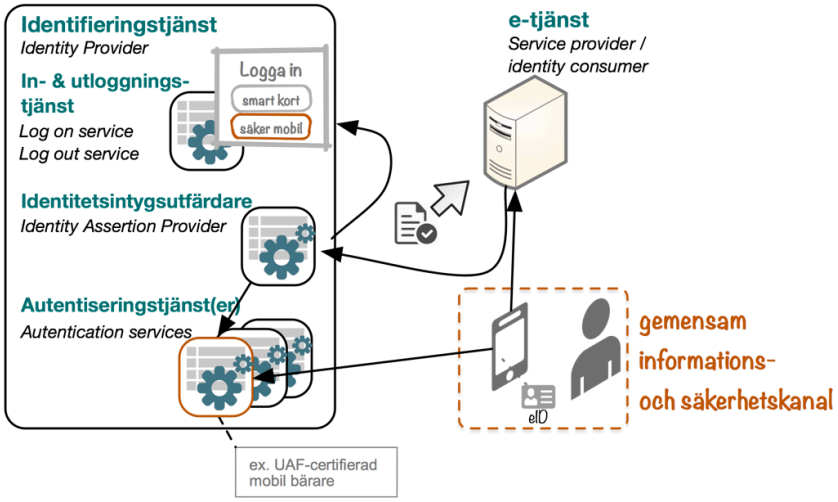
5.5.3 Autentisering in-band respektive out-of-band

Även om nya anpassade metoder kan anslutas i IT-infrastrukturen, kvarstår ett problem: om autentiseringslösningen kräver viss mjuk- och hårdvara, t.ex. av säkerhetsskäl, behöver användarnas alla klienter också utrustas med denna mjuk- och hårdvara. T.ex. kan en lösning med smarta kort kräva speciella kortläsare och tillhörande drivrutiner.

Dessa extra tekniska krav på användarnas klienter blir allt svårare att hantera, dels för att lösningen behöver vara kompatibel med en teknisk plattform som är under ständig vidareutveckling och förändring (t.ex. uppgradering av operativsystem), dels för att användarna vill och ska kunna använda lämpliga olika verktyg för rätt situation, ibland

en läsplatta, i ett annat fall en stationär terminal med stor skärm och hög upplösning, i ett tredje fall kanske en digital tryckkänslig whiteboard.
Hur kan vi fortsätta att ge stöd för säker inloggning och även kunna införa nya säkra och smarta sätt att logga in, om dessa mjuk- och hårdvaruproblem hindrar?

Problemet ligger egentligen i att samma kanal alltid används för både informationsåtkomsten och säkerhetslösningen, vilket även kallas *in-band-authentication*.

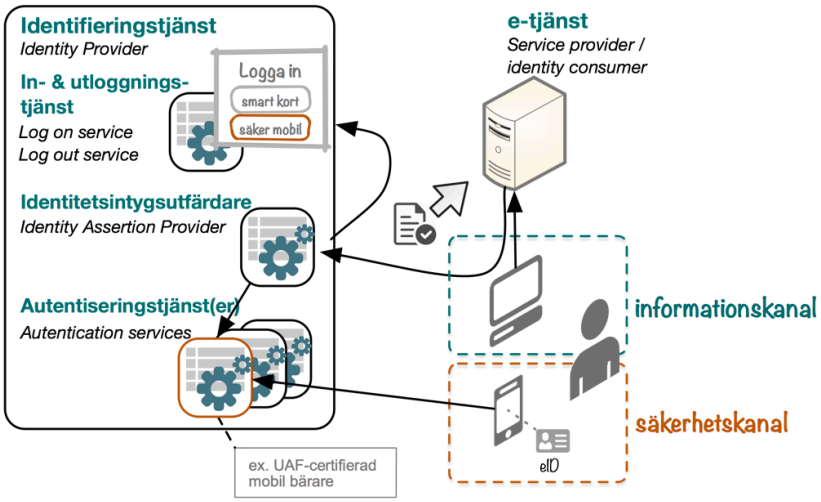


Figur 15. In-band authentication (IBA). Gemensam informations- och säkerhetskanal.

Detta kan hanteras genom att tillämpa styrande princip IA9, dvs. att

- Autentisering ska (vid behov) kunna ske i *separat säkerhetskanal* skild ifrån *informationskanalen* (där användaren arbetar med informationssystemet), även kallad *out-of-band authentication*.[9]

[9] Ett för många i Sverige välbekant exempel på *out-of-band authentication* är Mobilt BankID.



Figur 16. Out-of-band authentication (OOBA). Separata kanaler för informations- och säkerhetskanal.

Användning av en separat säkerhetskanal skapar ytterligare lös koppling mellan de komponenter som används vid informationsåtkomsten:

1. Klienten för informationsåtkomst (informationskanalen)
2. E-tjänsten (informationssystemet)
3. Användarens autentiseringslösning/e-identitet (säkerhetskanalen)
4. Identifieringstjänsten (IT-infrastruktur för identifiering)

Denna lösa koppling medger bland annat att mixa och anpassa utrustning för var och en dessa fyra delkomponenter; t.ex. kan en stationär enhet med kortläsare användas för att autentisera en användarsession på en smart mobil, och vice versa.

Det blir även möjligt att införa starka former av autentisering för utrustning som helt saknar möjlighet att koppla in extra hårdvara eller liknande.

5.5.4 Biometri

Biometrisk teknik kan minska den mentala belastningen på personalen om de slipper komma ihåg koder/lösenord, och istället utnyttja t.ex. ett fingeravtryck.

Biometrisk teknik kan därför med fördel utnyttjas i flerfaktorsautentisering för att ersätta faktorn ”något som man vet” eller ”något man har” med ”något man är”, t.ex. ersätta PIN-kod i lösningar med tvåfaktorautentisering. Biometrisk data ska dock inte spridas i onödan till tjänster i nätverket, utan hålls nära användaren själv, helst endast inom användarens personliga e-identitetsbärare (enligt principen #IA10).

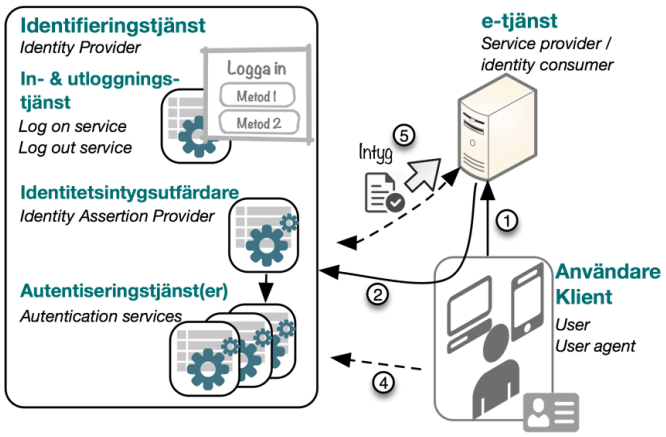
5.5.5 Specifika krav

- E-tjänster ska inte integrera direkt med autentiseringstjänst, utan begär av Identifieringstjänst att autentisera användaren på uppdrag av e-tjänsten.

- Identifieringstjänst ansvarar för att delegera autentisering till autentiseringstjänster.
- Identifieringstjänst ska stödja att lägga till (och ta bort) olika autentiseringsmetoder.
- Identifieringstjänst ansvarar för att leverera information om utförd autentisering via intyget, s.k. *autentiseringskontext* inklusive den tillitsnivå som den aktuella autentiseringsmetoden motsvarar.
- Identifieringstjänst ansvarar för att matcha ev. av e-tjänsten begärd tillitsnivå för autentisering, dvs. om e-tjänsten kräver tillitsnivå "T" ska denna antingen se till att autentisering sker på nivå "T" eller högre nivå, alternativt inte alls (dvs. inloggning ej möjlig).
- IT-infrastrukturen ska stödja såväl *out-of-band* som *in-band* autentisering.
- Biometrisk teknik kan utnyttjas i flerfaktorsautentisering där det är praktiskt för att ersätta ”något som man vet” eller ”något man har” med ”något man är”, t.ex. ersätta PIN-kod i lösningar med tvåfaktorautentisering. Biometrisk data ska dock inte spridas i onödan till tjänster i nätverket av integritetsskäl.

5.6 Identitetsintygsutfärdare

Identitetsintygsutfärdaren (*Identity Assertion Provider*) har rollen att utfärda säkra *identitetsintyg* som intygar en aktörs identitet och tillhörande egenskaper (attribut). Mottagaren av intyget är en e-tjänst, som antingen explicit begärt intyget alternativt



Figur 17. Utfärdande av identitetsintyg – basflöde (Streckad pil indikerar någon form av kommunikation där metoden beror på teknikval).

En identitetsintygsutfärdare kan realiseras av många olika produkter och stödja ett flertal tekniska protokoll parallellt som kan användas för anslutning till olika tekniska plattformar för e-tjänster och klienter. För tekniska krav kring protokollval etc., se vidare kap. 6.

5.7 Utfärdande och förmedling av intyg

Intyg kan i det generella fallet omfatta två olika typer:

- **Identitetsintyg**: intygar en aktörs säkerställda identitet och tillhörande egenskaper (attribut).
- **Åtkomstintyg**: intygar att aktör erhållit en rättighet att nå en viss resurs. Denna typ av intyg innehåller ingen identifierande information om aktören själv.

Båda intygstyperna kan levereras till e-tjänsten om behov finns av det.
Detta kapitel tar upp generella krav på utfärdande och konsumerande av identitet- och åtkomstintyg.

5.7.1 Princip för förmedling av intyg

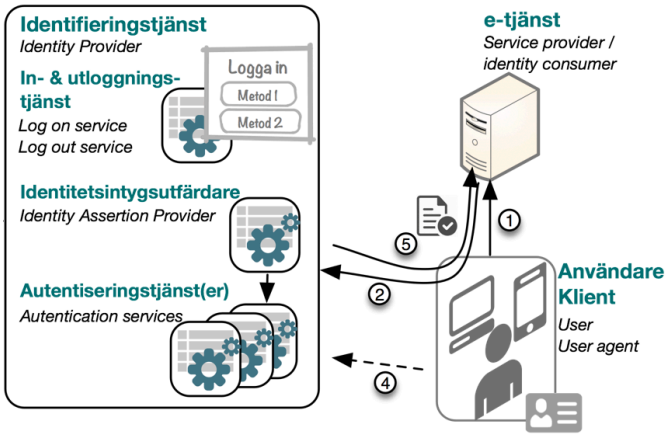
Intyg kan förmedlas tillbaka till e-tjänsten på två principiellt olika sätt:

- **Intyg direkt**: Intyget returneras direkt tillbaka till klienten som resultat av en begäran att erhålla intyg. Detta kallas även "*passing by value*".

Identitetsintyget kommuniceras i detta fall normalt via användarens klient ("*user agent*") vidare till e-tjänsten. Kommunikationsprincipen kallas här "*front channel*"[10].

- **Intyg via referens**: En referens till intyget returneras tillbaka till klienten. Intyget i sig (egentligen informationen som intyget representerar) kan sedan hämtas från identitetsintygsutfärdaren med hjälp av referensen. Detta kallas även "*passing by reference*". Identitetsintyget hämtas i detta fall av en skyddad del av e-tjänsten, normalt en serversida av e-tjänsten, och identitetsintygsutfärdaren kan kontrollera att e-tjänsten har rätt att hämta intygsinformation. Kommunikationsprincipen kallas här "*back channel*"[11]. Principen passar bra när man inte kan lita på klientsidan av e-tjänsten att hantera intyget säkert, t.ex. en mobil klientapp.

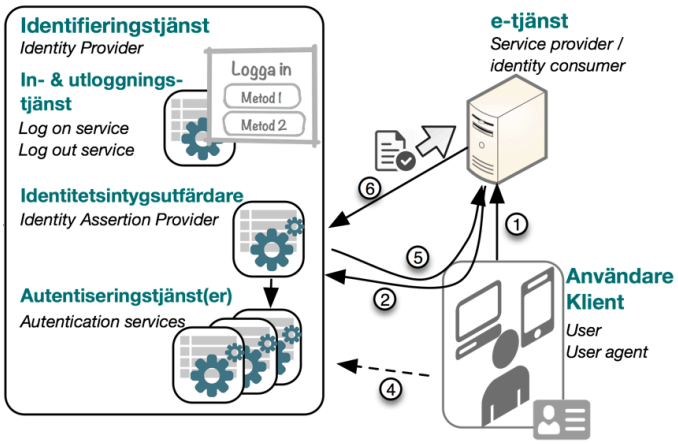
I bilderna nedan illustreras principerna när en användare loggar in och blir autentiserad och ett intyg erhålls. Principen gäller både för identitets- och åtkomstintyg.



Figur 18. Flöde för förmedling av intyg ("front channel")

Vid "*front channel*"-flöden bör alltså beaktas att identitetsintygen passerar klienten, vilket kräver att det finns ett adekvat skydd av klienten på användarens enhet.

[10] Exempel på sådana flöden är OpenID Connect Implicit flow och SAML Web SSO POST-profil.
[11] Exempel på sådana flöden är OpenID Connect Code flow och SAML Web SSO artifact-profil.



Figur 19. Flöde för förmedling av intyg via referens ("back channel")

"*Back channel*"-flöden är säkrare ur det perspektivet – det går att säkerställa att endast godkända och autentiserade e-tjänster kan försöka att hämta ut intyget.

5.7.2 Krav på intygets innehåll

Vad gäller innehållet i intyg finns både standardiserade delar och icke standardiserade där organisationer kan lägga till överenskomna attribut efter behov. Finns en identitets- och behörighetsfederation etablerad, är det en naturlig del att fastställa hur och vilka attribut som kan kommuniceras mellan organisationerna inom federationen.

Det finns några principiella egenskaper som intygen dock behöver förhålla sig till och därmed blir krav på en intygsutfärdare:

- Intyget ska innehålla giltighetstid[12] för intyget.
- Intyget ska vara digitalt signerat av utfärdaren så att dess avsändare kan säkerställas av alla mottagare.
- Intyget ska kunna innehålla *mottagare* (även kallad "audience"). Mottagare av intyget är den tjänst(er) som har rätt att använda ("konsumera") intyget. Denna kan användas för att skydda emot vissa attacker mot själva intyget (att intyg snappas upp och används av obehörigt system etc.).

[12] Även att ange en obegränsad giltighet räknas här som att ange giltighetstid.

5.7.3 Specifika krav

- En utfärdare av intyg ska stödja båda principerna för förmedling av intyg: *intyg direkt* samt *intyg via referens*.
- En e-tjänst ska stödja minst en av principerna för förmedling av intyg: *intyg direkt* samt *intyg via referens.* Val av princip avgörs beroende på e-tjänstens tekniska och säkerhetsmässiga förutsättningar. Hänsyn ska tas till att intyget kan skyddas på ett adekvat sätt.
- Intyg ska förmedlas över krypterad förbindelse. Se vidare [Transportsäkerhet] för specifika krav.

5.8 Identitetsdatalager

Ett betrott intygsutfärdande kräver en kvalitetssäkrad bakomliggande information om användare och organisationer, hanterad i *identitetsdatalagret*.

Identitetsdatalagret tillhandahåller en eller flera s.k. *attributkällor* som innehåller en organisations digitala identiteter för personer och organisationsenheter inklusive egenskaper (attribut) för dessa.

Respektive organisation går i god för att uppgifterna i attributkällan är kvalitetssäkrade, så att de kan utgöra grund för utgivning av e-identiteter, skapande av användarkonton i e-tjänster, attributbaserad behörighetsutvärdering osv.

Attributkällan ger stöd för attributbaserad behörighetsutvärdering genom att baserat på attributen skapa regler för åtkomst till information och funktion (åtgärd), t.ex. att viss befattning i organisationen får hantera ärenden av viss typ, att leg. läkare med förskrivningsrätt får ordinera läkemedel osv.

Egenskaper kopplade till användaridentiteter i identitetsdatalagret kan delas in i följande kategorier

- *Personliga egenskaper*.
  - Personliga egenskaper är egenskaper som användaren har oavsett om den är ledig eller arbetar, är anställd eller arbetslös. Dessa egenskaper har typiskt lång varaktighet. Exempel: namn, personnummer, legitimation osv.
- *Anställningsrelaterade egenskaper*
  - Anställningsrelaterade egenskaper är kopplade till medarbetares anställning. Användaren har dem typiskt så länge som hen innehar en viss tjänst hos en viss arbetsgivare. Exempel: befattning.
- *Uppdragsrelaterade egenskaper*
  - Uppdragsrelaterade egenskaper är kopplade till att användaren blivit tilldelad ett viss uppdrag (ansvar/befogenhet) i verksamheten, i viss process eller dylikt. Exempel: uppdrag att hantera uppföljning av informationssäkerheten inom organisationen, uppdrag att arbeta med vård och behandling av patienter för viss vårdenhet osv.
  - Uppdragsrelaterade egenskaper bör kunna användas för att modellera rättigheter inom godtycklig domän, där respektive domän definierar de rättigheter som kan tilldelas, t.ex. ”Rapportera ekonomiskt underlag”, ”Administrera personals anställningsuppgifter” osv.

Kategorierna ovan är viktiga att vara medveten om då det påverkar hur, varför och hur länge en medarbetare får en viss egenskap kopplad till sig, t.ex. att attributet följer av att medarbetaren just nu har ett visst uppdrag/ansvarsområde.

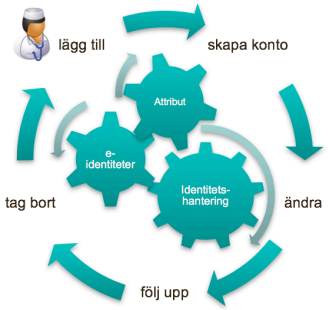
Attributkällan ger även information om organisationsidentiteter och hur dessa förhåller sig till varandra (organisationsstruktur) där så tillämpligt.

Flera olika vyer (perspektiv) av dessa identitetsstrukturer kan behöva tillhandahållas, t.ex. personvy, uppdragsvy, anställningsvy osv, beroende på det regelverk som behöver stödjas.

5.9 Provisioneringstjänst

Provisionering i generella termer betyder att ”tillhandahålla”. Inom referensarkitekturen för Identitet och åtkomst avser vi specifikt *provisionering av identitetsdata*, dvs. tillhandahålla kvalitetssäkrad identitetsdata till de mottagare som behöver det, t.ex. i syfte att skapa användarprofiler som sedan konsumeras i en e-tjänst.

Provisioneringen måste utgå ifrån resultatet av den livscykelhantering av identiteter som ständigt behöver fortgå inom organisationen, dvs. ta hänsyn till både skapande, förändring och borttag av identitetsdata.

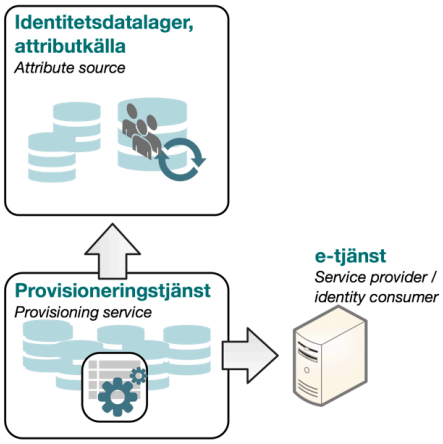


Figur 20. Förändring av identitetsdata är en ständigt pågående process

Provisionering ska här ses i ett brett perspektiv och kan bland annat omfatta

- Provisionera identitetsdata från masterdatakällor, t.ex. register över individers legitimationer, personaladministrativt system (anställningar, befattningar) till en organisationsgemensam attributkälla (identitetsdatalagret), dvs. en konsolidering av kvalitetssäkrad identitetsdata.
- Provisionera identitetsdata från identitetsdatalager till en e-tjänst, t.ex. för att automatiskt skapa och ta bort användarprofiler i e-tjänsten, dvs. en distribution av kvalitetssäkrad identitetsdata.

Provisioneringstjänst syftar till att ge stöd till automatisering av processen att provisionera identitetsdata, och kan tillhandahålla stöd för båda flödena ovan.



Figur 21. Provisioneringstjänst – tillhandahålla kvalitetssäkrad identitetsdata med stöd för automatisering.

Syftena med Provisioneringstjänst kan sammanfattas i

- Ge stöd för en automatiserad och kvalitetssäkrad process för att skapa en enhetlig vy av organisationens identitetsdata i attributkällan.
- Tillhandahålla tekniska gränssnitt för att konsumera identitetsdata där den behövs i IT-stödet, t.ex. i e-tjänster.

Notera att även att utfärdande och förmedlande av identitetsintyg är en form av provisionering av identitetsdata till e-tjänsten i realtid. Identitetsintyget ger grundläggande uppgifter om användaren, vilket för en del e-tjänster kan vara helt tillräckligt. Men e-tjänsten kan behöva ytterligare uppgifter, och vissa kan ha krav på att ett konto skapas i förväg i e-tjänsten, eventuellt med ett extra valideringssteg innan kontot blir aktivt.

Följande prioritetsordning bör användas vid provisionering enligt referensarkitekturen:

1. I första hand basera tillhandahållande av identitetsdata till e-tjänst på identitetsintyg.
2. Som komplement tillhandahålla identitetsdata via tjänstegränssnitt, där om möjligt standardiserade gränssnitt används, t.ex. nationellt tjänstekontrakt för behörighetsdata för medarbetare.

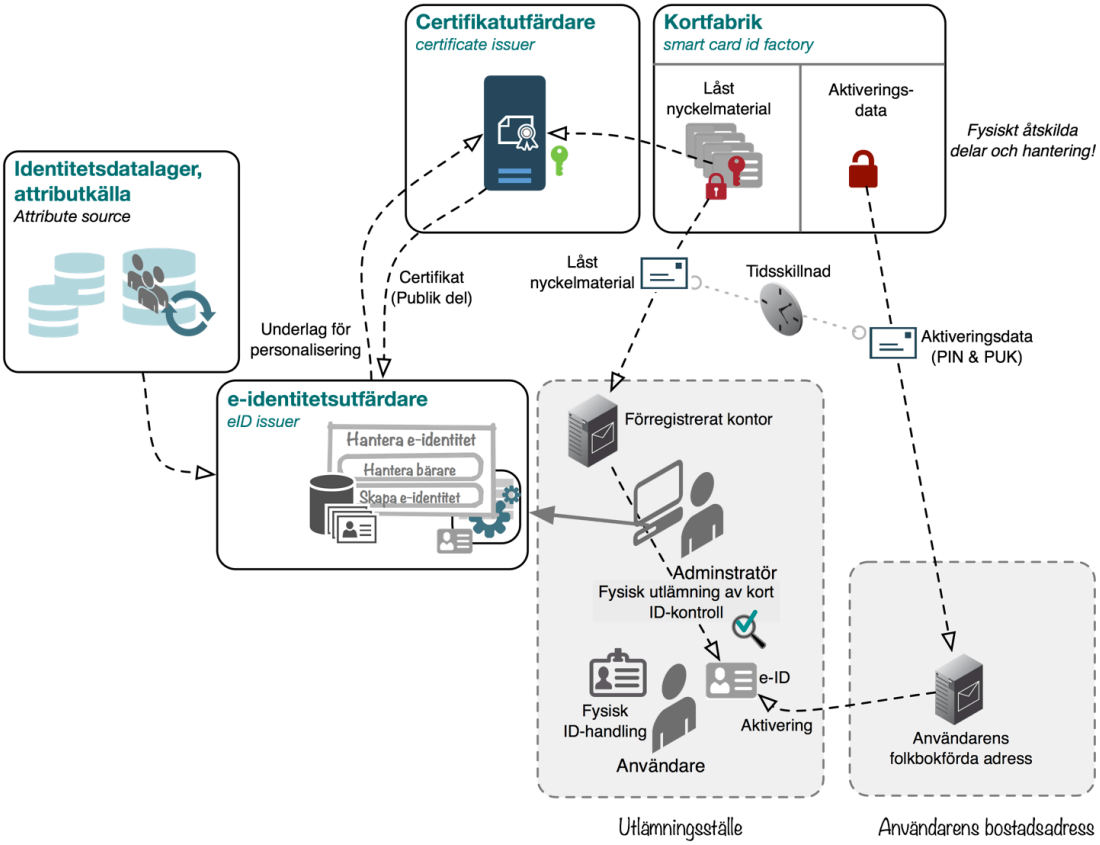
5.10 e-identitetsutfärdare

Utfärdande av e-identitet innebär att en slutanvändare eller ett system erhåller en e-identitet för att använda som dennes ”identitetshandling” i kommunikationen med IT-system. e-identiteten förvaras på en e-identitetsbärare, t.ex. ett smart kort med skyddat chip eller en skyddad del på en mobil enhet.

För att e-identiteten och dess bärare ska kunna ges hög tillit behövs den skyddas så att endast den rättmätiga ägaren kan använda den, normalt genom en extra autentiseringsfaktor som endast användaren/systemet själv känner till (t.ex. PIN-kod) eller är (t.ex. en biometrisk egenskap).

5.10.1 Utfärdande av e-identitet med administrativ process

Utfärdandet kan innebära en administrativ process där användaren identifierar sig med en godkänd fysisk id-handling, och en administratör effektuerar själva utfärdandet. För att nå en hög tillitsnivå bör leverans av e-identitetsbäraren med *nyckelmaterial* och *aktiveringsdata* ske i en separata fysiska kanaler, t.ex. personlig utlämning kombinerat med postutskick till folkbokföringsadress.



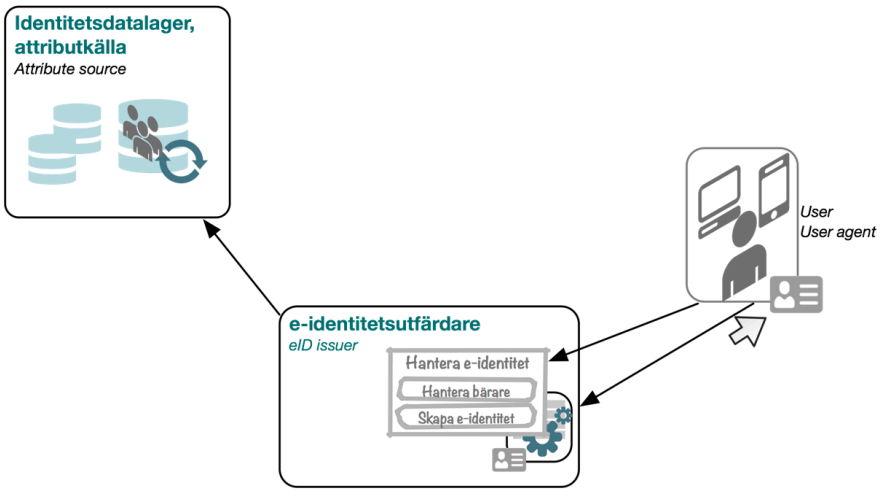
Figur 22. Utfärdande av e-identitet med administrativ process. Ex. med utfärdande till hårt certifikat på smart kort via en kortfabrik. Separerade kanaler för nyckelmaterial och aktiveringsdata. Fysisk legitimering vid utlämning.

I Figur 22 har använts ett exempel med utfärdande till hårt certifikat på ett smart kort. Nyckelmaterial och aktiveringsdata genereras på en säker s.k. ”kortfabrik”, där de typiskt hålls fysiskt åtskilda och säkras med stark autentisering och flerpersonerskontroll. Leveransen sker även den separat till olika adresser och med tidsskillnad för att förhindra att båda delarna kan påträffas samtidigt.

Användaren mottar aktiveringsdata (i detta fall PIN- och PUK-koder) på sin folkbokförda adress, och får sedan legitimera sig fysiskt vid ett utlämningsställe för att också erhålla det personliga smarta kortet. Användaren aktiverar sitt e-ID med aktiveringsdatat.

5.10.2 Utfärdande av e-identitet med självservice

Utfärdande av e-identitet kan även göras i en självservice-process, vilket alltså inte inbegriper en administratör, illustrerat i nedan bild.

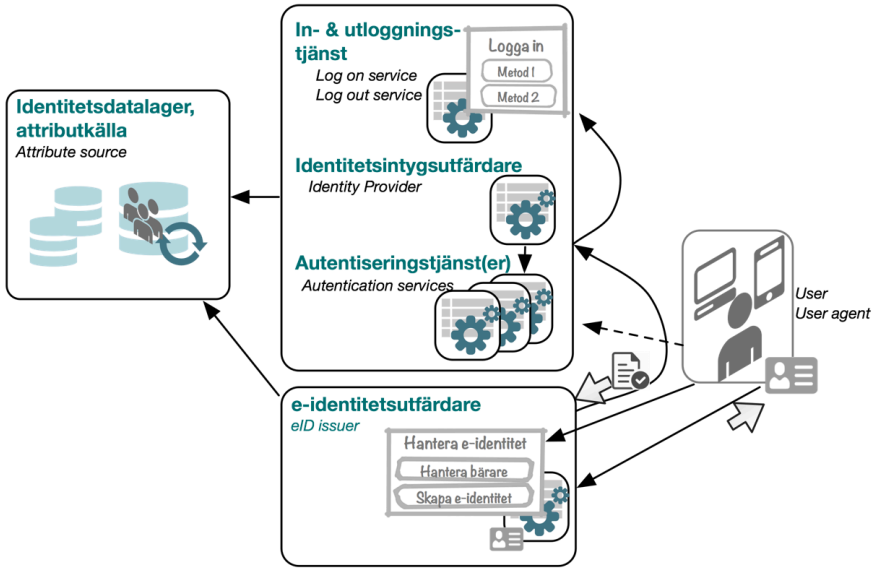


Figur 23. Utfärdande av e-identitet, självservice.

När användaren själv kan utföra detta steg elektroniskt uppnås en betydligt bättre skalbarhet och minskad administrativ börda.

5.10.3 Utfärdande av e-identitet med ärvd legitimering

Ett problem med en renodlad självservice är dock att det blir mycket svårare att veta att det verkligen är rätt individ som e-identiteten knyts till. Därför bör självservice-modellen kombineras med en administrativ utfärdandeprocess i botten. För att utfärda en ny e-identitet via självservice krävs att användaren först autentiseras med en tidigare utgiven e-identitet.



Figur 24. Utfärdande av e-identitet, självservice med möjlighet till s.k. ärvd legitimering.

På detta sätt ger referensarkitekturen stöd för s.k. *ärvd legitimering* där en legitimering (kontroll av identitet) som skett tidigare för att erhålla den första e-identiteten, kan ärvas vid utfärdandet av en ny e-identitet, med samma eller annan teknik och typ av e-identitetsbärare.

Via ärvd legitimering kan alltså såväl samma som annan typ av e-identitet utfärdas[13], t.ex.

- Förnyande av ett x509-certifikat på ett smart kort med det smarta kortet som bärare (samma typ utfärdas),
- Ny e-identitet utfärdas till en mobil e-identitetsbärare (mobil enhet), med stöd av ett certifikat på ett smart kort (annan typ utfärdas).

Processen kan göras elektronisk och via självservice, vilket ger stora skalfördelar[14].

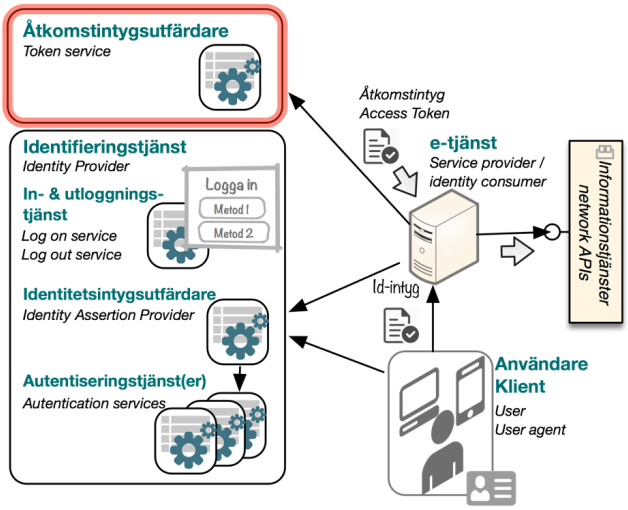
Vid ärvd legitimering kan dock aldrig tilliten till den nya e-identiteten vara högre än den som används vid utfärdandet, dvs. tillitsnivån är antingen den samma eller lägre för den nya e-identiteten.

[13] Notera att det kan finnas begränsningar där vissa tillitsnivåer eller e-identiteter inte får ärvas, t.ex. tillitsnivå LoA4 enligt nuvarande regelverk.

[14] Jämför utgivning av Mobilt BankID baserat på t.ex. inloggning med en säkerhetsdosa.

5.11 Åtkomstintygsutfärdare

Åtkomstintygsutfärdaren, även kallad *tokentjänst* (*token service*) utfärdar digitala *åtkomstintyg* som kan användas för att begära åtkomst till en viss resurs. Resursen kan vara en informationstjänst (ett nätverksbaserat api), eller en resurs inom en annan e-tjänst.



Figur 25. Princip för utfärdande av åtkomstintyg

5.11.1 Krav för att erhålla ett åtkomstintyg

Åtkomstintyget utfärdas till e-tjänsten endast på begäran och förutsatt att

- E-tjänsten är autentiserad och registrerad som godkänd mottagare av åtkomstintyg.
- Användaren är identifierad och autentiserad.
- Regelverket tillåter användaren åtkomst till den begärda resursen via e-tjänsten.
- Eventuellt även att användaren aktivt samtyckt (valbart, beror på policy).

I Åtkomstintygsutfärdaren kan sättas autentiseringskrav för att få ut ett visst åtkomstintyg (för viss tjänst och visst s.k. *scope*), både för användaren och e-tjänsten.

Antingen är användaren redan autentiserad och inloggad sedan tidigare dvs. singelinloggning (SSO) utnyttjas, alternativt utförs en ny användarautentisering hos Identifieringstjänsten.

E-tjänsten avkrävs autentisering via en skyddad privat nyckel. I dess enklaste form är detta en api-nyckel som tilldelats e-tjänsten i förväg. Även certifikatsbaserad autentisering (PKI) kan användas om Åtkomstintygsutfärdaren stödjer det.

5.11.2 Delegerad åtkomst via åtkomstintyg

Åtkomstintyget används sedan vid anrop till den skyddade resursen, oftast en informationstjänst, som verifierar åtkomstintygets giltighet och korrekthet (giltighetstid och signatur).

Beslutet att ge åtkomst till resursen (auktorisation) ligger strikt sett hos resursen själv. Åtkomstintyget kan ses som en *delegerad rättighet* från användaren till e-tjänsten att för användarens räkning få åtkomst till resursen. Även om intyget innehåller korrekt data för åtkomsten i fråga, äger resursen möjligheten att tillåta eller neka åtkomst baserat på underlaget, t.ex. om intyget kommer från en utfärdare som inte resursen litar på. Normalt finns det dock ett förlitande (*trust*) mellan Åtkomstintygsutfärdaren och de informationstjänster som Åtkomstintygsutfärdaren ger ut intyg för (de tillhör oftast samma organisation), varvid informationstjänsten tryggt kan ge åtkomst baserat på intyget.

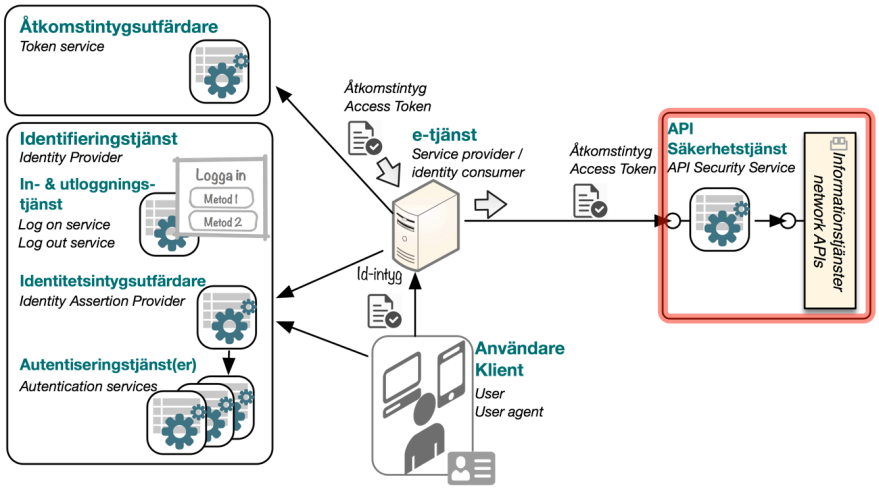
5.11.3 Giltighetstider och förnyelse av åtkomstintyg

Giltighetstiden för åtkomstintyg sätts relativt kort, bland annat för att minska dess exponering, men även ge möjlighet att stänga av en åtkomst på kort varsel. Åtkomstintygsutfärdaren kan därför även utfärda ett *förnyelseintyg* (*refresh token*) till e-tjänsten. Förnyelseintyget används endast i kommunikationen med Åtkomstintygsutfärdaren för att erhålla ett nytt åtkomstintyg, dvs. förnyelseintyget skickas aldrig med vid anropen till informationstjänster.

Även förnyelseintyget har en giltighetstid, vilken t.ex. kan avpassas till ett arbetspass i verksamheten.

5.12 API-säkerhetstjänst

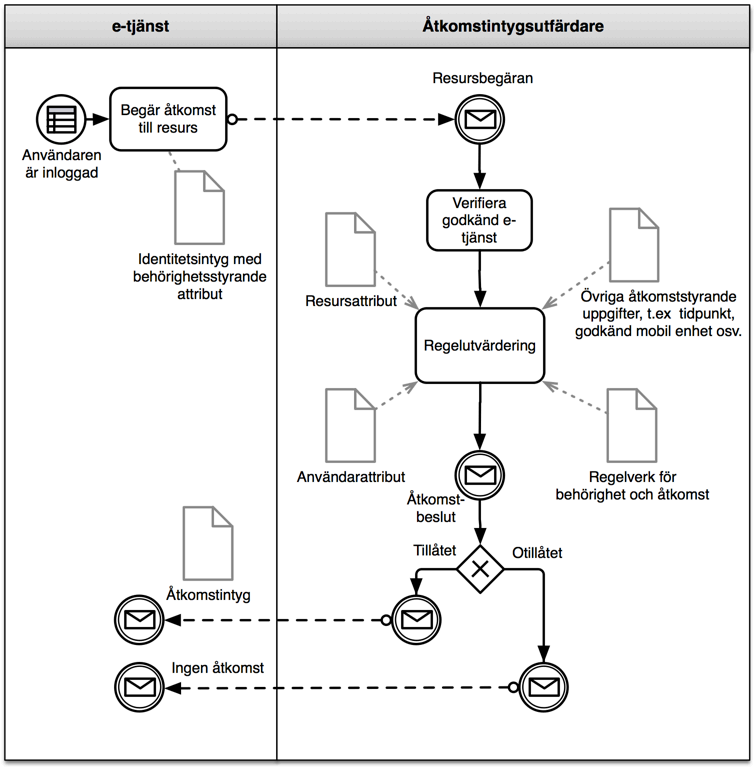
Det är oftast inte optimalt att låta varje informationstjänst hantera säkerhetslagret för verifiering av åtkomstintyg och auktorisation. Därför definierar referensarkitekturen en *API Säkerhetstjänst* vars uppgift är att utgöra säkerhetslagret för de informationstjänster som behöver hanteras, typiskt inom en organisation.



Figur 26. API Säkerhetstjänst säkerställer skydd av flera informationstjänster

Genom samverkan med och förlitande till Åtkomstintygsutfärdaren samt Identifieringstjänsten, kan åtkomsten till all information som informationstjänsterna tillhandahåller säkras genom ett centralt definierat åtkomstregelverk, för att säkerställa att rätt individ får åtkomst till rätt information under rätt förutsättningar.

Regelutvärderingen kan följa samma mönster som i kap. 4.4, men i detta fall görs utvärderingen centraliserat i IT-infrastrukturen:



Figur 27. Regelutvärdering av åtkomst till informationsresurser förlagd till IT-infrastrukturen. E-tjänsten erhåller ett åtkomstintyg om åtkomsten är tillåten.

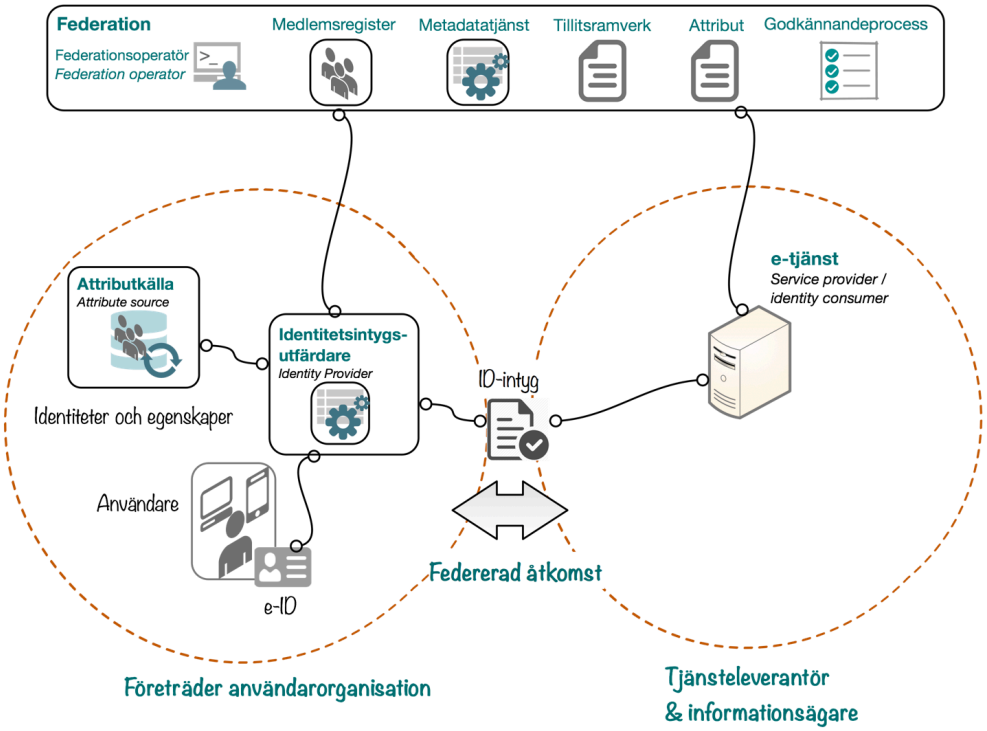
Eventuell federation av identiteter från andra organisationer, hanteras av Identifieringstjänst som ansluts till federationen i samverkan med andra parter, se vidare kap. 5.13.

5.13 Identitets- och behörighetsfederation

5.13.1 Federationens roll och nytta

Referensarkitekturen stödjer vidare ett federativt sätt att bygga upp och knyta samman IT-infrastrukturer för identitet och åtkomst hos olika organisationer, t.ex. landsting – kommun, region – nationell samverkansorganisation, landsting – privat utförare av vård, kommun - myndighet osv.

Federationen bygger på ett förlitande (*trust*) mellan organisationerna, vilket gör att man kan acceptera utfärdade identitetsintyg från annan part, och därigenom ge åtkomst till skyddade resurser utan att själv behöva administrera den andra partens medarbetare och deras e-identiteter och egenskaper.



Figur 28. Identitets- och behörighetsfederation. Federativ åtkomst till e-tjänst i annan organisation.

Några nyttoeffekter som erhålles med en identitets- och behörighetsfederation:

- Organisation som tillhandahåller e-tjänst(er) externt, t.ex. till andra landsting eller kommuner, regionalt eller nationellt, behöver inte administrera alla samverkande parters användare och deras enskilda egenskaper för att säkra identitet och behörighet; detta kan hanteras av respektive part med bibehållet regelverk.
- Organisation som nyttjar extern leverantörs e-tjänst, t.ex. en molntjänst från en privat tjänsteleverantör, en nationell e-tjänst osv, behöver inte förse den andra

parten med uppgifter om sina användare och organisationen för att få åtkomst till e-tjänsten. Istället kan organisationens medarbetare använda sin ordinarie IT-infrastruktur för inloggning och identifiering för åtkomst till tjänsteleverantörens e-tjänst.

5.13.2 Federationens grundbeståndsdelar

En identitets- och behörighetsfederations grundpelare är

- *Medlemsregister* – register över de parter som ingår i federationen. Med stöd av medlemsregistret kan ett tillförlitligt utbyte av information initieras.
- *Metadatatjänst* – hanterar säker information om vilka tjänster som är anslutna - primärt identitetsutfärdare och e-tjänster - samt deras egenskaper, förmågor och publika nycklar. Publika och privata nycklar används bl.a. för att signera och verifiera signaturer på intyg och metadatat självt.
- *Tillitsramverk* - beskriver tekniska och regulatoriska krav för ingående parter i federationen, t.ex. krav på att skydda privata krypteringsnycklar. Ger möjlighet att parterna kan samverka med olika lokalt anpassade lösningar och processer på samma *tillitsnivå*.
- Standardiserade och överenskomna *attribut* för utbyte av identiteter och tillhörande behörighetsstyrande egenskaper.
- *Godkännandeprocesser* för att
  - Godkänna och följa upp anslutning av användarorganisationer till federationen
  - Godkänna och följa upp anslutning av tjänster till federationen
  - Godkänna och klassificera e-identiteter med tillhörande autentiseringsmetod och utgivningsprocess.

Andra viktiga delar i federationen är

- Det *tekniska ramverket*, dvs. vilken överenskommen teknik som kan användas för informationsutbytet, uppdatering och signering av metadatat osv.
  - Det tekniska ramverket ska i tillämpliga delar följa referensarkitekturens krav.
- *Ombudshantering* – möjliggör att ett ombud kan företräda användarorganisationen vid anslutning till federationen.
  En fungerande ombudshantering kan vara viktig för en mindre användarorganisation och även för samverkansorganisationer där gemensamma tjänster (IdP-tjänster etc.) samutnyttjas av ett antal organisationer.

- En *federationsoperatör* utses normalt för att ansvara för förvaltning av de gemensamma regelverken, drift av metadatatjänsten, samt granskning och godkännandeprocesserna[15].

5.13.3 Tillitsramverk

En av grundpelarna för säkert federativt utbyte är ett överenskommet tillitsramverk, vilket bl.a. sätter gemensamma krav för att bedöma styrkan i (tilliten till) autentiseringslösningar och e-identiteter. Tillitsramverk för en federation brukar även avse krav på organisation och styrning, administrativ och fysisk säkerhet.

Det är viktigt att tillitsramverk utgår från nationellt tillitsramverk som i sin tur bör baseras på internationell standard för tillitsramverk. Helt egendefinierade tillitsramverk i respektive organisation leder snabbt till interoperabilitetsproblem och svårigheter att komma överens om säkerhetsnivåer och godkännandeprocesser.

I Sverige bör *E-legitimationsnämndens tillitsramverk (ELN-700)*[16] vara normerande där så är tillämpligt. Detta ramverk baserar sig i sin tur bland annat på den internationella standarden *ISO/IEC 29115*[17], vilken i sin tur har sina rötter i den amerikanska *NIST Electronic Authentication Guideline SP800-63*[18].
Även arbeten som *Kantara Initiative Identity Assurance Framework*[19] och *Stork*[20] *QAA - Quality of Authentication Assurance* har bidragit till de nuvarande tillitsramverken.

5.13.4 Tillitsnivåer

Tillitsramverket definierar *tillitsnivåer* (*level of assurance, LoA*) för att kategorisera vilken tillit man kan ha till respektive autentiseringslösning. Nivåindelningen i E-legitimationsnämndens tillitsramverk motsvarar också den som används i ISO/IEC 29115 och kan förenklat beskrivas som

- Nivå 1 (LoA1) – Ingen eller mycket begränsad form av tillit[21]
- Nivå 2 (LoA2) – Viss form av tillit

---

[15] Delar kan vara förstås i sin tur läggas på underleverantörer.

[16] ELN-0700, http://www.elegnamnden.se/download/18.64a656d113f4c7597011327/1372846099586/ELN-0700-v1.0-+Tillitsramverk+för+Svensk+e-legitimation.pdf

[17] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45138

[18] http://dx.doi.org/10.6028/NIST.SP.800-63-2

[19] https://kantarainitiative.org/confluence/display/LC/Identity+Assurance+Framework

[20] https://www.eid-stork.eu

[21] Används inte i ELN-700

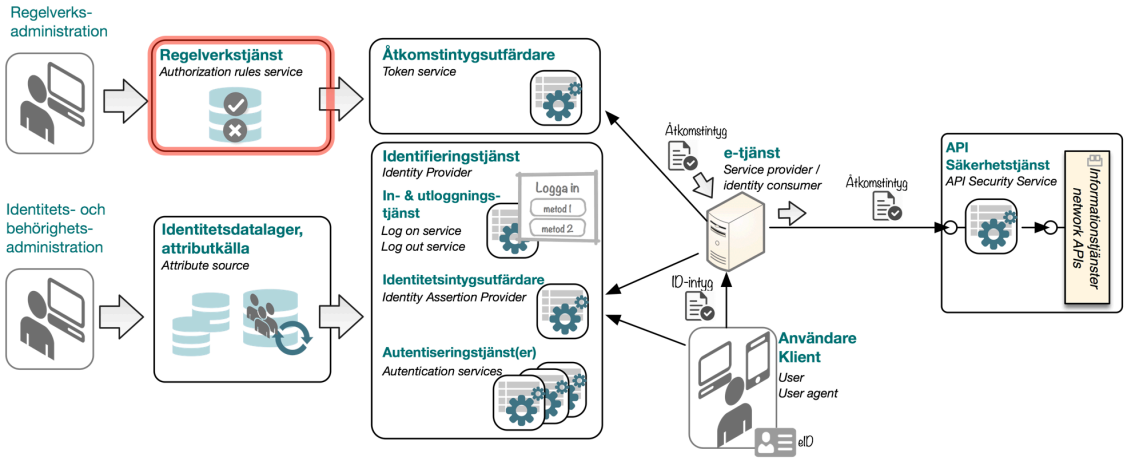
- Nivå 3 (LoA3) – Hög form av tillit
- Nivå 4 (LoA4) – Mycket hög form av tillit

5.13.5 Specifika krav

- Tillitsramverk ska utgå ifrån internationella/nationella tillitsramverk, där anpassningar och tillämpning kan göras för att möta domänspecifika krav och behov.
- E-legitimationsnämndens tillitsramverk bör vara normerande för utformning av tillitsramverk där så är tillämpligt.
- Skyddsvärdet för informationen som hanteras i en e-tjänst (informationsklassningen) och regulatoriska regler (lagrum etc.) avgör krav på (minsta) tillitsnivå för autentiseringslösningen.
- Begreppet *stark autentisering* som används i Socialstyrelsens och Datainspektionens föreskrifter bör likställas med tillitsnivå 3, vilket bland annat ställer krav på att en autentisering skall baseras på flera faktorer i samspel samt att innehavaren av identiteten har legitimerats på ett tillräckligt bra sätt i samband med utfärdandet av e-identiteten.
- Ägaren till en e-tjänst ansvarar för att sätta den tillitsnivå som (minst) krävs för åtkomst till e-tjänsten.

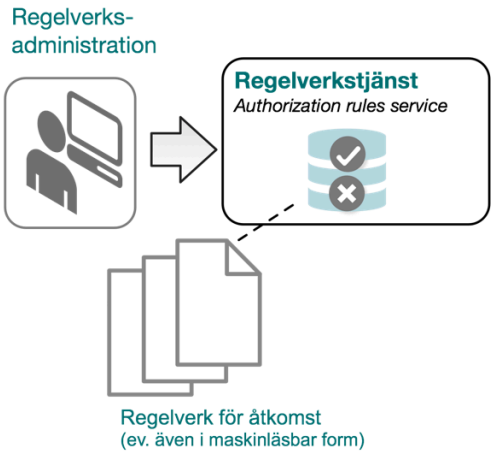
5.14 Regelverkstjänst

Regelverkstjänst representerar ett eller flera verktyg med syfte att samlat administrera regelverk för åtkomst och understödja implementering av regelverken.



Figur 29. Regelverkstjänst i förhållande till referensarkitektur för Identitet och åtkomst.

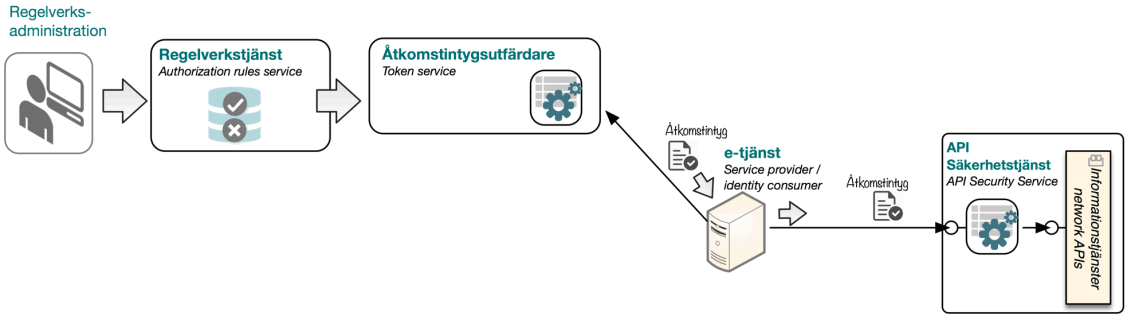
Regelverkstjänst är som sådan inte en obligatorisk teknisk tjänst i referensarkitekturen, utan står mer principiellt för en förmåga som behöver finnas i organisationen: att formulera och strukturerat dokumentera gällande regelverk. Regelverken behöver i grunden vara formulerade i en form som kan läsas och tolkas utan expertkunskaper, helst direkt författat av den verksamhet som berörs.



Regelverken implementeras i de system som behöver utvärdera åtkomst och fatta ett åtkomstbeslut. Dessa system, t.ex. en e-tjänst eller API Säkerhetstjänst, innehåller därmed en ”åtkomstbeslutspunkt” dvs. en s.k. *Policy Decision Point (PDP)*.
Om Regelverkstjänst även kan tillhandahålla beslutade regelverk i maskinläsbar form, skapas en möjlighet att läsa in tillämpbara regelverk i dessa system, och därmed uppnå en automatiserad hantering av implementeringen av regelverket. Nyttan med detta ökar

naturligtvis ju fler e-tjänster/system som kan hanteras på detta vis. Detta är dock i praktiken oftast för komplicerat och kostsamt för att nyttan ska överväga insatsen. Det saknas även en del att önska när det gäller maskinläsbara standardformat för åtkomstregler[22].

Kombinationen av Regelverkstjänst, Åtkomstintygsutfärdare och API-Säkerhetstjänst skapar däremot en möjlighet att via en sammanhållen administration definiera regelverk för en granulär informationsåtkomst via informationsgränssnitt (api:er).



Figur 30. Regelverkstjänst, Åtkomstintygsutfärdare och API-Säkerhetstjänst i kombination för att styra granulär åtkomst till information.

Här kan administrationen av regler även vara en integrerad del av systemet för utfärdande av åtkomstintyg, vilket kan förenkla handhavandet och underlätta att verifiera att rätt regler faktiskt också är implementerade.

Ett exempel på en regel som definieras i Regelverkstjänst:

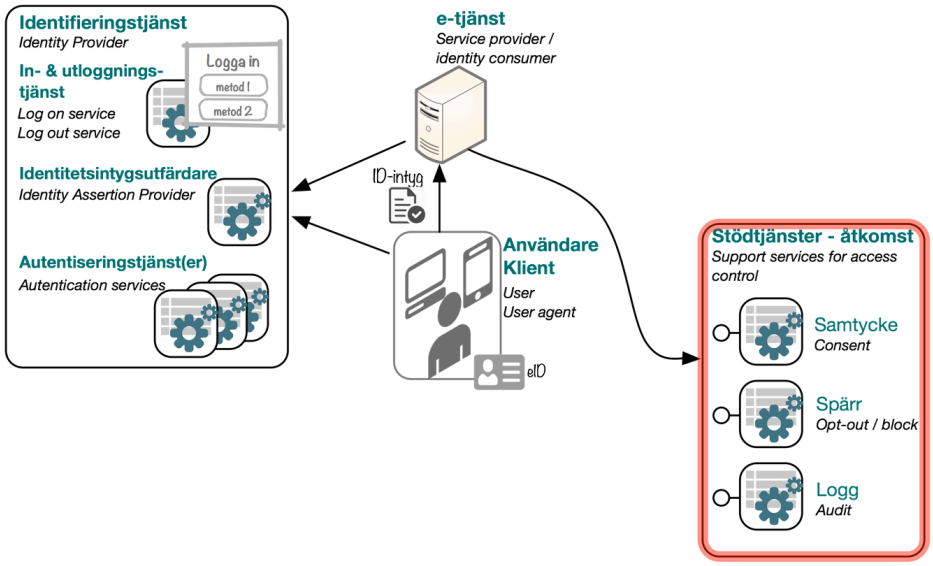
Användaren ska vara behörig (leg. läkare, leg. ssk), anställd med uppdrag inom verksamheten kring vård och behandling, samt vara i tjänst, för att få åtkomst till vårddokumentationen på vårdenheten.

T.ex. en anställd läkare som just nu är föräldraledig skulle med ovan regel alltså inte få se patienternas journalinformation.

[22]Ett standardalternativ är XACML, http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html. Erfarenheter visar dock att det kan vara svårt att fullt ut tillämpa XACML i praktiken.

5.15 Stödtjänster för reglering och uppföljning av åtkomst

För att möjliggöra för en organisation att korrekt reglera och följa upp åtkomsten till information, kan ytterligare stödtjänster och tillhörande informationskällor behöva användas.



Figur 31. Stödtjänster för reglering och uppföljning av åtkomst (exempel).

Stödtjänster inom detta område kan t.ex. hantera

- Individs samtycke
- Loggning och uppföljning av åtkomst

Exakt vilka stödtjänster som behövs beror bland annat på vilka regleringar som gäller i den aktuella verksamhetsdomänen och vilken information e-tjänsten hanterar.

5.15.1 Stödtjänster för åtkomst inom Hälso- och sjukvård

Inom Hälso- och sjukvård har ett antal stödtjänster definierats nationellt för att reglera och följa upp åtkomsten till patientinformation, primärt reglerat i Patientdatalagen. Dessa omfattar:

- Patientens samtycke till åtkomst av sammanhållen vårddokumentation.
- Patientens spärrar av tillgång till hens vårdinformation inom och mellan vårdgivare.
- Loggning och uppföljning av åtkomst till patientinformation.

Tjänsterna är reglerade genom nationella integrationsprofiler, tjänstekontrakt, se [RIVTA] för mer information.

6 Teknisk vy – tekniska regelverk

Hur ska tjänsterna utformas, vilka tekniska krav och regelverk ska/bör vi följa när vi realiserar tjänsterna? Teknik/standard-perspektivet.

Notera att detta avsnitt normalt behöver revideras med tätare intervall än de övriga avsnitten i referensarkitekturen pga. den tekniska utvecklingen på området.

6.1 Indelning av protokoll baserat på dess användning

I referensarkitekturen görs en uppdelning av protokoll för inloggning och auktorisation i följande typer:

- *Autentiseringsprotokoll*, t.ex. certifikatbaserat (client-tls), signaturbaserat.
- *Sign-in protokoll*, t.ex. OIDC 1.0, SAML2.0 (samlp), WS-TRUST
- *Intygstyp* även kallad *biljettyp* (*Token type*), t.ex. Json Web Token, OAuth token, SAML 2.0 token.

Autentiseringsprotokoll används för den primära autentiseringen av en dvs. kontroll av uppgiven identitet mot något slags ”äkthetsbevis”.

Sign-in protokoll används för att logga in i en e-tjänst eller få åtkomst till en resurs baserat på den primära autentiseringen. Det är dessa protokoll som oftast avses när man pratar om protokoll för SSO. Syftet med protokollen är att för e-tjänsten eller resursen förmedla ”bevis” för att identitet och ev. egenskaper är säkerställda och/eller åtkomst ska ges till resurs.

Intygstyp (*Token type, Assertion type*) standardiserar innehållet och används för att paketera ett stycke information som underlag för att e-tjänst/resurs ska acceptera och ge åtkomst, dvs underlag för auktorisation. *Identitetsintyg* innehåller uppgifter om autentiserad användare och egenskaper knutna till användaren. *Åtkomstintyg* specificerar rättigheter till specifik resurs (t ex. scope i OAuth2.0).

6.2 Rekommenderade protokoll per förmåga

Vid val av tekniska protokoll att använda för att implementera referensarkitekturen, ska de styrande principerna i kap. 3 vara vägledande. Inom detta område påverkar framförallt principerna #IA1, #IA3 och #IA5 dessa val, vilket leder till ett urval öppna internationella standarder för områden som t.ex.

- Anslutning av e-tjänster för federerad inloggning
- Singelinloggning (SSO)
- Autentisering
- Beskrivning och säker förmedling av identitet och egenskaper
- Hantering av federation och tillit
- Transportskydd (skydd av nätbaserad kommunikation)

Principen #IA5 kring plattformsneutralitet och stöd för de olika tekniska plattformar för e-tjänster finns inom en organisation, leder till att IT-infrastrukturen kan behöva stödja flera protokoll för en och samma förmåga parallellt.
Referensarkitekturen är därför uppbyggd genom separation av ansvar mellan komponenterna, så att detta stöd kan läggas in på ett fåtal centrala punkter i IT-infrastrukturen, utan att påverka t.ex. e-tjänsterna. Även om detta kan medföra en ökad kostnad för infrastrukturen, är det ett betydligt kostnadseffektivare alternativ än att alla e-tjänster måste byta till en viss teknisk plattform för att passa med säkerhetslösningarna.

Rekommendationer kring teknikval är av ovan skäl uppbyggda som *rekommenderad* (förstahandsval), och *stöds vid behov* (andrahandsval) i IT-infrastrukturen.

Förmåga	Rekommendation	Stöds vid behov
Anslutning av e-tjänst för federerad inloggning, SSO och utloggning. (*sign-in protocols*)	SAML 2.0[23] OpenID Connect (OIDC)[24]	WS-Trust, WS-Federation IWA/Kerberos[25] (dock enbart för lokal SSO)
Identitet och egenskaper. Intygstyp (*token type*)	SAML 2.0 Assertions JSON Identity Suite, JWT	SAML 1.0 Assertions
Delegerad åtkomst	OAuth 2.0 (förmågan saknas inom SAML 2.0-sviten)	Kerberos Constraint Delegation[26] (endast lokalt)
Provisionering. Tillhandahålla identiteter och egenskaper.	Nationellt definierade tjänstekontrakt för identitet och egenskaper SCIM SPML	
Autentisering (*authentication protocols*)	e-identitet med stöd för flerfaktorsautentisering på skyddad bärare. Metod baserad på stark asymmetrisk kryptering och utmaning-svar (*challenge response*). x509 certifikat / client-tls / digital signering PKCS#7 eller motsvarande. Identitetsbärare kompatibel med FIDO UAF/U2F (se kap. 6.5.3.1)	Annan, ev. leverantörsspecifik lösning med motsvarande tillitsnivå, t.ex. en generator för engångslösenord (*OTP*)
Federation & tillit Metadatahantering	SAML Metadata OpenID Connect Federation[27]	WS-Federation
Transportsäkerhet	Transport Layer Security (TLS). RFC7525 Recommendations for Secure Use[28]	

Figur 32. Sammanställning rekommenderade tekniska protokoll per förmåga inom Identitet och Åtkomst.

[23] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

[24] http://openid.net/developers/specs/

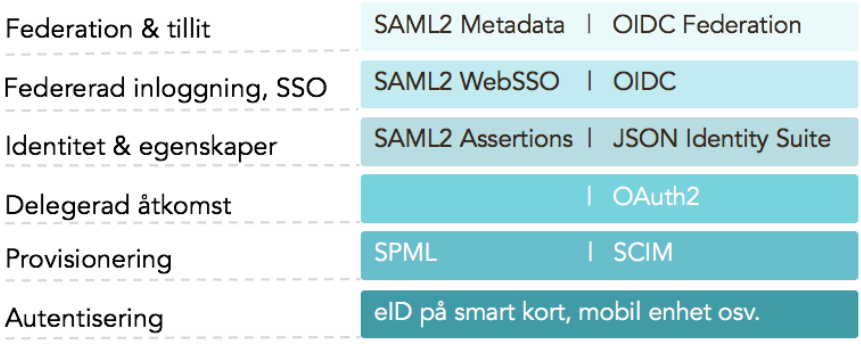
[25] Integrated Windows Authentication med Kerberos, även benämnd ”AD-integrerad inloggning med Kerberos”. Nackdel: saknar federativt stöd, ej optimal vid delade klientdatorer.

[26] https://technet.microsoft.com/en-us/library/jj553400(v=ws.11).aspx

[27] http://openid.net/specs/openid-connect-federation-1_0.html. **Notera** att denna är per ht-2016 en draft, varför implementationer bör ta hänsyn till att specifikationen kan komma att förändras i slutlig version.

[28] https://datatracker.ietf.org/doc/rfc7525/

De olika protokollen kan även delas in i protokollsviter som med följsamhet till en specifik kommunikationsteknik. I följande bild har de rekommenderade protokollen delats upp på sviter baserade på SOAP/XML respektive på HTTP/REST/JSON:



Figur 33.Teknikstack - rekommenderade tekniska protokoll per förmåga, uppdelat på stack för SOAP/XML resp. stack för HTTP/REST/JSON-baserad kommunikation.

Notera att två protokollsviter, SAML 2.0 resp. OpenID Connect/OAuth2, är rekommenderade, vilket innebär för interoperabiliteten att

- Identifieringstjänsten bör ha stöd för både SAML2 resp. OpenID Connect.
- E-tjänsten bör ha stöd för en av SAML 2.0 resp. OpenID Connect.

Orsaken till denna rekommendation är det är viktigt att ta till vara tidigare investeringar i säkerhetsteknik och anslutningar av e-tjänster. Den nyare OpenID Connect har flera fördelar gentemot SAML 2.0[29], varför det kan förutsättas att OpenID Connect successivt kommer att användas i allt större utsträckning. Den äldre och mognare SAML 2.0, som har gott stöd i många standardprodukter och används i ett stort antal globala och nationella identitetsfederationer, kommer dock att behöva stödjas under överskådlig tid, varför det är viktigt att infrastrukturen också ger stöd för SAML2.0-protokollen.

[29] Möjlighet till högre säkerhet, bättre interoperabilitet, bättre stöd för olika teknikplattformar (mobilt, nativa klienter), samt delegerad åtkomst via åtkomstintyg.

6.3 Protokoll för federerad inloggning och SSO

6.3.1 Specifika krav

6.3.1.1 SAML 2.0

Standardprofiler

För SAML 2.0 gäller att ingående identifieringstjänster (*Identity Providers*) och e-tjänster (*Service Providers*) ska stödja standardprofilerna

- *eGov 2.0*[30]
  Implementationsprofil som beskriver vilka delar av SAML som måste implementeras.

samt

- *saml2int*[31]
  Deploymentprofil som beskriver vilka delar av SAML 2.0 som måste vara i bruk samt hur dessa ska användas.

Profilerna beskriver bland annat hur SAML 2.0 *Web Browser SSO Profile* ska användas. Några följder av profilerna är att

- e-tjänster ska acceptera icke-ombedda intyg (*unsolicited responses*)
- all nätverkskommunikation mellan parterna ska skyddas med TLS på transportnivå.

Kompletterande krav

- För transportskydd med TLS följs rekommendationerna i RFC 7525[32] samt *OWASP*[33].
- Identifieringstjänsten (IdP) ska validera att *AssertionConsumerServiceURL* stämmer med metadata för e-tjänsten (SP).
- E-tjänst som anger tillitskrav på autentiseringen, ska stödja att ange denna enligt
  - SAML 2.0 Identity Assurance Profiles [IAP[34]] och [IANA LoA[35]].

[30] http://kantarainitiative.org/confluence/download/attachments/38929505/kantara-report-egov-saml2-profile-2.0.pdf

[31] http://saml2int.org/profile/current

[32] Recommendations for Secure Use of Transport Layer Security, https://tools.ietf.org/html/rfc7525

[33] https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

- OASIS definierade scheman för autentiseringsklasser[36].

- Rekommenderade tekniska bindningar för Web Browser SSO Profile:
  - För SP-initierad SSO (utgående från e-tjänsten): Redirect/POST Binding
  - För IdP-initierad SSO (utgående från intygsutgivaren): POST Binding

6.3.1.2 OpenID Connect

Standardprofiler

För OpenID Connect gäller att ingående Identifieringstjänster (*OpenID Provider, OP*) och e-tjänster (*Relying Parties, RP*) ska stödja standardprofilerna

- *OpenID Connect 1.0*[37] enligt *OpenID Connect Conformance Profiles*[38], minst stöd för en av profilerna
  - *Basic Relying Party (code flow)*
    - Rekommenderat förstahandsval.
    - Används då säkerhetskraven är höga; intyget exponeras inte i användarens klient (*user agent/browser*).
    - Anpassat för webbapplikationer, nativa (rika) klienter och mobila appar.
    - Kräver att applikationen har en serversida (*backend*) som kan autentisera sig mot Identifieringstjänsten (*OP*) för att hämta intyget.
  - *Implicit Relying Party (implicit flow)*
    - Används endast om applikationen saknar serversida (*backend*), t.ex. webbläsarbaserad klientapp.
    - Rekommenderas ej om säkerhetskraven är höga; intyg exponeras i användarens klient (*user agent/browser*).
  - *Hybrid Relying Party.*

---

[34] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.html
[35] https://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml
[36] https://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf
[37] http://openid.net/connect/
[38] http://openid.net/wordpress-content/uploads/2015/02/OpenID-Connect-Conformance-Profiles.pdf

- I princip som *Basic Relying Party,* men intyget skickas även till användarens klient (*user agent*/*browser*).
- Används endast vid behov. Hög säkerhet kan uppnås, men användarens klient måste kunna hantera intyget på ett säkert sätt.
- Kräver att applikationen har en serversida (*backend*) som kan autentisera sig mot Identifieringstjänsten (*OP*) för att hämta intyget.

Kompletterande krav

- E-tjänst och Identifieringstjänst bör stödja *Relying Party-initierad* utloggning enligt *OIDC Session Management*, i syfte att vid utloggning även logga ut ur SSO-sessionen hos Identifieringstjänsten (*OP*).
- Identifieringstjänster (*OP*) ska stödja
  - *OIDC Discovery* för att dynamiskt upptäcka information om tillgängliga Identifieringstjänster (*OPs*).
  - *Dynamic Registration* för att dynamiskt registrera klienter (*RPs*) hos en Identifieringstjänst (*OP*).
  - Att kunna utfärda digitalt signerade *JWT bearer tokens* som identitetsintyg.
  - Att kunna tillhandahålla *autentiseringskontext* i identitetsintyget *(authentication context class reference* och *authentication methods reference)*.
- Vid höga säkerhetskrav rekommenderas e-tjänster (*RPs*) och Identifieringstjänster (*OPs*) i tillämpliga delar följa profilerna
  - *HEART profile for OpenID Connect*[39].
    En profil för höjd säkerhet och ökad interoperabilitet.
  - *OIDC Enhanced Authentication Profile*[40].

[39] http://openid.net/wg/heart/

[40] **Notera** att denna är per 2016-11-15 en *draft-standard*, varför implementationer bör ta hänsyn till att specifikationen kan komma att förändras i slutlig version.

6.4 Protokoll för delegerad åtkomst

6.4.1 Specifika krav

6.4.1.1 OAuth 2.0

Standardprofiler

- OAuth 2.0[41] enligt RFC6749 OAuth 2.0 Authorization Framework [42]
- Säkerhetsanvisningar enligt RFC6819 OAuth 2.0 Threat Model and Security Considerations[43]

Kompletterande krav

- E-tjänst med behov av åtkomst till skyddade integrationsgränssnitt (api:er), bör ha möjlighet att använda följande profil för att utgående från ett tidigare erhållet identitetsintyg erhålla åtkomstintyg från Åtkomstintygsutfärdare:
  - *SAML2 Bearer Assertion - RFC 7522*[44]
    Profil för integration med existerande Identifieringstjänst baserad på SAML 2.0.
    alternativt
  - *JWT Bearer Assertion - RFC 7523*[45]
    Profil för integration med existerande Identifieringstjänst baserad på OpenID Connect.

[41] https://oauth.net/2/
[42] https://tools.ietf.org/html/rfc6749
[43] https://tools.ietf.org/html/rfc6819
[44] http://tools.ietf.org/html/rfc7522
[45] http://tools.ietf.org/html/rfc7523

6.5 Autentiseringsteknik

6.5.1 Specifika krav

- Protokoll för autentisering bör bygga på en kryptografisk stark (svårforcerad) metod.
- Protokoll för autentisering bör följa rekommenderande best-practise mönster, se kap. 6.5.2.
- Överenskomna tillitsramverk används för att jämföra/jämställa olika autentiseringslösningar, för att möjliggöra åtkomst till information av visst skyddsvärde på lika villkor oavsett autentiseringslösning.

6.5.2 Rekommenderat mönster för autentiseringsprotokoll

En vanlig och rekommenderad klass av starka metoder baseras på asymmetrisk kryptering med långa kryptonycklar i kombination med utmaning-svar (*challenge response*). Dessa metoder följer följande principflöde:

1. Autentiseringstjänsten skickar en utmaning till användarens autentiseringslösning (innehållande e-identiteten). Utmaningen innehåller inslag av slumpmässighet för att skydda emot uppspelningsattacker.
2. Autentiseringslösningen använder sin hemliga nyckel för att utföra en kryptografisk operation baserat på utmaningen och returnerar svaret till Autentiseringstjänsten.
3. Autentiseringstjänsten verifierar kryptografiskt att det är just den uppgivna e-identiteten som måste ha använts för att framställa svaret.

Tekniska metoder som kan användas för ovan inkluderar

- x509 certifikat / client-tls (på mjukvarubaserad eller hård bärare).
- digital signering med PKCS#7 eller motsvarande.

Autentiseringslösningen kan även utnyttja annan unik information som kan knytas till den enhet som används som identitetsbärare, t.ex. ett unikt serienummer eller dylikt, för att försvåra kopiering av e-identiteten till annan enhet.

6.5.3 Standardisering av autentiseringsmetoder

Autentiseringsmetoder är typiskt under ständig teknisk utveckling och området saknar en enhetlig standardisering. Dock finns internationella initiativ som syftar till att öka interoperabiliteten mellan olika leverantörers autentiseringslösningar.

6.5.3.1 FIDO Alliance

FIDO Alliance (se kap. 7) inkluderar två publika specifikationer för autentisering: UAF och U2F enligt nedan:

- *UAF* (*Universal Authentication Framework*) – erbjuder användaren att autentisera sig utan användarnamn/lösenord med hjälp av en certifierad identitetsbärare efter att användaren registrerat sin identitet och knutit identitetsbäraren till denna. Identitetsbäraren måste innehålla en så kallad UAF-implementation för att vara kompatibel med protokollet.

Figur 34. UAF principiell användarupplevelse (källa: FIDO Alliance)

- *U2F* (*Universal Second Factor*) – erbjuder användaren att använda en certifierad identitetsbärare som tillför en ytterligare faktor vid autentisering av en användare mot en applikation (t.ex. biometri eller en kodgenerator). Användaren kommer i detta fall att först autentisera sig med användarnamn/lösenord för att därefter krävas ytterligare en autentiseringsfaktor, realiserad i form av en U2F-kompatibel identitetsbärare.

Figur 35. U2F principiell användarupplevelse (källa: FIDO Alliance)

De olika delarna i en FIDO-baserad lösning kan certifieras av FIDO Alliance: identitetsbäraren, klientprogrammet respektive autentiseringstjänsten.

Notera: FIDO-specifikationerna adresserar dock inte hur identitetsbäraren knyts till den faktiska innehavaren dvs. slutanvändaren. En UAF/U2F-baserad lösning behöver därför kompletteras med en separat legitimeringskanal, aningen fysisk eller elektronisk, för att identifiera innehavaren i enlighet med den nivå av tillit man önskar uppnå på e-identiteten.
Exempel på detta är att använda mönstret för ärvd legitimering (kap. 5.10.3) i samband med registreringen av UAF/U2F-kompatibel autentiseringslösning.

6.6 Tekniska ramverk för federation

6.6.1 Specifika krav

- Metadata är den tekniska implementationen av medlemsregistret och används av samverkande infrastrukturtjänster för identitet och åtkomst. Identitetsintygsutfärdare (Identity Providers), e-tjänster (Service Providers/Relying Parties) samt eventuella stödtjänster (t.ex. Discovery Service) registreras i federationens metadata.
- Metadata ska vara digitalt signerat av federationsoperatören, vilket gör att metadatats riktighet kan verifieras av alla parter. Med stöd av metadata kan de ingående tekniska tjänsterna lokalisera och identifiera varandra på ett säkert sätt, dvs. det ger en förutsättning för säker kommunikation mellan tjänsterna.
- Utformning av metadata styrs av
  - För SAML 2.0: *OASIS SAML 2.0 metadata specification*[46]
  - För OIDC: *OIDC Federation 1.0*[47]
- Hantering av metadata styrs av
  - För SAML 2.0: *OASIS SAML 2.0 Metadata Interoperability Profile*[48]
  - För OIDC: *OIDC Federation 1.0* (se not ovan)

[46] http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[47] http://openid.net/specs/openid-connect-federation-1_0.html. **Notera** att denna är i skrivande stund en draft, varför implementationer bör ta hänsyn till att specifikationen kan komma att förändras i slutlig version.

[48] http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf

6.7 Tekniska regelverk för provisionering

6.7.1 Tekniskt mönster för provisionering

Provisionering av identitetsdata kan ske via olika tekniska mönster, där följande prioritetsordning bör följas vid teknisk utformning av provisionering till e-tjänst:

1. Tillhandahålla identitetsdata via identitetsintyg vid behov kompletterat med tjänstegränssnitt enligt principen fråge-svar (pull).
2. Tillhandahålla identitetsdata via prenumeration på förändringar i (visst urval av) identitetsdata (publish/subscribe)
3. Tillhandahålla identitetsdata via funktion som replikerar identitetsdata till e-tjänsten (push).

Motivet till prioritetsordningen är att sträva efter enkla lösningar och så lös koppling som möjligt mellan IT-infrastrukturen och e-tjänsterna (princip IT4), vilket underlättar förändringshantering och håller nere förvaltningskostnaderna.

Dock behöver hänsyn också tas till e-tjänstens tekniska förutsättningar vid val av provisioneringsteknik för den specifika e-tjänsten.
Principen att tillhandahålla kvalitetssäkrad identitetsdata från gemensamt identitetsdatalager är viktigare än teknikvalet; om alternativet är att administrera identitetsdata separat och manuellt i e-tjänsten, bör väljas den provisioneringsteknik som e-tjänsten har möjlighet att realisera.

Alternativ 3 (push) kan innebära att använda ett produktspecifikt tjänstegränssnitt som tillhandahålls av e-tjänsteleverantören för att skapa/ändra och ta bort identitetsdata i e-tjänsten. För att undvika hård koppling, bör integrationen i sådant fall implementeras som en adapter ovanpå ett generiskt tjänstegränssnitt. Därmed kan olika adaptrar läggas till och förändras oberoende av varandra.

6.7.2 Protokoll för provisionering

Det bör noteras att det viktigaste när det gäller gränssnitt för provisionering är egentligen inte protokollet i sig utan ett väl definierat och överenskommet innehåll, dvs de attribut som behöver överföras, eftersom det är ett innehållet som avgör vad som kan åstadkommas och vilka attribut som e-tjänst respektive attributkälla behöver kunna hantera.

Det finns dock standardiserade protokoll för syftet provisionering av identitetsdata och dessa bör om möjligt användas.

Rekommenderade protokoll

- Nationellt definierade tjänstekontrakt för identitet, behörighet och egenskaper
- SCIM

- SCIM RFC7644[49]
- SCIM stödjer både mönster för pull (GET) och push (POST).

- SPML 2.0 (eller senare)[50]
  - "SPMLv2 XSD Profile" för anpassning till XML och SOAP.

[49] https://tools.ietf.org/html/rfc7644
[50] https://www.oasis-open.org/standards#spmlv2.0

7 Bilaga: Förkortningar

Förteckning över ett urval använda förkortningar/beteckningar.

IAM	*Identity & Access Management*, Identitets- och åtkomsthantering
SSO	*Single sign-on*, Singelinloggning
SLO	*Single Logout*, Singelutloggning
HTTP	*Hypertext Transfer Protocol*. Kommunikationsprotokoll ovanpå TCP (*Transmission Control Protocol*)
REST	*Representational State Transfer (REST)* är ett IT-arkitekturbegrepp som beskriver ett sätt hur tjänster för maskin till maskin-kommunikation kan tillhandahållas. https://sv.wikipedia.org/wiki/Representational_State_Transfer
JSON	*JavaScript Object Notation*, ett kompakt, textbaserat format som används för att utbyta data. https://sv.wikipedia.org/wiki/JSON
SOAP	XML-baserat protokoll för utbyte av information i distribuerade miljöer. https://sv.wikipedia.org/wiki/SOAP
XML	*Extensible Markup Language*, ett standardiserat utbyggbart märkspråk. https://sv.wikipedia.org/wiki/XML
JWT	*JSON Web Token*, JSON-baserad öppen standard (RFC 7519) för skapande av åtkomst- och identitetsintyg (tokens).
TLS	*Transport Layer Security*, öppen standard för säkert utbyte av krypterad information mellan datorsystem. https://sv.wikipedia.org/wiki/Transport_Layer_Security
SAML	*Security Assertion Markup Language* https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

OIDC	*OpenID Connect*, OpenID Foundation http://openid.net
OAuth	Protokoll för delegerad åtkomst och auktorisation. Används även som underliggande protokoll för OIDC. https://oauth.net/2/
IdP, OP	*Identity Provider* respektive *OpenID Provider*. Identifieringstjänster inom SAML resp. OIDC.
SP, RP	*Service Provider* resp. *Relaying Party*. Beteckning på e-tjänst inom SAML resp. OIDC som tar emot intygade uppgifter om vem användaren är och dennes egenskaper och i syfte att kunna logga in användaren i e-tjänsten.
FIDO	*FIDO Alliance* är en icke vinstdrivande organisation med syfte att adressera interoperabilitet och användbarhet för autentiseringslösningar. https://fidoalliance.org
UAF	*Universal Authentication Framework*. Publik specifikation för autentisering från FIDO Alliance.
U2F	*Universal Second Factor*. Publik specifikation för autentisering från FIDO Alliance.
PKCS	*Public Key Cryptography Standards*. https://en.wikipedia.org/wiki/PKCS
IWA	*Integrated Windows Authentication*. https://en.wikipedia.org/wiki/Integrated_Windows_Authentication
SCIM	*System for Cross-domain Identity Management*. https://en.wikipedia.org/wiki/System_for_Cross-domain_Identity_Management
SPML	*Service Provisioning Markup Language*. https://en.wikipedia.org/wiki/Service_Provisioning_Markup_Language
SITHS	En tjänstelegitimation för både fysisk och elektronisk identifiering, med ursprung inom Hälso- och sjukvården.

	http://www.inera.se/TJANSTER--PROJEKT/SITHS/
AD	Active Directory, en typ av katalogtjänst. https://sv.wikipedia.org/wiki/Active_Directory
OWASP	Open Web Application Security Project https://www.owasp.org
IANA	Internet Assigned Numbers Authority http://www.iana.org