# Referensarkitektur för Identitet och åtkomst

## Utformning av IT-stöd för säkerställd identitet och åtkomst till rätt information vid rätt tillfälle, inom och mellan organisationer

Revision B

inera
Ett företag inom SKR

# Innehållsförteckning

# Revisionshistorik

| VERSION | DATUM | FÖRFATTARE | KOMMENTAR |
|---|---|---|---|
| Rev A | 2017-08-16 | Per Mützell | *Fastställd utgåva efter remiss i Ineras Arkitekturråd. Adderat kap. 1.3 Målgrupp. Rättelse: ”dataskyddsreform” ersatt av ”dataskyddsförordning”.* |
| Rev B PA1 | 2021-04-11 | Per Mützell | *Remissversion av Revision B. Huvudsakliga ändringar:*<br>- *Lagt till autentisering och auktorisation av system. Kompletterat med system som aktör där tillämpligt. Introducerar åtkomstintyg utfärdade till system, innehavsbevis, egenskaper för system och flöden som enbart omfattar system-till-system-kommunikation.*<br>- *Utökat med fler användningsfall för delegerad åtkomst från användare.*<br>- *Utökat kap. om Legitimeringstjänst/IdP samt delvis omstrukturerat. Mer om utloggning, avslutande av SSO, samverkan med flera IdP:er, val av IdP, tillhandahållande av attribut.*<br>- *Viss uppdatering av terminologi, bl.a. Legitimeringstjänst (IdP)*<br>- *Uppdaterat tekniska protokoll och referenser, inkl. stöd för system som aktör, anrop av system i flera led, innehavsbevis osv.* |
| Rev B PA2 | 2022-10-17 | Per Mützell | *Justerad efter feedback från Inera Arkitekturråd Regioner, Inera Sektion Arkitektur samt leverantörsnätverk.* |
| Rev B | 2023-03-27 | Per Mützell | *Fastställd utgåva efter remiss i Inera Arkitekturråd Regioner* |

# 1 Dokumentinformation

## 1.1 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 | Styrande principer, vägledande exempel och teknisk referensarkitektur för vård och omsorg. http://rivta.se/documents/ARK_0019/ |
| RIV-Kryptering | RIV Tekniska anvisningar - Anvisning för kryptering (ARK_0036) https://rivta.se/documents/ARK_0036/ |
| eIDAS | eIDAS-förordningen (910/2014). EU:s förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. http://data.europa.eu/eli/reg/2014/910/oj |

## 1.2 Målgrupp

Detta dokument riktar sig i första hand till IT-arkitekter, IT-strateger, IT-beslutsfattare samt beställare/utvecklare av såväl e-tjänster för slutanvändare som IT-infrastruktur för identitets- och åtkomsthantering.

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

## 1.3 Bakgrund och syfte

*Referensarkitektur för Identitet och åtkomst* syftar till att ge stöd till utformning av IT-stöd för säkerställd identitet och åtkomst till rätt information vid rätt tillfälle. Referensarkitekturen kan i tillämpliga delar appliceras både inom en organisation för lokalt IT-stöd, och vid samverkan mellan organisationer, till exempel för hantering av regionala och nationella e-tjänster. Användaren av tjänsterna kan vara såväl en medarbetare tillhörande en organisation, som en invånare som agerar i sin privata roll.

Referensarkitekturen är tänkt att användas som referensunderlag vid anskaffning och vidareutveckling av lösningar för identitets- och åtkomsthantering, vilket kan omfatta såväl upphandling av leverantörsprodukter, anpassning av befintlig IT-infrastruktur och kravställning på e-tjänster/IT-system för följsamhet till arkitekturen.

Valen av öppna standarder inom området är gjorda för att ge goda möjligheter att välja standardprodukter på marknaden för den IT-infrastruktur som behövs för att realisera arkitekturen, samtidigt som leverantörer av e-tjänster kan implementera allmänt användbara funktioner för identitet och åtkomst med standardgränssnitt som kan appliceras på flera marknadssegment.

Referensarkitekturen kan även fungera som en ”normerande mall” inom identitets- och åtkomsthantering, och på så sätt göra olika lösningarna enklare att kommunicera kring och jämföra med varandra. Leverantörer inom området uppmanas att beskriva sina produkter och lösningar relativt referensarkitekturen för att underlätta sådan jämförelse.

Dokumentet är indelat i fem huvudavsnitt:

- **Översiktlig orientering** över området identitets- och åtkomsthantering.
- **Styrande principer** - Vad är styrande för utformningen av referensarkitekturen och varför?
- **Verksamhetsvy** – Vilka behov hos verksamheter och enskilda individer inom området Identitet och Åtkomst syftar referensarkitekturen till att möta? Vilka förmågor inom området behövs för att stödja behovet?
- **Informationssystemvy** - Vilka infrastrukturtjänster behöver vi för att realisera/besitta beskrivna förmågor? Vad behöver e-tjänster och övriga IT-system ansvara för och förhålla sig till? Vilka principiella flöden och krav behöver stödjas?
- **Teknisk vy** - Hur ska tjänsterna utformas, vilka tekniska krav, protokoll och regelverk ska följas vid realisering av tjänsterna?

För använda förkortningar i texten och symboler i bildmaterialet, se *Bilaga: Förkortningar* samt *Bilaga: Symboler*.

## 1.4 Grundläggande begrepp och termer

***auktorisation (authorization)*** – (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***.

***autentisering (authentication)*** – 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, till exempel enbart ett hemligt lösenord (*enfaktorautentisering*) eller både ett tumavtryck och innehav av personlig smart mobil (*tvåfaktorautentisering*) osv.
Inom svensk författning förekommer även begreppet ***stark autentisering*** – ”autentisering som innebär att identiteten kontrolleras på två olika sätt”. För att räknas som ”stark” i detta sammanhang ska autentiseringen alltså baseras på (minst) två faktorer, men man bör även lägga till krav på att personens identitet har säkerställts på ett tillräckligt säkert sätt i samband med utfärdande av dennes e-id.

***attribut, egenskaper (attributes)*** – i detta sammanhang synonyma begrepp för egenskaper för användare, organisationer och IT-systemresurser. Exempel: yrkeslegitimation för personal, en privatpersons namn eller ett systems organisatoriska tillhörighet.

***delegering (delegation)*** – en aktör auktoriserar en annan aktör att verka i dess ställe (*on behalf of*).

***e-legitimering (electronic identification)*** – person legitimerar sig elektroniskt mot ett IT-system för att (be)visa vem hen är. Fastställande av personens identitet implicerar också autentisering.

***e-legitimation, e-id (eID)*** – elektronisk identitetshandling för legitimering mot IT-system.
En e-legitimation förvaras på en för ändamålet avsedd ***bärare***, vilket till exempel kan vara en USB-sticka, ett smart kort eller ett säkert utrymme på en mobiltelefon.

***e-legitimationsutfärdare (eID issuer)*** – part som tillhandahåller e-legitimation till personer.
Relaterat: ***utfärdande av e-id / e-legitimation (eID issuance)*** – en process för att en person får tillgång till en elektronisk identitetshandling (e-id). Utfärdandet kan till exempel innebära att en person får en e-legitimation på en mobil enhet för kommunikation med myndigheter. En person kan ha flera e-id / e-legitimationer som alla unikt identifierar personen.
När person själv hanterar delar eller hela utfärdandeprocessen för eget e-id kan begrepp som registrering, utfärdande via självservice osv. vara tillämpliga.

Relaterat: ***ärvd legitimering*** – process för att skapa ett nytt e-id med ett befintligt e-id som underlag. Exempel: ett mobilt e-id utfärdas baserat på att personen legitimerar sig elektroniskt med annat för ändamålet godkänt e-id i en tjänst för självadministration.

***e-tjänst*** (***Service Provider, SP)*** – IT-tjänst som tillhandahåller en funktion till användare. I federativa sammanhang tar en *Service Provider* emot intygade uppgifter om vem användaren är och dennes egenskaper i syfte att kunna identifiera, autentisera och tänkbart auktorisera användaren i IT-tjänsten. Även kallad ***Relying party (RP)*** och ***Identity Consumer***.

[2] Socialstyrelsens termbank

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

***identifiering (identification)*** – en process där en aktörs identitet fastställs, oftast med krav på *autentisering*.

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

***integrationstjänst /API (API)***– ett beskrivet tekniskt gränssnitt för utbyte av information över nätverket mellan en klientprogramvara och en serverprogramvara.

***klientenhet, användares enhet (client device)*** – begrepp som refererar till datorer, mobila enheter och andra fysiska enheter som användare nyttjar för att få tillgång till IT-system och applikationer.

***klient (user agent)*** – *(här)* den programvara som exekverar på klientenheten och agerar användarens gränssnitt.

***legitimeringstjänst/IdP (Identity Provider)****, även benämnd* ***identitetsintygstjänst*** – Tjänst i IT-infrastrukturen som utför identifiering och autentisering av användare på begäran av en e-tjänst (Service Provider). En användare kan legitimera sig elektroniskt via Legitimeringstjänst. Legitimeringstjänsten agerar även i rollen ***identitetsintygsutfärdare*** och utfärdar vid godkänd legitimering ett ***identitetsintyg*** (***ID token***) till e-tjänsten med begärda uppgifter om en identifierad och autentiserad användare.

***Policy Administration Point, PAP***. Inom mönster för auktorisation är PAP den förmåga som erbjuder administrativt gränssnitt för att redigera och hantera åtkomstregler.

***Policy Enforcement Point, PEP****.* Inom mönster för auktorisation är PEP den förmåga som genomdriver åtkomstbeslut som svar på en begäran om åtkomst till en resurs.

***Policy Decision Point, PDP****.* Inom mönster för auktorisation är PDP den förmåga som fattar ett åtkomstbeslut baserat på åtkomstpolicy, egenskaper för begärande part, egenskaper för begärd resurs osv.

***Policy Information Point, PIP****.* Inom mönster för auktorisation är PIP en källa för behörighetsstyrande attribut att använda som underlag för åtkomstbeslut.

***provisionering av (digital) identitetsdata (provisioning of identity data)*** – *(här)* process för att tillhandahålla kvalitetssäkrad information om elektroniska identiteter och tillhörande egenskaper, till exempel i syfte att skapa användarprofiler i identitetsdatalager och e-tjänster.

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

***regulatoriskt regelverk (regulatory framework)*** – sammanhållande term för lagar, förordningar, informationssäkerhetspolicys etc. som är styrande för hur lösningarna utformas.

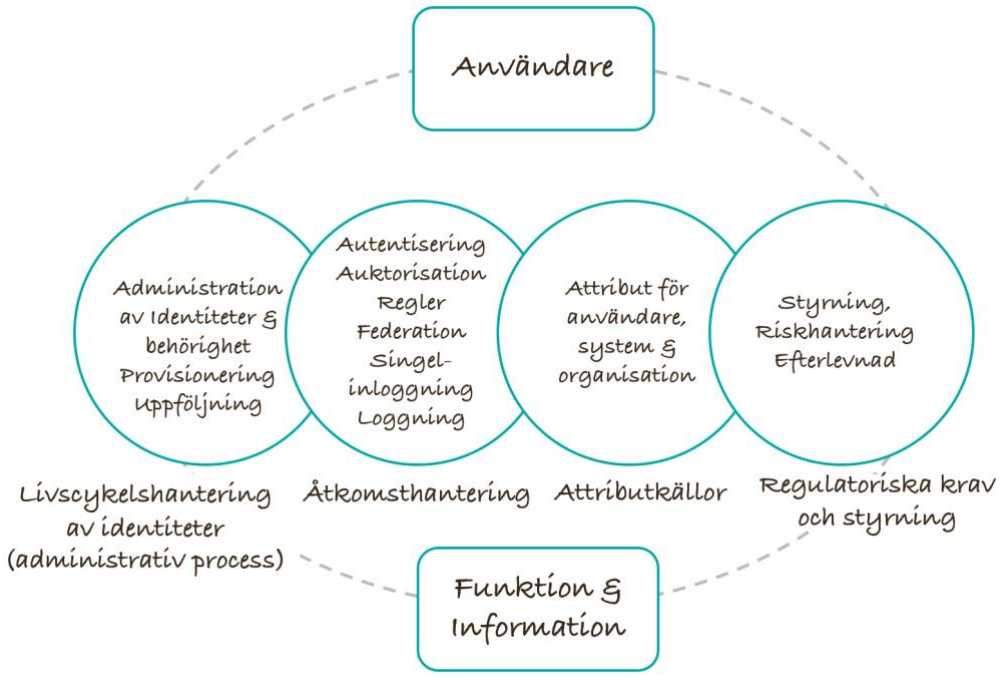
***singelinloggning (Single Sign-on, SSO)*** – en användare behöver endast logga in en gång för att nå de system som är anpassade till tjänsten. SSO är ett ganska vitt begrepp och det finns flera ”undervarianter” som alla kan kombineras: användaren återkommer till samma system inom en viss tid och slipper logga in igen; användaren går in i flera system med en gemensam inloggning.
Ett relaterad men strikt sett annat begrepp är *samordnad inloggningsfunktion* dvs. användaren kan använda samma inloggningsfunktion för flera olika system.

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

***åtkomstintygstjänst*** *(**access token service, authorization server**)* – tjänst som utfärdar ***åtkomstintyg*** för åtkomst till skyddade integrationsgränssnitt (API:er). Tjänsten agerar således *åtkomstintygsutfärdare.* Även kallad ***tokentjänst*** eller ***auktorisationstjänst***.

# 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.

Referensarkitekturen för Identitet och åtkomst syftar till att kunna användas såväl i medarbetarperspektiv (e-tjänster för professionen) som invånarperspektiv (e-tjänster riktade till privatpersoner).
Referensarkitekturen kan även tillämpas för att åstadkomma säker system-till-system-kommunikation.

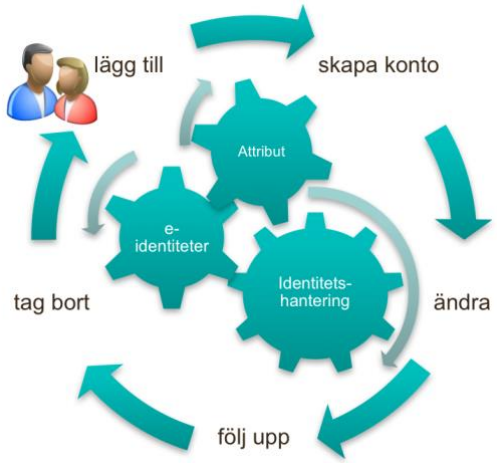
Styrande för vilken säkerhetsnivå som ska sättas är i huvudsak de regulatoriska kraven (lagar, föreskrifter etc.), informationens skyddsvärde samt verksamhetens riskbedömningar.
Referensarkitekturen har som målsättning att kunna stödja vid var tid gällande nationella, regionala och sektorsspecifika regelverk kring informationssäkerhet i samhället, till exempel inom hälso- och sjukvård, omsorg, skola, samhällsbyggnad osv.
Till exempel läggs grunden till säkerhetskraven inom hälso- och sjukvården i *Patientdatalagen* och

Socialstyrelsens föreskrifter och handböcker.
Det finns även mer generella regelverk att ta hänsyn till såsom *Dataskyddsförordningen*[3].

Organisationens riktlinjer för informationssäkerhet konkretiserar kravbilden ytterligare, till exempel 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, 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 *livscykelhantering av e-identiteter* och tillhörande egenskaper.




*Figur 2: Livscykelhantering 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.

Referensarkitekturen syftar i stort till att beskriva en modell för hur dessa funktioner kan realiseras i IT-stödet, hur samverkan kan etableras mellan olika organisationers IT-lösningar, och vilka krav som därmed ställs på e-tjänster respektive IT-infrastruktur.

[3] https://www.riksdagen.se/sv/dokument-lagar/

# 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 via identitetsfederation.
  - 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 tjänst för e-legitimering 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 och ny autentiseringsteknik utan att påverka anslutna e-tjänster.

**#IA3**: e-tjänster ansluts till IT-infrastrukturen för e-legitimering i första hand via standardiserad s.k. biljettbaserad teknik som levererar identitetsdata och grundläggande behörighetsgrundande 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 federerade 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 eller individuella behov 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-id/e-legitimationer, 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 bärare för e-id* för stark flerfaktorautentisering.

Motiv: Ger en flexibilitet som bättre kan stödja olika verksamhetsbehov och teknikskiften, och därmed minskar trösklarna för att införa säkra autentiseringslösningar i verksamheterna. Med anpassade lösningar för e-id och e-legitimering, ökar möjligheterna att i verksamheten implementera säkra lösningar för åtkomst till IT-stödet.

**#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, leder till starka tekniska krav och begränsningar på den utrustning som kan användas i IT-stödet.

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

Motiv: Biometriska data är integritetskänslig information. Det kan finnas fall då biometriska 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 hos verksamheter och enskilda individer:

- Uppfylla regulatoriska krav och behov av informationsskydd, till exempel krav på stark autentisering och möjlighet att följa upp åtkomst till information.
- Samordnad, enkel och säker singelinloggning (SSO) till lokalt, regionalt och nationellt IT-stöd (e-tjänster).
- Möjliggöra flexibla inloggningssätt anpassade till såväl individen, verksamheten som informationssäkerhetskrav.
- Möjliggöra mobila arbetssätt, både vad gäller användarnas 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 tillförlitliga e-id för elektronisk legitimering i IT-stödet.
- 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 sätt anpassade till verksamhetens och individens behov, utan teknisk låsning till vald säkerhetsteknik.
- Säker och behörig åtkomst till information som tillgängliggörs via integrationstjänster (API:er).

- Kunna samverka kring IT-lösningar över organisationsgränser, utan att säkerhet och identitet- och behörighetshantering blir ett hinder, till exempel
  - Samverkan via nationella och regionala e-tjänster.
  - Gemensamma verksamhetsstöd över organisationsgränser.
  - Samverkan med myndigheter – till exempel krav på federativ anslutning för att nå myndigheters integrationstjänster.
  - Nyttja molntjänster hos extern tjänsteleverantör via egen befintlig IT-infrastruktur och identitetshantering.

Behoven styr referensarkitekturen i en riktning mot

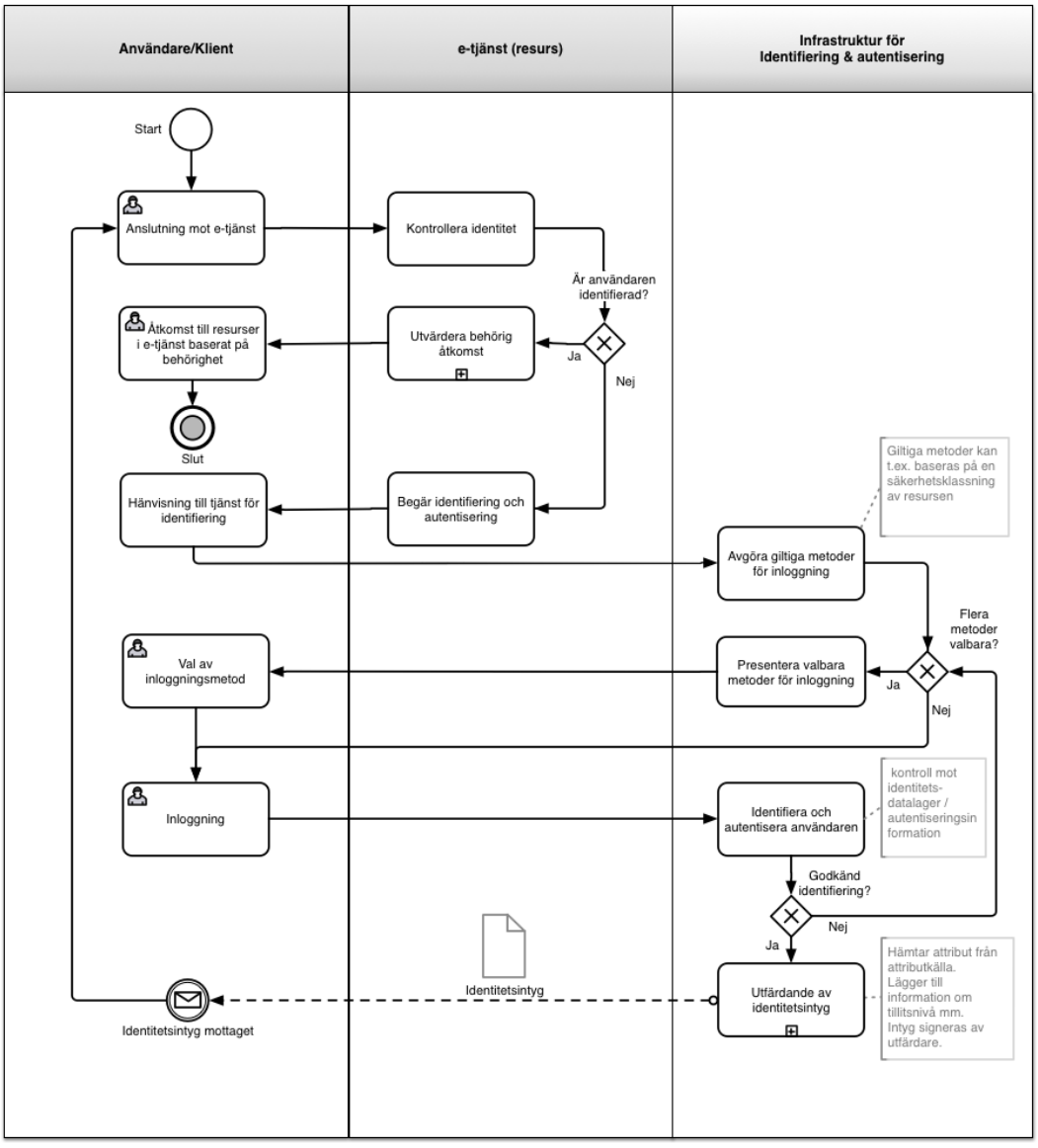
- Standardisering av säkerhetstekniken och gränsytorna mot övrigt IT-stöd.
- Separation av förmågor där respektive delsystem fokuserar på det den är ämnad för, såsom att tydligt skilja på att hantera säker inloggning respektive hantera verksamhetsinformation.
- Plattformsneutrala gemensamma lösningar 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 Identifiering och autentisering av användare

Följande flöde beskriver inloggning i en e-tjänst, där användaren kan vara en medarbetare i en verksamhet, en invånare osv. Flödet stöder singelinloggning, dvs. om 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 av användare*

IT-infrastrukturen behöver kunna tillhandahålla flera möjliga inloggningsmetoder som är anpassade för verksamhetens respektive individens behov och situation, t.ex. mobila arbetssätt (enligt princip IA2).

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

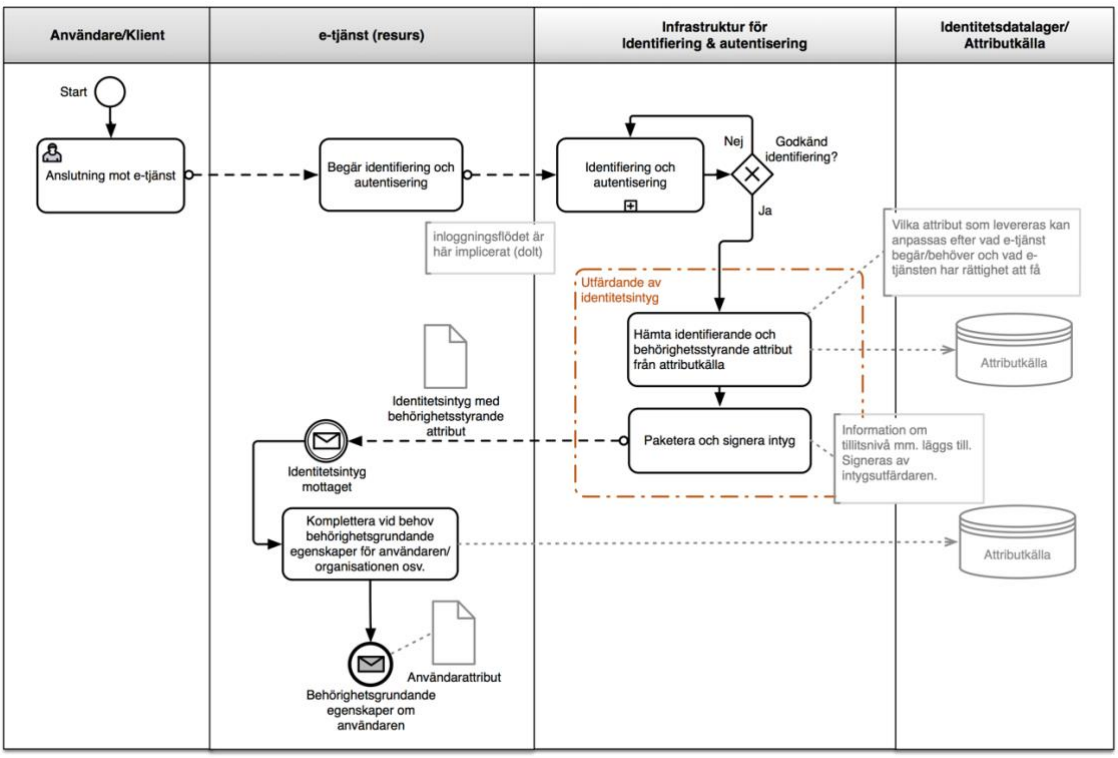
- Identifiering och autentisering av användare (*Legitimeringstjänst*).
- Stöd för olika inloggningsmetoder, eller mer precist autentiseringsmetoder (*Autentiseringstjänster*)
- Utfärdande av identitetsintyg (*Identitetsintygsutfärdare*), vilket skapar en säker men lös teknisk koppling mellan e-tjänsterna 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

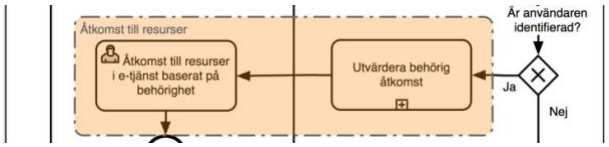
- Identifierande attribut.
- Behörighetsgrundande attribut.
- Uppgift om använd autentiseringsmetods styrka (den tillit som metoden att verifiera användarens identitet har).
- Vem som utfärdat och signerat intyget.

Utgående från identitetsintyget kan e-tjänsten behöva kompletterande uppgifter för att fullt ut kunna avgöra användarens rättigheter till resurser i e-tjänsten, till exempel 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.

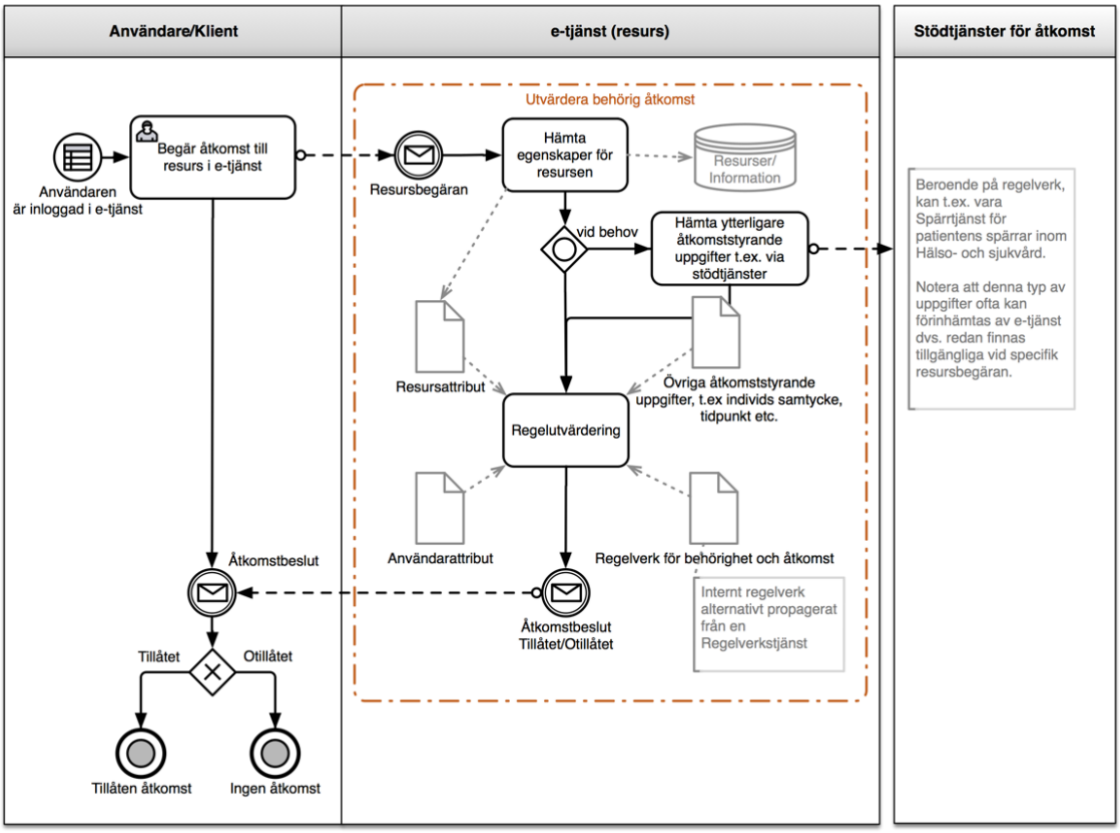
## 4.4 Åtkomst till resurser

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 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, till exempel vem som skapat informationen, informationsägare, begärd åtgärd (läsa, signera, registrera, handlägga ärende etc).
- *Andra åtkomststyrande uppgifter*, exempelvis 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. Ifall e-tjänsten tillhandahåller resurser för privatpersoner, kan kopplingen till rätt individs resurser (informationsägaren) vara det väsentliga i regelutvärderingen.

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 integrationstjänster.

## 4.5 Autentisering och auktorisation av system

I många former av elektroniskt informationsutbyte finns behov att autentisera och auktorisera ingående system. Ibland är även en användare delaktig ur ett identitets- och åtkomstperspektiv, men det kan även avse ren system-till-system-kommunikation (*machine-to-machine*, *m2m*).

Sådana mönster kan till exempel användas för att implementera

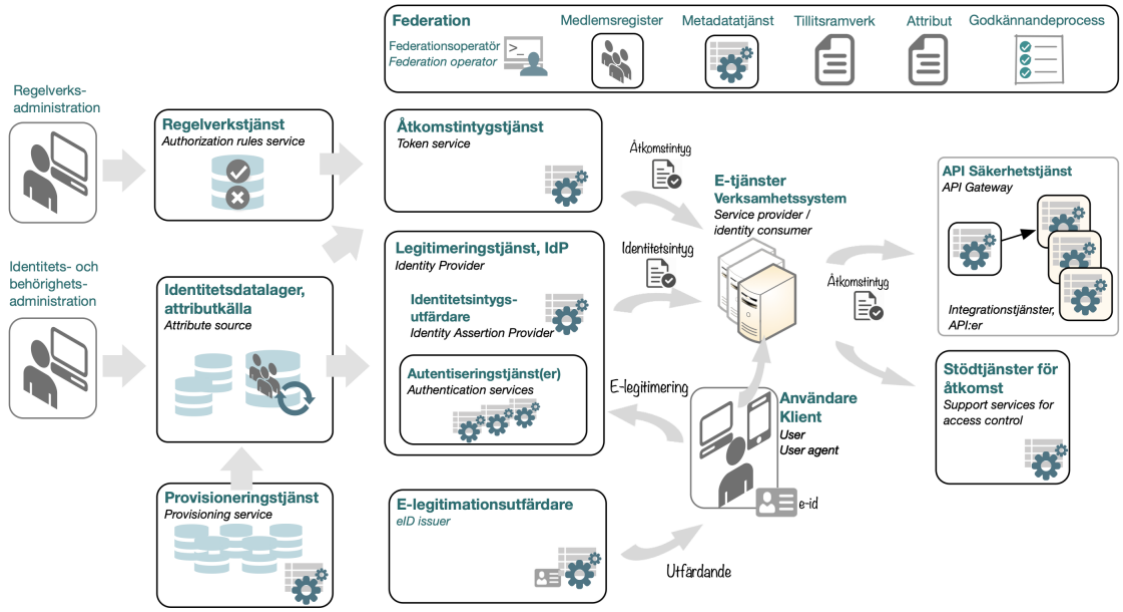
- Säker informationsöverföring mellan system såväl inom som över organisationsgränser.
- Automatiserade processer inom en organisation.
- Sammansatta integrationstjänster där system anropar system som i sin tur anropar system, och det finns behov autentisera och styra åtkomst för systemen i flera led.

# 5 Informationssystemvy

*Informationssystemvyn beskriver en referensarkitektur för hur samverkan och funktion uppstår via tjänster i IT-stödet. Vilka infrastrukturtjänster behöver vi för att realisera 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 här skall tolkas i vid mening och kan vara någon typ av digitalt informationssystem: ett regionalt webbaserat verksamhetssystem, ett kommunalt administrativt system, en mobil app, en nationell e-tjänst för invånare eller dylikt.

### Federerad e-legitimering

E-tjänsten tar hjälp av en eller flera betrodda *Legitimeringstjänster* att säkerställa användarens identitet enligt ett federativt mönster, även kallat *federerad e-legitimering*. Man kan säga att e-tjänsten har ”outsourcat” inloggning, identifiering och autentisering av användaren till legitimeringstjänsten.
Utgående från vald autentiseringsmetod samt begärd tillitsnivå nyttjar legitimeringstjänsten en *Autentiseringstjänst* för att utföra den faktiska användarautentiseringen. Legitimeringstjänsten utfärdar vid lyckat resultat ett *identitetsintyg* till e-tjänsten. E-tjänsten kan sedan med identitetsintyget som grund utvärdera om användaren ska få tillgång till e-tjänsten och bli inloggad.

### Singelinloggning

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

### Underlag för auktorisation

Identitetsintyget 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, till exempel personaladministrationen som sätter grundläggande egenskaper för en anställd medarbetare, till exempel befattning. Andra egenskaper kan tänkas hämtas från externa källor, till exempel uppgift om yrkeslegitimation, folkbokföringsuppgifter osv. 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, till exempel att göra viss uppföljning av verksamheten, hantera ekonomi etc.

### Utfärdande av e-legitimationer

Autentiseringen av användaren kräver att användaren elektroniskt kan bevisa för autentiseringstjänsten vem hen är. För detta utfärdas en s.k. *e-legitimation* till användaren via en *e-legitimationsutfärdare*, på någon form av bärare, till exempel ett smart kort, en säkerhetsdosa, en skyddad del av en mobil enhet eller dylikt. E-legitimationen har unika egenskaper som gör att det går att säkerställa att det är just den elektroniska identiteten som används vid e-legitimeringen.

### Granulär åtkomst till information via integrationstjänster

Referensarkitekturen kan även ge stöd för att ge användare och system granulär och säker åtkomst till information via *integrationstjänster* (API:er), genom samverkan mellan *Åtkomstintygstjänst* och *API Säkerhetstjänst*. Åtkomstintygstjänsten kan utfärda åtkomstintyg avseende åtkomst med visst omfång, som sedan kan användas för att anropa integrationstjänster. Integrationstjänsterna kan överlåta validering av åtkomstintygen till en *API Säkerhetstjänst (API Gateway)* för bättre separation mellan applikationslogik och säkerhetslager. Åtkomsträttigheter kan även *delegeras* från användaren till den e-tjänst eller app som behöver hämta informationsresurser från integrationstjänster å användarens vägnar.

### Regelverkstjänst

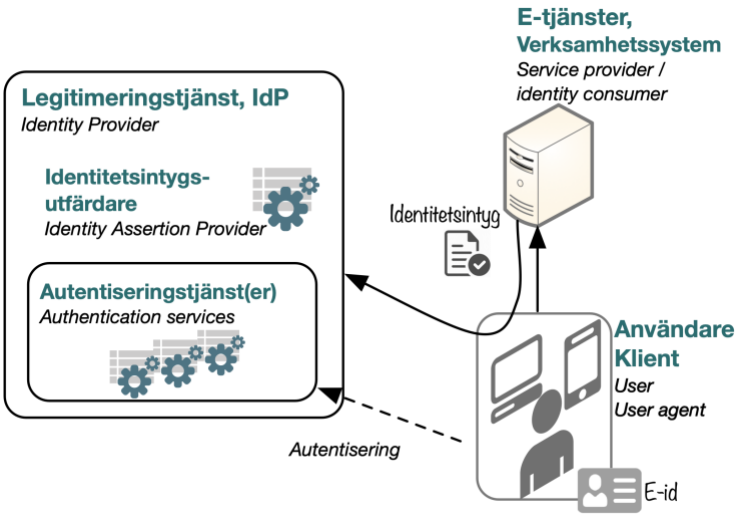
Att ge tillgång till resurser, e-tjänster och information, handlar i grunden om att sätta och tillämpa ett antal regler för åtkomst (*authorization rules*). Regelverket kan ofta vara ”på papper” som sedan implementeras (programmeras) i respektive e-tjänst, integrationstjänst osv.
Om det är många tjänster som ska skyddas, och/eller behovet att styra informationsåtkomsten är fingranulärt, kan ett mer skalbart sätt behövas 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. *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 användaridentiteter.
Federationens grundpelare är medlemmarna *(medlemsregistret)*, säker information om vilka tjänster som är anslutna *(metadatatjänst)*, ett *tillitsramverk* som definierar de krav som ställs på parterna, ett överenskommet innehåll *(attribut),* samt processer för att bli och vara ansluten *(godkännandeprocess)*.

## 5.2 Legitimeringstjänst (IdP)

Referensarkitekturen bygger på en konsolidering av e-legitimering av användaren till en *Legitimeringstjänst* även kallad *IdP* (*Identity Provider*) eller *Identitetsintygstjänst.*
Legitimeringstjänsten identifierar och autentiserar användaren på begäran av e-tjänsten, även kallad *Service Provider (SP),* som agerar ”förlitande part”.
Principen att e-tjänsten överlåter e-legitimeringen till en betrodd tjänst kallas även *federerad e-legitimering*. En legitimeringstjänst kan typiskt utföra autentisering av användare både vid inloggning och vid elektronisk underskrift i e-tjänster.




*Figur 9. Legitimeringstjänst, IdP*

Legitimeringstjänsten kan ses som ”navet” i IT-infrastrukturen för identitet- och åtkomst, där e-tjänster med olika tekniska förutsättningar kan ansluta via standardiserade gränssnitt för att åstadkomma elektronisk legitimering av användare.

En legitimeringstjänst kan stödja ett flertal tekniska protokoll parallellt som kan användas för anslutning av e-tjänster och autentiseringsklienter. För tekniska krav kring protokollval etc., se vidare kap. 6.

Legitimeringstjänsten ansvarar för

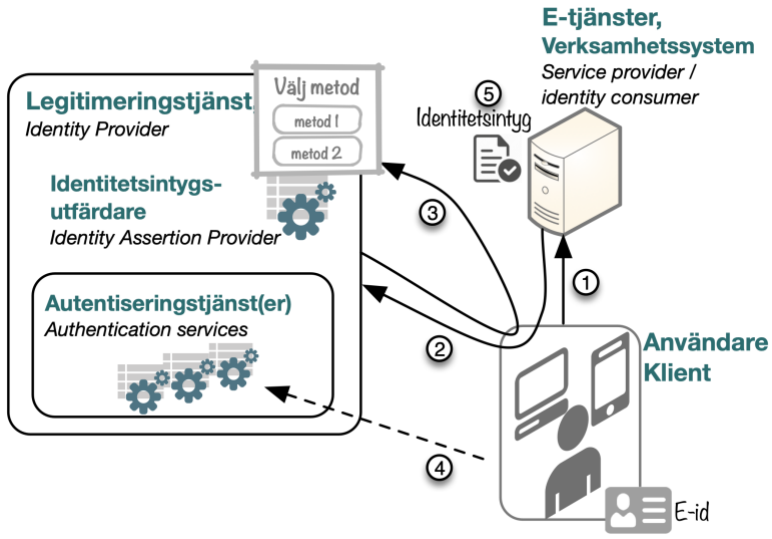
- att hantera användarens val av metod för e-legitimering (val av *autentiseringsmetod*) när flera val är aktuella.
- att säkerställa (verifiera) användarens identitet via en *Autentiseringstjänst*.
- att förmedla den säkerställda användaridentiteten och i förekommande fall tillhörande egenskaper (attribut) till e-tjänsten genom att *utfärda ett identitetsintyg*, dvs. agera i rollen *Identitetsintygsutfärdare*.

Legitimeringstjänsten kan även

- ge möjlighet till singelinloggning (SSO)

I följande avsnitt kommer dessa förmågor att beskrivas var och en. Vi börjar dock med att beskriva ett grundläggande flöde för inloggning i en e-tjänst med stöd av Legitimeringstjänst.

### 5.2.1 Inloggning i e-tjänst



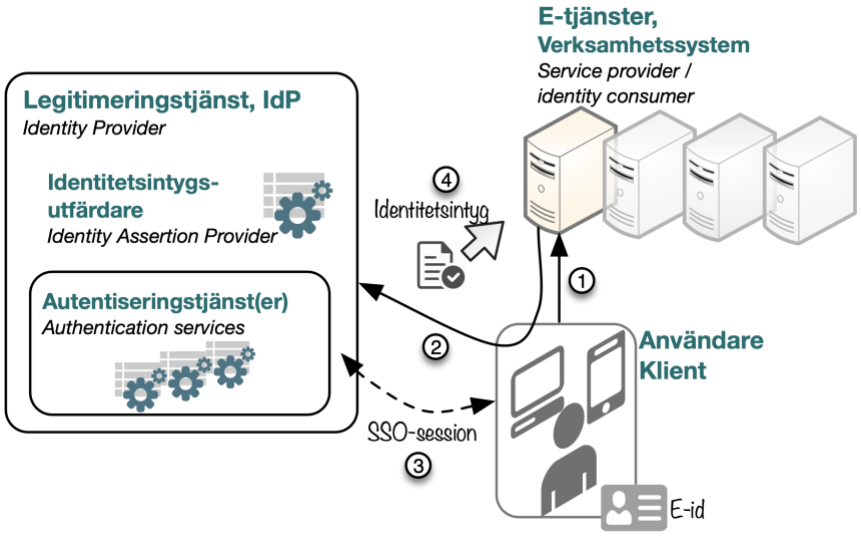

*Figur 10. Grundläggande flöde vid inloggning i e-tjänst*

Ett grundläggande flöde för inloggning till en e-tjänst kan beskrivas enligt följande:

1. Användaren väljer att logga in i en e-tjänst
2. E-tjänsten kräver en autentiserad användare och skickar en autentiseringsbegäran med krav på viss tillitsnivå till *Legitimeringstjänsten*. E-tjänsten förmedlar även vilka användaregenskaper (attribut) som önskas i retur vid lyckad autentisering.
3. *Legitimeringstjänsten* antas här inte ha någon tidigare session för singelinloggning (SSO-session) med denna klient, och styr därför om användaren till val av autentiseringsmetod (om det finns fler att välja mellan).
   Autentiseringsmetoder som motsvarar den tillitsnivå (eller -nivåer) som e-tjänsten begärt presenteras för användaren.[4]
4. Användaren legitimerar sig elektroniskt med vald autentiseringsmetod.
5. *Legitimeringstjänsten* utfärdar vid godkänd autentisering ett *identitetsintyg* med begärda användaregenskaper som returneras till e-tjänsten.[5]
6. E-tjänsten verifierar intygets giltighet, och om användaren är behörig att använda e-tjänsten blir användaren inloggad.

[4] Notera att detta steg kan hoppas över om autentiseringsmetoden redan är given.
[5] Exakt hur detta går till beror på valt protokoll, men vi återkommer till vilka principiella metoder som används.

### 5.2.2 Singelinloggning (SSO)




*Figur 11. Flöde vid singelinloggning - SSO*

Vid singelinloggning (SSO) påverkas flödet på så sätt att användaren inte aktivt behöver e-legitimera sig igen, genom att en SSO-session har etablerats med användarens klient (*user agent*) vid tidigare e-legitimering:

1. Användaren väljer att logga in i en e-tjänst
2. E-tjänsten kräver en autentiserad användare och skickar en autentiseringsbegäran med krav på tillitsnivå till *Legitimeringstjänsten*.
3. *Legitimeringstjänsten* har en giltig *SSO-session* med användarens klient. Ingen ny autentisering avkrävs.
4. *Legitimeringstjänsten* utfärdar ett *identitetsintyg* med begärda användaregenskaper som returneras 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: så länge det finns en giltig SSO-session kan användaren logga in i e-tjänsterna utan upprepad autentisering. Maximal sessionstid för SSO ska kunna sättas utifrån aktuella verksamhetskrav och säkerhetspolicys.

### 5.2.3 Avslutande av SSO-session och tvingande e-legitimering

Legitimeringstjänst som erbjuder singelinloggning (SSO) ska även tillhandahålla en funktion till ansluten e-tjänst som avslutar en användares SSO-session om sådan är etablerad. När SSO-sessionen är avslutad kommer Legitimeringstjänsten tvinga fram en ny e-legitimering om användaren försöker legitimera sig mot samma eller annan e-tjänst igen.

Legitimeringstjänsten ska även erbjuda möjlighet till tvingande e-legitimering (*forced authentication*) för en enskild autentiseringsbegäran. En sådan begäran ska alltid leda till en ny e-legitimering, men ev. etablerad SSO-session ska inte påverkas.

### 5.2.4 Utloggning ur e-tjänst

Viktigt att notera är 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.

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

### 5.2.5 Val av autentiseringsmetod

Legitimeringstjänsten kan eventuellt tillhandahålla flera autentiseringsmetoder samt ett tillhörande användargränssnitt för val av autentiseringsmetod.

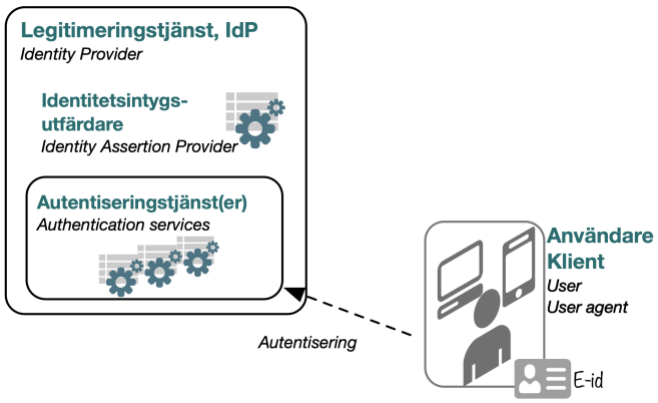

*Figur 12. Legitimeringstjänsten erbjuder användargränssnitt för val av autentiseringsmetod*

Respektive vald autentiseringsmetod kopplar sedan till en *Autentiseringstjänst* som ansvarar för det tekniska steget att faktiskt autentisera användarens identitet. Notera att autentiseringstjänster antingen kan realiseras av Legitimeringstjänsten själv eller utgöra fristående tjänster.

Gränssnittet mot användaren vid e-legitimering kan även hanteras av e-tjänsten själv. Detta förutsätter att Legitimeringstjänsten erbjuder respektive autentiseringsmetod som separata ändpunkter (*endpoints*) som e-tjänsten kan anropa.

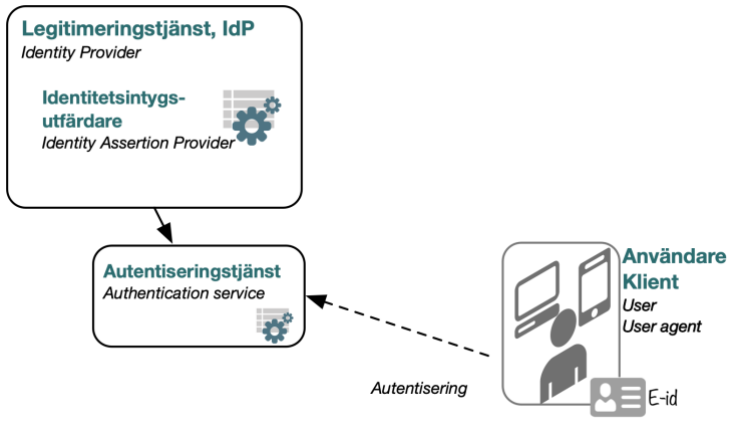
### 5.2.6 Autentiseringstjänst

En *Autentiseringstjänst* ansvarar för att utgående från en viss autentiseringsmetod autentisera användaren med en viss autentiseringsteknik, dvs. säkerställa användarens identitet.



*Figur 13. Autentiseringstjänst(er) inom ramen för en legitimeringstjänst*

En autentiseringstjänst kan antingen realiseras som en del av Legitimeringstjänsten som ovan eller utgöras av en fristående tjänst som i exemplet i följande bild.




*Figur 14. Fristående autentiseringstjänst*

### 5.2.7 Grundläggande principer för autentisering

I praktiken kan autentiseringssteget omfatta både att *identifiera* användaren dvs. bestämma en användaridentitet (till exempel personnummer eller ett tjänste-id) 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

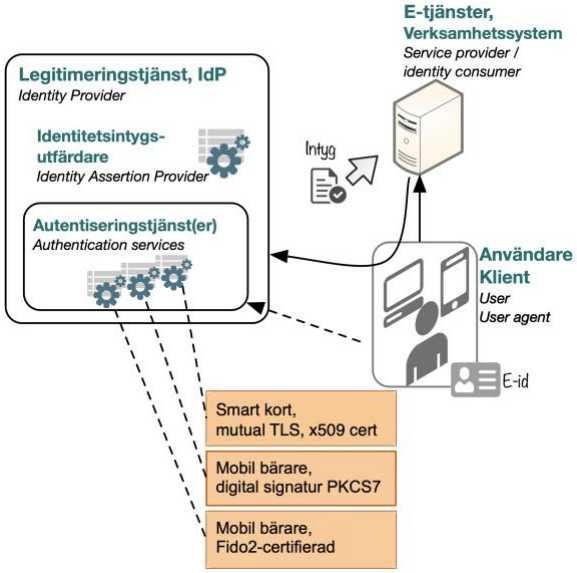
- Något (just denna) användaren vet,
- Något (just denna) användaren har
- Något (just denna) användaren är, dvs. någon egenskap hos användaren, även kallad *biometrisk* faktor.

Autentiseringen kan baseras på en eller flera av sådana faktorer, till exempel enbart ett hemligt lösenord (*enfaktorautentisering*), både ett fingeravtryck och innehav av en personlig bärare för e-legitimation (*tvåfaktorautentisering*) osv.

### 5.2.8 Stöd för multipla autentiseringsmetoder

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




*Figur 15. Multipla autentiseringsmetoder kan "pluggas in" inom en Legitimeringstjänst*

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

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

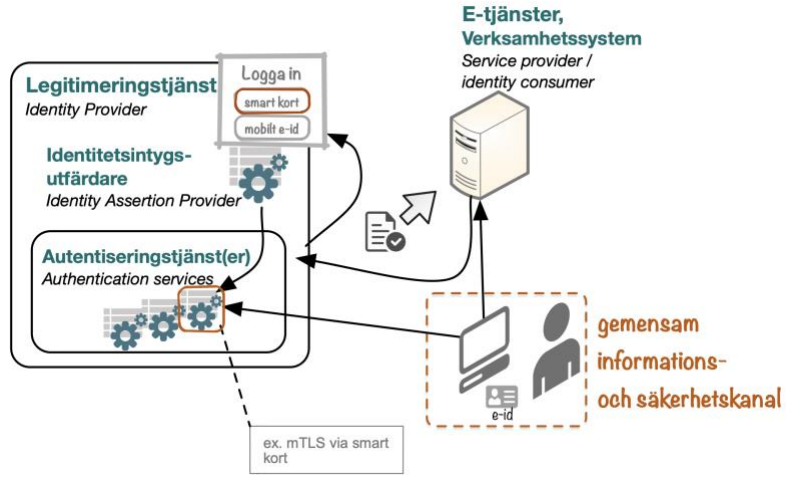
Den nya autentiseringsmetoden kan dessutom läggas till utan att e-tjänsternas anslutning till legitimeringstjänsterna behöver förändras.

### 5.2.9 Autentisering in-band och out-of-band

Även om nya anpassade autentiseringsmetoder kan anslutas i IT-infrastrukturen, kvarstår ett problem: om autentiseringslösningen kräver viss mjuk- och hårdvara, till exempel av säkerhetsskäl, behöver användarnas alla klienter också utrustas med denna mjuk- och hårdvara. Till exempel 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?

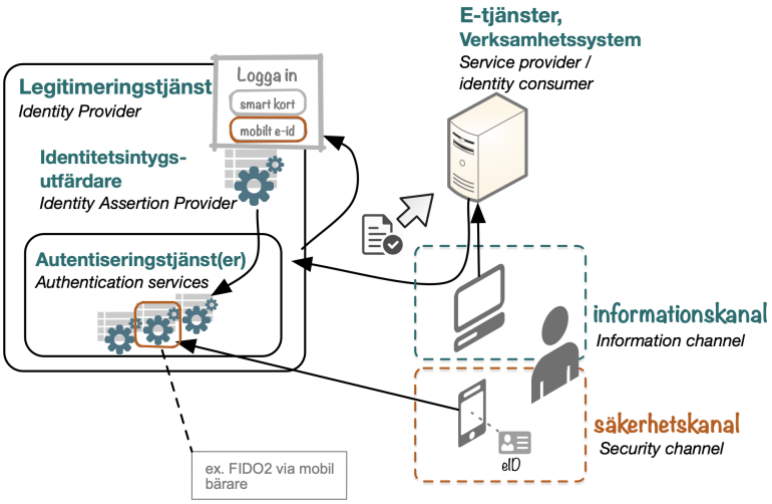
Problemet ligger egentligen i att samma kanal alltid används för både informationsåtkomsten och säkerhetslösningen, vilket även kallas *in-band-authentication*.




*Figur 16. 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*.[6]




*Figur 17. 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-legitimation (säkerhetskanalen)
4. Legitimeringstjänsten (IT-infrastruktur för e-legitimering)

[6] Exempel på *out-of-band authentication* är Mobilt BankID, Mobilt SITHS och Freja eID.

Denna lösa koppling medger bland annat att mixa och anpassa utrustning för var och en dessa fyra delkomponenter; till exempel 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.

### 5.2.10 Autentisering med biometrisk teknik

Biometrisk teknik kan förenkla för användaren om hen slipper komma ihåg koder/lösenord, och i stället utnyttja till exempel 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. Biometriska data ska dock inte spridas i onödan till tjänster i nätverket, utan hålls nära användaren själv, helst endast inom användarens personliga bärare för e-legitimationen (enligt principen #IA10).

### 5.2.11 Tillhandahållande av användarattribut

Legitimeringstjänsten ansvarar för att utifrån en autentiseringsbegäran från e-tjänst leverera efterfrågade användarattribut i identitetsintyget, baserat på data i betrodd attributkälla (se vidare kap. 5.4. angående identitetsdatalager)

Legitimeringstjänsten bör i möjligaste mån tillhandahålla användarattributen utan krav på användarinteraktion så att användarupplevelsen inte störs av onödiga dialoger och val. Detta är normalt okomplicerat när det gäller attribut som entydigt vid varje tillfälle kan fastställas utifrån aktuell användare, t.ex. personliga egenskaper som personens namn och personnummer.

Det finns dock fall där e-tjänsten behöver ett specifikt attributvärde utav flera möjliga värden kopplade till samma användare. Det kan t.ex. avse vilket uppdrag (av flera) och för vilken organisation (av flera) som användaren för tillfället agerar inom e-tjänsten, vilket kan tänkas styra vilken åtkomst användaren får och även hur åtkomsten dokumenteras/loggas.

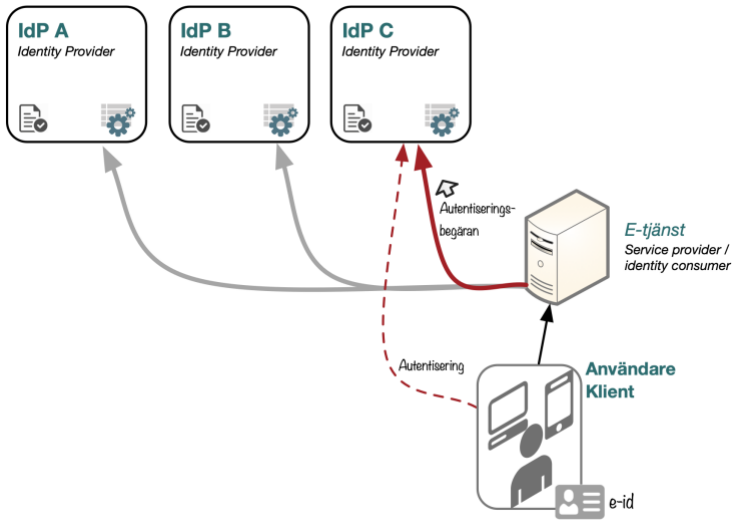
För att hantera leverans av den typen av användarattribut till e-tjänst kan ett av följande alternativ tillämpas:

1. Legitimeringstjänsten returnerar utan användarinteraktion en lista av alla värden för attribut som är multivärda, t.ex. användarens alla medarbetaruppdrag (om flera förekommer). E-tjänsten får vid behov ansvara för ev. val av vilket värde som ska gälla vid respektive tillfälle inom e-tjänsten.
2. Legitimeringstjänsten presenterar ett användarval där användaren får välja aktuellt värde av ett multivärt attribut där fler alternativa värden finns. Enbart valt värde returneras i identitetsintyget.
3. E-tjänsten hämtar multivärda attribut direkt från attributkällan, dvs. begär inte dessa attribut i identitetsintyget. E-tjänsten får vid behov ansvara för ev. val av vilket värde som ska gälla vid respektive tillfälle inom e-tjänsten.

Legitimeringstjänster kan välja att erbjuda alternativ 1 eller 2 eller båda, men det är som nämnts rekommenderat att om möjligt undvika användarinteraktion i legitimeringstjänsterna för tillhandahållande av attribut.

### 5.2.12 Samverkan med flera legitimeringstjänster

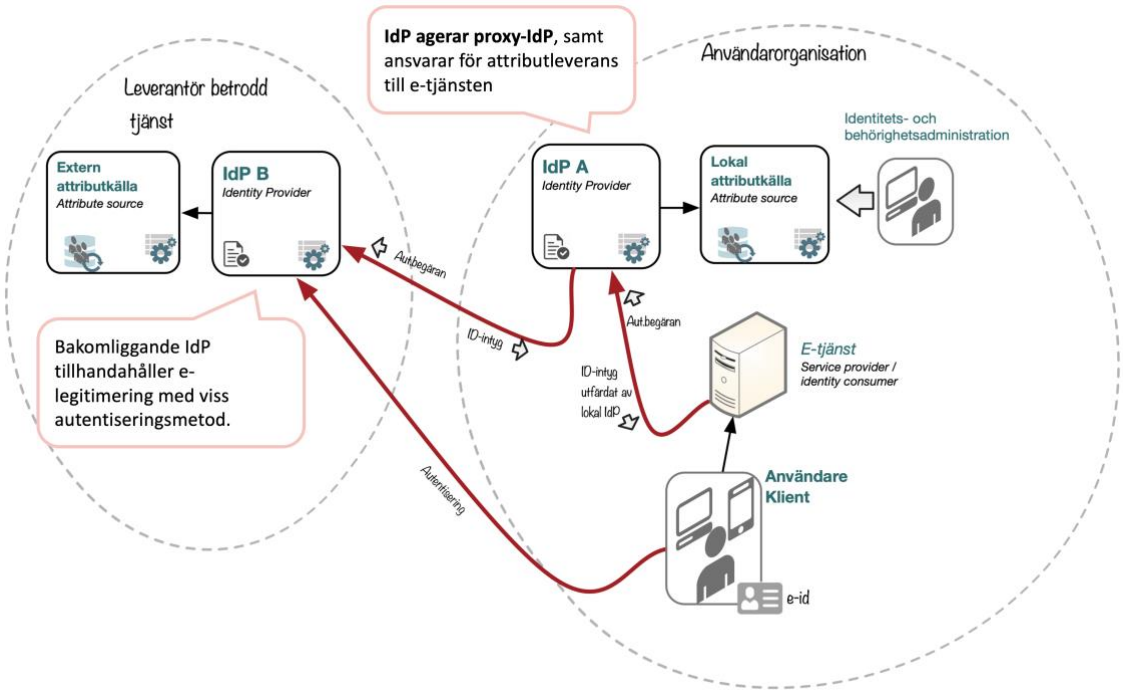
En e-tjänst kan etablera samverkan med flera legitimeringstjänster (IdP:er). På detta sätt kan ges stöd för flera olika typer av e-legitimationer i e-tjänsten i de fall utfärdare av e-legitimation tillhandahåller separata legitimeringstjänster. Mönstret kan även tillämpas i federativa scenarion, till exempel för att tillåta extern organisation att använda sin egen IdP vid inloggning i en e-tjänst.




*Figur 18. En e-tjänst är direkt ansluten till flera IdP:er. Not: autentiseringstjänsterna visas inte explicit för att förenkla bilden.*

En potentiell nackdel med mönstret är att det inte stödjer singelinloggning (SSO) mellan olika legitimeringstjänster. Man kan även tappa en del av möjligheten till en sammanhållen och enhetlig användarupplevelse om legitimeringstjänsterna ”tar över” användardialogen.

Ett annat sätt att samverka med flera legitimeringstjänster är att en IdP agerar proxy (*proxy IdP*) mot annan IdP. I bilden nedan är e-tjänsten ansluten till IdP A som i sin tur är ansluten till IdP B.




*Figur 19. En IdP agerar proxy mot annan IdP.*

Tekniskt sett agerar IdP A som en *Service Provider* (*SP*) i förhållande till IdP B, precis som e-tjänsten gör gentemot IdP A, så samma tekniska protokoll kan tillämpas i båda fallen.

Syftet med detta mönster är även här att ge tillgång till flera legitimeringstjänster och autentiseringsmetoder i e-tjänsten, men i detta fall behålls möjligheten till SSO, och det kan vara enklare att realisera en mer sammanhållen användarupplevelse.

Att tänka på vid användning av IdP som proxy:

- Den IdP som e-tjänsten är ansluten till ansvarar alltid för utfärdande av identitetsintyg och dess attributinnehåll till e-tjänsten.
- Avväg noga lämpligaste källa (lokal eller extern) för de av e-tjänsten begärda attribut med hänsyn tagen till vilken källa som är mest auktoritativ (master) för attributet.
- Undvik om möjligt att begära attribut av den bakomliggande IdP-tjänsten som kan leda till användarinteraktioner, för en bättre sammanhållen användarupplevelse. Ofta kan det räcka med ett attribut som unikt identifierar användaren från den externa attributkällan.

De båda mönstren ovan (direktansluten respektive proxy) kan även kombineras. Ett exempel på användning av detta är att i svenska e-tjänster tillföra möjlighet till e-legitimering med utländska e-id enligt eIDAS-förordningen [eIDAS]; e-tjänsten ansluts till en särskild IdP som agerar gemensam proxy-IdP i Sverige för uthopp till andra länders legitimeringstjänster.

### 5.2.13 Principer för att välja legitimeringstjänst

Om en e-tjänst är ansluten till flera legitimeringstjänster behöver avgöras vilken som ska användas vid en specifik e-legitimering.
Valet av legitimeringstjänst (även kallat *anvisning*) kan realiseras med hjälp av olika arkitekturella mönster:

- E-tjänsten realiserar en egen funktion där användaren kan välja legitimeringstjänst.
- E-tjänsten nyttjar en *Anvisningstjänst* som realiserar en gemensam funktion för att välja legitimeringstjänst.
- Inloggningslänkar till e-tjänsten kompletteras med förvald legitimeringstjänst.

Alla ovan alternativ ger stöd för referensarkitekturens principiella krav kring utfärdande och förmedling av identitetsintyg enligt kap. 5.3. Det är även möjligt att använda flera av mönstren i kombination.
I följande avsnitt beskrivs dessa mönster översiktligt och deras respektive för- och nackdelar.

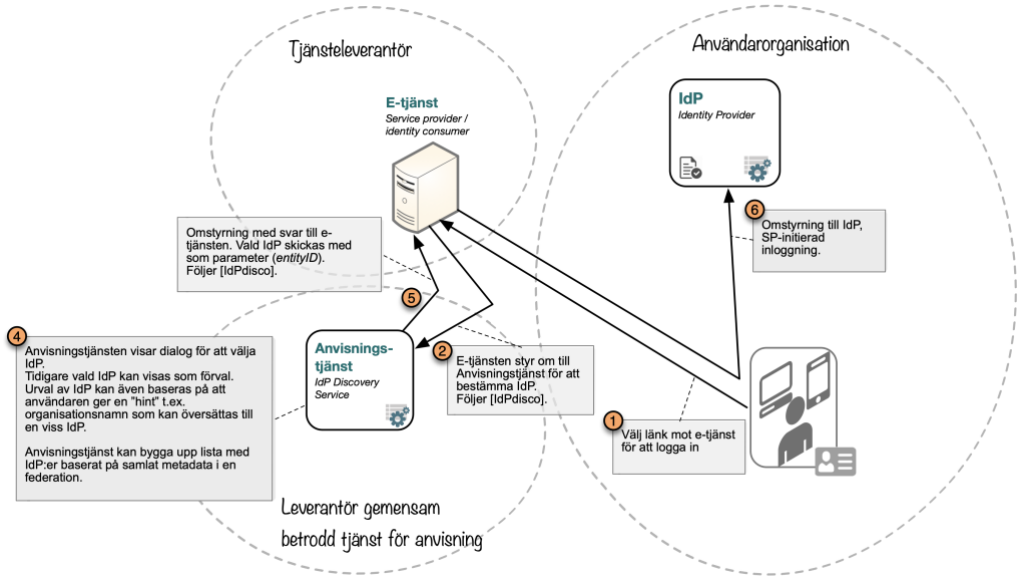
#### 5.2.13.1 E-tjänsten realiserar val av legitimeringstjänst

I detta fall realiserar e-tjänsten en valdialog där användaren kan välja från tillgängliga legitimeringstjänster. Vad som presenteras i valdialogen kan baseras på metadata för de anslutna legitimeringstjänsterna. Inom en federation kan den samlade metadatat i federationen med fördel användas. E-tjänsten kan även använda något användaren ger som input till att översätta till en viss legitimeringstjänst (till exempel baserat på användarens organisatoriska tillhörighet).

En fördel med mönstret är att det är relativt enkelt att implementera och att få beroenden skapas.
En nackdel kan vara att mönstret inte skalar särskilt bra för att hantera ett stort antal e-tjänster. Det blir även ett extra återkommande moment för användare att ange valet; e-tjänsten bör därför ha funktion för att minnas användarens tidigare val och använda det som förvalt värde så långt det är möjligt.

#### 5.2.13.2 Anvisningstjänst

En annan möjlighet är att använda en *Anvisningstjänst* för val av legitimeringstjänst, vilken då flera e-tjänster kan nyttja. Även här kan valdialogen baseras på metadata för anslutna legitimeringstjänster, men eftersom tjänsten ska kunna användas av flera e-tjänster fungerar mönstret bättre inom en federation med samlade metadata.




*Figur 20. Val av IdP via en anvisningstjänst*

Fördelar med mönstret är att det går effektivt att realisera funktionen för ett stort antal e-tjänster, och det finns standardprotokoll[7] som reglerar utbytet med en Anvisningstjänst.

En nackdel är att det kan vara svårt att åstadkomma en bra användarupplevelse med risk att användaren får ett extra återkommande moment som kan vara störande.
Anvisningstjänst bör ha funktion för att minnas användarens tidigare val och använda det som förvalt värde så långt det är möjligt.
Lösningen tenderar att bli en kompromiss med begränsad möjlighet att anpassa till verksamhetens behov, då den gemensamma tjänsten typiskt ska fungera för många olika organisationer och e-tjänster inom en federation.

#### 5.2.13.3 Inloggningslänkar med förvald legitimeringstjänst

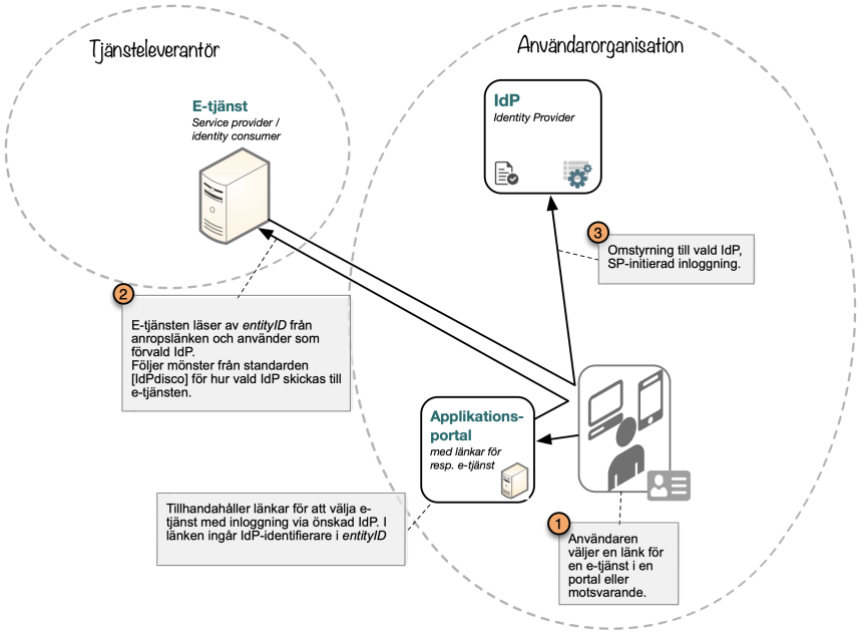
Detta mönster går ut på att tillhandahålla länkar för att nå e-tjänsterna som anpassas till användarorganisationens behov av val av legitimeringstjänst.

Länkarna kompletteras med en parameter innehållande en unik identifierare för den legitimeringstjänst som ska vara förvald. När e-tjänsten får ett anrop på länken kan identifieraren läsas av och användas som förvald legitimeringstjänst.

En organisation kan bygga en lista av länkar baserat på metadata från den legitimeringstjänst som organisationen normalt använder.

Länkarna kan tillhandahållas på valfritt sätt, till exempel via en applikationsportal eller liknande.

[7] *Identity Provider Discovery Service Protocol and Profile [IdPDisco]*, se “Teknisk vy – tekniska regelverk”




*Figur 21. Inloggningslänkar till e-tjänster med förvald legitimeringstjänst publicerade i en applikationsportal*

En fördel med mönstret är att användaren inte explicit behöver ange/välja vilken legitimeringstjänst som ska användas, vilket kan ge en bättre användarupplevelse än de andra alternativa mönstren.
Mönstret kan nyttja tillämpliga delar av standardprotokoll[8] för att kommunicera vald legitimeringstjänst.

Mönstret passar bäst att tillämpa inom en organisation eller mellan samverkande organisationer som använder samma legitimeringstjänst. Däremot passar det mindre bra för att publicera publika inloggningslänkar för andra organisationer att använda; här kan i stället något av de andra mönstren tillämpas.

### 5.2.14 Specifika krav

- Legitimeringstjänst ska erbjuda e-legitimering av användare på begäran från anslutna e-tjänster.
- E-tjänsten ansvarar för att begära e-legitimering för användare via en eller flera Legitimeringstjänster. E-tjänster ska inte integrera direkt med autentiseringstjänster.
- Legitimeringstjänst ska stödja att e-tjänsten anger krav på tillitsnivå för begärd e-legitimering. Den av e-tjänsten begärda tillitsnivån (eller någon av tillitsnivåerna som begärs om flera) ska gälla för utförd autentisering, och annars ska returneras att autentisering inte kunde utföras.
- Vid godkänd e-legitimering ska Legitimeringstjänst returnera ett signerat *identitetsintyg* till e-tjänsten som begärde e-legitimering. Legitimeringstjänst ska även returnera

[8] *Identity Provider Discovery Service Protocol and Profile [IdPDisco]*, se "Teknisk vy – tekniska regelverk"

information om utförd autentisering, s.k. *autentiseringskontext* inklusive den *tillitsnivå* som den använda autentiseringsmetoden motsvarar.

- Legitimeringstjänst bör i möjligaste mån tillhandahålla användarattributen utan krav på användarinteraktion så att användarupplevelsen inte störs av extra dialoger/val.
- Vid användning av IdP som proxy bör attributinnehållet i identitetsintyg returnerade av bakomliggande IdP minimeras till de identifierande attribut som är nödvändiga för att säkerställa att det är rätt användare.
- Legitimeringstjänst ansvarar för att delegera autentisering till autentiseringstjänster. Legitimeringstjänst ska stödja att lägga till (och ta bort) autentiseringstjänster och tillhörande autentiseringsmetoder.
- Legitimeringstjänst som erbjuder flera autentiseringsmetoder ska tillhandahålla användargränssnitt för val av autentiseringsmetod, men ska även möjliggöra att respektive autentiseringsmetod anropas separat från e-tjänsten utan behov av val av metod.
- IT-infrastrukturen för identitet och åtkomst 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.
- Legitimeringstjänst bör tillhandahålla funktion för singelinloggning (SSO). Maximal sessionstid för SSO ska kunna sättas utifrån aktuella verksamhetskrav och säkerhetspolicys.
- Legitimeringstjänst som tillhandahåller SSO-funktion, ska också tillhandahålla en möjlighet för e-tjänsten att signalera utloggning ur SSO-sessionen, varvid SSO-sessionen för aktuell användare ska avslutas. Avslutad SSO-session ska medföra att ny e-legitimering krävs vid användarens nästa försök att logga in i en ansluten e-tjänst.
  Not: Legitimeringstjänst kan även välja att erbjuda s.k. singelutloggning (SLO), men detta är inget krav enligt referensarkitekturen.
- Legitimeringstjänst ska erbjuda möjlighet till tvingande e-legitimering (*forced authentication*) för en enskild autentiseringsbegäran, vilket ska medföra att ev. SSO-session då inte används.
- 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 en legitimeringstjänst, ska e-tjänsten också anropa legitimeringstjänsten för att begära utloggning ur SSO-sessionen.
- E-tjänsten bör ha funktion för automatisk utloggning vid inaktivitet, vilken ska kunna anpassas efter aktuella behov samt informationssäkerhetskrav.

## 5.3 Utfärdande och förmedling av intyg

Intyg för identitet och åtkomst kan i det generella fallet omfatta två olika typer:

- **Identitetsintyg**: intygar en aktörs säkerställda identitet och tillhörande egenskaper (attribut).
- **Åtkomstintyg**: intygar att en aktör erhållit en rättighet att nå en viss resurs. Denna typ av intyg *kan* (men måste inte) även innehålla identifierande information om aktören som fått rättigheten.

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

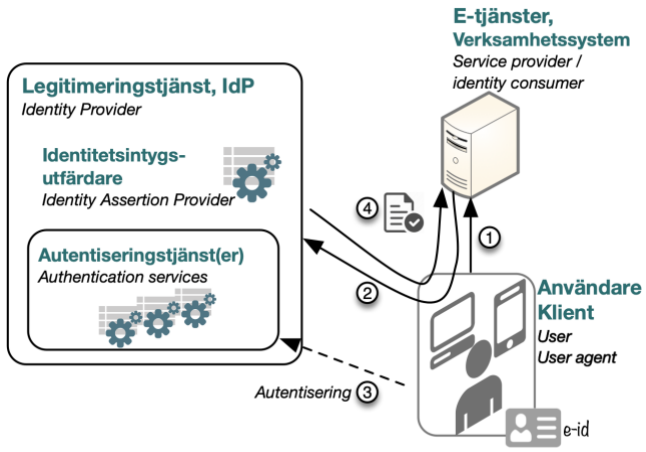
### 5.3.1 Princip för förmedling av intyg

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*"[9].
- **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*"[10]. Principen passar bra när man inte kan lita på klientsidan av e-tjänsten att hantera intyget säkert.

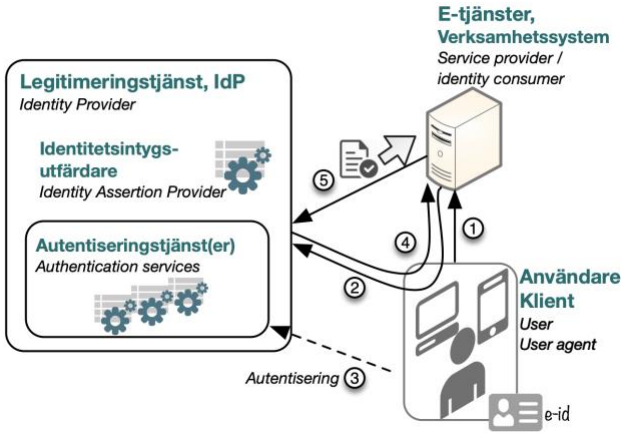
I bilderna nedan illustreras principerna när en användare loggar in och blir autentiserad och ett intyg erhålls. Principen gäller både för identitets- och åtkomstintyg.

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




*Figur 22. 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.



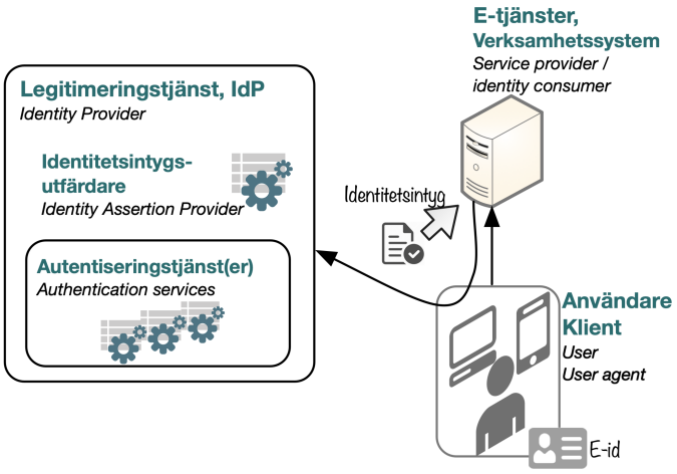

*Figur 23. Flöde för förmedling av intyg via referens ("back channel")*

"*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.

### 5.3.2 Ombedda eller oombedda intyg?

***Ombedda intyg***

E-tjänsten (Service Provider, SP) begär normalt explicit att få ett intyg av en legitimeringstjänst (IdP) genom att skicka en autentiseringsbegäran och erhålla intyget i retur. Denna princip kallas *ombedda intyg* (*solicited assertions*), se följande figur.




*Figur 24. Identitetsintyg som ombett intyg*

Ombedda intyg ska vara förstahandsvalet och stöds av de tekniska protokollsviter som är rekommenderade inom referensarkitekturen. Uppgiftsminimering kan tillämpas avseende personuppgifter eftersom inte fler uppgifter behöver överföras än vad e-tjänsten begär. Vidare kan e-tjänsten direkt styra den tillitsnivå för e-legitimeringen som krävs för åtkomst till (delar av) e-tjänsten.

### *Oombedda intyg*

Alternativt kan användaren först utföra e-legitimering hos legitimeringstjänsten, varefter intyget skickas till e-tjänsten som ett svar utan en föregående begäran, s.k. *oombedda intyg* (*unsolicited assertions*). För att användaren ska komma till önskad e-tjänst efter e-legitimeringen måste speciella länkar utformas som leder till önskad legitimeringstjänst, men som också innehåller information om till vilken e-tjänst legitimeringstjänsten ska styra om användaren till efter godkänd e-legitimering.

Ett syfte med *oombedda intyg* kan vara att en organisation önskar ha kontroll över vilken legitimeringstjänst som ska användas för medarbetare i organisationen, i de fall en e-tjänst har stöd för flera legitimeringstjänster.

*Oombedda intyg* har dock flera nackdelar och rekommenderas därför inte:

- Det saknas stöd för *oombedda intyg* i några i referensarkitekturens centrala rekommenderade tekniska protokoll[11].
- Det saknas standardisering för utformning och behandling av de länkar som behöver hanteras av legitimeringstjänster för att styra om användaren till e-tjänsten.
- Oombedda intyg stödjer inte s.k. djuplänkning till e-tjänsten, dvs. att användaren kan länka till valfri del av e-tjänsten.
- Uppgiftsminimering avseende personuppgifter blir svårt att tillämpa eftersom e-tjänsten inte kan styra vilka uppgifter som överförs utifrån behovet.

[11] OpenID Connect saknar stöd för oombedda intyg

- E-tjänsten kan inte anpassa den tillitsnivå för e-legitimeringen som krävs för åtkomst till (delar av) e-tjänsten. Det går till exempel inte att tillämpa en högre tillitsnivå för vissa funktioner inom en e-tjänst (*step-up authentication*).

### 5.3.3 Specifika krav

- En Legitimeringstjänst som agerar utfärdare av identitetsintyg ska stödja båda principerna för förmedling av intyg: *intyg direkt* samt *intyg via referens*.
- En tjänst som agerar utfärdare av intyg för identitet och/eller åtkomst ska sätta krav på autentisering av den begärande aktören, typiskt med krav på tillitsnivå. Autentiseringskraven kan antingen gälla en användare, ett system eller både och beroende på vilket interaktionsmönster som används.
- 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 (transportkryptering). Se [RIV-Kryptering] för specifika krav.
- Principen *ombedda intyg* (*solicited assertions*) bör användas, dvs. att e-tjänsten begär att få intyg av legitimeringstjänst.

Vad gäller innehållet i intyg för identitet och åtkomst 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 dock några principiella egenskaper som intygen behöver förhålla sig till och därmed blir krav på en utfärdare av intyg:

- Intyget ska ha en explicit specificerad giltighetstid.
- Intyget ska vara digitalt signerat av utfärdaren så att dess avsändare kan säkerställas av alla mottagare.
- Intyget ska kunna innehålla *avsedd mottagare* (*audience*). Avsedd mottagare av intyget är den/de tjänst(er) som har rätt att använda (“konsumera”) intyget.
- Utöver obligatoriska standardattribut gäller principen att e-tjänsten styr vilka attribut som begärs och potentiellt erhålls i intyget. Principen kring uppgiftsminimering avseende personuppgifter eller annan känslig information ska tillämpas.

## 5.4 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. När identitetsintyg ställs ut till privatpersoner kan t.ex. folkbokföringsregistret vara aktuell som attributkälla.

Respektive organisation går i god för att uppgifterna i attributkällan är kvalitetssäkrade, så att de kan utgöra grund för utgivning av digital identitetsinformation, 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), till exempel 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 visst 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, till exempel ”Rapportera ekonomiskt underlag”, ”Administrera personals anställningsuppgifter” osv.

Kategorierna ovan är viktiga att vara medveten om då det påverkar hur, varför och hur länge en användare får en viss egenskap kopplad till sig, till exempel att attributet följer av att en medarbetare för närvarande har ett visst uppdrag/ansvarsområde.

Attributkällor kan även tillhandahålla information om organisationsidentiteter och hur dessa förhåller sig till varandra (organisationsstruktur) där så tillämpligt.

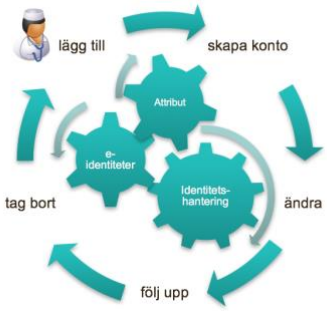
Flera olika vyer (perspektiv) av dessa identitetsstrukturer kan behöva tillhandahållas, till exempel personvy, uppdragsvy, anställningsvy osv, beroende på det regelverk som behöver stödjas.

Attributkällor kan även användas för att tillhandahålla egenskaper för system, för att till exempel stödja attributbaserad behörighetsutvärdering även vid ren system-system-kommunikation.

## 5.5 Provisioneringstjänst

Provisionering i generella termer betyder att ”tillhandahålla”. Inom referensarkitekturen för Identitet och åtkomst avser vi specifikt *provisionering av identitetsdata*, dvs. tillhandahålla kvalitetssäkrade 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.

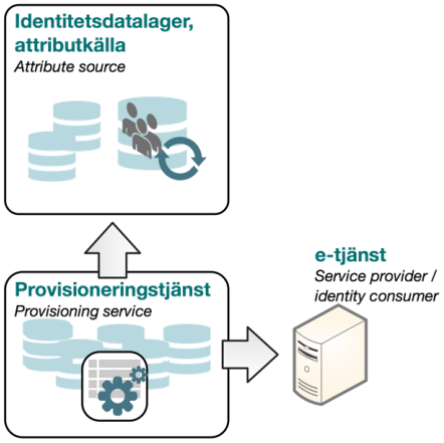



*Figur 25. Förändring av identitetsdata är en ständigt pågående process*

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 kvalitetssäkrade identitetsdata.
- Provisionera identitetsdata från identitetsdatalager till en e-tjänst, t.ex. för att automatiskt skapa och ta bort användarprofiler i e-tjänsten, dvs. distribution av kvalitetssäkrade identitetsdata.

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




*Figur 26. Provisioneringstjänst – tillhandahålla kvalitetssäkrade 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, till exempel i e-tjänster.

Notera 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 integrationstjänster (API:er), till exempel ett API för behörighetsdata för medarbetare.

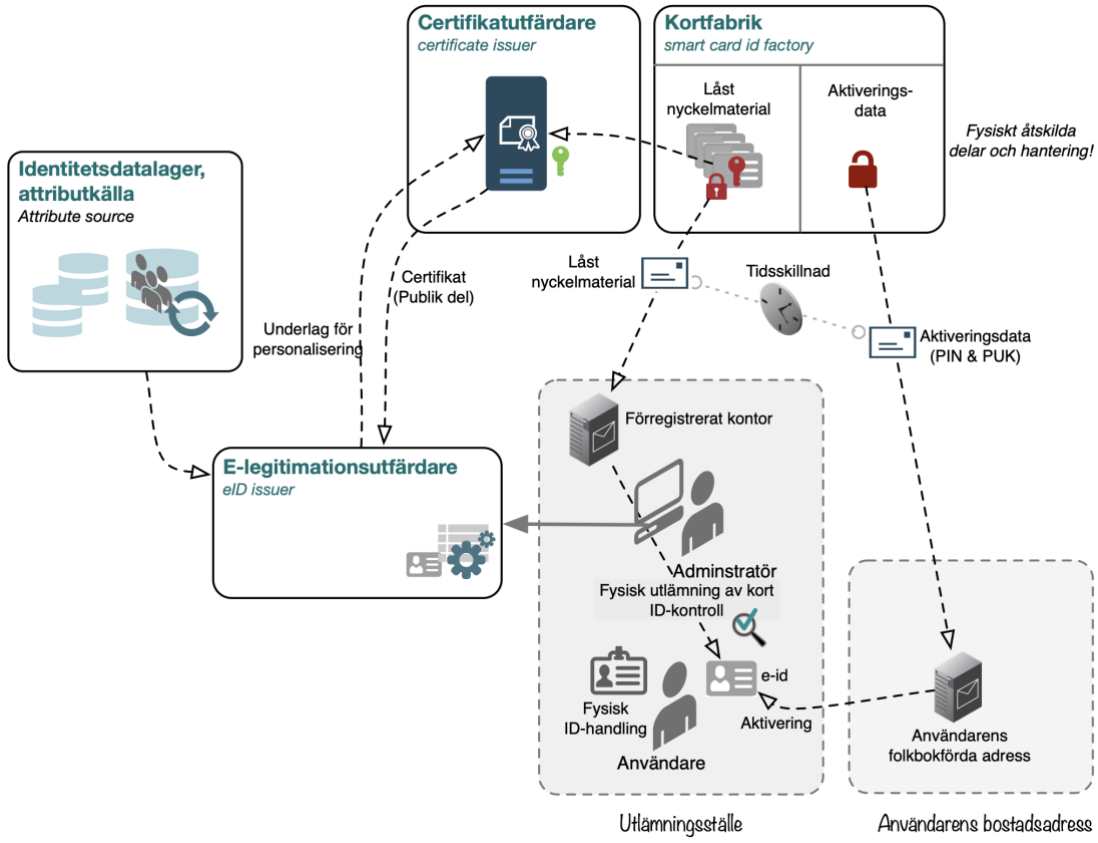
## 5.6 E-legitimationsutfärdare

*Utfärdande av e-legitimation* (även kallad *e-id*) innebär att en person erhåller en e-legitimation för att använda som hens elektroniska identitetshandling i kommunikationen med digitala system. E-legitimationen förvaras på en bärare, till exempel ett smart kort med skyddat chip eller en skyddad del på en mobil enhet.

För att e-legitimationen 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 personen själv känner till, till exempel en säkerhetskod, eller egenskap hos personen, till exempel en biometrisk egenskap.

### 5.6.1 Utfärdande av e-legitimation med administrativ process

Utfärdandet av en e-legitimation kan innebära en administrativ process där den tilltänkta mottagaren identifierar sig med en godkänd fysisk id-handling, och en administratör effektuerar själva utfärdandet. För att nå en hög tillitsnivå bör leverans av bäraren för e-legitimationen med *nyckelmaterial* respektive *aktiveringsdatat* ske i separata fysiska kanaler, till exempel personlig utlämning kombinerat med postutskick till folkbokföringsadress.



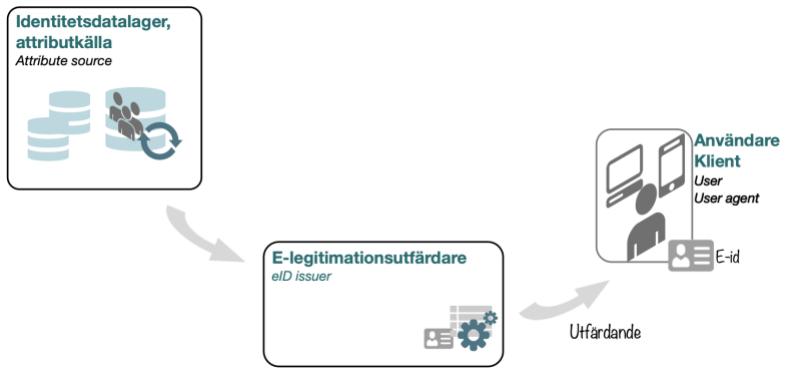

*Figur 27. Utfärdande av e-legitimation med administrativ process. Ex. med utfärdande till hårt certifikat på smart kort via en kortfabrik. Separerade kanaler för nyckelmaterial och aktiveringsdatat. Fysisk legitimering vid utlämning.*

I Figur 27 har använts ett exempel med utfärdande till hårt certifikat på ett smart kort. Nyckelmaterial och aktiveringsdatat 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 aktiveringsdatat (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.

### 5.6.2 Utfärdande av e-legitimation via självservice

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

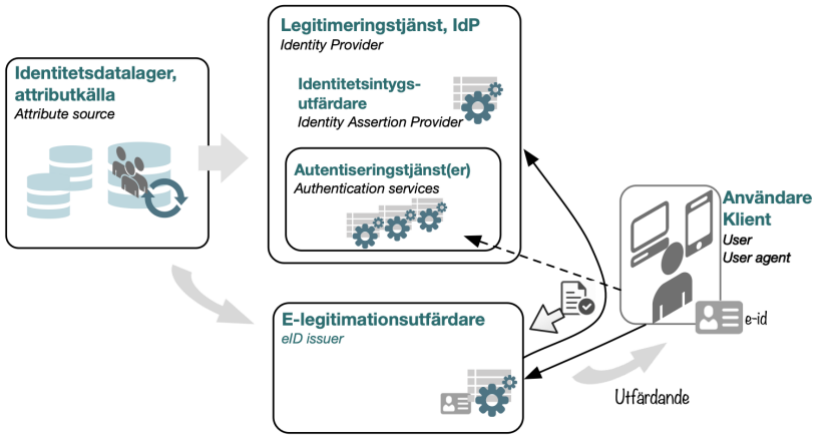



*Figur 28. Utfärdande av e-legitimation via självservice.*

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

### 5.6.3 Utfärdande av e-legitimation med ärvd legitimering

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



*Figur 29. Utfärdande av e-legitimation via självservice med 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-legitimationen, kan ärvas vid utfärdandet av en ny e-legitimation, med samma eller annan teknik och typ av bärare.

Via ärvd legitimering kan alltså såväl samma som annan typ av e-legitimation utfärdas[12], till exempel

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

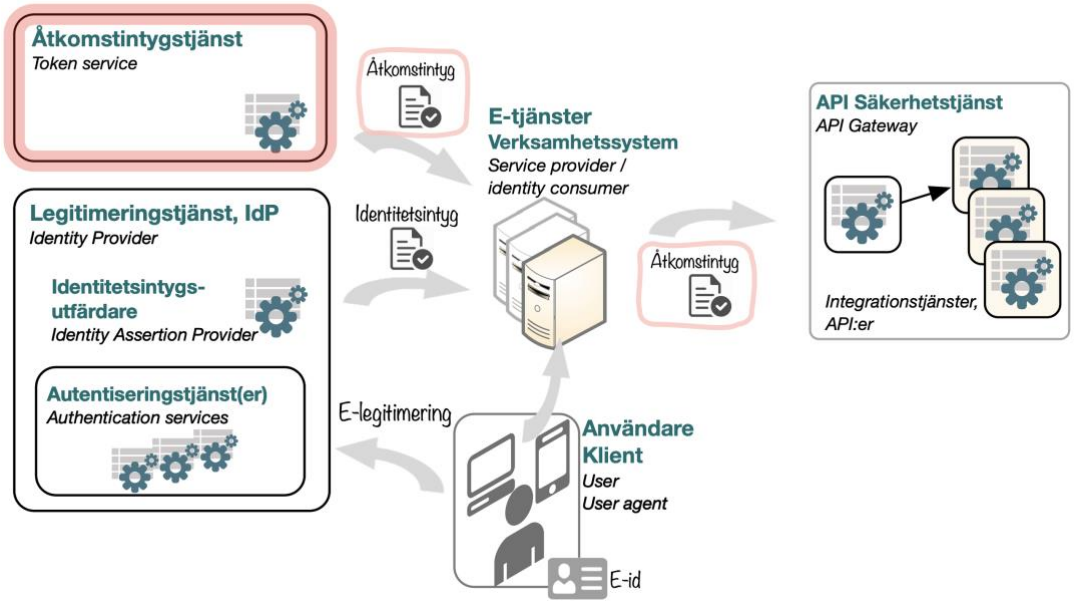
Processen kan göras digital och via självservice, vilket ger stora skalfördelar.

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

## 5.7 Åtkomstintygstjänst

### 5.7.1 Utfärdande av åtkomstintyg

*Åtkomstintygstjänst*, även kallad *Tokentjänst* (*Token service* och även förekommande *Authorization server*) utfärdar digitala *åtkomstintyg* som kan användas för att få åtkomst till en viss resurs. Resursen nås normalt via en integrationstjänst (oftast ett nätverksbaserat API), vilken kan vara en intern tjänst inom ramen för e-tjänsten i ett sammanhållet system, eller en till e-tjänsten extern tjänst.

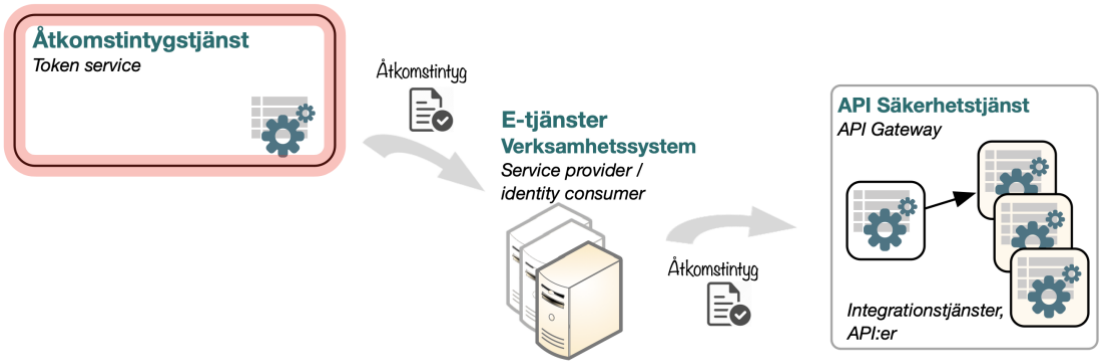



[12] Notera att det kan finnas avtalsmässiga begränsningar kring ärvd legitimering.

*Figur 30. Utfärdande och användning av åtkomstintyg*

Åtkomstintygstjänst agerar ”åtkomstbeslutspunkt” (*Policy Decision Point, PDP)*, och det system som ser till att åtkomstbeslutet verkställs (till exempel en integrationstjänst) agerar på motsvarande sätt *Policy Enforcement Point (PEP).*

Åtkomstintyg utfärdas baserat på autentiserad aktör och begärd resurs, där aktör kan vara en användare eller ett system. Vid ren system-till-systemkommunikation utfärdas åtkomstintyg baserat på rättigheter som systemet självt har tilldelats, vilket kan tillämpas för till exempel automatiserade processer.

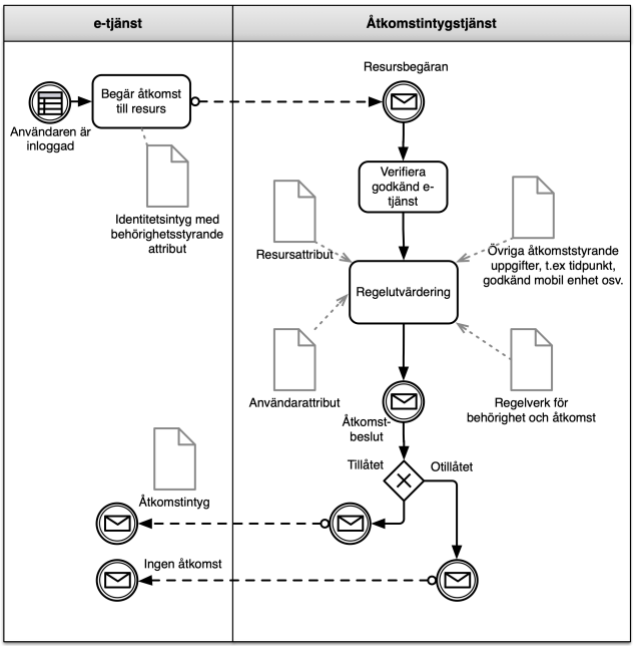



*Figur 31. Utfärdande och användning av åtkomstintyg - enbart systemaktörer*

### 5.7.2 Åtkomsthantering med stöd av åtkomstintyg

Genom samverkan med och förlitande till Åtkomstintygstjänst samt i förekommande fall Legitimeringstjänst, kan åtkomsten till resurser som integrationstjänster tillhandahåller hanteras genom ett centralt definierat åtkomstregelverk, för att säkerställa att rätt aktör (person och/eller system) 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 32. Regelutvärdering av åtkomst till informationsresurser förlagd till IT-infrastrukturen. E-tjänsten erhåller ett åtkomstintyg om åtkomsten är tillåten.*

För att även stödja åtkomst för användare från andra organisationer, kan federation nyttjas där andra parters legitimeringstjänster ansluts, se vidare kap. 5.11.

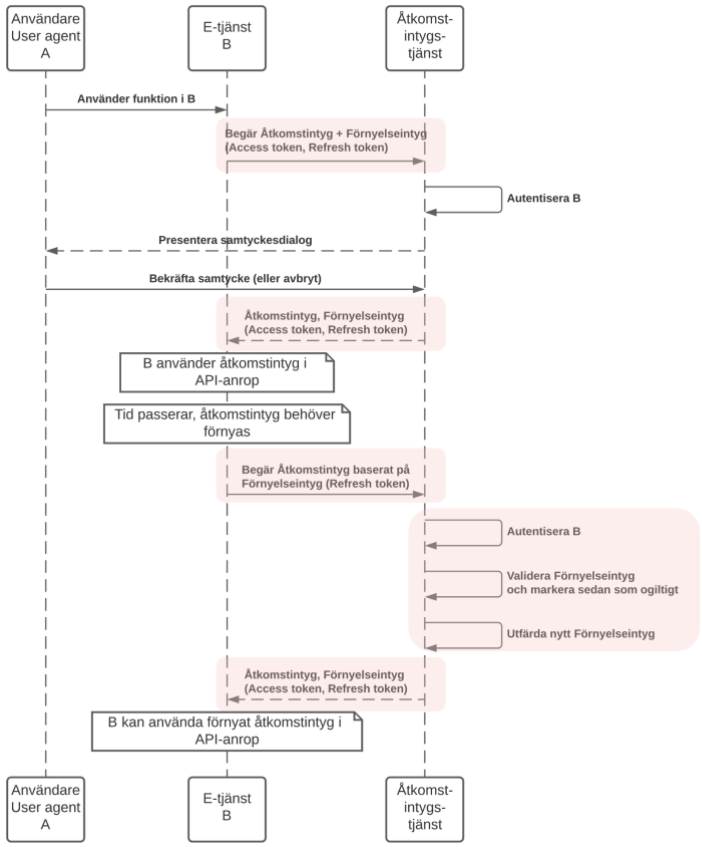
Åtkomstintygstjänst stödjer även flöden med delegering av åtkomsträttigheter. Ett typiskt fall är när en användare delegerar sina åtkomsträttigheter gällande en resurs till en e-tjänst, så att e-tjänsten kan få åtkomst till resursen. Delegering kan även tillämpas för ren system-till-systemkommunikation.

Flöden med enbart systemaktörer beskrivs först i kommande avsnitt, då flöden som även inbegriper användare delvis bygger vidare på samma interaktionsmönster.

### 5.7.3 Förnyelse av åtkomstintyg

Giltighetstiden för åtkomstintyg sätts i regel relativt kort, både för att minska dess exponering, och ge möjlighet att stänga av en åtkomst på kort varsel. För inte behöva upprepa processen med användarautentisering och utvärdering av åtkomsträttigheter allt för ofta, kan Åtkomstintygstjänsten på begäran även utfärda ett *förnyelseintyg* (*Refresh token*) tillsammans med åtkomstintyget.

Förnyelseintyg används endast i kommunikationen med den betrodda Åtkomstintygstjänsten för att erhålla ett nytt åtkomstintyg, dvs. förnyelseintyget skickas aldrig med vid anropen till andra system. Vidare krävs alltid ny autentisering av det system som använder förnyelseintyget mot Åtkomstintygstjänsten. Normalt förbrukas förnyelseintyget när det används för att minska dess attackyta, och Åtkomstintygstjänsten kan samtidigt utfärda ett nytt förnyelseintyg till det autentiserade systemet.




*Figur 33. Utfärdande av förnyelseintyg (Refresh token) samt förnyelse av åtkomstintyg.*

Även förnyelseintyget har en giltighetstid, vilken kan anpassas till aktuella verksamhetskrav (till exempel till längden av ett arbetspass).

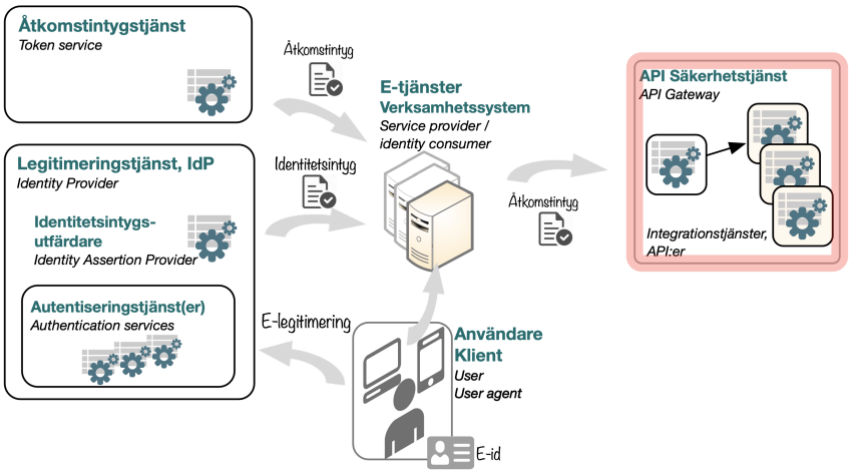
### 5.7.4 Specifika krav

- Åtkomstintygstjänst ska erbjuda utfärdande av digitala *åtkomstintyg* som kan användas för att få åtkomst till resurser, typiskt tillhandahållna via integrationstjänster. Åtkomstintygstjänst ska i samband med utfärdandet kunna agera ”åtkomstbeslutspunkt” (*Policy Decision Point, PDP)*.
- För utfärdande av åtkomstintyg krävs minst en autentiserad aktör, där aktör kan vara en användare eller ett system.
- När s.k. publika klienter[13] (*public clients*) begär åtkomstintyg, ska extra tekniska skydd tillämpas för att skydda mot risken att *intygsreferensen* fångas upp av obehörig, eftersom klienten i detta fall inte kan säkert autentiseras mot Åtkomstintygstjänsten. För anvisning vilka tekniska protokoll som bör implementeras, se kap. 6.
- Åtkomstintygstjänst bör även kunna utfärda förnyelseintyg till autentiserade system. Förnyelseintyg bör vara av typen ”engångs” dvs. de förbrukas omedelbart vid användning.

[13] Klienter som inte säkert kan autentiseras mot Åtkomstintygstjänsten, exempelvis en nativ app på desktop eller mobil.

## 5.8 API Säkerhetstjänst

Det är oftast inte optimalt att låta varje integrationstjänst hantera säkerhetslagret för verifiering av åtkomstintyg och auktorisation. Därför definierar referensarkitekturen en *API Säkerhetstjänst* (även benämnd *API Gateway*) vars uppgift är att realisera säkerhetslagret för de integrationstjänster som behöver hanteras, typiskt inom en organisation. *API Säkerhetstjänst* kan ansvara för både autentisering av anropande system och kontroll av åtkomstintygets giltighet.




*Figur 34. API Säkerhetstjänst agerar gemensamt säkerhetslager för skydd av flera integrationstjänster (API:er)*

## 5.9 Autentisering och auktorisation av system

Nedan avsnitt beskriver principiella flöden tillämpliga vid system-till-system-kommunikation och hur autentisering och auktorisation av ingående system kan hanteras. För rekommenderade tekniska protokoll för dessa flöden se anvisningarna i kap. 6.

### 5.9.1 Registrering av systemidentiteter

En förutsättning för ett säkert informationsutbyte mellan system är att systemen är säkert identifierade och att tillit kan etableras till systemen. Detta förutsätter i sin tur att systemen har genomgått en registreringsprocess (*on-boarding*) och erhållit en systemidentitet som andra parter/system kan förhålla sig till. Registreringen kan ske direkt mellan de parter som ska kommunicera, eller hos en federationsoperatör (tredje part) för att skapa tillit till systemidentiteten för alla som litar på federationen. Det behövs även rutiner för att vid behov avregistrera system och tilliten till dem (*off-boarding*).

Registrering av en systemidentitet kan ske på många olika sätt. Referensarkitekturen omfattar dock enbart metoder som baseras på asymmetriska nyckelpar för att möjliggöra god skalbarhet, stöd för standardiserad säkerhetsteknik samt en hög tillitsnivå då det hemliga nyckelmaterialet aldrig behöver kommuniceras till andra parter[14]. I samtliga fall förutsätts även att systemet är en s.k. ”konfidentiell klient” dvs. har möjlighet att förvara det hemliga nyckelmaterialet på ett säkert sätt (*confidential client*).

Metoderna kan delas in i följande kategorier:

- ”Öppen PKI”
  Systemet erhåller ett certifikat från en s.k. *öppen* PKI, varvid här menas att flera olika certifikatutfärdare kan användas så länge utfärdaren uppfyller alla krav som ställs för att etablera tilliten i fråga. Metoden används typiskt när ett stort antal parter/användare ska kunna kommunicera säkert med ett stort antal parter/system, och där parterna inte i förväg har möjlighet att explicit etablera tillit, till exempel vid utfärdande av certifikat till publika webbservrar.
  Metoden passar sämre när säkerhetskraven är höga och behov finns att styra det exakta regelverket för registreringsprocessen för att uppnå önskad tillit. Detta eftersom processen blir beroende av olika policys, rutiner och ev. svagheter hos de olika certifikatutfärdarna. Oftast får man anpassa sig till en allmänt vedertagen nivå, och många gånger förlitar sig systemen på leverantörers s.k. *trustlists* för godkända certifikatutfärdare. Metoden kräver även kontroller mot utfärdarens revokeringstjänst.
  Vid system-till-system-kommunikation kombineras normalt metoden med att registrera en unik del av certifikatet, ett attribut, den publika nyckeln eller hela certifikatet (s.k. *pinning*). På så sätt kan säkerheten höjas, men samtidigt blir administrationen mer betungande och beroendet till certifikatutfärdarna kvarstår.

- ”Sluten PKI”
  Systemet erhåller ett certifikat från en s.k. *sluten* PKI, varvid här menas att använd certifikatutfärdare används dedikerat till att utfärda särskilda certifikat för att auktorisera

[14] Det är vanligt förekommande att registrera system med en systemidentifierare samt en hemlig kod (lösenord) som delas med den part som ska förlita sig på systemidentiteten. Metoden avrådes dock inom denna referensarkitektur pga. bristande skalbarhet, avsaknad av federativt stöd och svårigheter att på ett säkert sätt påvisa vilken aktör som faktiskt autentiserades.

system inom en viss specifik tillämpning/domän.
En fördel med metoden är att den förlitande parten/federationen får full kontroll över registreringsprocessen, men en relativt stor nackdel är att de anslutande parterna blir tvungna att hantera olika certifikat mot olika tjänster, vilket kan resultera i svårigheter att implementera tekniken i parternas system. Även denna metod kräver kontroller mot utfärdarens revokeringstjänst.
Metoden kan på samma sätt som för öppen PKI kombineras med s.k. *pinning* mot certifikatet eller delar av.

- ”Publik nyckel-registrering”
  Systemet registreras med sin publika nyckel i kombination med en systemidentifierare. Denna metod innebär således alltid s.k. *pinning* mot den publika nyckeln. Ofta förpackas den publika nyckeln i ett certifikat signerat av systemet självt, för att knyta nyckeln till systemet i fråga i ett standardiserat format.
  Metoden har flera fördelar: den skalar mycket bra – från enskilda bilaterala utbyten till större federationer, samtidigt som de förlitande parterna (ev. via federation) kan ha full kontroll över registreringsprocessen för såväl on- som off-boarding av systemen.
  De anslutande parterna behöver vidare endast hantera en publik nyckel/ett certifikat för säker kommunikation med många olika tjänster, vilket underlättar den praktiska implementeringen.

### 5.9.2 Interaktionsmönster för system-system-kommunikation

Referensarkitekturen omfattar två grundläggande interaktionsmönster vid system-till-system-kommunikation, som också kan kombineras för att möta mer komplexa integrationsbehov:

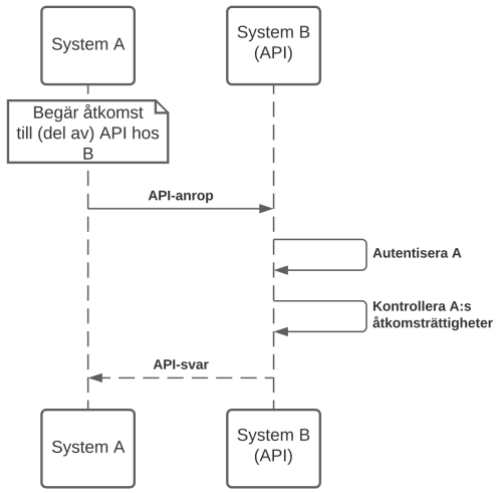
- **System-till-system**.
  Ett system A anropar ett annat system B, där systemet A behöver autentiseras och auktoriseras för anropet i fråga.

- **System-till-system med delegering** (*delegation*).
  Ett system A anropar ett annat system B, där system B i sin tur anropar system C på uppdrag av (*on behalf of*) och med delegerade rättigheter från A, för att kunna leverera ett svar tillbaka till A. I detta fall behöver både A och B autentiseras och auktoriseras för de respektive anropen.

Systemen i dessa interaktionsmönster kan tillhöra samma organisation eller olika organisationer. I det senare fallet kan tillämpas bilateralt förlitande mellan organisationerna, alternativt nyttjas federation för bättre skalbarhet, där en federationsoperatör tillhandahåller en process för registrering av system kopplad till ett tillitsramverk.

### 5.9.3 System-till-system

I sin mest grundläggande form av system-till-systemkommunikation anropar ett system A (klient) en integrationstjänst (API) hos ett annat system B (server).



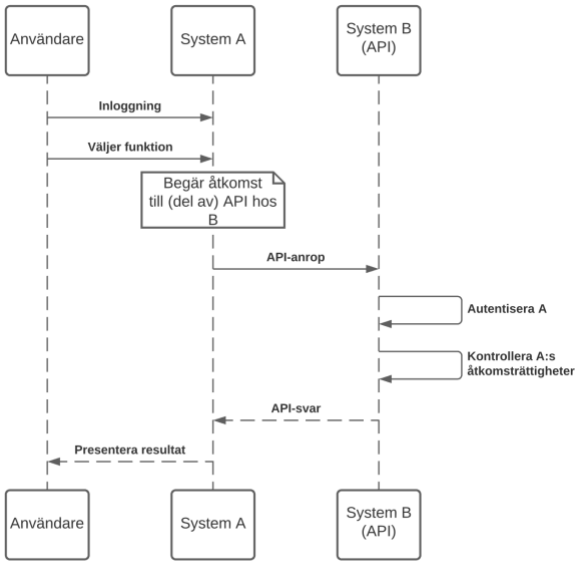

*Figur 35. Grundläggande mönster för system-system-kommunikation (fråga-svar-interaktion)*

I detta fall ansvarar serversystemet för autentisering och auktorisation av varje enskilt anrop. För rekommenderade protokoll för autentisering av system se kap. 6.5.5. Serversystemet måste vidare hantera förlitande till de systemidentiteter som ska hanteras.

Interaktionsmönstret är relativt enkelt att implementera men skalar sämre med många parter inblandade avseende hantering av tillit till och autentisering av system samt åtkomstregelverk kopplat till nya verksamhetskrav.
Detta kan delvis åtgärdas genom att lägga till en *API Säkerhetstjänst* (*API Gateway*, kap. 5.8) framför som avlastar serversystemen från implementationen av säkerhetslagret, men i större systemlandskap med många parter kvarstår att administrationen ofta blir betungande och svår att överblicka.

En mer skalbar hantering av tillit till och autentisering av system kan åstadkommas genom att tillämpa federationsprinciperna i kap. 5.11, där federationen fungerar som en tredje part för tillit (ett ”tillitsankare”) där registrering av systemidentiteterna sker.

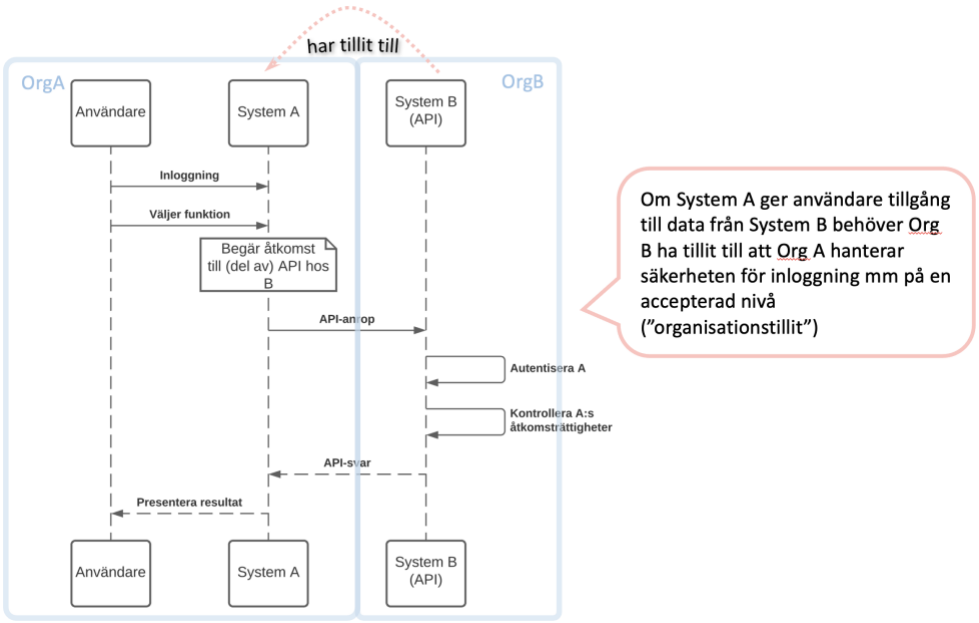
Notera att System A kan också vara en e-tjänst dvs. erbjuder funktionalitet till användare enligt följande bild.




*Figur 36. System-system-kommunikation, e-tjänst till API.*

Interaktionsmönstret mellan A och B ur ett IAM-perspektiv är dock här detsamma som ovan; ifall API:et hos B kräver uppgifter om aktuell användare, behöver A skicka med dessa uppgifter som attribut i API-anropet till B, alltså som en del av nyttolasten.

Tillhör systemen olika organisationer förutsätter mönstret en tillit till att för A ansvarig organisation hanterar säkerheten avseende användarautentisering, spårbarhet osv. på en för B accepterad nivå. Detta mönster refereras ibland som ”organisationstillit”, beskrivet schematiskt i följande bild.

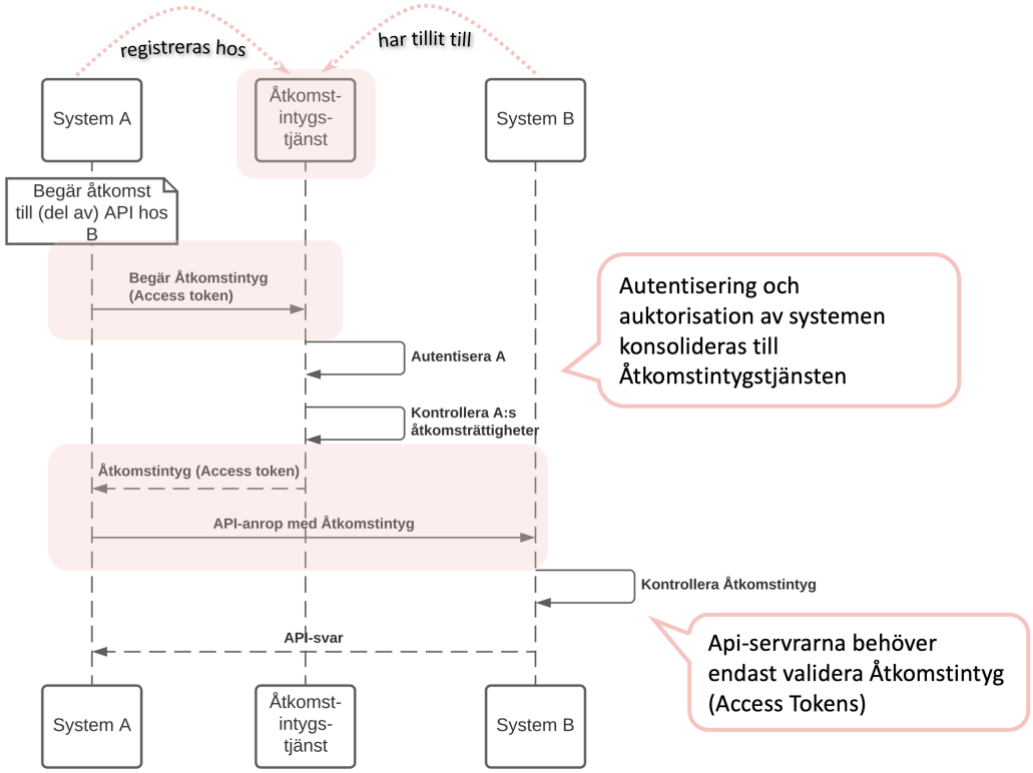



*Figur 37. System-system-kommunikation med s.k. organisationstillit*

Som nämnts ovan behöver varje system som erbjuder ett API enligt detta grundläggande mönster hantera auktorisation av alla anrop, dvs. en kontroll av behörig åtkomst för anropande system. En mer skalbar och effektiv hantering av åtkomst kan åstadkommas genom att addera konceptet *åtkomstintyg*, se följande kapitel.

### 5.9.4 System-till-system – med stöd av åtkomstintyg

För att uppnå hög skalbarhet och mer flexibel hantering av autentisering och auktorisation kan *Åtkomstintygstjänst* nyttjas även för ren system-system-kommunikation.

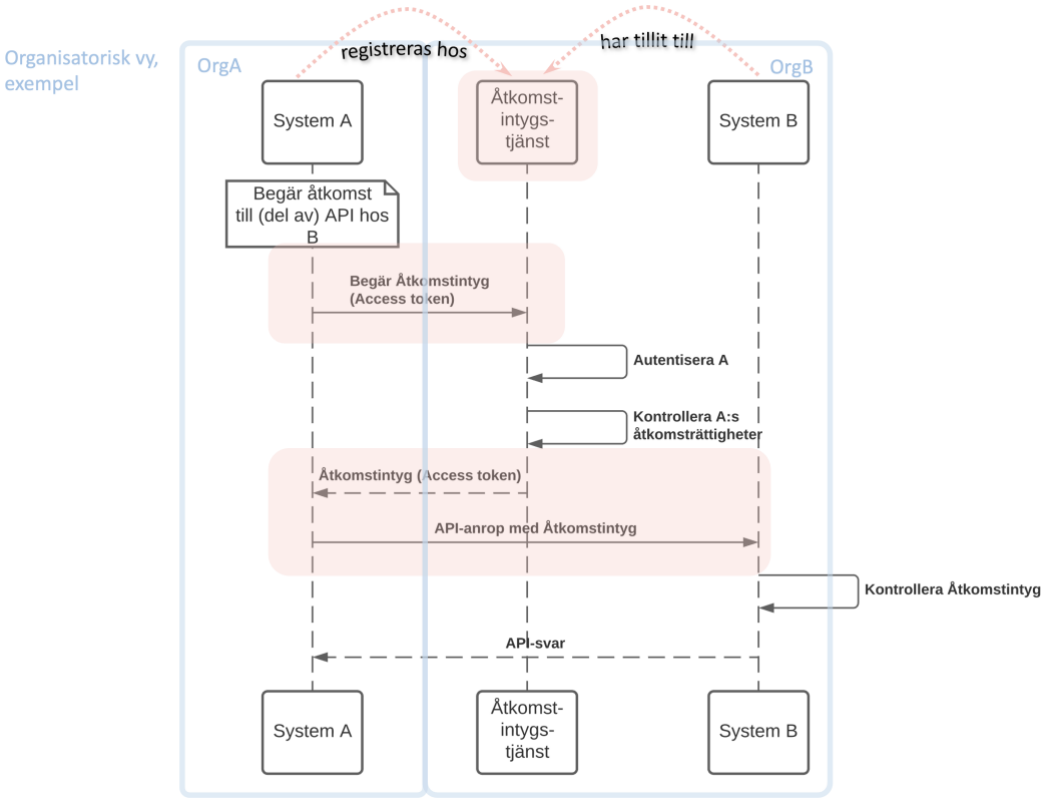



*Figur 38. System-system-kommunikation med stöd av åtkomstintyg*

I detta mönster kan autentisering och auktorisation konsolideras till Åtkomstintygstjänsten för potentiellt många serversystem och API:er[15]. Åtkomsten kan anpassas både till det anropande systemet i sig och dess egenskaper samt vilket API-omfång[16] (*resource*/*scope*) som systemet begär. Det tilldelade API-omfånget kan dessutom både minskas resp. utökas relativt det begärda omfånget beroende på aktuell åtkomstpolicy.
System som tillhandahåller API:er ansvarar ur ett åtkomstperspektiv primärt endast för att kontrollera åtkomstintygets giltighet och omfång. En förutsättning är att systemet litar på Åtkomstintygstjänsten och att intygen är digitalt signerade av densamma.

Oftast tillhör Åtkomstintygstjänsten ansvarsmässigt samma organisation som systemet som tillhandahåller API:et, vilket gör att ansvar för åtkomstregelverket och dess implementation blir tydligare. Den anropande systemet kan tillhöra samma organisation eller annan organisation.

[15] Jämför referensarkitekturens motsvarande mönster för konsolidering av IAM-funktionaliteten till legitimeringstjänsten avseende autentisering av användare.
[16] Omfång kan till exempel vara ”läs tjänst A” eller ”skriv tjänst B”




*Figur 39. System-system-kommunikation med stöd av åtkomstintyg - Organisatorisk vy, exempel*

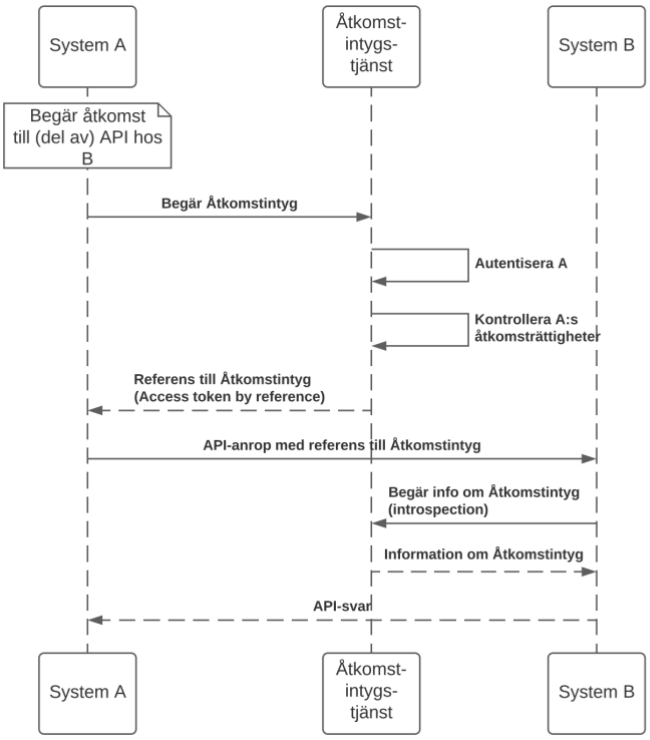
Åtkomstintyget (*access token*) kan såsom beskrivs i kap. 5.3.1 förmedlas antingen direkt, varvid åtkomstintyget och dess innehåll kan konsumeras direkt av API:et, eller via en referens, i vilket fall serversystemet behöver hämta information om åtkomstintyget från Åtkomstintygstjänsten (*token introspection*).

#### 5.9.4.1 System-system med åtkomstintyg direkt

Direkta åtkomstintyg har fördelen att kommunikationsmönstret blir relativt enkelt, skalbart och oftast mer effektivt. Normalt behöver inte innehållet i åtkomstintyg hållas dolt för det auktoriserade systemet själv, vilket underlättar ev. felsökning och förståelse för flödet. Vid behov att skydda innehållet från insyn även för anropande system bör krypterade åtkomstintyg användas.

#### 5.9.4.2 System-system med åtkomstintyg via referens

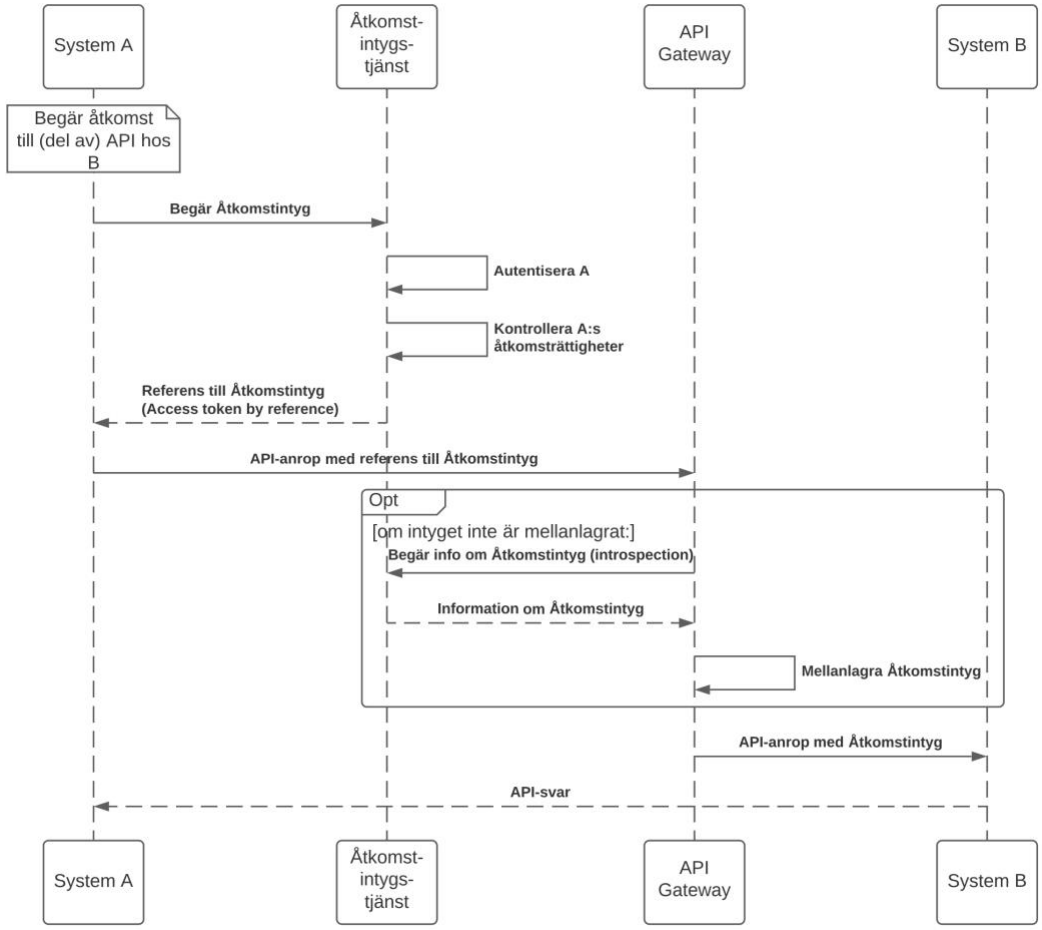
Genom att använda åtkomstintyg via referens är det möjligt att vid behov hämta ytterligare information om intyget från Åtkomstintygstjänsten (*token introspection)*, till exempel information om systemaktören som begärde intyget.




*Figur 40. Åtkomstintyg via referens och token introspection.*

System som begär ut information om åtkomstintyg behöver autentiseras och auktoriseras. Som minimum behöver åtkomsträttigheter ges till aktuella serversystem. Även klientsystem kan vid behov ges rättighet att hämta information om åtkomstintyget.

Användning av åtkomstintyg via referens medför ett komplexare kommunikationsflöde med ett större realtidsberoende till Åtkomstintygstjänsten. Det kan även leda till en sämre effektivitet/prestanda pga. att antalet anrop och systemautentiseringar ökar.
Dessa potentiella nackdelar kan dock till stor del undvikas genom att använda en *API Säkerhetstjänst* (*API Gateway*) för att hantera all *token introspection* för bakomliggande API-servrar. Genom att mellanlagra (*cacha*) token-informationen kan antalet anrop till Åtkomstintygstjänsten minskas. Det är även möjligt att låta *API Säkerhetstjänst* begära ett nytt åtkomstintyg med direkt innehåll att förmedla till bakomliggande API:er för kontroll, dvs. de två mönstren kan kombineras enligt följande figur.



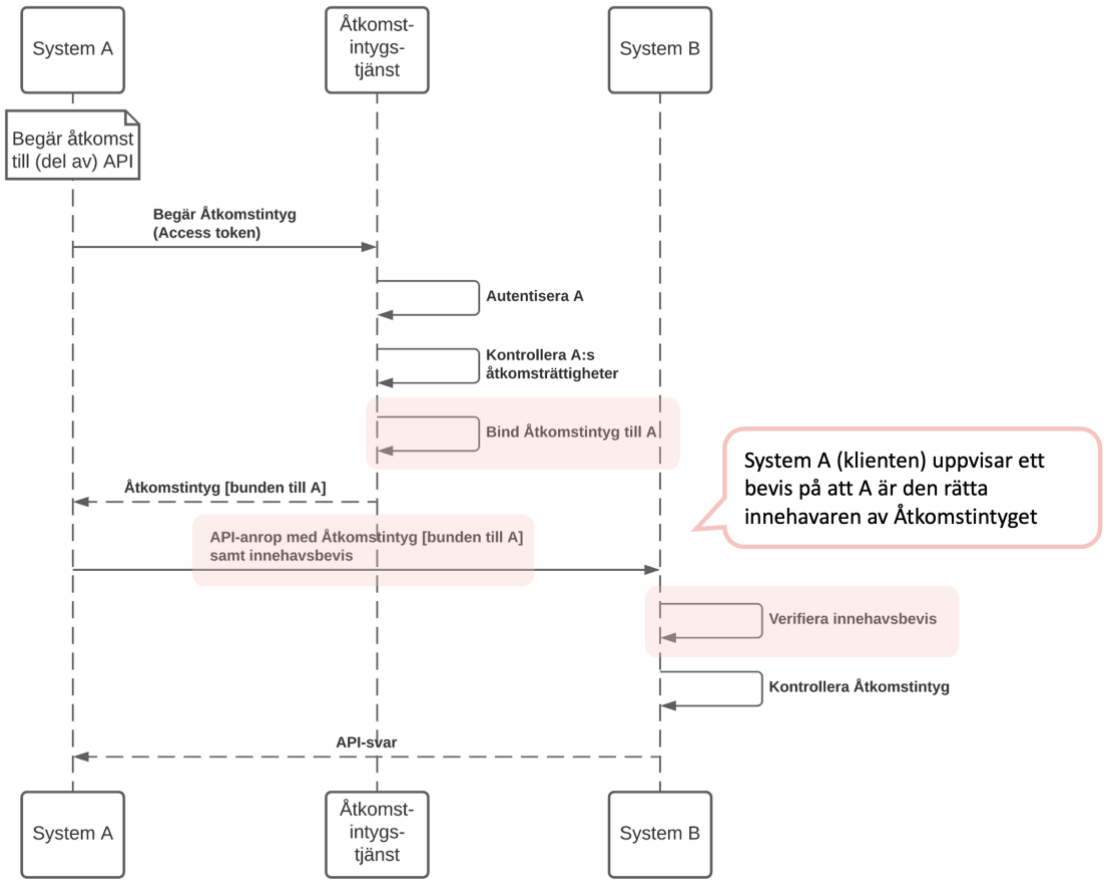

*Figur 41. Token Introspection med mellanlagring i API Gateway*

### 5.9.5 Bevisa innehav av åtkomstintyg

För att stärka skyddet mot att åtkomstintyget kommer i orätta händer och används i återuppspelningsattacker (*replay attacks*), kan användning av åtkomstintyg kompletteras med s.k. *innehavsbevis* (*proof-of-possession, PoP*). Innehavsbevis innebär att det klientsystem som erhållit ett åtkomstintyg kan för serversystemet presentera ett sorts bevis att det anropande klientsystemet är samma system som fick intyget utfärdat till sig. Åtkomstintyget begränsas redan vid dess utfärdande till att bara kunna användas av det system som begär intyget (benämns även *sender-constrained token*).

Innehavsbevis kan tillämpas på alla grundläggande flöden för utfärdande och användning av åtkomstintyg utan att helt nya interaktioner läggs till. Det som tillkommer är att

- Åtkomstintygstjänsten binder åtkomstintyget till det begärande systemet.
- Anropande system presenterar *innehavsbevis* tillsammans med åtkomstintyget i API-anropet.
- Serversystemet verifierar innehavsbeviset.

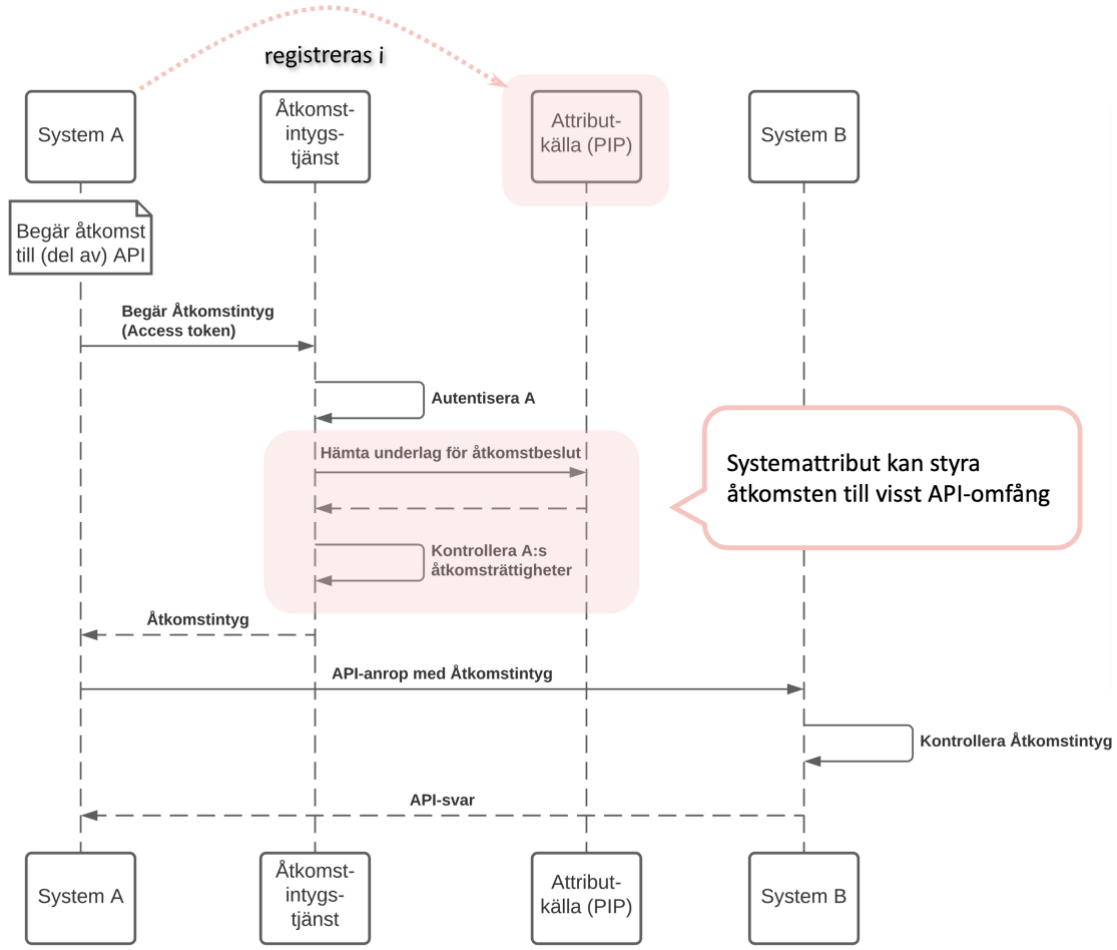



*Figur 42. Åtkomstintyg med innehavsbevis (Proof-of-possession)*

### 5.9.6 Hantera egenskaper för system

För att kunna tillämpa en åtkomstpolicy i ovan flöde behöver Åtkomstintygstjänsten information om vilka rättigheter som gäller för olika system. I de enklaste fallet kan informationen baseras på att rättighet till resurser (API-metod, omfång etc.) konfigureras för respektive system i en källa kopplad till Åtkomstintygstjänsten, eventuellt definieras även grupper av system för att koppla olika rättighetsuppsättningar.

I det mer generella fallet kan Åtkomstintygstjänst nyttja en eller flera betrodda *attributkällor* för att erhålla egenskaper (attribut) för registrerade systemidentiteter, i analogi med hur attributkällor kan användas för personer och organisationer.
Även för system kan attributbaserad behörighetsutvärdering med fördel nyttjas för att uppnå god skalbarhet och flexibilitet. Till exempel kan ett systemattribut hämtad från en betrodd attributkälla implicera rätt till åtkomst till resurser utifrån satt åtkomstpolicy. En attributkälla vars information används som underlag för åtkomstbeslut kallas även för *Policy Information Point (PIP).*




*Figur 43. Egenskaper för system i attributkälla som underlag för åtkomstbeslut*

Attributkällan kan tillhöra samma eller annan organisation än Åtkomstintygstjänsten, och mönstren för system-system-kommunikation kan förstås tillämpas även här.

### 5.9.7 System-till-system med delegering

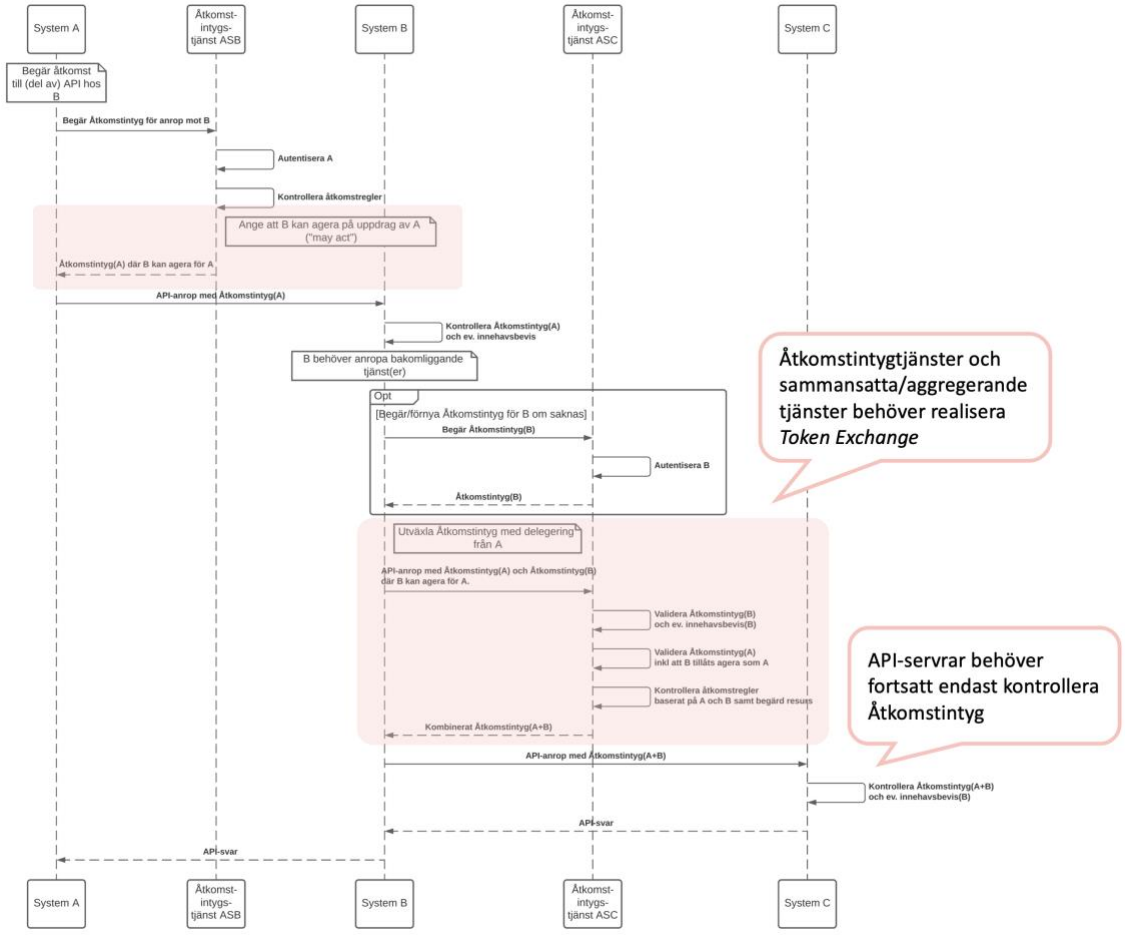
I det andra grundläggande interaktionsmönstret tillför vi *delegering* av anropande systems åtkomsträttigheter till ett mellanliggande system.
Ett system A anropar ett annat system B, där system B i sin tur behöver anropa system C på uppdrag av (*on behalf of*) och med delegerade rättigheter från A. Interaktionsmönstret kan till exempel tillämpas för en sammansatt tjänst som aggregerar information från flera bakomliggande tjänster, vilka i sin tur behöver kunna styra åtkomst baserat på det ursprungliga klientsystemet (system A i detta fall).

Här behöver både A och B autentiseras och auktoriseras för de respektive anropen, och A ska ges möjlighet att utifrån en åtkomstpolicy delegera rättigheter till B för att kunna utföra det begärda uppdraget.

Interaktionsmönstret omfattar flera åtkomstbeslut, där underlaget för besluten ska kunna inkludera både A:s och B:s rättigheter. Åtkomsthanteringen realiseras som i tidigare flöde genom Åtkomstintygstjänst och åtkomstintyg. I flödet nedan skyddas respektive resursanrop av separata Åtkomstintygstjänster för att stödja att tjänsterna B och C *kan* tillhöra olika organisationer, varvid

förlitande måste etableras mellan Åtkomstintygstjänsterna.
Mönstret kan även tillämpas inom en organisation/säkerhetsdomän och i dessa fall är det vanligt att samma Åtkomstintygstjänst hanterar hela flödet.

I flödet ingår en utväxling av åtkomstintyg (*token exchange*) där åtkomstintyg från system A och B utgör underlag för ett kombinerat åtkomstintyg som används för själva resursanropet mot system C.




*Figur 44. System-system-kommunikation med delegering*

Notera att åtkomstintygstjänsten ASC, som styr åtkomst till C, har vid delegering möjlighet att applicera åtkomstregler baserat en kombination av rättigheter för A och rättigheter för B. Åtkomstintygstjänsten ASC kan även verifiera att B givits rättighet att agera på uppdrag från A eftersom detta kan anges i åtkomstintyget för A.

I ett fall där det bara finns verksamhetskrav på att reglera åtkomsten utifrån åtkomsträttigheter för system A (den ursprungliga API-klienten) och inte för system B, kan delar i flödet utgå. B kan i detta fall tillåtas att agera som om det ur åtkomstperspektivet vore system A (*impersonation*). Åtkomstintygstjänsten ASC baserar då validering och åtkomst på enbart åtkomstintyg för A och växlar mot ett åtkomstintyg för anrop mot C.
De tekniska ramverken inom referensarkitekturen har stöd för båda koncepten *delegation* och *impersonation*, och ytterst bör verksamhetskraven styra valet.

Även detta interaktionsmönster stödjer att använda innehavsbevis och därmed binda åtkomstintygen till respektive auktoriserad avsändare, precis som basflödet ovan med enbart system A och B. Även attributkällor kan förstås nyttjas bakom Åtkomstintygstjänsterna, vilket inte tagits med i bilden.

### 5.9.8 Specifika krav

- Registrering av systemidentiteter och autentisering av dessa ska baseras på att systemet innehar en unik hemlighet som inte behöver kommuniceras med förlitande parter, normalt i form av ett asymmetriskt nyckelpar där endast den publika nyckeln kommuniceras till andra parter.
- Registrering av systemidentiteter via metoden ”Publik nyckel-registrering” rekommenderas för att möjliggöra god skalbarhet och god kontroll över regelverket för registrering/avregistrering.
  Även s.k. öppen resp. sluten PKI kan nyttjas för registreringsprocessen där så tillämpligt, men beroendet som skapas till certifikatutfärdarnas policys, rutiner och ev. svagheter behöver då beaktas.
- Alla i informationsutbytet ingående system ska kunna förvara förekommande hemligt nyckelmaterial och åtkomstintyg på ett säkert sätt (även kallat *confidential clients*).
- Vid höga krav på skalbarhet, flexibel hantering av autentisering och auktorisation och många ingående parter i informationsutbytet rekommenderas att
  - hantera registrering av systemidentiteter via federation.
  - använda systemidentifierare i form av globalt unika URL/URI för att kunna använda samma identifierare i alla informationsutbyten och undvika namnkonflikter.
  - använda åtkomstintyg utfärdade av Åtkomstintygstjänst(er).
  - vid behov använda betrodda attributkällor för att hämta egenskaper (attribut) för registrerade systemidentiteter.
- Direkta åtkomstintyg rekommenderas vid system-till-systemkommunikation för ett skalbart, effektivt och enkelt kommunikationsflöde.
  Vid behov att skydda innehållet i åtkomstintyget från insyn kan krypterade åtkomstintyg användas. Det rekommenderas dock att utforma innehållet i intygen så att de inte innehåller sådan information som skulle motivera kryptering.
- Om åtkomstintyg via referens används ska system som begär ut information om åtkomstintyg autentiseras och auktoriseras. Som minimum behöver ges rättigheter till de system som tillhandahåller integrationstjänsterna. Även anropande system kan om lämpligt ges rättigheter att hämta information om åtkomstintyget.
- Vid höga krav på informationssäkerhet rekommenderas att system som konsumerar åtkomstintyg kräver s.k. *innehavsbevis* (*proof-of-possession*).
- Vid system-till-systemkommunikation som omfattar anropskedjor (A→B→C…) där de bakomliggande serversystemen behöver kunna styra åtkomst baserat på de ursprungliga klientsystemens rättigheter, rekommenderas mönstret ”System-till-system – med delegering” med utväxling av åtkomstintyg (*token exchange*).

## 5.10 Delegerad åtkomst från användare

När en användare nyttjar någon form av digital tjänst kan många gånger behov finnas att den digitala tjänsten får åtkomst till information i externa källor som användaren har åtkomsträttigheter till.

Till exempel kan användaren vilja använda en app som visar upp egna hälsodata från olika källor, såsom ett system för medicinsk provtagning, en app som samlar in mätvärden från en blodtrycksmätare osv. I andra fall kan användaren vilja dela med sig av (publicera) uppgifter från en app till en e-tjänst, till exempel i syfte att rapportera in mätvärden från en app för datafångst till ett telemedicinskt system vid ordinerad egenvård.

Användaren har åtkomsträttigheter till var och en av dessa datakällor avseende de egna uppgifterna, men den använda appen har i sig inga rättigheter att få åtkomst till dessa.
Med hjälp av auktoriserad och tidsbegränsad delegering av användarens åtkomsträttigheter, kan appen tillfälligt verka ”på uppdrag” av användaren och hämta och/eller publicera uppgifter i datakällan.

### 5.10.1 Interaktionsmönster för delegerad åtkomst från användare

Nedan interaktionsmönster omfattar delegering av åtkomsträttigheter från en användare till någon form av digital tjänst. Notera att den digitala tjänsten kan utgöras av såväl en app på användarens enhet (publik klient) eller e-tjänst med skyddad serverdel (konfidentiell klient).

- **Delegering av användarens rättigheter**
  Mönster: Användare(A) → B → C med delegering (*user delegation*).
  Användare A använder app eller en e-tjänst B, som i sin tur behöver anropa ett system C på uppdrag av (*on behalf of*) användaren A.

Användaren kan till exempel vara informationsägare eller via ett åtkomstregelverk ha rättigheter till uppgifter i C.

Användarens rättigheter behöver tillfälligt delegeras till B, vilket hanteras med hjälp av en Åtkomstintygstjänst samt att användaren autentiseras via en Legitimeringstjänst (IdP).
Åtkomstintyget kan ses som en *delegerad rättighet* från användaren A till appen/e-tjänsten B att för användarens räkning få åtkomst till resursen.
Resurs-servern C ansvarar för att åtkomstintygets giltighet och omfång kontrolleras, och utifrån det verkställa det åtkomstbeslut som tagits i Åtkomstintygstjänsten.

Beroende på aktuellt åtkomstregelverk kan användarens aktiva medgivande[17] behövas för att auktorisera visst informationsutbyte mellan B och C, vilket i så fall ingår som en användardialog i flödet.

Precis som för ren system-till-system-kommunikation, kan systemen B och C tillhöra samma organisation eller olika organisationer. Om systemen tillhör olika organisationer behöver särskilt

[17] Notera att detta inte ska förväxlas med ev. krav på inhämtande av samtycke i en viss legal kontext. Här avses enbart användarens möjlighet att godkänna eller neka den aktuella informationsöverföringen mellan systemen med användande av hens uppgifter och rättigheter.

beaktas hur förlitande mellan systemen regleras samt hur förekommande attributkällor hanteras, se vidare avsnitt 5.10.2.

Interaktionen kan realiseras på några olika sätt beroende på vilka förutsättningar som finns, vilket ger oss följande varianter av mönstret:

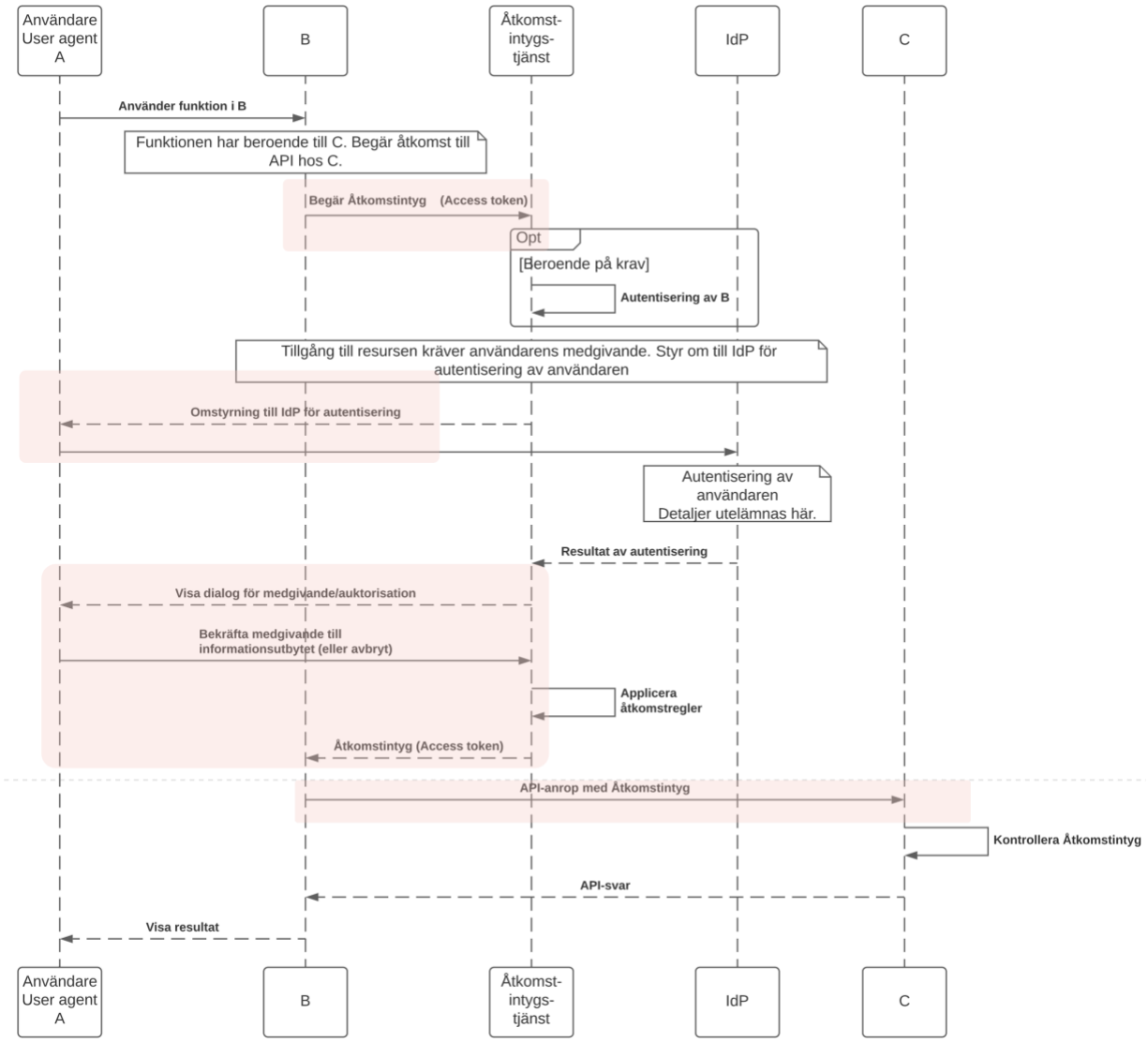
- Delegerad åtkomst via förnyad användarautentisering.
  I samband med utställande av åtkomstintyg för en viss begärd API-åtkomst krävs autentisering av användaren, vilket hanteras genom omstyrning till en Legitimeringstjänst (IdP).
- Delegerad åtkomst direkt vid inloggning.
  Åtkomstintyg för API-åtkomst ställs ut i samband med inloggningen i appen/e-tjänsten B.
- Delegerad åtkomst via intygsväxling (*Token Exchange*).
  Utställande av åtkomstintyg baseras på tidigare utställt identitetsintyg för användaren som växlas till ett åtkomstintyg för den begärda åtkomsten.

Dessa interaktionsmönster beskrivs och jämförs i följande avsnitt. För rekommenderade tekniska protokoll för dessa flöden se anvisningarna i kap. 6.

#### 5.10.1.1 Delegerad åtkomst via förnyad användarautentisering

För att erhålla ett åtkomstintyg med delegerade rättigheter krävs att användaren är autentiserad, vilket i detta fall hanteras genom omstyrning till en Legitimeringstjänst (IdP) som Åtkomstintygstjänsten har etablerad tillit till.

I figuren nedan har vi antagit att användarens medgivande krävs för den aktuella informationsöverföringen.




*Figur 45. Delegerad åtkomst via förnyad autentisering av användare (A) till e-tjänst eller app (B) för åtkomst till informationsresurs hos integrationstjänst (C).*

Mönstret förutsätter att det är verksamhetsmässigt acceptabelt för användarna att förnya legitimeringen för API-åtkomsten.

Notera att IdP-tjänsten i flödet ovan inte behöver användas för inloggning till B, även om det är ett möjligt scenario. Autentisering för inloggning till B respektive autentisering i syfte att få åtkomst till C är logiskt sett separata flöden.

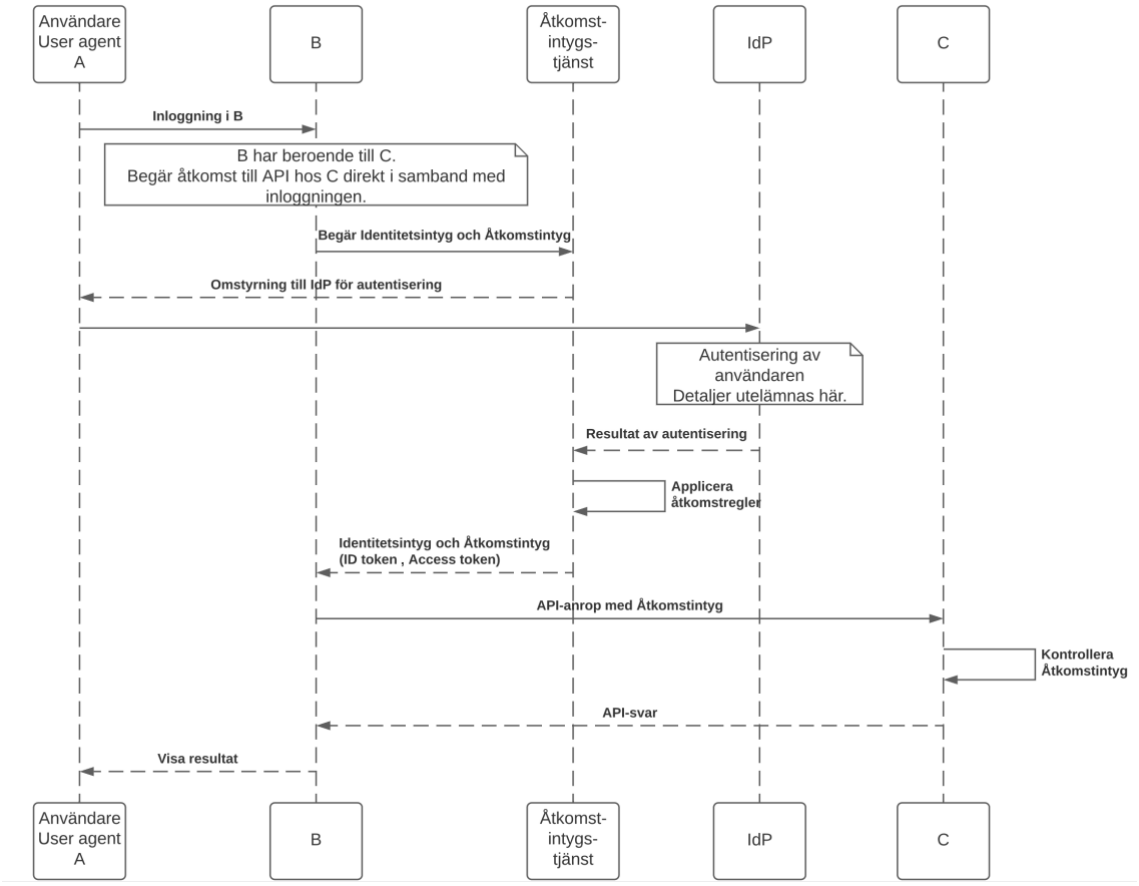
I de fall användaren erbjuds att använda samma IdP-tjänst för inloggning i B och för åtkomst till C, finns möjlighet att nyttja *single sign-on (SSO)* för att minska antalet förnyade legitimeringar en användare behöver utföra.

Krav *kan* ställas på autentisering och auktorisation av B för att erhålla åtkomstintyget, men mönstret fungerar även utan detta, eftersom auktorisationen kan baseras enbart på delegering av användarens åtkomsträttigheter.
Mönstret går därför att tillämpa både med konfidentiella och publika klienter (*confidential and*

*public clients*); således kan B vara såväl en skyddad e-tjänst som en publik app på användarens enhet.

### 5.10.1.2 Delegerad åtkomst i samband med inloggning

Om förutsättningar finns att ha samma IdP-tjänst och Åtkomstintygstjänst i hela flödet blir det möjligt att begära åtkomstintyget redan i samband med inloggning i B. Därmed kan förnyade användarautentiseringar undvikas helt, och flödet kan göras både effektivt och användarvänligt.




*Figur 46. Delegering av åtkomst till C utförs direkt i samband med inloggning till B.*

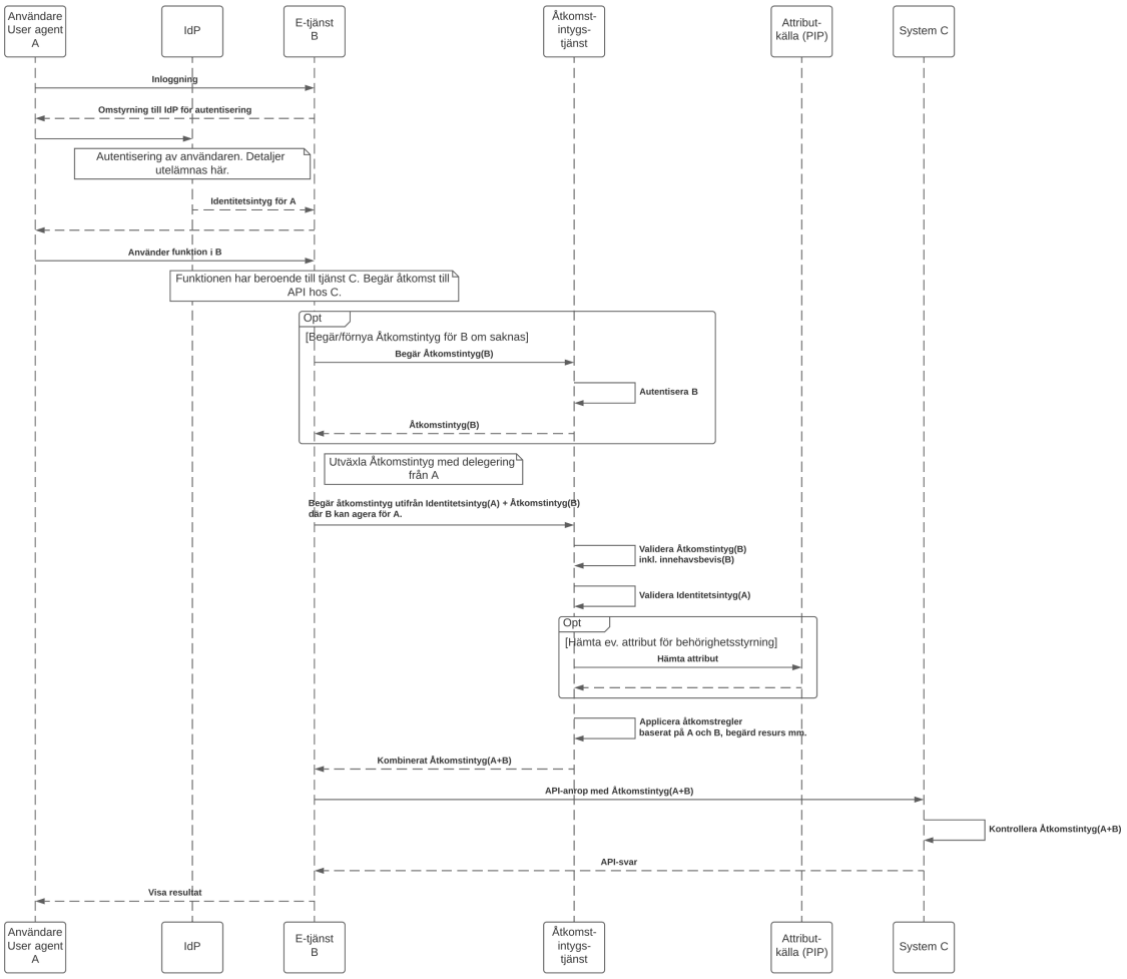
De system (C) som tillhandahåller bakomliggande API:er måste här ha full tillit till de åtkomstintyg som ställs ut av Åtkomstintygstjänsten och därmed den regeladministration som utförs i denna. Detta mönster är därför lättare att realisera när samma part har kontroll över både IAM-tjänsterna och API-servrarna, till exempel inom en organisation eller viss applikation.

Krav kan ställas på autentisering och auktorisation av B för att erhålla åtkomstintyget, men mönstret fungerar även utan detta, således kan B vara såväl en skyddad e-tjänst som en publik app på användarens enhet (*confidential and public clients*).

### 5.10.1.3 Delegerad åtkomst via intygsväxling

Vid delegerad åtkomst med hjälp av intygsväxling använder e-tjänsten B identitetsintyget från användarens inloggning i B, för att begära ett åtkomstintyg för API-åtkomsten i C (s.k. *Token*

*Exchange*). Åtkomstintygstjänsten behöver därmed inte styra om användaren till en IdP för förnyad autentisering.




*Figur 47. Delegerad åtkomst via intygsväxling (Token Exchange) från användare till e-tjänst för åtkomst till resurs hos integrationstjänst. I detta fall har antagits att behörighetsstyrande attribut hämtas från en betrodd attributkälla.*

Delegerad åtkomst från användare med hjälp av intygsväxling kan vara lämpligt när

- det inte är acceptabelt ur ett användarperspektiv att användarna behöver förnya sin e-legitimering för API-åtkomsten enligt avsnitt 5.10.1.1,
- förutsättningarna saknas för att tillämpa delegering direkt vid inloggning enligt avsnitt 5.10.1.2.

Eftersom B i detta fall ansvarar för användarautentisering och korrekt hantering av identitetsintyget, vilket Åtkomstintygstjänsten behöver förlita sig på, kräver detta mönster att B är en skyddad e-tjänst (*confidential client*) som autentiseras och vars behöriga åtkomst kontrolleras.

Vidare krävs ett förlitande mellan Åtkomstintygstjänsten och de legitimeringstjänster (IdP:er) som används, där krav till exempel kan ställas på autentiseringens tillitsnivå. För bättre skalbarhet kan även här tillit etableras till legitimeringstjänster ingående i en federation.

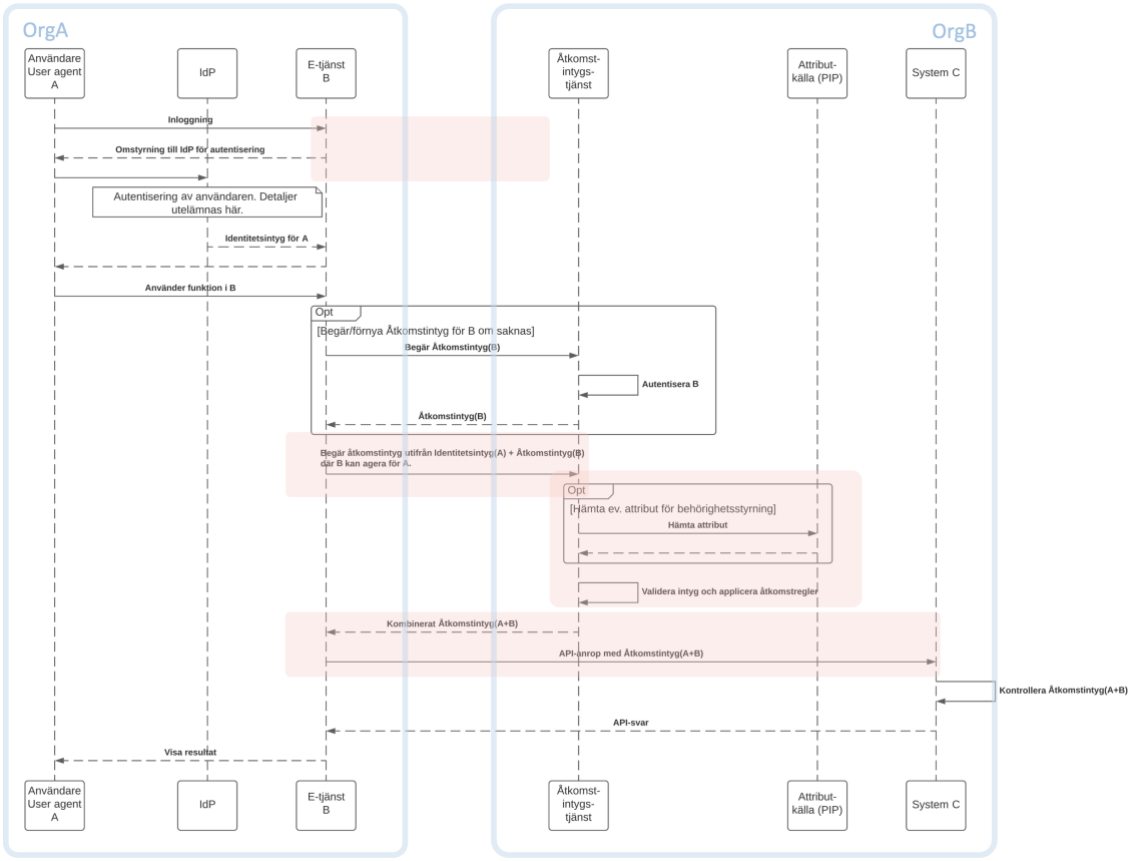
Om detta mönster används behöver även följande tas hänsyn till:

- Utfärdade intyg har oftast begränsningar för vilka system som är ämnade att konsumera intyget (*audience restrictions*). Specifikt behöver Åtkomstintygstjänsten vara definierad som godkänd konsument av identitetsintyg från aktuella legitimeringstjänster.
- Giltighetstider för intyg som konsumeras i anropskedjorna behöver särskilt tas hänsyn till, särskilt avseende identitetsintyg utställda av legitimeringstjänsten. Interaktionsmönstret kan behöva anpassas därefter.

### 5.10.2 Delegerad åtkomst över organisationsgränser

Om delegerad åtkomst används för informationsutbyte mellan organisationer, till exempel då konsumerande e-tjänster tillhör andra organisationer än de system som tillhandahåller bakomliggande API:er, behöver ett antal aspekter särskilt beaktas.

- Organisation som tillhandahåller informationsresurser till andra parter bör beakta vilka attributkällor som används som underlag för behörighetsstyrning, hur dessa attributkällor föds med data, och vilka regelverk/avtal som gäller. Det kan till exempel finnas krav på att officiellt register används som attributkälla, att behörighetstilldelning i attributkällan följer ett överenskommet regelverk osv.
- Organisation som tillhandahåller informationsresurser till andra parter behöver etablera tillit till de legitimeringstjänster som ska kunna användas. Organisationen både kan och bör sätta krav på tillitsnivå för användarautentiseringen, baserat på etablerade tillitsramverk.
- Mönstret i sig hindrar inte tekniskt sett att part med kontroll över anropande e-tjänst (till exempel driftspersonal) skulle kunna tillskansa sig obehörig åtkomst till information som tillgängliggörs inom e-tjänsten för behöriga medarbetare. Detta gäller i princip oavsett teknisk lösning för informationsöverföringen till e-tjänsten. Det förutsätts att detta regleras mellan organisationerna utanför den tekniska lösningen, t.ex. genom avtal, revision eller motsvarande.




*Figur 48. Delegerad åtkomst med informationsutbyte mellan organisationer. I detta exempel används intygsväxling (Token Exchange) från användare till e-tjänst för åtkomst till resurs hos integrationstjänst.*

### 5.10.3 Specifika krav

- Åtkomstintygstjänst ska endast tillåta delegering av en användares åtkomsträttigheter under förutsättning att
  - Användaren är identifierad och autentiserad på en tillitsnivå som motsvarar verksamhetskrav.
  - Identitetsintyg accepteras i förekommande fall endast från specificerade IdP:er som etablerats tillit till. Federation kan användas för detta.
  - Användarens medgivande till informationsutbytet har inhämtats, förutsatt att inte aktuellt åtkomstregelverk anger annat.
  - Ev. krav på att autentisera och auktorisera den tjänst som begär åtkomstintyget har beaktats.
- Vid delegering av en användares åtkomsträttigheter ska autentiseringskrav för den tjänst som begär åtkomstintyg (*client*) kunna konfigureras i Åtkomstintygstjänst. Åtkomstintygstjänst bör även stödja icke autentiserad tjänst (*public client*).

- Förmedling av åtkomstintyg vid delegering från användare bör ske via principen *intyg via referens*[18], för att skydda mot risken att åtkomstintyg fångas upp av obehörig (*interception attacks*).

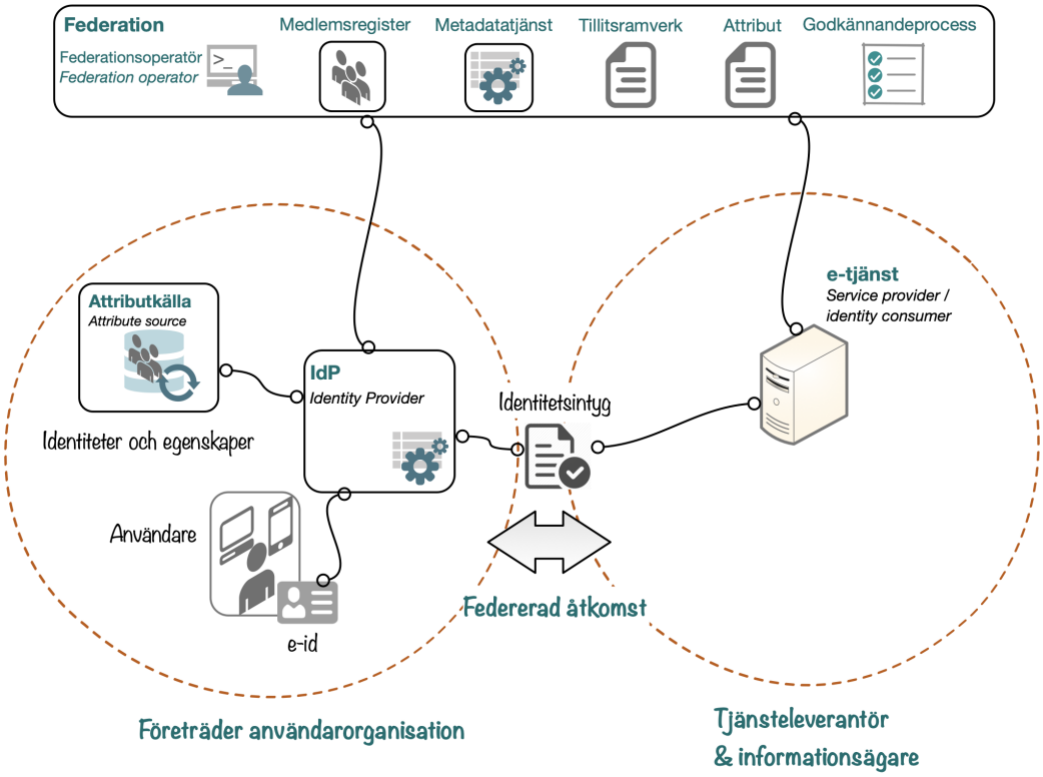
[18] Exempel: *OAuth2 Authorization Code Flow* implementerar intyg via referens.

## 5.11 Identitets- och behörighetsfederation

### 5.11.1 Federationens roll och nytta

Referensarkitekturen stödjer vidare ett federativt sätt att hantera identitet och åtkomst vid elektroniskt utbyte mellan olika organisationer.

Federation bygger på ett förlitande (*trust*) mellan organisationerna och till registrerade tjänster inom federationen. Genom att nyttja federationens signerade information som utgångspunkt för tillit till andra parters system kan en part välja att acceptera utfärdade identitetsintyg från annan part, och därigenom ge åtkomst till skyddade resurser utan att själv behöva administrera den andra partens medarbetare, autentiseringslösningar och ev. även behörighetsstyrande egenskaper.




*Figur 49. Identitets- och behörighetsfederation. Federativ åtkomst till e-tjänst i annan organisation.*

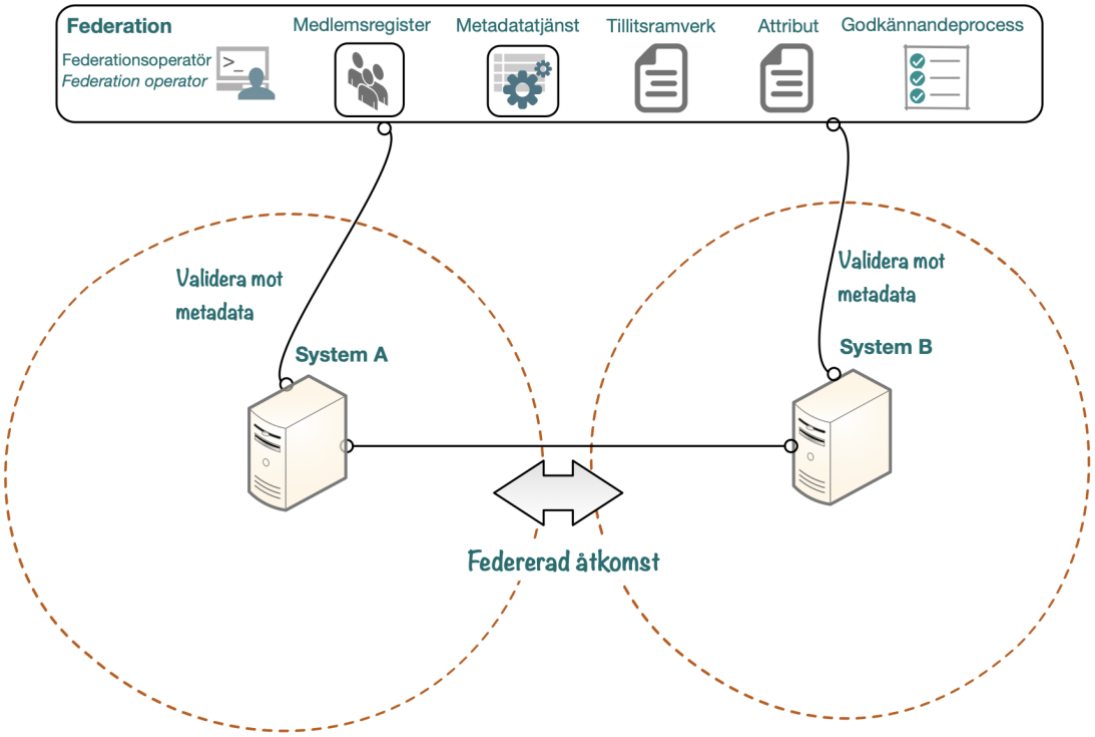
Några nyttoeffekter som erhålles med en identitets- och behörighetsfederation:

- Organisation som tillhandahåller e-tjänst(er) externt till andra organisationer behöver inte administrera 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, till exempel 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. I

stället kan organisationens medarbetare använda sin ordinarie IT-infrastruktur för inloggning och identifiering för åtkomst till tjänsteleverantörens e-tjänst.

- Med gemensamma tillitsramverk och tillhörande godkännandeprocesser, behöver inte varje ansluten part ”uppfinna” sitt ramverk och processer för att godkänna säkerhetslösningar och andra parter att kommunicera med. Autentiseringslösningar och utfärdade e-id kan åsättas en enhetlig klassificering (tillitsnivå) inom federationen.

Federation kan även nyttjas för ren system-system-kommunikation. Genom att registrera de system som behöver kommunicera säkert med varandra och deras publika nycklar i federationens metadata, kan alla parter säkert verifiera varandra ömsesidigt (se ”Publik nyckel-registrering” i kap.5.9.1).




*Figur 50. Federativt etablerad säker system-system-kommunikation*

Genom federationens processer för registrering, avregistrering och tillhörande incidenthantering, kan full kontroll erhållas över vilka parter som vid var tid kan kommuniceras säkert med, och samtidigt uppnås skalfördelar när antalet parter och system växer.

### 5.11.2 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 anslutna tjänster och system – legitimeringstjänster, e-tjänster, åtkomstintygsutfärdare osv. – samt deras egenskaper, förmågor och publika nycklar. Publika och privata nycklar används för att signera och

verifiera signaturer på intyg och metadatat självt. Inom federationen definieras processer för utbyte av metadata i samband med registrering av ingående tjänster.

- *Tillitsramverk* – beskriver tekniska och regulatoriska krav för ingående parter i federationen, till exempel krav på skydd av privata krypteringsnycklar. Tillitsramverket möjliggör för parterna att använda olika lokala lösningar och processer för identitet och åtkomst, och ändå samverka via jämförbara *tillitsnivåer*.
- 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.

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, se vidare kap. 6.
- *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.

### 5.11.3 Tillitsramverk

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

Det är viktigt att tillitsramverket utgår från nationella 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 *Tillitsramverk för kvalitetsmärket Svensk e-legitimation (DIGG)*[19] vara normerande där så är tillämpligt. Detta ramverk baserar sig i sin tur bland annat på den internationella standarden *ISO/IEC 29115*[20], vilken i sin tur har sina rötter i amerikanska *NIST Digital Identity*

[19] https://www.digg.se/digital-identitet/e-legitimering/tillitsnivaer/tillitsramverket

[20] https://www.iso.org/standard/45138.html

*Guidelines SP800-63*[21].
Även arbeten som *Kantara Initiative Identity Assurance Framework*[22] har bidragit till de nuvarande tillitsramverken.

### 5.11.4 Tillitsnivåer

Ett tillitsramverk definierar *tillitsnivåer* (*level of assurance, LoA*) för att kategorisera vilken tillit man kan ha till respektive autentiseringslösning. Nivåindelningen kan förenklat beskrivas som

- Nivå 1 (LoA1) – Ingen eller mycket begränsad tillit
- Nivå 2 (LoA2) – Viss tillit
- Nivå 3 (LoA3) – Hög tillit
- Nivå 4 (LoA4) – Mycket hög tillit

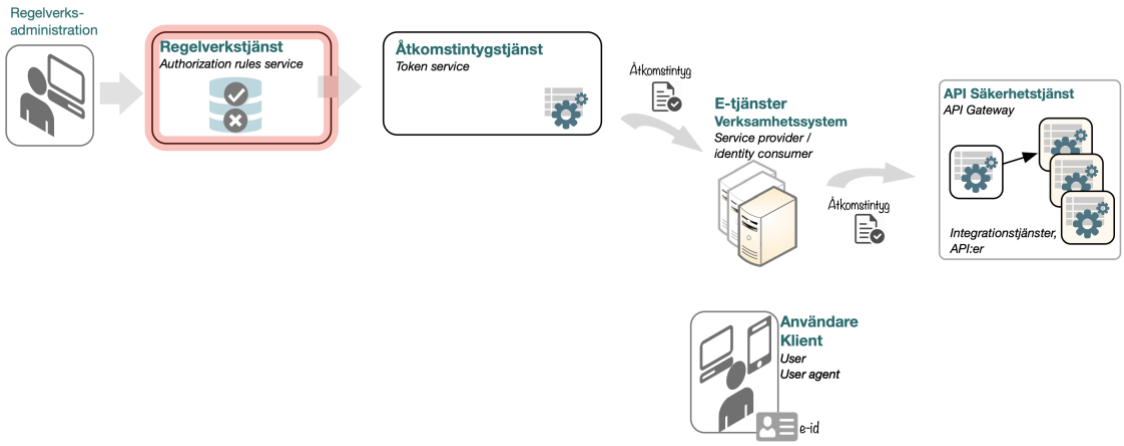
### 5.11.5 Specifika krav

- Tillitsramverk ska utgå ifrån internationella/nationella tillitsramverk, där anpassningar och tillämpning kan göras för att möta domänspecifika krav och behov.
- Digitaliseringsmyndighetens (DIGG) *Tillitsramverk för kvalitetsmärket Svensk e-legitimation* bör vara normerande för utformning av tillitsramverk där så är tillämpligt.
- Ägaren till en e-tjänst ansvarar för att sätta den tillitsnivå som (minst) krävs för åtkomst till e-tjänsten.
- 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 bland annat används i Socialstyrelsens 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.
- Metadatautbyte i samband med registrering av tjänster i federationen bör hanteras enligt principer i etablerade standardiserade tekniska ramverk. Se vidare kap. 0.

[21] https://pages.nist.gov/800-63-3/
[22] https://kantarainitiative.org/identity-assurance-framework/

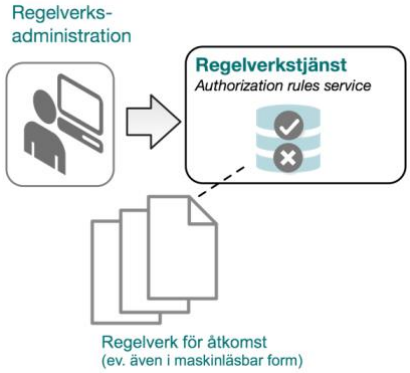
## 5.12 Regelverkstjänst

*Regelverkstjänst* representerar i referensarkitekturen ett eller flera verktyg med syfte att samlat administrera regelverk för åtkomst och understödja implementering av regelverken. Denna förmåga brukar även kallas *Policy Administration Point (PAP)*.




*Figur 51. 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.




*Figur 52. Administration av regelverk för åtkomst*

Regelverken implementeras i de system som behöver utvärdera åtkomst och fatta ett åtkomstbeslut. Dessa system, till exempel en e-tjänst eller en Åtkomstintygstjänst, 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[23].

Kombinationen av Regelverkstjänst, Åtkomstintygstjänst och API-Säkerhetstjänst skapar däremot en möjlighet att via en sammanhållen administration definiera regelverk för en granulär informationsåtkomst via integrationstjänster (API:er). 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 skulle kunna definieras i Regelverkstjänst:

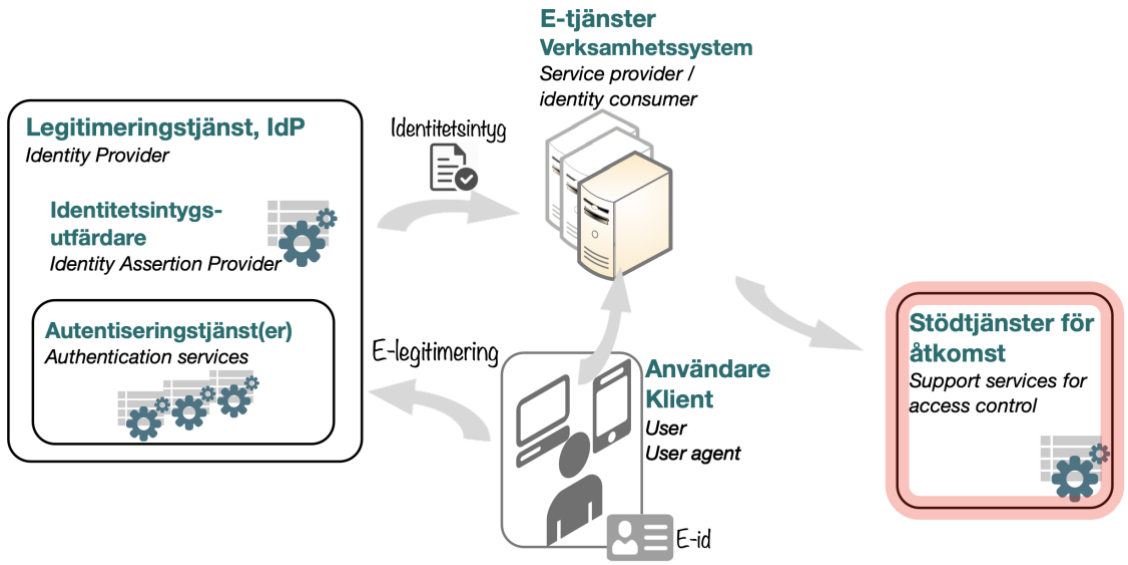
*Användaren ska vara behörig (leg. Läkare, leg. Ssk), anställd med uppdrag inom verksamheten kring vård och behandling, samt vara i tjänst, för att få åtkomst till vårddokumentationen på vårdenheten.*

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

[23]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.

## 5.13 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 53. Stödtjänster för reglering och uppföljning av åtkomst (exempel).*

Stödtjänster inom detta område kan till exempel 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.

### 5.13.1 Stödtjänster för åtkomst inom Hälso- och sjukvård

Inom Hälso- och sjukvård har ett antal stödtjänster definierats för att reglera och följa upp åtkomsten till patientinformation.
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 gemensamma integrationsprofiler, 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 tekniska protokoll och format

I referensarkitekturen görs en uppdelning av tekniska protokoll, format och ramverk inom identitet och åtkomst i följande kategorier.

***Sign-in/out-protokoll*** används för att logga in i (och ut ur) en e-tjänst och få åtkomst till en resurs baserat på den primära autentiseringen. Protokollen kan ge stöd för federativ inloggning och singelinloggning (SSO). Via protokollen kan e-tjänsten erhålla ”bevis” i form av identitetsintyg att identitet och ev. egenskaper är säkerställda enligt en viss tillitsnivå.

***Protokoll för delegerad åtkomst*** (*delegated access*) används för att förmedla åtkomsträttigheter från en aktör till en annan. Aktörerna kan både vara användare och system.

***Format för identitets- och åtkomstintyg***, även kallat ***intygstyp*** eller *biljettyp* (*token type*). Intygstypen 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 identifiering och auktorisation. *Identitetsintyg* innehåller uppgifter om autentiserad användare och egenskaper knutna till användaren. *Åtkomstintyg* specificerar rättigheter till specifik resurs, men kan även innehålla egenskaper knutna till användaren/aktören.

***Autentiseringsprotokoll*** används för den primära autentiseringen av en aktör, dvs. kontroll av uppgiven identitet mot något slags ”äkthetsbevis”. Protokollen kan till exempel baseras på skapande och verifiering av en digital signatur.

***Tekniska ramverk för federation*** vars syfte är att på ett interoperabelt och säkert sätt kunna utforma, hantera och utbyta federationens metadata och möjliggöra tillit.

***Protokoll för provisionering*** används för att på ett strukturerat sätt tillhandahålla kvalitetssäkrade identitetsdata till system/e-tjänster.

I följande avsnitt beskrivs rekommendationer kring teknikval i respektive kategori.

## 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 framför allt principerna #IA1, #IA3 och #IA5 dessa val, vilket leder till ett urval öppna internationella standarder för områden såsom

- Anslutning av e-tjänster för federerad inloggning
- Singelinloggning (SSO)
- Delegerad åtkomst
- Autentisering
- Hantering av federation och tillit
- Beskrivning och säker förmedling av identitet och egenskaper

Principen #IA5 kring plattformsneutralitet i kombination med att det normalt finns många olika tekniska plattformar för e-tjänster inom en organisation, leder till att IT-infrastrukturen för identitet och åtkomst 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 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 IAM-lösningarna.

Rekommendationer kring teknikval är av ovan skäl uppbyggda som *rekommenderad*, respektive *stöds vid behov*.

| Förmåga | Rekommendation | Stöds vid behov |
|---|---|---|
| Federerad inloggning, SSO och utloggning. (*sign-in/sign-out protocols*) | OpenID Connect[24] (första-handsval)<br>SAML 2.0[25] | WS-Trust, WS-Federation<br>IWA/Kerberos[26] (enbart för lokal SSO, saknar federativt stöd) |
| Delegerad åtkomst (*delegated access*) | OAuth 2.0<br>(förmågan saknas inom SAML 2.0-sviten) | Kerberos-begränsad delegering (KCD)[27] (endast lokalt) |
| Format för identitet och egenskaper.<br>Intygstyp (*token type*) | JSON Identity Suite, JSON Web Token (JWT) [28]<br>SAML 2.0 Assertions | |
| Autentisering (*authentication protocols*) | e-id med stöd för flerfaktorsautentisering på skyddad bärare.<br>Autentiseringsteknik baserad på stark asymmetrisk kryptering och utmaning-svar (*challenge response*).<br>Se kap. **Error! Reference source not found.**. för rekommenderade protokoll. | Annan, ev. leverantörsspecifik lösning med motsvarande tillitsnivå, t.ex. en generator för engångslösenord (*OTP*) |
| Federation & tillit Metadatahantering (*federation, trust and metadata*) | SAML Metadata<br>OpenID Connect Federation[29] | WS-Federation |
| Provisionering. Tillhandahålla identiteter och egenskaper. (*provisioning*) | Attributkällor för identitet och egenskaper, med företrädesvis nationellt överenskomna API-specifikationer.<br>SCIM | SPML |

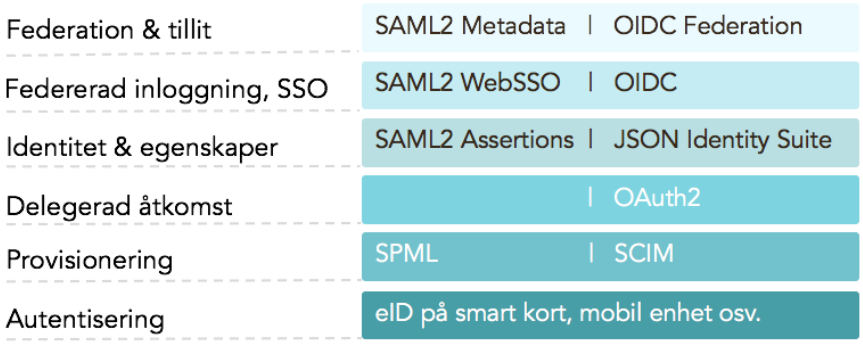
*Figur 54. Sammanställning rekommenderade tekniska protokoll per förmåga inom Identitet och Åtkomst.*

Notera att de flesta protokoll inom området identitet och åtkomst har i sin tur beroende till ett säkert transportprotokoll, där normalt TLS[30] används. Dock är transportsäkerhet strikt sett ett

[24] https://openid.net/developers/specs/
[25] https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
[26] *Integrated Windows Authentication med Kerberos*, även benämnd ”AD-integrerad inloggning med Kerberos”.
[27] https://docs.microsoft.com/en-us/windows-server/security/kerberos/kerberos-constrained-delegation-overview
[28] https://datatracker.ietf.org/doc/html/rfc7519
[29] https://openid.net/specs/openid-connect-federation-1_0.html. **Notera** att denna är i status ”implementers draft”, varför implementationer bör ta hänsyn till att specifikationen kan komma att förändras något i slutlig version.
[30] https://datatracker.ietf.org/wg/tls/documents/

eget område där det bör finnas särskilda tekniska anvisningar, varför detta inte tas upp explicit i denna referensarkitektur.

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




*Figur 55. Teknikstack - rekommenderade tekniska protokoll per förmåga, uppdelat på stack för SOAP/XML resp. stack för HTTP/REST/JSON-baserad kommunikation.*

Notera att två protokollsviter, SAML2 resp. OpenID Connect/OAuth2, är rekommenderade, vilket innebär för interoperabiliteten att

- Legitimeringstjänst (IdP) bör ha stöd för både SAML2 resp. OpenID Connect.
- E-tjänst bör ha stöd för en av OpenID Connect resp. SAML2.

Orsaken till denna rekommendation är det är viktigt att ta till vara tidigare investeringar i säkerhetsteknik och anslutningar av e-tjänster.

OpenID Connect i kombination med det underliggande protokollet OAuth2 har flera fördelar gentemot SAML 2, bland annat

- Möjlighet till delegerad åtkomst
- Bättre stöd för blandade teknikplattformar (mobilt, nativa klienter osv.)
- Bättre stöd och integration i moderna utvecklingsverktyg

OpenID Connect gäller därför som rekommenderat val vid nyutveckling, såvida inte yttre omständigheter kräver SAML2, t.ex. för att kunna ansluta till en SAML2-federation.
Det kan förutsättas att OpenID Connect successivt kommer att användas i allt större utsträckning. Den äldre och mognare SAML 2, 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-protokollen.

## 6.3 Protokoll för federerad inloggning och SSO

### 6.3.1 Specifika krav

- IdP (*Identity Provider*) ska stödja både *OpenID Connect* och *SAML2*.
- E-tjänst (Service Provider) ska stödja minst en av *OpenID Connect* eller *SAML2*.
- IdP ska stödja att validera signatur för autentiseringsbegäran som signerats av e-tjänsten. Om e-tjänst indikerat i metadata/konfiguration att alltid använda signerade autentiseringsbegäran måste IdP neka osignerade autentiseringsbegäran för e-tjänsten.
- IdP ska kunna tillhandahålla autentiseringskontext i identitetsintyget som förmedlar den tillitsnivå som autentiseringen uppnådde (*authentication context*).
- Ombedda identitetsintyg (*solicited assertions*) bör användas för relationen e-tjänst – IdP, dvs. att e-tjänsten explicit begär att få identitetsintyget från IdP.
  E-tjänst rekommenderas att inte acceptera oombedda identitetsintyg[31] (*unsolicited assertions*).
- E-tjänst och IdP bör stödja utloggningsbegäran initierad av e-tjänsten. IdP ska på sådan begäran avsluta ev. aktiv SSO-session för användaren hos IdP.
  E-tjänst behöver inte stödja att ta emot utloggningssvar eller utloggningsbegäran. IdP behöver inte implementera utgående utloggningsbegäran (*single logout*).
- E-tjänst som nyttjar val av IdP (anvisning) via antingen inloggningslänkar med förvald IdP eller en Anvisningstjänst bör följa tillämpliga delar av
  - *Identity Provider Discovery Service Protocol and Profile* [IdPDisco[32]]

#### 6.3.1.1 SAML 2.0

För SAML2.0 gäller följande krav:

***Standardprofiler***

- *SAML 2.0 Web Browser SSO Profile*.

***Kompletterande krav***

- IdP ska för en inkommande autentiseringsbegäran ge stöd för både *HTTP-Redirect* och *HTTP-POST Binding*.
- E-tjänst kan för autentiseringsbegäran använda antingen *HTTP-Redirect* eller *HTTP-POST Binding*.

[31] Oombedda intyg stöds inte av OpenID Connect

[32] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf Not: denna är ej låst till SAML-implementationer, stöd för andra protokoll ges genom ett generiskt http-redirect-flöde.

- IdP ska validera att *AssertionConsumerServiceURL* stämmer med konfigurerat metadata för e-tjänsten.
- E-tjänst som anger krav på tillitsnivå för autentiseringen, ska stödja att ange denna enligt
  - *SAML 2.0 Identity Assurance Profiles* [IAP[33]] och [IANA LoA[34]].
  - OASIS definierade scheman för autentiseringsklasser[35].
- Användning av utloggningsbegäran ska i tillämplig utsträckning följa *SAML2 SingleLogout profile*.

#### 6.3.1.2 OpenID Connect

För OpenID Connect gäller följande krav:

***Standardprofiler***

- *OpenID Connect 1.0*[36]
- *Authorization Code Flow* (åtkomstintyg via referens).
  - *PKCE* (*Proof Key Code Exchange*[37])
    Måste tillämpas för applikationer som saknar en säker serversida (*public client,* t.ex. en rent klientbaserad app),
    och bör tillämpas för applikationer med en säker serversida (*confidential client*, t.ex. en webbapplikation serverside).

***Kompletterande krav***

- E-tjänst och Legitimeringstjänst bör stödja *Relying Party-initierad* utloggning enligt *OIDC Session Management*, i syfte att vid utloggning även logga ut ur SSO-sessionen hos Legitimeringstjänsten (*OP*).
- Legitimeringstjänster (*OP*) ska stödja
  - *Discovery OpenID Connect Discovery*[38] för att dynamiskt upptäcka information om tillgängliga Legitimeringstjänster (*OPs*).
  - *Dynamic Registration* för att dynamiskt registrera klienter (*RPs*) hos en Legitimeringstjänst (*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).*

[33] https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.html
[34] https://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml
[35] https://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf
[36] http://openid.net/connect/
[37] https://datatracker.ietf.org/doc/html/rfc7636
[38] https://openid.net/specs/openid-connect-discovery-1_0.html

- *JSON Identity Suite* bör tillämpas i första hand avseende format för att hantera identitet och egenskaper. IdP ska kunna utfärda identitetsintyg i form av digitalt signerade *JWT bearer tokens*.
- Vid höga säkerhetskrav rekommenderas e-tjänst och IdP i tillämpliga delar följa
  - *Health Relationship Trust Profile for OAuth 2.0*[39].

[39] https://openid.net/wg/heart/ Notera att profilen applicerar även på OpenID Connect som baseras på OAuth2.

## 6.4 Protokoll för delegerad åtkomst

### 6.4.1 Specifika krav

#### 6.4.1.1 OAuth 2.0

***Standardprofiler***

Följande standarder används vid behov av delegerad åtkomst mellan olika aktörer för åtkomst till skyddade integrationsgränssnitt:

- *OAuth 2.0*[40] enligt *RFC6749 OAuth 2.0 Authorization Framework*[41]
- Säkerhetsanvisningar enligt *RFC6819 OAuth 2.0 Threat Model and Security Considerations*[42]
- Implementationer av OAuth 2.0 bör följa aktuell version av *OAuth 2.0 Security Best Current Practice*[43]
- Åtkomstintygs innehåll och format bör följa *RFC9068 JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens*[44]
- Användning av åtkomstintyg bör kompletteras med *innehavsbevis* (*proof-of-possession*) enligt någon av
  - *OAuth 2.0 DPoP - Demonstrating Proof-of-Possession at the Application Layer*[45]
    Kontroll av innehavsbevis på applikationsnivån oberoende av transportprotokoll och autentiseringsteknik.
  - *RFC8705 OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens*[46]
    Kontroll av innehavsbevis med beroende till transportprotokollet och autentiseringstekniken som måste vara Mutual-TLS.

***Kompletterande krav – Delegering användare-system (u2m)***

Vid behov att delegera åtkomsträttigheter från en användare till ett system:

- *OAuth 2.0* enligt *RFC6749*
- *OAuth2.0 Authorization Code Flow* för intyg via referens.
- För autentisering av användaren används identitetsintyg via legitimeringstjänst och ”Protokoll för federerad inloggning och SSO” enligt ovan.

[40] https://oauth.net/2/
[41] https://datatracker.ietf.org/doc/html/rfc6749
[42] https://datatracker.ietf.org/doc/html/rfc6819
[43] https://datatracker.ietf.org/doc/html/draft-ietf-oauth-security-topics
[44] https://datatracker.ietf.org/doc/html/rfc9068
[45] https://datatracker.ietf.org/doc/html/draft-ietf-oauth-dpop
[46] https://datatracker.ietf.org/doc/html/rfc8705

Vid behov att även hantera åtkomsträttigheter för mellanliggande system och/eller kompletterande åtkomstregelverk kan även följande profiler övervägas:

- *RFC8693 Token Exchange*[47]
  med stöd för identitetsintyg enligt både SAML2 och OpenID Connect.
- *RFC 7522 – SAML2 Profile for OAuth 2.0 Client Authentication and Authorization Grants*[48].
  med stöd för identitetsintyg enligt SAML 2.0.
- *RFC 7523 - JWT Profile for OAuth 2.0 Client Authentication and Authorization Grants* [49]
  med stöd för identitetsintyg enligt OpenID Connect.

***Kompletterande krav – System-system (m2m)***

För att kunna konsolidera åtkomsthanteringen till Åtkomstintygstjänst(er) vid system-system-kommunikation:

- *OAuth2 Client Credentials Flow* (RFC6749#4.4)

Vid behov att hantera anropskedjor med delegering till mellanliggande system:

- *RFC8693 Token Exchange*[50]
  med stöd för identitetsintyg enligt både SAML2 och OpenID Connect.

[47] https://datatracker.ietf.org/doc/html/rfc8693
[48] https://datatracker.ietf.org/doc/html/rfc7522
[49] https://datatracker.ietf.org/doc/html/rfc7523
[50] https://datatracker.ietf.org/doc/html/rfc8693

## 6.5 Protokoll för autentisering

### 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.
- E-id och dess bärare ska ha tekniska skydd mot manipulation och kopiering som svarar mot den aktuella tillitsnivån.

### 6.5.2 Rekommenderat mönster för autentiseringsprotokoll

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

1. Autentiseringstjänsten (serversidan) skickar en utmaning till användarens autentiseringslösning. Utmaningen innehåller inslag av slumpmässighet för att skydda emot uppspelningsattacker.
2. Autentiseringslösningen (klientsidan) 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 följer dessa principer inkluderar till exempel digital signatur med privat nyckel och Mutual-TLS med x.509-certifikat.

### 6.5.3 Standardisering av autentiseringsteknik

Autentiseringslösningar är typiskt under ständig teknisk utveckling och området saknar en enhetlig standardisering. Dock finns internationella standardiseringsinitiativ som syftar till att öka interoperabiliteten mellan olika leverantörers autentiseringslösningar. Baserat på dessa listas ett urval rekommenderade autentiseringsprotokoll i följande avsnitt. Här görs en uppdelning i autentisering av användare resp. system för att tydliggöra hur protokollen typiskt tillämpas för respektive användningsområde. Dock baseras ofta dessa på gemensamma grundläggande algoritmer och protokoll.

### 6.5.4 Protokoll för autentisering av användare

Detta avsnitt innehåller ett urval av rekommenderade protokoll för autentisering av användare.

#### 6.5.4.1 Mutual-TLS med x.509-certifikat

Med hjälp av en säker bärare för x.509-certifikat och tillhörande privata nyckelmaterial (till exempel ett chip-försett smart kort) kan en användare autentiseras typiskt med två faktorer (tillgång till bäraren samt en kod eller dylikt). Protokollet mellan klienten och autentiseringstjänsten är Mutual-TLS, dvs. både klient och autentiseringstjänst verifierar den andra partens certifikat kryptografiskt.

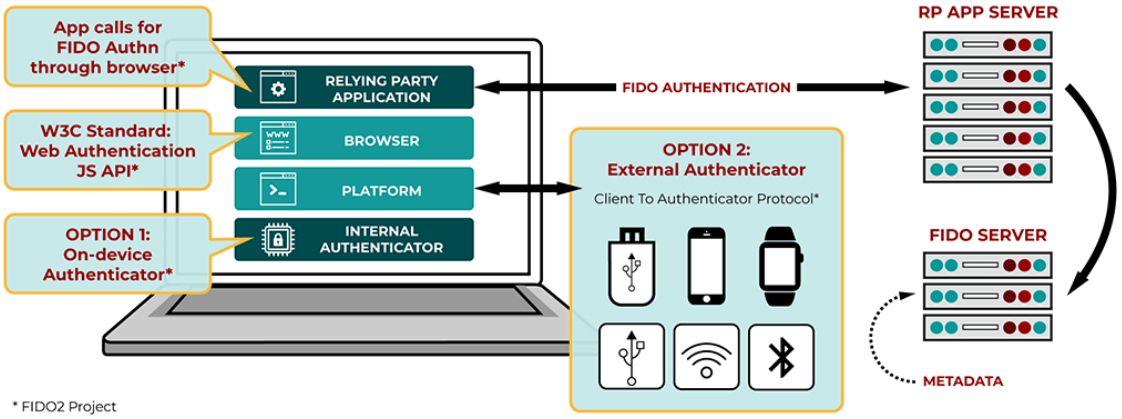
Normalt sker användaridentifieringen kopplat till visst attribut i certifikatet och certifikaten måste kontrolleras avseende spärr och giltighetstid.

#### 6.5.4.2 FIDO2

FIDO2 består av två primära publikt specificerade delprotokoll:

- *Web Authentication* (*W3C*)[51], ett standardiserat webb-api för kommunikation mellan klient och autentiseringstjänst.
- *Client-to-Authenticator Protocol* (*CTAP*, *FIDO Alliance*)[52], ett standardiserat api på klienten för kommunikation med extern bärare för användarens e-id.

FIDO2 möjliggör att användaren kan autentiseras med en eller flera faktorer med hjälp av en certifierad bärare efter att användaren registrerat sin identitet och knutit bäraren till denna.




De olika delarna i en FIDO/FIDO2-baserad lösning kan certifieras av FIDO Alliance: bäraren för e-id, klientprogrammet respektive autentiseringstjänsten.

#### 6.5.4.3 FIDO UAF (CTAP1)

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

[51] https://www.w3.org/TR/webauthn-2/
[52] https://fidoalliance.org/specifications/


*Figur 56. UAF principiell användarupplevelse (källa: FIDO Alliance)*

#### 6.5.4.4 FIDO U2F (CTAP1)

*U2F* (*Universal Second Factor*) även kallad *CTAP1* – erbjuder användaren att använda en certifierad bärare 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/CTAP1-kompatibel bärare.


*Figur 57. U2F principiell användarupplevelse (källa: FIDO Alliance)*

En bärare som stödjer U2F/CTAP1 kan även integreras i en FIDO2-lösning.

Notera: FIDO-specifikationerna adresserar inte processen för hur e-legitimationen/bäraren knyts till användaren som erhåller en e-legitimation. En lösning behöver därför kompletteras med en separat legitimeringskanal, antingen fysisk eller elektronisk, för att identifiera användaren i enlighet med den nivå av tillit man önskar uppnå på e-legitimationen.
Exempel på detta är att använda mönstret för ärvd legitimering (kap. 5.6.3) i samband med registreringen av FIDO-kompatibel autentiseringslösning.

### 6.5.5 Protokoll för autentisering av system

Detta avsnitt innehåller ett urval av rekommenderade autentiseringsprotokoll för system-system-kommunikation.

#### 6.5.5.1 Mutual-TLS med x.509-certifikat

Systemen lagrar här varsin privat nyckel skyddat. X.509-certifikat utfärdas till systemen baserat på motsvarande publika nyckel. Ömsesidigt förlitande till certifikatutfärdaren (eller det specifika certifikatet) konfigureras in i klient- resp. serversystemen.

Protokollet mellan klientsystemet och serversystemet är Mutual-TLS, dvs. både klient och server verifierar den andra partens certifikat kryptografiskt.
Certifikaten kontrolleras avseende spärr, giltighetstid och godkänd utfärdare.

Identifieringen av klientsystemet kan ske kopplat till visst attribut i certifikatet, alternativt knyts hela certifikatet mot systemidentiteten (certifikatspinning).

#### 6.5.5.2 Digital signatur över standardiserad token

Systemen lagrar också här varsin privat nyckel skyddat. Klientsystemets publika nyckel registreras (”publik nyckel-registrering” enligt kap. 5.9.1) hos förlitande part, antingen hos serversystemet direkt eller via en federativ funktion som flera tjänster litar på.

Protokollet mellan klientsystemet och serversystemet omfattar skapande och verifiering av en digital signatur över en standardiserad token och kan till exempel utgöras av

- *private_key_jwt*[53], där token är en signerad *JSON Web Token* (*JWT*). Metoden rekommenderas för OAuth2-baserade protokoll.
- *PKCS#7 Cryptographic Message Syntax (CMS)*[54].

Notera att autentiseringsprotokollet normalt kombineras med kryptering av transportprotokollet, typiskt realiserat med TLS.

[53] Se *RFC 7523 - JWT Profile for OAuth 2.0 Client Authentication and Authorization Grants*
[54] https://en.wikipedia.org/wiki/PKCS_7

## 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. IdP:er (Identity Providers), e-tjänster (Service Providers/Relying Parties) samt eventuella stödtjänster (till exempel 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*[55]
  - För OIDC: *OIDC Federation 1.0*[56]
- Hantering av metadata styrs av
  - För SAML 2.0: *OASIS SAML 2.0 Metadata Interoperability Profile*[57]
  - För OIDC: *OIDC Federation 1.0*

[55] https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
[56] https://openid.net/specs/openid-connect-federation-1_0.html. **Not:** implementers draft, ej fastställd standard
[57] https://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 fråga-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 kvalitetssäkrade 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[58]
  - SCIM stödjer både mönster för pull (GET) och push (POST).

[58] https://tools.ietf.org/html/rfc7644

- SPML 2.0 (eller senare)[59], andrahandsval.
  - "SPMLv2 XSD Profile" för anpassning till XML och SOAP.

[59] https://www.oasis-open.org/standards#spmlv2.0

# 7 Bilaga: Förkortningar

Förteckning över ett urval använda förkortningar/beteckningar.

| | |
|---|---|
| FIDO | *FIDO Alliance* är en icke vinstdrivande organisation med syfte att adressera interoperabilitet och användbarhet för autentiseringslösningar.<br>https://fidoalliance.org |
| HTTP | *Hypertext Transfer Protocol*.<br>Kommunikationsprotokoll ovanpå TCP (*Transmission Control Protocol*) |
| IAM | *Identity & Access Management*, Identitets- och åtkomsthantering |
| IANA | Internet Assigned Numbers Authority<br>http://www.iana.org |
| IdP, OP | *Identity Provider*, *OpenID Provider*.<br>Legitimeringstjänster inom SAML resp. OIDC. |
| IWA | *Integrated Windows Authentication.*<br>https://en.wikipedia.org/wiki/Integrated_Windows_Authentication |
| JSON | *JavaScript Object Notation*, ett kompakt, textbaserat format som används för att utbyta data.<br>https://sv.wikipedia.org/wiki/JSON |
| JWT | *JSON Web Token*, JSON-baserad öppen standard (RFC 7519) för skapande av åtkomst- och identitetsintyg (tokens). |
| REST | *Representational State Transfer (REST)* är ett IT-arkitekturbegrepp som beskriver ett sätt hur tjänster för maskin till maskin-kommunikation kan tillhandahållas.<br>https://sv.wikipedia.org/wiki/Representational_State_Transfer |
| SSO | *Single sign-on*, Singelinloggning |
| SLO | *Single Logout*, Singelutloggning |
| SOAP | XML-baserat protokoll för utbyte av information i distribuerade miljöer<br>https://sv.wikipedia.org/wiki/SOAP |

| | |
|---|---|
| OIDC | *OpenID Connect*, OpenID Foundation<br>https://openid.net |
| OAuth2 | Protokoll för delegerad åtkomst och auktorisation. Används även som underliggande protokoll för OIDC.<br>https://oauth.net/2/ |
| PAP | *Policy Administration Point*<br>https://en.wikipedia.org/wiki/Attribute-based_access_control |
| PEP | *Policy Enforcement Point*<br>https://en.wikipedia.org/wiki/Attribute-based_access_control |
| PDP | *Policy Decision Point*<br>https://en.wikipedia.org/wiki/Attribute-based_access_control |
| PIP | *Policy Information Point*<br>https://en.wikipedia.org/wiki/Attribute-based_access_control |
| PKCS | *Public Key Cryptography Standards*.<br>https://en.wikipedia.org/wiki/PKCS |
| PoP | *Proof-of-Possession,* innehavsbevis med syfte att bevisa rättmätigt innehav av en nyckel, ett åtkomstintyg eller dylikt. |
| SAML2 | *Security Assertion Markup Language 2.0*<br>https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language |
| SCIM | *System for Cross-domain Identity Management*.<br>https://en.wikipedia.org/wiki/System_for_Cross-domain_Identity_Management |
| SPML | *Service Provisioning Markup Language*<br>https://en.wikipedia.org/wiki/Service_Provisioning_Markup_Language |
| SP, RP | *Service Provider* resp. *Relying Party*.<br>Beteckning på e-tjänst inom SAML resp. OIDC som tar emot intygade uppgifter om vem användaren är och dennes egenskaper (*identitetsintyg*) i syfte att kunna logga in användaren i e-tjänsten. |
| TLS | *Transport Layer Security*, öppen standard för säkert utbyte av krypterad information mellan datorsystem<br>https://sv.wikipedia.org/wiki/Transport_Layer_Security |

| | |
|---|---|
| UAF | *Universal Authentication Framework*.<br>Publik specifikation för autentisering från FIDO Alliance. |
| U2F | *Universal Second Factor.*<br>Publik specifikation för autentisering från FIDO Alliance. |
| URI, URL | *Uniform Resource Identifier*, *Uniform Resource Locator*<br>https://datatracker.ietf.org/doc/html/rfc3986 |
| XML | *Extensible Markup Language*, ett standardiserat utbyggbart märkspråk<br>https://sv.wikipedia.org/wiki/XML |

# 8 Bilaga: Symboler

Nedan beskrivs några ofta förekommande symboler i dokumentets bildmaterial.

| | |
|---|---|
|  | Tillhandahåller en funktionellt avgränsad systemtjänst |
|  | E-tjänst (IT-tillämpning/applikation) |
|  | Datakälla |
|  | I arkitekturbeskrivning över samverkande tjänster:<br>indikerar kommunikation mellan samverkande komponenter. Komponenten varifrån pilen utgår initierar kommunikationen.<br><br>I flödesbeskrivningar: indikerar flödesriktning (A leder till B) |
|  | Variant av kommunikation mellan samverkande komponenter där kommunikationen inte behöver vara en teknisk del av det övriga kommunikationsmönstret. Kommunikationen kan t.ex. gå ”out-of-band” eller vara ett manuellt steg. |
|  | Indikerar en relation mellan samverkande komponenter (utan specificerat kommunikationsmönster). |
|  | Indikerar ett flöde av information från en komponent till en annan. |
|  | Användare (fysisk person) |
|  | Klientenhet – begrepp som refererar till datorer, mobila enheter och andra fysiska enheter som användare nyttjar för att nå IT-resurser |
|  | Elektronisk identitetshandling (e-id / e-legitimation) |
|  | Fysisk identitetshandling |

| | |
|---|---|
|  | Identitetsintyg resp. åtkomstintyg |
|  | Elektroniskt certifikat |
|  | Nyckelmaterial för kryptografiska funktioner med publik och privat nyckel. |