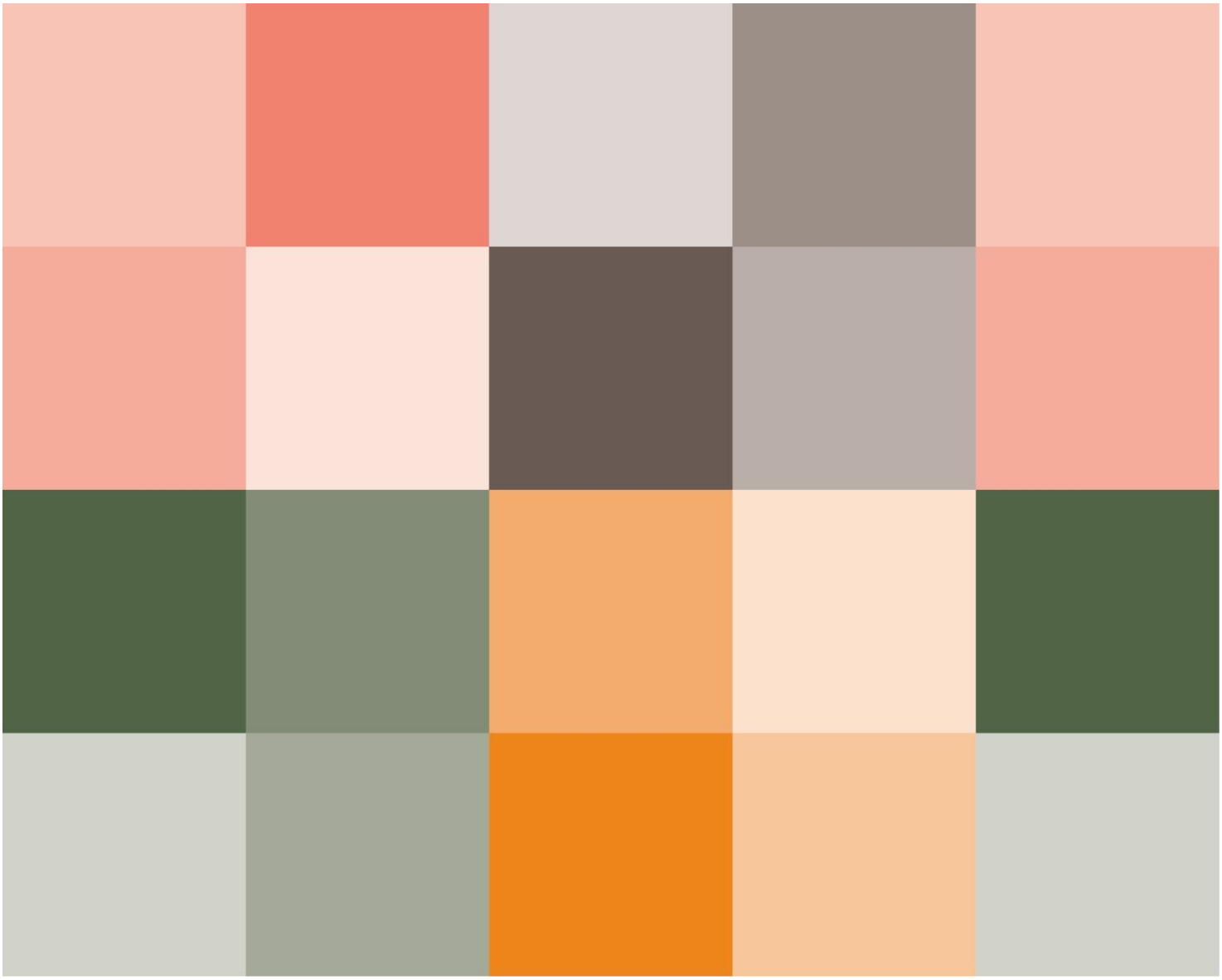


Auktorisation

Byggblocksbeskrivning

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Byggblocket Auktorisation tillhör byggblockskategorin Tillit och säkerhet som möjliggör standardiserade digitala funktioner för säkert informationsutbyte och syftar till att stödja byggblock i kategorin Digitala tjänster, Informationsutbyte och Informationshantering. Byggblocket Auktorisation omfattar digital infrastruktur och tjänster för att säkert och digitalt kunna auktorisera människor, organisationer och smarta saker.

Viktiga aktiviteter i närtid:

- Delta i framtagandet av en referensarkitektur som beskriver informationsutbyte inom den digitala infrastrukturen med stöd av både identitet (autentisering) och åtkomst (auktorisation)
- Möjliggöra auktorisation av
    - privatpersoner
    - medarbetare över organisationsgränser
    - ombud i digitala tjänster
    - organisationer

Innehållsförteckning

1 Auktorisation

	Utveckling	Förvaltning
Färdledande myndighet	DIGG	DIGG
Samverkande myndigheter	DIGG	DIGG

1.1 Övergripande beskrivning

Auktorisation innebär behörighetskontroll dvs att kontrollera vad en identifierad aktör kan/får göra/utföra. Att kontrollera om en aktör är behörig att ta del av information eller använda en funktion (resurs). En resurs kan t.ex. vara en e-tjänst eller ett API.

Aktörer definieras inom byggblocket Identitet som människor, organisationer och smarta saker. Människor inom ramen för den digitala infrastrukturen agerar främst i rollen som (externa) konsumenter av information och tjänster. Organisationer och smarta saker kan agera både som konsumenter och producenter av information och tjänster.

Beslutet att ge en användare åtkomst till en resurs ligger hos resursen själv. En behörighetskontroll bör göras när användaren vill få tillgång till en resurs och vilken behörighetskontroll som bör göras är beroende av vilken resurs användaren vill få tillgång till.

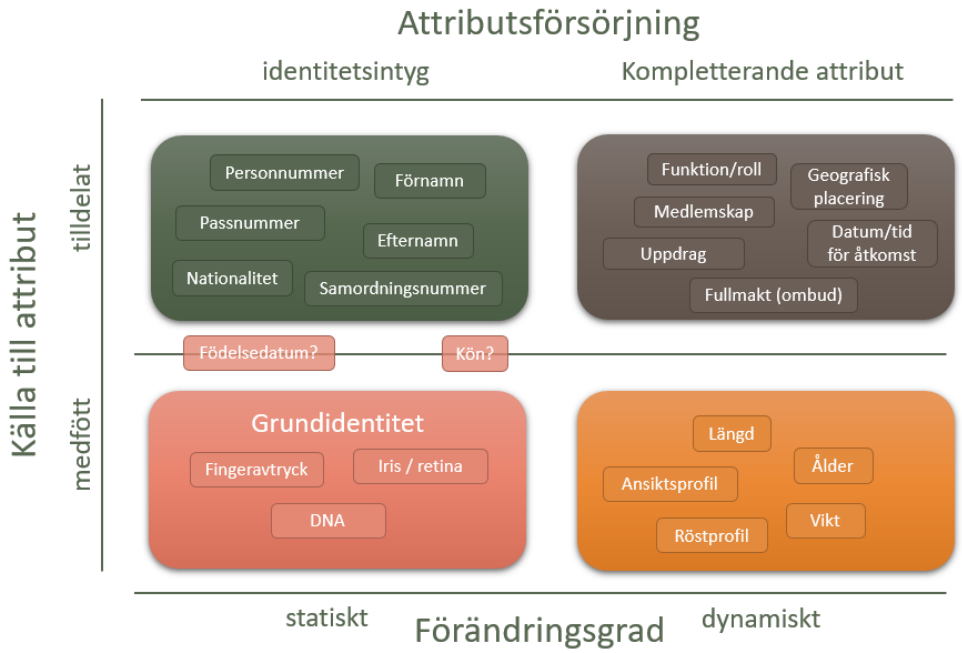
Tillgång till aktuell behörighetsinformation är centralt för kontrollera om en användare ska få tillgång till, och vilken typ tillgång till, en digital tjänst.

För att enskilda resurser själv ska kunna göra en behörighetskontroll behövs möjligheter att inhämta attribut om användaren som ska ligga till grund för beslutet att tillåta åtkomst eller inte.

Exempel på vad behörigheter för människor kan baseras på:

- Grunddata, tex vilken funktion eller roll en användare har inom ett företag

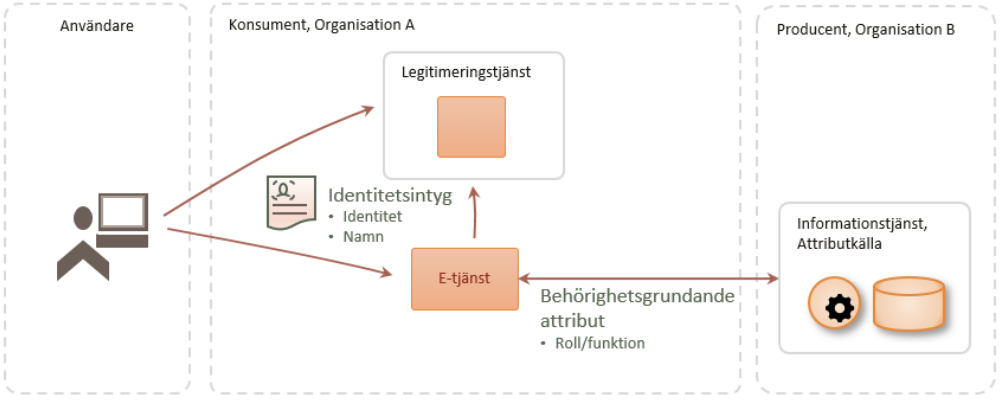
- Anställning, tex vilken roll eller vilka uppdrag en användare har blivit tilldelade av sin arbetsgivare
- Fullmakter, tex om användaren är ombud för ett företag



Figur 1 - Exempel på behörighetsgrundande attribut för människor

Exempel på olika fall när människor eller organisationer behöver auktoriseras och olika källor för behörighetsgrundande information.

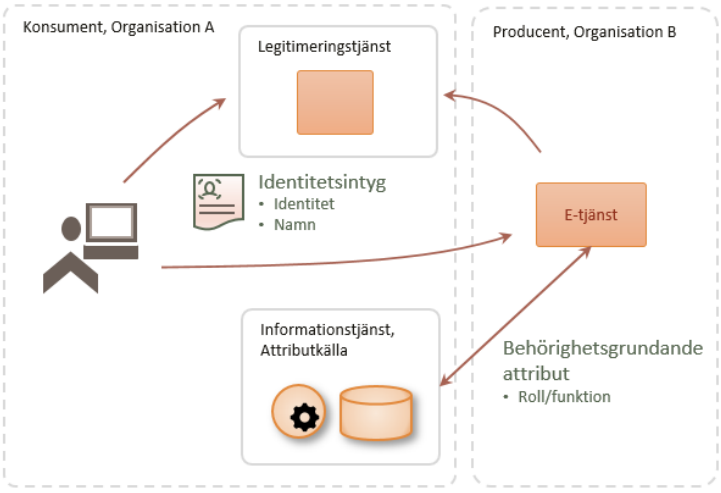
1. Privatperson – organisation



Figur 2 - Behörighetsinformation baseras på grunddata

En privatperson och använder en e-tjänst som tillhandhålls av en organisation, tex en myndighet, gör detta som regel för att hantera information som rör dem själva. I många av dessa fall räcker det oftast att autentisera personen och ingen ytterligare auktorisation behövs. Men ofta behöver e-tjänsten inhämta fler behörighetsgrundande attribut. Exempelvis en användares roll eller funktion i ett företag eller om användaren är registrerad som vårdnadshavare.
Attribut som ofta hanteras av en annan myndighet än den myndighet som tillhandahåller e-tjänsten.

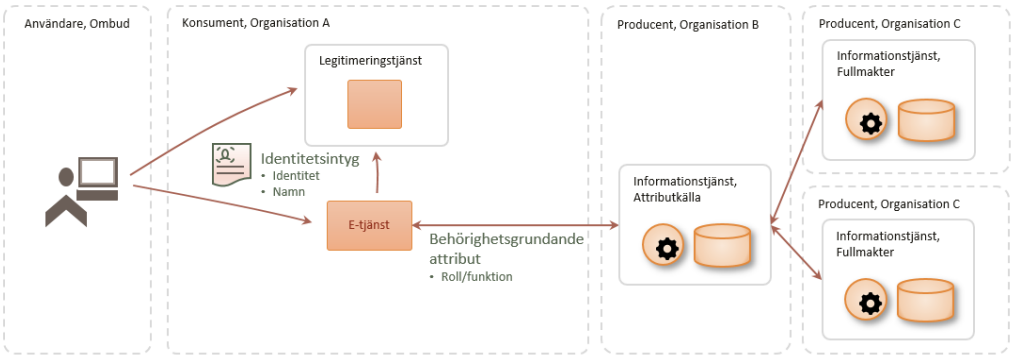
2. Medarbetare – organisation



Figur 3 - Behörighetsinformation baseras på tex roller, uppdrag som är tilldelade arbetsgivaren

En medarbetare som använder en e-tjänst tillhörande en annan organisation för att genomföra sina arbetsuppgifter. I detta fall räcker det inte med att bara autentisera användaren utan e-tjänsten behöver komplettera med ytterligare uppgifter tex arbetsgivare, roll eller uppdrag, för att göra den behörighetskontroll som behövs.

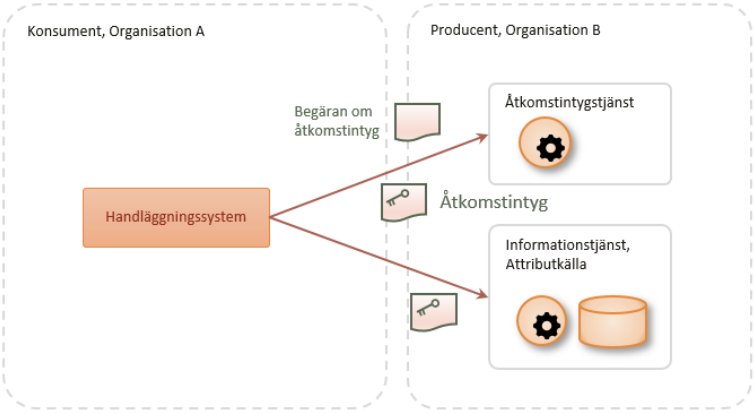
3. Ombud – organisation



Figur 4 - Behörigheterna baseras fullmakter som användaren har fått av tex ett företag som användaren är ombud för

En användare har blivit tilldelad en fullmakt och loggar in i en e-tjänst för att agera ombud åt en juridisk person. I det här fallet kan det behövas sammansatta tjänster för att sammanställa behörighetsinformation från flera olika källor.

4. Organisation – organisation



Figur 5 - Behörighetsinformation hanteras av den organisation som tillhandahåller tjänsten

En organisation använder en annan organisations API:er vid system- till systemkommunikation.

1.2 Målbild

Visionen för byggblocket är att det ska vara enkelt och säkert att genomföra en behörighetskontroll av en aktör som vill använda en tjänst inom den digitala infrastrukturen.

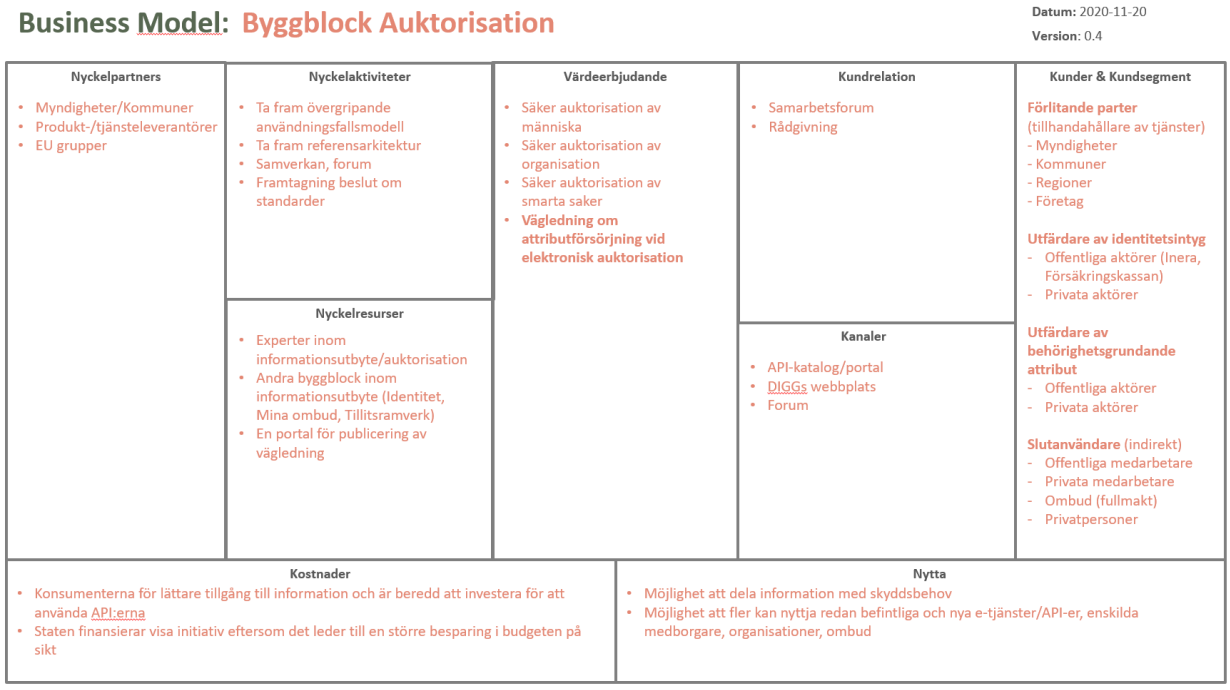
Inom den digitala infrastrukturen ska det vara:

- Enkelt att hitta information om behörighetstjänster
- Enkelt att ingå avtal med andra aktörer
- Enkelt att integrera med andra aktörer
- Enkelt att utveckla nya och förvalta redan befintliga tjänster

För att nå målbilden har byggblocket tagit fram ett antal värdeerbjudanden.

1.2.1 Värdeerbjudanden (BMC)

En översiktstavla enligt modellen Business Model Canvas (BMC)[1] har tagits fram för att visualisera och tydliggöra byggblockets olika värdeerbjudanden för aktuella kundsegment



Figur 6 - Business Model Canvas (BMC)

Värdeerbjudanden som finns nu eller inom två år:

1. Säker auktorisation av människor
    - Privatpersoner
    - Medarbetare

[1] https://www.strategyzer.com/canvas/business-model-canvas

- Ombud

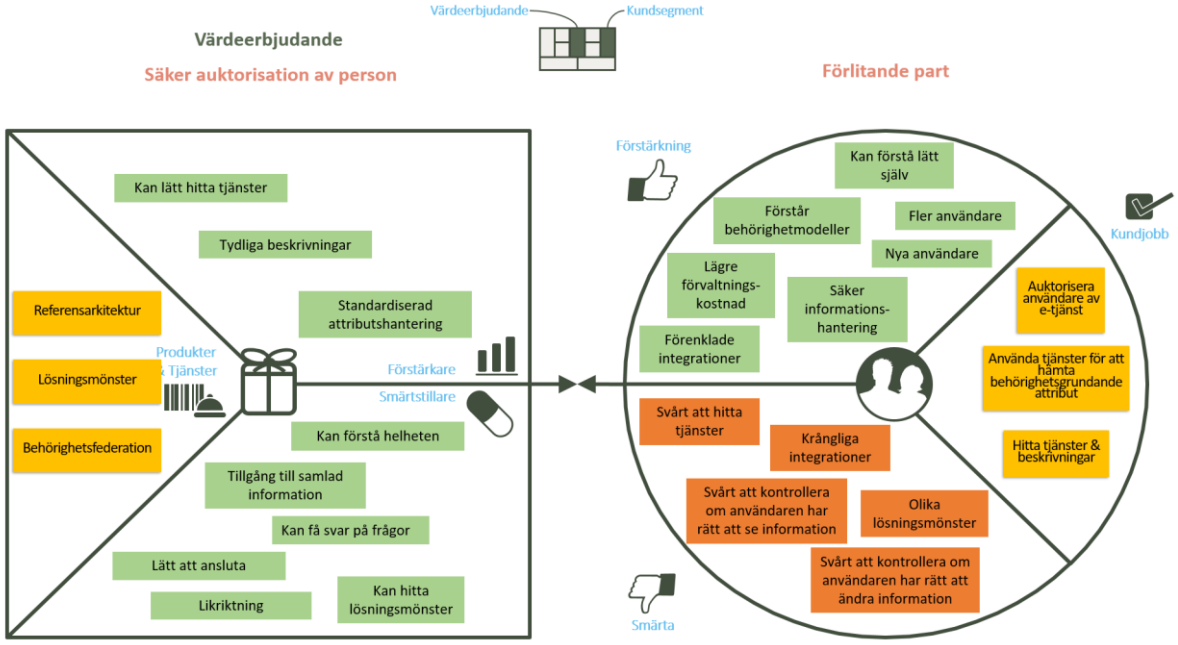
2. Säker auktorisation av organisationer
3. Vägledning om attributsförsörjning vid elektronisk auktorisation

Värdeerbjudanden som kan komma på längre sikt:

- Säker auktorisation av smarta saker

1.2.2 Värdekartor (VPC)

Varje värdeerbjudande i BMC-modellen kan detaljeras i en s.k. värdekarta (Value Proposition Canvas, VPC[2]). Värdekartan beskriver hur ett visst värdeerbjudande består av produkter och tjänster inom byggblocket som matchar behov hos ett visst kundsegment som är identifierat för byggblocket.

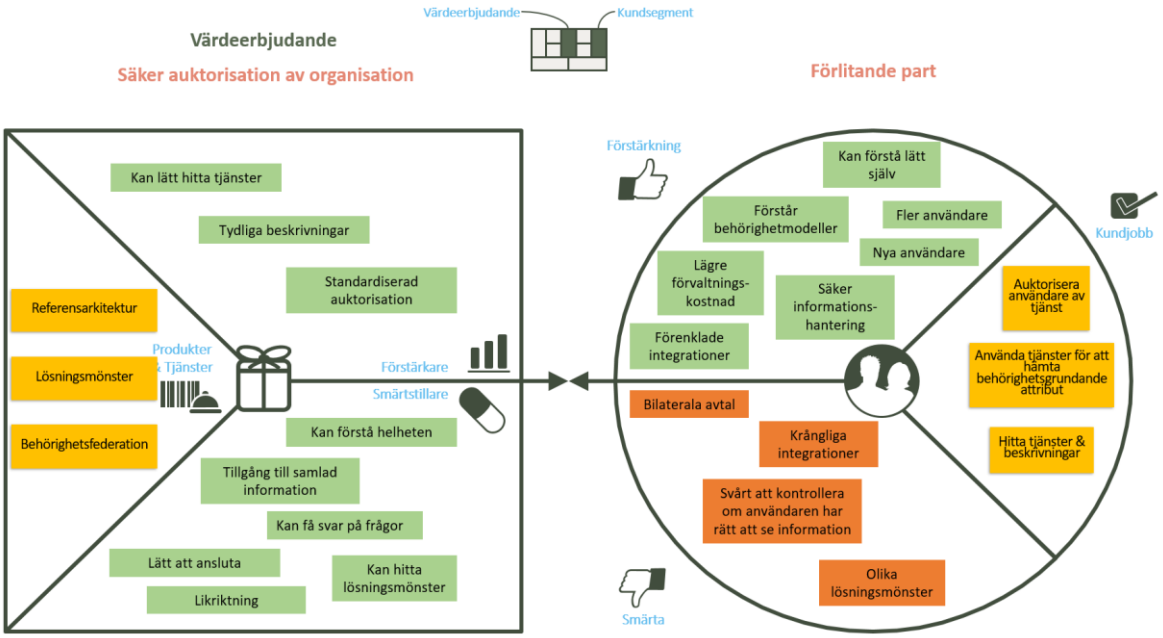


Figur 7 - VPC Säker auktorisation av person

Att genomföra en behörighetskontroll kan vara krångligt, det finns många olika typer av information som behörigheter kan baseras på, tex grunddata, anställning eller fullmakter. Det innebär att integrationer kan behöva göras med många olika parter, vilket kan innebära många olika avtal.

[2] https://www.strategyzer.com/canvas/value-proposition-canvas

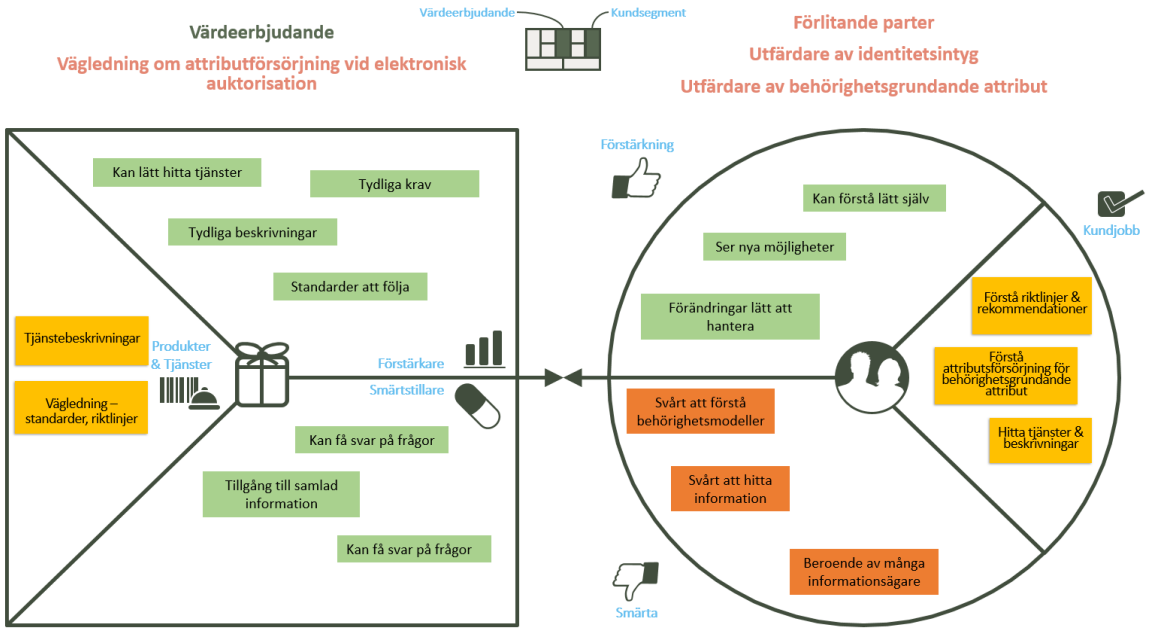
För att underlätta för organisationer att auktorisera användare i sina e-tjänster behövs likriktning inom den digitala infrastrukturen.



Figur 8 - VPC Säker auktorisation av organisation

Det finns ett stort behov inom den inom den digitala infrastrukturen att kunna auktorisera andra organisationer. Och på samma sätt som för auktorisation av människor kan innebära det integrationer med många olika parter.

Även här behövs likriktning för att underlätta informationsutbyte mellan organisationer.



Figur 9 - VPC Vägledning om attributsförsörjning

För att kunna genomföra en säker auktorisation av både människor och organisationer behövs väl strukturerad behörighetsinformation. Inom den digitala infrastrukturen kommer med stor sannolikhet mycket av informationen vara distribuerad. Det innebär att det behövs tydlig vägledning i form av riktlinjer, regelverk och standarder, om hur digitala tjänster ska försörjas med behörighetsgrundande information.

Produkter och tjänster nu och inom två år:

1. En referensarkitektur som beskriver informationsutbyte med stöd av både identitet (autentisering) och åtkomst (auktorisation) för aktörer som deltar i den digitala infrastrukturen

   Referensarkitekturen behövs för att uppnå
   - Interoperabilitet
   - Skalbarhet
   - Flexibilitet

Referensarkitekturen är till för att både konsumenter och producenter få stöd i utvecklingen av nya, eller integrationer mellan redan etablerade, tjänster.

2. Väl beskrivna lösningsmönster ingår som en del i referensarkitekturen för att beskriva särskilda auktorisationsflöden mellan en konsument och en producent. Lösningsmönstren ska tydligt beskriva vem som är ansvarig för att genomföra auktorisation

3. En eller flera behörighetsfederationer. Syftet är att federationerna ska hålla reda på information om alla tekniskt anslutna parter. De ska även hjälpa medlemmar att identifiera och auktorisera andra medlemmar, och kan även innehålla den information som krävs för att etablera teknisk anslutning till olika parter.

På längre sikt ser också ut att finnas behov av

- Stöd för anonymisering och pseudonymisering
- Att öppna upp delar av den digitala infrastrukturen för privat sektor
- Tillhandhålla förvaltningsgemensamma tjänster för auktorisation
- Tillhandhålla för digitala behörigheter över landsgränser, tex EU:s SEMPER-initiativ

1.3 Målgrupper och införandestrategi

Målgrupper för byggblock Auktorisation är:

1. offentlig förvaltning (primär målgrupp)
2. privatpersoner och företag som användare
3. leverantörer, däribland privata och offentliga eID-utfärdare
4. privat sektors på eID förlitande aktörer

1.4 Avgränsningar

Hur behörigheter för smarta saker ska hanteras inom den digitala infrastrukturen är en fråga som behöver hanteras i fortsatt vidareutveckling av byggblock inom Tillit och säkerhet.

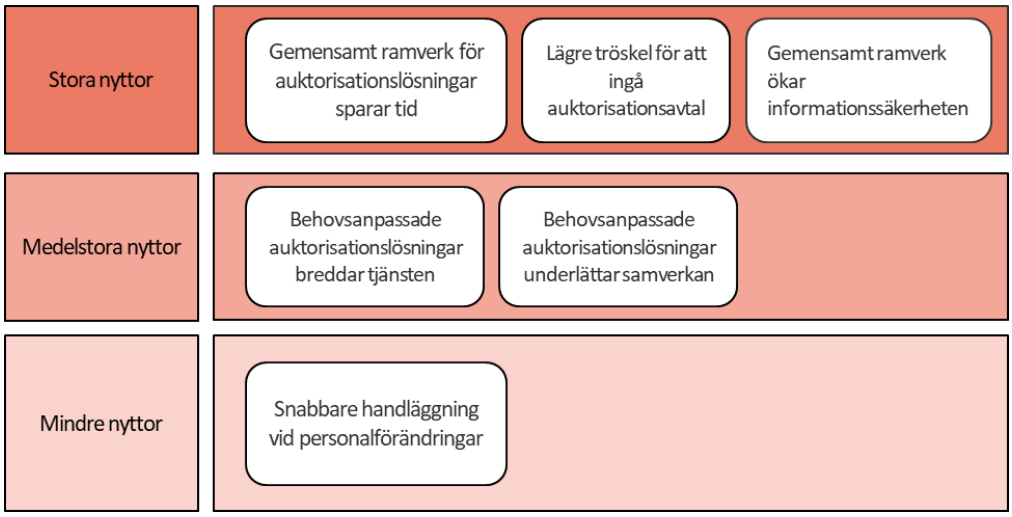
2 Nyttoanalys

2.1 Beskrivning av identifierade nyttor

Auktorisation skapar nyttor främst för offentlig sektor, men även för företag och medborgare. Nyttorna uppstår framförallt genom tidsbesparingar för offentliga aktörer genom att de exempelvis kan ansluta till ett avtal kopplat till en auktorisationslösning istället för att ta fram ett eget avtal. Auktorisation skapar också i stor utsträckning nyttor i andra byggblock genom att erbjuda ett gemensamt ramverk för auktorisation.

Eftersom byggblocket Auktorisation är i ett tidigt utvecklingsskede är det inte möjligt att kvantitativt beräkna hur stora nyttorna kommer bli. Vi har därför som ett första steg uppskattat den inbördes storleksordningen för nyttorna inom byggblocket. Men i dagsläget ligger det inga beräkningar bakom dessa uppskattningar. Det saknas därför en specifik uppskattning av storleken på nyttorna. I vilken storleksordning som nyttorna befinner sig, relativt varandra, redovisas i **Error! Reference source not found.** nedan. För utförligare beskrivning av genomförandet hänvisas till Metodbilagan[3].

Figur 10: Uppskattat storleksintervall med rangordning av samtliga nyttor



[3] Nyttoanalysens metodbilaga, Slutrapportens bilagor, https://www.digg.se/informationsutbyte-och-grunddata

2.2 Nyttor i form av tids- och kostnadsbesparingar

De främsta tid- och kostnadsbesparingarna som kommer realiseras handlar om anslutning till nationella ramverk och auktorisationslösningar. Då byggblocket än så länge är i en tidig utvecklingsfas har konkreta uppskattningar av nyttan inte kunnat göras.

2.2.1 Gemensamt ramverk för auktorisationslösningar sparar tid

Ett gemensamt ramverk för auktorisationslösningar sparar tid vid uppdatering av lagändringar eller liknande. Istället för att alla som har bilaterala auktorisationsavtal ska uppdatera sina egna avtal så kan det standardiserade avtalet eller ramverket för auktorisationslösningen uppdateras centralt. De aktörer som vill ha auktorisationsavtal med andra aktör behöver heller inte lägga tid på att skapa ett eget avtal när det finns ett gemensamt ramverk för auktorisationslösningar. Dessa tidsbesparingar förväntas tillfalla offentlig sektor.

2.2.2 Lägre tröskel för att ingå auktorisationsavtal

Tröskeln för att ingå auktorisationsavtal blir lägre när det finns färdiga nationella och behovsanpassade ramverk. Kostnaden blir lägre för att ingå ett avtal till följd av tidigare nämnda tidsbesparingar kopplade till formulering av avtal. Nyttan följer av att det blir en lägre tröskel för att ingå avtal där information kan delas, ändras eller visas för externa, privata eller offentliga aktörer. Nyttan som skapas av detta förväntas främst tillfalla offentlig sektor.

2.2.3 Snabbare handläggningar vid personalförändringar

Vid personalförändringar i offentlig sektor blir auktorisation som inte är baserad på grunddata lättare att hantera. Detta då auktorisationen istället baseras på tillgång till en tjänst för en tjänsteman snarare än tillgång till grunddata. Detta beräknas leda till tidsbesparingar för offentlig sektor och företag.

2.2.4 Nyttornas storlek är svåra att uppskatta

Eftersom detta byggblock är i ett tidigt utvecklingsstadium är det svårt att kvantitativt uppskatta hur stora nyttorna kommer bli. Nyttorna är också i mångt och mycket indirekta, det vill säga de är realiserbara i förhållande till andra byggblock eller i förhållande till det offentliga digitala ekosystemet som helhet. Det innebär att även om nyttorna var möjliga att beräkna i dagsläget så skulle de verka små om de begränsas till att omfatta endast byggblocket.

2.3 Nyttor i form av bättre tjänster och nya användningsområden

Auktorisation som byggblock ger i första hand en högre informationssäkerhet genom att standardisera funktionalitet och regelverk för behörighet till information. Byggblocket möjliggör också för större samverkan med offentlig sektor genom att skapa olika behovsanpassade lösningar.

2.3.1 Gemensamt ramverk för auktorisationslösningar ökar informationssäkerheten

Ett gemensamt ramverk för auktorisationslösningar ger en säkrare och mer korrekt digital säkerhet. Detta innebär inte att specifika auktorisationslöningar behöver se likadana ut, utan det handlar om en standard som ska uppfyllas för att täckas av det gemensamma ramverket. Med den typen av standard blir alla auktoriseringslösningar som ingår i det gemensamma ramverket säkra och korrekta. Detta förväntas skapa kvalitativa nyttor genom ökad säkerhet.

2.3.2 Behovsanpassade auktorisationslösningar breddar tjänsten och underlättar samverkan

Ett gemensamt ramverk för auktorisationslösningar möjliggör olika typer av säkra lösningar som är anpassade efter de behov som finns inom offentlig sektor. Ett gemensamt ramverk fungerar som en grund för företag att utveckla tjänster som kräver olika typer av auktorisation för att fungera. Exempelvis blir det enklare för ett företag att utveckla en applikation som kräver auktorisation mot en offentlig aktör. Ett gemensamt ramverk fungerar således som en möjliggörare för auktorisationsbaserad innovation. Det gemensamma ramverket gör det även enklare för offentlig sektor att samverka med företag. Detta då det blir enklare att ta fram avtal som berör auktorisering enligt en tillförlitlig, säker och standardiserad mall. Detta förväntas leda till nyttor genom ökad kvalitet och fler användningsområden.

2.4 Potential för ytterligare nyttor

Utöver de nyttor som redogjorts för ovan kommer Auktorisation kunna skapa flera nyttor. Men dessa nyttor kräver aktiviteter och funktioner som ligger dock långt fram tiden och är än så länge på ett idéstadium. Vi har därför valt att inte uppskatta storleksordningen på dessa nyttor.

2.4.1 Utveckling av auktorisationslösningar

För att ytterligare förenkla anslutning till auktorisationslösningar kan det komma att skapas federationer kring lösningar. Federationerna är då anpassade efter respektive auktorisationslösning vilken i sin tur är behovsanpassad efter vad som

efterfrågas gällande auktorisation inom offentlig sektor. Detta skulle kunna skapa nyttor genom ökad kvalitet.

2.4.2 Regelverk med öppen källkod

Det kan komma att skapas ett regelverk för öppen källkod som är tillgänglig för digitalt erfarna aktörer att ansluta till. Regelverket berör då respektive auktorisationslösning. Detta skulle underlätta anslutning och sänka förvaltningskostnader. Denna funktion skulle då skapa nyttor genom tids- och kostnadsbesparingar.

2.4.3 Utveckling av behörighetssystem

Behörighetssystem kan komma att utvecklas. Detta skulle säkerställa att behörighet förblir korrekt över tid, samt att auktorisation utan personnummer kan komma att bli möjligt. Detta skulle inte bara höja informationssäkerheten utan även bredda användningsområdet för byggblocket till att omfatta fler aktörer samt privata användare. Denna funktion skulle därmed skapa nyttor genom ökad kvalitet.

3 Finansieringsanalys

Kostnader består av utredningskostnader för att ta fram referensarkitektur, regelverk och riktlinjer. Utveckling- eller förvaltningskostnader för eventuella förvaltningsgemensamma behörighetstjänster är inte inkluderade.

[TSEK]	Anslag	Lån	Avgift	Bidrag	Totalt
År 1	3600	0	0	0	3600
År 2	4400	0	0	0	4400
År 3	5200	0	0	0	5200
Totalt	13200	0	0	0	13200

4 Rättslig analys

I nuvarande läge har ingen rättslig analys genomförts eftersom byggblocket fortfarande är i analysfas. Det är finns inga tillräckligt konkreta förslag på lösningar vilket har gjort att det inte varit möjligt att göra juridiska bedömningar.

5 Färdplan

5.1 Nyckelaktiviteter

5.1.1 Referensarkitektur för helheten

Tätt samarbete kring helheten för relaterade byggblock inom Tillit och säkerhet, framför allt byggblocken Identitet och Tillitsramverk men även byggblocken Spårbarhet och Tillgänglighet som i nuläget ej är startade.

5.2 Identifierade milstolpar

Nr	Beskrivning	Klart datum	Klartkriterier	Ansvarig
	Behörigheter - Grunddata Behovsanalys förvaltningsgemensamma attributskällor	2021 Q1	Behovsanalys av förvaltningsgemensam infrastruktur för behörighetsgrundande attribut	DIGG i samverkan
	Attribut och ansvariga för attributskäller identifierade	2021 Q3	Ansvarsfördelning och ägarskap utrett Juridiska förutsättningar utredda	DIGG i samverkan
	Behörigheter - eID för medarbetare	2021 Q3	Attributsförsörjning kopplat till eID för medarbetare Regelverk och riktlinjer för kompletterande attribut	DIGG i samverkan
	Behörighet för organisationer	2021 Q4	Regelverk och riktlinjer för auktorisation av organisationer	DIGG i samverkan
	Utkast till referensarkitektur	2021 Q4	Referensarkitektur ute för remiss	DIGG i samverkan

	Beslutad referensarkitektur	2021 Q4	Referensarkitekturen kommunicerad och accepterad	DIGG i samverkan
	Behörigheter – Fullmakter	2021-2022	Attributsförsörjning kopplat till fullmakter Regelverk och riktlinjer för kompletterande attribut	DIGG i samverkan
	Säkra API:er	2021-2022	Regelverk och riktlinjer för att implementera säkra API:er	DIGG i samverkan
	Digital infrastruktur för behörighet	2022-2023	Förvaltningsgemensamma attributstjänster för grunddata Ev. behörighetstjänst för auktorisation utomlands Ev. förvaltningsgemensamma behörighetstjänster för mindre behov	DIGG i samverkan
	Stöd till anonymisering och pseudonymisering	2022-2023	Behovsanalys genomförd	DIGG i samverkan
	Behörighet för smarta saker	2023	Behovsanalys genomförd	DIGG i samverkan

5.3 Identifierade beroenden

Beskrivning	Förslag på hantering	Ansvarig
Byggblock Identitet förutsättning för helhetslösning för nationell identitets- och behörighetshantering	Fortsatt arbete med arkitektur, säkerhet och juridik över byggblocken enligt föreslagen styrmodell.	DIGG
Byggblock Tillitsramverk förutsättning för helhetslösning för digital infrastruktur, definierar krav på konsumenter och producenter	Fortsatt arbete med arkitektur, säkerhet och juridik över byggblocken enligt föreslagen styrmodell.	DIGG i samverkan
Byggblock Tillgänglighet förutsättning för nationella standarder för tillgänglighet och servicenivåavtal (SLA) som påverkar kvalitetskrav på nationella behörighetstjänster inom den digitala infrastrukturen.	Förutsättningsskapande byggblock Tillgänglighet ej startat. Initiera utveckling i samverkan med byggblock Identitet.	DIGG
Byggblock Spårbarhet förutsättning för nationella standarder för spårbarhet och gemensam logghantering och logguppföljning som påverkar kvalitetskrav för nationell behörighetshantering.	Förutsättningsskapande byggblock Spårbarhet ej startat. Initiera utveckling i samverkan med byggblock Identitet.	DIGG
Byggblock API-hantering förutsättning för API-standarder för behörighetshantering, provisionering och attributförsörjning.	Fortsatt arbete med arkitektur, säkerhet och juridik över byggblocken enligt föreslagen styrmodell.	DIGG

Byggblock API-hantering skapar även förutsättningar för auktorisation av organisationer och smarta saker		

6 Risk- och konsekvensanalys

En övergripande risk- och konsekvensanalys har genomförts inom byggblocket. De identifierade riskerna och förslag på åtgärder finns dokumenterat på en skyddad lagringsyta hos DIGG.

Byggblocket påverkar den förvaltningsgemensamma digitala infrastrukturen vilket visas i den dokumenterade riskanalysen. Dokumenterade risker, sårbarheter och hot bedöms i beskrivna scenarion kunna ge konsekvenser för hela den digitala infrastrukturen och behöver analyseras vidare. Förslag till åtgärder och hantering av risker, hot och sårbarheter i riskarbete har visat sig kunna minska sannolikheten och sänka konsekvenser om risken ändå inträffar på både kort och lång sikt.

Ett fortsatt systematiskt informationssäkerhetsarbete kommer ske genom att löpande och kontinuerligt värdera sårbarheter, risker och hot inom byggblocket utifrån vilken etapp/fas byggblocket befinner sig i. Vi har även påbörjat riskarbetet av beroenden mellan byggblock inom den digitala infrastrukturen och mot grunddatadomänerna för att riskanalysera och fastställa robusthet och säkerhetsskydd för helheten i den digitala infrastrukturen.