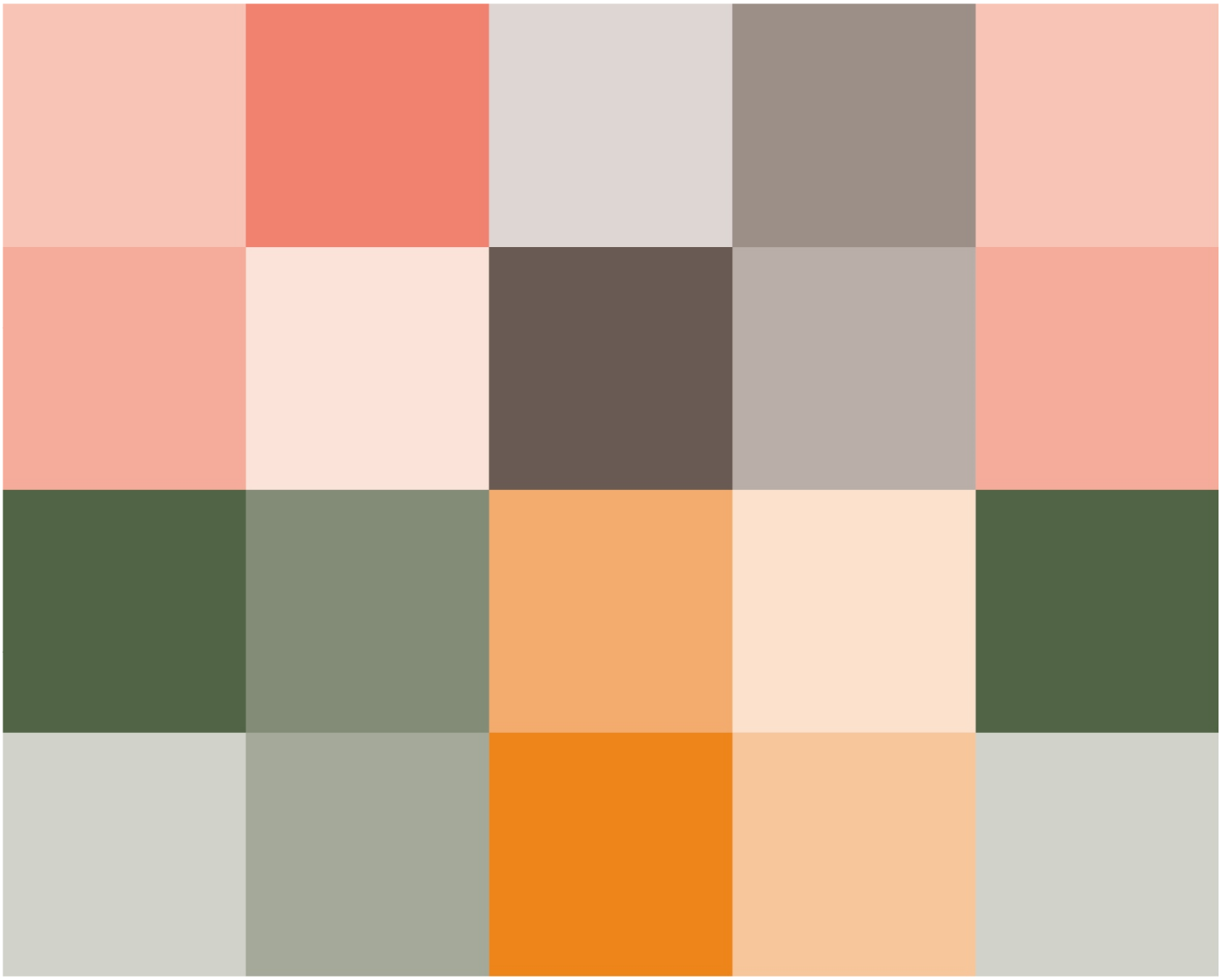


Accesspunktsoperatör – Beskrivning

Beskrivning av rollen som Accesspunktsoperatör inom Plattform för eDelivery

Version: 2022-12-09

Målgrupper: Verksamhetsutvecklare, IT-arkitekt, Leverantör

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Sammanfattande beskrivning av rollen som Accesspunktsoperatör inom Plattform för eDelivery och dess federationer

Dokumentet innehåller en övergripande beskrivning av rollen som Accesspunktsoperatör, rollens grundläggande begrepp inom ramen för Plattform för eDelivery och dess federationer.

En Accesspunktsoperatör är en tjänsteleverantörsroll för en aktör som tillhandhåller en eller flera accesspunktstjänster till en eller flera aktörer som deltar i en federation, i rollen som Deltagare.

En accesspunktstjänst är en förmedlingstjänst som tillhandhåller en accesspunkt med funktioner för utbyte av information och meddelanden mellan aktörer enligt standardiserade protokoll på ett asynkront, säkert, och tillförlitligt sätt.

En accesspunkt möjliggör utbyte av känsliga uppgifter och meddelanden som är informationssäkerhetsklassade på nivå 3, enligt MSB skala.

Plattformsansvarig ansvarar för att systematisk och ändamålsenlig *informera, engagera, kvalitetssäkra, granska, plattformsgodkänna, ansluta, kontrollera, och avveckla* accesspunktsoperatörer.

Federationens federationsägare ansvarar för att systematisk och ändamålsenlig *granska, federationsgodkänna, och ansluta* en accesspunktsoperatör till en federation samt övervaka och *kontrollera* en accesspunktsoperatörs agerande inom federationen.

Innehållsförteckning

Figurer

1 Inledning

En inledande beskrivning av rollen som Accesspunktsoperatör inom Plattform för eDelivery

Denna sektion innehåller en beskrivning av rollen som Accesspunktsoperatör (AP-operatör), rollens beståndsdelar och funktioner inom ramen för Plattform för eDelivery och dess federationer.

Rollen som Accesspunktsoperatör beskrivs utifrån verksamhetsutvecklares, IT-arkitekters och leverantörers perspektiv. Motsvarande beskrivningar av Plattform, Federation och rollen som Deltagare återfinns i dokumenten ”Plattform – Beskrivning”, ”Federation - Beskrivning” och ”Deltagare - Beskrivning”.

Vad är en Accesspunktsoperatör?

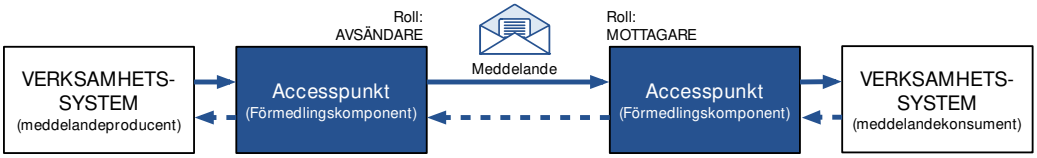
En Accesspunktsoperatör är en tjänsteleverantörsroll för en aktör som tillhandhåller och ansvarar för en eller flera accesspunktstjänster till aktörer som besätter rollen som Deltagare i en eller flera federationer.

Vad är en Accesspunktstjänst och Accesspunkt?

En *accesspunktstjänst* (AP-tjänst) är en *accesspunkt* (AP) som erbjuds som en tjänst. En AP förmedlar säkert information och meddelanden mellan aktörer enligt standardiserade protokoll, tekniska specifikationer och accesspunktens komponentspecifikation. En accesspunkt och dess funktioner implementeras av *accesspunktsprogramvara* (AP-programvara).

Vad gör en accesspunkt?

En accesspunkt utför accesspunktsfunktioner (AP-funktioner) för säker asynkron förmedling av information och meddelanden mellan aktörer enligt en 4-hörnsmodell och standardiserade gränssnitt (API).



Figur 1 Illustration av 4-hörnsmodellen med accesspunkter

En accesspunkts generella funktioner och API:er är definierade i EU:s byggblock ”eDelivery - Access Point” tillsammans med tekniska standarder för kommunikation - AS4.

En accesspunkt och dess specifika funktioner, datamängder, API och GUI specificeras och regleras i dokumentet ”*Accesspunkt - Komponentspecifikation*”.

En accesspunkt ingår i vissa transportmodeller såsom ”Bas” och Utökad Bas”. Dessa *transportmodeller* beskriver och reglerar helheten för hur en accesspunkt kan eller ska användas tillsammans med andra tjänster såsom SML och SML. Transportmodellen ”Utökad Bas” reglerar hur en AP förmedlar meddelanden som är signerade och krypterade av avsändande Deltagare.

Varje meddelande utbyts inom ramen för en federation. Ett meddelande innehåller därmed en referens till aktuell federationen. Dessutom använder en accesspunkt funktionscertifikat kopplade till federationen för att autentisera andra accesspunkter inom federationen.

[*Se respektive transportmodellspecifikation för information om hur utbytet går till*.]

Användning av accesspunkter stödjer digital samverkan med utbyte av känsliga uppgifter mellan deltagare som är informationssäkerhetsklassade på nivå 3, enligt MSB skala.

[se följande sektion med Informationssäkerhets- och tillitsmodell för mer information]

En federation kan anpassa och bygga ut plattformens ramverk, regler, rutiner, specifikationer och informationssäkerhets- och tillitmodell så att accesspunktsoperatörer kan delta i federationen.

[se federationens federationsdeklaration för detaljerad information]

Hur blir en aktör en Accesspunktsoperatör?

Plattformen och dess plattformsansvarig ansvarar för att systematisk och ändamålsenlig *informera, engagera, kvalitetssäkra, granska, plattformsgodkänna, ansluta, kontrollera, och avveckla* Accesspunktsoperatörer.

Plattformen ansvarar således främsta för att tillhandahålla *kännedom* om de aktörer som besätter rollen som Accesspunktsoperatörer.

Genom ett anslutningsförfarande organiserat av plattformsansvarig kan en aktör erhålla ett *plattformsgodkännande* som gör att aktören kan agera som Accesspunktsoperatör inom plattformen.

En federation och dess federationsägare ansvarar för att systematisk och ändamålsenlig *granska, federationsgodkänna, ansluta* en accesspunktsoperatör till en federation samt *kontrollera* en accesspunktsoperatör agerande inom en federation.

Genom ett anslutningsförfarande organiserat av en federationsägare kan en aktör erhålla ett *federationsgodkännande* som gör att aktören kan delta och agera i en federation och dess miljöer.

[se följande sektion med Anslutningsmodell för mer information]

Användningsfall för Accesspunktsoperatörer

En accesspunkt kan levereras på många olika sätt enligt gällande regler, specifikationer och transportmodeller.

[Se sektionen "För Leverantörer" för mer information om hur en accesspunkt kan levereras till en Deltagare]

1.1 Styrande regler, rutiner och avtal för accesspunktsoperatörer

Följande dokument reglerar en aktör som besätter rollen som Accesspunktsoperatör.

- *Accesspunktsoperatör – Gemensamma Regler och Rutiner*
    - Specificerar de *gemensamma* regler och rutiner som är tillämpliga för de aktörer som besätter rollen som Accesspunktsoperatör inom plattformen och i dess federationer.
- *Federationsdeklaration [FED]*
    - Specificerar *federationsspecifika* anpassningar av, tillägg till och avvikelser från "Accesspunktsoperatör - Gemensamma regler och rutiner" som en Accesspunktsoperatör ska följa efter ett federationsgodkännande.
- *Miljöspecifikation*
    - Reglerar en Accesspunktsoperatör när den agerar i en federations miljö.
- *Accesspunktsoperatör – Anslutningsresa för AP-operatör,*

    - Regleras hur en anslutning till plattformen och federationer går till.
- *Accesspunktsoperatörsavtal* med Plattformsansvarig,
    - Reglerar ansvar och skyldigheter inom Plattformen och dess federationer.
- *”Accesspunkt - Komponentspecifikation*
    - Reglerar en accesspunkt, dess funktioner, datamängder, API:er och GUI:s.
- *Transportmodellspecifikation*
    - När en Accesspunktsoperatör är plattformsgodkänd för en transportmodell ska accesspunktsoperatören följa de regler och rutiner som specificerad i relevant *transportmodellspecifikation* inom en federation.

[*Se dokumentet ”Ramverk för Plattform för eDelivery” för styrande dokument avseende andra aktörsroller*.]

1.2 Ändringshantering

Detta dokument ingår i Ramverk för Plattform för eDelivery. Ändringar i dokumentet sker enligt plattformens Ändrings och Införande process.

1.3 Målgrupper

Detta dokument syftar till att stödja följande roller och intressenter i deras arbete, dess informationsbehov samt ge svar på vanligt förekommande frågeställningar.

Intressenter:

- Verksamhetsutvecklare (business analyst)
    - Analyserar verksamheters behov av digital samverkan
    - Stödjer verksamhetsutvecklingsprojekt under dess olika faser.
    - Utvärderar ramverk, plattformar, infrastrukturer, och teknologier för digital samverkan ur ett verksamhetsperspektiv
    - Utför systematiskt och riskbaserat informationssäkerhetsarbete.
    - Kravställer utveckling av system för digital samverkan
    - Stödjer utveckling system för digital samverkan
- IT-arkitekt (lösningsarkitekt, samverkansarkitekt, infrastrukturarkitekt)
    - Utvärderar ramverk, plattformar, infrastrukturer, och teknologier för digital samverkan ur ett informationssystemperspektiv

- Utför systematiskt och riskbaserat informationssäkerhetsarbete.
- Kravställer utveckling av informationssystem för digital samverkan
- Utvärderar, analyserar, designar, och dokumenterar informationssystem
- Stödjer utveckling av informationssystem för digital samverkan
- Tar fram arkitekturer för informationssystem för digital samverkan

1.4 Referenser

Kortnamn	Länk	Kommentar
FED	Federationens federationsdeklaration	Specifika regler och rutiner som gäller för en federation
RAM	Ramverk för Plattform för eDelivery	Specifikation av ramverket
ROT	DIGG:s Ramverk för organisationstillit	

2 För Verksamhetsutvecklare

Denna sektion innehåller en anpassad beskrivning av rollen Accesspunktsoperatör för verksamhetsutvecklare

Denna sektion beskriver övergripande rollen som Accesspunktsoperatör inom plattformen och dess federationer för verksamhetsutvecklare.

2.1 Anatomi och begrepp

I denna sektion beskrivs kortfattat plattformens grundläggande anatomi och begrepp relaterade till rollen som Accesspunktsoperatör.

2.1.1 Grundläggande Anatomi

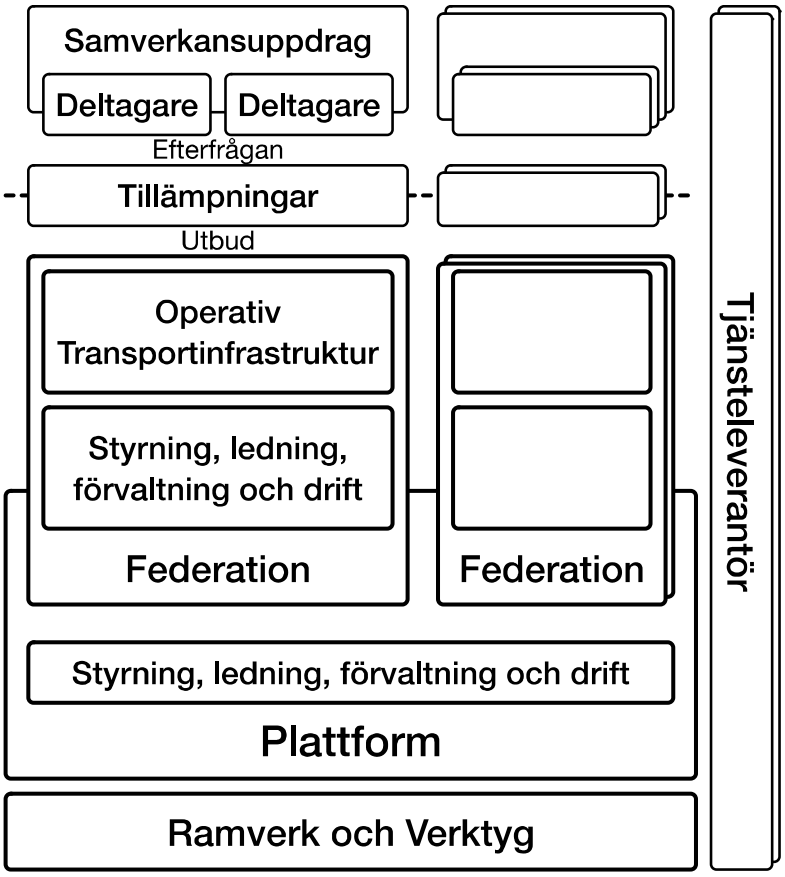
Plattformen är en *operativ*, mjukvarubaserad, centralstyrd, och utvecklingsbar basplatta som erbjuder möjligheter till värdeskapande digital samverkan och nätverkseffekter mellan aktörer inom ramen för federationer.

En federation ansvarar för att organisera en sammanslutning av självständiga och kända aktörer med *likartade och kompatibla* krav på tillit, säkerhetsåtgärder, och funktioner.

Aktörer som digitalt vill samverka inom *samverkansuppdrag* ansluter sig till en federation vilken *erbjuder* en *operativ transportinfrastruktur* med systemisk tillit, rätt säkerhet, tjänster, och tillämpningar med samverkansprocesser, meddelanden, och

transportmodeller som *tillfredsställer* aktörernas behov och krav. En till en federation ansluten aktör benämns som *Deltagare*.

Plattformen och dess federationer är baserade på ett underliggande, *gemensamt* och sammanhållet *ramverk* som anpassas av federationer för att tillfredsställa de *specifika* krav på tillit, funktioner och säkerhet som deltagare i deras samverkansuppdrag *efterfrågar*.



Figur 2 Illustration av plattformens anatomi och huvudbegrepp

2.1.2 Accesspunktsoperatör

En Accesspunktsoperatör (AP-operator) är en *tjänsteleverantörsroll* för en aktör som tillhandhåller en eller flera *accesspunktstjänster* till Deltagare i en eller flera federationer.

En AP-operatör erbjuder accesspunktjänster till Deltagare enligt ett nyttjandeavtal mellan Deltagare och AP-operatören, samt tillämpliga tekniska specifikationer och transportmodeller.
[*Se "Plattform – Avtalsmodell" för detaljerad information.]*

En AP-operatör agerar *på uppdrag av* Deltagaren.

För en AP-operatör är det viktigt att kunna efterleva de krav som ställs i relevant *dataskyddslagstiftning* för att kunna agera inom en federation och dess miljöer.

En AP-operatörs generella agerade regleras av dokumentet *"Accesspunktsoperatör – Gemensamma Regler och Rutiner"*, samt i federations specifika regler och rutiner vilka deklareras i federationens *federationsdeklaration.*

2.1.3 Accesspunktstjänst

En *accesspunktstjänst* (AP-tjänst) är en *accesspunkt* (AP) som erbjuds som en tjänst.

En accesspunktstjänst (AP-tjänst) kan *levereras* till Deltagare på många olika sätt. *[se sektion med För Leverantörer för mer information]*.

En AP-tjänst kan hantera fler än en Deltagare i samma AP-tjänst. Se *"Accesspunktsoperatör – Gemensamma Regler och Rutiner"* och *"Accesspunkt - Komponentspecifikation"* för principer och regler som gäller för separation av AP-tjänster och dess AP-funktioner mellan Deltagare.

2.1.4 Accesspunkt

En *accesspunkt* (AP) är en komponent som utför standardiserade accesspunktsfunktioner (AP-funktioner) för säker asynkron förmedling av information och meddelanden mellan aktörer enligt en 4-hörnsmodell.

Accesspunkter utgör en vital del i vissa federationer för att kunna implementera principen *"anslut en gång och utbyt meddelanden med alla deltagare i en federation"*.

En Accesspunkts *grundläggande* funktioner definieras primärt i *EU:s byggblock "eDelivery" med komponenten "Access Point"* och dess tekniska standarder för kommunikation, till exempel *AS4.*

En accesspunkts *specifika* funktioner, datamängder, API:er och GUI:s specificeras i detalj i *"Accesspunkt - Komponentspecifikation"*.

En accesspunkt ingår i vissa transportmodeller som är baserade på en 4-hörnsmodell. Se transportmodellerna "Bas" och Utökad Bas" för detaljer om hur accesspunkter förmedlar meddelanden enligt 4-hörnsmodellen.

[*Se dokumenten "Accesspunkt - Komponentspecifikation", "Transportinfrastruktur - Beskrivning", "Transportprofil AS4", och "Kuverteringsprofil – XHE" för mer information om accesspunkter*]

2.1.5 Deltagare

En Deltagare är en roll som spelas av en aktör som är ansluten av och agerar i en federation, och utbyter information och meddelanden mellan varandra inom ramen för samverkansuppdrag med hjälp av en federations operativa transportinfrastruktur, miljöer, transportmodeller, (accesspunkts-)tjänster, och tillämpningar med samverkansprocesser och meddelanden.

Rollerna och identiteterna som Accesspunktsoperatör och Deltagare är alltid åtskilda, även om dessa roller kan besättas av samma aktör.

[Se dokumentet "Deltagare – Beskrivning" för mer information om rollen som Deltagare]

2.1.6 Plattform

Plattformen erbjuder en basplatta med möjligheter till *nätverkseffekter* genom olika *värdeskapande mekanismer*, *delning av resurser* såsom organisation, regler, rutiner, specifikationer och federationers operativa transportinfrastruktur med plattformstjänster.

Plattformen och dess plattformsansvarig ansvarar för att systematisk och ändamålsenlig *informera, engagera, kvalitetssäkra, granska, plattformsgodkänna, ansluta, kontrollera, och avveckla kontrollera* accesspunktsoperatörer.

[Se dokumentet "Plattform – Beskrivning" för mer information om plattformen]

2.1.7 Federation

En federation och dess federationsägare *ingår* i plattformen med fokus på och ansvar för att långsiktigt *administrativt* och *operativt* stödja samverkande aktörer (Deltagare) och deras gemensamma mål utifrån juridiska, verksamhets-, organisatoriska, säkerhetsmässiga, och tekniska perspektiv.

En Federation erbjuder tillit, regler, rutiner, specifikationer, funktioner, tjänster, och säkerhetsåtgärder som är *anpassade* till aktörers behov av digital samverkan.

[Se dokumentet "Federation – Beskrivning" för mer information om plattformen]

En federation ansvarar för att systematisk och ändamålsenlig *granska, federationsgodkänna, ansluta, övervaka, och kontrollera accesspunktsoperatörer.* [*Se sektionen med anslutningsmodell för mer information.*]

2.1.8 Federations operativa Transportinfrastruktur

Deltagare i en federation utbyter information och meddelanden med hjälp av *transportmodeller* inom ramen för en *federations operativa transportinfrastruktur (FOT).*

En federations operativ transportinfrastruktur erbjuder en *unik* uppsättning av tillit, säkerhetsåtgärder, tekniska säkerhetskrav, servicenivåer, transportmodeller, samverkansprocesser, meddelanden och tjänster som tillfredsställer Deltagares behov i deras *olika* typer av digitala samverkan.

En operativ transportinfrastruktur är juridiskt, processmässigt, tekniskt och semantisk *separerad* från andra federationers transportinfrastrukturer.

[Se dokumentet "Transportinfrastruktur – Beskrivning" för detaljerad information]

Aktörer kan delta i *fler än en federation.* I detta fall måste en aktör vara medveten om att federationer erbjuder olika grader av tillit och säkerhetsåtgärder, vilket innebär att informationssäkerhetsklassad information och meddelanden inte per automatik kan utbytas inom fler än en federation eller överföras mellan federationer.

Detaljer om hur en federations transportinfrastruktur är uppsatt och bestyckad med tjänster *specificeras* i federationens federationsdeklaration samt i miljöers miljöspecifikationer.

[Se dokumentet "Federation - Beskrivning" för allmän information om federationers transportinfrastrukturer]

2.1.9 Transportmodell

En transportmodell *specificerar hur* ett utbyte av information och meddelanden går till utifrån juridiska, verksamhets-, säkerhetsmässiga, och tekniska perspektiv med hjälp av tjänster inom ramen för en miljö.

En transportmodell *skiljer sig åt* från andra transportmodeller avseende bland annat arkitekturstil (4-hörnsmodell, 2 hörnsmodell), interaktionsmönster (meddelande-kvittens, prenumerera-publicera, en-till-många), adressering,

egenskaper (asynkron, synkron), säkerhetsåtgärder (signering, kryptering), felhantering, etcetera.

[Se sektion med transportmodell för mer information]

2.1.10 Miljöer i Federation

En miljö tillhandahåller en *sammanhållen operativ transportinfrastruktur* med samkonfigurerade tjänster avsedd för ett viss*t syfte* med fastställda regler för dess användning.

Följande standardtyper av miljöer finns definierade inom plattformen:

- *Testmiljöer* används för utforskande verksamhet och prototyping.
- *QA*-miljöer används för kvalitetssäkring, kvalificering och godkännanden.
- P*roduktionsmiljöer* används av aktörer för att utföra sina uppdrag genom utbyte av skarpa meddelanden.

[Se dokumentet "Transportinfrastruktur – Beskrivning" för detaljerad information]

[Se dokumentet med "Federation – Beskrivning" för mer information]

2.1.11 Tjänster inom Miljöer

En miljö tillhandahåller olika typer av *tjänster* till anslutna Deltagare samt andra tjänster såsom Accesspunktsoperatörer.

En tjänst tillhandahåller olika *funktioner, datamängder, API och GUI*. Exempel utgör deltagaradressering, tjänsteadressering, PKI, och certifikatspublicering.

En federation ansvarar ytterst för att bestämma de servicenivåer som gäller för de tjänster som ingår i en miljö. Dessa servicenivåer baseras på de grundläggande servicenivåer som beskrivs i respektive tjänsts underliggande komponentspecifikation.

En tjänst erbjuds och driftsätts av en *tjänsteoperatör*. Exempel utgör

- *Plattformstjänst* som erbjuds av Plattformsansvarig som operatör.
- *Federationstjänst* som erbjuds av Federationsägare som operatör.
- *Deltagartjänst* som erbjuds av Tjänsteleverantörer till en Deltagare
  - En *Accesspunktstjänst* är en Deltagartjänst som kan levereras på många sätt där accesspunktens operatör agerar på uppdrag av Deltagaren
- *Extern tjänst* erbjuds av extern operatör utanför plattformen.

En *federationstjänst* etableras och *ansluts* till en federation på begäran av federationsägare enligt överenskommelse med plattformsansvarig.

En *plattformstjänst* etableras och *ansluts* till en federation på begäran av Federationsägare i överenskommelse med plattformsansvarig.

[Se dokumentet "Transportinfrastruktur – Beskrivning" för mer information]

2.2 Informationssäkerhets- och tillitsmodell

Federationer inom plattformen stödjer utbyte av informationssäkerhetsklassad information och meddelanden som är baserad på˚ egenskaper och funktioner med fokus på˚ hög säkerhet och systemisk tillit med principen att skapa trygghet och förtroende för alla aktörer.

Tillit är att en organisation har bevisade förmågor som tillsammans med det systematiska informationssäkerhetsarbetet samt tillitsramverk för identitet och teknik, ger förutsättningar för en trygg och effektiv digitalisering [ROT].

En förutsättning för att kunna skapa ett säkert och effektivt informationsutbyte är att samtliga ingående aktörer känner tillit till de övriga aktörerna, till en sådan nivå˚ att de kan acceptera den risk som informationsutbytet innebär. Känslan av tillit omfattar aktörens automatiserade processer, dess arbetssätt samt till den infrastruktur som används [ROT].

[*Se dokumentet "Plattform – Informationssäkerhets- och tillitsmodell" för beskrivande information om plattformens tillits- och säkerhetsskapande åtgärder, principer och rekommendationer.*]

[*Se dokumentet "Accesspunktsoperatör – Gemensamma Regler och Rutiner" för styrande regler.]*

2.2.1 Hantering av Certifikat

Certifikat ingår som en viktig beståndsdel i grundutbudet av säkerhetsåtgärder inom en operativ transportinfrastruktur och dess anslutna transportmodeller.

Exempel på typ av certifikat utgör:

- *Funktionscertifikat* kopplade till en tjänst.
  - *TLS/SSL*-certifikat för säker kommunikation och skalskydd.
  - *AP*-certifikat för autentisering av accesspunktstjänst. Dessa är utfärdade per federation och miljö.

  - *Informations*-certifikat för signering av information som en tjänst administrerar och tillhandhåller.
  - *Deltagar*-certifikat för kryptering och signering av meddelanden och nyttolaster mellan Deltagarnas verksamhetssystem.
- *Användare*-certifikat för användare i plattformen i samband med inloggning, kryptering samt signering av informationsmängder

Utfärdande av certifikat styrs generellt av ramverket och tilldelas en Accesspunktsoperatör vid anslutning till plattformen.

[Se dokumentet "Plattform – Informationssäkerhets-, och Tillitsmodell" för mer allmän information]

[Se dokumentation av respektive transportmodell för detaljerad information om användning av certifikat.]

[*Se federations federationsdeklaration för specifik information.*]

2.2.2 Servicenivåer

Samtliga i plattformen och dess federationers förekommande tjänster är definierade med servicenivåer.

Servicenivåerna för plattformstjänster och federationstjänster beskrivs per miljö i respektive miljös miljöspecifikation.

Plattformens förteckning av grundkrav på servicenivåer återfinns i *"Plattform – Informationssäkerhets- och tillitsmodell"*.

2.3 Avtalsmodell

I plattformen ingår en avtalsmodell som beskriver på˚ en övergripande nivå˚ de avtal och övriga juridiska dokument som används i plattformen samt vilka parter som är involverade.

För accesspunktsoperatörer är följande avtal och juridiska dokument samt information om personuppgiftsbehandling relevanta:

- Tecknas med Plattformsansvarig
  - Användarvillkor för accesspunktsoperatörer
  - Information om personuppgiftsbehandling
  - Anslutningsavtal
- Tecknas med Deltagare

– Tjänsteutnyttjandeavtal

[*Se dokumentet "Plattform - Avtalsmodell" för information om plattformens avtalsmodell och juridiska dokument.*]

2.4 Deltagarmodell

I plattformen ingår en deltagarmodell beskriver regler som styr vilka typer av aktörer som kan anslutas till och agera i plattformen och dess federationer i rollen som Deltagare.

Definition: En deltagarmodell är en specifikation av regler som styr vilka typer av fysiska eller juridiska personer som kan anslutas till och delta i plattformen och dess federationer i rollen som deltagare.

En federation kan anpassa plattformens deltagarmodell så den passar federationen syfte och tillämpningar. Denna anpassning deklareras i federations federationsdeklaration.

[*Se dokumenten "Plattform – Regler" och "Federation – Gemensamma Regler och Rutiner" för de gemensamma regler som styr plattformens och federationers deltagarmodeller.]*

[se en federations federationsdeklaration för federationens deltagarmodell.]

2.5 Leverantörsmodell

En viktig del i plattformen och dess federationer är tillgången till leverantörer. Leverantör bidrar till att skapa *nytta* för primära nyttohemtagare såsom myndigheter, regioner, kommuner och privata utförare då dessa kan använda deras utbud för säker och tillitsfull digital samverkan.

Med leverantörerna skapas *nätverkseffekter*, ju fler produkter och tjänster desto fler Deltagare som snabbt och effektivt kan säkert utbyte av information och meddelande. Ju fler Deltagare ju fler potentiella kunder för leverantörerna.

Plattformen ansvarar för att systematisk och ändamålsenlig *kvalitetssäkra* vissa typer av tjänster och tjänsteleverantörer såsom plattformstjänster och accesspunktsoperatörer som Deltagare använder.

En federation kan systematisk och ändamålsenlig kvalitetssäkra produkter, tjänster och tjänsteleverantörer, utöver de som plattformen hanterar, som federation anser kunna leverera nytta till federationens Deltagare.

[se dokumentet "Plattform – Beskrivning" med sektionen Leverantörsmodell för mer information]

2.6 Identifiering av Accesspunktsoperatör

Alla accesspunkter och dess AP-operatör identifieras genom *AP-identifierare* som är unika inom en federations miljö.

Identifieraren tilldelas av plattformen genom plattformens anslutningsförfarande för AP-operatörer.

Denna identifierare används bland annat i certifikat som tilldelas en AP-operatör och för att identifiera avsändande och mottagande accesspunkt i meddelanden.

Identifieraren är uppbyggd enligt ett identifieringssystem som är godkänt inom Plattformen och för Federation.

En aktör kan ansluta sig och besätta rollen som AP-operatör fler än en gång och därmed tilldelas fler än en AP-identifierare med tillhörande certifikat.

[*Se Anslutningsresan för AP-operatörer för detaljerad information*.]

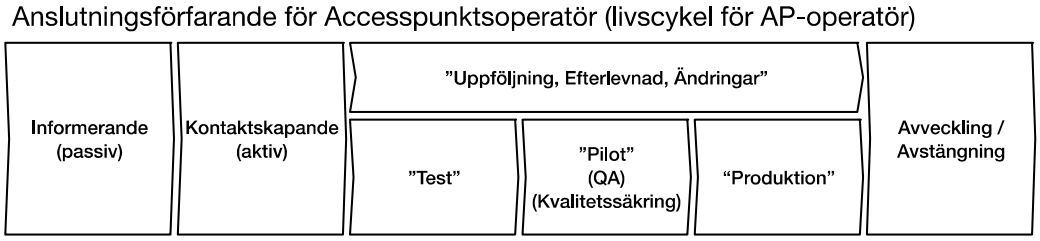
2.7 Anslutningsmodell

Plattformen och dess federationen innehåller beståndsdelar som över tiden måste kopplas in och ihop. Detta sker organiserat, samordnat, och systematisk genom olika anslutningsförfaranden inom ramen för en administrativ anslutningsmodell.

2.7.1 Anslutning av Accesspunktsoperatör till Plattform och Federation

Aktörer som vill besätta rollen som Accesspunktsoperatör ansluts generellt sett av plattformsansvarig till plattformen och specifikt av federationsägaren till federationen.

En AP-operatör går igenom ett antal *faser* i sitt engagemang över tiden i plattformen och dess federationers miljöer.



Figur 3 Illustration av anslutningsförfarande och livscykel för AP-operatör

[*En detaljerad specifikation av anslutningsförfarandet för AP-operatörer återfinns i dokumentet ”Anslutningsresa för AP-operatör”.*]

Två viktiga delmoment för en AP-operatör är *plattforms- och federationsgodkännandet.*

En Accesspunktsoperatör kan bli *plattformsgodkänd* för deltagande i plattformen och en transportmodell av plattformsansvarig genom kvalificering i en QA-miljö, vilket innebär att AP-operatörens organisation och programvara har uppnått en tillräcklig kvalitetsnivå för att kunna delta i plattformen. Ett plattformsgodkännande räcker inte för att kunna ansluta till en federations produktionsmiljö, för detta krävs även ett federationsgodkännande.

I en QA-miljö, som drivs av federationen, kan en Accesspunktsoperatör bli *federationsgodkänd* av federationsägaren. Ett federationsgodkännande innebär att federationsägaren anser att accesspunktsoperatören följer federationens specifika regler för accesspunktsoperatörer och kan delta och agera i federationens produktions-miljö.

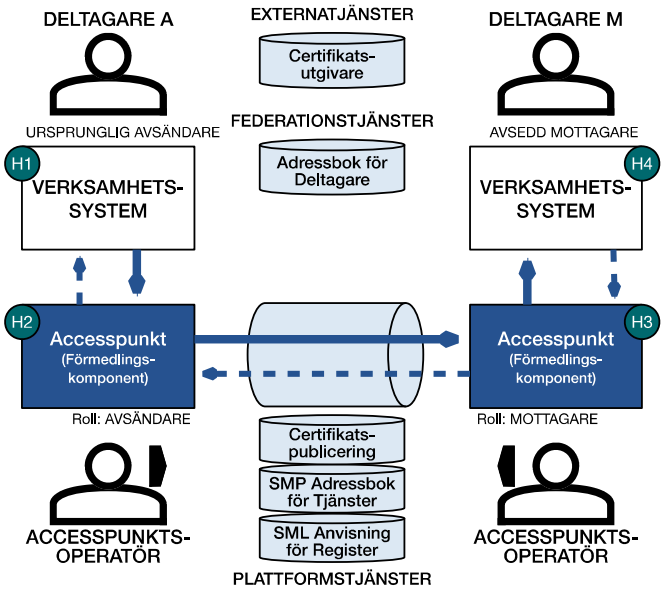
2.8 Transportmodell

Följande transportmodeller inbegriper accesspunkter:

- Transportmodell – Bas:
  - Baserad på EU-byggblocket eDelivery som är en 4-hörnsmodell där meddelandena utbyts asynkront genom användning av accesspunkter som förmedlar meddelanden enligt TLS/SSL krypterad kommunikation. Varje meddelande kvitteras med dels en synkron transportkvittens och en asynkron meddelandekvittens.
- Transportmodell – Utökat Bas:

– Utbyggnad av Transportmodell – Bas genom att lägga till att meddelanden signeras och krypteras av avsändare, vilket innebär att meddelanden inte kan läsas av mellanliggande accesspunkter.

[Se dokumentation av respektive transportmodell för mer information]



Figur 4 Illustration av 4-hörnsmodell med användning av tjänster

I de transportmodeller där accesspunkter används är rollerna och identiteterna som Deltagare och Accesspunktsoperatör åtskilda, även om dessa roller besätts av samma aktör.

En transportmodell *ansluts* till en federation på begäran av Federationsägare i överenskommelse med plattformsansvarig.

[Se dokumentet "Plattform - Beskrivning" för mer information]

2.8.1 Hantering av Certifikat

En AP-operatör får ut certifikat som en del i anslutning till en federations miljö. Certifikaten används för kryptering och signering av meddelanden mellan accesspunktsfunktioner samt för att visa att accesspunktsoperatören är godkänd att agera inom aktuell federation och miljö.

Det innebär att olika roll-baserade certifikat används för att säkert överföra meddelande i vissa transportmodeller. En Deltagares certifikat används när meddelanden krypteras och signeras av en Deltagare, och

Accesspunktsoperatörers certifikat används för kommunikation mellan accesspunkter,

[Se dokumentation av respektive transportmodell för mer information]

2.9 Rutiner för Accesspunktsoperatör

En Accesspunktsoperatör bör tillhandahålla systematiska och ändamålsenliga rutiner inom olika områden.

- Styrning och ledning
- Informationssäkerhet
- Anslutning av Accesspunktsoperatör
- Uppföljning, tillsyn, och efterlevnadskontroll
- Deltagartjänster
- Support och felhantering
- Driftavbrott och incidenthantering

[*Se dokumentet "Accesspunktsoperatör – Gemensamma Regler och Rutiner" och federationens federationsdeklaration för detaljerad information om bör och ska krav på rutiner.*]

[*Se även plattformens anslutningsmodell och dess anslutningsförfaranden för mer information.]*

2.9.1 Styrning och ledning

En Accesspunktsoperatör har rutiner för att leda förbättringsarbete och att utveckla organisationens tillitsgrundande förmågor.

2.9.2 Informationssäkerhet

En Accesspunktsoperatör tillhandahåller egna rutiner för ett systematiskt och riskbaserat informationssäkerhetsarbete.

2.9.3 Anslutning av Accesspunktsoperatör

Plattformen ansluter Accesspunktsoperatör genom ett anslutningsförfarande.

2.9.4 Uppföljning, tillsyn, och efterlevnadskontroll

Plattformen tillhandahåller rutiner för uppföljning, tillsyn och efterlevnadskontroll av anslutna Accesspunktsoperatör.

2.9.5 Samordning och samverkan

Plattformen tillhandahåller olika forum och rutiner samordning och samverkan med de aktörer som agerar inom plattformen och dess federationer.

- Planerade och anslutna tjänsteleverantörer såsom accesspunktsoperatörer.

2.9.6 Deltagartjänster

En Accesspunktsoperatör ansvarar för drift av tjänster som agerar på uppdrag eller i namnet av Deltagare.

De servicenivåer som gäller för deltagartjänster bestäms i en federations miljöspecifikation men kan justeras enligt avtal mellan Accesspunktsoperatör och Deltagare.

2.9.7 Support och Felhantering

En Accesspunktsoperatör stödjer den egna verksamheten med etablerade rutiner för felhantering och support.

2.9.8 Driftavbrott och Incidenthantering

En Accesspunktsoperatör analyserar, bedömer och vidtar löpande åtgärder som lagar och förordningar ställer på den egna verksamheten för driftavbrott och incidentrapportering.

En Accesspunktsoperatör stödjer den egna verksamheten och övriga anslutna aktörer med etablerade rutiner för driftavbrott och incidenthantering.

3 För IT-arkitekter

Denna sektion innehåller en anpassad beskrivning av rollen Accesspunktsoperatör för IT-arkitekter

En Accesspunktsoperatör tillhandhåller en accesspunkt vars funktioner, datamängder, API:er, och GUI:s beskrivs och regleras i dokumentet *”Accesspunkt - Komponentspecifikation*”. I detta dokument finns det beskrivningar och regler för hur en accesspunkt fungerar utifrån ett IT-perspektiv.

En transportmodell beskriver hur Deltagare utbyter information med hjälp av tjänster såsom en accesspunktstjänst. I transportmodellens specifikation finns det beskrivningar och regler för hur dessa tjänster används utifrån ett IT-perspektiv.

4 För Leverantörer

Denna sektion innehåller en anpassad beskrivning av för leverantörer

Denna sektion beskriver översiktligt hur accesspunkter, accesspunktsfunktioner, accesspunktsprogramvaror och accesspunktstjänster kan erbjudas till Deltagare samt hur en accesspunkt kan integreras med Deltagares verksamhetssystem.

Hur Deltagare väljer att upphandla, integrera, driftsätta, utföra och placera AP påverkar den totala tilliten till och säkerheten för aktörers digitala samverkan och hantering av digital information.

Det är speciellt viktigt att Deltagares säkerhetsfunktioner för hantering av privata nycklar samt paketering, signering, och kryptering av meddelanden sker på ett säkert sätt.

4.1 Leverans av Accesspunktstjänster

Accesspunktstjänster kan erbjudas till Deltagare på en rad olika sätt. Denna sektion beskriver översiktligt vanligt förekommande leveranssätt.

4.1.1 Intern AP-tjänst

En AP-tjänst kan driftsätts och utföras internt hos en Deltagare och då utförs AP-tjänsten på noder och nätverkssegment som kontrolleras av Deltagaren.

I detta fall besätter en aktör både rollen som Deltagare och Accesspunktsoperatör och måste därmed hantera anslutningsförfaranden och certifikat per respektive roll.

Varianter på intern AP-tjänst:

- *Egenutvecklad* AP-programvara som utvecklas av en Deltagare, eventuellt med hjälp av 'open source' programvara.
- *Inköpt* AP-programvara som köps in som AP-Produkt.

4.1.2 Extern AP-operatör

En AP-tjänst kan driftsätts och utföras externt, utanför en Deltagares fulla kontroll men på uppdrag av Deltagaren. AP-tjänsten körs då på noder och i nätverkssegment som inte (helt) kontrolleras av Deltagaren.

I detta fall finns det två olika aktörer som enskilt besätter rollerna Deltagare och Accesspunktsoperatör, och som hanterar egna anslutningsförfaranden och certifikat.

Varianter på extern AP-operatör:

- *Extern* AP-operatör utför AP-tjänst hos den *externa* AP-operatören.
- *Extern* AP-operatör driftsätter och utför AP-tjänst *internt* hos Deltagare.
- En *helhetslösning* erbjuds av AP-operatör med olika funktioner inklusive en accesspunkt vilken driftsätts och utförs externt hos AP-operatören. Ett exempel på en extern helhetslösning är ”säkra brevlådor” som körs i molnet och som möjliggör för en Deltagare att ladda ned meddelanden i klartext så att meddelandet kan signeras, krypteras och sändas till avsedd mottagare. *Säkerhet*: I denna typ av lösning ska det ställas extra krav på tillit mellan Deltagaren och AP-operatören avseende hur *säkerhetsfunktioner* såsom nyckellagring och tillgång till privata nycklar, signering och kryptering av meddelanden sker externt hos den externa AP-operatören.

4.1.3 Delad AP-tjänst

En AP-tjänst kan hantera fler än en Deltagare i samma AP-tjänst. Se ”*Accesspunktsoperatör – Gemensamma Regler och Rutiner*” och ”*Accesspunktsoperatör - Komponentspecifikation*” för principer och regler som gäller för separation av AP-tjänster och dess AP-funktioner.

I detta fall måste en AP-operatör separat hantera inre säkerhet mellan Deltagares verksamhetssystem och AP-tjänst, adressboks- och SMP-registrering, certifikat, loggning, etcetera per deltagare. Dessa aspekter kan och bör beröras i avtalet mellan Deltagare och AP-operatör.

4.1.4 Placering av AP

En AP kan placeras på olika sätt, i noder och nätverkssegment i förhållande till deltagares verksamhetssystem vilket påverkar inre och extern säkerhet.

- AP är fullt integrerad i verksamhetens programvaror.
- AP är integrerad i specialiserad integrationsprogramvara.
- AP utförs som tjänst på noder inom verksamhetens skalskydd och brandväggar.
- *AP utförs som tjänst på noder inom en avdelad och skyddad zon (DMZ) inom skalskyddet.*

- AP utförs som tjänst på noder utan för verksamheten och dess skalskydd men tillsammans med andra tjänster såsom fakturahantering eller ekonomisystem vilka används av verksamheten.
- AP utförs som extern tjänst på noder utan för verksamheten och dess skalskydd.

Det viktigt att den inre säkerheten mellan Deltagares verksamhetssystem och AP-funktioner hanteras på ett sätt som motsvarar gällande dataskyddslagstiftning, regelverk, informationssäkerhetsklassning av de meddelanden som utväxlas samt de specifikationer som styr inre säkerhet inom gällande federation.

4.1.5 Upphandling

Vid upphandling och införskaffande av AP-programvara, AP-funktioner, AP-tjänster eller AP-operatörer är det viktigt se till att dessa är följsamma mot gällande regler, regler och specifikationer som deklareras i Ramverket för Plattformen samt i federationers federationsdeklaration.

Dessutom måste AP-operatörer genomgå ett anslutningsförfarande inom plattformen och ett för varje federation där de kvalitetssäkras och godkänns (plattformsgodkännande och federationsgodkännande). Se dokumenten ”Plattform – Beskrivning” för allmän information och ”AP -Operatör – Anslutningsresa för AP-operatör” för detaljerad information.

4.2 Integration mellan Deltagares verksamhetssystem och accesspunkter

En accesspunktstjänst utför funktioner för överföring av meddelanden på uppdrag av Deltagare och dess verksamhetssystem. I detta fall finns det en inre integration mellan de komponenter som utför verksamhetsorienterade funktioner och de som utför accesspunktsfunktioner, vilken regleras i dokumentet ”Accesspunkt – Komponentspecifikation.”

Denna inre integration kan ske på många olika sätt vilket illustreras av följande fall

- *Full integration*: AP-funktioner är helt integrerade med verksamhetssystem.
- *Specialiserad integration*: verksamhetssystem kommunicerar med AP enligt protokoll eller komponenter som leverantör av AP-programvara tillhandahåller.
- *API*: verksamhetssystem kommunicerar med AP via ett standardiserat API.

- *Konnektor*: verksamhetssystem kommunicerar med AP via en mellanliggande modul eller komponent som tillhandahåller specialiserad funktionalitet som inbegriper användning av AP-funktioner.