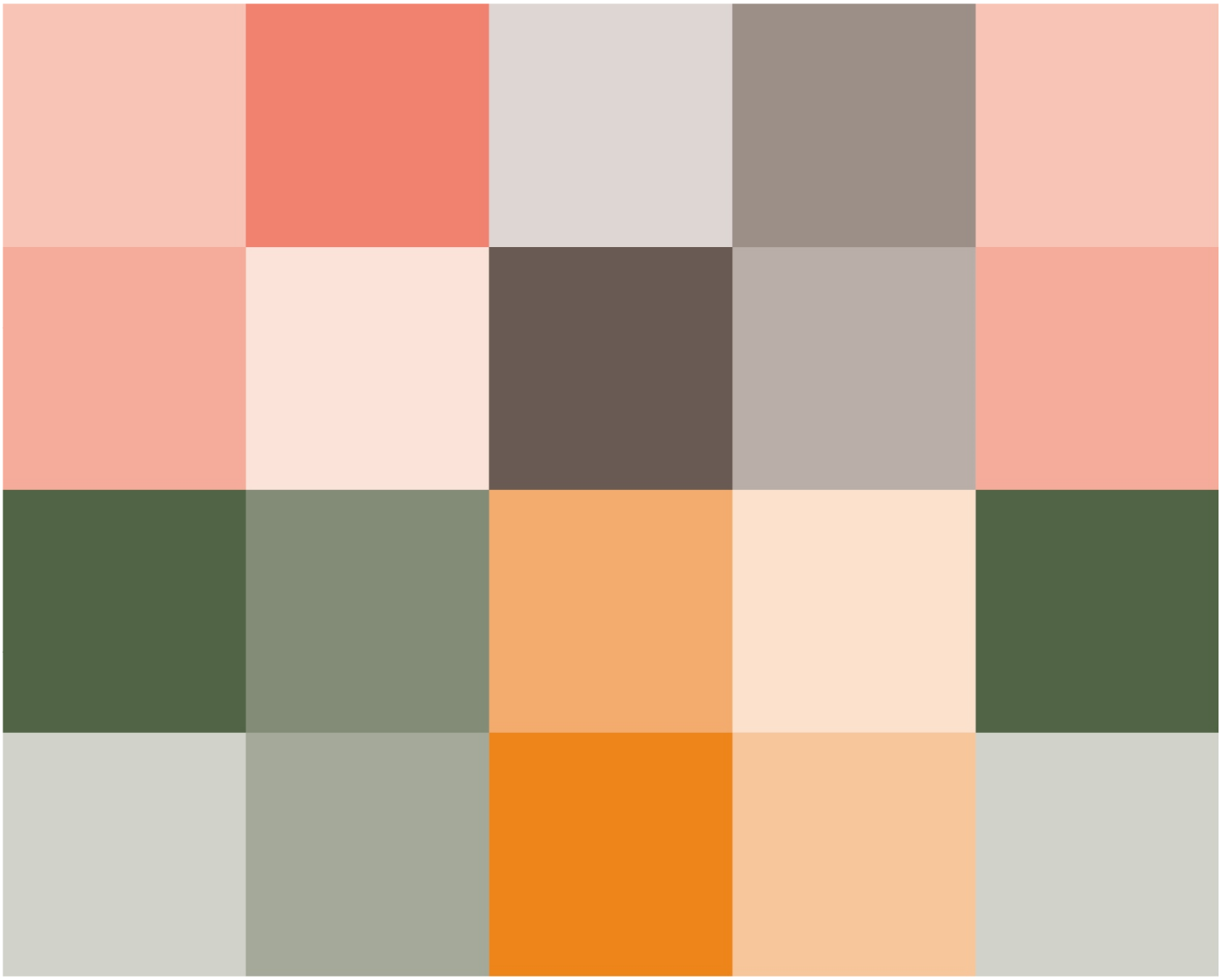


Komponentspecifikation - Accesspunkt

Specifikation av Komponent - Accesspunkt

Version: 1.0 Målgrupper: Verksamhetsutvecklare, IT-arkitekter

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Sammanfattande beskrivning av komponenten Accesspunkt

Detta dokument innehåller en specifikation av komponenten:

Benämning: Accesspunkt

Version: 1.0

Livscykelstatus: Under utveckling

Ägare: DIGG

Nyckelord: Accesspunkt; Förmedlingskomponent; Komponent

En *accesspunkt* (AP) är en förmedlingskomponent som levererar standardiserade funktioner för asynkront utbyte av rekommenderade meddelanden enligt specifika transportmodeller och tekniska specifikationer, inom en federations miljö.

En AP adresserar *dynamiskt* avsändares meddelanden till rätt mottagande accesspunkt och mottagares verksamhetssystem genom att använda adressregister innehåller tjänsters metadata kopplat till deltagare. Se komponentspecifikationerna för SML och SMP för detaljerad information.

Innehållsförteckning

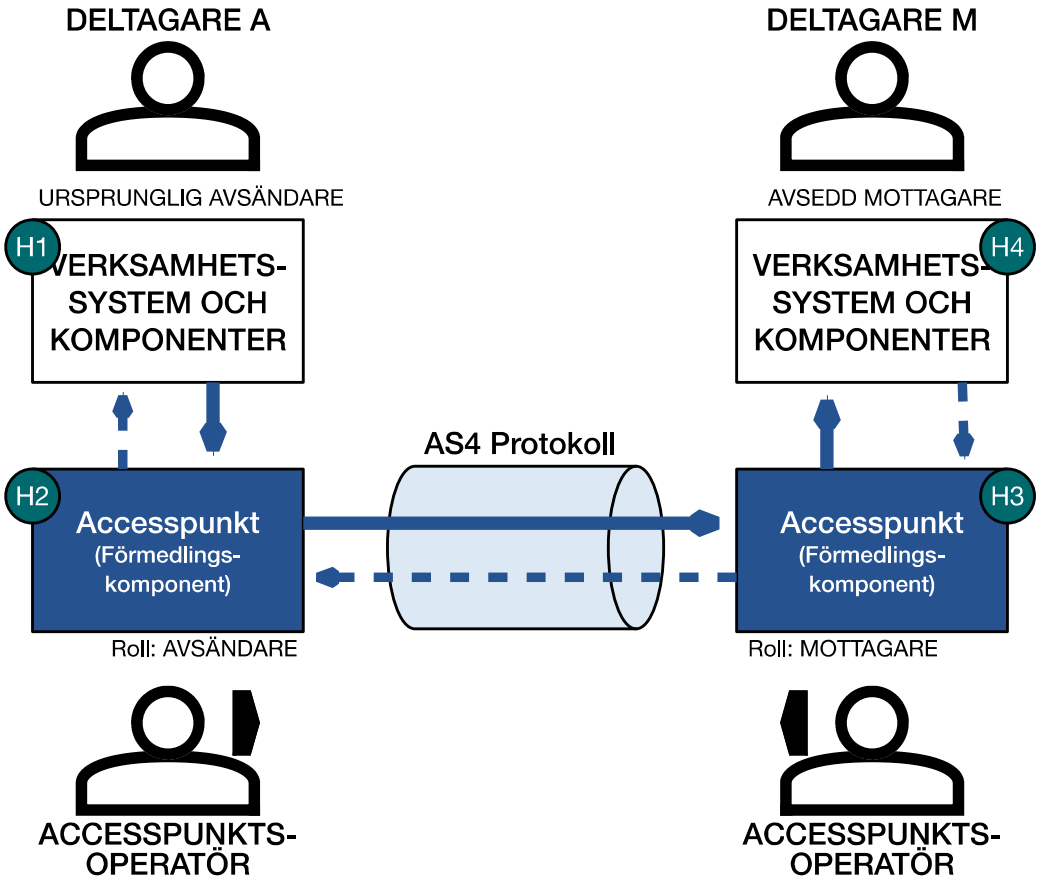
1 Inledning

Inledande beskrivning av komponenten Accesspunkt

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

En AP:s grundläggande funktioner definieras i EU:s byggblock ”eDelivery” med komponenten ”Access Point” och dess tekniska standarder för kommunikation.

En AP utgör en vital del i vissa federationer för att kunna implementera principen ”anslut en gång och utbyt meddelanden med alla deltagare i en federation”.



Figur 1 Översiktlig beskrivning av en accesspunkts och dess funktion

1.1 Beroenden till specifikationer och komponenter

Denna komponent använder och är följsam mot följande specifikationer:

- CEF eDelivery AS4 Profile [AS4-DIGITAL]
- Transportprofil för AS4
- Kuverteringsprofil för XHE

Denna komponent beror av att följande komponenter finns tillgängliga:

- Service Metadata Locator [SML-OASIS]
- Service Metadata Publisher [SMP-OASIS]
- PKI för Accesspunkter

1.2 Målgrupper

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

Intressenter:

- Verksamhetsutvecklare
  - 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
  - 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, dokumenterar och utvärderar informationssystem
  - Stödjer utveckling av informationssystem för digital samverkan
  - Tar fram arkitekturer för informationssystem för digital samverkan, analyserar, designar, bygger, och testar programvaror.

1.3 Externa referenser

Kortnamn	Länk	Kommentar
AS4-OASIS	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.html	OASIS AS4 Standard
AS4-DIGITAL	https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4	CEF eDelivery AS4 Profile
SMP- OASIS	https://docs.oasis-open.org/bdxr/bdx-smp/v1.0/bdx-smp-v1.0.html	OASIS SMP Standard
SML-OASIS	http://docs.oasis-open.org/bdxr/BDX-Location/v1.0/BDX-Location-v1.0.html	OASIS SMP (BDXL) Standard

2 För Verksamhetsutvecklare

Information som är riktad till verksamhetsutvecklare

2.1 Inledning

Denna specifikation beskriver en Accesspunkts grundläggande funktioner, API:er och regler.

2.2 Egenskaper hos komponent

Asynkron utväxling av meddelanden. Signerar och krypterar. Använder ett standardiserat transportprotokoll som nyttjas i många sammanhang och internationellt. Är agnostisk avseende meddelandetyp.

2.3 Nyttor med användning

Användning av en Accesspunktsfunktion i 4-hörsmodellen ger

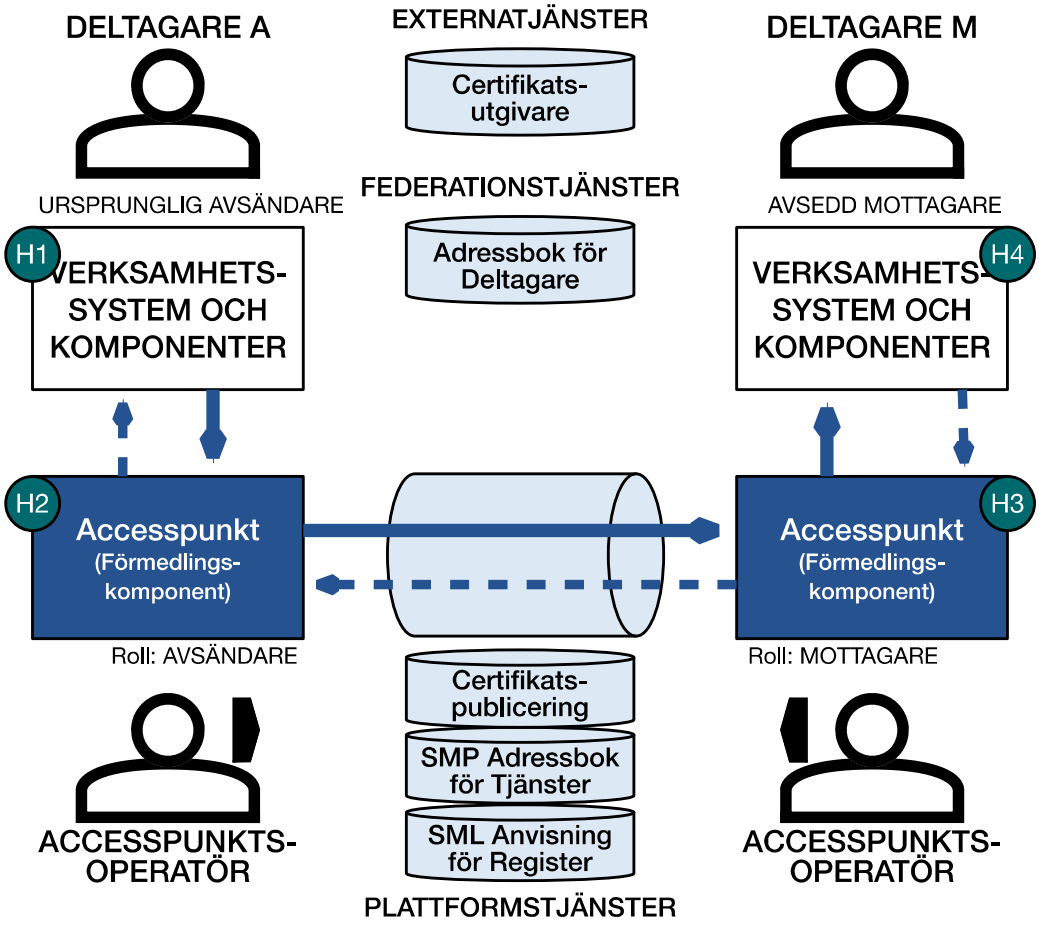
- möjlighet för Deltagare att använda en tjänsteoperatör för den tekniska kommunikationen (överföringen)
- möjlighet för tjänsteoperatörer att etablera stordriftsfördelar då de kan erbjuda samma tjänst till flera kunder
- asynkron överföring gör det möjligt att ha en lösare koppling mellan Deltagarnas system vilket ställer lägre krav på tillgänglighet

Användning av dynamisk adressering ger

- automatiserad inhämtning av tekniska adressuppgifter från aktuell och säker källa
- möjlighet att kontrollera om mottagaren har stöd för aktuell meddelandetyp och samverkansprocess
- dynamisk adressering gör det enkelt för Deltagare att byta lösning inga statiska/hårdkodade behöver ändras hos motparterna

2.4 Hur komponenten fungerar

Accesspunktsfunktioner kommunicerar på ett standardiserat sätt och med dynamiskt inhämtad parametersättning för att meddelandeutväxling ska kunna göras på ett säkert sätt. I 4-hörnsmodellen, återfinns Accesspunktsfunktionen i hörn 2 och 3 där den skickar och ta emot meddelanden åt Deltagarna (hörn 1 och 4). Nedan beskrivs på en övergripande nivå hur meddelandeutväxling enligt 4-hörnsmodellen ser ut.



Figur 2 En accesspunkts roll i en 4-hörns transportmodell.

2.4.1 Deltagares Funktioner – Avsändare (Hörn 1)

Dessa sektion innehåller typiska funktioner som en deltagare utför i förhållande till en accesspunkt när ett meddelade skickas via accesspunkter till avsedd mottagare.

- Kontrollera att mottagaren är registrerad i federationen
- Ta reda på mottagarens identifierare för adressering
- Ta reda på att mottagaren använder samma format för nyttolast
- Skapa och validera meddelande (och vid behov signera och/eller kryptera)
- Överlämna meddelande till Accesspunktsfunktionen för förmedling.

2.4.2 AP Funktioner – Avsändare (Hörn 2)

- Ta emot/hämta meddelande som ska förmedlas från Avsändande Deltagare
- Validera att meddelandet är korrekt kuverterat
- Hämta teknisk adress/parametrar
- Signera, kryptera och skicka meddelande
- Logga utväxlingen
- Vid behov, notifiera Avsändande Deltagare

2.4.3 AP Funktioner – Mottagare (Hörn 3)

- Ta emot meddelande från avsändande AP-funktion
- Dekryptera kuvert, kontrollera signatur och kvittera mottagning enligt transportprotokollets principer
- Logga utväxlingen
- Validera att meddelandet är korrekt kuverterat
- Logga utväxlingen
- Överlämna meddelande till Mottagande Deltagare
- Vid behov, notifiera Mottagande Deltagare

2.4.4 Deltagares Funktioner – Mottagare (Hörn 4)

- Ta emot/hämta meddelande som inkommit AP-funktionen
- Kontrollera signatur på kuvertet och dekryptera dess nyttolast
- Validera att meddelandets nyttolast följer formatets regler och struktur
- Lagra
- Skapa och lämna kvittens

2.5 Villkor och förutsättningar för användning

För att en Accesspunkt skall kunna användas inom en federations miljö krävs att Accesspunktsoperatören har blivit godkänd samt erhållit ett certifikat som är giltigt för användning i federationens miljö. För produktionsmiljö i en federation gäller normalt att ett antal tester genomförts, en försäkran om överenstämmelse fyllts i och godkänts, samt att avtal mellan Accesspunktsoperatören och Plattformsansvarig tecknats.

2.6 Aktörer och roller

Roll	Beskrivning
Accesspunktsoperatör	En tjänsteleverantörsroll för en fysisk eller juridisk person som tillhandhåller en eller flera accesspunktstjänster.
Deltagare	En roll som spelas av en fysisk eller juridisk person som utbyter data och meddelanden inom en federation med hjälp av en federationens transportinfrastruktur, dess miljöer och tjänster.
Plattformsansvarig	En roll som spelas av en fysisk eller juridisk person som äger, styr, leder, utvecklar, förvaltar, driftar och stödjer plattformen.

3 För IT-arkitekter

3.1 Regler

Accesspunkten utför ett antal operationer vid avsändning och mottagning utöver de som strikt beskrivs i transportprotokollet och transportmodellen. Dessa regler beskrivs nedan.

3.1.1 Följsamhet gentemot tekniska specifikationer

[a] En AP-funktion ska vara följsam gentemot de principer, regler, tekniska specifikation och rutiner som är aktuella i de federationers miljöer som AP-funktionen agera inom.

3.1.2 Transportmodeller

En accesspunkt erbjuder dess funktioner inom ramen för standardiserade transportmodeller. En transportmodell definierar hur information och meddelanden utbyts in i sin helhet och den roll som en accesspunkt spelar tillsammans med andra komponenter och dess funktioner.

[a] En AP-funktion måste ha stöd för de transportmodeller som används i den federation som den är godkänd för

[b] En AP-funktion får inte vägra mottagning av ett meddelande från en annan godkänd AP-operatör om försändelsen görs på ett sätt som är följsamt gentemot specifikationer och regler

3.1.3 Användning av tjänstemetadata

[a] En AP-funktion måste använda tjänstemetadatat på avsett sätt och i enlighet med specifikationen för ”Transportprofil AS4”

[b] En AP-funktion får inte sända ett meddelande vars typ inte överensstämmer med den som är angiven i tjänstemetadatat

[c] I federationsdeklarationen regleras huruvida en AP-funktion får cacha (tillfälligt lagra) tjänstemetadata och i så fall hur länge

[A1] Om AP-funktionen får cacha (tillfälligt lagra) tjänstemetadata

[A2] Hur länge cachad (tillfälligt lagrad) tjänstemetadata kan användas innan ny tjänstemetadata måste hämtas från SMP

3.1.4 Användning av kuvert

[a] Försändelser skall alltid vara förpackade i enlighet med specifikationen ”Kuverteringsprofil XHE”

3.1.5 Identifiering av Accesspunkt

Identifiering av AP-operatör i AS4 FromParty

[a] En AP-funktion måste använda den identifierare som tilldelats och som återfinns i det AP-certifikat som utfärdats för aktuell federations miljö.

Identifiering av AP-operatör i AS4 ToParty

[b] Identifierare av mottagande AP-funktion ska hämtas från det AP-certifikat (attributet CN) som återfinns i tjänstemetadatat (SMP)

3.1.6 Kontroll meddelandekuvert och AS4

[a] AP-funktionen ska kontrollera att FinalRecipient i AS4 SOAP överensstämmer med XHE/ToParty

[b] AP-funktionen ska kontrollera att OriginalSender i AS4 SOAP överensstämmer med XHE/FromParty

[c] AP-funktionen ska kontrollera att Service och Action i AS4 SOAP överensstämmer med meddelandetyp och processtyp i XHE

[d] Om fel identifieras ska försändelsen hanteras enligt reglerna för ”inkorrekt mottagare/tjänst”

3.1.7 Loggning och spårbarhet

[a] En avsändande AP-funktion ska logga åtminstone de uppgifter som beskrivs *Informationsmodell: Händelselogg*

[b] En mottagande AP-funktion ska logga åtminstone de uppgifter som beskrivs i *Informationsmodell: Händelselogg:*

3.2 Felhantering vid meddelandeutväxling

3.2.1 Inkorrekt mottagare/tjänst

[a] Ett meddelande som tagits emot av AP-funktionen som är adresserad till en Deltagare som AP-operatören inte betjänar måste hanteras på följande sätt

1. Händelsen ska loggas med uppgifter enligt *Informationsmodell: Händelselogg*
2. Det inkomna meddelandet (kuvert+nyttolast) ska raderas
3. Felmeddelande som beskrivs i AS4-profilen kan rapporteras synkront av AP-funktionen till avsändande AP

3.2.2 Ej följsamt kuvert

[a] En meddelande som tagits emot av AP-funktionen som inte är följsam till XHE Kuverteringsprofil alternativt inte följer principer för överenstämmelse mellan AS4 SOAP-kuvert och XHE Kuverteringsprofil ska hanteras på följande sätt

1. Händelsen ska loggas med uppgifter enligt *Informationsmodell: Händelselogg* inklusive felorsak som visar varför försändelsen inte är följsam
2. Det inkomna meddelandet (kuvert+nyttolast) ska raderas

3.2.3 Onåbar SMP

Hantering av situation då SMP-slagning av tjänstemetadata inte går att göra på grund av att SMP-tjänsten är onåbar

[a] En AP-funktion kan göra återförsök för adressuppslagning om SMP-tjänsten inte är nåbar

[b] Antalet återförsök och hur länge återförsök ska göras bestäms i nyttjandeavtalet mellan Deltagaren och AP-operatören.

[c] Avsändande Deltagare ska notifieras om ett meddelande inte går att förmedla pga onåbar SMP

3.2.4 Mottagare inte registrerad i SMP

[a] Avsändande Deltagare ska notifieras om ett meddelande inte går att förmedla pga mottagande Deltagare inte är registrerad i SMP

3.2.5 Onåbar mottagande AP-funktion

[a] Om mottagande AP-funktion inte är nåbar kan återsändningsförsök göras. Uppgift om antal och tid som återförsök ska göras bestäms i federationsdeklarationen.

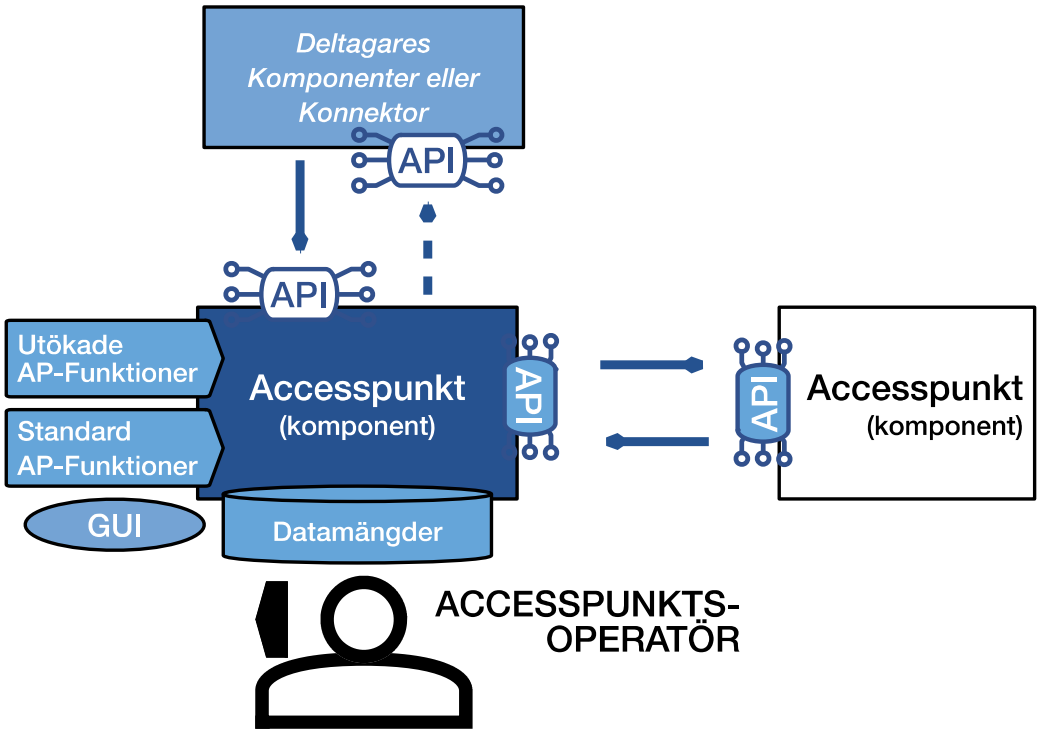
[A3] Antalet återsändningsförsök vid onåbar mottagande AP-funktion

[A4] Hur länge återsändningsförsök ska pågå vid onåbar mottagande AP-funktion

[b] Deltagaren ska notifieras om ett meddelande inte går att förmedla pga onåbar mottagande AP

3.3 Accesspunktens olika API:er

Accesspunkten har ett antal APIer. Accesspunktens använder AS4-standarden som API för utväxling av meddelanden med andra Accesspunkter. Deltagaren interagerar också med Accesspunkten genom API:er. Vilka API-specifikationer som kan användas mellan Deltagare och Accesspunkt är inte reglerat utan överlåts till aktörerna att bestämma utifrån deras behov.



Figur 3 Accesspunktskomponentens delar

3.3.1 API: Accesspunkt till Accesspunkt, AS4

Detta API beskrivs generellt sett av EU:s eDelivery AS4 Profile och specifikt för denna komponent i ”Transportprofil AS4”.

3.3.2 API: Deltagare till Accesspunkt

En programvara som implementerar denna specifikation kan erbjuda olika API:er till användare av Accesspunkten och dess funktioner. I denna version av komponentspecifikation definieras inget standardiserat API.

3.3.3 API: Accesspunkt till Deltagare

En programvara som implementerar denna specifikation kan erbjuda olika API:er mellan Accesspunkt, dess funktioner och användare. I denna version av komponentspecifikation definieras inget standardiserat API.

3.4 Informationsmodeller

3.4.1 Informationsmodell: Händelselogg

En AP ska logga åtminstone följande uppgifter för händelsen: ”Utgående meddelande”.

Benämning	**Händelse**
Identifierare för mottagande accesspunkt	Utgående meddelande
Mottagande accesspunkts certifikat och signatur på kvittens (AS4 signalmeddelande)	Utgående meddelande
Avsändningstidpunkt	Utgående meddelande
Identifierare för avsändande och mottagande Deltagare	Utgående meddelande
AS4 Message ID	Utgående meddelande
AS4 Conversation ID	Utgående meddelande
Felorsak	Utgående meddelande

En AP ska logga åtminstone följande uppgifter för händelsen: ”inkommet meddelande”.

Benämning	**Händelse**
Identifierare för avsändande accesspunkt	Inkommet meddelande
Avsändande accesspunkts certifikat och signatur	Inkommet meddelande
Mottagningstidpunkt	Inkommet meddelande
Identifierare för avsändande och mottagande Deltagare	Inkommet meddelande
AS4 Message ID	Inkommet meddelande
AS4 Conversation ID	Inkommet meddelande
Felorsak	Inkommet meddelande

3.5 Informationssäkerhet- och tillit

För informationssäkerhet- och tillit så finns styrande regler och rutiner i ramverket för Plattformen och AP-operatör måste kontrollera vilka regler som gäller för uppsättning av en AP-komponent.

AP-komponentens säkerhetsåtgärder och servicenivåer ska utgå från aktuella transportmodeller och transportprotokoll samt miljöer för aktuell federation.

AP-operatör ansvarar för att AP-komponenten informationssäkerhetsklassas.

Vägledande beskrivning kring informationssäkerhet och IT-säkerhet finns i ”Plattform – Informationssäkerhet och tillit”