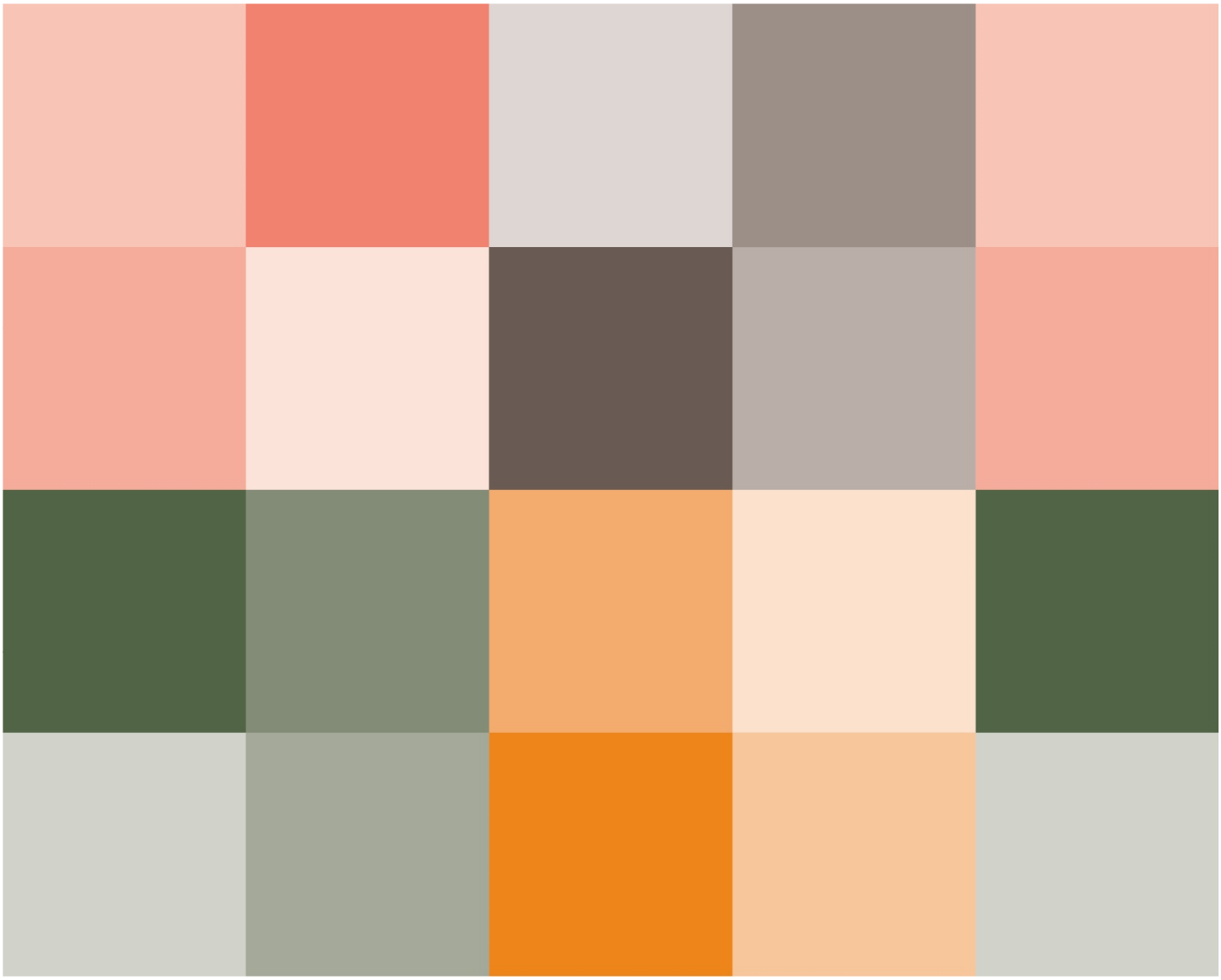


Transportmodell – Utökad Bas

Specifikation av Transportmodell Utökad Bas

Version: 1.0 Målgrupper: Verksamhetsutvecklare, IT-arkitekter, Säkerhetsansvarig

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Sammanfattning beskrivning av transportmodell Utökad Bas

Detta dokument innehåller en specifikation av transportmodellen:

Identitet: base-ext-sigenc

Version: 1.0

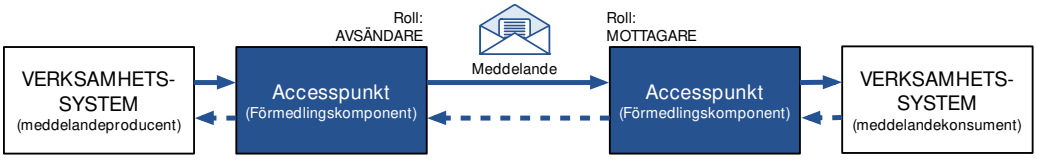
Livscykelstatus: Fastställd

Ägare: DIGG

Arkitekturstil: CEF eDelivery 4-hörnsmodell

Nyckelord: transportmodell; utbytesmönster; säkerhetsåtgärder

Transportmodell Utökad Bas är en utökning av den funktionalitet som beskrivs i Transportmodell Bas. Utökningen innebär att meddelanden som ställs ut av Deltagaren ska krypteras och signeras redan i Deltagarens system och dekrypteras i den mottagande Deltagarens system. Det innebär att accesspunktsoperatörerna inte har access till nyttolasten i klartext.



Innehållsförteckning

1 Inledning

Inledande beskrivning av transportmodellen

Detta dokument specificerar endast de aspekter av transportmodellen som skiljer sig från Transportmodell Bas och de båda dokumenten måste därför läsas tillsammans

1.1 Beroenden till specifikationer

Utöver de specifikationer som Transportmodell Bas använder ska implementationer även vara följsamma gentemot:

- Certifikatspublicering – REST-bindning mot SMP

Utöver de tjänster som Transportmodell Bas använder behöver även följande komponenter eller tjänster finns tillgängliga:

- Certifikatspubliceringstjänsten

1.2 Dokumentstruktur

Detta dokument innehåller följande delar:

- Beskrivning av komponenten för verksamhetsutvecklare
- Beskrivning av komponenten för IT-arkitekter

Regler är formaterade och identifierade enligt följande formatmall:

[a] regeltext för första regeln a.

[b] regeltext för andra regeln b.

En regel refereras unikt inom plattformen genom ”<dokument> ’-’ <sektion i dokument> ’.’ <regelidentitet>”. Exempel: ”plattform-2.1.a”.

En regel refereras lokalt inom dokument genom ”<sektion>’. ’<regelidentitet>”. Exempel: ”4.1.a”.

1.3 Målgrupper

Detta dokument syftar till att stödja följande 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, utvecklare)
  - Utvärderar ramverk, plattformar, infrastrukturer, och teknologier för digital samverkan ur ett informationssystemperspektiv
  - Kravställer utveckling av informationssystem för digital samverkan
  - Utför systematiskt och riskbaserat informationssäkerhetsarbete.
  - Utvärderar, analyserar, designar och dokumenterar informationssystem
  - Stödjer utveckling av informationssystem för digital samverkan
  - Tar fram arkitekturer för informationssystem för digital samverkan
- Säkerhetsansvarig
  - Utvärderar, analyserar, designar och dokumenterar informationssäkerhetsåtgärder
  - Utför systematiskt och riskbaserat informationssäkerhetsarbete.

2 För Verksamhetsutvecklare

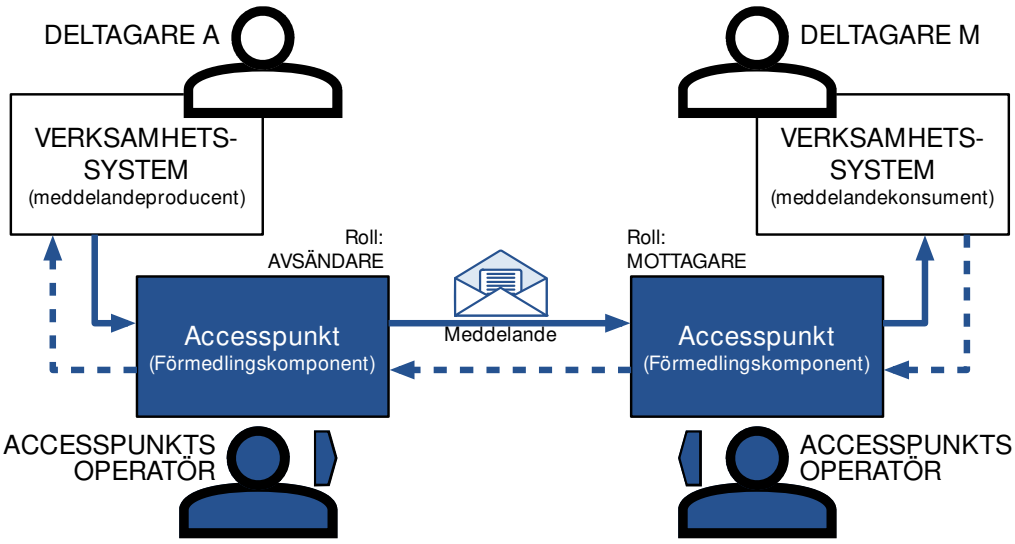
Information som är riktad till verksamhetsutvecklare

2.1 Inledning

Denna transportmodell utökar Transportmodell Bas genom att kräva signering av meddelandet och kryptering av dess nyttolast. Meddelandekvittenser ska signeras men inte krypteras.

2.2 Arkitekturstil

Se Transportmodell Bas



Figur 1 Illustration av 4-hörnsmodellen och dess roller

2.3 Egenskaper hos transportmodellen

Grundläggande egenskaper beskrivs i Transportmodell Bas.

Denna transportmodell kräver att Deltagaren dessutom krypterar/signerar meddelanden. Signaturen kan användas för kontroll av ursprung.

2.4 Nyttor med användning

Nedan följer exempel på nyttor som möjliggörs vid användningen av de funktioner och tjänster som transportmodellen stipulerar.

CEF eDelivery 4-hörsmodell ger

- Se Transportmodell Bas

Användning av SML/SMP ger

- Se Transportmodell Bas

Obligatorisk meddelandekvittens ger

- Se Transportmodell Bas

Användning av kuverteringsprofil XHE ger

- Se Transportmodell Bas

Användning av Deltagares signering/kryptering av meddelande ger

- utökad kontroll av ett meddelandes ursprung

- utökad försäkran om att Deltagarens tjänsteleverantör inte får tillgång till meddelandet i klartext.

Användning av Certifikatspubliceringstjänsten ger

- förenklad distribution av de publika certifikat som används för kryptering och för autentisering av motparten (den Deltagare man utväxlar meddelanden med)

2.5 Hur transportmodellen fungerar

Som Transportmodell Bas med utökad funktionalitet för signering och kryptering av meddelanden redan i Deltagarens verksamhetssystem/tjänst.

2.6 Villkor och förutsättningar för användning

Se Transportmodell Bas med följande tillägg:

Deltagarna måste vara överens (genom princip inom federation eller bilateralt) om vilka slags certifikat och certifikatsutgivare som ska användas för signering och kryptering av meddelanden.

I federationsdeklarationen regleras huruvida Certifikatspubliceringstjänsten ska användas eller om certifikat ska utväxlas/distribueras manuellt mellan Deltagarna.

Om Certifikatspubliceringstjänsten används måste Deltagarens verksamhetssystem/meddelandetjänst som ska kryptera och/eller kontrollera avsändares certifikat ha access till tjänsten.

2.7 Aktörer och roller

Roll	Beskrivning
Deltagare	Den organisation som i en samverkansprocess med en annan Deltagare utväxlar meddelanden
Accesspunktsoperatör	Den organisation som utför accesspunktsfunktioner för förmedling av meddelanden på uppdrag av Deltagare

2.8 Översiktliga användningsfall

Se Transportmodell Bas med följande tillägg:

Exempel på användningsfall då denna transportmodell kan användas är:

Överföring av elektroniska meddelanden som bedömts vara av så känslig natur att utökad kontroll av avsändarens identitet behöver göras och/eller

då Deltagarens Accesspunktsoperatör inte får hantera meddelandets innehåll i klartext.

2.9 Tranportmodellen

Se Transportmodell Bas med följande tillägg:

2.9.1 Händelser

Deltagare krypterar, dekrypterar, signerar meddelanden samt kontrollerar att signatur gjorts av avsändande Deltagare

2.9.2 Loggning och spårning

Inga tillägg

2.9.3 Validering

Inga tillägg

2.9.4 Felhantering

Inga tillägg

2.9.5 Incidenthantering

Inga tillägg

2.10 Tillämpning av Meddelandemodellen

Inga tillägg

2.11 Tillämpning av Kuverteringsmodellen

[a]	Nyttolast i det meddelande som utväxlas med denna transportmodell ska krypteras av avsändande Deltagare enligt de principer som beskrivs i Kuverteringsprofil XHE.
[b]	Meddelandekvittens som utväxlas med denna transportmodell ska inte krypteras
[c]	Meddelande (och meddelandekvittens) som utväxlas med denna transportmodell ska krypteras av avsändande Deltagare enligt de principer som beskrivs i Kuverteringsprofil XHE.

2.12 Tillämpning av Adresseringsmodellen

Inga tillägg

2.13 Tillämpning av Samverkansmodellen

Inga tillägg

2.14 Tillämpning av Informationssäkerhets- och tillitmodellen

2.14.1 Säkerhetsåtgärder

Denna transportmodell baseras på tjänster och tekniska specifikationer som etablerar en rad säkerhetsmekanismer.

Säkerhetsåtgärd	**Security Function (CEF/EU)**	**Definition/Omfattning**
Förändringsskydd under transport	Transport Integrity	**AP till AP** genom AS4 kryptering och signering samt TLS **Deltagare till Deltagare** genom kryptering av nyttolast
Identifiering/ Ursprungskontroll av avsändare	Authentication Sender	**AP till AP** genom matchning av AP-certifikatet subjekt och transportkuvertets identifierare för avsändande AP. **Deltagare till Deltagare** genom avsändande Deltagares signatur och slagning i Certifikatspubliceringstjänsten för att verifiera att avsändaren använder rätt certifikat.
Auktorisation av Sändning	Authorisation of Sending	**AP till AP** genom att certifikat visar att AP är godkänd för aktuell federation och miljö **Deltagare till Deltagare** genom slagning i SMP och tillit till att denna information är korrekt.
Identifiering av mottagare	Receiver Authentication	**AP till AP** genom att certifikat i tjänstemetadatat visar att AP är godkänd för aktuell federation och miljö. Kontroll av att den synkrona kvittensens signatur överensstämmer med certifikat från tjänstemetadata. **Deltagare till Deltagare** genom slagning i SMP och tillit till att denna information är korrekt samt genom slagning i

		Certifikatspubliceringstjänst för att verifiera mottagarens certifikat
Förändringsskydd av meddelande	Message Integrity	**AP till AP** genom AS4 kryptering och signering samt TLS **Deltagares integration med sin AP** genom inre säkerhet **Deltagare till Deltagare** genom kryptering av nyttolast
Insynsskydd för kommunikation	Message Confidentiality – non-persistent	**AP till AP** genom AS4 kryptering samt TLS **Deltagare till Deltagare** genom kryptering av nyttolast
Insynsskydd för lagrade meddelanden	Message Confidentiality – persistent	**Deltagare till Deltagare** genom kryptering av nyttolast
Tidstämpel på meddelande	Message Timestamp	**AP till AP** genom AS4 tidsstämpel (signerad av avsändande AP) **Deltagare till Deltagare** genom att kuvert är tidsstämplat (och signerat)
Ursprungskontroll av (av)sändare	Addressee Identification / Party Identification	**AP till AP** genom matchning av AP-certifikatet subjekt och transportkuvertets identifierare för avsändande AP. **Deltagare till Deltagare** genom slagning i Certifikatspubliceringstjänsten för att kontrollera att avsändarens signatur är i överenstämmelse avsändarens publicerade certifikat
Oavvislighet av meddelande	Non Repudiation of Origin	**AP till AP** genom att meddelande signeras med avsändandes APs certifikat. **Deltagare till Deltagare** genom att meddelandet är signerat

Oavvislighet av kvittens	Non-Repudiation of Receipt	**AP till AP** genom att transportkvittens signeras med mottagande APs certifikat. **Deltagare till Deltagare** genom att meddelandet är signerat
Robust meddelandeutväxling	Reliable Message	**AP till AP genom** synkron transportkvittens **Deltagare till Deltagare** genom asynkron meddelandekvittens

3 För IT-arkitekter

Information som är riktad till IT-arkitekter

3.1 Inledning

Nedan beskrivs i mer detalj de tekniska aspekterna för denna transportmodell.

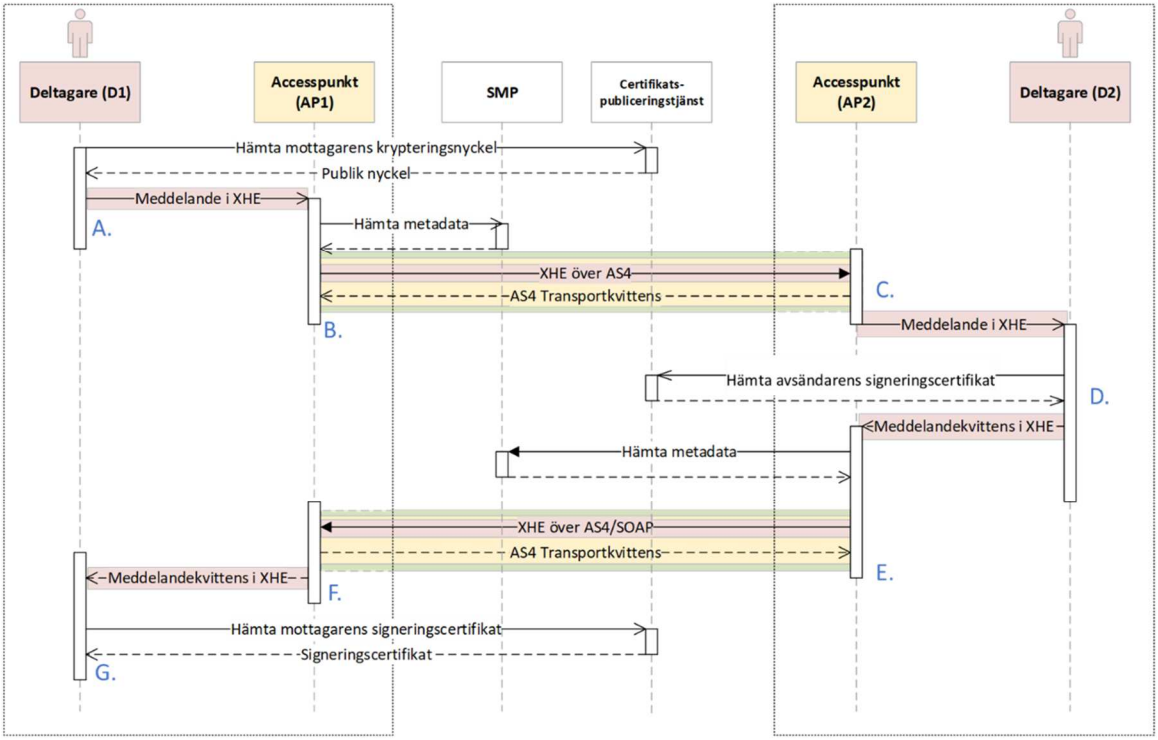
3.2 Tekniska villkor och förutsättningar för användning

Se Transportmodell Bas med följande tillägg:

[a]	Om federationen använder Certifikatspubliceringstjänsten ska Deltagares certifikat vara publicerad där
[b]	Om federationen inte använder Certifikatspubliceringstjänsten ska Deltagares certifikat i förväg vara ömsesidigt kända/utväxlade
[c]	En Deltagare som skickar meddelande enligt Transportmodell Utökad Bas ska vara registrerad i SMP för att kunna ta emot meddelandekvittens enligt samma transportmodell.
[d]	Då ett meddelande mottagits enligt Transportmodell Utökad Bas ska meddelandekvittens returernas enligt samma Transportmodell.

3.3 Översiktliga tekniska användningsfall

Nedan beskrivs två typiska användningsfall av denna transportmodell. Båda användningsfallen kan överskådligt illustreras med hjälp av detta sekvensdiagram



Figur 2 Illustration av sekvensen av aktiviteter

3.3.1 Tekniskt AF: Översändning av meddelande med positiv kvittens

Detta användningsfall beskriver hur ett meddelande transporteras och kvitteras enligt Transportmodell Utökad Bas.

De antaganden och moment i flödet som skiljer sig från Transportmodell Bas är markerade med gul färg.

Användningsfall	
Beskrivning	Lyckad överföring av krypterat och signerat meddelande som tas emot, dekrypteras, valideras, accepteras och kvitteras.
Roller	Deltagare (D1 och D2), Accesspunktsoperatör (AP1 och AP2)
Antaganden	Båda Deltagare är registrerad på korrekt sätt i SMP. Båda Deltagare har publicerat sina publika certifikat i Certifikatspubliceringstjänsten.
Flöde	**A. Förbereda, validera, kryptera, kuvertera, signera och initiera överföring (Deltagare 1)** 1. Deltagare (D1) avser sända meddelande till en annan Deltagare (D2).

	2. D1 skapar och validerar meddelandet utifrån de principer som beskrivs i aktuell meddelandespecifikation. 3. D1 gör slagning mot Certifikatspubliceringstjänsten för att hämta D2 publika nyckel 4. D1 krypterar meddelandets nyttolast 5. D1 förpackar meddelandet i ett kuvert i enlighet med Kuverteringsprofil XHE. I kuvertet framgår bland annat identifierare för avsedd mottagare (D2), samverkansprocess och meddelandetyp. 6. D1 signerar meddelandet med sitt certifikat 7. D1 överlämnar meddelandet till sin accesspunktsoperatör (AP1). B. **Adressuppslagning, transportkuvertering och överföring av meddelande (Accesspunktsoperatör 1)** 8. AP1 gör, baserad på kuvertets uppgifter, slagning i SMP för att hämta nödvändiga parametrar för att utföra en överföring enligt Transportprofil AS4. 9. AP1 kontrollerar att AP2:s certifikat som hämtats från SMP är utfärdat till en för federationen godkänd accesspunkt. 10. AP1 använder AP2:s publika nyckel som hämtats från SMP för att kryptera innehållet i AS4-försändelsen. 11. AP1 etablerar en säker anslutning (enligt de principer för TLS som används i federationen) till AP2 och sänder meddelandet. C. **Mottagning av meddelande, transportkvittering och loggning (Accesspunktsoperatör 2)** 12. AP2 tar emot AS4-försändelsen och kontrollerar att dess signatur är korrekt och att certifikatet är utfärdat till en för federationen godkänd accesspunkt. 13. AP2 returnerar en synkron AS4-kvittens på att meddelandet tagits emot. 14. AP1 och AP2 loggar händelsen. 15. AP2 kontrollerar att kuvertet är i överensstämmelse med vad som gäller för den avsedda mottagaren och överlämnar meddelandet till D2.

	D. **Mottagning av meddelande, validering och skapande av meddelandekvittens (Deltagare 2)** 16. D2 gör slagning i Certifikatspubliceringstjänsten för att hämta D1 certifikat 17. D2 kontrollerar att certifikat är giltigt och validerar signaturen 18. D2 dekrypterar meddelandets nyttolast med sin privata nyckel. 19. D2 validerar att meddelandets nyttolast är följsamt gentemot dess specifikations regler. 20. D2 konstaterar att nyttolasten är korrekt och accepterar mottagningen. 21. D2 skapar en meddelandekvittens med referens till det mottagna meddelandet och med statuskod som visar att det accepterats 22. D2 validerar, kuverterar och signerar meddelandekvittensen i enlighet med Kuverteringsprofil XHE och överlämnar meddelandet till AP2. E. **Adressuppslagning, transportkuvertering och överföring av meddelandekvittens (Accesspunktsoperatör 2)** 23. AP2 kontrollerar kuvert, gör slagning i SMP och överför meddelandet till AP1 enligt Transportprofil AS4. F. **Mottagning av meddelandekvittens, transportkvittering och loggning (Accesspunktsoperatör 1)** 24. AP1 tar emot AS4-försändelsen och kontrollerar att dess signatur är korrekt och att certifikatet är utfärdat till en för federationen godkänd accesspunkt. 25. AP1 returnerar en synkron AS4-kvittens på att meddelandet tagits emot. 26. AP1 och AP2 loggar händelsen. 27. AP1 kontrollerar kuvert och överlämnar meddelandet till D1. **G. Mottagning av meddelandekvittens (Deltagare 1)** 28. D1 gör slagning i Certifikatspubliceringstjänsten för att hämta D2 certifikat 29. D1 kontrollerar att certifikat är giltigt och validerar meddelandekvittensens signaturen

	30. D1 läser meddelandekvittensen och kan konstatera att D2 tagit emot och accepterat meddelandet. 31. *Flödet klart*.
Resultat	Meddelande överfört från D1 till D2 och kvittens om att det accepterats har returnerats till D1.
Exempel	Överföring av meddelande som bär känslig information såsom en orosanmälan eller registerutdrag

3.3.2 Tekniskt AF: Översändning av meddelande som ej accepteras på grund av valideringsfel av nyttolast

Detta användningsfall beskriver hur ett meddelande transporteras och där meddelandet inte accepterats då avsändaren oavsiktligt modifierat meddelandet efter att det signerats och på så sätt brutit förändringsskyddet. Meddelandekvittens innehåller orsakskod som kan hjälpa avsändande deltagare i sin felsökning.

De antaganden och moment i flödet som skiljer sig från Transportmodell Bas är markerade med gul färg.

Användningsfall	
Beskrivning	Överföring av krypterat och signerat meddelande som innehåller fel då förändringsskyddet brutits innan det skickas. Meddelanden tas emot, dekrypteras, valideras, accepteras ej och kvitteras.
Roller	Deltagare (D1 och D2), Accesspunktsoperatör (AP1 och AP2)
Antaganden	Båda Deltagare är registrerad på korrekt sätt i SMP. Båda Deltagare har publicerat sina publika certifikat i Certifikatspubliceringstjänsten.
Flöde	**A. Förbereda, validera, kryptera, kuvertera, signera och initiera överföring (Deltagare 1)** 1. Deltagare (D1) avser sända meddelande till en annan Deltagare (D2). 2. D1 skapar och validerar meddelandet utifrån de principer som beskrivs i aktuell meddelandespecifikation.

	3. D1 gör slagning mot Certifikatspubliceringstjänsten för att hämta D2 publika nyckel 4. D1 krypterar meddelandets nyttolast 5. D1 förpackar meddelandet i ett kuvert i enlighet med Kuverteringsprofil XHE. I kuvertet framgår bland annat identifierare för avsedd mottagare (D2), samverkansprocess och meddelandetyp. 6. D1 signerar meddelandet med sitt certifikat *7. D1 gör oavsiktligt en förändring av meddelandets XML-struktur och bryter därmed förändringsskyddet* 8. D1 överlämnar meddelandet till sin accesspunktsoperatör (AP1). B. **Adressuppslagning, transportkuvertering och överföring av meddelande (Accesspunktsoperatör 1)** 9. AP1 gör, baserad på kuvertets uppgifter, slagning i SMP för att hämta nödvändiga parametrar för att utföra en överföring enligt Transportprofil AS4. 10. AP1 kontrollerar att AP2:s certifikat som hämtats från SMP är utfärdat till en för federationen godkänd accesspunkt. 11. AP1 använder AP2:s publika nyckel som hämtats från SMP för att kryptera innehållet i AS4-försändelsen. 12. AP1 etablerar en säker anslutning (enligt de principer för TLS som används i federationen) till AP2 och sänder meddelandet. C. **Mottagning av meddelande, transportkvittering och loggning (Accesspunktsoperatör 2)** 13. AP2 tar emot AS4-försändelsen och kontrollerar att dess signatur är korrekt och att certifikatet är utfärdat till en för federationen godkänd accesspunkt. 14. AP2 returnerar en synkron AS4-kvittens på att meddelandet tagits emot. 15. AP1 och AP2 loggar händelsen. 16. AP2 kontrollerar att kuvertet är i överensstämmelse med vad som gäller för den avsedda mottagaren och överlämnar meddelandet till D2.

	D. **Mottagning av meddelande, validering av signatur och skapande av meddelandekvittens (Deltagare 2)** 17. D2 gör slagning i Certifikatspubliceringstjänsten för att hämta D1 certifikat 18. D2 kontrollerar att certifikat är giltigt och validerar signaturen 19. D2 upptäcker att signaturen inte validerar korrekt då meddelandet 20. D2 dekrypterar **inte** meddelandets nyttolast 21. D2 skapar en meddelandekvittens med referens till det mottagna meddelandet och med statuskod som visar att det ej accepterat och med orsakskod att signaturen inte stämmer 22. D2 validerar och kuverterar och signerar meddelandekvittensen i enlighet med Kuverteringsprofil XHE och överlämnar meddelandet till AP2. E. **Adressuppslagning, transportkuvertering och överföring av meddelandekvittens (Accesspunktsoperatör 2)** 23. AP2 kontrollerar kuvert, gör slagning i SMP och överför meddelandet till AP1 enligt Transportprofil AS4. F. **Mottagning av meddelandekvittens, transportkvittering och loggning (Accesspunktsoperatör 1)** 24. AP1 tar emot AS4-försändelsen och kontrollerar att dess signatur är korrekt och att certifikatet är utfärdat till en för federationen godkänd accesspunkt. 25. AP1 returnerar en synkron AS4-kvittens på att meddelandet tagits emot. 26. AP1 och AP2 loggar händelsen. 27. AP1 kontrollerar kuvert och överlämnar meddelandet till D1. **G. Mottagning av meddelandekvittens och validering av signatur (Deltagare 1)** 28. D1 gör slagning i Certifikatspubliceringstjänsten för att hämta D2 certifikat 29. D1 kontrollerar att certifikat är giltigt och validerar meddelandekvittensens signaturen

	30. D1 läser meddelandekvittensen och kan konstatera att D2 inte accepterat meddelandet. 31. D1 kan med ledning av meddelandekvittensens orsakskoder förstå varför avvisning skett och kan rätta/korrigera sin lösning. *Flödet klart.*
Resultat	Meddelande överfört från D1 till D2 och kvittens om att det inte accepterats har returnerats till D1.
Exempel	Överföring av meddelande som bär känslig information såsom en orosanmälan eller registerutdrag