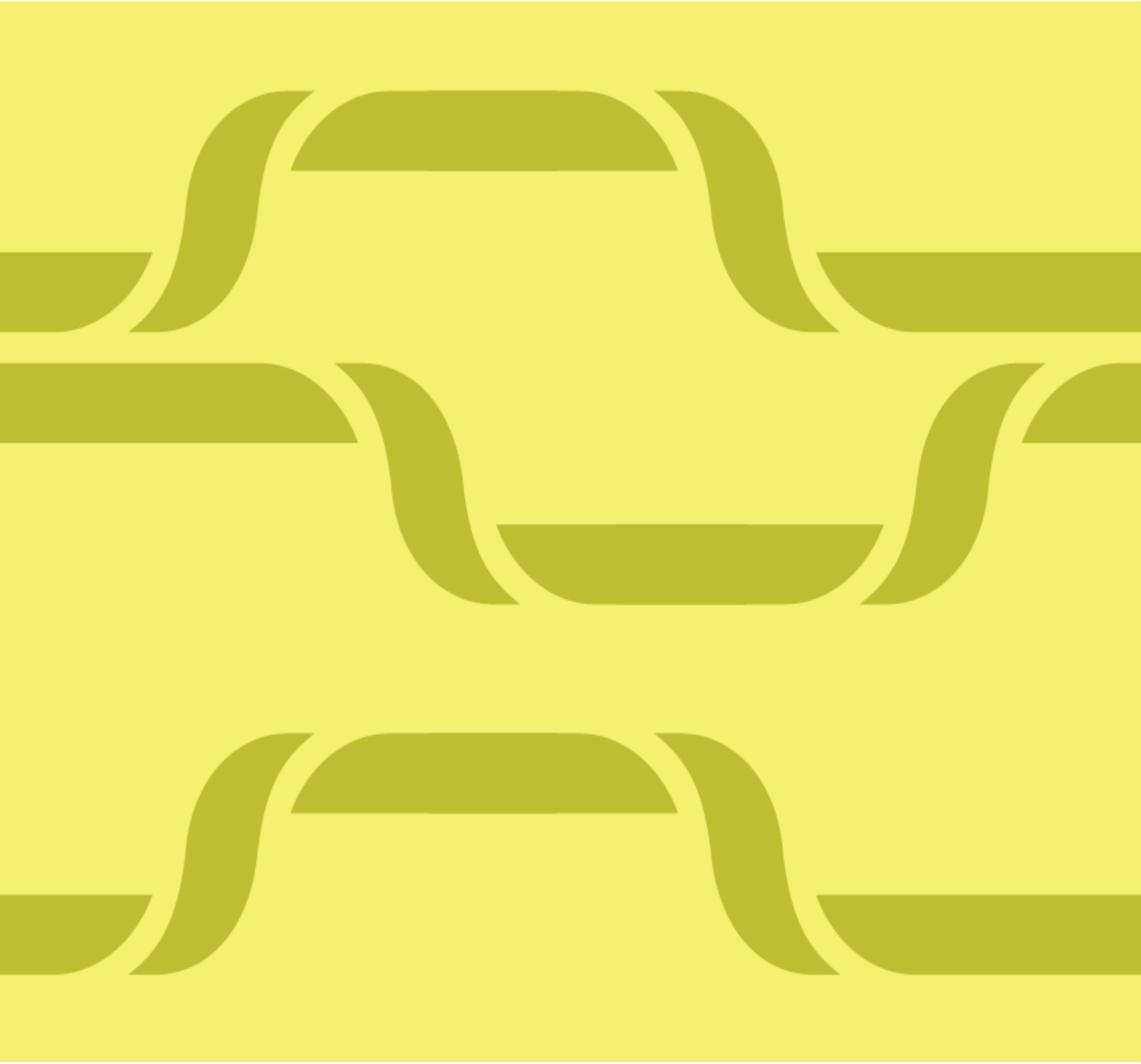
SFTI
SINGLE FACE TO INDUSTRY

PM - Beskrivning av Peppols modell för transport av meddelanden



MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

KAMMARKOLLEGIET

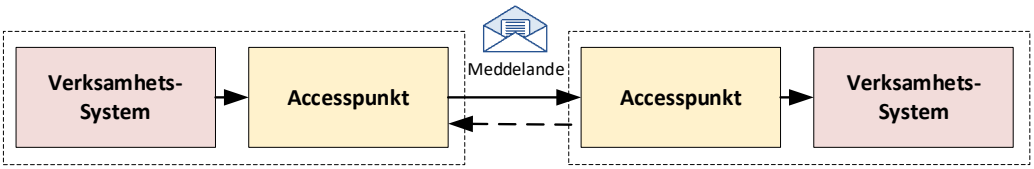
Sveriges Kommuner och Regioner

Upphandlingsmyndigheten

Innehållsförteckning

1 Sammanfattning

Detta dokument innehåller en beskrivning av Peppols transportmodell. Transportmodell beskriver hur meddelanden överförs och kvitteras mellan deltagare via mellanliggande och förmedlande accesspunkter, vilka tillhandahålls av accesspunktsoperatörer.



Figur 1 - Bilden visar att meddelanden överförs mellan verksamhetssystem och accesspunkter

Peppol nyttjar de säkerhetsmekanismer som ingår i transportprotokollet AS4 i kommunikationen mellan accesspunkterna. Specifika säkerhetsmekanismer (krypteringsalgoritmer, transportprotokoll osv) för accesspunktens integration med deltagarens system regleras inte i detalj, men det ställs krav i Peppols ramverk att lämpliga säkerhetsmekanismer ska tillämpas.

Överföring av meddelanden samt kvittenser mellan accesspunkterna är alltid krypterade och signerade vilket ger insynsskydd, förändringsskydd och oavvislighet.

1.1 Version dokument

Version: 1.0
Datum: 2023-05-03
Författare: Martin Forsberg
Organisation: SFTI

2 Inledning

2.1 Inledande beskrivning av transportmodellen

Detta dokument beskriver Peppols ”transportmodell”, alltså hur meddelanden överförs mellan affärsparter på ett grundläggande sätt via tredje män, accesspunktsoperatörer, enligt Peppols principer.

2.2 Målgrupper

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

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 säkerhets- och verksamhetsperspektiv
- Utför systematiskt och riskbaserat informationssäkerhetsarbete.
- Kravställer utveckling av system för digital samverkan
- Stödjer utveckling av 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.

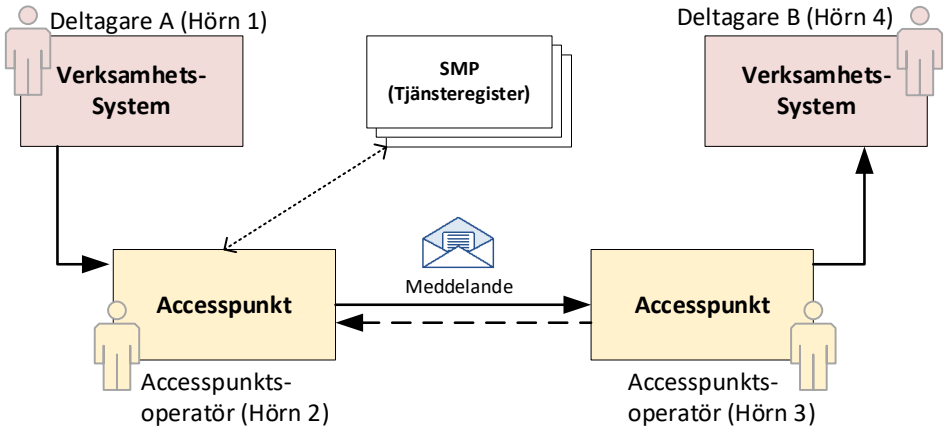
3 Om Peppols transportmodell

3.1 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

3.2 Arkitekturstil

Peppols 4-hörnsmodell ger möjlighet för deltagare i infrastrukturen att nyttja tjänsteleverantörer som tillhandahåller accesspunktsfunktioner.



Figur 2 Illustration av 4-hörnsmodellen och dess roller

Meddelandeutväxling enligt denna transportmodell är asynkron mellan Deltagarnas system (men synkron mellan accesspunkterna) vilket innebär att eventuellt svar (exempelvis leverantörens orderkvittens som svar på köparens order) returneras i form av en ny försändelse.

För adresseringen av meddelanden görs dynamisk uppslagning gentemot tjänstregister. Tjänsteregister (SMP, Service Metadata Publishers) publicerar signerade uppgifter om Deltagarens tekniska ändpunkten/mottagningspunkt. Uppgifterna används av den avsändande accesspunkten för att förbereda (kryptera/signera) försändelsen och att förmedla den till korrekt adress.

Peppols infrastruktur har flera tjänstregister och för att välja rätt register använder accesspunkten den centrala anvisningstjänsten (SML, Service Metadata Locator + DNS).

Meddelanden som skickas genom Peppols infrastruktur är alltid förpackade i ett tekniskt kuvert (SBDH, Standard Business Document Header) som innehåller uppgifter om identitet för avsändare och mottagare samt typ av meddelande.

3.3 Nyttor med användning

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

4-hörnsmodell 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
- möjlighet att med asynkron överföring ha en lösare koppling mellan Deltagarnas system vilket ställer lägre krav på tillgänglighet

Användning av SML/SMP 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 som gör det enkelt för Deltagare att byta lösning då inga statiska/hårdkodade konfigureringar behöver ändras hos motparterna

Användning av tekniska kuvertet SBDH ger

- accesspunktsoperatören möjlighet att ha en rationell hantering av inkommande och utgående meddelanden
- ett standardiserat sätt att identifiera de parametrar som behövs vid slagning i SML/SMP

3.4 Hur Peppols transportmodell fungerar

Det elektroniska affärsmeddelandet (exempelvis en e-faktura) kuverteras i enlighet med SBDH-standarden och överförs via accesspunktsfunktioner med AS4-protokollet. Avsändande accesspunktsfunktion gör en adressuppslagning mot SMP-tjänsten. Därefter överförs meddelandet till mottagarens accesspunktsfunktion som omedelbart kvitterar (synkront) att meddelandet tagits emot. Meddelandet överlämnas därefter till Deltagarens verksamhetssystem som kontrollerar att meddelandet är följsamt enligt aktuell meddelandespecifikation.

Säkerhetsmekanismerna för överföringen (signerad och krypterad) mellan accesspunktsfunktionerna är *specifikt* reglerade genom Peppols transportprotokoll (AS4). Peppol reglerar *inte specifika* säkerhetsmekanismer avseende kryptering/signering för integrationen mellan Deltagaren och dess Accesspunktsoperatör, annat än att parterna måste tillse att integrationen görs på ett säkert sätt (inre säkerhet som kravställs i Peppols avtalsmodell[1]).

17. Confidentiality and Data Protection

17.1. The Parties shall implement appropriate technical and organizational measures to protect the integrity and continuous operation of the Peppol Interoperability Framework and all data exchanged across the Peppol Network against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other forms of processing contrary to this Agreement and applicable law. Taking into account the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the data exchange and the nature of the data to be protected respecting the minimum requirements set out in the Security provisions in the Internal Regulations and/or Operational Procedures. Either Party shall take steps to ensure that any natural person acting under the authority of the respective Party in relation to this Agreement complies with the applicable information security requirements.

Figur 3 Utdrag ur Peppols Accesspunktsoperatörsavtal

3.5 Villkor och förutsättningar för användning

Transportmodellen baseras på ett asynkront utväxlingsmönster som gör att det lämpar sig för situationer där Deltagarnas verksamhetssystem bör/måste vara löst kopplade till varandra.

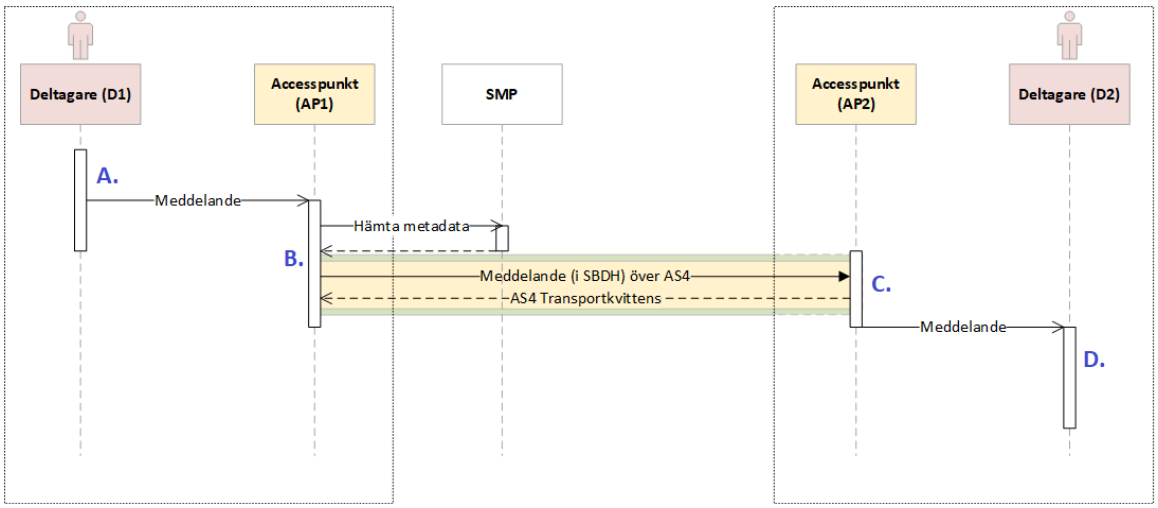
Peppols transportmodell ger en hög säkerhet genom användning av standardiserade säkerhetsmekanism samt att de inblandade parternas ansvar är kravställda och dokumenterade. I undantagsfall kan det vara aktuellt att försäkra sig om en högre tillitsnivå för att ett informationsutbyte ska kunna etableras. Om två Deltagare har behov av att utväxla känslig information kan de tillsammans granska och visa hur deras respektive inre säkerhet garanteras. En sådan granskning kan innebära att Deltagarna visar vilka säkerhetsmekanismer som nyttjas vid integrationen med accesspunktsoperatören, vilka lagkrav[2] som gäller i sammanhanget och vilka övriga säkerhetsrelaterade krav som ställts.

3.6 Översiktligt användningsfall

Nedan beskrivs ett typiskt användningsfall av denna transportmodell. Användningsfallet kan överskådligt illustreras med hjälp av nedan sekvensdiagram.

[1] Inre säkerhet som ställs I Peppols avtalsmodell (https://openpeppol.atlassian.net/wiki/spaces/AF/pages/2891251733/Peppol+Interoperability+Framework+1+July+2022)

[2] Exempelvis Lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (https://riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2020914-om-tystnadsplikt-vid_sfs-2020-914)



Figur 4 Illustration av sekvensen av aktiviteter

3.6.1 AF: Översändning av meddelande

Detta användningsfall beskriver hur ett meddelande transporteras och kvitteras i Peppols transportmodell.

Användningsfall	
Beskrivning	Lyckad överföring av meddelande som tas emot och valideras.
Roller	Deltagare (D1 och D2), Accesspunktsoperatör (AP1 och AP2)
Antaganden	Mottagande Deltagare (D2) är registrerad på korrekt sätt i SMP.
Flöde A	**Förbereda, validera, kuvertera 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 förpackar meddelandet i ett kuvert i enlighet med Kuverteringsprofil SBDH. I kuvertet framgår bland annat identifierare för avsedd mottagare (D2), samverkansprocess och meddelandetyp. 4. D1 överlämnar meddelandet till sin accesspunktsoperatör (AP1).
Flöde B	**Adressuppslagning, transportkuvertering och överföring av meddelande (Accesspunktsoperatör 1)** 5. AP1 gör, baserad på kuvertets uppgifter, slagning i SMP för att hämta nödvändiga parametrar för att utföra en överföring enligt Transportprofil AS4.

	6. AP1 kontrollerar att AP2:s certifikat som hämtats från SMP är utfärdat till en för Peppol certifierad accesspunktsoperatör. 7. AP1 använder AP2:s publika nyckel som hämtats från SMP för att kryptera innehållet i AS4-försändelsen. 8. AP1 etablerar en säker TLS-anslutning till AP2 och sänder meddelandet.
Flöde C	**Mottagning av meddelande, transportkvittering och loggning (Accesspunktsoperatör 2)** 9. AP2 tar emot AS4-försändelsen och kontrollerar att dess signatur är korrekt och att certifikatet är utfärdat till en för Peppol certifierad accesspunktsoperatör. 10. AP2 returnerar (synkront) en signerad AS4-kvittens på att meddelandet tagits emot. 11. AP1 och AP2 loggar händelsen. 12. AP2 kontrollerar att kuvertet är i överensstämmelse med vad som gäller för den avsedda mottagaren och överlämnar meddelandet till D2.
Flöde D	**Mottagning av meddelande, validering och skapande av meddelandekvittens (Deltagare 2)** **13.** D2 validerar att meddelandets nyttolast är följsamt gentemot dess specifikations regler. **14.** *Flödet klart*.
Resultat	Meddelande överfört från D1 till D2.
Exempel	Överföring av faktura

4 Säkerhetsåtgärder för informationssäkerhet och tillit

4.1 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 **Deltagares integration med sin AP** genom inre säkerhet
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 slagning i SMP och tillit till att denna information är korrekt.
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
Förändringsskydd av meddelande	Message Integrity	**AP till AP** genom AS4 kryptering och signering samt TLS

		Deltagares integration med sin AP genom inre säkerhet *Inget obrutet förändringsskydd Deltagare till Deltagare*
Insynsskydd för kommunikation	Message Confidentiality – non-persistent	**AP till AP** genom AS4 kryptering samt TLS **Deltagares integration med sin AP** genom inre säkerhet
Insynsskydd för lagrade meddelanden	Message Confidentiality – persistent	*Nyttjas ej i denna Transportmodell*
Tidstämpel på meddelande	Message Timestamp	**AP till AP** genom AS4 tidsstämpel (signerad av avsändande AP) **Deltagare till Deltagare** genom att kuvert är tidsstämplat *(ej signerad i denna Transportmodell)*
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 interna register och process/verksamhetskontroll att motparten är känd.
Oavvislighet av meddelande	Non Repudiation of Origin	**AP till AP** genom att meddelande signeras med avsändandes APs certifikat. **Deltagare till Deltagare** *ingen kryptologisk säkerhetsmekanism för oavvislighet i denna Transportmodell*
Oavvislighet av kvittens	Non-Repudiation of Receipt	**AP till AP** genom att transportkvittens signeras med mottagande APs certifikat. **Deltagare till Deltagare** *ingen kryptologisk säkerhetsmekanism för oavvislighet i denna Transportmodell*

Robust meddelandeutväxling	Reliable Message	**AP till AP genom** synkron transportkvittens med omsändningspolicy vid avbrott **Deltagare till Deltagare** *Inge specifik mekanism enligt denna transportmodell*