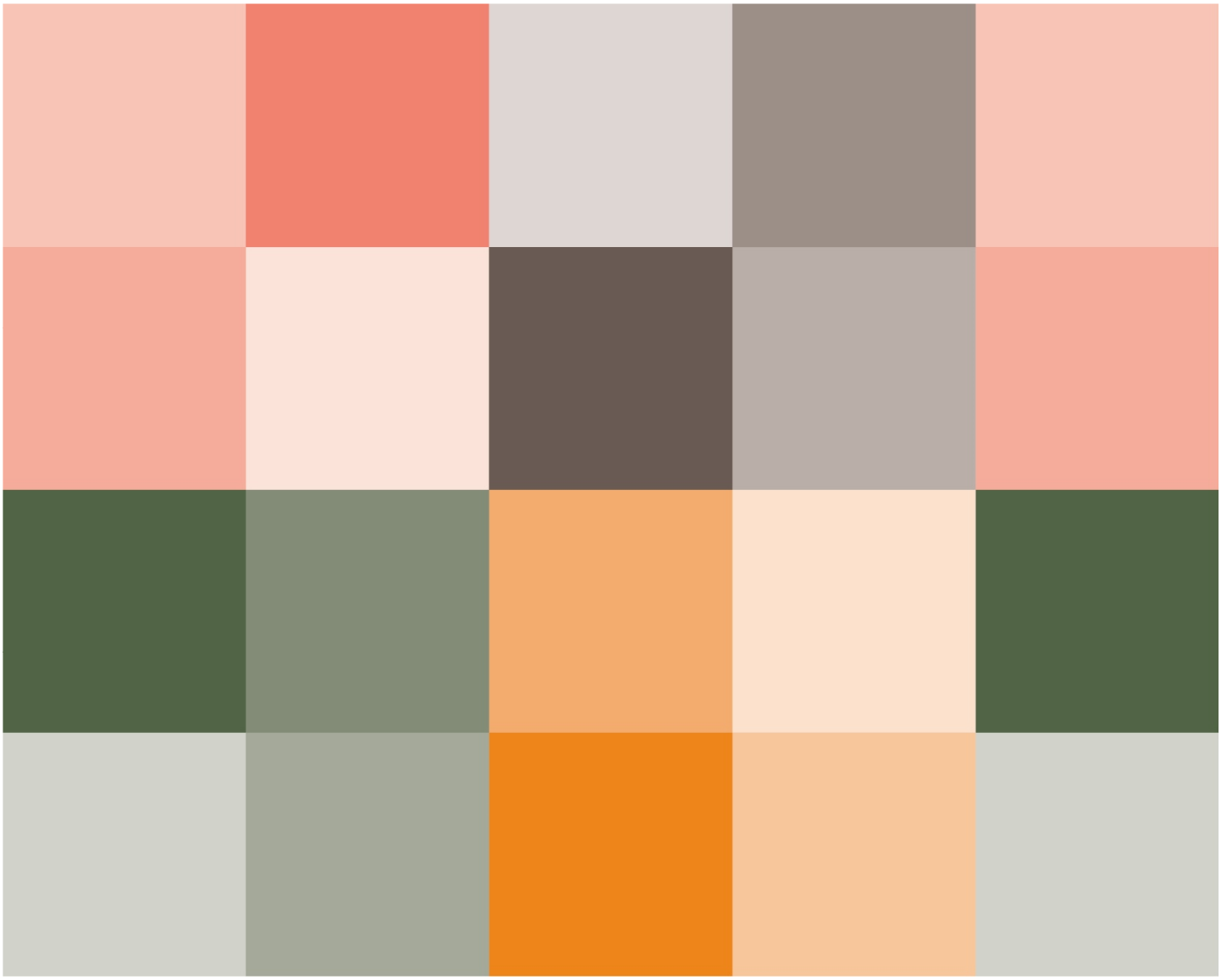


Transportprofil AS4

Beskrivning av tekniska transportprofil för AS4

Version: 1.0

Målgrupper: IT-arkitekter, utvecklare

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Sammanfattning av transportprofil för AS4

Denna transportprofil beskriver hur accesspunktsfunktioner ska vara konfigurerade för att agera i en federations transportinfrastruktur. Profilen är en specificering och delmängd av den profil som tagits fram av CEF/EU-kommissionen.

Identitet: digg-transport-as4-v1_0

Version: 1.0

Livscykelstatus: Fastställd

Ägare: DIGG

Nyckelord: transportprofil;AS4;pmode

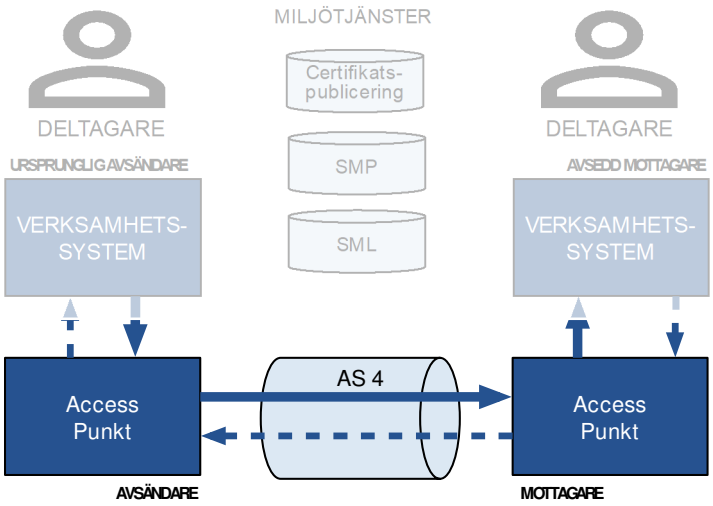
Innehållsförteckning

1 Inledning

Kort beskrivning av dokumentet

Detta dokument specificerar hur information utbyts mellan accesspunktsoperatörer enligt kommunikationsprotokollet AS4 och med ytterligare precisering av CEF eDelivery AS4 Profile.

Denna transportprofil beskriver enbart avvikelser från, restriktioner av och preciseringar till de underliggande eDelivery specifikationer som ska användas för kommunikation inom transportinfrastrukturen. För detaljerad information hänvisas till underliggande specifikationer.



Figur 1Illustration av transportprofilens fokus

Denna AS4-profil använder en delmängd funktionaliteten som beskrivs i CEF eDelivery AS4-profilen.

Denna AS4-profil använder miljötjänsterna SML och SMP.

1.1 Målgrupper

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

Intressenter:

- IT-arkitekter och utvecklare
  - Som utvärderar, analyserar, designar, bygger, och testar programvaror.

1.2 Dokumentstruktur

Detta dokument innehåller följande delar:

- Övergripande beskrivning
- Parametersättning av AS4 (P-Modes)
- Kompletterande regler och beskrivningar kring accesspunktsfunktions användning av AS4

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 Referenser

Referens till	Länk	Kommentar
AS4	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html	Standardprofil av transport-protokollet ebMS v3
[CEFAS4] CEF eDelivery AS4 Profile	https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4	

1.4 Federationsspecifika anpassningar

Detta dokument innehåller ett par regler, krav eller principer som en federation kan anpassa i federationsdeklarationen. Dessa anpassningspunkter är numrerade enligt formen [A1],[A2] osv.

2 Profilering av AS4

2.1 Sammanfattning

Detta dokument specificerar hur information utbyts mellan Accesspunktsoperatörer enligt kommunikationsprotokollet AS4 och med ytterligare precisering av CEF eDelivery AS4 Profile.

Transportprofilen använder och preciserar följande underliggande tekniska profiler:

- eDelivery AS4 Profile, version: 1.15, och dess ”Common profile”.

2.2 Övergripande beskrivning av transportkommunikation med AS4

Denna profil erbjuder följande grundläggande egenskaper.

[a]	En accesspunktsfunktion måste använda och följa de riktlinjer som beskrivs nedanstående tabell

Functionality	ebMS 3.0 AS4
Core Messaging	Web Services
Internet Transport	HTTP 1.1
Transport Layer Integrity, Sender Authentication, Receiver Authentication and Message Confidentiality (Non-Persistent)	Transport Layer (SSL / TLS) Security
Message and PayloadPackaging	SOAP 1.2 with attachments
Routing and Dispatching, SOA integration	Mandatory "Service" and "Action" header elements
Exchange Patterns	One Way
Exchange Pattern Bindings	Push
Payload Compression Kompression av nyttolast	Gzip (**)

Functionality	ebMS 3.0 AS4
Message Identification	ebMS 3.0 "MessageId"
Message Correlation	ebMS 3.0 "ConversationId"
Message Timestamp	ebMS 3.0 "Timestamp" and WS-Security "Timestamp"
Party Identification för Accesspunkter	ebMS 3.0 "From" and "To" party identifiers.
Party Identification för Deltagare	BusinessInfo/originalSender och finalRecipient
Non-Repudiation of Origin	WS-Security 1.1 using XML Signature
Message Confidentiality	WS-Security 1.1 using XML Encryption
Non-Repudiation of Receipt	Signed Receipt Signal Message
Reliable Message	AS4 reception awareness feature for lightweight, interoperable reliable messaging

2.3 Detaljerad beskrivning av transportprofil

2.3.1 P-Mode parametrar

P-Mode-parametrar är ett koncept som används inom ebMS/AS4 för att referera till de konfigurationsuppgifter som gäller för ett visst standardiserat informationsutbyte. Tabell nedan visar de parametrar som har preciserats jämfört med CEF AS4 Profile som denna profil baseras på. I de fall denna profil inte ger information om en konfigurationsparameter så nyttjas CEF AS4 Profile. Kolumnen ”Värde som ska användas” förklarar på vilket sätt som parametern ska användas för att vara följsam gentemot denna transportprofil.

Processing Mode Parameter	Värde som ska användas
PMode.BusinessInfo.Service	Det Process-ID som avses. [a] Den typ av process (SMP ProcessIdentifier) som avses, Exempel: bdx:noprocess **Mappning SMP:** *SignedServiceMetadata/ServiceMetadata/ServiceInformation /Processlist/Process/ProcessIdentifier*
PMode.BusinessInfo.Service.type	Identifieringsystem för Process-ID [b] Fast värde för Service type: urn:fdc:digg.se:edelivery:process **Mappning SMP:** *SignedServiceMetadata/ServiceMetadata/ServiceInformation /Processlist/Process/ProcessIdentifier@type*

PMode.BusinessInfo.Action	[c] Den typ av meddelande/tjänst (SMP DocumentIdentifier) som avses, ska anges enligt följande struktur: «scheme id»::«document identifier» Exempel: busdox-docid-qns:: urn:riv:infrastructure:messaging:MessageWithAttachments:3::messagePayload##3.0::tm-base-ext-sigenc **Mappning SMP:** *SignedServiceMetadata/ServiceMetadata/ServiceInformation /DocumentIdentifier* Och *SignedServiceMetadata/ServiceMetadata/ServiceInformation /DocumentIdentifier/@scheme*
PMode.BusinessInfo.MPC	[d] Fast värde enligt CEF eDelivery AS4-profil: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultMPC
PMode.Protocol.Address TransportProfile	[e] Fast värde för identifierare av transportprofil: digg-transport-as4-v1_0 **Mappning SMP:** *SignedServiceMetadata/ServiceMetadata/ServiceInformation /Processlist/Process/ServiceEndpointList /Endpoint/@transportProfile*

PMode.Security.X509.Signature.Certificate	Accesspunktscertifikat som använts för signering av sändande AP [f] Accesspunktscertifikat som används ska vara det certifikat som tilldelats Accesspunktsoperatören för aktuell federation och miljö.
PMode.Security.X509.Encryption.Certificate	Mottagande accesspunktscertifikat som används för kryptering av sändande AP [g] Accesspunktscertifikat som används för kryptering ska vara det som mottagande accesspunktsfunktion publicerat som en del i ServiceMetadatat. **Mappning SMP:** *SignedServiceMetadata/ServiceMetadata/ServiceInformation /Processlist/Process/ServiceEndpointList /Endpoint/Certificate*
PMode.MEP	[h] Fast värde för MEP enligt CEF eDelivery AS4-profil: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay
PMode.MEPBinding	[i] Fast värde för MEP-binding enligt CEF eDelivery AS4-profil: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/push
PMode.Initiator.Party	[j] Initiator Party ska anges med värden för Common Name på avsändarens accesspunktscertifikat (C2). Exempel: AP0040-SDK-PROD
PMode.Initiator.Party.type	[k] Fast värde för Initiator Party type: urn:fdc:digg.se:edelivery:transportprofile:as4:partytype:ap

PMode.Initiator.Role	[l] Fast värde för initiator Role enligt CEF eDelivery AS4-profil: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator
PMode.Responder.Party	[m] Responder Party ska anges med värdet för Common Name på mottagarens Accesspunktscertifikat (C3). Exempel: AP0045-SDK-PROD
PMode.Responder.Party.Type	[n] Fast värde för Responder Party type: urn:fdc:digg.se:edelivery:transportprofile:as4:partytype:ap
PMode.Responder.Role	[o] Fast värde för Responder Role: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder
PMode.BusinessInfo.Properties – originalSender	Identifieraren för sändande Deltagare (C1) [p] originalSender ska anges och ha värdet för sändande Deltagare
PMode.BusinessInfo.Properties – finalRecipient	Identifieraren för mottagande Deltagare (C4) [q] finalRecipient ska anges och ha värdet för mottagande Deltagare **Mappning SMP:** *SignedServiceMetadata/ServiceMetadata/ServiceInformation/ParticipantIdentifier*

2.4 Användning av TLS

Denna profil specificerar grundregler (default) för användning av TLS (Transport Layer Security). I det fall regeln anpassas specificeras det i federationsdeklarationen.

2.4.1 Certifikatsutgivare

Grundregel [a]

TLS ska användas och endast utgivare av TLS-certifikat som finns på ”Mozilla Network Security Services” lista ”List of pre-loaded CA-certificates) ska användas. TLS-konfigurationen ska vara åtminstone av ”grade A” enligt SSL Labs gradering.

Anpassning [A1]

Specificering av accepterade utgivare för TLS-certifikat

2.4.2 Autentiseringsmetod

Grundregel [b]

Accesspunktsfunktioner som agerar i eDelivery transportinfrastruktur ska använda ”one-way authentication”.

Anpassning [A2]

Om ”two-way authentication” (mutual TLS) ska användas i stället för grundprincipen ”one-way authentication”

2.4.3 Portar för SSL/TLS-trafik

Grundregel [c]

Port 443 ska användas för TLS

Anpassning [A3]

Om andra portar än 443 får användas för TLS vid utväxling av meddelanden mellan accesspunktsfunktioner

2.5 Felhantering vid felaktig mottagare/tjänst

En accesspunktsfunktion behöver ha funktionalitet för att kontrollera att inkommande anrop överensstämmer med den avsedda mottagaren och meddelandetyp.

[a] Accesspunktsfunktionen ska kontrollera att den betjänar den adresserade Deltagaren för den specifika meddelandetypen.

[b] Om den adresserade Deltagaren inte betjänas för den specifika meddelandetypen, kan accesspunktsfunktionen avvisa meddelandet och synkront returnera ett ebMS-Error.

[c] Om accesspunktsfunktionen använder ebMS-Error för att avvisa meddelanden ska felkodattributet sättas till *EBMS:0004* (Other Error) och dess allvarlighetsattribut ska sättas till *failure* samt ska errorDetail-attributet ha värdet *NOT_SERVICED* för att indikera att den adresserade Deltagaren inte betjänas av accesspunktsfunktionen.

2.6 Användning av kuvert

Kuverteringsprofil XHE beskriver hur ett meddelande kuverteras. Kuvertet bär på information som accesspunktsfunktionen använder för adressuppslagning i SMP samt parametersättning av AS4 SOAP. Kuvertet bär även på en identifierare för den federation som accesspunktsfunktionen ska förmedla meddelandet inom.

[a]	Meddelanden som utväxlas i eDelivery transportinfrastruktur ska vara kuverterade i enlighet med *Kuverteringsprofil XHE.*
[b]	Accesspunktsoperatören måste tillse att Deltagaren den betjänar är godkänd för att delta i federationen.

2.7 Spårning av konversationer

Meddelandet som förmedlas har i kuvertet en globalt unik identifierare som en accesspunktsfunktion kan använda för spårning.

[a]	SOAP-attributet ConversationID ska innehålla den globalt unika identifieraren för meddelandets kuvert (Kuverteringsprofil XHE).

2.8 Hantering av stora meddelanden

Denna profil specificerar grundkrav (default) för accesspunktsfunktioners kapacitet att skicka och ta emot stora meddelanden. Med storlek avses antal Byte som meddelandet (XHE inklusive nyttolast[1]) upptar när meddelandet lagras som en xml-fil. I det fall regeln anpassas specificeras det i federationsdeklarationen.

Grundregel [a]	Accesspunktsfunktionen ska ha kapacitet att ta emot och skicka meddelanden med en storlek av minst 100 MB
Anpassning [A4]	Nedre storleksgräns på meddelande som en accesspunktsfunktion åtminstone ska kunna ta emot och skicka.

2.9 Validering av nyttolast

Validering av nyttolast (genom XML-schema, schematron mm) görs av Deltagarens verksamhetssystem/meddelandetjänst. Återkoppling av validering görs i en egen försändelse genom en separat meddelandekvittens som skapas av Deltagarens verksamhetssystem/meddelandetjänst.

Resultat av validering av nyttolast ska alltså inte återrapporteras genom den synkrona AS4-kvittensen.

2.10 Användning av PKI

Alla försändelser som utväxlas mellan accesspunktsfunktioner i eDelivery transportinfrastruktur ska signeras och krypteras på AS4/SOAP-nivå.

Certifikat för kryptering hämtas genom att accesspunktsfunktionens certifikat publiceras som en del av service metadatat.

[1] Notera att då XML-encryption i XHE används kan nyttolasten bli större än i klartext.

Accesspunktsfunktionen ska vara konfigurerad för att acceptera försändelser till/från andra accesspunktsfunktioner i samma federation, det vill säga sådana accesspunktsfunktioner som har certifikat utgivna av samma intermediära certifikatsutgivare.

[a]	Den sändande accesspunktsfunktionen måste kontrollera att mottagande accesspunktsfunktion är godkänd för att agera i federationen och miljön genom att verifiera att certifikatet är utfärdat av aktuell CA
[b]	Den sändande accesspunktsfunktionen ska kontrollera mottagande accesspunktsfunktions certifikat gentemot spärrlista.

Sändande accesspunktsfunktion använder sitt certifikat för att signera försändelsen.

[c]	Den mottagande accesspunktsfunktionen måste kontrollera att sändande accesspunktsfunktion är godkänd för att agera i federationen och miljön genom att verifiera att certifikatet är utfärdat av aktuell CA
[d]	Den mottagande accesspunktsfunktionen ska kontrollera sändande accesspunktsfunktions certifikat gentemot spärrlista.
[e]	Om en Accesspunktsoperatör är godkänd för att agera i flera federationer parallellt ska accesspunktsfunktionen hanteras isolerat för varje federation.
[f]	Accesspunktsfunktionen ska vara konfigurerad för att lita på det certifikat som används av SMP för signering av metadata i aktuell federation och miljö
[g]	Accesspunktsfunktionen ska kontrollera SMP-certifikat gentemot spärrlista.