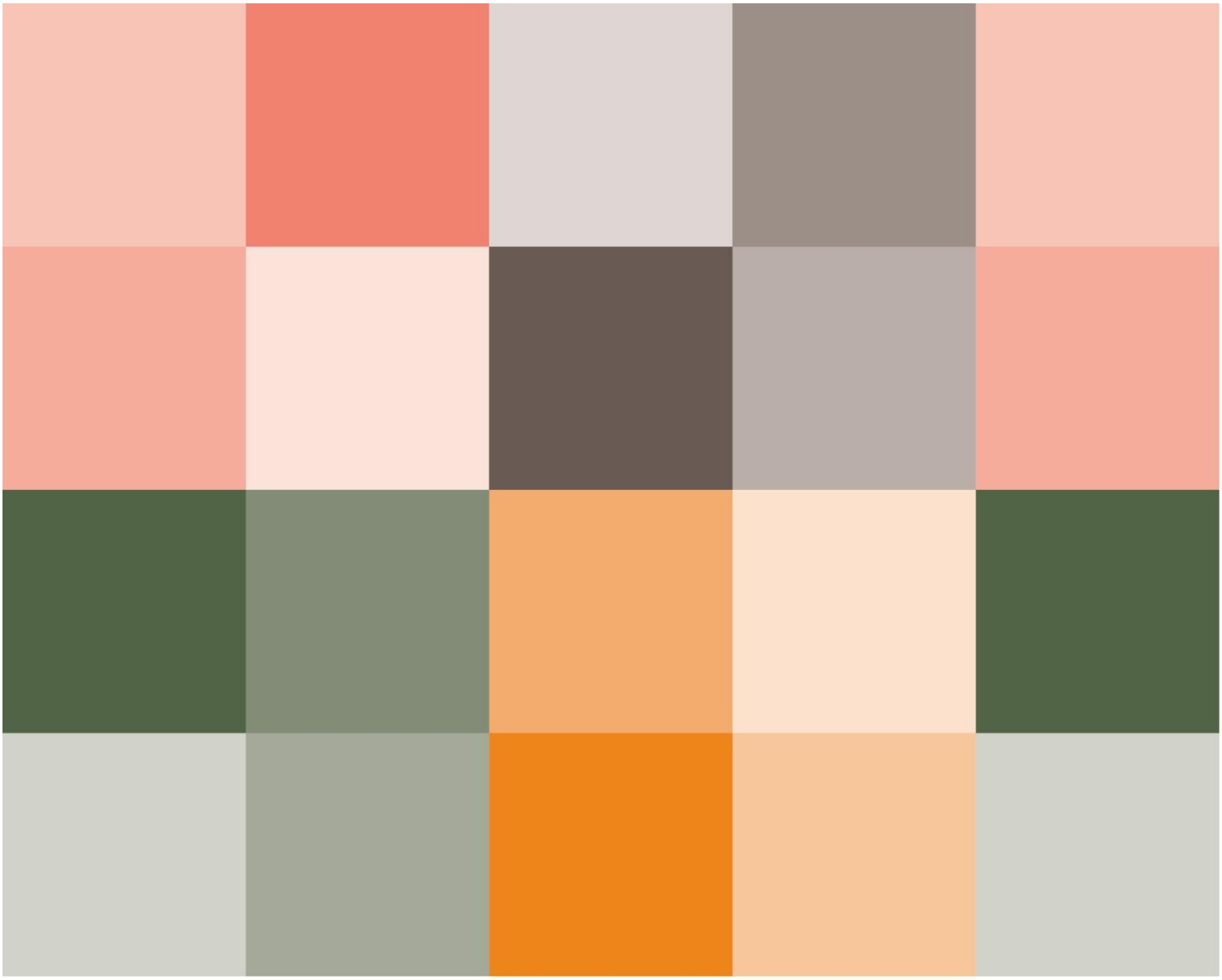


SMP

Komponentspecifikation

Version: 1.0 Målgrupper: Verksamhetsutvecklare, IT-Arkitekter

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Sammanfattande beskrivning av komponenten SMP

Detta dokument innehåller specifikation av komponenten:

Benämning: SMP

Version: 1.0

Livscykelstatus: Fastställd

Ägare: DIGG

Nyckelord: Metadata; Uppslagning; Tjänst; Adressering; eDelivery; Dynamisk

SMP komponenten möjliggör en gemensam struktur för publicering av Deltagares tjänsters metadata, en viktig del i digitaliseringsarbetet i offentlig sektor. Det publicerade metadatat är signerat för att garantera riktighet och följer standard: Specifikation Oasis SMP SPEC 1.0. Varje instans hanterar en miljö i en federation.

SMP är uppdelad i en administrationsdel och en uppslagsdel. Dessa har olika servicenivåer. Administrationsdelen har krav på sig att vara tillgänglig under kontorstid, medan uppslagsdelen ska kunna vara tillgänglig utifrån specifikation per miljö.

Aktörer som samverkar med SMP administrationsdel har olika roller, systemadministratör, federationsadministratör, och accesspunktsadministratör. Uppslag av metadata är publikt tillgängligt.

SMP ska registreras i en SML så att accesspunkter och andra kan hitta rätt SMP instans.

Som en del av plattformen ger SMP följande nyttor:

- Den möjliggör tillits- och certifikatshantering mellan accesspunkter
- Den säkerställer dataintegritet för accesspunktsoperatören genom användning av digitala signaturer.
- Den gör att en accesspunkt kan hitta en deltagare.

Innehållsförteckning

1 Inledning

Inledande beskrivning av komponenten SMP

Syftet med Service Metadata Publisher (SMP) komponenten är att lagra och distribuera servicemetadata om Deltagare i den federation och miljö där komponenten används.
Komponenten är uppdelad i en publiceringsdel och en administrationsdel.

Publiceringsdelen är den del där servicemetadata publiceras och kan kommas åt i realtid för att en accesspunkt skall kunna genomföra en meddelandeöverföring enligt ramverket.

Administrationsdelen är den del där servicemetadatat hanteras (läggs till, tas bort eller uppdateras) och är skyddad av stark autentisering.

SMP komponenten består av följande delar:

- Publiceringsdel
    - API: ServiceGroup
    - API: SignedServiceMetadata
    - GUI: Saknas
- Administrationsdel
    - API: Saknas (endast för intern användning)
    - GUI: Administration
- Information
    - Publiceringsinformation
    - Administrationsinformation

1.1 Beroenden till specifikationer och komponenter

Denna specifikation är följsam mot följande specifikationer eller dokument

- Service Metadata Publishing (SMP) Version 1.0 (oasis-open.org)
    - http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/bdx-smp-v1.0.html

Denna komponent beror av att följande komponenter finns tillgängliga:

- Service Metadata Locator (SML)

Denna komponent förbättras genom användning av följande komponenter:

- PKI för Accesspunkter (PKI)
- CertifikatPublicering (CertPub)

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
SMP-OASIS	http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/bdx-smp-v1.0.html	Specifikation av API för publiceringsdel.
SMP-SPEC	https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+SMP+-+1.10	Riktlinjer för implementation av en SMP.
MSB-KLASS	https://www.msb.se/RibData/Filer/pdf/25602.pdf	MSB's modell för klassning av information.

2 För Verksamhetsutvecklare

2.1 Inledning

SMP gör att de accesspunkter som ingår i en eDelivery federation kan registrera sina deltagare, samt slå upp andras deltagare och ta reda på deras adresser i plattformen och vilka meddelanden som kan skickas till dem.

2.2 Egenskaper hos komponent

SMP håller information om deltagare och deras metadata. Detta metadata kan slås upp av accesspunkter. Metadata innehåller adresser i plattformen och tjänster. SMP's publiceringsdel är alltid tillgänglig och kan i sin tur nås via uppslag i SML.

2.3 Nyttor med användning

SMP är en nödvändig del av en eDelivery miljö. SMP gör att accesspunkter kan skicka meddelanden mellan varandra utan att en accesspunkt i förväg behöver känna till andra accesspunkter eller vilka deltagare som hanteras av denna.

2.4 Hur komponenten fungerar

SMP håller internt registrerade accesspunktsoperatörer och deras deltagare. Ett GUI finns för att uppdatera information För att administratörer ska få tillgång till detta GUI behöver de registrera sig via DIGG.

2.5 Villkor och förutsättningar för användning

För att använda SMP behöver en accesspunktsoperatör teckna avtal med DIGG för varje miljö inom en specifik federation. En deltagarorganisation behöver teckna avtal med federation för att dess metadata ska kunna slås upp i SMP.

En SMP implementation behöver godkännas av DIGG för att få användas inom en federation som DIGG hanterar.

2.6 Aktörer och roller

Roll	**Beskrivning**
Accesspunktsoperatör	Hanterar registrering av egna deltagare och deras metadata.
Alla	Kan slå upp deltagare och deras metadata

Systemadministratör	Hanterar accesspunkter och användare.
Federationsoperatör	Hanterar deltagares status inom en federation.

För att en användare hos en aktör ska kunna tilldelas någon av rollerna behöver den vara godkänd och registrerad av DIGG samt vara starkt autentiserad (med e-legitimation) vid inloggning. En användare måste kunna kopplas till en enskild person.

2.7 Översiktliga användningsfall

2.7.1 AF: Upplägg av accesspunkt

En ny accesspunkt har tillkommit och behöver registreras i SMP.

Användningsfall	
Beskrivning	En accesspunkt (AP) registreras i SMP.
Roller	AF utförs av Federationsadministratör
Antaganden	Accesspunkten finns i federationen.
Flöde	Accesspunkten läggs in, därefter sätts minst en användare som accesspunktsadministratör för denna AP. Notera att inläggning i användarregister för inloggning behöver ske separat från SMP.
Resultat	Accesspunkten finns i SMP och accesspunktsadministratören kan lägga in deltagare för denna..
Verksamhets-regler	En accesspunkt måste vara godkänd innan den läggs in.
Exempel	-

2.7.2 AF: Upplägg av deltagare

En deltagare läggs in i SMP.

Not: Även en programvara som ger ett API för detta kan anses följa denna komponentspecifikation.

Användningsfall	
Beskrivning	Ett deltagare konfigureras
Roller	AF utförs av Accesspunktsadministratör (AA)
Antaganden	Deltagaren finns i federationen.
Flöde	AA lägger in deltagare och registrerar dess information.
Resultat	Deltagaren väntar på godkännande av federationsadministratör.
Verksamhets-regler	Deltagarens metadata kommer inte att publiceras förrän den har blivit godkänd..
Exempel	-

2.7.3 AF: Godkännande av deltagare

Granskning och godkännande av deltagare.

En användare i rollen Federationsadministratör granskar en deltagare som väntar på godkännande. Federationsadministratören godkänner deltagaren, deltagarens metadata blir då tillgängliga för uppslag. SMP registrerar också deltagaren i SML som tillhörande till denna SMP.

Alternativt flöde: Deltagaren godkänns inte. Accesspunktsoperatören kan senare uppdatera eller ta bort deltagaren ur SMP. GUI:Administration används för detta.

Användningsfall	
Beskrivning	En deltagare granskas.
Roller	AF utförs av Federationsadministratör (FA)
Antaganden	Deltagararen ingår i federationen..
Flöde	FA ser att deltagare behöver granskas och godkänner. (Altarnativflöde, deltagaren godkäns inte)
Resultat	Om deltagaren godkänts (och har metadata) kommer den att publiceras i SML.
Verksamhets-regler	Om deltagaren ej godkänns måste FA och AA tillsammans reda ut vad som behövs för godkännande..
Exempel	-

2.7.4 AF: Uppslag av metadata

En accesspunkt behöver veta hur den ska kontakta en deltagare. Efter att ha slagit upp deltagaren i SML har accesspunkten hittat SMP för deltagaren.

Accesspunkten slår upp deltagaren och för information om vilken accesspunkt som hanterar deltagaren och vilka tjänster som deltagaren ger. API:Servicegroup och API:SignedServiceMetadata används för detta.

Användningsfall	
Beskrivning	Uppslag av metadata
Roller	AF utförs av deltagare eller accesspunkt via API. (Ingen kontroll av behörighet görs.)

Antaganden	Deltagaren finns registrerad i SMP.
Flöde	Klient har slagit upp deltagare i SML och fått DNS-adress till SMP för deltagare. Klient anropar adressen och får servicegroup från SMP. Data i denna används för att klienten ska slå upp metadata för specifika tjänster.
Resultat	Klienten har önskat metadata.
Verksamhets-regler	Metadata är signerat så att klienten kan verifiera att det är korrekt.
Exempel	-

2.8 API: Servicegroup

Detta API ger information om en deltagare samt vilka services den har. Svaret innehåller en länk till detaljerad information om varje service där den detaljerade informationen följer API:SignedServiceMetadata.

Detta API följer specifikation i [SMP-OASIS].

2.9 API: SignedServiceMetadata

Detta API ger metadata som behövs för att genomföra en översändelse av en meddelandetyp till en Deltagare. Informationen som returneras i funktionen är signerad.

Detta API följer specifikation i [SMP-OASIS].

2.10 GUI: Administration

Detta GUI används av användare med samtliga roller men rollen avgör vilka detaljsidor som användaren får se och vilka data som får ses och ändras.

Accesspunktsoperatörer begränsas så att de endast får se deltagare som hör till de accesspunkter som de är ansvariga för. En accesspunktsoperatör kan dock hantera flera accesspunkter.

2.11 Informationsmodell: Publiceringsinformation

Informationsmodellen för publicerat data är i sin helhet importerad från Oasis-specifikationen. Möjligheten till ”Redirect” som finns med i Oasis finns inte med i denna version av SMP. I loggar tas med information som behövs för att kunna leverera tjänst på ett enligt övriga krav.

2.11.1 Informationssäkerhetsklassning

DIGG har klassificerat komponenten utifrån det metodstöd och rekommendationer som Myndigheten för samhällsskydd och beredskap (MSB 0040-09) tagit fram för informationsklassificering, se [MSB-KLASS].

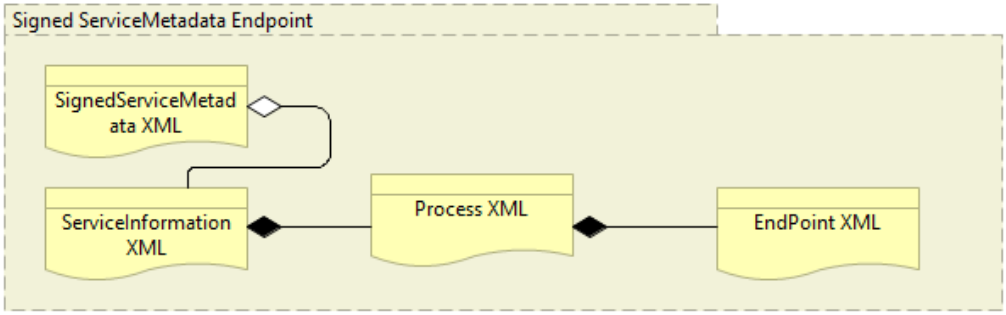
SMP Publiceringstjänst – Informationssäkerhetsklassning

Komponent	Konfidentialitet	Riktighet	Tillgänglighet
• Information om användarorganisationens (party) metadata.	Nivå 0 - Försumbar	Nivå 3 - Allvarlig	Nivå 2 - Betydande
• Teknisk adress till AP	Nivå 0 - Försumbar	Nivå 3 - Allvarlig	Nivå 2 - Betydande
• Loggar	Nivå 2 - Betydande	Nivå 3 - Allvarlig	Nivå 1 – Måttlig

2.11.2 Översikt

Uppslag i Participant Endpoint ger en deltagare och en lista med id på dess metadata. Utifrån id i denna lista kan det signerade metadatat slås upp.

Service Group XML innehåller service metadata, däremot inte signerat metadata.



2.12 Informationsmodell: Administrationsinformation

Informationsmodellen behöver göras så att allt metadata som levereras från publiceringsdelen kan hanteras samt att säkerhet och rollhantering kan upprätthållas. I loggar tas med information som behövs för att kunna leverera tjänst samt spåra vad en användare har gjort. Systemadministratör kan se loggar över samtliga händelser, en accesspunktsoperatör kan se loggar över vad som hänt för dennes accesspunkter.

2.12.1 Informationssäkerhetsklassning

Klassificering enligt [MSB-KLASS].

SMP Administrationsdel - Informationssäkerhetsklassning

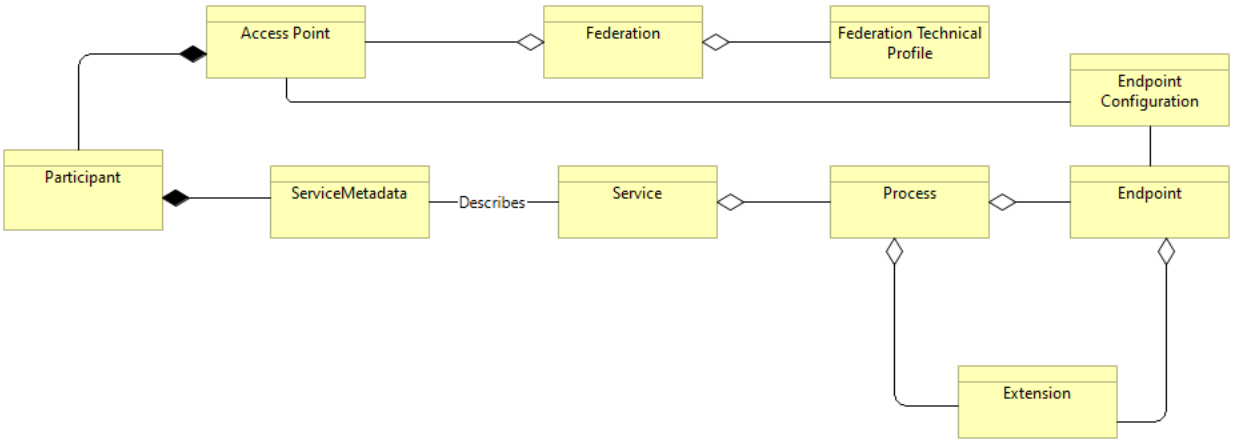
Komponent	Konfidentialitet	Riktighet	Tillgänglighet
• Information om användarorganisatio	Nivå 1 - Måttlig	Nivå 3 - Allvarlig	Nivå 1 - Måttlig -

nens (party) metadata.			
• Teknisk adress till AP	Nivå 1 - Måttlig	Nivå 3 - Allvarlig	Nivå 1 – Måttlig
• Loggar	Nivå 2 - Betydande	Nivå 3 - Allvarlig	Nivå 1 – Måttlig
• Användare	Nivå 2 - Betydande	Nivå 3 - Allvarlig	Nivå 1 – Måttlig

2.12.2 Översikt

Federation och Federation Technical Profile specificerar vilka typer av processer som kan ingå i federationen. Endast en Federation får finnas i varje instans av SMP.

Endpoint Configuration definieras per service provider (Access Point) och används som mall för de Endpoints som finns för service providerns deltagare.



2.13 Informationssäkerhet- och tillit

Komponentens uppgift är att publicera, administrerar samt lagra och distribuera servicemetadata om Deltagare i den federation och miljö där komponenten används. För informationssäkerhet- och tillit så finns styrande regler och rutiner för komponenten beskriven i transportinfrastrukturen.

Komponenten är uppdelad i en

- Publiceringsdel där servicemetadata publiceras och distribueras signerat i realtid för att accesspunkt skall kunna genomföra meddelandeöverföring. Åtkomsten skyddas med funktionscertifikat.
- Administrationsdel där servicemetadatat hanteras (läggs till, tas bort eller uppdateras) är skyddad av stark autentisering(identifiering) och auktorisering(behörighet) för registrerade administratörer.

Säkerhetsåtgärder och servicenivåer finns övergripande beskrivna i transportmodeller samt miljöer per federation.

2.14 Stödmaterial

Inget specifikt stödmaterial finns för denna komponent.

3 För IT-arkitekter

Information som är riktad till IT-arkitekter

3.1 Inledning

En SMP måste uppfylla de villkor som ges i [SMP-OASIS] och [SMP-SPEC].

3.2 Tekniska villkor och förutsättningar för användning

Komponenten behöver köras med brandväggar för inkommande och utkommande trafik. Utåt ska endast möjlighet för uppdatering mot SML finnas.

Inåt ska API för hämtning av metadata vara öppet för samtliga klienter medan API och/eller användargränssnitt för administration skyddas med säker autentisering.

Uppdatering via administrationsgränssnittet ska loggas.

3.3 Tekniska aktörer och roller

Se även avsnitt 2.6.

Roll	**Beskrivning**
Driftansvarig	Utför de tekniska användningsfallen.
Förvaltningsansvarig	Beslutar när uppgradering ska göras.

3.4 Översiktliga tekniska användningsfall

Se även avsnitt 2.7.

3.4.1 Tekniskt AF: Backup

Backup av den information som lagts in i SMP ska göras regelbundet.

3.4.2 Tekniskt AF: Återställning

Om något har hänt med SMP som har gjort att data är felaktigt så ska data återställas från senast korrekta backup.

3.4.3 Tekniskt AF: Uppgradering

Om en ny version av SMP finns tillgänglig och det är beslutat att den ska användas så ska den nya versionen ersätta den gamla. Alla data som fanns innan ska finnas tillgängliga efteråt. Detta kan göras genom Backup/Återställning eller genom att data finns kvar sedan den tidigare versionen. En uppgradering ska göras så att den i minsta möjliga mån stör den ordinarie driften, framför allt uppslagning.

3.5 API

Se avsnitt 2.8 och 2.9

3.6 Tekniskt GUI

Inga andra GUI än de som beskrivs i 2.10 finns specificerade.

3.7 Datamodell: Administrativ information

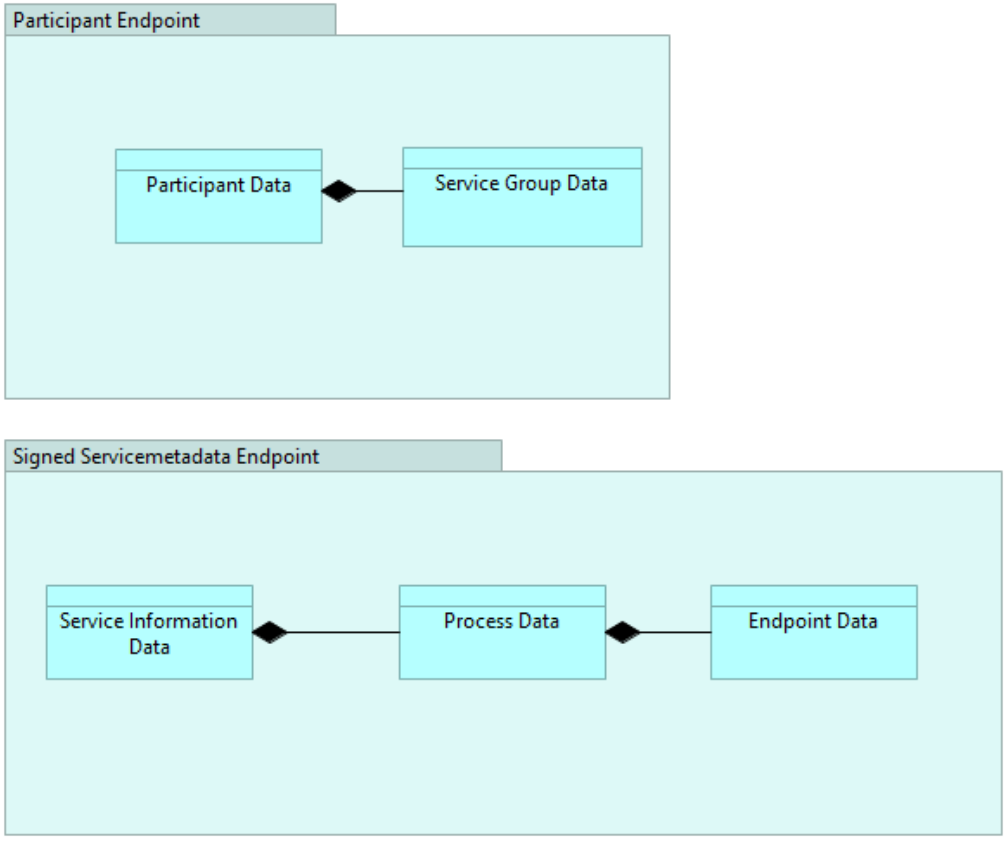
Denna lämnas fritt till implementationen, betrakta dock informationsmodellen i 2.12.

3.8 Datamodell: Publicering

Datamodell för publicerat data ska följa [SMP-OASIS] förutom att användande av Redirect inte krävs.

3.8.1 Översikt

Nedanstående är en mer implementationsinriktad variant av modellerna i 2.8 och 2.9.



3.8.2 IT-säkerhet

SMP's egna nycklar som används för att signera metadata måste hållas säkra.

GUI ska kunna säkras så att användare måste identifiera sig med certifikat.

En Accesspunktsoperatör ska endast kunna se och ändra administrativt som hanteras av den (de) accesspunkt som hanteras av operatören.

En SMP ska kunna begränsas så att de enda utgående kopplingarna görs för att registrera deltagare i SML.

Eftersom uppslag mot publiceringsdelen är öppna och tillgängliga för alla klienter behöver SMP kunna hantera överbelastningsattacker riktade mot publiceringsdelen.

3.9 Open API Specifikation

Ingen Open API specifikation behöver ges av komponenten.

3.10 Teknologisk bindning till REST och XML

Publiceringsgränssnittet använder REST tjänster och levererar data i XML form.

4 Generella servicenivåer

Denna sektion specificerar generella servicenivåer som gäller för tjänster som implementerar denna komponent.

Servicenivåer för programvaror som implementerar denna komponent	
Administrationsdel	**Krav**
GUI	Tillgänglig under kontorstid för typiska användare. Servicefönster kan förekomma
Publiceringsdel	**Krav**
API	Hög tillgänglighet hela dygnet. Exakta värden beror på federation.

5 Appendix

Inga appendix