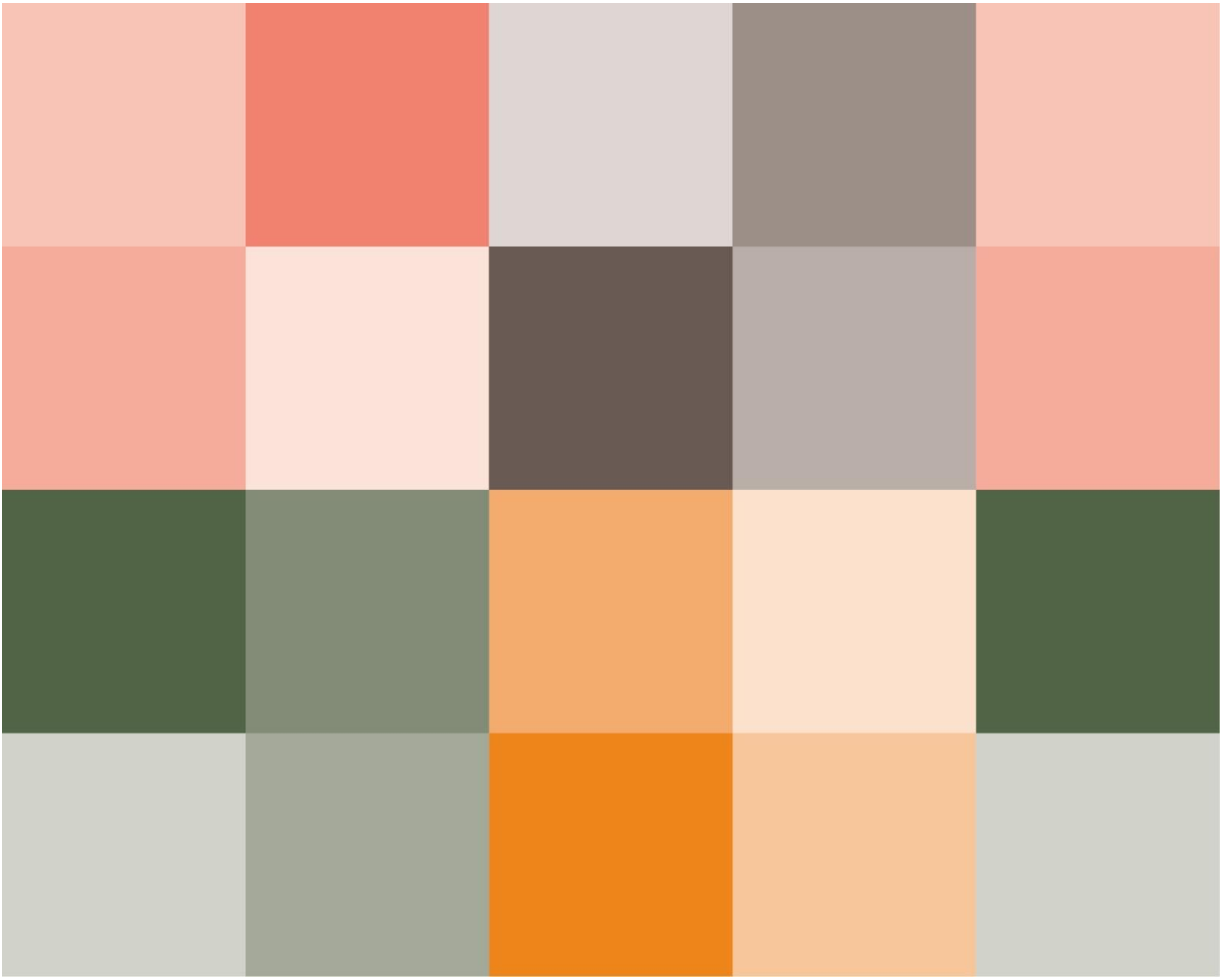


Certifikatspublicering – REST-bindning till SMP

Beskrivning av teknisk REST-bindning för certifikatspublicering

Version: 1.0

Målgrupper: IT-arkitekter, utvecklare

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Denna specifikation beskriver det publika gränssnitt som ger möjlighet att hämta en Deltagarorganisations certifikat. Publicerade certifikat kan användas i två syften – signeringscertifikat och certifikat för kryptering. Kryptering och signering mellan Deltagarorganisationernas system görs i enlighet med Kuverteringsspecifikationen (XHE) och Transportmodell Utökad Bas.

Denna specifikation beskriver inte hur ett certifikat registreras utan beskriver uteslutande hur automatiskt uppslagning och hämtning av publicerade certifikat utförs.

Denna specifikation beskriver hur Certifikatspubliceringstjänsten exponerar certifikat som en utökning av eDelivery servicemetadata (SMP).

Innehållsförteckning

1 Inledning

Denna specifikation beskriver det REST-baserade gränssnitt som används för att hämta certifikat samt det XML-format som används för publiceringen.

Denna specifikation beskriver hur Certifikatspubliceringstjänsten exponerar certifikat som en utökning av eDelivery servicemetadata (SMP).

1.1 Dokumentstruktur

Detta dokument innehåller följande delar:

- Beskrivning av XML-strukturen för publicering av certifikat som en utökning av SMP SignedServiceMetadata
- Beskrivning av hur uppbyggnaden av en REST-baserade URL för att hämta publicerade certifikat

1.2 Målgrupper

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

Intressenter:

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

1.3 Referenser

Referens till	Länk	Kommentar
SMPv1	https://docs.oasis-open.org/bdxr/bdx-smp/v1.0/bdx-smp-v1.0.html	

2 Certifikatspublicering med bindning mot SMP

2.1 Informationsmodell

Tabellen nedan beskriver de uppgifter som är relevanta för certifikatspublicering. Respektive uppgift beskrivs kort samt har en placering (XPATH) i syntaxen SMP v1 SignedServiceMetadata XML Schema. Mer detaljer kring XML-strukturen beskrivs i kapitlet Syntaxmappning.

Informationsentitet	**Beskrivning (placering i parantes)**
Deltagarens identifierare	Den identifierare som Deltagarorganisationen använder eDelivery Transportinfrastruktur *(SignedServiceMetadata/ServiceMetadata/ServiceInformation/ParticipantIdentifier)*
Certifikat	Deltagarens certifikat för signering och kryptering *(SignedServiceMetadata/ServiceMetadata/ServiceInformation/Extension/smc:Certificate/smb:ContentBinaryObject)*
Typ av certifikat	Typ av certifikat (signering eller kryptering) *(SignedServiceMetadata/ServiceMetadata/ServiceInformation/Extension/smc:Certificate/smb:TypeCode)*

2.2 Syntaxmappning

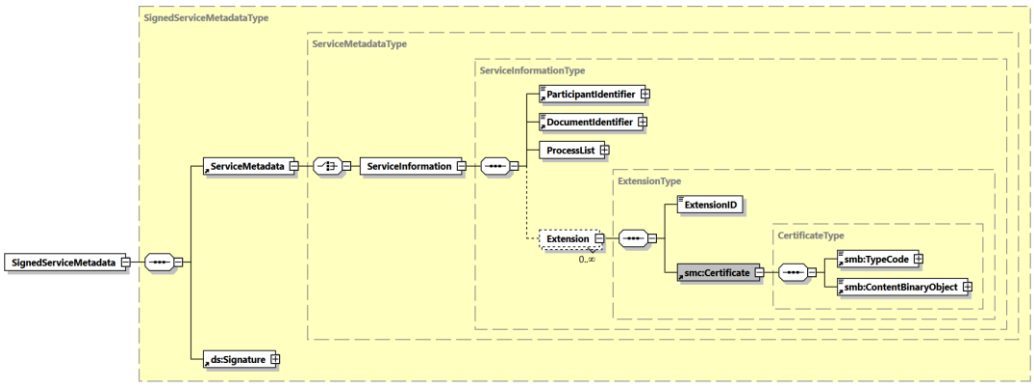
Kard	**Elementnamn**	**Kommentar**
	SignedServiceMetadata	Rot-element
1..1	• ServiceMetadata	
1..1	• • ServiceInformation	
1..1	• • • ParticipantIdentifier	Deltagarens identifierare
1..1	• • • ParticipantIdentifier/@scheme	Typ av identifiare fast värde;

		iso6523-actorid-upis
1..n	• • • Extension	
1..1	• • • • ExtensionID	Typ av extension, Fast värde: urn:fdc:digg.se:edelivery:xml-extension:smp-certpub:1.0
1..1	• • • • smc:Certificate	
1..1	• • • • • smb:TypeCode	Typ av certifikat. Kod för certifikat som använts av sändaren för signering: urn:fdc:digg.se:edelivery:certpub:signing-cert Kod för certifikat som använts för kryptering: urn:fdc:digg.se:edelivery:certpub:encryption-cert
1..1	• • • • • smb:ContentBinaryObject	Certifikatet i PEM-format (BASE64-kodat)
1..1	• • • • • smb:ContentBinaryObject/mimeCode	Fast värde: application/base64

2.2.1 Namnrymder

Namnrymder och exempelprefix som används i XML-strukturen

Prefix	**Namnrymd**
[default]	http://docs.oasis-open.org/bdxr/ns/SMP/2016/05
smc	http://docs.oasis-open.org/bdxr/ns/SMP/2/AggregateComponents
smb	http://docs.oasis-open.org/bdxr/ns/SMP/2/BasicComponents



2.2.2 Lokalisering av certifikat

XPath för lokalisering av certifikat i XML-strukturen

Typ	XPath
Signerings-certifikat	/SignedServiceMetadata/ServiceMetadata/ServiceInformation/Extension[ExtensionID="urn:fdc:digg.se:edelivery:xml-extension:smp-certpub:1.0"]/smc:Certificate[smb:TypeCode="urn:fdc:digg.se:edelivery:certpub:signing-cert"]/smb:ContentBinaryObject
Krypterings-certifikat	/SignedServiceMetadata/ServiceMetadata/ServiceInformation/Extension[ExtensionID="urn:fdc:digg.se:edelivery:xml-extension:smp-certpub:1.0"]/smc:Certificate[smb:TypeCode="urn:fdc:digg.se:edelivery:certpub:encryption-cert"]/smb:ContentBinaryObject

3 REST-bindning

Lokalisering av certifikatspubliceringen enligt denna specifikation använder de principer som gäller för slagning i SMP. En URL byggs upp enligt för DNS/SML-slagning som genom NAPTR anvisar webb-adressen till publiceringstjänsten.

Sändande applikation hämtar krypteringscertifikat genom slagning mot den mottagningstjänst som gäller för meddelandetypen som ska krypteras. Mottagande applikation hämtar signeringscertifikat (för kontroll av att mottaget meddelande är signerat med rätt certifikat) genom slagning mot den mottagningstjänst som används för meddelandekvittens.

En URL byggs upp med hjälp av deltagarens identifierare och den aktuella mottagningstjänsten.

Resurs	URI	HTTP Metod	XML rot element
Certifikats-publicering	/{identifier scheme}::{id}/services/ {docType}	GET	<SignedServiceMetadata>

Exempel:

https://domän/iso6523-actorid-upis%3A%3A0203%3Areceivingexample.se/services/busdox-docid-qns%3A%3Aurn%3Ariv%3Ainfrastructure%3Amessaging%3Amessagewithattachments%3A2%3A%3Amessage%3A%3A2.0%3A%3Atm-base-ext-sigenc

För mer information om REST-bindningen, se [SMPv1] kapitel 3.4.1 REST interface

3.1 Kontroll av resultatets signatur

Certifikatsinformationen ingår i det signerade service-metadata som returneras av tjänsten. Kontroll av signaturen görs enligt principerna i [SMPv1] 3.6.2.2 Verifying the signature.

3.2 Typiskt scenario (icke normativt)

Nedan följer en enkel beskrivning av de steg som avsändare respektive mottagare gör för att nyttja certifikat för signering och publicering.

Förutsättning

Deltagarna har publicerat sina certifikat i Certifikatpubliceringstjänsten.

Avsändaren

1. Skapar nyttolast
2. Hämtar krypteringscertifikat genom att göra en slagning i Certifikatspubliceringstjänsten baserat på mottagarens identifierare och den meddelandetyp (för nyttolasten) som är aktuell
3. Krypterar nyttolast med det certifikat som mottagaren angivit som krypteringscertifikat
4. Placerar krypterad nyttolast i kuvert (XHE)
5. Signerar kuvertet med det egna signeringscertifikatet

6. Skicka

Mottagaren

1. Tar emot meddelande
2. Kontrollerar meddelandets integritet genom att validera signaturens riktighet
3. Hämtar avsändarens signeringscertifikat genom att göra en slagning baserad på avsändarens identifierare och den meddelandetyp som används för meddelandekvittens.
4. Kontrollerar att samma certifikat använts för signering som också hämtats från certifikatpubliceringstjänsten
5. Dekryptera nyttolasten med egna privata nyckeln (som hör ihop med det krypteringscertifikat som avsändaren använt)
6. Validera att nyttolast är följsamt med aktuellt meddelandeformat (XML Schema/schematron eller motsvarande)
7. Skapa kvittensmeddelande och placera i kuvert (XHE)
8. Signera kvittens
9. Skicka kvittens