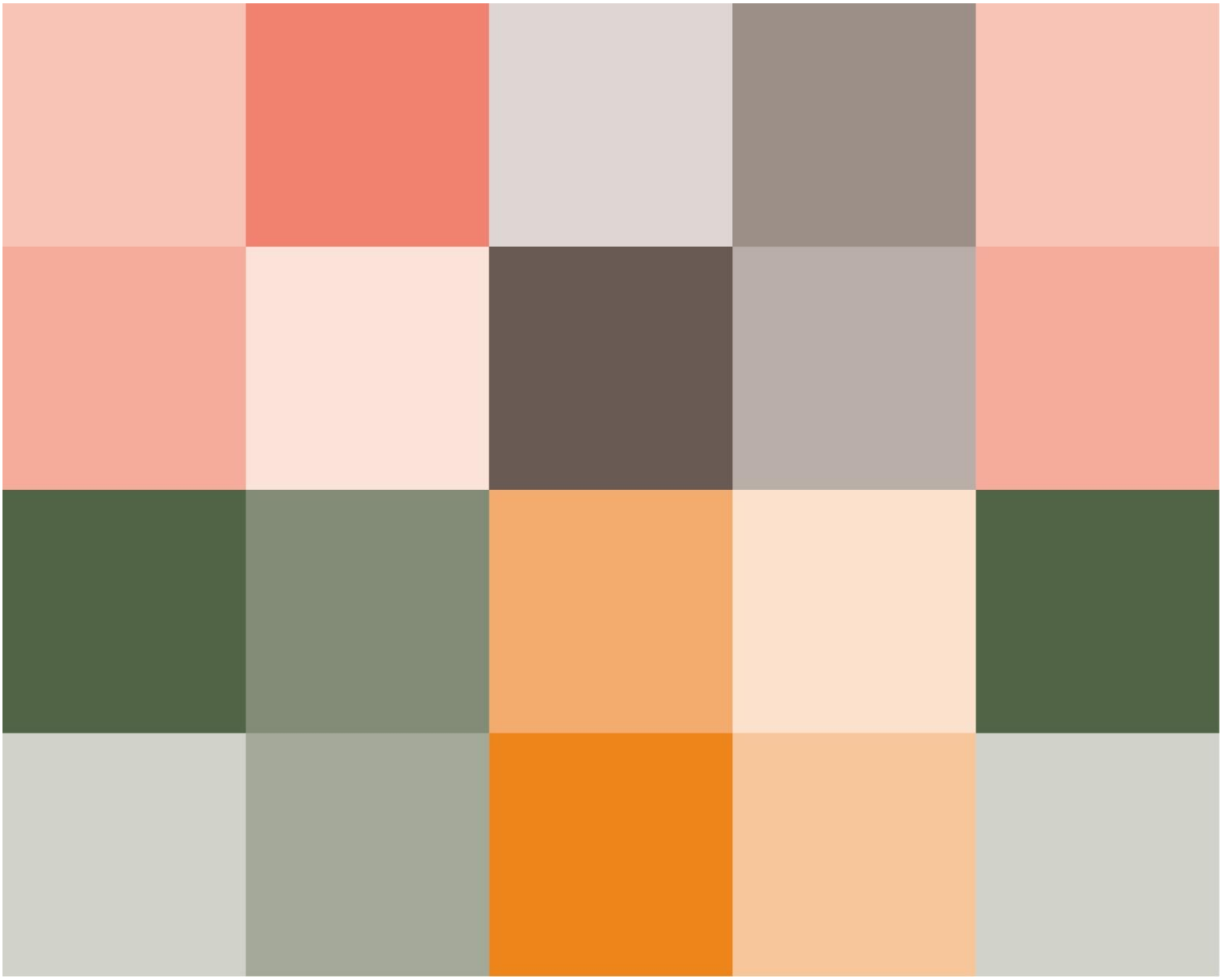

CertPub

Komponentspecifikation

Version: 1.0 Målgrupper: Verksamhetsutvecklare, IT-arkitekter

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Sammanfattande beskrivning av komponenten CertPub

Benämning: CertPub (Certifikatpublicering)

Version: 1.0

Livscykelstatus: Fastställd

Ägare: DIGG

Nyckelord: Certifikat; Deltagarcertifikat; eDelivery; Dynamisk hantering

CertPub ger möjlighet att registrera, publicera och hämta en Deltagares certifikat. Publicerade certifikat kan användas i två syften – signering eller kryptering.

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

Aktörer som samverkar med Certpub administrationsdel har rollen federationsadministratör. Uppslag av certifikat är publikt tillgängligt.

Certpub är specifik för en federation och en miljö.

Som en del av plattformen ger CertPub följande nyttor:

- Den möjliggör tillit och certifikatshantering mellan deltagare genom att
  - Den säkerställer integritet genom att certifikat är digitalt signerade av komponenten.
  - Den möjliggör integritet vid varje överföring av meddelanden mellan deltagare.
- Den säkerställer riktighet och spårbarhet genom krav på säker inloggning i administrationsgränssnittet för att kunna publicera korrekt information.

Innehållsförteckning

1 Inledning

Syftet med CertPub är att registrera, publicera och hämta en Deltagares certifikat. Publicerade certifikat kan användas i två syften – signering eller kryptering.

Detta gör att en deltagare kan slå upp en annan deltagares certifikat för att kryptera ett meddelande till denna eller kontrollera om ett meddelande är signerat av den andra deltagaren.

Komponenten är uppdelad i en publiceringsdel och en administrationsdel.

Publiceringsdelen är den del där certifikat publiceras och kan kommas åt i realtid.

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

Denna komponent består av följande delar:

- Publiceringsdel
  - API:Certifikathämtning
  - GUI: Saknas
- Administrationsdel
  - API: Saknas (endast för intern användning)
  - GUI: Administration
- Informationsmodell
  - Certifikat

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:

- Service Metadata Locator (SML)

- Service Metadata Publisher (SMP)
- PKI för Accesspunkter (PKI)

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
  -

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 SMP. Certifikatspubliceringen kan använda ”extension” här för att returnera certifikat.

MSB-KLASS	https://www.msb.se/RibData/Filer/pdf/25602.pdf	MSB's modell för klassning av information.
X509	https://www.itu.int/rec/T-REC-X.509	Standard för PKI certifikat.

2 För Verksamhetsutvecklare

Information som är riktad till verksamhetsutvecklare

2.1 Inledning

CertPub ger möjlighet till ökad säkerhet och tillit mellan deltagare genom att meddelanden kan krypteras och verifieras.

2.2 Egenskaper hos komponent

Certpub håller de certifikat som används av deltagare för kommunikation inom miljön.

2.3 Nyttor med användning

Risken att någon obehörig får tillgång till information eller kan skicka falsk information undviks.

2.4 Hur komponenten fungerar

CertPub håller internt de registrerade certifikaten för varje deltagare. Dessa läggs upp av en Federationsadministratör och blir sedan publikt tillgängliga.

2.5 Villkor och förutsättningar för användning

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

2.5.1 Situationer där komponenten kan eller ska nyttjas

- CertPub används för att lagra och publicera publika certifikat för deltagare.

2.5.2 Situationer där komponenten ej kan eller ska nyttjas

- Certpub ska inte användas för att lagra certifikat för accesspunkter.

2.6 Aktörer och roller

Typ av Aktör	**Beskrivning**
Accesspunkt (även publikt öppen)	Kan slå upp deltagares certifikat.
Roll	**Beskrivning**
Federationsoperatör	Hanterar deltagares certifikat inom en federation.

För att en användare ska kunna tilldelas rollen Federationsoperatör 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

Denna komponent kan användas enligt följande användningsfall:

2.7.1 AF: Upplägg av certifikat

Användningsfall	
Beskrivning	Ett certifikat för deltagare läggs in i CertPub
Roller	AF utförs av Federationsadministratör
Antaganden	Deltagaren finns i federationen.
Flöde	Federationsadministratör har fått ett certifikat av deltagaren på ett säkert sätt. Administratören lägger in certifikatet via GUI.
Resultat	Certifikatet finns registrerat för deltagaren och kan slås upp i CertPub.

Verksamhets-regler	Federationsadministratör behöver verifiera att certifikatet verkligen tillhör deltagaren.
Exempel	-

2.7.2 AF: Uppslag av certifikat

Användningsfall	
Beskrivning	Ett certifikat för deltagare hämtas via uppslagning.
Roller	AF utförs av deltagare som vill veta certifikat för annan deltagare. (Notera att operationen kommer att vara publikt tillgänglig.)
Antaganden	Deltagaren som söks är inlagd.
Flöde	En deltagare ska skicka till en annan deltagare. Den sändande deltagare hämta certifikat för den mottagande och krypterar meddelandet med den mottagandes certifikat.
Resultat	Den som gör uppslaget ser den sökta deltagarens certifikat.
Verksamhets-regler	-
Exempel	-

2.8 API: Certifikathämtning

Detta API används för att hämta de certifikat som hör till en deltagare. Det kan finnas ett signeringscertifikat, ett krypteringscertifikat eller bägge.

Extension möjligheten i [SMP-OASIS] kan användas för att slå upp certifikaten.

2.9 GUI: Administration

GUI används av federationsadministratör för att lägga till och ändra certifikat.

2.10 Informationsmodell: Certifikat

CertPub kan se certifikatet som ren text utan att hantera dess interna struktur men är fri att göra så om det underlättar för användning.

2.10.1 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].

CertPub Informationssäkerhetsklassning

Del	Konfidentialitet	Riktighet	Tillgänglighet
Information om certifikat	Nivå 1 - Måttlig	Nivå 3 - Allvarlig	Nivå 3 – Allvarlig
Administrationsdel	Nivå 2 – Betydande	Nivå 3 - Allvarlig	Nivå 1 – Måttlig

2.11 Informationssäkerhet- och tillit

Komponentens uppgift är att publicera, administrerar samt lagra och distribuera certifikat för 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 certifikat publiceras och distribueras signerat i realtid för att deltagare ska kunna verifiera varandra. Åtkomsten skyddas med funktionscertifikat.
- Administrationsdel där certifikaten 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.

2.12 Stödmaterial

Inget specifikt stödmaterial finns för denna komponent.

3 För IT-arkitekter

Information som är riktad till IT-arkitekter

3.1 Inledning

De certifikat som publiceras förutsätts följa standard enligt [X509].

3.2 Tekniska villkor och förutsättningar för användning

Komponenten behöver köras med brandväggar för inkommande och utgående trafik. Utåt behöver inga öppningar göras.

Inåt ska API för hämtning av certifikat 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

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

3.4 Översiktliga tekniska användningsfall

Se även avsnitt **Fel! Hittar inte referenskälla.**.

3.4.1 Tekniskt AF: Backup

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

3.4.2 Tekniskt AF: Återställning

Om något har hänt med CertPub 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 CertPub 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 Tekniskt GUI

Inga specifika tekniska GUI finns.

3.6 Datamodell: Certifikat

Certifikaten kan behandlas som en sträng av text. För detaljer om deras struktur se [X509].

3.6.1 IT-säkerhet

De certifikat som lagras får inte förändras av CertPub. CertPub ska endast tillåta användare med säker autentisering att uppdatera certifikat.

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

3.7 Open API Specifikation

Ingen Open API specifikation behöver ges av komponenten.

3.8 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 tjänster som implementerar denna komponent	
Administrationsdel	**Krav**
GUI	Tillgänglig under kontorstid för typiska användare. Servicefönster kan förekomma

Publiceringsdel	Krav
API	Tillgänglig 24/7. Upp till 99.99 procent åtkomst. Exakta värden beror på federation.

5 Bilagor

Restbindning: Certpub - Komponentspecifikation-v1.0-Bilaga - REST-bindning