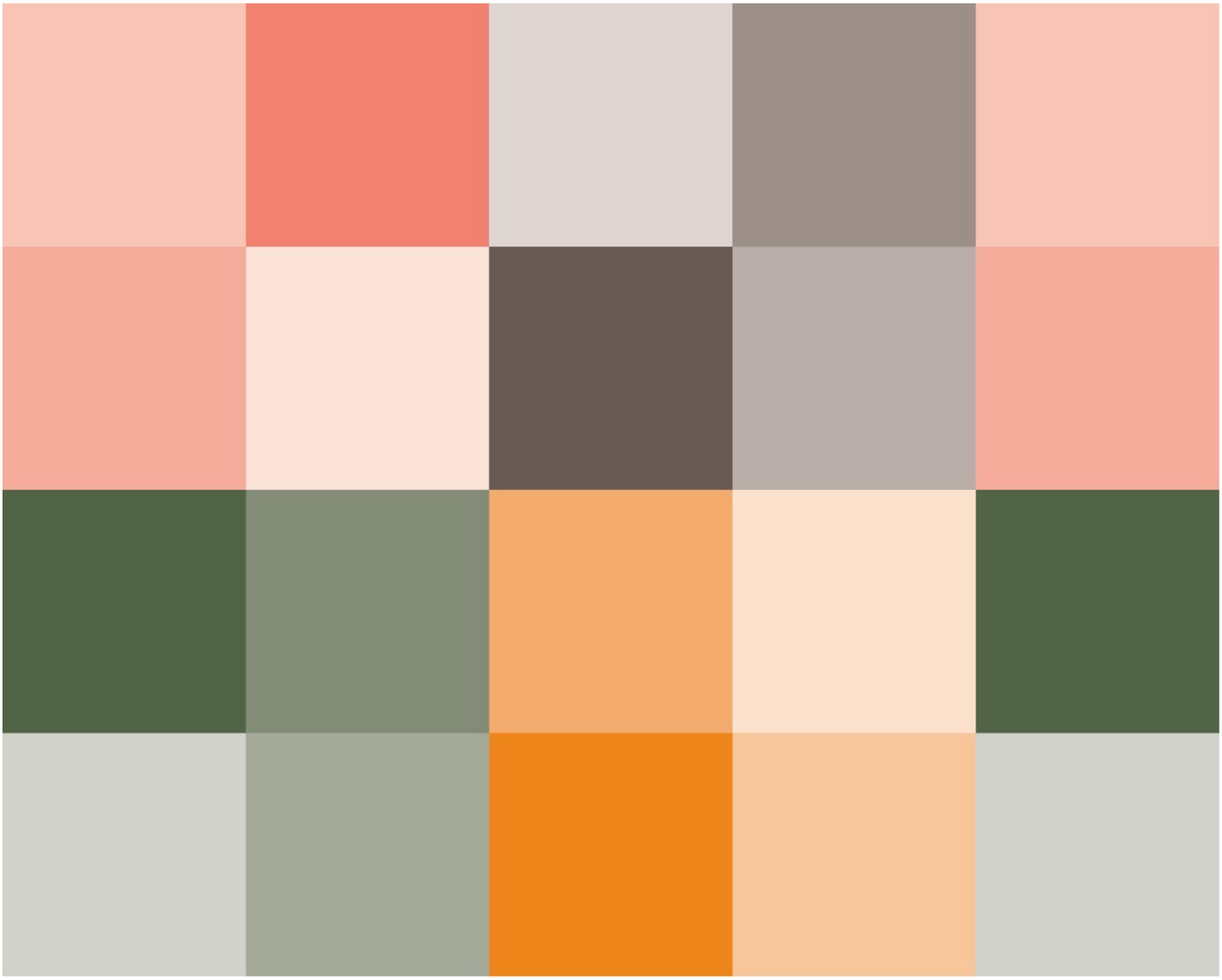

PKI för Accesspunkter

Komponentspecifikation

Version: 1.0 Målgrupper: Verksamhetsutvecklare, IT-Arkitekter

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Benämning: PKI för Accesspunkter

Version: 1.0

Livscykelstatus: Fastställd

Ägare: DIGG

Nyckelord: PKI; eDelivery; Accesspunktcertifikat

Komponenten hanterar utfärdande av certifikat. Dessa certifikat används uteslutande av accesspunkter för att dessa skall kunna identifiera varandra som legitima accesspunkter och för att kunna kryptera och signera meddelanden mellan accesspunkterna. Certifikatsutgivningen är specifik för den miljö där certifikatet ska användas i samt för den federation som accesspunktsoperatören är godkänd för.

De centrala funktionerna för utfärdande och administration av certifikat utgörs av en certifikatfabrik som tillverkar och signerar certifikaten samt en spärrtjänst där certifikat som inte längre skall vara giltiga kan spärras, detta kan också kontrolleras av accesspunkterna.

Som en del av plattformen ger PKI för Accesspunkter följande nyttor:

- Den möjliggör tillits- och certifikatshantering mellan accesspunkter
- Kontrollerad, säker och standardiserad hantering av samtliga accesspunktcertifikat inom en federation
- Dedikerad certifikatkedja per federationsmiljö

Innehållsförteckning

Sammanfattning **1**

1 Inledning **4**

1.1 Beroenden till specifikationer och komponenter *4*

1.2 Målgrupper *4*

1.3 Externa Referenser *5*

2 För Verksamhetsutvecklare **5**

2.1 Inledning *6*

2.2 Egenskaper hos komponent *6*

2.3 Nyttor med användning *6*

2.4 Hur komponenten fungerar *6*

2.5 Villkor och förutsättningar för användning *6*

2.6 Aktörer och roller *6*

2.7 Översiktliga användningsfall *6*

2.7.1 AF: Utfärda Certifikat 6

2.7.2 AF: Revokera certifikat 7

2.7.3 AF: Kontrollera certifikat 8

2.8 API: OCSP *9*

2.9 API: CRL *9*

2.10 GUI: Administration *9*

2.11 Informationsmodell: Certifikat *9*

2.11.1 Informationssäkerhetsklassning 9

2.12 Informationssäkerhet- och tillit *10*

2.13 Stödmaterial *10*

3 För IT-arkitekter **10**

3.1 Inledning *10*

3.2 Tekniska villkor och förutsättningar för användning *11*

3.3 Tekniska aktörer och roller *11*

3.4 Översiktliga användningsfall *11*

3.4.1 Tekniskt AF: Backup 11

3.4.2 Tekniskt AF: Återställning 11

3.4.3 Tekniskt AF: Uppgradering 11

3.5 API 11
3.6 Tekniskt GUI 11
3.7 Datamodell: Certifikat 11
3.8 Open API Specifikation 12

4 Generella servicenivåer 12

5 Appendix 12

1 Inledning

Inledande beskrivning av komponenten PKI för accesspunkter

Syftet med PKI för Accesspunkter (PKIAP) är att skapa och möjliggöra kontroll av certifikat som används av SMP och av Accesspunkter. Certifikat utgivna av den är endast tänkta att användas för dessa ändamål, inte för generell certifikatshantering.

Komponenten ger ett administrationsgränssnitt där en användare kan skapa eller revokera certifikat efter att accesspunkterna skickat in så begäran om detta. Den ger också ett API för att kontrollera certifikats giltighet enligt [OCSP] samt kan leverera en certificate revocation list [PKI].

- API och GUI
  - API: OCSP
  - API: CRL
  - GUI: Administration
- Information
  - Certifikat

API'erna är publicerade mot internet medan GUI ej behöver vara tillgänglig utåt.

Det finns en option att ha ett internt API som kan användas av SMP när en AP skapas där men den beskrivs inte ytterligare i denna version av komponentbeskrivningen.

1.1 Beroenden till specifikationer och komponenter

PKIAP använder och är följsam mot följande specifikationer:

- X.509 PKI och CRL, [PKI]
- X.509 OCSP [OCSP]

Denna komponent har inga beroenden mot andra komponenter.

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

Referens till	Länk	Kommentar
PKI	https://datatracker.ietf.org/doc/html/rfc5280	Specifikation för PKI och CRL.
OCSP	https://datatracker.ietf.org/doc/html/rfc6960	Specifiation för OCSP

2 För Verksamhetsutvecklare

Information som är riktad till verksamhetsutvecklare

2.1 Inledning

PKI för accesspunkter gör att en eDelivery federation har kontroll över vilka **certifikat** som används och säkerställer att accesspunkterna inom en federation endast kommunicerar med varandra.

2.2 Egenskaper hos komponent

PKI för accesspunkter håller de certifikat som har utfärdats och information om de som har revokerats. En klient kan kontrollera om ett certifikat har getts ut av komponenten och om det fortfarande är giltigt.

2.3 Nyttor med användning

PKI för accesspunkter undviker beroende mot externa certifikatsleverantörer och gör att endast godkända AP-operatörer får certifikat.

2.4 Hur komponenten fungerar

Komponenten håller internt de utgivna certifikaten. En administratör kan granska dessa och vid behov revokera dem.

2.5 Villkor och förutsättningar för användning

En implementation av komponenten behöver godkännas av DIGG för att få användas inom en federation som DIGG hanaterar.

2.6 Aktörer och roller

Roll	**Beskrivning**
Accesspunktsoperatör	Kontrollerar certifikat från andra accesspunkter samt SMP's signering av metadata.
Systemadministratör	Utfärdar certifikat för accesspunkter

2.7 Översiktliga användningsfall

Denna komponent kan användas enligt följande användningsfall:

2.7.1 AF: Utfärda Certifikat

En ny accesspunkt har tillkommit och behöver registreras ett certifikat

Användningsfall	
Beskrivning	En accesspunkt (AP) får ett certifikat.
Roller	AF utförs av Federationsadministratör
Antaganden	Accesspunkten finns i federationen.
Flöde	Accesspunkten skickar en begäran om certifikat. Federationsadministratören skapar certifikatet och tillser att det även registreras i SMP. Federationsadministratören levererar certifikatet till accesspunktsoperatören.
Resultat	Certifikatet finns inlagt i komponenten och kan användas av AP.
Verksamhets-regler	Federationsadministratören måste kontrollera att certifikatsbegäran kommer från rätt organisation.
Exempel	-

2.7.2 AF: Revokera certifikat

Användningsfall	
Beskrivning	Ett certifikat ska ej längre användas och revokeras därför.
Roller	AF utförs av Federationsadministratör
Antaganden	

Flöde	Federationsadministratören hittar det existerande certifikatet och begär att det ska revokeras.
Resultat	Det kommer då att publiceras i nästa CRL samt försök att kontrollera det ger att det är revokerat.
Verksamhets-regler	Det behöver utredas varför certifikatet ej längre är giltigt.
Exempel	-

2.7.3 AF: Kontrollera certifikat

Användningsfall	
Beskrivning	En accesspunkt (AP) får ett certifikat presenterat av annan AP den vill kommunicera med.
Roller	AF utförs maskinellt av AP
Antaganden	
Flöde	Accesspunkten skickar en OCSP begäran till PKIAP för accesspuntker. .
Resultat	Svaret anger om certifikatet är utfärdat av PKIAP för accesspunkter eller ej samt om det är giltigt eller ej..

Verksamhets-regler	-
Exempel	-

2.8 API: OCSP

Se [OCSP]. Användande av OCSP gör att klienten alltid får en aktuell bild av certifikatets giltighet. Nackdelen är att komponenten måste vara tillgänglig.

2.9 API: CRL

Se [PKI]. Användande av CRL har nackdelen att CRL-filer kan bli stora efter hand. (Detta lär dock inte hända för denna komponent eftersom antalet accesspunkter är relativt litet.) CRL-filer kan laddas ner och användas under en tidsperiod. Det har nackdelen att en revokering som händer under den tidsperioden inte upptäcks, men har fördelen att komponenten inte behöver vara tillgänglig för kontroll.

2.10 GUI: Administration

I detta GUI kan en administratör skapa, lista och revokera certifikat.

2.11 Informationsmodell: Certifikat

För certifikat, se [PKI].

De utgivna certifikaten lagras lokalt.

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]. Informationens skyddsvärde bestäms genom att relatera till konsekvenser som otillåten spridning av information och meddelanden inom plattformen riskerar att leda till.

Konsekvensnivåer är värderad i en av fyra skyddsklasser i informationssäkerhetsklassningsmodellen nedan.

Informationssäkerhetsklassning

Del	Konfidentialitet	Riktighet	Tillgänglighet
Certifikat	Publik	Nivå 3 – Allvarlig	Nivå 2 – Betydande
Interna nycklar	Nivå 3 - Allvarlig	Nivå 3 - Allvarlig	Nivå 2 – Betydande

2.12 Informationssäkerhet- och tillit

Komponentens uppgift är att publicera, administrerar samt lagra och distribuera certifikat för accesspunkter 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

- Kontrolldel där klienter kan kontrollera om certifikat har revokerats eller inte. Denna del är öppen för alla.
- Administrationsdel där certifikat hanteras (läggs till, tas bort eller uppdateras) är skyddad av stark autentisering(identifiering) och auktorisering(behörighet) för registrerade klienter (admistratörer eller SMP).

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

2.13 Stödmaterial

Inget specifikt stödmaterial finns för denna komponent.

3 För IT-arkitekter

Information som är riktad till IT-arkitekter

3.1 Inledning

En PKIAP måste uppfylla de villkor som ges i [PKI] och [OCSP]

3.2 Tekniska villkor och förutsättningar för användning

Komponenten behöver skydda administratörsgränssnittet, till exempel genom att det endast är tillgängligt för intern användning. PKIAP behöver ej själv nå ut men inåt måste URL för att hämta CRL och kontrollera OCSP vara öppen.

3.3 Tekniska aktörer och roller

Se även avsnitt 2.6

Typ av Aktör	Beskrivning
Driftansvarig	Utför de tekniska användningsfallen
Förvaltningsansvarig	Beslutar när uppgradering ska göras

3.4 Översiktliga användningsfall

Se även avsnitt 2.7

3.4.1 Tekniskt AF: Backup

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

3.4.2 Tekniskt AF: Återställning

Om något har hänt med PKIAP 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 PKIAP 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 kontroll av certifikat.

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: Certifikat

Hur data lagras internt lämnas fritt till implementationen, betrakta dock informationsmodellen och säkerhetskraven.

3.8 Open API Specifikation

Ingen Open API specifikation finns för denna komponent.

4 Generella servicenivåer

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

Servicenivåer för programvaror som implementerar denna komponent	
Administrationsgränssnitt	**Krav**
GUI	Tillgänglig under kontorstid, alt. Tillgänglig när certifikat behöver skapas eller revokeras
Uppslag	**Krav**
CRL	Tillgänglig dygnet runt. Kraven på nedtid kan sättas lägre än krav för nedtid på OCSP.
OCSP	Tillgänglig dygnet runt. Låg nedtid.

5 Appendix

Inga appendix.