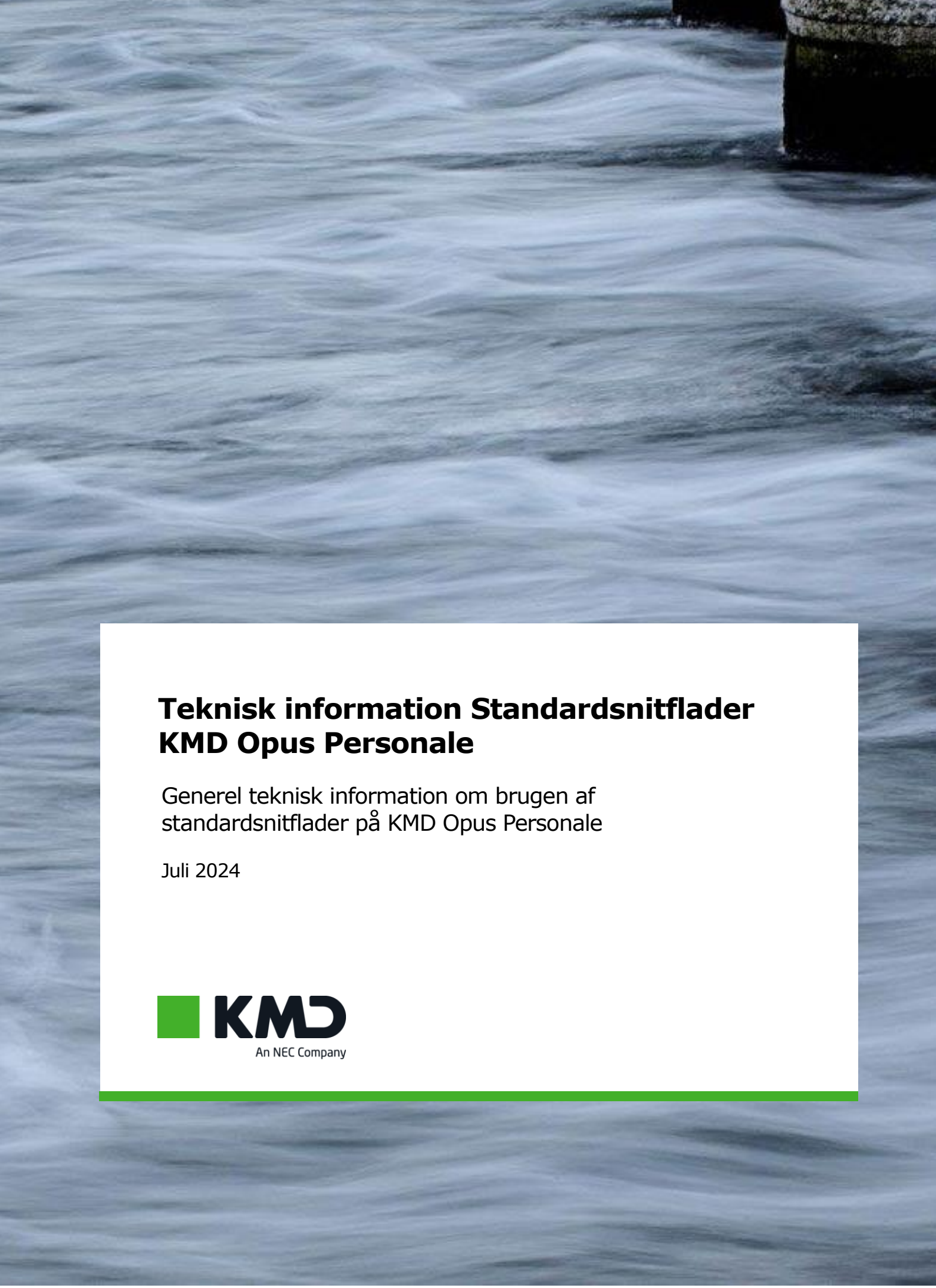

Teknisk information Standardsnitflader KMD Opus Personale

Generel teknisk information om brugen af standardsnitflader på KMD Opus Personale

Juli 2024

KMD
An NEC Company

Indhold

Certifikater

GENERELT OM CERTIFIKATER
Når et eksternt system skal integreres med KMD Opus Personale via standardsnitflader, kræves der en sikkerhedsmodel baseret på certifikater til system-til-system kommunikation.

Standarden for disse certifikater er OCES3, som tilbydes gennem MitID Erhverv og typisk anvendes i form af systemcertifikater. Disse certifikater er specielt designet til identifikation og beskyttelse af IT-systemer.

I tilfælde af standardintegration har KMD og den pågældende systemleverandør allerede koordineret alle aspekter vedrørende brugen af certifikater.

Ved individuel integration er disse forberedelser ikke til stede, hvilket betyder kunden har en opgave med at fremskaffe og overdrage certifikatet til KMD. Dette er beskrevet i de følgende afsnit.

INDIVIDUEL INTEGRATION
Kunden eller leverandøren skal forberede og fremsende den offentlige del af et OCES3 certifikat med fuld kæde til KMD, som derefter varetager opsætning.

Dette svarer grundlæggende til, at kunden/leverandøren giver KMD en nøgle, hvorefter KMD sørger for at denne virker til låsen.

Erfaringer viser, at de fleste IT-afdelinger og leverandører er velbevandrede med processen for bestilling og håndtering af OCES3-certifikater.

Hvis det er kunden som stiller med certifikatet, så er det vores anbefaling man anvender et nyt certifikat, som ikke anvendes til andre formål.

Hvis det er leverandøren som stiller med certifikatet, så kan denne godt anvende det samme certifikat til det samme system på tværs af kunder, så længe det er samme system og samme formål det anvendes til.

KLARGØRING AF CERTIFIKAT
Ved levering af den offentlige del af certifikatet til KMD, er det vigtigt at inkludere den fulde certifikatkæde. Dette omfatter eksport af både brugerens eget certifikat og de tilhørende CA-certifikater (Certificate Authority).

En fuldstændig certifikatkæde er nødvendig for, at KMD kan bekræfte certifikatets gyldighed i sin helhed.

Efter eksporten bør kunden eller leverandøren verificere, at certifikatkæden er korrekt og komplet. Dette sikrer, at alle nødvendige komponenter er til stede og korrekt arrangeret fra brugerens certifikat til rodcertifikatet (se eksempler på næste side)

Korrekt verifikation er kritisk for at forhindre sikkerhedsproblemer eller afvisning ved brug af certifikatet.

Den offentlige del af certifikatet og certifikatkæden skal gemmes i et standardformat, fortrinsvis PEM.

OVERDRAG CERTIFIKAT TIL KMD
Den offentlige del af certifikatet pakkes i en .zip-fil og sendes til kundens kontaktperson hos KMD.

Pakningen i en .zip fil er nødvendigt for at undgå, at certifikatet blokeres af KMD's IT-sikkerhedssystemer.

HUSK FORNYELSE
Det er essentielt, at kunden sørger for, at KMD modtager opdaterede certifikater, før de nuværende udløber, for at undgå pludselige afbrydelser i systemfunktionaliteten.

Kontrol af certifikat inden fremsendelse til KMD

Et offentligt OCES3-certifikat med fuld kæde består af flere certifikater, der sammen skaber en verificerbar sti fra et servercertifikat til et rodcertifikat.

Det er vigtigt at denne certifikatkæde er på plads og verificeret, inden certifikatet sendes til KMD.

Certifikatkæden inkluderer:

1. **Servercertifikat (OCES3-certifikat)**: Det certifikat, der er udstedt til den specifikke server af CA'en.
2. **Mellemcertifikater** (Intermediate Certificates): Certifikater, der forbinder servercertifikatet til rodcertifikatet. Disse udstedes også af CA'en.
3. **Rodcertifikat** (Root Certificate): Det øverste certifikat i kæden, som er selvsigneret af CA'en.

Du skal sikre at disse certifikater er kombineret eks. i en fil der hedder fullchain.pem eller tilsvarende.

Når du sender certifikaterne, skal du kun inkludere de offentlige certifikater. Du skal **ikke** inkludere private nøgler.

Manuel kontrol af certifikatet

1. **Åbn certifikatet (eks. fullchain .pem) i en teksteditor og inspicer dette**:
   - Servercertifikatet, mellemcertifikaterne og rodcertifikatet skal være til stede og arrangeret i denne rækkefølge:

```
-----BEGIN CERTIFICATE-----
(Server Certificate)
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
(Intermediate Certificate 1)
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
(Intermediate Certificate 2,
hvis relevant)
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
(Root Certificate)
-----END CERTIFICATE-----
```

Kontrol med OpenSSL:

1. **Verificér certifikatkæden ved brug af OpenSSL**:
   - Brug følgende OpenSSL-kommando til at verificere kæden:

```
openssl verify -CAfile
fullchain.pem
```

Sikkerhed

GENERELT OM SIKKERHED
Som første led af sikkerhedsopsætningen på en standardsnitflade modtager KMD den offentlige del af et OCES3 certifikat fra en kunde/eksterne leverandør. Dette certifikat bliver konfigureret i KMD's API gateway på KMD Opus Personale.

Ved forbindelse til API gatewayen fra et eksterne system, ved brug af certifikatet, sker der validering af certifikatet hos KMD.

Herefter kontrolleres det, hvilke standardsnitflader og konkrete miljøer, som det pågældende certifikat har adgang til, således at det pågældende system ikke kan anvende standardsnitflader/end-points, som det ikke skal have adgang til.

Alt kommunikation mellem eksterne systemer og KMD Opus Personale forbliver krypteret via SSL/TLS, sikrer at data, der udveksles, er beskyttet mod aflytning eller manipulation.

Når først det konkrete eksterne system har adgang til det konkrete end-point, så er den videre sikkerhedshåndtering delegeret til det system som har logikken og regelsæt for den konkrete anvendelse af servicen (sikkerhedskoncept: delegated security).

Det er et generelt princip både for integrationspakker, såvel som individuelle standardsnitflader.

HVAD ER DELEGATED SECURITY?
Det er processen, hvor sikkerhedsbeslutninger delegeres til en eller flere betroet tredjepart. I denne kontekst er der tale om delegering af dele af sikkerheden til de eksterne systemer, som integrerer ind til KMD Opus Personale.

Det betyder at når man som kunde har bedt KMD om at give et andet system adgang til en eller flere standardsnitflader på kundens instans af Opus Personale, så tildeles dette system adgang til at kunne anvende disse.

KMD Opus Personale har tillid til, at dette system har ret til at udføre de handlinger, som det udfører, samt at det integrerende system har implementeret nødvendige og relevante tiltag (dataafgrænsninger, logning af brugerhandlinger m.v.) ud fra hvad der er relevant for de use-cases, man som kunde har bedt dette system understøtte.

Når et integrerende system eksempelvis udsøger data på en specifik medarbejder, så logger KMD Opus Personale at denne handling er udført af dette system. Det påhviler så det integrerende system at logge hvilken konkret bruger der har gjort det. Skal der foretages afgrænsning til specifikke medarbejdere, så skal det også håndteres af det integrerende system.

HVORFOR DENNE MODEL?
Modellen anvendes da standardsnitfladerne skal understøtte mange forskellige systemer, use-cases og kombinatorikker for afgrænsning/filtrering – og det således er mest hensigtsmæssigt at det integrerende system, som har logikken og forståelsen for den forretningsmæssige afgræsning, også håndhæver denne.

Det er en kendt model med kendte principper, som anvendes på mange centrale systemer og registre som CPR-registret. Når en dataansvarlig beder leverandøren af et integrerende system om integrere mod CPR registret, så har dette system adgang til meget data. Det forudsættes så, at leverandøren sikrer relevant sikkerhed på det enkelte system (Eks. at dette dataafgrænser og logger brugeradfærd). CPR registret har ikke store komplekse regelsæt og opsætninger for, hvilke data det enkelte system kan tilgå.

KMD Opus Personale håndhæver eksempelvis sikkerhedsadgang og logning for det konkrete system der integrerer, mens det konkrete system håndhæver sikkerhedsadgang og logning for de konkrete brugerne og deres anvendelse via dette system.

Uden denne model skulle KMD Opus Personale skal megen viden om alle processer, sikkerhedsafgrænsninger og use-cases, der er i eksterne systemer. Denne viden vil altid i bedste fald være hullet, hvilket ville føre til en unødig og uoverskuelig kompleksitet i administration i KMD Opus Personale – hvilket ikke er ønskværdigt, da dette i sig selv kan udgøre en sikkerhedstrussel.

Modellens svaghed er, at det forudsættes at det eksterne system har implementeret nødvendige organisatoriske og tekniske foranstaltninger i forhold til den sikkerhed man som kunde finder nødvendig for det pågældende system.

IMPLEMENTERING AF YDERLIGERE SIKKERHED

Hvis man som kunde ikke har den nødvendige tillid til de eksterne systemer, som skal integrere ind til KMD Opus Personale, så er det vores grundlæggende anbefaling at man ikke integrerer disse.

Hvis man alligevel ønsker at gøre dette, men ønsker skærpede foranstaltninger mellem systemerne – så er dette ikke muligt på standardsnitfladerne på KMD Opus Personale.

En mulig løsning er, at man implementerer sine egne tekniske faciliteter (proxy/integrationsplatform) mellem standardsnitfladerne på KMD Opus Personale og det eksterne system. Dette er der principielt set ikke noget problem ved, men man skal være opmærksom på, at man påtager sig en stor opgave, som ikke er supporteret fra KMDs side.