DIGITALISERINGSSTYRELSEN

Notat

februar 2023
Den Danske Stat
TSP/pld/sibeh
Version 1.0

Private nøgler og egenkontrol for OCES og kvalificerede certifikater fra Den Danske Stat CA

Indledning

Dette dokument beskriver kravet om egenkontrol (sole control) i forhold anvendelse af private nøgler tilknyttet et certifikat udstedt af et CA fra Den Danske Stat tillidstjenesteudbyder. Dokumentet behandler udelukkende certifikater udstedt til fysiske person og der er primært fokus på erhvervsbrugere registreret i MitID Erhverv.

Krav fra certifikatpolitikker og vilkår

Både certifikatpolitikker for OCES-certifikater og kvalificerede certifikater har et krav om beskyttelse af den private nøgle knyttet til udstedte certifikater.

Politikker
[KRAV 6.2.8-01] *CA skal sikre, at certifikatholders private nøgle ikke kan anvendes, uden at certifikatholderen i hvert tilfælde har autoriseret anvendelsen, således at certifikatholderen opretholder egenkontrol over sin private nøgle.*

Dette kan ske

- *Gennem aftale der forpligter certifikatindehaver og certifikatholder, hvis den private nøgle genereres og anvendes alene under certifikatholders kontrol.*
- *Ved hjælp af en kombination af tekniske kontroller og aftaler, der forpligter certifikatindehaver, certifikatholder og andre relevante parter, hvis den private nøgle genereres og anvendes helt eller delvis via en tillidstjeneste.*

[KRAV 6.4.1-02] *CA skal gennem aftale og/eller tekniske kontroller sikre, at certifikatholders private nøgle er effektivt beskyttet mod uautoriseret anvendelse med brug af aktiveringsdata.*

Vilkår
Digitaliseringsstyrelsen adresserer ovenstående ved at have indskrevet krav om egenkontrol i vilkår:

Vilkår for organisationen:

6.3 Beskyttelse af privat nøgle ved generering

Certifikatindehaver er forpligtet til at etablere det fornødne teknisk grundlag og administrative kontroller til at sikre, at den private nøgle genereres sikkert og under kontrol af Certifikatholder.

[..]

Som en del af det tekniske grundlag og de administrative kontroller skal Certifikatindehaver sikre, at Certifikatholder til stadighed kan have egenkontrol over egen nøgle.

Vilkår for medarbejderen:

19 Anvendelse af OCES brugercertifikater

[..]

Certifikatholder er forpligtet til at beskytte den private nøgle, så kompromittering, ændring, tab og uautoriseret brug forhindres. Der skal således tages rimelige forhold ved beskyttelse af sikkerhedsmekanismer, herunder valg og beskyttelse af kodeord. Certifikatholder skal altid hemmeligholde kodeord, så andre ikke får kendskab hertil.

Certifikatholder skal i forbindelse med udstedelse og efterfølgende anvendelse af den private nøgle sikre at dette sker på en sådan måde, at egenkontrollen med nøglen bibeholdes.

Bemærk at der for kvalificerede certifikater yderligere er krav om at den private nøgle er beskyttet af et kvalificeret elektronisk signaturgenereringssystem (QSCD).

Egenkontrol

Egenkontrol er et centralt element for elektroniske signaturer og det indgår implicit i eIDAS definition af en avanceret elektronisk signatur:

Artikel 26 [..]

En avanceret elektronisk signatur skal opfylde følgende krav:

[..]

c) den genereres ved hjælp af elektroniske signaturgenereringsdata, som underskriveren med en høj grad af tillid kan anvende og har fuld kontrol med [..]

Generelt vil egenkontrol betyde, at brugeren til stadighed har kontrol over, hvornår og hvad der signeres. Hvis den private nøgle (kaldt *signaturgenereringsdata* i eIDAS) overdrages til en person eller en proces, hvor det ikke kan sikres, at brugeren autoriserer enhver anvendelse i form af en aktiv handling, opretholder brugeren ikke længere egenkontrol. Bemærk, at hvis brugeren har konfigureret anvendelsen af den private nøgle, så der skal angives aktiveringsdata hver gang, der skal

foretages en operation med den private nøgle og aktiveringsdata udelukkende er i brugerens besiddelse, vil der som udgangspunkt være tale om egenkontrol.

Men der kan også være situationer, hvor bruger "låser op" for den private nøgle med aktiveringsdata én gang per begrænset session[1] og herefter anvender nøgle flere gange uden brug af aktiveringsdata. Dette er typisk tilfælde i løsninger baseret på såkaldte smartcards. Hvis brugeren her er i kontrol med hvornår der foretages operationer med den private nøgle gennem aktive handlinger, kan egenkontrollen godt være opretholdt.

Der kan være konfigurationer og arbejdsmåder i brugerens miljø, der vil forhindre at brugeren kan opretholde egenkontrol. Dette kunne fx være situationer, hvor supportere har mulighed for at overtage brugerens arbejdscomputer, men bemærk, at det er ikke alene begrænset til dette eksempel.

Gode spørgsmål til afklaring af om egenkontrol er:

- Er det udelukkende brugeren, der kan anvende den private nøgle?
- Kan der foretages operationer med den private nøgle uden at brugeren foretager en aktiv handling i hvert tilfælde?
- Kan brugeren notere, hvornår den private nøgle har været anvendt?

Hvis der ikke kan svares "Ja" til disse spørgsmål, er det tvivlsomt om egenkontrol er opretholdt.

[1] Varigheden af en session skal overvejes i sammenhæng hvordan nøglen opbevares.