

Notat

september 2015

Dispensation vedr. krav til adgangskode i OCES-Certifikatpolitikkerne

Digitaliseringsstyrelsen har i forbindelse med arbejdet om ændrede adgangskodekrav for NemID med nøglekort modtaget en anmodning fra Nets DanID A/S om dispensation i forhold til kravet i OCES-Certifikatpolitik for Personcertifikater vers. 4 punkt 7.2.8 samt OCES-Certifikatpolitik for Medarbejdertcertifikater vers. 5 punkt 7.2.8:

”Såfremt certifikatindehaverens nøglepar efter generering opbevares centralt hos CA skal følgende opfyldes:

Adgangskoden skal vælges fra et udfaldsrum på mindst 36^6 mulige koder, for eksempel som 6 tegn valgt ud af 36 bogstaver, tal og specialtegn.”

Digitaliseringsstyrelsen har derfor indhentet oplysninger til brug for vurdering af anmodningen.

Digitaliseringsstyrelsen har modtaget

1. Nets DanIDs' risikoanalyse vedr. ændringer til adgangskodekrav.
2. Vurdering af risikoanalyse og samlet sikkerhed fra PWC
3. Opfølgende dialog med PWC

Analyserne konkluderer, at NemID fortsat vil være på et højt sikkerhedsniveau selvom, brugere fremover vælger at anvende en fire cifret kode, idet der dels fortsat er spærret for udtommende sogning – nu allerede ved tre forkerte forsøg, dels er implementeret mitigerende sikkerhedstiltag fx i form af krav til adgangskoden, så der ikke kan vælges fire ens cifre, en fortløbende talrække eller en talrække fra CPR-nummeret, der sikrer, at løsningen stadig opnår et højt sikkerhedsniveau.

Digitaliseringsstyrelsen har på den baggrund valgt at dispensere fra det nævnte krav i certifikatpolitikkens punkt 7.2.8.