OTP-politik

Januar 2012

Version 2.0

Indholdsfortegnelse

1. Indledning

1.1. Baggrund og formål

I den fælles sikkerhedsløsning (OCES II) udgør OTP-enheden en central autentifikationsmekanisme, som danske banker og offentlige institutioner er blevet enige om at bruge. For at opnå en fælles standard og et harmoniseret sikkerhedsniveau er det vigtigt, at der findes en fælles politik, som regulerer OTP-enheders livscyklus.

OTP-enheden styrker brugerautentificeringen i infrastrukturen. Brugeren får en fysisk enhed, som er uafhængig af brugerens pc, og som sammen med en statisk adgangskode udgør en 2-faktor autentificeringsmekanisme.

Formålet med dette dokument er at beskrive politikken for fremstilling, opbevaring, distribution og brug af OTP-enheder. Alle parter, som er involveret i en eller flere aktiviteter i forbindelse med fremstilling og distribution af OTP-enheder, skal overholde de krav, som er beskrevet i dette dokument.

De krav, som er beskrevet i dette dokument, SKAL revideres af en ekstern uafhængig it-revisor for at sikre, at de bliver implementeret korrekt i organisationen, og at den ansvarlige organisation overholder de anførte krav og vilkår.

OTP-politikken ejes og vedligeholdes af Nets DanID, der fungerer som udsteder af OTP-enheder.

Nets DanID Koordinationsudvalget skal til enhver tid høres, hvis der skal udføres væsentlige ændringer i OTP-politikken. Nets DanID Koordinationsudvalget består af repræsentanter fra Digitaliseringsstyrelsen (DIGST), den finansielle sektor og Nets DanID. DIGST, bankerne og Nets DanID kan foreslå ændringer til politikken. Nets DanID er ansvarlig for at samle alle ændringer samt at forberede et nyt udkast af OTP-politikken, som derefter SKAL sendes til godkendelse hos Nets DanID Koordinationsudvalget. OTP-politikken SKAL gennemgås, når der foretages væsentlige ændringer i relation til sikkerhedsinfrastrukturen, som kan have konsekvenser for OTP-politikken.

1.2. Kildehenvisninger

1) Certifikatpolitik for OCES-personcertifikater (Offentlige Certifikater til Elektronisk Service), version 4. (https://www.signatursekretariatet.dk/certifikatpolitikker.html).
2) Certifikatpolitik for OCES-medarbejdercertifikater (Offentlige Certifikater til Elektronisk Service), version 5. (https://www.signatursekretariatet.dk/certifikatpolitikker.html).
3) Nets DanID Certification Practice Statement. (https://www.certifikat.dk/export/sites/dk.certifikat.oc/da/download/repository.html).
4) RFC 2119 ”RFC key words”.
5) FIPS 140-2 level 3, Security Requirements for cryptographic Modules.
6) CWA 14167-2 Cryptographic Module for CSP Signing Operations – Protection Profile.
7) NemID Regler(https://www.nemid.nu/).
8) Finanstilsynets Vejledning om Lov om forebyggende foranstaltninger om hvidvask af udbytte og finansiering af terrorisme http://www.finansraadet.dk/tal--fakta/lovgivning-og-regulering/hvidvask.aspx.

1.3. Forkortelser

CPS:	Certification Practice Statement.
HSM:	Hardware Sikkerhedsmodul.
MOCES CP:	Certifikatpolitik for OCES-medarbejdercertifikater.
DIGST:	Digitaliseringsstyrelsen.

NIST:	National Institute of Standardization and Technology.
OCES:	Offentlige (Public) Certifikater til Elektronisk Service.
OTP:	One Time Password.
POCES CP:	Certifikatpolitik for OCES-personcertifikater.
SRP:	Secure Remote Password.

1.4. Terminologi

Adgangskode:	Brugerens private adgangskode.
Bruger-id:	Identifikation, der entydigt refererer til en specifik bruger.
Midlertidig adgangskode:	Den midlertidige adgangskode benyttes til at aktivere en brugerkonto.
Nøgle:	Den engangskode, som fremstilles af OTP-enheden.
Nøglekort:	Et kort med påtrykte nøglenumre og nøgler.
Nøglenummer:	Nøglenummeret angiver hvilken nøgle, der skal anvendes på nøglekortet.
Nøgleviser:	En elektronisk OTP enhed, som kan fremstille engangskoder kaldet nøgler.
OTP-enhed:	En OTP-enhed, som kan være enten et nøglekort med nøglenumre og nøgler, et system der kan foretage telefonopkald og oplæse engangskoder eller en elektronisk enhed, der kan fremstille engangskoder.
OTP Udsteder:	Nets DanID.

I dette dokument har ordene: “SKAL”, SKAL IKKE”, ”MÅ”, MÅ IKKE”, “PÅKRÆVET”, “BØR”, ”BØR IKKE”, ”ANBEFALES”, ”KAN” og ”VALGFRIT” (skrevet i kapitæler som her) den mening, som er beskrevet i RFC2119.

2. Krav til OTP- enheder

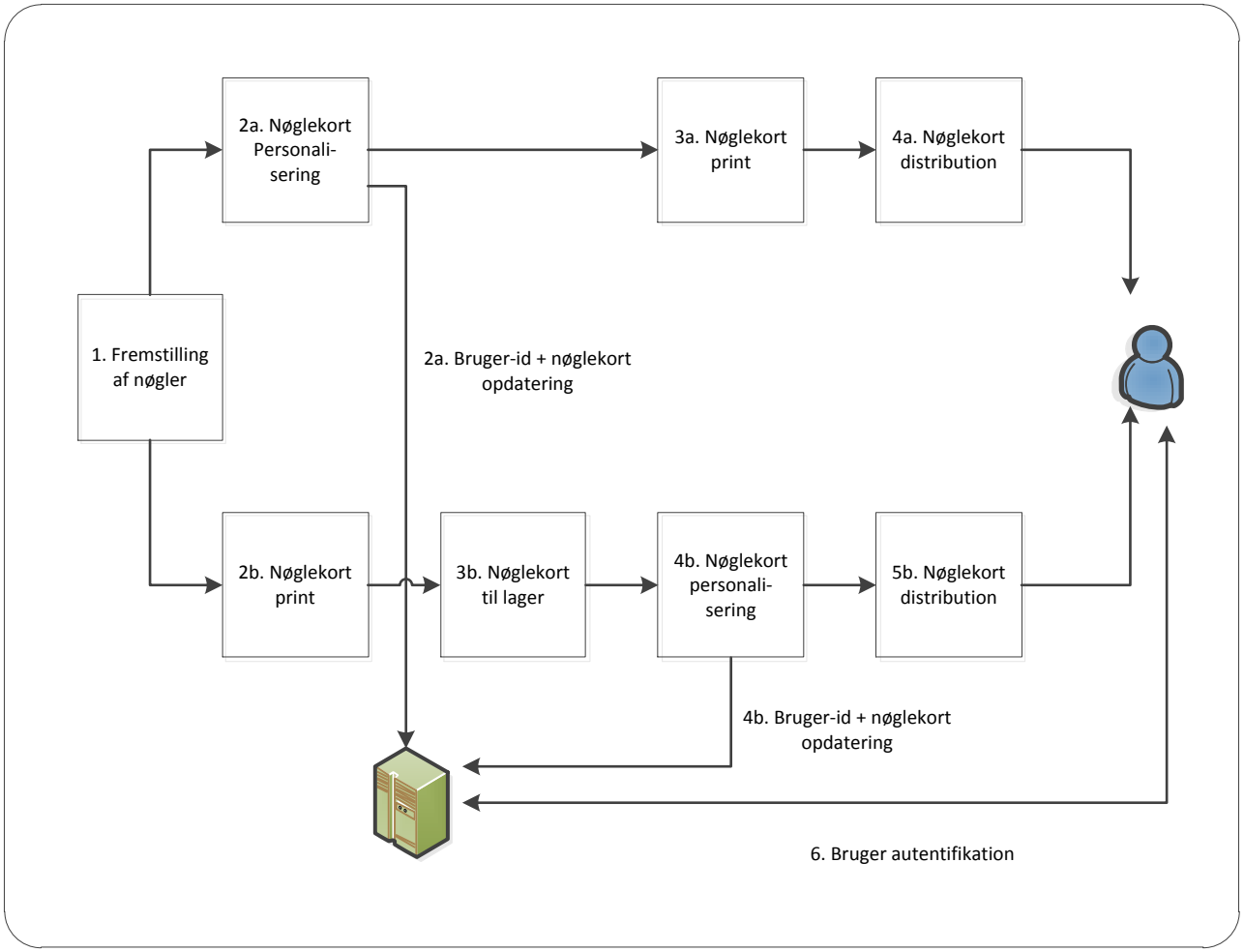
2.1. Generelle krav til OTP-enheder

De krav, som beskrives i dette kapitel, gælder alle OTP-enheder, uafhængig af enhedernes fysiske udformning.

1) Det MÅ IKKE være muligt at kunne gætte sig til den næste engangskode.
2) Længden af engangskoden skal være minimum 6 tegn.
3) For alle OTP-enheder gælder – inklusive systemer beregnet til blinde brugere – at de SKAL godkendes af OTP-udstederen.

3. Introduktion til nøglekort

Produktion og distribution af nøglekort
Nedenstående diagram viser overordnet processen for fremstilling og distribution af nøglekort til brugere. Nøglekort SKAL personaliseres inden de sendes til brugerne.



Figur 1 – Fremstilling og distribution af nøglekort

I diagrammet i figur 1 tages udgangspunkt i processen for fremstilling af nøgler (1). Nøglekort KAN leveres til brugere via to forskellige distributionskanaler a) og b):

a) **Postomdeling**. Ved postomdeling personaliseres nøglekortet til en specifik bruger, og oplysninger om brugeren og nøglekortet kædes sammen i databasen (2a). Nøglekortet fremstilles (3a) og sendes med post til brugeren (4a).
b) **Personlig udlevering**. Ved personlig udlevering fremstilles nøglekort (2b), og nøglekort sendes i pakker til RA, som sørger for, at de bliver opbevaret sikkert (3b). Personalisering og oplysninger om brugeren og nøglekortet kædes sammen i databasen (4b). Udlevering til brugeren (5b).

Brug af Nøglekort

Før nøglekortet kan benyttes, skal allerede registrerede brugere igennem en autentificeringsproces (6) for at aktivere brugerkontoen.

3.1. Krav til trykte nøglekort

I dette afsnit beskrives det trykte nøglekort som OTP-enhed. Nøglekortet indeholder nøgler. Alle nøgler har fået tilknyttet et indekseringsnummer kaldet et nøglenummer. Når brugeren skal autentificeres i en session, skal brugeren, ud over at indtaste bruger-id og personlig adgangskode, indtaste en nøgle, som er indekseret med et nøglenummer fastlagt af OTP-udstederen.

1) Der MÅ IKKE være nogen form for sammenfald af nøgler på nøglekortet.
2) Nøglenummeret SKAL bestå af minimum fire uforudsigelige tal.
3) Nøglekortet SKAL kun sendes til en adresse, som er sikkert registreret af OTP-udstederen. Ved enhver anmodning om ændring af den registrerede adresse SKAL brugeren autentificeres.
4) Hver nøgle på nøglekortet SKAL kun kunne anvendes én gang
.

3.2. Krav til nøgler der distribueres pr. telefon

Det kan være nødvendigt at distribuere nøgler via andre kanaler, fx telefon- og mobilnetværk, når der benyttes systemer, der automatisk ringer brugeren op og oplæser nøglen for brugeren.

1) Nøgler til denne type enheder MÅ kun være gyldige i korte tidsrum.
2) Den distributionskanal, som benyttes til at distribuere nøgler og midlertidige adgangskoder, SKAL være uafhængig af den kanal, som benyttes til autentificering. IP-telefoner eller andre forbindelser, som ikke er krypterede, MÅ IKKE benyttes som distributionskanal.
3) Det telefonnummer, som benyttes til distributionen af nøgler, SKAL være registreret af OTP-udstederen på en sikker måde. Autentificering af brugere er PÅKRÆVET ved enhver anmodning om ændring af telefonnummer.

3.3. Krav til fremstilling af nøglekort

Fysisk og logisk sikkerhed

1) Fremstilling af nøglekort SKAL foregå i et miljø, der er fysisk og logisk sikret imod uautoriseret indtrængen. Produktionslokaliteterne SKAL være indrettet som specifikke sikkerhedsområder i overensstemmelse med DS 484:2005 eller tilsvarende (se figur 1, proces 3a og 2b).

2) Fremstilling af nøglenumre og nøgler til nøglekort SKAL foregå ved brug af et sikkert HSM (hardware security module), som gør brug af en sikker pseudo-vilkårlig nummergenerator, der er godkendt af en international standardiseringsorganisation (ref. 1.2 (4)) som fx NIST. Opstartsværdien (seeding) SKAL være vilkårlig og fremstillingsprocessen for denne fyldestgørende dokumenteret.

3) Overførelsen af nøgler og nøglenumre SKAL være sikret imod aflytning og uautoriseret manipulation i perioden fra fremstillingen i HSM til nøglekortfremstillingen hos producent (se figur 1 proces 1 til 3a og 2b).

4) De oplysninger, der er brugt i fremstillingen af et nøglekort SKAL slettes kort tid efter fremstillingen af nøglekortet (maksimum 120 timer efter fremstillingen) (se figur 1, proces 3a og 2b).

5) Nøglekort SKAL forsegles i ugennemsigtige neutrale kuverter (se figur 1, proces 3a og 2b).

3.4. Krav til opbevaring af nøglekort, midlertidig adgangskode og cd-rom

Nøglekort, midlertidig adgangskode og cd-rom SKAL opbevares sikkert hos RA-virksomheder for at undgå uautoriseret adgang til lageret af nøglekort (se figur 1, proces 3b). Følgende SKAL gælde:

1) Nøglekort, midlertidig adgangskode og cd-rom SKAL opbevares i et sikkert aflåst skab, hvortil der er begrænset adgang.
2) Kun det bestemte antal nøglekort, midlertidig adgangskode og cd-rom til en specifik bruger MÅ tages fra skabet af medarbejdere hos RA.

3.5. Krav til distribution af nøglekort

Nøglekort SKAL distribueres på sikker vis for at undgå uautoriseret adgang til nøglekortene. Følgende SKAL gælde (se figur 1, proces 4a og 5b):

1) Brugeren SKAL være registreret og autentificeret inden nøglekortet sendes til brugeren.
2) Andre følsomme oplysninger MÅ IKKE vedlægges i samme kuvert, hvis nøglekortet sendes med posten.
3) RA-medarbejderen SKAL sikre, at kuverten er intakt, såfremt den leveres direkte fra RA-medarbejderen til brugeren.
4) Der skal føres log over hvilken brugere, der har fået leveret et nøglekort, og hvilken medarbejder hos RA'en, der har autoriseret denne levering i de tilfælde, hvor et nøglekort er blevet personligt leveret til brugeren.

3.6. Krav til midlertidig adgangskode

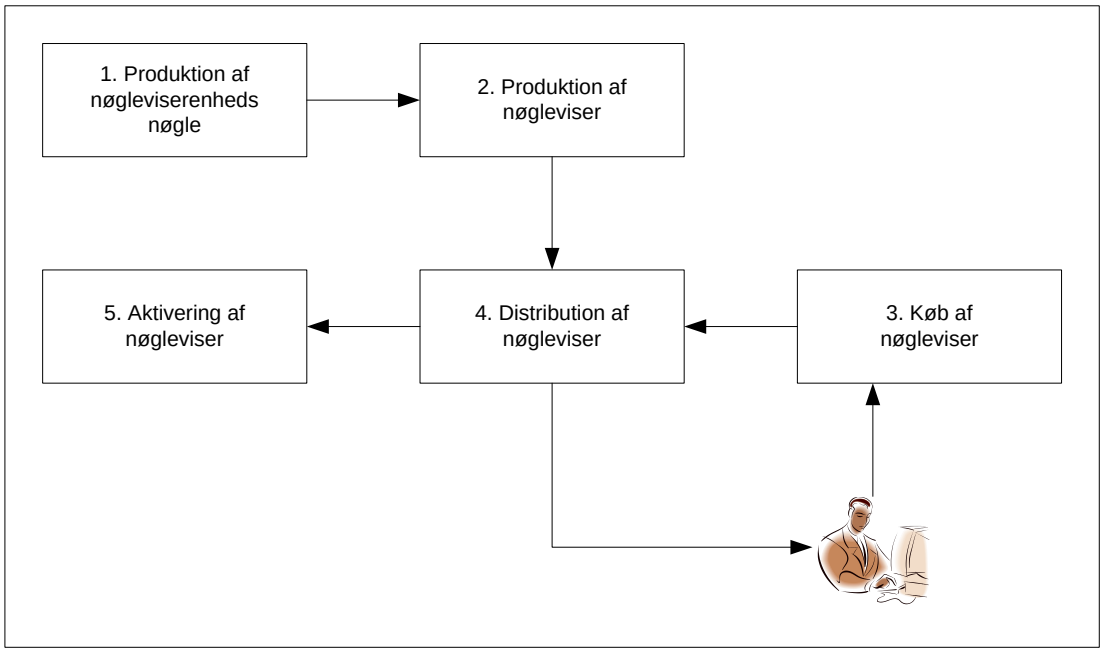
Brugeren benytter den midlertidige adgangskode til at aktivere brugerkontoen før nøglekortet tages i brug. Den midlertidige adgangskode SKAL kommunikeres til brugeren på sikker vis. Følgende SKAL som minimum gælde:

1) Den midlertidige adgangskode SKAL bestå af minimum 6 tal.
2) Den midlertidige adgangskode KAN leveres til brugere på forskellige pålidelige måder
   a) En forseglet, ugennemsigtig og neutral kuvert, som leveres direkte til brugeren.
   b) En forseglet, ugennemsigtig og neutral kuvert, som sendes med posten til en pålideligt registreret adresse.
   c) En sms til en pålideligt registreret mobiltelefon.
   d) En CD-ROM pakke i en forseglet og neutral pakke, som leveres direkte til brugeren.
   e) En CD-ROM pakke i en forseglet og neutral pakke, som sendes med posten til en pålideligt registreret adresse.
3) Det system, som fremstiller den midlertidige adgangskode, SKAL kunne modstå angreb, der har karakter af udtømmende søgning på kryptografiske nøgler.
4) Gyldigheden af den midlertidige adgangskode SKAL begrænses for at undgå uautoriseret brug. Gyldighedsperioden BØR defineres i forhold til den benyttede distributionskanal.

4. Introduktion til nøgleviser

Produktion af nøgleviser

Nedenstående figur viser produktion og distribution af nøgleviser.



Figur 2.- Produktion og distribution af nøgleviser

I proces 1. fremstilles en unik krypteringsnøgle, der i proces 2. skal installeres i nøgleviseren. Nøgleviseren sendes til distributionsstedet. I proces 3. køber brugeren nøgleviseren og bestillingen sendes til distributionsstedet. I proces 4. tildeles brugeren en specifik nøgleviser og nøgleviseren distribueres til brugeren. I proces 5. aktiveres nøgleviseren til brugeren.

Brug af nøgleviser
Nøgleviseren indeholder en knap. Når den aktiveres fremkommer den aktuelle nøgle i et display på nøgleviseren. Når brugeren skal autentificeres i en session, skal brugeren, ud over at indtaste bruger-id og personlig adgangskode, indtaste den nøgle, som fremkommer i nøgleviserens display indenfor en bestemt tidsgrænse.

4.1. Krav til nøgleviser

I dette afsnit beskrives kravene til nøgleviser.

1) Fremstilling af nøgler SKAL være resultatet af tiden og en unik nøgle for nøgleviseren.
2) Nøgleviseren SKAL kun sendes til en adresse, som er autentificeret af brugeren inden registrering af OTP-udstederen. Ved enhver anmodning om ændring af den registrerede adresse SKAL brugeren autentificeres.
3) Der SKAL håndhæves maksimumniveauer for hvor meget en nøgleviser må afvige i tid (drifte).
4) Batterilevetiden SKAL være minimum 4 år.

4.2. Krav til fremstilling af Nøgleviser

Fysisk og logisk sikkerhed

1) Fremstilling og distribution af nøgleviser SKAL efterleve den til enhver tid gældende Nets DanID's CPS (ref. 1.2 pkt. 3).

2) Fremstilling af krypteringsnøgle til hver enkel nøgleviser SKAL foregå ved brug af et sikkert HSM (hardware security module), som gør brug af en sikker pseudo-vilkårlig nummergenerator, der er godkendt af en international standardiseringsorganisation (ref. 1.2 (4)) som fx NIST. Opstartsværdien (seeding) SKAL være vilkårlig og fremstillingsprocessen for denne fyldestgørende dokumenteret.

3) Overførelsen af krypteringsnøgler til nøgleviserproduktionsudstyret SKAL være sikret imod aflytning og uautoriseret manipulation i perioden fra fremstillingen i HSM til nøgleviserfremstillingen hos producent (se figur 1 proces 1 til 3a og 2b).

4) De oplysninger, der er brugt i fremstillingen af en nøgleviser, SKAL slettes kort tid efter fremstillingen af nøgleviser (maksimum 120 timer efter fremstillingen) (se figur 1, proces 3a og 2b).

4.3. Krav til distribution af Nøgleviser

Nøgleviser SKAL distribueres på sikker vis for at undgå uautoriseret adgang til nøgleviserne. Følgende SKAL gælde (se figur 2, proces 4):

1) Brugeren SKAL være registreret og autentificeret inden nøgleviser sendes til brugeren.
2) Nøgleviser SKAL forsegles i ugennemsigtige neutrale kuverter (se figur 2, proces 4).
3) Andre følsomme oplysninger MÅ IKKE vedlægges i samme kuvert som nøgleviser fremsendes med.

5. Krav til brugerregistrering

Brugeren SKAL autentificere sig inden registrering.

1) Autentifikation og legitimation SKAL være på niveau med certifikatpolitikkerne for udstedelse af POCES/MOCES eller leve op til kravene for etablering af nyt kundeforhold jf. ref. 8 i danske banker.

6. Krav til personalisering og aktivering af nøglekort/nøgleviser

Se figur 1, proces 2a og 4b og figur 2 proces 4 og 5.

1) Nøglekort/nøgleviser SKAL personaliseres inden det leveres til brugere.
2) Personaliseringen og aktiveringen af brugerkontoen SKAL logges af OTP-udstederen.

7. Krav til brug af nøglekort/nøgleviser

Udsteder af nøglekort SKAL gennem aftale forpligte bruger til at overholde reglerne fastsat af OTP-udsteder for brug af nøglekort/nøgleviser (ref.7)

8. Krav til autentificeringsprotokol

1) Følsomme oplysninger, herunder nøglenummer og nøgler, MÅ KUN kommunikeres gennem et åbent netværk via en sikker kommunikationskanal.
2) Secure Remote Password (SRP) KAN benyttes til dette formål.

9. Krav til OTP back-end

9.1. OTP validering

OTP valideringskarakteristika: Sikkerheden i en OTP-løsning relaterer sig til; om hvorvidt en engangskode kan kædes direkte sammen med en specifik bruger og denne brugers OTP-enhed.

9.1.1. Krav til validering af nøgler fra trykte nøglekort

1) Der MÅ kun kunne accepteres en engangsnøgle for en given bruger på et givet tidspunkt.
2) Et nøglenummer SKAL være uforudsigeligt, men referere entydigt til en given nøgle på et specifikt nøglekort.
3) Det system, som validerer nøgler og adgangskoder, SKAL indeholde modforanstaltninger, der beskytter imod udtømmende søgning på adgangskoder og engangsnøgler samt indeholde forholdsregler for at modvirke angreb, der vil blokere systemet.
4) Alle loginforsøg SKAL logges.
5) Der KAN sendes en varsel til en bruger, når der et begrænset antal nøgler tilbage på nøglekortet.

9.1.2. Krav til validering af nøgler fra nøgleviser

1) Det system, som validerer nøgler og adgangskoder, SKAL indeholde modforanstaltninger, der beskytter imod udtømmende søgning på adgangskoder og engangsnøgler samt indeholde forholdsregler for at modvirke angreb, der vil blokere systemet.
2) Alle loginforsøg SKAL logges.
3) Systemet, der validerer nøgler, SKAL acceptere det, som burde være den aktuelle nøgle (hvis nøgleviseren ikke er kommet ud af synkronisering). Systemet BØR derudover acceptere nøgler i et variabelt (dog med en max størrelse) tidsinterval for at tage hensyn til, at uret i nøgleviseren kan afvige fra uret i det centrale backend system. Systemet BØR også indeholde funktionalitet til automatisk at detektere hvor meget en nøgleviser har driftet og herudfra flytte midten af det tidsintervalvindue, som der accepteres nøgler indenfor.

9.2. Administration af nøgler

Nøglenumre og nøgler SKAL være krypterede, når de opbevares i elektronisk form.

1) Kryptografiske nøgler (master keys) til beskyttelse af nøgler og nøglenumre SKAL være krypterede af en HSM nøgle, som kun genereres, benyttes og opbevares i certificerede sikkerhedsmoduler. (Ref. 1.2 FIPS 140-2, Level 3 og 4, eller lignende European Standard CWA 14167-2 Cryptographic Module for CSP Signing Operations – Protection Profile).
2) Hvis en HSM nøgle eksporteres fra modulet, fx til backup-formål, BØR nøglen transporteres enten (1) i krypteret form, hvor krypteringsnøglen er beskyttet med dobbelt kontrol eller (2) ved brug af opdelt viden og dobbelt kontrolprocedurer. Hvis procedureopdelt viden benyttes SKAL:

a) adgangskontrolsystemet til det kryptografiske modul særskilt autentificere den sikkerhedsadministrator, som indtaster hver enkelt nøglekomponent.

b) mindst to nøglekomponenter SKAL indgå til at rekonstruere den originale kryptografiske nøgle.

3) Intet enkeltindivid BØR alene have adgang fysisk eller logisk til nøgleadministrationsressourcer.

4) Al nøgleadministration SKAL logges.

- o 0 o -