UGRADERT

Norsk BankID sertifikatpolicy for BrukerstedsBankID v 2.9

august 2016

BankID sertifikatpolicy
status: godkjent versjon
dato: 11. august 2016

Bits AS
Postboks 2644 Solli
0203 Oslo

Tlf: 23 28 45 10
epost: post@bits.no

Kvalitetsstyring

Godkjenningsprosedyre for denne versjonen av dokumentet: Versjon 2.8 og 2.9– tekniske endringer fremlagt for og godkjent av BSK / Bits Faggruppe BankID. Versjon 2.3 inneholder en presisering av brukerstedets plikter i forhold til underleverandører, i seksjon 2.1.3 Dokumentet er godkjent i versjon 2.0 av FU etter høring i bankene og BankID samarbeidet Denne versjonen er tilpasset for generell publisering på linje med sertifikatpolicy for BankID kvalifiserte personsertifikater. Den er derfor en del omarbeidet fra versjon 1.0 og 1.1, som forelå på engelsk.
Distribusjon (bare for dokumenter med begrenset distribusjon): Dette dokumentet har åpen distribusjon på Internett.
Vedlikeholdsprosedyre: Se kap 8.

Dokumenthistorie

Versjon	Dato	Endr.nr / kommentarer	Dokument-ansvarlig	Godkjennes av
2.9	Juli 2016 Innført betegnelsen Bits AS.	Xxx	RHa	
2.8	Juli 2015 Synliggjort krav om 24/7 sperretjeneste. Presisert inn krav om kundeforhold i kap 1.3. Dokumenteierskap overført til BankID Norge AS. Erstattet begrepet Basis BrukerstedsBankID med Filbasert BrukerstedsBankID.	Xxx	RHa	
2.7	Sep 2013 Redaksjonelle endringer fra versjon 2.6.2	xxxx	RHa	BSK Faggr BankID
2.6.2	Sep 2013 Lagt inn åpning i kap 4.4.4. og 4.4.7 for å kjøre med eldre sperreliste i definert unntakstilstand	xxxx	RHa	BSK Faggr BankID
2.6.1	Feb 2013 Presisert ansvar for logging i kap 4.5.2. Innført "Finans Norge"	xxxx	RHa	BSK Faggr BankID
2.6	Sep 2012 Satt inn nye nivå-3 overskrifter 2.2.1 og 4.8.1 samt noen mindre justeringer i overskrifter for å få større likhet mellom dokumenter	xxxx	RHa	BSK
2.5	Feb 2012 Ny logo. Rydding og ajourhold av referanser. Presisert tekst om driftsmiljø i kap 5.1.2, kap 6.5 og kap 6.7. Presisert FNO til FNO Servicekontor i beskrivelse av oppgaver Tatt inn varsling i kap 2.8.4. -- Klargjort varslingsplikt i kap 2.1.2 og 2.1.3.	xxxx	RHa	FU
2.4	Sept 2010 Gjort endringer fordi FNO overtar oppgavene fra Sparebankforeningens Servicekontor og Finansnæringens servicekontor. Praktiske og redaksjonelle endringer behandlet i BSK Faggruppe 7.09.2010	xxxx	RHa	FU
2.3	Mars 2010 Lagt til et punkt om at brukerstedet kun skal bruke underleverandører det har tillit til	xxxx	RHa	FU
2.2	Juni 2009 Endret bruksområdet slik at signert datautveksling mellom to virksomheter som har BrukerstedsBankID, inngår	xxxx	RHa	FU
2.1.1	Mars 2008 Lagt inn en tekstlig presisering i kap 4.5.1	xxxx	RHa	FU
2.1	Jan 2008 Lagt inn presiseringer om krav til sperring (suspendering eller tilbakekalling) i kap 4.4.	xxxx	RHa	FU
2.0	Juni 2006 Versjon godkjent av FU 22.06.06. Innholdsmessig identisk med v1.9.1	xxxx	LA	FU
1.9.1	Juni 2006 Innarbeiding av kommentarer fra høring, april-mai 2006.	xxxx	LA	FU
1.9	Mars 2006 Norsk versjon, utkast, for publisering Begrepet ”brukerstedssertifikater” innføres for denne typen virksomhetssertifikater.	xxxx	LA	FU
1.1	Okt 2005 Enterprises registered in other EEA countries may obtain certificates. A number of editorial changes	xxxx	RHa	FU
1.0	April 2003 First approved version	xxxx	RHa	FU

INNHOLDSFORTEGNELSE

DEFINISJONER

I dette dokumentet forstås med følgende begreper:

Aktiveringsdata: Data, utenom kryptografiske nøkler, som trengs for tilgang til nøkkellagre, og som selv må behandles på sikker måte (f. eks. PIN-kode eller passord / passfrase).

Autentisere: Bekrefte/verifisere en påstått identitet. Prosessen sikrer autentisitet/ekthet.

Bank: Bank som er tilknyttet Finans Norge Servicekontor, samt norske og utenlandske banker og kredittinstitusjoner som med samtykke fra FNO Servicekontor utsteder BankID.

BankID: Ett eller flere nøkkelpar og elektroniske sertifikater som en bankkunde (sertifikat-holder) kan benytte til å sikre elektronisk meldingsutveksling med en bank eller med en banks kunde.

Brukersted: Enkeltpersonforetak og annen juridisk person (privat eller offentlig virksomhet og forvaltning) som har fått utstedt BankID for bruk ved kommunikasjon mellom brukerstedets nettsted og andre sertifikatholdere.

BrukerstedsBankID: En BankID utstedt til en virksomhet og som identifiserer virksomheten og eventuelle enheter eller funksjoner i virksomheten. En BrukerstedsBankID kan være en av to varianter: Filbasert BrukerstedsBankID eller HSM-basert BrukerstedsBankID.

Delt hemmelighet: Informasjon som består av ett eller flere hemmelige elementer, som bare er kjent av de to involverte partene, og der minst ett hemmelig element har vært distribuert over en sikker kanal. En delt hemmelighet brukes under sertifiseringsprosessen for å autentisere kunden.

Enhetsregisteret: Norsk offentlig register som inneholder registrerte virksomheter i Norge. Tildeler virksomhetene et unikt organisasjonsnummer.

Fellesutsteder: En juridisk person som utsteder BankID på oppdrag fra en gruppe banker og benytter et nivå 1-sertifikat utstedt av rot-CA for dette formål (jfr. kap 1.3.1).

Filbasert BrukerstedsBankID: En BrukerstedsBankID der de private nøklene lagres som en beskyttet nøkkelfil.

HSM: Sikkerhetsmodul for fysisk og logisk beskyttelse av private nøkler (maskinvare).

HSM-basert BrukerstedsBankID: En BrukerstedsBankID der nøkler genereres og lagres i en HSM.

Installasjonskode: Sikkerhetskode som mottas fra banken når BrukerstedsBankID bestilles. Denne engangskoden anvendes i forbindelse med aktivering av BrukerstedsBankID.

Nøkkellager: Det logisk og fysisk definerte miljøet hvor sertifikatholders private nøkkel blir lagret.

Objektidentifikator (OID): En sekvens av heltall som entydig refererer til et objekt. Med objekt forstås her f. eks. en definert informasjonsstruktur eller en spesifikasjon.

Registeringsenhet (RA): En enhet som påtar seg å korrekt bekrefte identiteten til en fremtidig sertifikatholder. Dette må gjøres av den enkelte bank, eller en betrodd tjenesteleverandør for denne.

Sertifikat (Offentlig nøkkel sertifikat): En sekvens av data som inneholder sertifikatholders offentlige nøkkel sammen med annen informasjon, og som er gjort umulig å forfalske ved at informasjonen er signert med en sertifikatutstеders private nøkkel.

Sertifikatpolicy (CP): Et dokument som inneholder regler for hvordan sertifikater utstedes og behandles, og som dermed definerer hvilken tillit man kan ha til sertifikatene.

Sertifikatholder : Bankkunde som er abonnent på sertifiseringstjenester og har fått utstedt BankID. I denne policyen er sertifikatholder en virksomhet. Samme virksomhet som er sertifikatholder, kan også forekomme i rollen som sertifikatmottaker.
(Kommentar: Begrepet sertifikatinnehaver kan også brukes.)

Sertifikatkontrollør: En tiltrodd tjeneste som bekrefter status på sertifikater for en sertifikat-mottaker.

Sertifikatmottaker: Den som mottar et signert dokument eller melding med tilhørende sertifikat, og som skal verifisere og etablere tillit til det mottatte materiale.

Sperre: Gjøre et sertifikat ugyldig. En sperring kan være tidsbegrenset (suspendering) eller permanent (tilbakekalling).

Tjenesteleverandør: En organisasjon eller enhet som forestår praktiske oppgaver innenfor utstedelse av sertifikater, eller utfører andre tjenester relatert til elektronisk signatur på vegne av bank.

Utstede BankID: Signere BankID med den private nøkkelen tilhørende et nivå 1-sertifikat utstedt av rot-CA.

Utsteder av BankID: Bank eller Fellesutsteder som kan utstede BankID.

Utstedersystem (Certification Authority system): Praktisk realisering av rollen som Utsteder av BankID. Utstedersystemet signerer sertifikatholderes offentlige nøkler og annen sertifikatinformasjon med sin private nøkkel.

Valideringstjeneste: Se sertifikatkontrollør.

Virksomhet: En juridisk person (privat eller offentlig virksomhet og forvaltning), som er registrert i Enhetsregisteret eller et tilsvarende offentlig register innenfor EØS-området, og som har konto i en norsk bank.

Virksomhetskunde: Vil i dette dokumentet betegne virksomheter som ennå ikke er blitt sertifikatholdere.

FORKORTELSER

BSK	Bankenes Standardiseringskontor (nå Bits AS)
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
ETSI	European Telecommunication Standard Institute
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Standards Organisation
ITU	International Telecommunications Union
KEK	Key Encryption Key
NIST	National Institute of Standards and Technology
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request for Comment
RSA	Rivest, Shamir, Adleman
TCP/IP	Transmission Control Protocol / Internet Protocol

Referanser

Number	Short name	Reference
[1]	Regler om BankID	Interbankregler om elektronisk BankID (Regler om BankID), juni 2000 med senere endringer. . Nyeste versjon kan hentes fra Finans Norge.
[2]	FIPS-140-1	"Security Requirements for Cryptographic Modules", NIST, US Dept. of Commerce, FIPS 140-1, 1994 and FIPS 140-2, 2002
[3]	Hvitvaskingsloven med forskrifter	"Lov 2009-03-06 nr 11 om tiltak mot hvitvasking og terrorfinansiering mv." med forskrifter.
[4]	Bank/kunde-avtalen	Avtale mellom bank og kunde om elektronisk BankID. For virksomheter er avtalen basert på mønster til "Avtalevilkår for BrukerstedsBankID" og for personer er avtalen basert på mønster til "Avtalevilkår for BankID personsertifikat". Mønsteravtalene er utarbeidet av FNO Servicekontor.
[5]	RFC2527	"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", S.Chokhani, W.Ford, RFC2527, March 1999
[6]	X509	Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, ITU-T X.509, 11/2008
[7]	Rot-CA's CP/CPS	Norwegian BankID Root CP/CPS v2.3, August 2016
[8]	Certificates	BankID External Certificates (gjeldende versjon)
[9]	Personopplysningsloven	"Lov om behandling av personopplysninger", Lov 2000-04-14-31 med senere endringer
[10]	E-signatur loven	"Lov om elektronisk signatur", Lov 2001-06-15-81, sist endret 2005-06-17
[11]	BSK Sikkerhetskravdokument	Bits / BSK: Samlet kravdokument for sikkerhet i BankID; nyeste versjon

1 INNLEDNING

1.1 OVERSIKT

Dette dokumentet beskriver sertifikatpolicy for BankID-sertifikater til virksomheter (BrukerstedsBankID). BankID kan utstedes av banker som er tilknyttet Finans Norge Servicekontor, samt utenlandske banker og kredittinstitusjoner som med samtykke fra Finans Norge Servicekontor har sluttet seg til regler om BankID.

Dette dokumentet er ugradert og har fri distribusjon. Beskrivelse av sikkerhet og tekniske valg i løsningene er derfor på et relativt overordnet nivå. Dokumentet er organisert i samsvar med vanlig praksis og internasjonal standardisering [5] for sertifikatpolicy dokumenter.

Denne sertifikatpolicy beskriver de krav som banker i Norge stiller til BrukerstedsBankID. Det spesifiseres to ulike varianter: en Filbasert variant, der private nøkler lagres som en beskyttet fil, og en HSM-basert variant, der private nøkler lagres i en fysisk sikkerhetsmodul.

En bank som tilbyr BankID, skal inngå avtale med sertifikatholder. Denne skal være på det språk banken vanligvis bruker i kommunikasjon med kunden og forklare rettigheter og plikter for sertifikatholder.

En BankID består av ett, to eller tre nøkkelpar; hvert par bestående av en privat og en offentlig nøkkel. BankID utstedt i henhold til denne versjonen av sertifikatpolicy består av to nøkkelpar.

Når et utstedersystem lager et sertifikat, attesterer utsteder av BankID bindingen mellom den offentlige nøkkelen og virksomhetens offisielle navn og dens nummer i det norske Enhetsregisteret eller tilsvarende register. Samtidig ivaretar sertifikatet at den offentlige nøkkelen er beskyttet mot endring (integritetsbeskyttelse). Den enkelte nøkkel skal kun bli brukt i samsvar med den funksjon som står angitt i sertifikatet.

1.2 IDENTIFIKASJON AV POLICY

Dette policy-dokumentet beskriver sertifikatpolicy for BrukerstedsBankID som er sertifikater utstedt virksomheter som er BankID brukersteder.

Alle BankID-sertifikater skal inneholde en entydig objektidentifikator (OID) som viser hvilken policy sertifikatet er utstedt under. Ut fra dette feltet skal en sertifikatmottaker eller sertifikatkontrollør automatisk kunne avgjøre om et sertifikat passer til en gitt type anvendelse.

For BrukerstedsBankID basert på nøkler lagret i beskyttet fil, skal denne identifikatoren benyttes:
Object Identifier (OID):
{joint-iso-itu-t(2) country(16) norway(578) organisasjon(1)
bankenes-standardiseringskontor(16) policy(1) corporate(6) soft(1) 1}

For BrukerstedsBankID der private nøkler lagres i maskinvare (HSM) skal denne identifikatoren benyttes:
{joint-iso-itu-t(2) country(16) norway(578) organisasjon(1)
bankenes-standardiseringskontor(16) policy(1) corporate(6) hsm(2) 1}

1.3 BRUKSOMRÅDE OG AKTØRER

Dette dokumentet beskriver regler for bruk av BrukerstedsBankID utstedt til bankenes virksomhetskunder. Virksomheten vil som oftest ha et kontoforhold til utstedende bank, men regelverket tillater utstedelse av BrukerstedsBankID til virksomheter uten kontoforhold.

En bank kan enten selv være utsteder av BankID med eget utstedersystem på nivå 1, eller inngå avtale med en fellesutsteder. Navnet på fellesutsteder kan leses ut fra sertifikatene (se

kap 3.1). Forholdet mellom bankene som bruker fellesutsteder og denne er regulert av en tjenesteavtale.

1.3.1 Utsteder av BankID

Beskrivelsen i denne seksjonen gjelder både for banker og fellesutstedere som utsteder BankID.

Utstedere av BankID er organisert i et hierarki med én rot-CA og ett nivå underordnede utstedere av BankID (nivå 1). Rot-CA utsteder sertifikater på nivå 1 i henhold til Regler om BankID [1].

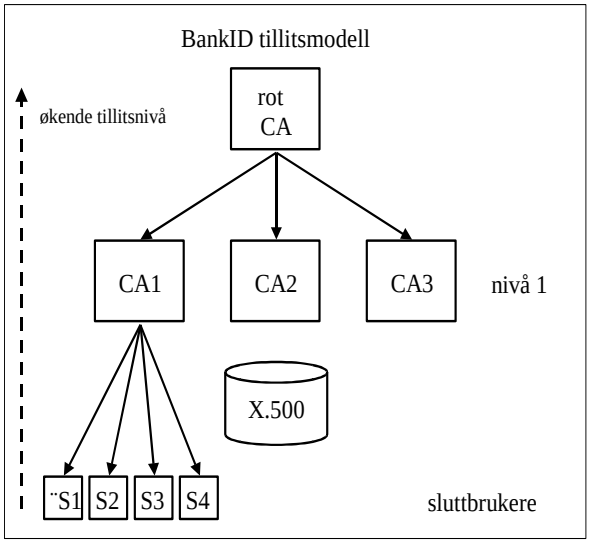
Rot-CA ble etablert av Finansnæringens Servicekontor (FNS) og Sparebankforeningens Servicekontor. Fra 1.1.2010 har Finans Norge Servicekontor overtatt oppgavene fra servicekontorene, herunder oppgaven som rot-CA. Prosedyrer rundt drift av rot-CA system skal godkjennes av Bits AS (tidligere Bankenes Standardiseringskontor (BSK)).

Foruten banker kan også fellesutstedere utstede BankID, men avtale [4] med kunde / sertifikatholder om utstedelse og bruk av BankID skal alltid inngås med en bank.

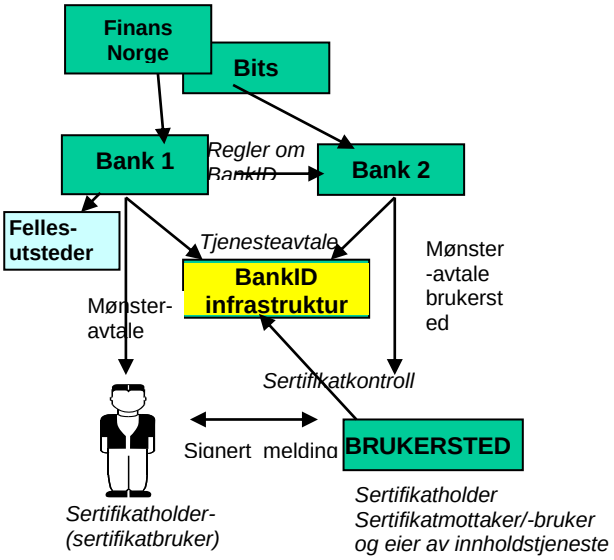
Bank som utsteder BankID, kan selv etablere et utstedersystem eller benytte en fellesutsteder til å forestå utstedelsen av sertifikater.

En utsteder av BankID i samsvar med dette dokumentet skal:

a) operere i samsvar med betingelsene i dette dokumentet,
b) lage et dokument som beskriver praksis for sertifikatutstedelse (CPS) og som refererer til den aktuelle sertifikatpolicy,
c) bruke systemløsninger som er godkjent av Bits. Godkjenningen skal også omfatte utsteders produksjonsmiljø og eventuelle bruk av tjenesteleverandører,



Figur 1 - BankID tillitsmodell



Figur 2 – Avtaler i BankID

1.3.2 Registreringsenhet

En registreringsenhet (RA) skal operere i samsvar med betingelsene i dette dokumentet. Registreringsenheten må også operere i samsvar med CPS som tilhører en utsteder av BankID.

Bank har ansvar for RA-funksjonen, også i de tilfeller der en fellesutsteder utsteder BankID for banken. Dette ansvaret må være ivaretatt i avtaler mellom bank og fellesutsteder.

Banker kan selv være RA, eller la seg bistå av en tjenesteleverandør. Banken er uansett ansvarlig for de tjenestene registreringsenheten utfører.

1.3.3 Virksomheter / sertifikatholdere

I dette dokumentet [og tilhørende CPSer med underliggende dokumentasjon] er sertifikatholder en juridisk person (privat eller offentlig virksomhet og forvaltning), som er registrert i Enhetsregisteret eller et tilsvarende offentlig register innenfor EØS-området, og som har et kundeforhold til vedkommende bank [1]. BankID utstedt til juridiske personer kan benyttes av maskinvare og applikasjoner.

En virksomhet kan være mottaker av en melding sikret med en PersonBankID eller AnsattBankID. I samhandling mellom en virksomhet og en fysisk person må virksomheten forholde seg til kravene som stilles i dette policydokumentet. Innehaveren av PersonBankID eller AnsattBankID må forholde seg til de krav som stilles i den aktuelle policy for sin BankID.

1.3.4 Anvendelighet

Sertifikater utstedt under denne sertifikatpolicy blir brukt mellom brukersteder og fysiske personer som bruker BankID til å utføre følgende sikkerhetstjenester:

- autentisering
- digital signering.

Sertifikater utstedt under denne sertifikatpolicy kan også brukes mellom to virksomheter som er BankID brukersteder til å utveksle digitalt signert informasjon.

Begge parter må ha inngått avtale med sin bank om bruk av BankID. Virksomhet som er brukersted**,** må ha signert lisensbetingelser for BankID Server programvare og dokumentasjon som ledd i avtale med banken om bruk av BrukerstedsBankID, se mønsteravtale [4].

Virksomheten må sammen med BankID benytte slik programvare, maskinutrustning eller det sikkerhetsutstyr som banken spesifiserer. Banken kan stille nye krav til programvare/ maskinutrustning/sikkerhetsutstyr der dette er nødvendig av sikkerhetsmessige grunner eller ved nødvendige oppgraderinger av BankID. Dersom BankID blir aktivert i et datamaskinmiljø som ikke oppfyller BankIDs sikkerhetskrav, kan dette medføre risiko for misbruk. Banker vil opplyse sine kunder om krav og råd for bruksmiljøet.

Dersom banken utvider eller begrenser anvendelsesområdet for BankID, herunder beløpsmessige begrensninger, vil kunden motta varsel om dette. Anvendelsesområdet er nærmere beskrevet i brukerdokumentasjonen.

Sertifikater utstedt under denne sertifikatpolicy, kan ikke benyttes som grunnlag for å utstede andre sertifikater eller legitimasjonsinstrumenter.

1.4 KONTAKTINFORMASJON

BankID Norge AS er gitt ansvar for å fastsette og forvalte sertifikatpolicyer i BankID. Bits AS redigerer standarder og policy for BankID på oppdrag for BankID Norge, og er ansvarlig for vedlikehold av BankIDs policyer og dette dokumentet. Dette følger av “Regler om BankID” §4.1 [1].

Dette dokumentet er utgitt av Bits AS på vegne av deltakende utstedere. Bits er også registrert innehaver av BankID policyer.

Postadresse:
Bits AS
Postboks 2644 Solli,
0203 OSLO
telefon: 23 28 45 10
e-post: post@bits.no

2 ALMINNELIGE BESTEMMELSER

Dette kapitlet setter opp hovedtrekk i aktørenes plikter.

En bank som er sertifikatutsteder (CA) eller registreringsenhet (RA) har de plikter som følger nedenfor. I tillegg plikter bank å:

- forholde seg til IKT-forskriftene fra Finanstilsynet
- være sertifikatholders avtalepart og kontaktpunkt
- ved bruk av fellesutsteder, inngå de nødvendige avtaler med denne
- ha ansvar overfor andre banker i BankID Samarbeidet, for de sertifikatene banken har inngått avtale om
- etterkomme bestemmelser i "Regler om BankID" [1], relevante deler av CP/CPS for Rot-CA [7], denne sertifikatpolicy og tilhørende CPS

En bank som ønsker å tilby BankID må levere skriftlig erklæring om at banken har forstått og akseptert de plikter som "Regler om BankID" [1], Rot-CA's CP/CPS [7] og BankIDs policyer medfører.

2.1 PLIKTER

2.1.1 Plikter for utsteder av BankID, herunder fellesutsteder

Utsteder av BankID skal:

- utstede, sperre eller fornye sertifikater
- foreta alle tekniske kontroller som beskrevet i kap. 4 til 6 i dette dokumentet og tilhørende CPS
- opprette og vedlikeholde en database over sertifikater
- opprette og periodiskvedlikeholde informasjon om tilbakekalte og sperrede sertifikater og gjøre informasjon om sperring tilgjengelig for sertifikat-kontrollører
- beskytte sine private nøkler som beskrevet i kap. 4 til 6
- produsere hendelseslogger og system-status informasjon for arkivering
- etterkomme bestemmelser i "Regler om BankID" [1], relevante deler av CP/CPS for Rot-CA [7], denne sertifikatpolicy og tilhørende CPS

Oppgavene i listen over skal utføres korrekt av både banker og fellesutstedere. I tillegg til listen må fellesutsteder

- innhente godkjenning fra Bits
- oppfylle krav til soliditet i forhold til e-signaturloven [10]
- inngå avtale med bankene som benytter denne fellesutstederen.

En sertifikatutstеders private nøkkel for utstedelse av sertifikater skal bare brukes til å signere sertifikater og CRLer.

2.1.2 Plikter for registreringsenhet (RA)

Registreringsenhet (RA) skal:

- kontrollere og stadfeste identiteten av personer som bestiller sertifikat på vegne av en virksomhet, verifisere at personen er autorisert til å handle på vegne av virksomheten, samt ta vare på informasjon som bevitner at korrekt prosedyre er fulgt.
- veilede og hjelpe kunden i registreringsprosessen
- utføre prosedyrene beskrevet i kap. 3 for å forvisse seg om at virksomheten eksisterer, er registrert i et nasjonalt register og fyller vilkårene for å få BrukerstedsBankID.
- sammenstille og videresende til utsteder den informasjon om kunden som er nødvendig for å kunne utstede BankID
- legge til rette for at det blir brukt eller tildelt et riktig entydighetsbegrep for å identifisere virksomheten
- ha mulighet til å initiere sperring av sertifikater

- bistå sine brukerstedskunder når de kontakter banken med mistanke om at det har vært forsøkt brukt en kompromittert eller forfalsket BankID, og hvis banken ser at mistanken er begrunnet, kontakte utstederbank for antatt kompromittert BankID
- etterkomme bestemmelser i "Regler om BankID" [1], relevante deler av CP/CPS for Rot-CA [7], denne sertifikatpolicy og tilhørende CPS.

2.1.3 Plikter for sertifikatholder (innehaver av BrukerstedsBankID)

Viktige plikter for sertifikatholder skal også stå i bank/kunde- avtalen [4].

Sertifikatholder skal:

- følge anviste prosedyrer når det søkes om sertifikat
- oppgi korrekt og fullstendig informasjon når det søkes om sertifikat
- sette seg inn i avtalevilkår for utstedelse og bruk av BankID, gjøre disse tilgjengelige for det personell som har behov for å kjenne dem og bekrefte overfor banken at vilkårene aksepteres
- kun benytte underleverandører som brukerstedet har tillit til, og følge prosedyrer i samsvar med bank/kunde avtalen
- verifisere at informasjon i det mottatte sertifikatet er korrekt og varsle banken om eventuelle feil
- utføre de pålagte tester og aktiveringssekvenser
- bruke nøkler og sertifikater bare i forbindelse med BankID-sertifisert programvare og i samsvar med tiltenkt bruk
- beskytte passord, PIN-koder og aktiveringsdata, samt private nøkler og forsikre seg om at disse holdes hemmelige
- informere banken om forhold av betydning for avtaleforholdet, herunder endringer i opplysninger gitt ved utstedelse
- på forespørsel kunne dokumentere hvilke IT-systemer og prosesser, eventuelt også personer som har tilgang til å bruke private nøkler
- rapportere på anvist måte til banken (eller dens tjenesteleverandør) ved enhver mistanke om at brukerstedets private nøkkel er blitt kjent for andre
- rapportere til banken ved enhver mistanke om at aktiveringsdata eller passord eller kan ha blitt kjent for andre
- umiddelbart slutte å bruke en BankID hvor brukerstedets private nøkkel eller aktiveringsdata mistenkes å ha blitt kjent for andre
- dersom det er begrunnet mistanke om at noen har forsøkt å bruke en kompromittert eller forfalsket BankID mot brukerstedet, umiddelbart kontakte sin egen utstederbank for å varsle om dette.

2.1.4 Plikter for sertifikatmottaker

Sertifikatmottaker kan være en bank, en virksomhet eller en person.

Sertifikatmottaker skal:

- kontrollere sertifikatets gyldighet og ikke akseptere det hvis det er sperret, utløpt eller på annen måte avsluttet
- kontrollere og forholde seg til eventuelle bruksbegrensinger for sertifikatet som følger av inngåtte avtaler eller av den sertifikatpolicy sertifikatet er utstedt under
- bruke sertifikatet og tilhørende offentlige nøkkeldata bare for det formål som er angitt i sertifikatet (f.eks. gjennom bruk av feltet *certificatePolicies*)

2.1.5 Plikter for tjenesteleverandør

En tjenesteleverandør kan utføre hele eller deler av en banks eller en fellesutstеders funksjoner. Tjenesteleverandøren må opptre i samsvar med dette dokumentet og tilhørende CPS samt skriftlige avtaler mellom partene.

Sertifikatholder og sertifikatmottaker skal alltid forholde seg til den bank han har avtale med, uavhengig av om funksjoner blir utført hos en fellesutsteder eller en tjenesteleverandør.

2.2 ERSTATNINGSANSVAR

2.2.1 Banks ansvar

Ansvarsforhold mellom bank og kunde er regulert av avtaler, både når kunde er sertifikatholder og sertifikatmottaker.

Både der banken er utsteder av BankID og der banken benytter en fellesutsteder, er bankens ansvar regulert i avtalen mellom banken og sertifikatholder [4]. Utsteder av BankID vil videre alltid kunne holdes erstatningsansvarlig etter e-signaturlovens regler om erstatningsansvar.

Banks ansvar gjelder også der bank eller utsteder har benyttet en tjenesteleverandør.

For øvrig vil banken kunne holdes erstatningsansvarlig på alminnelig kontraktsmessig grunnlag. Ved bruk av BankID for finansielle transaksjoner som omfattes av finansavtale-loven, vil ansvarsreglene i finansavtaleloven regulere bankens ansvar for disse transaksjonene.

Ansvarsfordeling mellom bankene, herunder regressansvar, er regulert gjennom avtaler mellom bankene.

2.2.2 Registreringsenhets (RA) ansvar

Det er banken som gjennom avtale påtar seg erstatningsansvar overfor kunden, også for oppgaver som en eventuell tjenesteleverandør av registreringsenhet har påtatt seg. Benytter banken en tjenesteleverandør som registreringsenhet, skal registreringsenhetens ansvar overfor banken være nærmere regulert i avtale mellom registreringsenhet og bank.

2.2.3 Sertifikatholders ansvar

Sertifikatholders ansvar reguleres i avtale [4] mellom bank og sertifikatholder. Bruker kunden BankID, programvare eller dokumentasjon i strid med inngått avtale, herunder uberettiget endrer eller manipulerer BankID eller programvare, kan banken holde kunden erstatnings-ansvarlig for bankens tap som følge av dette.

Kunden vil videre etter alminnelige rettsregler kunne bli gjort ansvarlig for disposisjoner som er foretatt av noen som har fått mulighet til å disponere kundens BankID på grunnlag av forsettlig eller uaktsom handling eller unnlatelse fra kundens side.

2.2.4 Sertifikatmottakers ansvar

Sertifikatmottaker kan være enten fysisk person eller virksomhet. Sertifikatmottakers ansvar reguleres i avtale [4] med bank.

2.3 ØKONOMISK ANSVAR

Bankens økonomiske ansvar er begrenset til kr 100.000,- for hver transaksjon [4]. Beløpsgrensen gjelder ikke dersom banken, dens tjenesteleverandør eller noen annen banken er ansvarlig for, har opptrådt forsettlig eller grovt uaktsomt.

Hvis sertifikatholder [og sertifikatmottaker] ikke oppfyller forpliktelsene i kap. 2.1.3. og 2.1.4, kan de holdes erstatningsansvarlige for eventuelle tap som oppstår, eventuelt kan deres erstatningskrav mot banken bli redusert eller falle bort som følge av brudd på forpliktelsene.

Banker som bruker en fellesutsteder til å utstede BankID, må sørge for at fellesutstederen har tilstrekkelige økonomiske ressurser i samsvar med e-signaturlovens [10] soliditetskrav. Ansvarsforholdet mellom banken og fellesutsteder, og mellom banken og andre tjenesteleverandører er regulert av avtaler mellom disse.

2.4 LOVVALG OG TVISTELØSNING

Tvister om utstedelse og bruk av BankID skal løses i tråd med norsk lov. Eventuell sak skal føres for norske domstoler. Tvister mellom en forbruker og bank om tjenester levert av bank kan kunden normalt bringe inn for Bankklagenemnda for uttalelse.

2.5 GEBYRER

Beskrives ikke i dette dokumentet. Den enkelte bank fastsetter priser overfor sine kunder.

2.6 TILGJENGELIG INFORMASJON

2.6.1 Publisering av informasjon om utsteder av BankID

Dette dokumentet skal gjøres tilgjengelig på www.bankid.no og deltakende bankers hjemmesider. For regler om vedlikehold og versjonskontroll, se kap 8.

Utstedere av BankID skal gjøre tilbakekallingsinformasjon tilgjengelig for tjenesteleverandører av BankID sertifikatkontrolltjeneste, se kap 4.4.

For å opprettholde tillitshierarkiet skal CA-sertifikater fortsatt gjøres tilgjengelige helt til alle underliggende sertifikater er utløpt.

2.6.2 Tilgang til dokumentasjon

Dette dokumentet med BankID sertifikatpolicy er ugradert og kan uten restriksjoner leses av alle.

Adgang til å lese CPS vil bli gitt individuelt på “need-to-know”-basis.

Policy-dokumenter, CPS, CRLer og annen informasjon om sertifikater lagret i lagringsenhet skal være beskyttet mot uautorisert endring.

2.7 SAMSVARSREVISJON

Banker, fellesutstedere og deres tjenesteleverandør skal undergå periodisk samsvarsrevisjon. Samsvarsrevisjonen skal i regelen foretas minst hvert tredje år. I tillegg skal det foretas samsvarsrevisjon ved nyetableringer eller større endringer i løsningene hos etablerte utstedere. Dette skal sikre at deres operasjon er i samsvar med krav i policy og CPS.

Revisjon av bank, fellesutsteder eller tjenesteleverandør for å bekrefte at de oppfyller andre krav enn BankID sertifikatpolicy (f. eks. fra offentlige myndigheter), kan komme i tillegg til ovennevnte samsvarsrevisjon. Bankene og deres tjenesteleverandører vil være gjenstand for revisjoner og kontroller fra:

- Kredittilsynet eller respektive tilsynsmyndighet for utenlandske banker
- Evt. selvpålagt ekstern revisjon i forhold til kvalitetsstandarder i ISO 9000-serien
- Evt. selvpålagt ekstern revisjon i forhold til standarder for sikkerhet og god praksis
- Post- og Teletilsynet (i forbindelse med utstedelse av kvalifiserte sertifikater)
- Bits AS
- Interne revisjons- og kontrollfunksjoner.

2.7.1 Hvem utfører samsvarsrevisjon

Samsvarsrevisjon skal utføres av en uavhengig person som ikke er ansatt i banken som blir revidert, fellesutsteder eller hos deres tjenesteleverandør.

Bits har rett til å godkjenne samsvarsrevisor. Valget bør gjøres i avtale mellom utsteder av BankID, tjenesteleverandør og Bits

2.7.2 Hva omfatter samsvarsrevisjon

Formålet er å bedømme om krav i BankID sertifikatpolicy oppfylles og sammenlikne utsteder av BankIDs praksis med krav i sertifikatpolicy og beskrivelser i CPS. Policy og CPS er obligatoriske bakgrunnsdokumenter. Ytterligere gradert sikkerhetsdokumentasjon kan legges fram og tas i betraktning under samsvarsrevisjon.

Også registreringsenhets (RA) operasjon skal være gjenstand for samsvarsrevisjon.

2.7.3 Oppfølging

Enhver uoverensstemmelse mellom reglene definert i policy og CPS, og reell operasjon hos bank, fellesutsteder eller tjenesteleverandør skal rapporteres til ansvarlig ledelse hos den aktuelle part og Bits. Disse skal sammen definere korrektive tiltak og et tidspunkt for når rettelsene skal være utført. Bits skal vurdere om bank umiddelbart skal informeres om forhold som angår fellesutsteder eller tjenesteleverandør som banken bruker.

Parten som er blitt revidert, bestemmer hvem som får tilgang til resultater av samsvars-revisjon. En konkluderende oppsummering skal ikke graderes og skal gjøres allment tilgjengelig på forespørsel. Denne bør inneholde informasjon om eventuelle avvik av betydning for sertifikatmottakers tillit til sertifikatene, men skal utelate detaljer som kan brukes til å angripe systemet.

Parten som er blitt revidert, må forplikte seg til enten å bringe sin praksis i samsvar med policy og CPS, eller sende inn begrunnede forslag for å endre policy/CPS.

2.8 KONFIDENSIALITET

Banker har taushetsplikt etter regler i Finansforetaksloven 9-6, med mindre annet følger av lovbestemt opplysningsplikt. Fellesutsteder og bankers/fellesutstederes tjenesteleverandører vil gjennom avtale med banken være underlagt tilsvarende taushetsplikt. Videre kommer e-signaturloven [10] og personopplysningsloven [9] til anvendelse.

Utsteder av BankID skal informere om sine gjeldende regler og rutiner for behandling av personopplysninger.

2.8.1 Typer informasjon som skal holdes konfidensiell

Banker og fellesutstedere av BankID har ansvar for at bl.a. følgende typer informasjon holdes konfidensiell:

a) data om sertifikatholdere eller virksomheter som ikke kan leses ut av sertifikatet eller en eventuell offentlig tilgjengelig katalogtjeneste
b) utsteders og registreringsenhets private nøkler
c) passord, PIN-koder og andre aktiveringsdata, så lenge opplysningene befinner seg hos bank / utsteder
d) alle sertifikatholderes private nøkler hvis disse på noe stadium er blitt behandlet av utsteder eller dennes tjenesteleverandør
e) loggdata
f) dokumentasjon som gir ytterligere detaljer om operasjonelle prosedyrer hos utsteder av BankID og dennes tjenesteleverandør.

I tillegg skal informasjon om, aktiverings- og autentiseringsdata for sertifikatholdere, transaksjonsdata og teknisk sikkerhet i infrastrukturen holdes konfidensiell.

2.8.2 Typer informasjon som ikke anses konfidensiell

Følgende typer informasjon som behandles av utstedere av BankID, anses ikke konfidensiell:
a) sertifikater
b) tilbakekallingsstatus for et sertifikat
c) sertifikatpolicy for kvalifiserte sertifikater og for BrukerstedsBankID.

Informasjon om sertifikatholdere (navn, fødselsdato etc.) som kan leses ut av sertifikater, anses ikke konfidensiell.

Det skal ikke være mulig å reservere seg mot å komme på tilbakekallingslistene, eller mot at sertifikatstatus for BankID blir gjort kjent for godkjente sertifikatkontrollører.

2.8.3 Utlevering av informasjon

Hovedregelen er at bank har taushetsplikt som angitt i kap 2.8.1. Utlevering av informasjon kan skje som følge av lovbestemt opplysningsplikt.

For utlevering utover pålagt opplysningsplikt eller innsynsrett kreves sertifikatholders godkjennelse.

2.8.4 Varsling

Ved sikkerhetshendelser relatert til utstedelse og bruk av BankID har banker, fellesutstedere og tjenesteleverandører plikt til å varsle hverandre. Bits og BankID Norge skal gi retningslinjer for varsling. Informasjon som blir utvekslet, skal ikke identifisere enkeltkunder med unntak av når det blir varslet for å begrense eller forebygge misbruk av BankID eller tap av økonomiske midler for den enkelte kunde.

2.9 RÅDERETT

Sertifikatholder har disposisjonsrett til sitt sertifikat, inkl. retten til å be om sperring (tilbakekalling / suspendering).

Banken eier BankID-programvare og dokumentasjon som blir distribuert i forbindelse med BankID-tjenester.

3 IDENTIFIKASJON OG LEGITIMERING

Dette kapitlet beskriver regler og praksis som skal følges for å identifisere og kontrollere legitimasjon for personer og virksomheter (organisasjoner) før de kan få utlevert sertifikater.

3.1 FØRSTE GANGS REGISTRERING

3.1.1 Navnetyper

I sertifikater skal feltet "subject" og feltet "issuer" inneholde informasjon av typen "Distinguished Name" - (DN) som definert i X.500 rammeverket. Et DN er en sekvens av betegnelser (attributter) om en entitet (f. eks. en person eller virksomhet) som unikt definerer vedkommende.

SERTIFIKATHOLDERS NAVN
Dette dokumentet omhandler BrukerstedsBankID, bundet til en virksomhet som er BankID brukersted.

Attributt	Viktighet	Krav til innhold
Country (C)	Oblig	Landet der virksomheten er registrert. Skal ha verdien 'NO' for virksomheter registrert i Norge.
Organisation Name(O)	Oblig	Skal inneholde virksomhetens offisielle navn slik det er registrert i Enhetsregisteret eller tilsvarende offentlig register.
Serial Number (SN)	Oblig	Skal inneholde virksomhetens organisasjonsnummer i Enhetsregisteret eller tilsvarende offentlig register innenfor EØS-området.
Organisational Unit (OU)	Valgfritt	Felt som brukes til å angi enheter eller funksjoner innen virksomheten
Common Name (CN)	Oblig	Alminnelig brukt navn på virksomheten

SERTIFIKATUTSTEDERS NAVN
I sertifikatet for sertifikatsigneringsnøkkelen til en utsteder av BankID skal feltet "subject" inneholde informasjon av typen "Distinguished Name" - (DN).

Attributt	Viktighet	Krav til innhold
Country (C)	Oblig	Land hvor utsteder av BankID er registrert.
Organisation (O)	Oblig	Skal inneholde offisielt registrert navn på organisasjon som eier utstedersystem (bank eller fellesutsteder)
Organisational Unit (OU)	Oblig	Skal inneholde unikt nummer fra Enhetsregisteret som identifiserer organisasjon (juridisk person)som eier utstedersystem(bank eller fellesutsteder).
Common Name (CN)	Oblig	Skal inneholde teksten "BankID " ,alminnelig brukt navn på CA, teksten "bank", og valgfritt en ekstra alfanumerisk verdi for å identifisere den enkelte CA hvis utsteder har flere.

Samme "Distinguished Name" skal også finnes som navn på sertifikatholder(subject) i utsteders nivå-1 sertifikat.

Flere regler for navnene i BankID Sertifikater fremgår av BankID External Certificates [8].

3.1.2 Meningsinnhold av navn

Bruk av pseudonymer er ikke tillatt i BrukerstedsBankID.

Unik identifikator i sertifikatholders serialNumber er vanligvis virksomhetens organisasjonsnummer i Enhetsregisteret eller tilsvarende register av virksomheter i annet EØS-land. Formatet på serialNumber skal være:

- LL-NNNNNNN ,der LL er ISO-3166 landkode og NNNNNNN er nummeret i det respektive nasjonale register. Landkode er ikke nødvendigvis i bruk for alle norske virksomheter.

- Eller
  - DUNS-MMMMMMM der MMMMMMM er et globalt unikt nummer tilordnet av Dun&Bradstreet

Norske tegn "æ, ø, å" kan brukes. Tegnrepresentasjon ellers skal følge norsk standard (ISO-8859-1).

3.1.3 Entydighet av navn

Attributtene som utgjør en sertifikatholders DN, skal entydig identifisere sertifikatholderen.

Organisasjonsnummer som definert ovenfor sikrer at virksomheter er entydig definert. Registreringsenhet er ansvarlig for å verifisere at organisasjonsnummer er korrekt og at virksomheten har rett til å benytte dette.

3.1.4 Bevis for eierskap til privat nøkkel

Virksomhetskunden genererer selv sine nøkler. For Filbasert BrukerstedsBankID skjer dette ved hjelp av programvare godkjent av BankID Samarbeidet. For HSM-basert BrukerstedsBankID skal nøklene genereres i virksomhetens HSM.

Når nøkkelpar er generert, må virksomhetskunden bevise eierskap og kontroll over den private nøkkelen. Dette gjøres ved å generere og sende en signert forespørsel til BankID CA. Hvis forespørselen kan verifiseres som korrekt, vil CA generere og publisere et sertifikat basert på den tilhørende offentlige nøkkel.

3.1.5 Utstedelse av BankID til virksomheter

3.1.5.1 Autentisering av virksomhet

Som en del av registreringsprosessen for BrukerstedsBankID skal det fremlegges en firmaattest fra Enhetsregisteret eller Foretaksregisteret i Norge, eller fra tilsvarende register i annet land innenfor EØS-området.

Virksomheter som er basert utenfor Norge, men som har et organisasjonsnummer fra Enhetsregisteret, kan registreres under dette nummeret.

Virksomheter som er basert utenfor Norge og som ikke har norsk organisasjonsnummer, kan registreres under et utenlandsk organisasjonsnummer dersom RA kan få en bekreftelse på virksomhetens identitet som gir samme nivå av tillit som en norsk firmaattest.

RA skal verifisere og arkivere kopi av identitetsdokumenter. Banken skal logge at det blir inngått avtale om utstedelse av BankID. Loggdata skal oppbevares i minimum 10 år, eller minst 5 år etter at kundeforholdet er opphørt.

3.1.5.2 Autentisering av virksomhetens representant

Banken i rollen RA skal verifisere identiteten av den personen som inngår avtale om BrukerstedsBankID på vegne av virksomheten

Personen må ha signaturrett i virksomheten og påtar seg formelt ansvaret for virksomhetens håndtering av sin BrukerstedsBankID.

Personen med signaturrett kan utnevne en annen person som har det tekniske og praktiske ansvar for virksomhetens BankID-programvare, nøkler og sertifikater. Herunder praktisk gjennomføring av registreringsprosedyrer samt være kontaktpunkt i forbindelse med

tilbaketrekking eller suspensjon av sertifikatet. Dette kan være en ansatt i virksomheten eller en ekstern person ansatt hos en tjenesteleverandør. Identiteten til denne personen skal også verifiseres av Banken. Det må finnes en fullmakt eller et hierarki av fullmakter fra person med signaturrett ned til personen som har det tekniske og praktiske ansvar for registrering og installasjon.

Banks behandling av registreringsdata og andre kundedata skal følge Personopplysnings-loven [9].

3.1.5.2.1 Nye kunder

Hvis virksomheten er ny kunde i banken, må en representant med signaturrett for virksomheten fysisk møte opp og fremlegge et legitimasjonsdokument som banken finner tilfredsstillende. Alternativt kan personen med signaturrett benytte en elektronisk tjeneste og autentiseres med sin BankID (PersonBankID eller AnsattBankID).

Banken er forpliktet til å beholde i sikker forvaring en kopi av fremlagte legitimasjons-dokumenter. Bankens plikt til å oppta legitimasjon av sine kunder er regulert av lover og forskrifter om hvitvasking [3].

3.1.5.2.2 Eksisterende kunder

Virksomheter, som allerede har et kundeforhold til banken og der representant tidligere er blitt identifisert i henhold til forrige punkt, kan registrere som beskrevet i forrige punkt, eller gjennom registreringsprosess som bygger på andre sikre prosedyrer.

Dette forutsetter at banken allerede har utført en fullverdig kontroll av personens identitet, og at personen kan aksessere registreringsenheten gjennom en tjeneste som bruker en godkjent autentiseringsmetode, ref: Kap 6 i Samlet kravdokument for sikkerhet i BankID [11].

3.1.6 Nye kunder med andre sertifikater

Det er for tiden ingen avtaler med andre utstedere om samtrafikk eller gjensidig godkjennelse av sertifikater. Det skal pr. i dag ikke utstedes BrukerstedsBankID basert på sertifikater fra andre utstedere.

3.1.7 Kontroll av personopplysninger

Personopplysninger, som f. eks. fødselsnummer og navn, skal bli sammenliknet (av registreringsenhet) med informasjon i et offisielt register, eller et annet tilgjengelig register som har høy datakvalitet og som banken har tillit til. Det må verifiseres at oppgitte opplysninger samsvarer med en eksisterende person oppført i registeret.

3.2 RUTINEMESSIG FORNYELSE

Rutinemessig fornyelse medfører også nøkkelskifte.

Før nøkler og sertifikater utløper, er virksomheten selv ansvarlig for å generere nye nøkler og få dem sertifisert.

Fornyelsesprosessen består av disse elementene:

- Generering av nye nøkler
- Sertifisering av ny offentlig nøkkel
- Bevis for besittelse av både ny og gammel nøkkel
- Henstilling til sertifikatholder om å slette alle spor av gammelt nøkkelpar når nye nøkler er installert i produksjonsmiljø.
- Utløp av sertifikatet for det gamle nøkkelparet.

Gyldighet og utløp av sertifikater beskrives i kapittel 4.7. Fornyelse initieres av sertifikatholder og kan utføres i løpet av en periode på 6 uker før sertifikatets utløpsdato. Ved fornyelse kan sluttbrukeren fortsette å ha de samme aktiveringsdata (passord).

Banken er ansvarlig for å varsle virksomheten senest 6 uker før sertifikat og nøkler utløper.

Hvis sertifikatholder ikke fornyer sertifikatet før utløpsdatoen, må samme prosedyre som for fornyelse etter tilbakekalling følges.

3.3 NYTT SERTIFIKAT ETTER TILBAKEKALLING

Etter tilbakekalling må virksomheten få et nytt sertifikat på samme måte som ved første gangs registrering. Prosedyrene i punktene 3.1.4 – 3.1.5 skal følges.

3.4 FORESPØRSEL OM TILBAKEKALLING

Utsteder av BankID skal støtte tilbakekalling og suspendering. (se kap. 4.4.)

4 OPERASJONELLE KRAV

Dette kapitlet beskriver overordnede operasjonelle krav til utstedere av BankID, registrerings-enheter og virksomheter /sertifikatholdere.

4.1 SØKNAD OM SERTIFIKAT

Identifisering av personer skal utføres som beskrevet i kapittel 3.

Registreringsenhet skal innhente alle opplysninger om virksomheten og dens representanter som er nødvendig for å utstede BankID.

4.2 UTSTEDELSE AV SERTIFIKAT

BankID utstedes basert på en bestilling som virksomhetskunden aktivt har deltatt i. BrukerstedsBankID forutsetter at virksomheten har forberedt sitt system og utført nødvendige tester. Når BankID er blitt utstedt, innebærer dette at banken har godkjent bestillingen.

Som en del av prosessen for å ta i bruk BankID skal virksomhetskunden motta en delt hemmelighet bare kjent av banken og kunden. Virksomhetskunden bruker denne delte hemmeligheten til å autentisere seg under utstedelse av BankID.

4.2.1 Forberedelser

Kommunikasjon mellom registreringsenhet og utsteder skal være sikret mot uønsket innsyn og manipulasjon med metoder beskrevet i CPS. Forespørsler om å få utstedt sertifikat skal være sporbar ned til den individuelle RA-operatør.

Virksomhetskunde skal motta:

- en kopi av avtalen bank-sertifikatholder [4]
- veiledning om prosedyrer for installasjon og initialisering av nøkler og sertifikater, inkludert nøkkelgenerering, samt veiledning om bruk
- en delt hemmelighet som er nødvendig for sikker utstedelse og aktivering av sertifikat
- programvare for nøkkelgenerering, innsending av sertifikatforespørsel og bruk av BrukerstedsBankID.

Rot-CA sertifikat skal være tilgjengelig fra flere tiltrodde kilder (for eksempel via autorisert programvare som distribueres).

Virksomheten må til enhver tid påse at delt hemmelighet, aktiveringsdata og private nøkler ikke kommer på avveie.

4.2.2 Nøkkelgenerering

4.2.2.1 Filbasert BrukerstedsBankID

For Filbasert BrukerstedsBankID skal virksomheten selv generere nøkkelpar ved hjelp av programvare som er levert av banken og godkjent av utsteder. Denne programvaren skal også lage en sertifikatforespørsel til CA.

Programvaren skal lagre nøkler i en logisk adskilt og sikret dataenhet, nøkkelfilen. Valg og initialisering av passord som beskytter nøkkelfilen skal være en del av nøkkelgenereringsprosessen.

4.2.2.2 HSM-basert BrukerstedsBankID

For HSM-basert BrukerstedsBankID skal nøkkelpar genereres i virksomhetens HSM. Det skal benyttes en HSM som er utprøvet og benytter kjente grensesnitt. BankID programvare lager, ved hjelp av virksomhetens HSM, en sertifikatforespørsel til CA.

Virksomheten skal lagre private nøkler i HSM, som er en særskilt sikret fysisk modul. Valg og initialisering av passord som logisk beskytter tilgang til nøklene skal være en del av nøkkelgenereringsprosessen.

En HSM for BrukerstedsBankID må tilby fysisk sikring av den private nøkkelen samt kunne utføre de nødvendige kryptografiske operasjoner som involverer den private nøkkelen. Det stilles ingen generell krav verken til de operasjonelle omgivelser der HSM opererer eller til formell evaluering av dens funksjoner.

4.2.3 Produksjon av sertifikater

Utstedersystem skal bruke informasjon fra registreringsenheten og fra sertifikatforespørselen til å lage BankID sertifikater.

Hvis det på noe stadium av sertifikatproduksjonen forekommer problemer, skal utsteder av BankID trekke tilbake alle sertifikater som kan ha blitt berørt av avviket i produksjons-prosessen og starte sertifikatgenerering for disse sertifikatholderne på nytt igjen.

Utsteder av BankID skal bruke sin sertifikatsigneringsnøkkel for å signere BrukerstedsBankID sertifikater.

4.2.4 Distribusjon og utlevering

Prosedyrer for distribusjon og utlevering skal tilfredsstille følgende:

Bank eller registreringsenhet sender ut en delt hemmelighet til virksomheten. Personen som utfører registrering på vegne av virksomheten, skal anvende den delte hemmeligheten til autentisering før sertifisering kan finne sted.

Minst en del av den delte hemmeligheten skal utleveres til virksomhetskunden over en sikret og autentisert kanal.

Når sertifikatproduksjonen er fullført, sendes sertifikatet til sertifikatholderen. Hvis det oppstår feil under noen del av sertifikatgenereringen, skal CA trekke tilbake de sertifikatene som er berørt. I dette tilfelle må virksomheten bestille BrukerstedsBankID på nytt.

Bankens RA-funksjon skal når som helst kunne be om informasjon om et sertifikats status.

4.3 AKSEPT AV SERTIFIKATER

Utsteder skal gjøre informasjon om at sertifikat er blitt generert, tilgjengelig for brukersted.

Virksomheten har indirekte akseptert BankID og sertifikater når:

- Avtale er inngått enten elektronisk eller på papir,
- Sertifikatet er produsert, og virksomheten har begynt å bruke dette.

Virksomheten har dermed status som BankID sertifikatholder.

4.4 SPERRING AV SERTIFIKATER

For å sperre en BankID kan utstedere av BankID velge enten å tilbakekalle den permanent eller å suspendere den. En suspendert BankID kan gjenåpnes, dersom bank har full visshet om identiteten på rette innehaver og om at grunnlaget for sperringen er falt bort.

Det vil generelt stilles strengere krav til visshet og til dialogen med sertifikatholder for å tilbakekalle et sertifikat enn for å iverksette en tidsbegrenset suspendering.

Bank eller tjenesteleverandør skal logge og arkivere alle forespørsler om sperring, inkl. hvordan forespørselen ble mottatt og hvilken handling utsteder iverksatte.

Tjenesteleverandør for CA-system er forpliktet til skriftlig å informere en sertifikatholders bank umiddelbart etter at et sertifikat er blitt tilbakekalt eller suspendert. Banken må så gjøre informasjonen tilgjengelig for sin kunde.

Utsteder av BankID må gjøre korrekt og oppdatert informasjon tilgjengelig for sertifikat-kontrollører. Informasjon om sperrede sertifikater skal være tilgjengelig 24 timer pr. døgn, alle dager.

Tilbakekallingsinformasjon skal inneholde alle sperrede (tilbakekalte og suspenderte) sertifikater. Utløpte sertifikater kan bli fjernet fra påfølgende lister.

Utsteder av BankID skal lage en oppdatert tilbakekallingsliste minst en gang pr. time og umiddelbart gjøre denne tilgjengelig for sertifikatkontrollører. Innimellom tilbakekallingslistene skal utstedersystem sende sanntidsoppdateringer til sertifikatkontrollør.

4.4.1 Når skal det tilbakekalles

Sertifikater skal tilbakekalles når den private nøkkelen forbundet med sertifikatet er blitt kjent for andre eller mistenkes kompromittert, eller når informasjonen i sertifikatet ikke lenger er korrekt.

Eksempler på årsaker for tilbakekalling er:
- uautorisert eller mistenkt uautorisert tilgang til private nøkler,
- tapte nøkler,
- kompromittering eller tyveri av aktiveringsdata,
- kjent misbruk av et sertifikat,
- virksomheten har skiftet navn,
- virksomheten er ikke lenger berettiget til å ha sertifikatet,
- virksomheten går konkurs eller opphører,
- opphør av virksomhetens kundeforhold til banken.

4.4.2 Hvem kan be om tilbakekalling

Disse kan be om tilbakekalling:
- Navngitte ansatte eller andre representanter for virksomheten, som er gjort kjent for CA,
- Bank som har inngått avtale med kunden,
- Registreringsenhet,
- Utsteder av BankID.

Domstoler kan ved dom eller kjennelse beslutte å sperre et sertifikat. Utsteder av BankID må bidra til at dette blir iverksatt.

4.4.3 Prosedyrer for tilbakekalling

Sertifikatholder kan anmode om tilbakekalling på følgende måter:
- ved personlig oppmøte med legitimasjon hos registreringsenhet,
- ved en signert anmodning,

Bank eller registreringsenhet kan søke uavhengig bekreftelse før de iverksetter tilbakekalling. Tilbakekalling pr. usignerte elektroniske meldinger krever at sertifikatholder presenterer annen identifikasjon som er godkjent av banken. Banken skal verifisere forespørsel om sperring ved å kontakte ansvarlig person for brukerstedet. Hvis banken ikke lykkes i å få

bekreftelse, og det er grunn til å tro at forespørselen er berettiget, skal sertifikatet suspenderes inntil virksomheten har bekreftet eller avkreftet forespørselen.

Dersom en bank ikke er i stand til å opprettholde sine forpliktelser overfor øvrige deltakere i BankID Samarbeidet, er det laget rutiner for å sperre alle sertifikater for banken og dens kunder. Dette gjelder også for banker som bruker fellesutsteder.

4.4.4 Ventetid

Informasjon om sperret sertifikat skal være tilgjengelig for sertifikatkontrollører senest 15 minutter etter at forespørselen ble registrert og akseptert. I enkelte situasjoner med driftsavvik (se kap 4.4.7) kan det tillates at sperreinformasjon ikke blir oppdatert over en noe lengre periode.

4.4.5 Suspendering

Utsteder av BankID skal støtte suspendering (tidsbegrenset sperring).

Alle betingelser som er tilstrekkelige for tilbakekalling, er også tilstrekkelige for suspendering. I tillegg godtas melding over telefon til bank eller registreringsenhet, eller via usignert anmodning. Bank kan også velge å tilby sine sertifikatholdere mulighet til å suspendere sin BankID gjennom selvbetjente løsninger.

Suspendering kan bli iverksatt når sertifikatholder ber om å bli sperret, og ikke kan identifisere seg på en måte som anses betryggende nok for å tilbakekalle. Bank kan også velge å suspendere BankID når en annen person enn oppgitt ansvarlig kontaktperson ringer inn på vegne av sertifikatholder, og vedkommende ka begrunne hvorfor suspensjon skal foretas. Bank skal alltid forvisse seg om melders identitet i samsvar med bankens rutiner.

Krav til melding til sertifikatholder etc. er identiske for suspendering som for tilbakekalling.

4.4.6 Begrensninger for suspensjonsperiode og gjenåpning

Maksimal suspensjonsperiode er 30 dager. Hvis sperringen ikke er opphevet innen det, blir den en permanent tilbakekalling. Ved oppheving av sperring (gjenåpning) må banken foreta sikker identifisering av sertifikatholder.

Gjenåpning av suspendert BankID kan bare skje hvis det er bevist innenfor suspensjons-perioden at grunnlaget for sperringen er falt bort.

Alle forespørsler om gjenåpning av en suspendert BankID skal logges. Loggingen skal dokumentere hvordan identifisering av sertifikatholder har foregått.

4.4.7 Hyppighet for utstedelse av lister med sperreinformasjon (CRL)

Utsteder av BankID skal i regelen utgi en oppdatert liste med sperreinformasjon (CRL) minst en gang pr. time og umiddelbart gjøre denne tilgjengelig for sertifikatkontrollører. I en situasjon med driftsavvik kan det tillates å ha en ekstra ventetid for overføring av sperrelister, slik at sperrelister kan være opptil 25 timer gamle. Det skal dokumenteres når en slik avvikssituasjon oppstår, og når den ender. Etter avsluttet avvik skal man umiddelbart tilbake tilnormal drift med sperrelister som blir tilgjengeliggjort .

Hver CRL skal oppgi tidspunkt for neste planlagte CRL-utstedelse.

En ny CRL kan bli produsert tidligere enn oppgitt tid for neste planlagte CRL-utstedelse.

Meldinger for sanntidsoppdateringer fra utsteder til sertifikatkontrollør kommer i tillegg (se 4.4.9).

4.4.8 Krav til kontroll av sertifikatstatus

Sertifikatmottaker har ansvar for sertifikatkontroll, inklusive kontroll av om sertifikatet er sperret.

4.4.9 On-line sertifikatkontroll

Det skal brukes on-line kontroll av sertifikatstatus der svar hentes fra en tiltrodd sertifikatkontrollør.

Innimellom de periodiske oversendelser av lister med sperreinformasjon skal utstedersystem sende sanntidsoppdateringer til sertifikatkontrollør. Listene med tillegg av sanntidsoppdateringer er grunnlagsinformasjon for on-line sertifikatkontroll.

Sertifikatkontrollør må ha tilgang til oppdatert sertifikatstatus for å godkjenne bruk av sertifikat. Andre sertifikatholdere eller sertifikatmottakere kan ikke forvente å få direkte adgang til lister med sperreinformasjon. Alle sertifikatholdere og sertifikatmottakere av BankID vil ha adgang til sertifikatkontrolltjenesten for å spørre om status på et sertifikat (validering).

Sertifikatkontrolltjenesten kan ha tilgang på tilleggsinformasjon om sertifikatholder og vil bare gjøre slike tilleggsdata tilgjengelig for sertifikatmottakere som har et legitimt behov, og har inngått avtale om dette.

Det skal brukes en kommunikasjonsprotokoll som sikrer at integriteten og ektheten i svar fra sertifikatkontrollør blir ivaretatt.

4.5 SIKKERHETSLOGG OG REVISJON

Prosedyrene her gjelder for alle maskiner som er involvert i utstedelse av sertifikater og CRL.

Sikkerhetsloggen er et verktøy for å dokumentere og gjenfinne informasjon om sikkerhets-relevante hendelser i BankID. Sikkerhetsloggen kan forstås som et distribuert sett av data lokalisert hos RA, utstedersystemer og sentrale lagringsenheter.

Sikkerhetsloggen brukes for å opprettholde et sikkert produksjonsmiljø.

Loggene skal lagres sikkert og kunne gjøres tilgjengelige for konsultasjon på rimelig tid.

4.5.1 Hendelser som logges

Sikkerhetsloggen skal skrive ned relevante hendelser:

- Hendelser på CA-systemet hos utsteder av BankID
- Hendelser på registreringsenhet
- Hendelser i drift av CA-system hos utsteder av BankID og registreringsenhet
- Hendelser i sentrale lagringsenheter.

4.5.2 Gjennomgang av sikkerhetslogg

Loggene skal opprettes i sanntid og kan når som helst bli inspisert av en operatør som har tilstrekkelige tilgangsrettigheter. For CA-systemet og sentrale servere i den operasjonelle infrastruktur skal det enten være en kontinuerlig maskinell overvåking som varsler om sikkerhetssensitive hendelser og spor etter fiendtlig oppførsel, eller en gjennomgang av en operatør med tilstrekkelig rettigheter, minst en gang daglig. For RA-systemene skal det finnes rutiner for maskinell gjennomgang som skal gjenkjenne nærmere spesifiserte negative hendelser og trender.

4.5.3 Lagring av sikkerhetslogg

Viktige hendelser i drift av utstedersystemene skal lagres i 10 år.

Logging av bruk av BankID sertifikater skal lagres i 10 år.

Øvrige elementer i sikkerhetsloggen vil bli lagret i en periode mellom 3 måneder og 10 år avhengig av en vurdering av behov og risiko.

4.5.4 Beskyttelse av sikkerhetslogg

Sikkerhetslogger skal ha integritetsbeskyttelse. Alle poster skal ha en individuell tidsangivelse.

Bare klarert personell hos bank, registreringsenhet eller tjenesteleverandør skal ha adgang til loggene.

4.5.5 Sikkerhetskopi (backup) av sikkerhetslogg

Sikkerhetskopi skal lagres i en separat lokasjon og omfattes av samme sikkerhetskrav som originalen.

4.6 ARKIV

4.6.1 Poster i arkivet

Denne seksjonen stiller krav til arkivering av informasjon som anses mindre relevant for oppfølging av sikkerhetsproblemer enn sikkerhetsloggen.

Eksempler på informasjon som skal lagres i poster i arkivet:

- Registrering av nye sertifikatholdere
- Forespørsler om å få utstedt sertifikater
- Utstedte sertifikater
- Avtaler om sertifikater og beskyttelse av nøkler og aktiveringsdata
- Fornyelse av sertifikater med tilhørende meldinger
- Historikk om nøkkelskifter på utstedersystem
- Forespørsel om sperring (tilbakekalling eller suspendering) med tilhørende meldinger
- Historisk sperre- og tilbakekallingsinformasjon
- Nåværende og utgåtte policyer og CPSer.

4.6.2 Lagring av arkivdata

Arkivdata skal lagres i 10 år.

4.6.3 Beskyttelse av arkivdata

Bare klarert personell hos bank, registreringsenhet eller tjenesteleverandør skal ha tillatelse til å lese arkivdata.

Arkivdata skal ha integritetsbeskyttelse mot uønsket endring eller sletting.

4.6.4 Sikkerhetskopi av arkivdata

Arkivdata skal skrives til ikke-flyktige media.

Arkivert elektronisk informasjon skal finnes i to kopier, på to forskjellige steder.

4.6.5 Tilgang til arkivdata

Bank, utsteder og tjenesteleverandør skal oppfylle konfidensialitetskrav i kap. 2.8; herunder Personopplysningsloven [9].

Bank har også ansvar for å sikre at arkivdata er tilgjengelig i maskinlesbar form gjennom hele arkiveringsperioden, også om utsteder av BankIDs operasjon blir avbrutt, suspendert eller avsluttet.

Hvis bank, utsteder og tjenesteleverandør avbryter, suspenderer eller avslutter sin virksomhet, skal bank bekjentgjøre at arkivet fortsatt er tilgjengelig. Forespørsler om informasjon skal rettes til bank eller til den organisasjon banken har utpekt til å ta i mot slike forespørsler.

4.7 NØKKELSKIFTE

Nye nøkler for rot-CA og andre CA'er skal genereres i god tid før utløp, slik at sertifikater på nivået under alltid skal være signert med en gyldig nøkkel. Det er utarbeidet rutiner for utstedelse av nye sertifikater.

Rot-CAs nøkler er gyldige i 26 år. Nye nøkler blir generert hvert 14. år.
Nivå 1 nøkler er gyldige i 12 år. Nye nøkler blir generert hvert 8. år.
Nøkler for BankID brukersteder er gyldige i 4 år og må fornyes hvert 4. år.

4.8 KOMPROMITTERING OG KATASTROFEBEREDSKAP

Bank må ha en skriftlig instruks med tiltak som må iverksettes av og overfor sikkerhets-ansvarlige hos utsteder og registreringsenhet, sertifikatholdere og sertifikatmottakere ved en potensiell katastrofe. (f. eks. hvis utsteders private nøkkel er kompromittert).

Bank som er rammet, må, som minimum:

- Offentliggjøre en erklæring om hendelsen som kan leses av sertifikatholdere, sertifikatmottakere og andre utstedere av BankID.

Ved kompromittering av utsteders private nøkler må utsteder av BankID:

- Sørge for at sertifikater utstedt under den kompromitterte nøkkelen ikke blir akseptert. Dette kan gjøres ved at sertifikatkontrollører alltid svarer negativt om disse.
- Forberede utstedelse av nye sertifikater for de som er rammet.
- Melde sertifikat knyttet til den private nøkkelen for tilbakekalling.

4.8.1 Katastrofeberedskap

Utsteder av BankID må også ha instrukser som beskriver hvilke betingelser som skal gjelde for fortsatt drift i en situasjon med større feil eller katastrofer. Utsteder må forsikre seg om at tjenesteleverandører har løsninger som oppfyller disse kravene.

4.9 OPPHØR AV UTSTEDER AV BANKID

Med opphør av utsteder menes en situasjon hvor alle logiske funksjoner knyttet til utstedelse av BankID opphører permanent. Et nøkkelskifte er ikke et opphør.

Betingelsene under gjelder når utsteder av BankID opphører kontrollert og har tid til å varsle forbindelser om hva som vil skje. Betingelsene er ikke anvendbare i nødsituasjoner.

Før en utsteder av BankID opphører med sine tjenester, skal den:

- Informere eier av overordnet CA (i praksis BankID rot-CA) om sine planer, med minst 6 måneders varsel.
- Informere bankens kunder (sertifikatholdere, sertifikatmottakere, virksomheter) og andre utstedere av BankID, med minst 6 måneders varsel.

- Offentliggjøre informasjon om sine planer, med minst 3 måneders varsel.
- Sikre at alle relevante databaser, arkiver og dokumenter blir tatt vare på i henhold til dette dokumentet, policy og CPS.

Banknæringen har utarbeidet prosedyrer som skal følges opp dersom en deltakende bank eller registreringsenhet blir satt under administrasjon.

4.9.1 Endring av forhold mellom bank og fellesutsteder

Hvis en bank ønsker å avslutte sitt forhold til en fellesutsteder, og vil begynne å utstede på et annet utstedersystem, vil de gamle sertifikatene forbli gyldige frem til utløpsdato hvis de ikke trekkes tilbake.

Et forhold mellom bank og fellesutsteder er derfor ikke avsluttet før alle sertifikater er utløpt eller trukket tilbake. Partenes ansvar er i denne perioden som i en ordinær driftssituasjon

5 SIKKERHETSKONTROLLER

Dette kapitlet beskriver praktiske sikkerhetskontroller for sikker drift av utstedersystem hos utsteder av BankID og registreringsenhet.

Dette dokumentet gir bare overordnet informasjon. Mer informasjon finnes i CPS. De mest sikkerhetskritiske detaljer står bare i graderte dokumenter hos banker og tjenesteleverandør.

Bits skal godkjenne implementering av sikkerhet hos utsteder og tjenesteleverandør.

5.1 FYSISKE SIKKERHETSKONTROLLER

Fysiske sikkerhetskontroller skal implementeres for å kontrollere tilgang til utstedersystemets maskinvare og programvare. Dette omfatter maskinen der selve utstedelsen av BankID foregår og alle eksterne sikkerhetsmoduler og media. All fysisk aksess til produksjonsmiljøet skal logges.

Nøklene for å signere sertifikater og tilbakekallingslister skal holdes fysisk beskyttet.

Klarert personell skal inspisere det sentrale produksjonsmiljøet minst ukentlig. Resultatet av inspeksjonene skal logges.

5.1.1 Produksjonsmiljø

Maskinvare for sertifikatutstedelse skal bli driftet fra et sikret miljø.

Maskinvare som produserer eller oppbevarer konfidensielle data, skal bli driftet fra et sikret miljø.

Sikret miljø skal være fysisk atskilt fra omkringliggende miljøer. Det skal finnes kontroller for å overvåke adkomst og adgang til sikret miljø.

5.1.2 Fysisk tilgang

Det skal foretas kontinuerlig adgangskontroll til det sikre driftsmiljøet. Det må alltid benyttes mer enn en mekanisme for autentisering for å bli gitt tilgang til utstedersystemet eller til maskiner som oppbevarer konfidensielle data tilknyttet sertifikattjenesten.

Produksjonsmiljøet skal inndeles i ulike sikkerhetssoner. For hver sone skal det defineres hvilke roller av personell som har tilgang. Tilgang skal kun gis definerte roller.

Operasjon av system som utsteder BankID og befinner seg i sikret miljø, krever at personell fra minst to roller er til stede (se kap.5.2). Adgangskontrollsystemet må kunne gjenkjenne personene og rollene, og det skal alltid benyttes mer enn en mekanisme for autentisering for å bli gitt tilgang til utstedersystemet eller til maskiner som oppbevarer konfidensielle data tilknyttet sertifikattjenesten.

For både sikret miljø og for det kontrollerte driftsmiljøet på utsiden av dette skal det foretas kontinuerlig adgangskontroll.

Tilgang til driftsalarmer krever autorisasjon og korrekt autentisering fra et forhåndsgodkjent maskinmiljø.

Prosedyrene for adgangskontroll skal identifisere personell som er autorisert til å komme inn i sikkert miljø og kontrollert driftsmiljø.

Effekten av den fysiske adgangskontrollen skal bli testet ut og verifisert periodisk.

Bankene må gjennom sine CPSer vise at det er gjort tiltak for å forhindre og / eller skadebegrense feil ved:

- strømbrudd og klimaanlegg,
- vannskader,
- brann
- fysisk beskyttelse av lagringsmedia.

Alle lagringsmedia som inneholder sensitiv informasjon, skal bli betryggende makulert før de blir kastet.

5.1.3 Plassering av sikkerhetskopi

Utsteder av BankID må ha et sted å lagre sikkerhetskopi og datamedia slik at det ikke vil forekomme tap av data eller manipulering og uautorisert bruk av lagret informasjon. Valg av lagringssted skal sikre at data ikke går tapt gjennom hendelser med feil på normalt driftssted.

Fysisk sikring for sikkerhetskopier skal være på samme nivå som andre miljøer med sikkerhetskopier for verdifulle banktransaksjoner.

De samme krav for kryptering av data gjelder for data til sikkerhetskopi som for andre produksjonsdata. Datatrafikk mellom lokasjonene skal gå over et sikret og lukket nett.

5.1.4 Sikkerhet for registreringsenhet

Sikkerhet for registreringsenhet (RA) skal følge bestemmelser i kravdokument utgitt av Bits. Bank har ansvar for at sikkerhetskravene blir fulgt. Bits kan kreve innsyn i de sikkerhetstiltak som er implementert.

5.2 ORGANISATORISKE KONTROLLER

Utsteder av BankID bærer det fulle ansvar for all behandling av data og maskinvare for utstedelse av sertifikater og tilbakekallingslister, uansett om enkelte oppgaver utføres av andre tjenesteleverandører.

Adgangskontrollprosedyrer, mekanismer og lister må bli gjennomgått (dvs. verifiseres og oppdateres) periodisk.

5.2.1 Tiltrodde roller

En rolle defineres her som retten til å utføre spesifikke oppgaver. Følgende tiltrodde roller er definert for drift av komponenter hos utsteder av BankID og registreringsenhet:

a) Operatør – Tjenesteleverandørs nøkkelholder
b) Tilsynshavende (supervisor)
c) Nøkkelholder hos utsteder av BankID
d) Logg- og revisjonsansvarlig

5.2.2 Antall personer pr. oppgave

Minst to personer i to roller må være med for å få fysisk tilgang til driftsmiljøet og utføre oppgaver på utstedersystemer. For å få tilgang til utstedersystem må disse være gjennom flere nivåer med autentisering, både gjennom noe de vet og noe de har. Minst to individer skal være utpekt til hver rolle.

Nøkkelgenerering og initialisering av sikrede lagringsmedia for utstedersystemet skal kreve at minst tre personer er til stede, i rollene a), b) og c) over. Etter første gangs nøkkelgenerering vil personen i rolle c) være utstyrt med et spesielt sikkerhetskort som må leses inn i en sikkerhetsmodul. Dette gjør det enkelt å skille sikkerhetssensitive oppgaver som involverer nøkkelholder, fra normal drift av utstedersystemet.

Hvis nøkler skal skrives ut for splittet lagring, må det være en nøkkelholder til stede for hver del nøkkelen splittes opp i.

Når media eller komponenter som kan inneholde hemmelige nøkler, skal avhendes, må minst to tiltrodde personer være til stede for å forvisse seg om at makulasjonen er forskriftsmessig.

5.3 PERSONELLMESSIG SIKKERHET

5.3.1 Kvalifikasjoner, erfaring og klarering

Personell som arbeider med utstedelse av BankID, må ha kunnskap, erfaring og kvalifikasjoner til å utføre sin rolle. Ansatte får ikke ha andre oppgaver som kan stå i konflikt med pålegg og ansvar som følger av roller de har i forbindelse med utstedelse av BankID.

5.3.2 Bakgrunnssjekk

Personell kan bli gjenstand for bakgrunnssjekk av rulleblad, i den grad dette er i samsvar med norsk lov.

5.3.3 Opplæring

Opplæring av personell vil foregå i et dedikert testmiljø.

5.3.4 Sanksjoner for brudd på instruks

Alt personell skal stå ansvarlige for sine handlinger. En funksjonær som begår alvorlige brudd på policy, CPS og instrukser, enten dette er uaktsomt eller med forsett, skal:

a) få sine rettigheter inndratt
b) være gjenstand for interne disiplinforføyninger
c) eventuelt, bli anmeldt for strafferettslig forfølgelse

5.3.5 Kontraktspersonell

Kontraktspersonell som skal utføre tiltrodde roller og oppgaver, skal ha vært ansatt av sin nåværende arbeidsgiver i minst 6 måneder. Kontraktspersonell kan bli gjenstand for de samme sanksjoner som ansatte ved brudd på instrukser.

5.3.6 Utlevering av dokumentasjon

Personell skal signere en relevant taushetserklæring før de får utlevert gradert dokumentasjon.

Det finnes ytterligere regler i CPS for hvilken dokumentasjon som kan tas ut av sikrede miljøer, og hvordan dette kan gjøres.

6 TEKNISKE SIKKERHETSKONTROLLER

Dette kapitlet gir en oversikt over regler for nøkkelhåndtering og tilhørende tekniske sikkerhetskontroller. Det beskrives overordnet hvordan generering og håndtering av nøkler foregår for utstedere av BankID og for virksomhetskunder.

6.1 NØKKELGENERERING OG INSTALLASJON

6.1.1 Generering av nøkkelpar

6.1.1.1 Generering av utsteders nøkkelpar

Utsteders nøkkelpar skal genereres i en sikkerhetsmodul (HSM). All bruk av private nøkler skal foregå inne i HSM.

Prosessen for å lage utsteders nøkkelpar skal involvere rollene beskrevet i kap. 5.2.2.

6.1.1.2 Generering av nøkkelpar for registreringsenhet

RAs nøkkelpar for sikker kommunikasjon med utsteder av BankID skal genereres av nivå-1 CA og distribueres sikkert til registreringsenheten.

6.1.1.3 Generering av nøkkelpar for virksomheten

For Filbasert BrukerstedsBankID:

Nøkkelgenerering gjøres av BankID programvare, som er distribuert kontrollert til virksomheten. Programvaren skal benytte en pseudo-random generator.

For HSM-basert BrukerstedsBankID:

Nøkkelpar skal genereres i en HSM.

6.1.2 Overlevering av privat nøkkel til virksomhet

Virksomheten genererer selv den private nøkkelen.

6.1.3 Innsendelse av offentlig nøkkel til utsteder av BankID

Offentlige nøkler skal sendes til utsteder av BankID i en signert sertifiseringsforespørsel.

6.1.4 Utlevering av utsteders offentlige nøkkel til sertifikatmottakere

Offentlig nøkkel for utsteder av BankID vil finnes i et sertifikat utstedt av BankID rot-CA (se kap.1.3.1). Hovedregelen er at utsteder av BankID er ansvarlig for å gjøre tilgjengelig et gyldig CA nivå 1-sertifikat, slik at dette kan brukes av autoriserte sertifikatkontrollører.

Rot-CA's sertifikat skal være tilgjengelig fra tiltrodde kilder. Dette gjøres initielt for nye sertifikatholdere, eller på forespørsel.

Offentlige nøkler for utstedere av BankID vil bli distribuert til parter med behov for nøklene. Det anses ikke nødvendig å dele disse nøklene ut til alle sertifikatmottakere, fordi sertifikatmottakere vil kommunisere med en sertifikatkontrollør for å verifisere gyldighet av sertifikatholderes sertifikater. Sertifikatmottakere vil derfor bare trenge den offentlige nøkkelen til sertifikatkontrolløren man bruker. Sertifikatkontrollør vil i sin tur være ansvarlig for korrekt og oppdatert tilgang til alle utstederes offentlige nøkler.

6.1.5 Nøkkellengder

Nøkkellengder vil bli løpende gjenstand for revurdering.

Nøkkellengden for rot-CA må være minimum 4096 bits for RSA.
Nøkkellengden for nivå-1-CA [utsteder av BankID] må være minimum 2048 bits for RSA.
Nøkkellengden for BrukerstedsBankID må være minimum 1024 bits for RSA.

6.1.6 Nøkkelbruk (som i X.509 v3 "keyUsage" feltet)

BankID har forskjellige nøkkelpar for autentisering, signering og kryptering. For BankID utstedt under denne versjonen av sertifikatpolicy er nøkkelparet for kryptering ikke tatt i bruk.

6.2 BESKYTTELSE AV PRIVATE NØKLER

Utsteders private nøkler skal alltid lagres i en HSM og aldri forlate denne i klartekst.

BrukerstedsBankID lagres slik:

Filbasert BrukerstedsBankID:
Nøklene kan lagres i programvare. Private nøkler skal ligge i en logisk adskilt og sikret dataenhet, nøkkelfilen. Nøkkelfilen skal være beskyttet av et passord med følgende egenskaper:

- Passordet skal velges av virksomhetens formelle eller tekniske representant, definert i kap 3.1.5
- Passordet skal bare kunne endres av personene nevnt i forrige punkt
- Passordet skal ha minst 7 tegn, hvorav ikke alle er bokstaver
- Passordet kan være meget langt

HSM-basert BrukerstedsBankID:
Nøklene lagres i en HSM og forlater aldri denne i klartekst. HSM må tilfredsstille krav stilt i kapittel 4.2.2.2 og 6.2.1 i dette dokumentet. Passord som brukes for å initiere HSM eller beskytte nøkler i HSM skal følge reglene over.

6.2.1 Standarder for krypto-moduler

HSM som brukes for å generere og lagre hemmelige og private nøkler i rot-CA og utstedersystem [nivå-1-CA], skal som minimum være i samsvar med FIPS 140-1 [2], nivå 3.

HSM skal ha fysisk sikkerhet med sensorer som oppdager forsøk på å manipulere eller klusse ved dem.

CPS skal gi mer informasjon om HSM og oppsummere resultatene av evalueringen.

HSM som brukes til HSM-basert BrukerstedsBankID skal ha fysisk sikkerhet med sensorer som oppdager forsøk på å manipulere eller klusse ved dem. Fysiske sikringstiltak i HSM skal være veldokumentert og kunne fremlegges for BSK.

6.2.2 Private nøkler (multi-person kontroll)

Enhver adgang til utsteders private nøkler krever to-personers kontroll. Dette betyr at ingen enkelt person alene har det som kreves for å få adgang til miljøet der privat nøkkel lagres.

For registreringsenheter og personer eller virksomheter som er sertifikatholder, tillates en-persons kontroll.

6.2.3 Sikkerhetskopi av private nøkler

6.2.3.1 Utsteder av BankIDs private nøkler

Det skal tas sikkerhetskopi av private nøkler for nivå-1-CAer. Alle utstedersystemer skal kunne gjenopprettes etter driftsproblemer. Dette omfatter også gjenoppretting av hemmelige nøkkelverdier i HSM. Nøkkelmateriale skal aldri eksporteres i klartekst, men under en nøkkelkrypteringsnøkkel (KEK).

Sikkerhetskopier av nøkkelmateriale skal deles opp i minst to komponenter som alene ikke gir noe informasjon om de hemmelige nøklene, og som fordeles på betrodde personer i forskjellige organisasjoner. Innlesing krever at begge organisasjonene er til stede.

Også KEK må splittes i to deler, hvor hver nøkkelholder har ansvar for sin ene nøkkeldel.

6.2.3.2 Sertifikatholders private nøkkel

Virksomheten kan lagre en beskyttet kopi av sine nøkler.

For Filbasert BrukerstedsBankID er nøkler lagret i en beskyttet fil. Det kan tas kopier av denne filen. Virksomheten er ansvarlig for betryggende lagring av filen og tilhørende passord.

For HSM-basert BrukerstedsBankID kan det benyttes HSM-funksjoner for nøkkel backup og eksport. Sikkerhet og kvalitet i disse funksjonene skal være dokumentert.

6.2.4 Arkivering av nøkler

Private nøkler for utstedere av BankID arkiveres ikke.

6.2.5 Innlegging av private nøkler i kryptomoduler

Private nøkler på utstedersystem blir generert inne i en kryptomodul (HSM). Hvis gjenopp-retting er nødvendig, kommer den inn som et kryptogram, kryptert under KEK.

For HSM-basert BrukerstedsBankID skal gjenoppretting alltid foregå ved at nøkkelen importeres i HSM som et kryptogram.

6.2.6 Aktivering av private nøkler

Privat nøkkel for utsteder av BankID er beskyttet mot innsyn og uautorisert bruk. Bare algoritmiske funksjoner inne i HSM kan få tilgang til denne nøkkelen.

For Filbasert BrukerstedsBankID:
Nøkkelfilen skal være beskyttet slik at tilgang til nøklene forutsetter kjennskap til korrekt passord. Ett og samme passord kan beskytte alle private nøkler i en nøkkelfil.

For HSM-basert BrukerstedsBankID:
Det er ingen krav til lukking eller deaktivering av nøkkellager. Nøkkellager kan være aktivt og tilgjengelig for legitim bruk så lenge det er en aktiv sesjon mellom HSM og den aktuelle applikasjonen.

6.2.7 Deaktivering av private nøkler

For å kunne aktivere private nøkler må korrekte aktiveringsdata ha blitt oppgitt.

6.2.8 Destruksjon av private nøkler.

For Filbasert BrukerstedsBankID:

Sertifikatholderen kan slette en nøkkelfil fra sitt driftsmiljø. Sletting av en nøkkelfil innebærer ikke sikker fysisk fjerning av nøklene. Ved rutinemessig fornyelse av nøkler og sertifikat bør sertifikatholder slette alle spor av gammelt nøkkelpar når nye nøkler er installert i produksjonsmiljø.

For HSM-basert BrukerstedsBankID:
HSM skal som et minimum kunne gjøre en nøkkel permanent utilgjengelig. Tilgang til denne operasjonen skal kreve autentisering.

6.3 ANDRE EGENSKAPER VED NØKKELHÅNDTERING

6.3.1 Arkivering av offentlige nøkler

Alle offentlige nøkler skal bli arkivert av utsteder i minimum 10 år etter utløp eller tilbakekalling.

6.3.2 Bruksperiode for offentlige og private nøkler

Et sertifikat kan bli brukt til å verifisere en signatur, også etter at sertifikatet er utløpt eller etter at sertifikatet er tilbakekalt, så sant det kan vises at signaturen ble laget før utløp eller tilbakekalling / suspendering.

Sertifikater og nøkler i BrukerstedsBankID er gyldige i fire år.

6.4 AKTIVERINGSDATA

Passord som beskytter bruken av private nøkler skal være i henhold til reglene i kapittel 6.2.

Aktiveringsdata skal oppgis hver gang det etableres en sesjon med nøkkellager.

6.4.1 Valg og initiering av aktiveringsdata

Virksomheten velger selv sitt faste passord innenfor gjeldende regler.

6.5 DATAMASKINSIKKERHET

Alle unødvendige funksjoner skal være avslått på utstedersystem og RAs datamaskiner. Sistnevnte omfatter både RA-systemet hos bank og maskiner som kommuniserer med disse hos tjenesteleverandør for utstedelse av BankID.

Det skal finnes autentisering, aksesskontroll og sporbarhet ned til individnivå på alle operasjoner og transaksjoner som påvirker bruk av nivå-1-CAs private nøkkel. Det skal skilles mellom rollene definert i kap. 5.2.1.

Maskinene som kjører sertifikatkontroll skal befinne seg innenfor brannmurer og være omfattet av adgangskontroll som krever to personer til stede for å utføre sensitive operasjoner på disse.

Alle produksjonsdata relatert til sertifikatutstedelse skal være lagret på lagringsenheter som er sikret mot feil eller tap av data.

6.6 TEKNISKE KONTROLLER FOR SYSTEMETS LIVSSYKLUS

6.6.1 Systemutvikling

Utvikling av programvare for utstedersystemer og registreringsenheter skal utføres i et kontrollert miljø som, sammen med minst en av underliggende betingelser, kan beskytte mot feil i programvare eller i versjonskontroll:

a) programvareleverandøren skal ha et kvalitetssystem i samsvar med internasjonale standarder; eller

b) programvareleverandøren skal ha et kvalitetssystem som er tilgjengelig for inspeksjon på forespørsel.

Det skal verifiseres at programvare som benyttes for utstedelse av BankID er ekte slik den ble levert fra leverandør.

6.6.2 Drift

Atskilte roller, som beskrevet i kap. 5.2, skal implementeres og håndheves av utsteder av BankID og tjenesteleverandør. Krav til beskyttelse av private nøkler beskrevet i kap 6.2, skal alltid være oppfylt.

Utsteder av BankID og deres tjenesteleverandører skal ha full kontroll over alle sine HSMer under alle faser av HSMs ”livssyklus”, og være sikker på at integriteten av enheten er ivaretatt fra frakt og lagring via initiering og bruk til kontrollert fjerning eller ødeleggelse av hemmelige nøkler når enheten tas ut av bruk.

Virksomheter skal påse at driftsmiljøet for deres BrukerstedsBankID og tilhørende programvare er forsvarlig sikret, både fysisk og logisk.

6.7 NETTVERKSSIKKERHET

Teksten under reflekterer bruk av TCP/IP. Hvis en annen nettverksprotokoll brukes, må et likeverdig sikkerhetsnivå implementeres, dokumenteres i CPS og godkjennes av Bits.

Vertsmaskiner som brukes til utstedelse av BankID, skal ikke være direkte tilgjengelige fra åpne nettverk. Mellom eksterne nettverk og lukket nett der utstedersystemet befinner seg, skal det beskyttes etter den til enhver tid rådende praksis for god beskyttelse av nettverksressurser. Utstedersystemet skal være beskyttet av minst to nivåer med brannmurer eller andre logiske adgangskontroller.

Innsending av data fra RA til utstedersystem skal gå over et lukket nett der bare kjente maskiner har adgang.

Rot-CA skal aldri kobles til noe kommunikasjonsnettverk av noe slag.

På maskiner som brukes til utstedelse av BankID skal alle kommunikasjonsporter som ikke eksplisitt trengs, være avstengt, og programprosesser som bruker disse portene, skal være slått av. Konfigurasjonen av maskinene skal bli gjennomgått jevnlig, og det skal foretas tester for å verifisere at det ikke finnes andre veier inn til CA-systemene.

7 SERTIFIKATER OG TILBAKEKALLINGSLISTER

Dette kapitlet er på ingen måte en spesifikasjon, men en helt overordnet forklaring av noen av de feltene som inngår i sertifikater og tilbakekallingslister som benyttes i BankID policyer. Teknisk informasjon om sertifikater og profiler står i intern dokumentasjon som blir distribuert på "need-to-know"-basis.

7.1 SERTIFIKATPROFIL

BankID sertifikater består av en kombinasjon av standard felter, standard utvidelser og private utvidelser. Tabellen under gir en overordnet forklaring av feltene i BrukerstedsBankID. For programmerere og andre som trenger detaljkjennskap til feltene og deres koding henvises til mer detaljert dokumentasjon [8].

Navn	Norsk betegnelse	Type	Verdi / kommentar
Version	Versjon	Std, Obl	**2**, indikerer at det brukes formatet X.509, versjon 3 [6].
CertificateSerial Number	Sertifikatets Serienummer	Std, Obl	Sertifikatets "løpenummer" fra utsteder
Signature Algorithm	Signatur-algoritme	Std, Obl	**sha1RSA** (identifikasjon av algoritmer brukt til å signere sertifikatinnholdet)
Issuer	Utsteder	Std, Obl	Navn på utsteder av BankID, for format se kap 3.1.
Validity	Gyldig fra	Std, Obl	Dato
	Gyldig til	Std, Obl	Dato
Subject	Sertifikatholder (emne)	Std, Obl	Navn på sertifikatholder, for format se kap 3.1.
SubjectPublic KeyInfo	Offentlig nøkkel (fellesnøkkel)	Std, Obl	Binær koding av sertifikatholders offentlige nøkkel, med parametre
certificatePolicies	Sertifikatpolicy (sertifikatkriterier)	SU, Obl	OID for den sertifikatpolicy som sertifikatet er utstedt i forhold til.
BankName	Bank navn	PU, Obl	Navn på den bank som har inngått avtale om BankID med sertifikatholder
BankRegNumber	Bank register nummer	PU, Obl	Fire-sifret nummer som identifiserer bank som har inngått avtale om BankID med sertifikatholder
Authority Information Access	Gyldighets-kontroll (Informasjons-tilgang for instans)	SU, Obl	URL-adresse som peker til sertifikat-kontrollørtjeneste som må konsulteres for å validere sertifikatstatus
AuthorityKey Identifier	Nøkkelversjon for utsteder (Nøkkelidentifi-kator for instans)	SU, Obl	Beregnet hash-verdi over utsteders offentlige nøkkel
SubjectKey Identifier	Nøkkelversjon for sert. holder (Nøkkelidenti-fikator for emne)	SU, Obl	Beregnet hash-verdi over sertifikat-holders offentlige nøkkel
KeyUsage	Bruk av nøkler	SU,Obl,Krit	Bruksbegrensning som må følges av programvare som bruker bankID nøkler og sertifikater. Tre forskjellige sertifikater med hver sin valgte bitmap er definert. **Non-repudiation**, eller **DigitalSignature/KeyAgreement**,

Navn	Norsk betegnelse	Type	Verdi / kommentar
SubjectAltName	AlternativtNavn	SU[1]	E-post adresse for sertifikatholder

Forklaring til type-kolonnen:
Std: Feltet er definert i X.509-standarden [6]
SU: Standard utvidelse – feltet er definert i en anerkjent referanse
PU: Privat utvidelse – feltet er definert for bruk i BankID sertifikater
Obl: Obligatorisk felt – må finnes i alle sertifikater i samsvar med denne sertifikatpolicy
Krit: Kritisk felt – må kontrolleres av all programvare som skal bruke sertifikatet.

BrukerstedsBankID kan inneholde to BankID-definerte utvidelser; *BankRegNumber* og *BankName* som identifiserer ansvarlig utsteder av BankID. Når sertifikatinnholdet listes ut av ”fremmed programvare”, fremstår disse som tekstfelter, pekt til av en OID-sekvens av heltall.

7.2 TILBAKEKALLINGSLISTER

Det skal brukes standardformat, X.509, versjon 2 av tilbakekallingslistene [6].

Tid for neste oppdatering skal alltid skrives til tilbakekallingslistene.

[1] Det er foreløpig ikke utstedt BankID-sertifikater som bruker dette feltet.

8 ADMINISTRASJON AV SPESIFIKASJONER

8.1 ADMINISTRASJON AV ENDRINGER

Banker, tjenesteleverandør og Bits kan ta initiativet til endringer i policy. Sertifikatholdere eller brukere kan foreslå endringer gjennom en bank som deltar i BankID Samarbeidet. Bits AS skal administrere endringer og ta endringsforslag opp i en arbeidsgruppe bestående av:

- Bits' administrasjon
- Banker (i egenskap av avtalepart for BankID og registreringsenhet)
- BankID Norge AS
- Nets Norge AS (i egenskap av tjenesteleverandør for rot-CA).

Bits har ansvaret for godkjenning av endringer. BankID Norge AS har kontrollansvar for nye versjoner.

Redaksjonelle eller typografiske endringer kan gjøres av Bits uten å varsle noen annen part.

Viktige endringer innenfor bruksområde, sertifikatinnhold, nøkkellagring, nøkkellengder og oppbevaring av nøkler, kan resultere i at det må lages en ny policy. Også større forandringer på andre områder kan føre til at det blir laget en ny policy.

Innenfor en policy kan alle endringer foretas med 90 dagers varsel.

Endringer som etter Bits' vurdering ikke vil ha betydelig innvirkning for en stor del av sertifikatholder og sertifikatmottakere, kan foretas med 30 dagers varsel.

Alle foreståtte endringer vil bli meddelt skriftlig til registrerte utstedere av BankID, og vil bli gitt en fremskutt plass på BankIDs internett-sider.

Alle andre endringer enn de redaksjonelle eller typografiske vil bli forankret gjennom en høringsprosess i bankene.

8.2 PUBLISERING OG VARSLING

Dette dokumentet og annen ugradert BankID-informasjon, kan skaffes fra:

- websiden http://www.bankid.no i elektronisk form,
- post@bits.no over elektronisk post
- Bits, ved å bruke kontaktinformasjonen i punkt 1.4.

Ved endringer i betingelser eller ansvarsfordeling i utstedelse og bruk av BankID, skal dette kunngjøres over http://www.bankid.no uten unødvendig opphold, og om nødvendig i en ny versjon av dette dokumentet.

Ved endringer i betingelsene mellom bank og kunde (sertifikatholder eller sertifikatmottaker), eller i anvendelsesområdet for BankID, skal dette kunngjøres av banken uten unødvendig opphold.

8.3 GODKJENNELSE AV CPS

Hver enkelt bank som skal inngå avtale om utstedelse av BankID, er ansvarlig for å utarbeide CPS i samarbeid med sin tjenesteleverandør. Banker som har stor tjenestemessig og systemmessig likhet, kan slutte seg til en tjenesteleverandørs felles CPS-dokument. CPS skal uttrykke samsvar med tiltakene i policy og dette dokumentet. Enhver CPS som er laget innenfor en BankID-policy skal godkjennes av Bits. Godkjenning er påkrevet når dokumentet er nytt og ved større endringer.

I tillegg til CPS vil det også finnes gradert dokumentasjon tilknyttet drift og operasjon av utstedersystemene. Disse dokumentene kan ikke påregnes distribuert til publikum.

NORSK-ENGELSK ORDLISTE

Ettersom mye dokumentasjon av BankID og PKI-systemer generelt er på engelsk, kan en slik ordliste være nyttig.

Norsk	Engelsk
aktivere	activate
autentisering	authentication
banklagret BankID	netcentric BankID
delt hemmelighet	shared secret
fornye	renew
gyldighetsperiode	validity
ikke-benekting	non-repudiation
installasjonskode	shared secret
integritet	integrity
lokallagret BankID	soft local BankID
personlig kode	PIN (activation data)
register over BankID	repository
registreringsenhet	registration authority (RA)
sertifikat	certificate
sertifikatholder	subscriber
sertifikatkontrollør	validation authority
sertifikatmottaker	relying party
sikkerhetskopi	backup
sperring	common term for suspension and revocation
suspendering	suspension
tilbakekalling	revocation
utstedelse	issuance
verifisering	verification