UGRADERT

Sertifikatpolicy for BankID på mobil - kvalifiserte sertifikater til fysiske personer, v 2.0

august 2016

BankID sertifikatpolicy
status: Godkjent
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: Denne versjonen inneholder ingen vesentlig tekniske og redaksjonelle endringer i forhold til tidligere godkjente versjoner. Endringene er behandlet i og godkjent av BSK Faggruppe BankID. Versjon 1.0: Godkjent av FU.
Distribusjon (bare for dokumenter med begrenset distribusjon): Dette dokumentet er ugradert og kan publiseres. Videre distribusjon er tillatt.
Vedlikeholdsprosedyre: Se kap 8.

Dokumenthistorie

Versjon	Dato	Endr.nr / kommentarer	Dokument-ansvarlig	Godkjennes av
2.0	110816		RHa	
		Fjernet eksempler med bruk av WAP Innført betegnelsen Bits AS		
1.5	210715		RHa	
		Synliggjort krav om 24/7 sperretjeneste. Innført BankID Norge AS som dokumenteier. Innført krav om kundeforhold i stedet for krav om konto. Justert definisjoner. Ny tekst om Folkeregister-kontroll i kap 3.1.2, tekst om kundeforhold i kap 1.3.		
1.4	040414		RHa	
		Redaksjonelle endringer i forhold til v 1.3.3.		
1.3.3	210813		RHa	
		Lagt inn tekst om Rutinemessig fornyelse uten brukermedvirkning i kap 3.2, Tillatt gyldighet av nøkler i inntil 5 år i kap 6.3.2		
1.3.2	301113		RHa	
		Lagt inn åpning i kap 4.4.4. og 4.4.7 for å kjøre med eldre sperreliste i definert unntakstilstand, Presisert ansvar for logging i kap 4.5.2. Innført "Finans Norge" som betegnelse		
1.3.1	240912		RHa	
		Presisert nedre aldersgrense i kap 1.3.4. Satt inn nye nivå-3 overskrifter i kap 2.2.1 og 4.8.1 for å få større grad av samsvar mellom dokumenter.		
1.3	280212		RHa	
		Ny logo. Rydding og ajourhold av referanser. Presisert FNO Servicekontor i beskrivelse av oppgaver Utvidet bruksområde i 1.3.5 . Byttet rekkefølge på seksjonene i kap 2.1 for å forenkle CPS-skriving. Lagt inn varslingsplikt i 2.8.4 Presisert tekst om driftsmiljø i kap 5.1.2, kap 6.5 og kap 6.7.		
1.2	100910		RHa	
		Tatt inn at fornyelse kan gjennomføres uten brukermedvirkning. Praktiske og redaksjonelle endringer vedtatt i BSK Faggruppe 8.9.10		
1.1	300610		RHa	
		Identisk med 1.09 b foruten noen mindre, redaksjonelle endringer.		
1.09.b	140610		RHa	
		Gjort endringer fordi FNO overtar oppgaver fra Sparebank-foreningens Servicekontor og Finansnæringens Servicekontor (Kvalitetssikret på dokument-QA med FNO og BBS)		
1.09	090610		RHa	
		En del mindre redaksjonelle endringer som tidligere er gjort i andre sertifikatpolicyer, bl. a. ikke-kvalifisert BankID på mobil		
1.01	060907		LiA	
		Lagt til krav til bankens RA-funksjon ved utstedelse av sertifikater		
0.92/ 1.0	230507		LiA	
		Godkjent av FU og gitt versjonsnummer 1.0		
0.91	080507		LiA	
		Endringer etter innspill fra DnBNOR		
0.9	260407		LiA	
		Endringer etter høring i bank.		
0.2	300107		LiA	
		Videre bearbeiding etter intern gjennomgang BSK		
0.1	050107		LiA	
		Første versjon av dokumentet (utgangspunkt er versjon 1.14 av policy for banklagret kvalifisert personsertifikat)		

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 Finans Norge Servicekontor kan utstede 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.

BankID på mobil: En BankID der den private nøkkelen er lagret på et SIM-kort og bare kan benyttes gjennom en definert Sikkerhetskanal

Banklagret BankID: BankID hvor private nøkler befinner seg i et sikret banksystem som beskytter nøklene slik at bare rettmessig innehaver kan bruke dem, når som helst fra hvilken som helst enhet tilknyttet Internett.

Engangskode: Hemmelig kode som banken utleverer på en sikker måte til sertifikatsøker og som sertifikatsøker oppgir i forbindelse med sertifikatutstedelse.

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).

IDPIN: Hemmelighet som sertifikatinnehaver velger og som beskytter BankID nøkler på SIM-kort mot uautorisert bruk.

Lagringsenhet: Sentralisert enhet som lagrer data og programvare for kontroll og dokumentasjon av BankID. I BankID på mobil inngår lagringsenhet i sikkerhetskanalen.

Lokallagret BankID: BankID hvor den private nøkkelen er lagret lokalt på sertifikatholders datamaskin. Nødvendig programvare for å bruke BankID lastes ned ved første gangs bruk og installeres fast på datamaskinen.

Mobilnummer: Telefonnummer til kundens mobiltelefon. Mobilnummeret er knyttet til det SIM-kortet som inneholder BankID nøklene.

Mobiloperatør: Operatør som tilbyr mobiltelefonitjenester. Mobiloperatør kan ha eget mobilnett eller helt eller delvis benytte andre operatørers infrastruktur. Mobiloperatøren utsteder SIM-kort til sine abonnenter.

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 person. Samme person 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.

Sertifikatsøker: Personkunde som søker om å få utstedt en BankID, men som ennå ikke er blitt sertifikatholder

Sikkerhetskanal: Infrastruktur som på en sikker måte a) kobler utsteder av BankID mot innehavers SIM-kort i forbindelse med utstedelse av BankID på mobil og b) kobler sertifikatmottager mot sertifikatholders SIM-kort ved bruk av BankID på mobil.

Sikkerhetskanalens kritiske komponenter: Enheter som har tilgang til autentiseringsdata eller andre hemmeligheter i klartekst, samt komponenter som utfører sikkerhetskontroller på vegne av sertifikatholder.

SIM: Subscriber Identification Module, bærer av kundens abonnementsforhold hos en mobiloperatør.

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 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.

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
RA	Registration Authority
RFC	Request for Comment
RSA	Rivest, Shamir, Adleman
SIM	Subscriber Identity Module
SMS	Short Message Service
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; 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 sertifikatholder om elektronisk BankID, basert på mønster til ”Avtalevilkår for PersonBankID” utarbeidet av Finans Norge 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]	ETSI TS 101 456	“Policy Requirements for Certification Authorities Issuing Qualified Certificates”, v1.4.3 (2007-05)
[12]	Bits Sikkerhetskravdokument	Bits / BSK: Samlet kravdokument for sikkerhet i BankID; versjon 2.8, mars 2015

1 INNLEDNING

1.1 OVERSIKT

Dette dokumentet beskriver sertifikatpolicy for BankID-sertifikater til fysiske personer (person-sertifikater). 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.

Dette dokumentet er skrevet for BankID på mobil, der private nøkler befinner seg sikret på et SIM-kort på kundens mobil, knyttet til et mobiltelefonabonnement hos en mobiloperatør.

BankID kan også støtte andre løsninger og andre typer nøkkelbærer (smartkort, lokallagret i filer på brukers datamaskin, banklagret etc.). Disse vil være beskrevet i andre sertifikatpolicyer.

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 ett nøkkelpar og ett sertifikat.

Når et utstedersystem lager et sertifikat, attesterer utsteder av BankID bindingen mellom den offentlige nøkkelen og sertifikatholderens identitet. 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 BankID sertifikater utstedt som kvalifiserte sertifikater til fysiske personer (PersonBankID), og der sluttbrukers private nøkler befinner seg på SIM-kortet i en mobiltelefon.

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 BankID på mobil personsertifikater, skal denne identifikatoren benyttes:
Object Identifier (OID):
{joint-iso-itu-t(2) country(16) norway(578) organisasjon(1)
bankenes-standardiseringskontor(16) policy(1) qualifiedCertificates(12) mobile(2) 1}

Denne sertifikatpolicy er kompatibel med policy QCP public i ETSI TS 101 456 [11]:
{itu-t(0) identified-organisations(4) etsi(0) qualified-certificate policies(1456)
policy-identifiers(1) qcp-public(2)}

1.3 BRUKSOMRÅDE OG AKTØRER

Dette dokumentet beskriver regler for bruk av sertifikater utstedt til fysiske personer. Personen vil som oftest ha et kontoforhold til utstedende bank, men regelverket tillater utstedelse av PersonBankID til personer 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 avtale om utstedelse av BankID.

En mobiloperatør kan inngå avtale med utstedere av BankID om å gjøre BankID på mobil tilgjengelig for sine abonnenter. Mobiloperatøren gjør da SIM-kortet tilgjengelig som nøkkellager for BankID nøkler.

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].

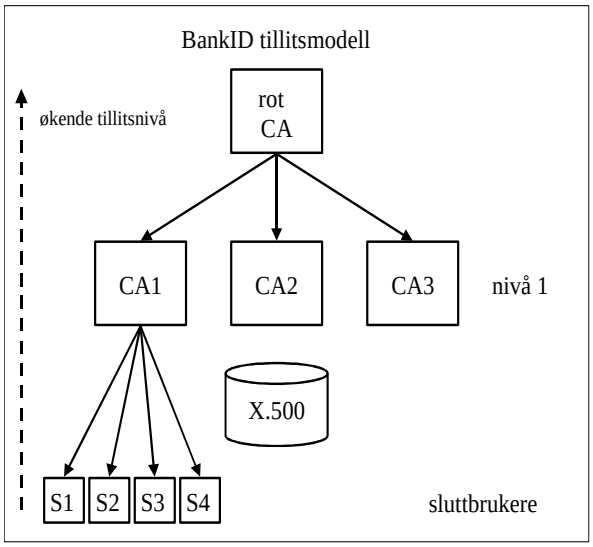
Rot-CA ble etablert av Finansnæringens Servicekontor (FNS) og Sparebankforeningens Servicekontor. Fra 1.1.2010 har Finans Norge Servicekontor overtatt servicekontorenes oppgaver, herunder oppgaven som rot-CA. Prosedyrer rundt drift av rot-CA system skal godkjennes av Bits AS (tidligere Bankenes Standardiseringskontor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

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

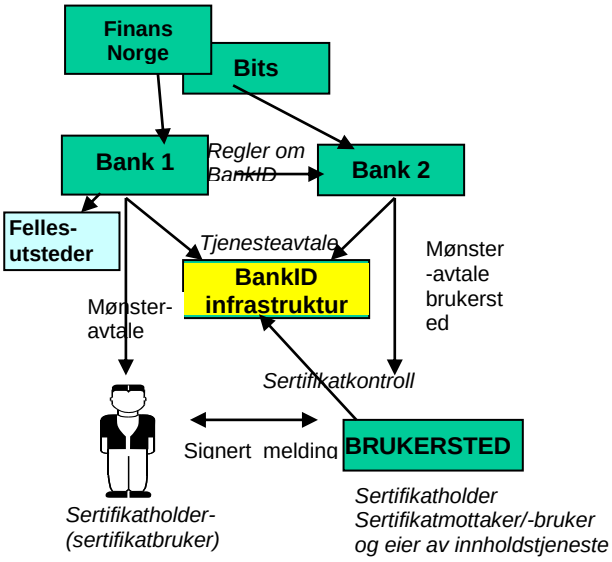
Bank som utsteder BankID, kan selv etablere et utstedersystem eller benytte en fellesutsteder til å forestå utstedelsen av sertifikater.

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 tillitmodell



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

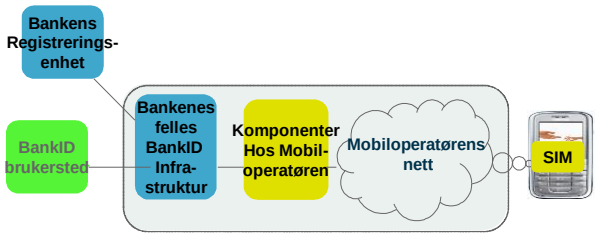
Banker kan selv være RA, eller la seg bistå av en tjenesteleverandør. Banken er uansett ansvarlig for tjenestene registreringsenheten utfører.

1.3.3 Mobiloperatør

Mobiloperatøren har ansvar for å tilby et nøkkellager på SIM-kortet, som er sikret i henhold til bankenes krav. I samarbeid med bank skal mobiloperatøren også tilby infrastruktur som er nødvendig for trygg og sikker utstedelse og bruk av BankID på mobil, heretter kalt Sikkerhetskanalen.

En mobiloperatør som inngår avtaler om BankID i samsvar med dette dokumentet skal:

a) operere sin del av Sikkerhetskanalen 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 omfatte mobiloperatørens løsninger og driftsmiljø for kritiske komponenter i Sikkerhetskanalen, samt SIM-kort og personalisering av disse.



Figur 3 Sikkerhetskanalen

Mobiloperatøren inngår i BankID avtalestruktur på denne måten:

Mobiloperatøren inngår rammeavtaler med Finans Norge om å tilby tjenesten BankID på mobil til sine abonnenter.

Mobiloperatøren inngår avtale med den enkelte mobilabonnent om å ta i bruk tjenesten BankID på mobil.

Mobiloperatøren inngår også avtaler med det enkelte BankID brukersted om bruk av tjenesten mot operatørens abonnenter.

1.3.4 Sertifikatholdere

I dette dokumentet [og tilhørende CPSer med underliggende dokumentasjon] er sertifikatholder en fysisk person, som har et mobilabonnement hos en mobiloperatør.

BankID kan ikke utstedes til personer under 15 år. I særlige tilfeller kan Finans Norge Servicekontor likevel tillate at BankID utstedes til personer under 15 år. Bank som utsteder BankID, kan velge å ha høyere aldersgrense.

En virksomhet som er BankID brukersted, kan være mottaker av en melding sikret med en BankID på mobil. I samhandling mellom en virksomhet og en privatperson må virksomheten forholde seg til en BankID policy for virksomheter. Dette dokumentet beskriver krav til virksomheter bare der dette er viktig for å forstå rettigheter, plikter og tillitsnivå for innehaver av BankID personsertifikat.

1.3.5 Anvendelighet

Sertifikater utstedt under denne sertifikatpolicy blir brukt mellom fysiske personer som er sertifikatinnehavere og brukersteder til å utføre de følgende sikkerhetstjenester:

- autentisering
- digital signering av kortere tekstmeldinger (opp til 120 tegn)

Sertifikater utstedt under denne sertifikatpolicy, kan bare brukes overfor BankID brukersteder. Brukerstedet kan for eksempel legge til rette for bruk knyttet til web-baserte tjenester eller til mobilbaserte tjenester (f. eks. SMS-baserte).

Også brukerstedet som sertifikatinnehaver kommuniserer med, må ha inngått avtale med sin bank om bruk av BankID. Brukerstedet må i tillegg ha inngått avtale med den mobiloperatøren hvor sertifikatinnehaver har sitt abonnement.

Sertifikatinnehaver må sammen med BankID benytte slik mobiltelefontype, abonnementstype eller det sikkerhetsutstyr som banken spesifiserer. Banken kan stille nye krav til mobiltelefontype, abonnement eller sikkerhetsutstyr der dette er nødvendig av sikkerhetsmessige grunner eller ved nødvendige oppgraderinger av BankID. Under utstedelse av BankID vil det bli gjort tekniske tester av telefon og abonnement. Dersom BankID blir aktivert eller brukt i et mobiltelefonmiljø som ikke oppfyller BankIDs sikkerhetskrav, kan dette medføre risiko for misbruk. Banker vil opplyse sine kunder om krav og råd for bruksmiljøet.

I tillegg til bruksområdene nevnt over kan sertifikatinnehavere av banklagret BankID benytte BankID på mobil som en av de to autentiseringsfaktorene for å få tilgang på sin private nøkkel. Det vil da bli foretatt en autentisering med BankID på mobil i stedet for bruk av annen engangspassordenhet. I dette tilfellet vil infrastrukturen for banklagret BankID fungere som sertifikatmottaker for BankID på mobil.

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 fra BankID Norge, og er ansvarlig for vedlikehold av 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.

2.1 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, 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.

En mobiloperatør som inngår avtale med BankID utstedere om å gjøre tilgjengelig BankID på mobil for sine abonnenter, har de plikter som følger nedenfor. Mobiloperatøren må levere skriftlig erklæring om at disse pliktene er forstått og akseptert.

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 periodisk vedlikeholde 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 sertifikatutsteders 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 sertifikatsøkere som beskrevet i kap. 3
- veilede og hjelpe personkunden i registreringsprosessen
- sammenstille og videresende til utsteder den informasjon om sertifikatsøkeren som er nødvendig for å kunne utstede BankID
- legge til rette for at det blir brukt eller tildelt et riktig entydighetsbegrep for å identifisere sertifikatholder
- innhente sertifikatsøkers mobilnummer
- ha mulighet til å initiere sperring av sertifikater
- 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

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 og bekrefte overfor banken at vilkårene aksepteres
- bruke nøkler og sertifikater bare i forbindelse med Sikkerhetskanalen og i samsvar med tiltenkt bruk
- beskytte IDPIN og forsikre seg om at denne holdes hemmelig
- informere banken om forhold av betydning for avtaleforholdet, herunder endringer i opplysninger gitt ved utstedelse
- rapportere på anvist måte til banken (eller dens tjenesteleverandør) ved enhver mistanke om at en privat nøkkel er blitt kjent for andre
- rapportere på anvist måte til banken eller mobiloperatøren hvis nøkkellager er tapt, stjålet, ødelagt eller kommet på avveie
- rapportere til banken ved enhver mistanke om at IDPIN kan ha blitt kjent for andre og følge bankens anvisninger
- umiddelbart slutte å bruke en BankID hvor den private nøkkelen eller IDPIN mistenkes å ha blitt kjent for andre

2.1.4 Plikter for sertifikatmottaker

Sertifikatmottaker kan være en bank eller en virksomhet.

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*)
- følge bankens retningslinjer for merking av transaksjoner, slik at den aktuelle Key Usage fremgår tydelig for sertifikatinnehaver.

2.1.5 Plikter for tjenesteleverandør

En tjenesteleverandør kan utføre hele eller deler av en banks eller en fellesutsteders funksjoner. Også komponenter i Sikkerhetskanalen kan være satt ut til tjenesteleverandører. Tjenesteleverandører 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.

Tjenesteleverandør skal:

- opprette og vedlikeholde hendelseslogger og arkiver i henhold til policy og CPS
- gjøre logger og arkiver tilgjengelige på grunnlag av gyldig og autorisert forespørsel.
- logge og arkivere historiske data om nøkkelbruk.

2.1.6 Plikter for mobiloperatør

Forholdet mellom mobiloperatør og bank er regulert i en egen avtale.

Mobiloperatøren skal:

- utstyre sine abonnenter med SIM-kort som tilfredsstiller krav til nøkkellager for BankID på mobil som beskrevet i kapittel 4 og 6
- informere kunden om særskilte betingelser knyttet til bruk av BankID på mobil
- tilby nødvendige komponenter i Sikkerhetskanalen i henhold til denne sertifikatpolicy
- sikre at private nøkler for BankID på mobil bare benyttes slik som angitt i denne sertifikatpolicy
- straks gi melding til banken hvis nøkkellager er tapt, kommet på avveie eller av andre grunner, for eksempel abonnementsmessige forhold, ikke lenger kan benyttes
- opprette og vedlikeholde hendelseslogger og arkiver i henhold til policy og CPS
- gjøre logger og arkiver tilgjengelige på grunnlag av gyldig og autorisert forespørsel fra bank
- tilby og inngå avtale om bruk av tjenesten med BankID brukersteder

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 for kvalifisert sertifikat.

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 finansielle transaksjonene.

Ansvarsfordeling mellom bankene, herunder regressansvar, er regulert gjennom avtaler mellom bankene. Ansvarsfordeling mellom bank og Mobiloperatør er regulert i egne avtaler.

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 som er sertifikatinnehaver eller brukersted. Sertifikatmottakers ansvar reguleres i avtale [4] med bank og i avtale med mobiloperatører.

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. 2.1.4. og 2.1.5, 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 Finansklagenemnda for uttalelse.

2.5 GEBYRER

Beskrives ikke i dette dokumentet. Den enkelte bank og mobiloperatør 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 BankID Samarbeidets lagringsenheter 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:

- Finanstilsynet 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
- Nasjonal Kommunikasjonsmyndighet (i forbindelse med utstedelse av kvalifiserte sertifikater)
- Bits AS
- Interne revisjons- og kontrollfunksjoner.

På samme måte skal det gjennomføres samsvarsrevisjon av mobiloperatørene for de delene av mobiloperatørens virksomhet som er knyttet til BankID på mobil.

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 eller mobiloperatør og Bitss.

2.7.2 Hva omfatter samsvarsrevisjon

Formålet er å bedømme om krav i BankID sertifikatpolicy oppfylles og sammenlikne utsteder av BankID sin 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 Finansforetakslovens §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

Bank, fellesutsteder og mobiloperatører har ansvar for at bl.a. følgende typer informasjon holdes konfidensiell:

a) data om sertifikatholdere som ikke kan leses ut av sertifikatet eller en eventuell offentlig tilgjengelig katalogtjeneste
b) utsteders og registreringsenhets private nøkler
c) engangskoder og andre aktiveringsdata, så lenge opplysningene befinner seg hos bank, utsteder eller mobiloperatør
d) loggdata
e) 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.

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 organisasjoner før de kan få utlevert sertifikater.

3.1 FØRSTE GANGS REGISTRERING

3.1.1 Navnetyper

I sertifikater skal feltene "subject" og "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) som unikt definerer vedkommende. OBS: En person kan ha mer enn ett sertifikat med samme distinguished name.

SERTIFIKATHOLDERS NAVN
Dette dokumentet omhandler personsertifikater, bundet til en persons identitet.

Attributt	Viktighet	Krav til innhold
Country (C)	Oblig	Skal ha verdien 'NO'.
Organisation (O)	Oblig	Skal ha verdien 'BankID - ' og navnet på utsteder av BankID.
Serial Number (SN) [1]	Valgfritt	Alfanumerisk verdi, som skal sikre at navnet er unikt [se pkt 3.1.2].
Organisational Unit (OU)	Valgfritt	Alfanumerisk verdi, som skal sikre at navnet er unikt [se pkt 3.1.2].
Common Name (CN)	Oblig	Alminnelig brukt navn på sertifikatholder.

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 som eier utstedersystem (juridisk person).
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

Navn på sertifikatholder hentes fra bankenes kunderegister. En person som skal bli BankID sertifikatiholder, skal være verifisert mot Folkeregisteret enten ved opprettelse av kundeforhold, ved inngåelse av nettbankavtale eller ved utstedelse av BankID.

De enkelte banker vil kunne opplyse om sin praksis for vask av registre og kontroll mot Folkeregisteret. Alle individer vil være knyttet entydig til et fødselsnummer eller D-nummer.

[1] Obligatorisk i alle sertifikater utstedt etter 1.12.2004. Alle sertifikater utstedt under denne policy må ha en unik identifikator i enten SN- eller OU-attributtet. OU er bare brukt t.o.m. nov 2004.

Bruk av pseudonymer er ikke tillatt i PersonBankID.

Unik identifikator i sertifikatholderes serialNumber er en sekvens av lesbare tegn, som entydig identifiserer sertifikatholder innenfor sertifikatene utstedt på dette utstedersystem. Regler for formatet av denne er gitt av Bits.

Formatet på sertifikatholders CommonName skal være:

```
<Family Name>,space<Given Names>
```

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 brukeren.

I navnesekvensen inngår en unik identifikator som blir tildelt sentralt og som dermed gjør at alle personer kan refereres entydig. Registreringsenhet er ansvarlig for å legge til rette for at en slik verdi kan tilordnes.

Hvis en person har flere BankID personsertifikater utstedt av samme utstedersystem (CA), vil disse ha samme DN.

3.1.3.1 Mobilnummer

Mobilnummer skal angis i sertifikatet, slik at sertifikatinnehaver kan identifiseres og adresseres via Sikkerhetskanalen.

Det kan til enhver tid være høyst ett aktivt (eller suspendert) sertifikat tilknyttet ett mobilnummer. Hvis en person har flere BankID på mobil sertifikater må disse være tilknyttet ulike mobilnummer.

3.1.4 Bevis for eierskap til privat nøkkel

I denne policy genereres nøkkelparet under sertifikatsøkers kontroll.
Når sertifikatsøker har generert sitt nøkkelpar, må sertifikatsøker bevise at privat nøkkel er under hans/hennes kontroll. Dette gjøres ved å signere en forespørsel til BankID CA. Hvis forespørselen er korrekt og verifiserbar, kan CA utstede et sertifikat basert på den tilhørende offentlige nøkkel.

3.1.5 Bruk av personsertifikat i organisasjoner

Det er mulig å utstede sertifikater til en person i rollen som disponent av bankkonto som tilhører en annen juridisk person (f. eks. en virksomhet). Sertifikatet utstedes til personen.

3.1.6 Utstedelse av BankID til personkunder

For å utstede BankID kreves det at personen selv samtykker og deltar aktivt i utstedelses-prosessen. Dette er ikke til hinder for at banken initierer utstedelsprosessen så lenge personkunden deltar aktivt.

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.

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

Kunden skal gjennom tekst i avtalen bli gjort oppmerksom på at innhold i PersonBankID på mobil vil inngå i meldingsutveksling med brukersteder. Kundens fødselsnummer inngår ikke i innhold av PersonBankID på mobil, og vil av utstederbank aldri utleveres til andre brukersteder enn slike som allerede har Kundens fødselsnummer lovlig registrert hos seg.

3.1.6.1 Nye kunder

Hvis personen er ny kunde i banken, må vedkommende fysisk møte opp og fremlegge et legitimasjonsdokument som banken finner tilfredsstillende.

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].

3.1.6.2 Eksisterende kunder

Personkunder som allerede har et kundeforhold til banken og som tidligere er blitt identifisert ved personlig fremmøte, kan registrere som beskrevet i punkt 3.1.6.1, eller gjennom en registreringsprosess som bygger på sikre prosedyrer for nettbanktjenester.

Dette forutsetter at banken allerede har utført en fullverdig kontroll av personens identitet, og at personkunden kan aksessere registreringsenheten gjennom en tjeneste (f. eks. nettbank) som bruker en godkjent autentiseringsmetode og som er utformet i henhold til Bits' tilleggskrav til RA ved utstedelse av BankID på mobil [12].

Bankkunder som ikke har benyttet nettbank, kan enten gå gjennom bankens prosedyre for å bli autorisert for nettbank, eller registrere slik det er beskrevet for nye kunder.

3.1.6.3 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 BankID basert på sertifikater fra andre utstedere.

Regler om BankID fastslår at det ikke er tillatt for en utsteder av BankID å utstede sertifikater for en ny kunde basert på en BankID utstedt av en annen bank.

Hvis kunden allerede har en BankID på mobil utstedt av en annen bank på samme mobilnummer, vil denne bli trukket tilbake i forbindelse med aktivering av ny BankID på mobil.

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.

Kundens mobilnummer skal verifiseres mot bankens registre så langt praktisk mulig. Dette er nærmere beskrevet i kap 6.10, "Tilleggskrav til RA ved utstedelse av BankID på mobil" i [12].

For personer som ikke har hatt kundeforhold til banken før 1. mars 2007 kreves det at norsk pass, utenlandsk pass eller annet dokument som er sidestilt med norsk pass, er fremvist før førstegangsutstedelse av BankID.

3.2 RUTINEMESSIG FORNYELSE

Det skilles mellom fornyelse med og uten brukermedvirkning.

3.2.1 Fornyelse uten brukermedvirkning

Fornyelse uten brukermedvirkning medfører ikke nøkkelskifte.

Fornyelse uten brukermedvirkning kan benyttes når BankID på mobil skal fornyes på grunn av periodisk utløp av sertifikatet. I tillegg skal fornyelse uten brukermedvirkning benyttes når det er systemmessige endringer som ikke påvirker kundens risikobilde eller brukeropplevelse.

Bank kan velge å varsle kundene dersom det skal foretas fornyelse uten brukermedvirkning. Fornyelse initieres av banken.

Det er ikke mulig å endre personopplysningene i sertifikatet ved denne typen fornyelse.

Fornyelsesprosessen består av disse elementene.
- Re-sertifisering av eksisterende offentlig nøkkel
- Tilbakekalling av det gamle sertifikatet. (Sertifikatet vil være tilbakekalt fra nytt sertifikat ble utstedt og til det er utløpt)

3.2.2 Fornyelse med brukermedvirkning

Rutinemessig fornyelse med brukermedvirkning medfører også nøkkelskifte. Denne typen fornyelse skal benyttes, hvis det er behov for å skifte ut nøkkellengde eller hashfunksjon, eller om det er mistanke om kompromittering av sluttbrukers nøkler. Ved fornyelse når en BankID på mobil har nådd sin utløpsdato, kan fornyelse med brukermedvirkning brukes.

For fornyelse med brukermedvirkning skal banken tilby en selvbetjent tjeneste, som benytter en godkjent autentiseringsløsning. Fornyelse initieres av kunden, som regel etter forutgående varsling fra banken.

Hvis det er endringer i opplysningene i sertifikatet, skal bank melde fra til kunden at det må foretas en reutstedelse av sertifikatet innen en gitt frist. Etter dette tidspunktet skal banken trekke sertifikatet tilbake hvis kunden ikke har reaktivert sertifikatet.

Fornyelsesprosessen består av disse elementene.
- Generering av nye nøkler og valg av IDPIN
- Sertifisering av ny offentlig nøkkel
- Tilbakekalling av sertifikatet for det gamle nøkkelparet. (Sertifikatet vil være tilbakekalt fra nytt sertifikat ble utstedt og til det er utløpt)

Hvis sertifikatholder ikke har fornyet sitt sertifikat før utløpsdatoen, må samme prosedyre som for fornyelse etter tilbakekalling følges.

3.3 NYTT SERTIFIKAT ETTER TILBAKEKALLING

Etter tilbakekalling må personkunden sende inn en sertifiseringsforespørsel på samme måte som ved første gangs registrering. Prosedyrene i punktene 3.1.4 – 3.1.6 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 personkunder /sertifikatholdere. Der det er angitt krav til Sikkerhetskanalen gjelder disse også for mobiloperatøren.

4.1 SØKNAD OM SERTIFIKAT

Identifisering av personer skal utføres som beskrevet i kapittel 3.

Registreringsenhet skal innhente alle personopplysninger nødvendig for å utstede BankID.

4.2 UTSTEDELSE AV SERTIFIKAT

BankID utstedes basert på en bestilling som kunden aktivt har deltatt i. Når BankID er blitt utstedt, innebærer dette at banken har godkjent kundens bestilling.

Som en del av prosessen for å ta i bruk BankID skal sertifikatsøker motta en engangskode fra banken. Denne engangskoden må kunden taste inn på telefonen i forbindelse med sin sertifikatforespørsel.

4.2.1 Forberedelser

Kommunikasjon mellom registreringsenhet og utsteder, samt kommunikasjon gjennom Sikkerhetskanalen, 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.

En sertifikatsøker skal motta:

- en kopi av avtalen bank-sertifikatholder [4]
- veiledning for bruk og eventuell installasjon av brukerens personlige sikkerhetsmiljø.

4.2.2 Nøkkelgenerering

Nøkkelpar genereres på sertifikatsøkers SIM-kort etter kundens godkjenning. SIM-kortet må være godkjent i henhold til krav i denne policy. Kunden velger en IDPIN på minimum 4 og maksimum 8 siffer, som beskytter nøklene mot uautorisert bruk.

4.2.3 Produksjon av sertifikater

Utstedersystem skal bruke informasjon fra registreringsenheten 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 BankID sertifikater.

4.2.4 Distribusjon og utlevering

Personkunden mottar en engangskode (også kalt bestillingskode) fra banken. Engangskoden kan distribueres til kunden i en selvbetjent tjeneste, som benytter en godkjent autentiseringsløsning.

Engangskoden kan også sendes til kunden over en annen sikker kanal.

Under aktiveringsprosessen blir kunden bedt om å oppgi sin engangskode ved å taste den inn på mobiltelefonen.

Når sertifikatproduksjonen er fullført, lagres sertifikatene i det sentrale sertifikatlageret, som inngår i Sikkerhetskanalen.

4.3 AKSEPT AV SERTIFIKATER

Utsteder skal gjøre informasjon om at sertifikat er blitt generert, tilgjengelig for banken. Banken har i sin tur ansvar for å informere sertifikatholder. Bank kan velge å la utsteder av BankID ta hånd om informasjonen direkte.

Banken skal i utlevert avtalemateriell [4] oppfordre sertifikatholder til å teste bruk av sin BankID mot BankIDs verktøyside.

Personkunden har indirekte akseptert BankID og sertifikater når:

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

Personkunden 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. Alle utstedere av BankID skal tilby sine sertifikatholdere tilgang til en tjeneste der kundene kan anmode om å få sperret sin BankID. Tjenesten skal være tilgjengelig 24 timer pr. døgn, alle dager. Alternativt kan sertifikatholder be om å få sperret et eller flere av elementene i aktiveringsdata som er nødvendig for å aktivere sin BankID.

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.

Mobiloperatør skal logge og arkivere alle forespørsler eller hendelser som kan føre til tilbakekalling.

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.

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

Utsteder av BankID skal lage en oppdatert liste med informasjon om sperrede sertifikater minst en gang pr. time og umiddelbart gjøre denne tilgjengelig for sertifikatkontrollører. Innimellom dette skal utstedersystem snarest mulig 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,
- kompromittering av aktiveringsdata,
- kjent misbruk av et sertifikat,
- sertifikatholder har skiftet navn,
- sertifikatholder er ikke lenger berettiget til å ha sertifikatet,
- opphør av sertifikatholders kundeforhold til banken
- opphør av sertifikatholders kundeforhold til mobiloperatør eller andre abonnementsmessige forhold
- SIM-kort eller IDPIN er kompromittert eller tapt
- utstedelse av nytt sertifikat knyttet til samme mobilnummer

4.4.2 Hvem kan be om tilbakekalling

Disse kan be om tilbakekalling:
- Sertifikatholder,
- 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.

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. Bank kan også velge å tilby sine sertifikatholdere mulighet til å suspendere sin BankID gjennom selvbetjente løsninger i f.eks. nettbank.

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

Bank kan også velge å suspendere BankID når en annen person ringer inn på vegne av sertifikatholder og kan begrunne hvorfor suspensjon skal foretas. Bank skal alltid forvisse seg om melders identitet i samsvar med bankens rutiner.

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

4.4.5.1 Mobiloperatørens plikt til å be om suspensjon

Mobiloperatør skal snarest og uten opphold informere banken ved mistanke om eller kjennskap til at nøkkellager er kompromittert eller tapt eller på annen måte er utilgjengelig for sertifikatholders bruk. Banken skal i slike tilfeller suspendere sertifikatet. Melding fra mobiloperatør i forbindelse med tapte, kompromitterte eller utilgjengelige SIM-kort skal gis på en forsvarlig sikret kanal, slik det avtales mellom bank og mobiloperatør.

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 til den normal 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 sertifikatkontroll-tjenesten for å spørre om status på et sertifikat (validering).

Sertifikatkontrolltjenesten kan ha tilgang på fødselsnummer eller annen tilleggsinformasjon om sertifikatholder. Slike tilleggsdata vil bare bli gjort 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, herunder også Sikkerhetskanalens kritiske komponenter.
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, sikkerhetskanal 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

Hendelsesloggen 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 Sikkerhetskanalens kritiske komponenter i forbindelse med nøkkelgenerering og sertifikatutstedelse

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, mobiloperatør 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
- Tekniske kontroller av mobiltelefon, abonnement og SIM-kort i forbindelse med utstedelse av sertifikater
- Hendelser i forbindelse med nøkkelgenerering på SIM-kort
- 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
- Hendelser hos mobiloperatøren som kan føre til tilbakekalling av et sertifikat
- 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 arkiv data

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, tjenesteleverandør og mobiloperatør 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 avslutter, avbryter eller suspenderer sin operasjon.

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 personsertifikater BankID på mobil er gyldige i 2 år og må fornyes hvert 2. 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 lenger 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.

Mobiloperatør må ha en skriftlig instruks med varsling og andre tiltak som må iverksettes overfor sikkerhetsansvarlige i BankID samarbeidet, sertifikatholdere og sertifikatmottakere ved en potensiell katastrofe, for eksempel hvis kritiske komponenter i Sikkerhetskanalen eller et større antall SIM-kort er kompromittert. I slike tilfeller skal bank og mobiloperatør sørge for at kompromitterte sertifikater ikke kan benyttes. Dette kan gjøres ved at Sikkerhetskanalen stenges for bruk for de aktuelle sertifikatene eller ved at sertifikatkontrollører alltid svarer negativt om disse.

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. Utstedere av BankID 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 sertifikatholdere, sertifikatmottakere 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.

En fellesutsteder må i tillegg sørge for at banker som bruker dens tjenester, får nødvendig informasjon til å fortsette sine BankID oppgaver hos en annen utsteder.

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 mobiloperatør

Hvis en avtale mellom mobiloperatør og bank termineres må alle sertifikater, som er knyttet til abonnement hos denne mobiloperatøren, trekkes tilbake.

4.9.2 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.

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

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.

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 insipisere 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 for sertifikatustedelse. 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.

Produksjonsutstyr som ikke håndterer strengt konfidensielle dta, kan plasseres i et kontrollert driftsmiljø på utsidena av det sikre miljøet.

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

Tilgang til driftsalarmer og logger 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 eller 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 presenteres. 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 fysiske personer som sertifikatinnehavere.

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 personkunde

Nøkkelpar skal genereres på personkundens SIM-kort i henhold til anerkjente prinsipper for generering av RSA nøkler. Før nøkkelgenerering kan starte må personkunden ha gitt sin godkjenning.

6.1.2 Overlevering av privat nøkkel til personkunde

I løsningen som omfattes av denne sertifikatpolicy befinner privat nøkkel seg alltid sikret på personkundens SIM-kort og forlater aldri denne. Det stilles derfor ikke spesielle krav til overlevering her.

6.1.3 Innsendelse av offentlig nøkkel til utsteder av BankID

Offentlig nøkkel skal sendes signert med privat nøkkel fra SIM-kort gjennom Sikkerhetskanalen og til utsteder av BankID.

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-CAs sertifikat og 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 være gjenstand for løpende vurdering.

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 personsertifikat må være minimum 1024 bits for RSA.

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

BankID på mobil har ett nøkkelpar, som benyttes for autentisering og signering. Når privat nøkkel benyttes til autentisering skal dette fremgå tydelig av innholdet som skal signeres, for både sertifikatholder og sertifikatmottakere.

6.2 BESKYTTELSE AV PRIVATE NØKLER

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

En sertifikatholders private nøkler befinner seg på et SIM-kort under sertifikatholderens kontroll. Nøklene er fysisk og logisk beskyttet av SIM-kortets adgangsmekanismer. Nøklene er beskyttet med en IDPIN ved at all bruk forutsetter at sertifikatholder først oppgir korrekt IDPIN. Nøklene skal blokkeres for all fremtidig bruk hvis verifikasjon av IDPIN feiler tre ganger på rad.

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.

6.2.1.1 Krav til SIM-kort som nøkkellager

SIM-kort som skal benyttes som nøkkellager for BankID personsertifikat skal være godkjent av Bits. For å oppnå slik godkjenning må mobiloperatøren dokumentere at den private nøkkelen har tilfredsstillende beskyttelse mot kompromittering og misbruk. Sentrale komponenter på SIM-kortet skal være sertifisert av en anerkjent institusjon. Bits gir nærmere angivelse av hvilken dokumentasjon som kreves.

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 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

Det finnes ingen sikkerhetskopi av sertifikatholders private nøkkel.

6.2.4 Arkivering av nøkler

Private nøkler for utstedere av BankID arkiveres ikke.

Det foretas ingen arkivering av sertifikatholderes private nøkler.

6.2.5 Innlegging av private nøkler i kryptomoduler

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

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.

Privat nøkkel for sertifikatholder skal være beskyttet av en IDPIN. For å kunne bruke sin private nøkkel må sertifikatholder oppgi korrekt IDPIN. Det skal ikke være mulig å utføre operasjoner med den private nøkkelen uten å oppgi korrekt IDPIN.

Sertifikatholder må beskytte sin IDPIN og sørge for at den aldri blir kjent for andre enn sertifikatholder selv.

6.2.7 Deaktivering av private nøkler

Private nøkler anses som midlertidig deaktivert når de ikke er i bruk, og inntil korrekte aktiveringsdata er blitt oppgitt.

6.2.8 Destruksjon av private nøkler

For å gjøre sine nøkler permanent utilgjengelige, må sertifikatholder anmode om tilbakekalling. En nøkkel som er tilbakekalt, suspendert eller utløpt, kan ikke benyttes.

Hvis SIM-kortet er ødelagt eller nøkkelen er blokkert, er nøkkelen permanent utilgjengelig.

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.

Personsertifikater og nøkler er gyldige i inntil fem år.

6.4 AKTIVERINGSDATA

IDPIN som beskytter den private nøkkelen skal bestå av minimum 4 og maksimum 8 siffer.

6.4.1 Valg og initiering av aktiveringsdata

Personkunden velger selv sin IDPIN innenfor reglene ovenfor. Sertifikatinnehaver kan når som helst endre sin IDPIN.

6.5 DATAMASKINSIKKERHET

Alle unødvendige funksjoner skal være avslått på utstedersystem, RAs datamaskiner og kritiske komponenter i Sikkerhetskanalen. Med kritiske komponenter menes her enheter som har tilgang til autentiseringsdata eller andre hemmeligheter i klartekst, samt komponenter som utfører sikkerhetskontroller på vegne av sertifikatholder.

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.

Det skal finnes autentisering, aksesskontroll og sporbarhet ned til individnivå på alle operasjoner og transaksjoner på kritiske komponenter i Sikkerhetskanalen.

Maskinene som kjører sertifikatkontroll eller sender sperreinformasjon til disse 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 enheter 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.

Kravene ovenfor skal også gjelde for kritiske komponenter i Sikkerhetskanalen.

6.6.2 Drift

Atskilte roller, som beskrevet i kap. 5.2., skal implementeres og håndheves av utsteder av BankID og tjenesteleverandør.

Utsteder av BankID og deres tjenesteleverandører skal ha full kontroll over alle 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.

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.

Sikkerhetskanalens kritiske komponenter skal også være konfigurert slik at de kun tilbyr den minimale funksjonalitet nødvendig for å utføre sine oppgaver.

Sikkerhetskanalen skal være forsvarlig beskyttet med anerkjente mekanismer. Kritiske komponenter skal stå bak minst to nivåer av brannmurer. Kommunikasjon i Sikkerhetskanalen som inneholder aktiveringsdata eller andre hemmeligheter skal være kryptert. Det skal finnes kryptografiske mekanismer for å identifisere avsender og sikre autentisitet av meldinger i Sikkerhetskanalen.

Et brukersted som ber om autentisering eller signering fra en sertifikatholder med BankID på mobil, må først identifiseres korrekt i Sikkerhetskanalen og forespørselen skal gå gjennom en brannmur.

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. 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
subjectDirectory Attributes – Date of Birth	Fødselsdato	SU, Obl	Sertifikatholders fødselsdato
subjectDirectory Attributes – telephone Number	Mobilnummer	SU, Obl	Mobilnummeret som er knyttet til SIM-kortet hvor nøklene ligger
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

Navn	Norsk betegnelse	Type	Verdi / kommentar
KeyUsage	Bruk av nøkler	SU,Obl,Krit	Bruksbegrensning som må følges av programvare som bruker BankID nøkler og sertifikater. Ett sertifikat er definert, med følgende bitmap:. **Non-repudiation** og **DigitalSignature**
Qualified Certificate Statements	Kvalifisert sertifikat erklæringer	SU,Obl	Referanse til erklæring om at dette sertifikatet er utstedt som kvalifisert sertifikat, og evt. om beløpsbegrensning

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.

BankID personsertifikater 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.

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 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. 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.

Hver mobiloperatør som inngår avtaler om BankID på mobil er ansvarlig for å utarbeide CPS. CPS skal uttrykke samsvar med kravene i denne sertifikatpolicy.

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
fornye	renew
gyldighetsperiode	validity
ikke-benekting	non-repudiation
engangskode	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