



Regler om BankID

Fastsatt av Finans Norge Servicekontor etter behandling i Bransjestyre betalingsformidling og infrastruktur 28.11.2013. Endret av Bits AS 26.03.2021.

1 Reglens omfang og virkeområde

Reglene gjelder utstedelse og behandling av BankID. Regler om BankID er et multilateralt avtaleverk som fastsetter rettigheter og plikter mellom utstedere av BankID (deltagere), Finans Norge Servicekontor og Bits AS (heretter benevnt Bits). Ingen andre enn deltagere kan påberope seg Regler om BankID.

BankID reguleres i henhold til lov av 15. juni 2018 nr. 44 om elektroniske tillitstjenester og forskrifter som bl.a. gjennomfører EUs forordning nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (heretter benevnt «eID-reglene»).

Rett til å utstede BankID (deltager) har foretak som har tillatelse til å drive betalingstjenestevirksomhet i Norge og rett til å delta i interbanksystemer meldt til EFTAs overvåkningsorgan i samsvar med rådsdirektiv 98/26/EF, jf. lov om betalingssystemer kapittel 4, og er tilknyttet Bits gjennom medlemskap i Finans Norge Servicekontor eller etter samtykke fra Bits har sluttet seg til Regler om BankID. Foretak gis tilgang basert på rettferdige, rimelige, ikke-diskriminerende vilkår.

BankID til fysiske personer har to sikkerhetsnivåer («Høyt» og «Betydelig»).

BankID Høyt skal tilfredsstillere eID-reglene til eID på sikkerhetsnivå Høyt, og er også en tillitstjeneste basert på kvalifiserte sertifikater for elektroniske signaturer. BankID Høyt benyttes til autentisering med strengeste krav til sikkerhet, og til signering av dokumenter.

BankID Betydelig skal tilfredsstillere eID-reglene til eID på nivå Betydelig. BankID Betydelig kan benyttes i situasjoner der det er krav til sterk kundeautentisering (SKA) og/eller annen to-faktorautentisering. BankID Betydelig kan benyttes i kombinasjon med BankID på nivå Høyt («Step up»).

eID-er og sertifikater utstedes av deltagere og godkjente fellesutstedere. Utstedelse og bruk av BankID kontrolleres av deltagerne. Fellesutstedere og underleverandører meldes til Bits etter reglene i punkt 6 (Bruk av fellesutstedere eller underleverandører for BankID-tjenester).

BankID Betydelig reguleres særskilt i punkt 3.7.

Ved utstedelse og behandling av BankID skal deltagerne etterleve den til enhver tid gjeldende lovgivning med tilhørende forskrifter, herunder lov om elektroniske tillitstjenester, samt stille krav overfor fellesutstedere og underleverandører om etterlevelse av regulatoriske krav og Regler om BankID. Deltagerne skal tilrettelegge systemer, regler og prosedyrer for å ivareta sikkerheten.

2 Vipps AS

Vipps AS (heretter benevnt Vipps) er et norskregistrert betalingsforetak med konsesjon fra Finansdepartementet etter finansforetaksloven § 2-10. Foruten å yte betalingstjenester i henhold til finansforetaksloven § 2-3, jf. finansavtaleloven § 11 første ledd, driver Vipps tilknyttet virksomhet bl.a. drift, forvaltning og utvikling av BankID og andre eID-produkter.

På vegne av deltagerne skal Bits skal søke et frivillig og hensiktsmessig samarbeid med Vipps slik at Bits og Vipps kan bistå hverandre til gjensidig nytte og behov for å oppfylle formålet med reglene her.

3 Utstedelse av nivå 1-sertifikat og BankID Høyt

3.1 Sertifikathierarkiet for BankID Høyt

Finansnæringens Servicekontor og Sparebankforeningens Servicekontor har i fellesskap etablert øverste nivå i et tillitshierarki og utstedt et rot-sertifikat til seg selv. På grunnlag av dette rot-sertifikatet og tilhørende nøkler, har servicekontorene utstedt nivå 1-sertifikater til utstedere av BankID Høyt.

Fra 1. januar 2010 overtok FNO alle oppgavene og det ansvar som tillå servicekontorene i egenskap av utsteder og innehaver av rot-sertifikatet. Fra denne dato var det FNO som foresto utstedelse av nivå 1-sertifikater til utstederne av BankID Høyt.

Fra 1. januar 2011 har Finans Norge Servicekontor overtatt alle oppgavene og det ansvar som tillå FNO i egenskap av utsteder og innehaver av rot-sertifikatet. Fra denne dato var det Finans Norge Servicekontor som forestår utstedelse av nivå 1-sertifikater til utstederne av BankID Høyt.

Fra 1. april 2016 overtok Bits hovedtyngden av de oppgavene og det ansvar som tillå Finans Norge Servicekontor.

Utsteder av BankID Høyt er den som signerer BankID Høyt med et nivå 1-sertifikat utstedt av Finansnæringens Servicekontor og Sparebankforeningens Servicekontor, FNO eller Finans Norge Servicekontor. Det skal fremgå av BankID Høyt hvem som er utsteder.

3.2 Utstedelse av nivå 1-sertifikat til utstedere av BankID Høyt

Finans Norge Servicekontor skal utstede nivå 1-sertifikat til deltager og andre (fellesutsteder) som har rett til å utstede BankID Høyt etter reglene her. Finans Norge Servicekontor kan benytte Bits til å utføre hele eller deler av prosessene ved utstedelse av nivå 1-sertifikatet.

Før det utstedes nivå 1-sertifikat skal deltager avgi en erklæring til Finans Norge Servicekontor om at den tiltrer Regler om BankID. Erklæringen skal underskrives av deltagers administrerende direktør. Dersom en eller flere deltagere ønsker å benytte en fellesutsteder skal dette opplyses i erklæringen, og erklæringen skal medunderskrives av fellesutstederens administrerende direktør. Bits skal når erklæringen er funnet i orden sende deltager, eventuell fellesutsteder og Vipps en bekreftelse på at vilkårene for å utstede BankID Høyt er til stede.

Før en fellesutsteder får utstedt nivå 1-sertifikat, skal fellesutstederen være godkjent av Bits etter reglene i pkt. 6.

Bits utarbeider standarderklæring som nevnt i andre ledd.

3.3 Hvem kan utstede BankID Høyt

BankID Høyt kan utstedes av deltagere som er tilsluttet dette regelverket. Andre enn deltagere kan etter særlig tillatelse fra Bits etter reglene i pkt. 6, utstede BankID Høyt på oppdrag fra en deltager eller en gruppe deltagere. Det er likevel alltid deltager som skal inngå avtale med egne kunder (sertifikatholder) om bruk av BankID Høyt.

Før deltager kan utstede BankID Høyt skal deltager også inngå Tjenestekjøpsavtale og Utstederavtale med Vipps, implementere og etterleve sikkerhetskrav fastsatt av Bits etter punkt 4.2 og anvende varemerket/logo som angitt i punkt 5.

3.4 Hvem kan BankID Høyt utstedes til

BankID Høyt kan utstedes til

- fysiske personer
- fysiske personer (brukere) som er ansatt hos eller utfører oppgaver for en juridisk person (privat eller offentlig virksomhet og forvaltning) som er registrert i Enhetsregisteret eller et tilsvarende offentlig register innenfor EØS-området, heretter kalt BankID til ansatte
- juridiske personer (privat eller offentlig virksomhet og forvaltning) som er registrert i Enhetsregisteret eller et tilsvarende offentlig register innenfor EØS-området.

BankID Høyt kan ikke utstedes til personer under 15 år. BankID Høyt kan likevel utstedes til personer mellom 13 og 15 år såfremt det foreligger vergesamtykke.

BankID Høyt skal ikke utstedes til personer som helt eller delvis er fratatt sin rettslige handleevne.

3.5 BankID Høyt som kvalifisert sertifikat

BankID til fysiske personer skal tilfredsstillende lovgivningens krav til kvalifisert sertifikat. Andre typer BankID Høyt sertifikater kan også registreres som kvalifiserte sertifikater.

3.6 Om BankID Høyt og lignende som grunnlag for utstedelse av banklegitimasjon

BankID Høyt skal ikke utstedes til fysiske personer på grunnlag av BankID Høyt utstedt av en annen deltager eller på grunnlag av andre typer elektronisk legitimasjon.

En BankID Høyt skal ikke benyttes som grunnlag for utstedelse av fysisk eller elektronisk legitimasjon. PersonBankID som en deltager selv har utstedt eller inngått avtale om kan likevel inngå som element for å utstede annen legitimasjon enn BankID Høyt til respektive kunder.

3.7 BankID på sikkerhetsnivå Betydelig

3.7.1 Virkeområdet for Regler om BankID

Regler om BankID gjelder for utstedelse og behandling av BankID Betydelig så langt reglene passer. Punktene 3.1-3.6, 8 og 10 gjelder ikke for BankID Betydelig.

3.7.2 Utstedelse og avtaleinngåelse

BankID Høyt som deltager selv har utstedt skal benyttes som grunnlag for å utstede BankID Betydelig til deltagers egne personkunder.

Deltagerne inngår avtale med egne personkunder om BankID Betydelig. Dette gjelder tilsvarende for deltagere som benytter fellesutsteder for utstedelse av BankID betydelig,

3.7.3 Utkontrakteringsavtale

Utstedelse av BankID Betydelig er frivillig for deltagerne. Før deltager kan utstede og inngå avtale med sine personkunder om BankID Betydelig, skal deltager eller deltagers fellesutsteder inngå utkontrakteringsavtale med Vipps AS om leveranser av tekniske utstedertjenester for BankID Betydelig.

3.7.4 Utfyllende regler. Unntak

Bits kan fastsette særlige krav til sikkerhet, beredskap og krisehåndtering for BankID Betydelig, ref. punkt 3.7.1.

4 BankID form og utførelse. Krav til fysisk og logisk sikkerhet

4.1 Fastsettelse av sertifikatpolicier

Bits fastsetter og forvalter sertifikatpolicier for BankID.

4.2 Krav til fysisk og logisk sikkerhet.

Bits skal innenfor rammen av disse regler fastsette krav overfor deltagerne om sikkerheten for BankID. Bits kan gjøre unntak fra egne krav i enkelttilfeller dersom dette er begrunnet i rettferdige, rimelige, ikke-diskriminerende hensyn.

Systemer og annen fysisk utrustning som benyttes for BankID, skal være i samsvar med krav til fysisk og logisk sikkerhet fastsatt av Bits. Bits har rett til å kontrollere at disse kravene er oppfylt. Bits kan typegodkjenne systemer og annen fysisk utrustning. Nektelse av godkjenning kan bare skje dersom dette er begrunnet i rettferdige, rimelige, ikke-diskriminerende vilkår.

Bits skal utarbeide og forvalte retningslinjer for kontroll og godkjenning av systemer eller annen fysisk utrustning, samt dekning av kostnader ved slik kontroll og godkjenning.

Krav til sikkerhet, typegodkjenning samt godkjennelses- og kontrollordninger skal Bits utforme produktnøytralt og ikke-diskriminerende slik at BankID-tjenestene kan operere i et konkurranseutsatt marked under samme rammevilkår som konkurrerende nasjonale og internasjonale ordninger for elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner.

5 Varemerke

Deltagerne skal alltid benytte et varemerke/logo for BankID sammen med eller på annen måte knyttes til sertifikatet slik at brukere og andre som kommer i kontakt med dette, identifiserer sertifikatet med varemerket og omvendt. På samme måte skal varemerket så langt det er mulig, knyttes til brukssituasjoner for sertifikatet, herunder være synlig på brukersteder og vise sertifikatholder at BankID kan anvendes.

Vipps har rettighetene til varemerket og fastsetter dets form, bruk og utførelse.

Dersom en deltager utsteder eller inngår avtale om et elektronisk sertifikat som ikke er BankID, skal utsteder påse at sertifikatet ikke kan forveksles med BankID.

6 Bruk av fellesutsteder eller underleverandører for BankID-tjenester

6.1 Krav om godkjenning av fellesutsteder

Deltager kan bare benytte fellesutsteder for produksjon av BankID eller levering av tjenester relatert til BankID dersom fellesutsteder er godkjent av Bits etter reglene nedenfor. Slik godkjenning kan også gis ved generelle regler. Bits kan generelt og i enkeltsaker gi nærmere bestemmelser om hvilke fellesutstedere som krever godkjenning.

6.2 Vilkår for godkjenning av fellesutsteder

Deltager som benytter fellesutsteder skal alene eller sammen med andre deltagere ha full styring og kontroll med fellesutstederen. Er fellesutstederen organisert som et aksjeselskap skal selskapet være heleid av deltagere som benytter fellesutstederen. Bestemmelsene i dette avsnittet gjelder ikke dersom fellesutstederen er en deltager.

Deltagere som benytter en fellesutsteder skal påse at fellesutsteder kan oppfylle soliditetskravene i henhold til relevant lovgivning samt dekke eventuelt ansvar som fellesutstederen kan pådra seg, herunder avtale som nevnt i neste ledd. I tillegg til tilstrekkelig egenkapital kan kravet om økonomiske ressurser oppfylles gjennom eierskap eller garantier/skadesløserklæringer fra den eller de deltagerne som benytter fellesutstederen eller ved forsikring.

Deltager skal inngå avtale med fellesutstederen som regulerer rettigheter og forpliktelser, angir oppgavefordelingen mellom partene, ansvarsforhold og avtalens varighet, samt de krav som følger av lovgivningen for øvrig.

6.3 Søknad om godkjenning av fellesutsteder - endringsmelding

Søknaden om godkjenning av en fellesutsteder skal minst inneholde opplysninger om:

- a. fellesutstедers navn, adresse og organisasjonsnummer,
- b. eier- og deltakerforhold, styresammensetning og daglig leder hos fellesutstederen
- c. de vilkår som er fastsatt for tilslutning til og deltakelse. Er samarbeidet om en fellesutsteder betinget av medlemskap, kapitalinnskudd og/eller garantier/skadesløserklæringer, skal det opplyses om dette,
- d. plan for løsning av operasjonelle forhold ved en deltagers inntredelse og uttredelse, herunder ved sperring av nivå 1-sertifikat og utstedte BankID,
- e. plan for organisering og drift av virksomheten hos fellesutstederen, herunder om oppgavefordelingen mellom fellesutsteder og deltagere, og
- f. tiltak for å sikre IKT-driften hos fellesutsteder, herunder om deltager har forsikret seg om at fellesutstederen oppfyller de krav som følger av Finanstilsynets IKT-forskrift.

Avtale som nevnt i pkt. 6.2 tredje ledd, skal vedlegges søknaden.

Søknaden sendes Bits med kopi til Finans Norge Servicekontor.

De samarbeidende deltagere eller fellesutstederen selv skal gi melding til Bits ved endring av betydning i forhold som nevnt i første ledd. Endring kan iverksettes dersom Bits ikke har truffet annen beslutning innen 4 uker etter at meldingen er mottatt.

6.4 Krav om deklarasjon av underleverandører

Deltagere og godkjente fellesutstedere som benytter en eller flere underleverandører for produksjon av BankID eller levering av tjenester relatert til BankID, skal sende melding til Bits om hvilke underleverandører deltageren eller fellesutsteder benytter.

Meldingen skal minimum inneholde opplysninger om underleverandørens navn og organisasjonsnummer, de funksjoner og oppgaver som utføres for deltager og andre opplysninger om underleverandørene og deres virksomhet som er av betydning for den kontroll Bits skal utføre med hensyn til fysisk og logisk sikkerhet, ved bruk av BankID. Endrede forhold som påvirker innsendte opplysninger skal uten ugrunnet opphold meldes til Bits.

Bits fastsetter nærmere regler om meldingens innhold, tilhørende dokumentasjon, innsendingsrutiner samt innsyn, tilsyn og kontroll med underleverandører. Bits kan generelt og i enkeltsaker gi nærmere regler om hvilke sikkerhets- og kvalitetskrav som skal stilles til underleverandører.

Bits kan utarbeide og publisere en oversikt over innmeldte underleverandører og fastsette rutiner for en forenklet innmeldingsordning.

6.5 Bankenes ansvar for egne underleverandører og fellesutstedere

Regler om BankID og bestemmelser gitt i medhold av disse gjelder uavhengig av hvilke underleverandører eller fellesutstedere som deltager benytter, og den enkelte deltager er ansvarlig overfor øvrige deltagere for at underleverandør og fellesutsteder følger reglene.

Deltager skal i avtale med eventuell underleverandør og fellesutsteder, pålegge denne ansvar for at leveransene tilfredsstillt kravene i disse regler og utfyllende bestemmelser gitt av Bits.

7 Innhold i BankID

BankID Høyt skal som et minimum inneholde følgende:

- a. angivelse av utsteder
- b. angivelse av sertifikatholderen
- c. gyldighetsperiode for BankID
- d. sertifikatholders signaturverifiseringsdata
- e. utstедers digitale signatur
- f. data som entydig identifiserer det enkelte BankID (serienummer)
- g. den deltager som inngår avtale med sertifikatholder
- h. angivelse av om BankID er kvalifisert sertifikat.

BankID Betydelig skal som et minimum inneholde følgende:

- a. angivelse av utsteder
- b. angivelse av innehaveren av BankID Betydelig
- c. gyldighetsperiode for BankID Betydelig
- d. data som entydig identifiserer det enkelte BankID (serienummer)
- e. den deltager som inngår avtale med innehaveren.

8 Nærmere om innholdet i BankID

Entydig angivelse av utsteder skal skje ved bruk av en unik identifikator.

Angivelse av sertifikatholderen skal skje ved hjelp av det navn banken benytter i sitt kunderegister og unik identifikator godkjent av Bits. Sertifikatholders fødselsdato skal også fremgå av sertifikatet for fysiske personer.

Utsteders digitale signatur skal kunne verifiseres ved hjelp av et sertifikat utstedt av servicekontorene, FNO eller Finans Norge Servicekontor. Bits kan fastsette nærmere regler om slike sertifikater, herunder for utstedelse, bruk, verifisering, sperring, ansvar, ansvarsfordeling i tilfelle kompromittering med videre.

9 Avtaleinngåelse. Deltagers kontroller ved utstedelse av BankID

9.1 Avtaleinngåelse

Deltager skal før utstedelse av BankID inngå skriftlig kundeavtale med sertifikatholder om bruk av BankID. For BankID til ansatte, skal deltager inngå kundeavtalen med virksomheten mens virksomheten innhenter erklæring fra bruker, se pkt. 10.1 og 10.4.

For utstedelse av BankID til juridiske personer kan deltager gi fullmakt til Vipps AS eller andre til å inngå avtalen med sertifikatholder på deltagerens vegne.

9.2 Behandling av personopplysninger

Personopplysninger som er nødvendige for å kunne utstede, bruke eller sperre et BankID, kan bare innhentes fra sertifikatholder selv eller med dennes uttrykkelige samtykke. Opplysningene kan bare benyttes til formål som er forenlig med dette regelverket, herunder statistiske formål, med mindre sertifikatholder har gitt sitt uttrykkelige samtykke til at opplysningene kan benyttes til andre formål. Deltager skal i kundeavtalen informere sertifikatholder om formålet med bruken av innsamlede personopplysninger og at opplysningene i forbindelse med bruk av BankID vil bli utlevert til andre sertifikatholdere.

9.3 Legitimasjonskontroll og identifisering av sertifikatholder

Ved utstedelse av BankID skal deltager forvise seg om sertifikatholders identitet. Kontroll av sertifikatholders identitet skal skje ved personlig fremmøte hos deltager eller en representant for deltager, med mindre sertifikatholder allerede er identifisert ved personlig fremmøte ved etablering av kundeforholdet, se egne regler for BankID Betydelig i punkt 3.7.

9.4 Krav til legitimasjonsdokumenter

Deltagers legitimasjonskontroll ved førstegangsutstedelse av BankID skal skje på grunnlag av fremlagt gyldig norsk pass, gyldig norsk nasjonalt ID-kort, gyldig utenlandsk pass eller andre dokumenter som etter en konkret risikobasert vurdering anses som gyldig legitimasjon med samme sikkerhetsnivå som norsk pass. Det er likevel ikke nødvendig med ny fremleggelse av pass ved utstedelse av BankID dersom pass ble fremlagt ved personlig fremmøte i forbindelse med etablering av kundeforholdet.

Kravet om fremleggelse av pass kan fravikes dersom deltager er sikker på personens identitet, og

- vedkommende etablerte sitt kundeforhold hos deltager før 1. mars 2007, eller
- kravet om fremleggelse av pass vil innebære en urimelig merbelastning for vedkommende, grunnet alder, helse eller andre særlige forhold.

Så fremt kravet om pass kan fravikes skal deltager i stedet kreve fremlagt annen form for legitimasjon etter de krav til fysiske legitimasjonsdokumenter som følger av hvitvaskingsloven med forskrifter.

9.5 Utfyllende regler og anbefalinger

Bits kan fastsette utfyllende regler om legitimasjonskontroll og identifisering av sertifikatholdere, herunder innehavere av BankID til ansatte etter reglene i pkt. 10.3.

Bits gir nærmere veiledning om forståelsen av reglene foran, hva som menes med norsk pass, dokumenter likestilt med norsk pass, og utenlandsk pass samt i hvilken grad deltager skal kreve tilleggsdokumentasjon for stadfesting av utenlandske personers identitet og bosted. Det kan også gis anbefalinger om praktisering av kontrollreglene.

10 Særskilte regler for BankID til ansatte

10.1 Virkeområde mv

BankID til ansatte skal bekrefte en knytning mellom en identifisert virksomhet (juridisk person) og en entydig identifisert fysisk person (brukeren) innenfor denne virksomheten.

Deltager skal før utstedelse inngå avtale med virksomheten om bruk av BankID til ansatte. Avtalen skal bl.a. inneholde vilkår om at BankID til ansatte bare skal benyttes av ansatte og oppdragstakere til tjenstlige oppgaver eller oppdrag på vegne av virksomheten.

10.2 Innhold i BankID til ansatte

BankID til ansatte skal i tillegg til krav som beskrevet i pkt. 7 inneholde virksomhetens navn og norsk organisasjonsnummer.

For virksomheter som ikke er registrert i Norge kan Bits godkjenne annen unik identifikator enn norsk organisasjonsnummer.

10.3 Legitimasjonskontroll

Ved inngåelse av avtale med virksomheten og utstedelse av BankID til ansatte skal deltager sørge for at det gjennomføres betryggende legitimasjonskontroll og identifisering av virksomheten, brukere av virksomhetens sertifikater og en ansvarlig fysisk person som representerer virksomheten overfor banken. Slik legitimasjonskontroll skal skje ved personlig fremmøte hos deltager eller representant for denne. Deltager skal følge de krav til legitimasjonskontroll og dokumenter som følger av punktene 9.3 til 9.5.

10.4 Erklæring fra brukere

Deltager skal gjennom avtale med virksomheten påse at virksomheten innhenter en erklæring fra brukerne om å følge de bruks- og sikkerhetsregler som gjelder for BankID til ansatte.

11 Legitimasjonskontroll ved utstedelse av BankID til juridiske personer

Ved inngåelse av avtale om BankID til juridiske personer skal den juridiske person være representert ved signaturberettiget eller en som har fått uttrykkelig fullmakt fra signaturberettiget til å inngå avtale om BankID på vegne av vedkommende juridiske person. Et enkeltpersonforetak skal være representert ved innehaveren av enkeltpersonforetaket eller en med fullmakt fra innehaver til å inngå avtale om BankID på vegne av enkeltpersonforetaket.

Den juridiske personen og den eller de fysiske personer som skal representere den juridiske personen, må være identifisert og kontrollert i henhold til regler om lov om tiltak mot hvitvasking.

12 Deltagernes gjensidige anerkjennelse av BankID

Deltager som inngår avtaler om BankID etter disse regler, skal legge til grunn at de som legitimerer seg ved bruk av et BankID der avtalen er inngått med annen deltager, er rette vedkommende, med mindre deltager har mistanke om at det foreligger brudd på disse reglene eller om at det benyttede BankID er misbrukt av uvedkommende.

13 Sperring og gjenåpning av BankID

Utstedere av BankID sertifikater skal ha systemer, regler og prosedyrer som gir utstedere adgang til å sperre (suspendere eller tilbakekalle) sertifikatet for videre bruk dersom det foreligger saklige grunner knyttet til sertifikatets sikkerhet, nøkler og der tilhørende koder er kommet på avveie eller sertifikatet inneholder feilaktige opplysninger.

BankID som er tilbakekalt kan ikke gjøres gyldig igjen. Deltager kan isteden velge å suspendere BankID midlertidig for inntil 30 dager. Deltager kan gjenåpne et suspendert BankID innen utløpet av 30 dagersfristen, så fremt grunnlaget for suspensjonen ikke lenger er til stede.

Deltager skal sørge for at det finnes hensiktsmessige rutiner for å motta og behandle meldinger fra egne kunder/sertifikatholdere som ønsker at BankID skal sperres.

Dersom BankID ikke lenger inneholder riktige opplysninger eller deltager blir kjent med at vilkårene for å utstede BankID til en sertifikatholder ikke lenger er til stede, skal deltager tilbakekalle vedkommende BankID og inndra det så langt det er mulig.

14 Validering

På forespørsel fra en sertifikatholder som deltager har inngått avtale om BankID med, skal deltager bekrefte eller avkrefte gyldigheten av et BankID. Bekreftelsen som gjelder BankID som andre deltagere har inngått avtale om, gis på bakgrunn av informasjon innhentet fra vedkommende deltager og på vegne av denne.

Den deltager som inngår avtale om BankID, skal sørge for at brukersteder i avtale pålegges å gjennomføre slike gyldighetsforespørslar.

En deltager skal på forespørsel fra en annen deltager bekrefte eller avkrefte gyldigheten av et BankID som deltager har inngått avtale om.

Svar på forespørsel fra sertifikatholder skal minimum inneholde:

- opplysning om BankID er tilbakekalt eller suspendert,
- opplysning om BankID er ukjent.

Bits kan fastsette krav utover minimum såfremt dette er nødvendig for ivaretagelse av rettferdige, rimelige og ikke-diskriminerende krav til sikkerhet.

15 Registrering og bruk av sertifikatopplysninger og fødselsnummer

15.1 Registrering av sertifikatopplysninger

Deltager skal etablere eller påse at det blir etablert et register over BankID den har inngått avtale om som grunnlag for å kunne besvare valideringsforespørslers etter pkt. 14. Registeret skal minst inneholde opplysninger om sertifikatholderens navn, fødselsdato og unik identifikator. Registeret skal fortløpende oppdateres med tilbakekalte og suspenderte BankID.

Utover disse krav kan Bits fastsette tilleggskrav til utsteders registrering av opplysninger som er nødvendig for ivaretagelse av sikkerhet.

15.2 Loggføring, arkivering og gjenfinning

Deltager skal etablere eller påse at det blir etablert tilfredsstillende rutiner for loggføring, arkivering og gjenfinning av opplysninger i forbindelse med utstedelse, tilbakekall, suspensjon og forespørslers.

Deltager skal lagre sertifikatopplysninger som nevnt i pkt. 15.1 første og annet avsnitt i minst ti år etter at gyldighetsperioden for et BankID er utløpt eller etter at det er tilbakekalt. Andre registrerte opplysninger (herunder valideringsforespørslers og -svar) skal lagres så lenge dette anses nødvendig i forhold til formålet med å registrere og lagre opplysningene.

Mottatte og registrerte opplysninger kan bare benyttes til formål som er forenlig med dette regelverket, herunder statistiske formål.

15.3 Registrering og utlevering av fødselsnummer

Deltager skal registrere fødselsnummer (11 siffer) for sertifikatholder deltager har inngått avtale om BankID med. Registreringen forutsetter at sertifikatholder uttrykkelig har akseptert at fødselsnummeret kan utleveres til brukersteder som sertifikatholder allerede har oppgitt fødselsnummer til eller som allerede har fødselsnummeret lovlig registrert hos seg.

Fødselsnummer kan bare utleveres til brukersteder som kan godtgjøre at tilgjengelige sertifikatopplysninger i BankID alene ikke er tilstrekkelig for å oppnå sikker identifisering av sertifikatholder og som allerede på lovlig vis har innhentet sertifikatholders fødselsnummer. Den enkelte deltager skal påse at det etableres tilfredsstillende rutiner for kontroll av at fødselsnummer bare utleveres til brukersteder som oppfyller disse vilkårene.

15.4 Behandlingsansvar

Deltager er ansvarlig for behandlingen av personopplysninger om sertifikatholder som deltager har inngått avtale om BankID med.

15.5 Bistandsplikt og informasjonsutveksling ved sikkerhetshendelser og misbruk

Deltagere som deltar i meldingsutveksling med bruk av BankID, er ved oppståtte sikkerhetshendelser eller hvis sertifikatet ikke lenger inneholder riktige opplysninger, forpliktet til å bistå øvrige involverte deltagere med å forhindre eller begrense omfanget av hendelsen eller misbruket, kartlegge hendelses- og årsaksforhold samt rette eventuelle feil.

I den grad oppfyllelsen av slik bistandsplikt gjør det nødvendig for deltager å innhente opplysninger om sertifikatholder(e), IP-adresser, valideringsinformasjon, informasjon om avvik og driftslogger, skal deltagerne utlevere slike opplysninger uten ugrunnet opphold. Utleveringsbegjæringen med angivelse av hvilke opplysninger som ønskes utlevert samt formålet med utleveringen, skal dokumenteres.

All distribusjon av personopplysninger og annen taushetsbelagt informasjon, skal skje på en sikker måte i overensstemmelse med personopplysningslovgivningen og krav fastsatt av Bits.

16 Ansvar

Deltager er erstatningsansvarlig for tap en annen deltager har lidt som følge av at den annen deltager eller kunde denne deltager har inngått avtale om BankID med, har stolt på et BankID, dersom deltager eller noen deltager hefter for (for eksempel en underleverandør eller fellesutsteder), har opptrådt uaktsomt i forbindelse med utstedelse, bruk eller validering av BankID.

Ved følgende skadeårsaker må deltager godtgjøre at den eller noen deltager hefter for, ikke har handlet uaktsomt («omvendt bevisbyrde»):

- a. BankID ble utlevert til uvedkommende,
- b. de obligatoriske minimumsopplysninger som ble lagt inn i BankID ikke var korrekte på utstedelsestidspunktet,
- c. BankID ikke inneholdt alle opplysninger som kreves i henhold til dette regelverket, ref. pkt. 7,
- d. deltager ikke har benyttet forsvarlige produkter og systemer for utstedelse av BankID og fremstilling av digital signatur,
- e. deltager ikke registrerte sin kundes/sertifikatholders tapsmelding eller sperring av BankID på korrekt måte og av denne grunn ga uriktig svar på en valideringsforespørsel.

Deltager er ikke erstatningsansvarlig etter reglene over for skade som skyldes at sertifikatet er brukt utenfor et nærmere angitt anvendelsesområde som klart er gjort kjent for den som har stolt på et BankID.

Deltagers ansvar etter første og andre ledd er i alle tilfeller begrenset til kr. 100.000,- for hver transaksjon.

Deltager er ikke erstatningsansvarlig for tap annen deltager har lidt som følge av at den annen deltager eller dens kunde har benyttet BankID som grunnlag for utstedelse av elektronisk sertifikat.

Hvis en deltager overfor egne kunder (sertifikatholdere) velger å validere BankID som en annen deltager har inngått avtale om uten å foreta kontroller som nevnt i pkt. 13, er den andre

deltageren ikke ansvarlig for eventuelle tap som følge av dette, med mindre den kan holdes ansvarlig på annet grunnlag.

Alminnelig regelverk om ansvarsregulering mellom banker ved betalingsformidling kommer for øvrig til anvendelse så langt de passer.

Ved bruk av BankID som er uberettiget fremstilt (dvs. falske BankID), og det for fremstillingen er benyttet nøkler som eies av Finans Norge Servicekontor, skal eventuelt tap dekkes av alle deltakere i forhold til det antall BankID de har inngått avtale om ved siste årsskifte før tapstidspunktet.

Brudd på Regler om BankID kan medføre sanksjoner etter Alminnelig regelverk for ansvarsregulering mellom banker ved betalingsformidling så langt de passer, samt ileggelse av reaksjon fra Bits dersom forholdet innebærer en betydelig sikkerhets- og tapsrisiko for andre deltakere.

17 Tap av retten til å utstede eller inngå avtale om BankID

En deltager kan fratras retten til å utstede eller inngå avtale om BankID dersom deltageren ved grov uaktsomhet eller forsett overtrer bestemmelser fastsatt i eller i medhold av disse regler. Alminnelig regelverk om ansvarsregulering mellom banker ved betalingsformidling pkt. 10 kommer til anvendelse så langt det passer ved vurderingen av om deltagerens rett til å utstede eller inngå avtale om BankID skal suspenderes eller tilbakekalles, eller om andre reaksjonsmidler skal tas i bruk overfor deltageren. Saksbehandlings- og klagereglene i regelverkets pkt. 11 til 12 får tilsvarende anvendelse så langt de passer.

En deltager som settes under offentlig administrasjon eller annen insolvensbehandling taper straks retten til å utstede eller inngå avtale om BankID. Deltageren kan likevel få tilbake retten til å utstede eller inngå avtale om BankID dersom administrasjonsstyret fullt ut påtar seg deltagerens forpliktelser og ansvar etter disse regler og lovgivning på området.

Bits kan sperre (suspendere eller trekke tilbake) et nivå 1-sertifikat dersom

- den som sertifikatet er utstedt til taper retten til å utstede eller inngå avtale om BankID eller opphører med sin virksomhet,
- Bits trekker tilbake godkjenning for en fellesutsteder, eller
- endringer i eierforhold, styresammensetning, manglende soliditet, manglende sikkerhetsrutiner eller andre grunner gjør at en fellesutsteder ikke oppfyller de krav man må kunne stille til slik utsteder.

Dersom en av flere deltakere som benytter fellesutsteder taper retten til å inngå avtale om BankID eller opphører med sin virksomhet, treffer Bits nærmere beslutninger om eventuell sperring av nivå 1-sertifikat.

Fratas noen retten til å utstede eller inngå avtale om BankID etter reglene i dette punkt, skal alle BankID som vedkommende har utstedt eller inngått avtale om, bli sperret uten nærmere beslutning. Det samme gjelder for BankID som er utstedt på grunnlag av et nivå 1-sertifikat som blir sperret.

Hvis en deltager settes under offentlig administrasjon eller annen insolvensbehandling, kan Bits etter søknad fra Bankenes Sikringsfond beslutte at sperring av BankID til fysiske personer som

deltager har utstedt eller inngått avtale om, utsettes i inntil tre måneder. Bankenes sikringsfond må i så fall påta seg deltagerens forpliktelser og oppgaver som utsteder, herunder det ansvar som følger av lov og disse Regler om BankID.

18 Fortolkning av reglene. Tvister

Oppstår det tvist mellom deltagere eller tvil om fortolkningen eller praktiseringen av disse reglene, kan deltageren eller Bits bringe saken inn for Finans Norges Fagutvalg kontrakt til uttalelse eller avgjørelse. Nærmere regler om behandling og avgjørelse i utvalget fremgår av Regelverk for tvisteløsning i Fagutvalg kontrakt.

19 Statistiske opplysninger om BankID

Deltagerne skal gi Vipps oversikt over antall BankID de har inngått avtale om ved hvert årsskifte. Videre plikter den enkelte deltager å gi statistiske opplysninger om bruk av BankID etter nærmere retningslinjer fastsatt av Vipps.

Bits kan hvert år innhente fra deltagere opplysninger som er nødvendig for å foreta fordeling av ansvar etter pkt. 16 åttende avsnitt.

20 Deltagere som ikke lenger utsteder BankID

En deltager som ikke lenger ønsker å utstede eller inngå avtale om BankID, skal straks melde fra om dette til Bits som vil iverksette nødvendige tiltak slik at deltageren ikke lenger kan utstede eller inngå avtale om BankID.

En deltager som ikke lenger inngår avtale om BankID, skal så lenge sertifikatholderen besitter gyldig BankID som deltageren har inngått avtale om, bekrefte gyldigheten av slike BankID, samt oppbevare informasjon om slike BankID i minst ti år etter siste gang det aktuelle BankID kunne ha vært benyttet av sertifikatholder.

21 Opphør av BankID

Dersom BankID avvikes, har den enkelte deltager plikt til å oppbevare informasjon om BankID den har inngått avtale om og til å bekrefte gyldigheten av slikt BankID i minst ti år etter siste gang det aktuelle BankID kunne ha vært benyttet av sertifikatholder.

22 Endring av reglene

Bits kan med bindende virkning foreta endringer i disse reglene.

23 Definisjoner

Autentisere	Bekreftede identiteten til avsender eller mottaker av et elektronisk dokument.
BankID	Ett eller flere elektroniske sertifikater som en sertifikatholder kan benytte til å sikre elektronisk meldingsutveksling med en annen sertifikatholder.

BankID FOI	Felles underleveranser av operasjoner og prosesser som deltagere og fellesutstedere er forpliktet til å benytte for deler av sin virksomhet relatert til BankID.
Brukersted	Enkeltpersonforetak og annen juridisk person (privat eller offentlig virksomhet og forvaltning) som har fått utstedt BankID for bruk ved kommunikasjon mellom brukerstedet og andre sertifikatholdere.
Fellesutsteder	En juridisk person som utsteder BankID på oppdrag fra en gruppe deltagere og benytter et nivå 1-sertifikat for dette formål. Der hvor Regler om BankID benytter begrepet deltager, gjelder reglene også for fellesutsteder så langt de passer
Gyldig BankID	Et BankID som ikke er tilbakekalt eller suspendert og gyldighetstiden ikke er utløpt.
Nivå 1-sertifikat	Sertifikat utstedt av Finansnæringens Servicekontor/Sparebankforeningens Servicekontor, FNO eller Finans Norge Servicekontor, som benyttes for å signere BankID som utstedes til deltageres kunder.
Sertifikatholder	Fysisk eller juridisk person som har fått utstedt BankID
Sikring av elektronisk meldingsutveksling	Bekreftede rett identitet til partene (autentisering), sikre innholdet mot endring (integritet), knytte meldingen til en bestemt part (ikke-benektning) og/eller skjule innholdet for uvedkommende (kryptere).
Utstede BankID	Signere BankID med utstederens private nøkkel som svarer til offentlig nøkkel i et nivå 1-sertifikat utstedt av Finansnæringens Servicekontor/Sparebankforeningens Servicekontor, FNO eller Finans Norge Servicekontor.