



Stø – BankID praksiserklæring

Versjon	v1.0 – norsk
Ikrafttredelsesdato	1. oktober 2026
Eier	Stø (utsteder / operatør av BankID-ordningen / identitetstilbyder)
Kontakt	policy@sto.no
Omfang	BankID (sikkerhetsnivå høyt) utstedt av Stø

Dokumentkontroll

Dato	Versjon	Beskrivelse av endringer	Godkjent av
23. september 2026	V 1.0-NO		Stø IDLG Policy Board



Dokumentkontroll	2
1 Innledning.....	5
1.1 Oversikt	5
1.2 Rettslig grunnlag	5
1.3 Deltakere	5
1.3.1 Utsteder	5
1.3.2 Registreringsenhet (identitets- og registreringstjenester).....	5
1.3.3 Sluttbrukere	5
1.3.4 Brukersteder	6
1.3.5 Andre underleverandører	6
1.3.6 Tillitsanker.....	6
1.3.7 Tilgjengelighet (universell utforming)	6
1.4 Bruk av BankID	6
1.4.1 Tillatt bruk	6
1.4.2 Forbudt bruk	7
1.4.3 Forvaltning av praksiserklæringen	7
1.5 Definisjoner og forkortelser	7
2 Publisering og ansvar for informasjonsarkiv	10
2.1 Publisering av informasjon om ordningen	10
2.2 Publiseringsfrekvens og kontroll	10
3 Identifisering og autentisering.....	11
3.1 Førstegangs identitetsvalidering (identitetskontroll av søkeren).....	11
3.1.1 Navn og identitetsattributter	12
3.2 Fornøyelse og reaktivering.....	12
3.3 Varsling og håndtering av anmodninger om suspensjon eller tilbakekalling	12
4 Livsløpshåndtering av BankID	14
4.1 Søknad om BankID	14
4.2 Behandling og godkjenning av søknaden.....	14
4.3 Utstedelse av BankID.....	14
4.4 Sluttbrukerens aktivering og bekreftelse	15
4.5 Suspensjon.....	15
4.6 Tilbakekalling.....	16
4.7 Status- og valideringstjenester	16
4.8 Opphør	17
5 Fysiske, organisatoriske og operasjonelle kontroller	18
5.1 Fysiske sikkerhetskontroller.....	18
5.2 Prosesskontroller og personellsikkerhet.....	18
5.3 Kontinuitet og katastrofegjenoppretting	18
5.4 Avvikling av ordningen	19

5.5 Risikostyring og sikkerhetsstyring.....	19
6 Tekniske sikkerhetskontroller	20
6.1 Generelt.....	20
6.2 Beskyttelse av sensitivt kryptografisk materiale	20
6.3 System- og nettverkssikkerhet.....	20
6.4 Sikkerhet i livsløpet til systemer og komponenter	21
7 Logging, overvåking og oppbevaring av dokumentasjon.....	22
7.1 Revisjonslogging og overvåking	22
7.2 Arkivering	22
8 Revisjon og egenerklæring.....	23
9 Andre forretningsmessige og juridiske forhold	24
9.1 Økonomisk ansvar	24
9.2 Konfidensialitet.....	24
9.3 Svindelforebygging og enhets-/risikosignaler.....	24
9.4 Personvern	24
9.5 Immaterielle rettigheter	25
9.6 Erklæringer og garantier	25
9.7 Ansvarsfraskrivelser og ansvarsbegrensninger	25
9.8 Varighet og opphør av praksiserklæringen	26
9.9 Lovvalg og tvisteløsning.....	26



1 Innledning

1.1 Oversikt

Dette dokumentet beskriver hvordan Stø AS («Stø») utsteder, forvalter og drifter BankID som en elektronisk identifikasjonsordning på sikkerhetsnivå høyt, i samsvar med eIDAS-kravene slik de er gjennomført i norsk rett. Dokumentet angir de overordnede rammene for BankID-ordningen, herunder roller og ansvar, utstedelse, bruk, livsløpshåndtering, tekniske og organisatoriske sikkerhetskontroller, logging, arkivering, revisjon og tilsyn.

Kommersielle vilkår, herunder priser, refusjonsbetingelser og vilkår for merkevare og lisensiering, reguleres av separate avtaler og omfattes ikke av dette dokumentet.

Dette dokumentet omfatter ikke andre tjenester som Stø leverer utenfor BankID-ordningen, herunder løsninger for digital identitetskontroll, tillitstjenester, KYC/AML-tjenester eller andre tilgrensende tjenester.

1.2 Rettslig grunnlag

BankID-ordningen som beskrives i dette dokumentet, bygger på eIDAS-forordningen (EU) nr. 910/2014 og Kommisjonens gjennomføringsforordning (EU) 2015/1502, slik regelverket er gjennomført i norsk rett. BankID utstedes og forvaltes som en elektronisk identifikasjonsordning på sikkerhetsnivå høyt.

Dette dokumentet angir Støs overordnede praksis for å oppfylle kravene til sikkerhetsnivå høyt, herunder krav til identitetskontroll, utstedelse, livsløpshåndtering, autentisering, tekniske og organisatoriske sikkerhetstiltak, logging, arkivering og revisjon.

Tekniske spesifikasjoner, herunder PKI- og kryptografiske detaljer, arkitektur, grensesnitt og operasjonelle krav, er beskrevet i kontrollert teknisk dokumentasjon.

Vedlegg 1 inneholder en tabell som knytter kapitlene i dette dokumentet til de relevante kravene i vedlegget til Kommisjonens gjennomføringsforordning (EU) 2015/1502.

1.3 Deltakere

1.3.1 Utsteder

Stø er et norsk selskap og eneste utsteder av BankID i Norge. Stø er ansvarlig for utstedelse, forvaltning, suspensjon, tilbakekalling og samlet drift av BankID-ordningen, herunder stabil og sikker leveranse av tjenesten.

Stø skal oppfylle pliktene som gjelder for utstedere av elektroniske identifikasjonsmidler på sikkerhetsnivå høyt. Dette omfatter blant annet å drifte og sikre systemene som understøtter utstedelse og bruk av BankID, tilby status- og valideringstjenester og opprettholde kontinuitet, sikkerhet og etterlevelse i ordningen.

1.3.2 Registreringsenhet (RA)

Registreringsenheter er juridiske personer som, etter avtale med Stø, kan utføre oppgaver knyttet til identitetskontroll og registrering i forbindelse med utstedelse og livsløpshåndtering av BankID. Dette kan omfatte kontroll av søkerens identitet, gjennomgang av søknadsopplysninger, registrering av personopplysninger og anmodning om utstedelse til Stø.

Registreringsenheter opptrer på vegne av Stø innenfor rammen av avtalen og etablerte prosedyrer. De skal oppfylle relevante sikkerhets-, konfidensialitets-, personvern- og revisjonskrav når de utfører oppgaver for BankID-ordningen. Stø skal ha avtaler, prosedyrer

og kontrollmekanismer som sikrer en ensartet og etterprøvbar praksis hos registreringsenhetene.

1.3.3 Sluttbrukere

Sluttbrukere er fysiske personer som får utstedt BankID på bakgrunn av identitetskontroll, registrering og aksept av gjeldende avtalevilkår. BankID er personlig og skal bare brukes av sluttbrukeren selv.

Sluttbrukeren skal beskytte BankID og tilhørende autentiseringsfaktorer, herunder passord, koder og andre hemmeligheter som brukes ved autentisering. Sluttbrukeren skal varsle Stø eller registreringsenheten uten ugrunnet opphold ved mistanke om misbruk, kompromittering, tap av kontroll eller feil i registrerte opplysninger.

1.3.4 Brukersteder

Brukersteder er juridiske personer som godtar BankID som elektronisk identifikasjonsmiddel for fysiske personer, og som bruker tjenesten til å verifisere sluttbrukerens identitet.

Før et brukersted kan bruke BankID, må det foreligge avtale med Stø eller en autorisert avtalepart, og brukerstedet må identifiseres og verifiseres i samsvar med etablerte prosedyrer. Kontrollene kan omfatte foretaksopplysninger, representasjonsrett, fullmakt eller prokura, firmaattest eller tilsvarende dokumentasjon, og vurdering av rettslig grunnlag der brukerstedet mottar eller behandler fødselsnummer eller andre identitetsopplysninger.

Brukerstedet skal overholde gjeldende vilkår, tekniske krav og sikkerhetskrav for bruk av BankID, herunder krav til integrasjon, validering av BankID-resultater, beskyttelse av eget integrasjonsmiljø og rapportering av misbruk, svindel eller sikkerhetshendelser. Stø eller en autorisert avtalepart kan suspendere, tilbakekalle eller avslutte brukerstedets tilgang til BankID dersom vilkårene ikke lenger er oppfylt, det foreligger mistanke om misbruk eller sikkerhetsbrudd, eller dette følger av avtale, lov eller krav fra relevant myndighet.

1.3.5 Underleverandører og tjenesteleverandører

Stø kan benytte underleverandører og tjenesteleverandører for operasjonelle eller tekniske deler av BankID-tjenesten, herunder teknisk infrastruktur, datasentertjenester, sikkerhetstjenester eller komponenter for identitetskontroll.

Slike oppgaver utføres under Støs ansvar og reguleres ved avtale. Stø skal påse at leverandørene oppfyller relevante krav til sikkerhet, konfidensialitet, personvern, drift og etterlevelse. Stø beholder det overordnede ansvaret for oppgaver som utføres av underleverandører og tjenesteleverandører.

1.3.6 Tillitsanker

I BankIDs tillitshierarki er tillitsankeret den øverste tillitskomponenten, som forvaltes av Finans Norge. Tillitsankerfunksjonen inngår i det samlede styrings- og tillitsrammeverket for BankID og påvirker ikke Støs rolle som utsteder og operatør av BankID-ordningen.

1.3.7 Tilgjengelighet og universell utforming

BankID skal være tilgjengelig for personer med nedsatt funksjonsevne og oppfylle relevante krav til universell utforming og tilgjengelighet der dette følger av norsk rett. Registrerings-, utstedelses- og bruksprosesser skal så langt det er relevant være ikke-diskriminerende og ivareta gjeldende tilgjengelighetskrav.

1.4 Bruk av BankID

1.4.1 Tillatt bruk



BankID kan brukes som elektronisk identifikasjonsmiddel for personidentifikasjon og autentisering i tjenester som har avtale om bruk av BankID. Dette omfatter blant annet nettbank, offentlige digitale tjenester og private brukersteder som er godkjent for bruk av BankID på sikkerhetsnivå høyt.

BankID skal bare brukes innenfor de formålene og bruksområdene som følger av gjeldende avtaler, BankID-vilkår, teknisk dokumentasjon og kravene til sikkerhetsnivå høyt.

1.4.2 Forbudt bruk

BankID skal ikke brukes i strid med BankID-vilkårene, gjeldende avtaler, relevant teknisk dokumentasjon eller på måter som kan svekke sikkerheten, integriteten, tilgjengeligheten eller tilliten til BankID-ordningen.

Sluttbrukere og brukersteder skal ikke dele, omgå, manipulere eller forsøke å misbruke BankID, autentiseringsfaktorer, integrasjoner, valideringssvar eller andre deler av tjenesten. Slik bruk kan medføre suspensjon, tilbakekalling, avslutning av tilgang eller andre tiltak etter avtale eller gjeldende rett.

1.4.3 Forvaltning av praksiserklæringen

Dette dokumentet forvaltes av Stø, som er ansvarlig for å gjennomgå, godkjenne, publisere og vedlikeholde dokumentet i samsvar med etablerte styringsprosesser. Vesentlige endringer skal behandles og formelt godkjennes før ny versjon publiseres.

Endringer i regelverk, standarder, sikkerhetskrav, risikobilde eller operasjonelle forhold kan medføre behov for å endre praksis eller oppdatere dette dokumentet. Godkjente versjoner skal publiseres på Støs nettsider sammen med en beskrivelse av vesentlige endringer.

Spørsmål om dette dokumentet kan rettes til Stø ved bruk av kontaktopplysningene nedenfor.

Postadresse: Stø AS, Postboks 9236 Grønland, N-0134 Oslo, Norge

Kundeservice og hendelsesrapportering: BankIDs hjelpesider

Policyhenvendelser: policy@stoe.no

1.5 Definisjoner og forkortelser

Følgende sentrale begreper og forkortelser gjelder for dette dokumentet:

Begrep	Definisjon
Søker	En fysisk person som søker om utstedelse av BankID, og som ennå ikke har fått utstedt et elektronisk identifikasjonsmiddel.
Sikkerhetsnivå høyt	Det høyeste sikkerhetsnivået som fastsatt ved lov, som gir svært høy tillit til en persons påberopte identitet, og som krever robust identitetsbekreftelse og sterke autentiseringsmekanismer.
Autentisering	Prosessen med å bekrefte at en påberopt identitet er ekte basert på bruk av et elektronisk identifikasjonsmiddel.
Autentiseringsmiddel	En mekanisme eller enhet som sluttbrukeren bruker for å autentisere seg, for eksempel en mobilapplikasjon, en maskinvarebrikke eller et passord.
Revisjonslogg	En kronologisk oversikt over hendelser og handlinger knyttet til utstedelse, forvaltning og bruk av BankID.

BankID	BankID-ordningen i Norge, utstedt av Stø på sikkerhetsnivå høyt.
Legitimasjon	Kombinasjonen av identitetsdata og autentiseringsmiddel som utstedes til en sluttbruker, og som gjør det mulig å autentisere seg mot nettbaserte tjenester.
Behandlingsansvarlig	Den fysiske eller juridiske personen som bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal brukes i henhold til personvernforordningen artikkel 4 nr. 7.
eIDAS-forordningen	Forordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked, som utgjør det rettslige grunnlaget for sikkerhetsnivåer for eID og for gjensidig anerkjennelse over landegrensene i EØS.
Elektronisk identifikasjonsmiddel	En materiell og/eller immateriell enhet som inneholder personidentifikasjonsdata, og som brukes til autentisering mot en nettbasert tjeneste.
Sluttbruker	En fysisk person som har fått utstedt BankID, og som er ansvarlig for riktig bruk og beskyttelse av identitetsmiddelet.
Utløp	Den naturlige avslutningen av gyldighetsperioden til en BankID, hvorefter BankID ikke lenger kan brukes og må fornyes eller utstedes på nytt.
Identitetsbekreftelse	De trinnene og prosedyrene som brukes for å fastslå og validere en søkers identitet før et elektronisk identifikasjonsmiddel utstedes.
Identitetskontroll	Prosessen med å bekrefte at en persons påberopte identitet svarer til personens virkelige identitet, gjennomført før utstedelse av BankID.
Utstedelse	Prosessen med å opprette, knytte og levere BankID til en verifisert sluttbruker, etter gjennomført identitetsbekreftelse og registrering.
Utsteder / operatør av ordningen	Stø AS, den juridiske enheten som er ansvarlig for å utstede og drifte BankID.
Sikkerhetsnivå (Level of Assurance, LoA)	Et mål på tilliten til prosessen for identitetskontroll og utstedelse, slik det er definert i eIDAS-forordningen artikkel 8.
Personopplysninger	Enhver opplysning om en identifisert eller identifiserbar fysisk person, slik det er definert i personvernforordningen (GDPR) artikkel 4 nr. 1.
Praksiserklæring (Practice Statement, PS)	Dette dokumentet, som beskriver selskapets praksis og regler for utstedelse og drift av BankID.
Reaktivering	Oppheving av en midlertidig suspensjon der grunnlaget for suspensjonen ikke lenger foreligger, og ordningens vilkår er oppfylt.
Registreringsenhet (RA)	En enhet som Stø har delegert myndighet til for å utføre oppgaver knyttet til identitetskontroll, registrering og visse livsløpsoppgaver ved utstedelse og forvaltning av BankID, for eksempel en BankID Fullmektig eller en annen autorisert partner.
Brukersted (avhengig part)	En enhet som benytter BankID til identifisering eller autentisering av en bruker.
Fornøyelse / ny utstedelse	Prosessen med å utstede en ny BankID til en sluttbruker etter utløp eller tap av en eksisterende BankID, i samsvar med gjeldende krav til identitetskontroll.



Tilbakekalling	Permanent ugyldiggjøring av en BankID før utløp.
Suspensjon	Midlertidig deaktivering av BankID.
Validering	Prosessen med å fastslå om en BankID er gyldig, suspendert, tilbakekalt eller ukjent.

2 Publisering og ansvar for informasjonsarkiv

2.1 Publisering av informasjon om ordningen

Stø publiserer informasjon om BankID-ordningen på sine nettsider. Offentlig tilgjengelig informasjon omfatter denne praksiserklæringen, informasjon som er nødvendig for å validere BankID, kontaktinformasjon for kundeservice og hendelsesrapportering, og henvisninger til relevant teknisk eller operasjonell dokumentasjon for bruk av tjenesten, herunder for brukere og brukersteder, revisjoner eller tilsyn.

Informasjonen skal være tilgjengelig for sluttbrukere, brukersteder, registreringsenheter, tilsynsmyndigheter og andre relevante parter i den grad informasjonen er offentlig eller ellers skal gjøres tilgjengelig etter gjeldende krav.

2.2 Publiseringsfrekvens og kontroll

Når dette dokumentet eller annen offentlig tilgjengelig informasjon om BankID-ordningen oppdateres, publiseres den nyeste godkjente versjonen uten ugrunnet opphold.

Mindre endringer kan publiseres løpende uten særskilt varsel. Vesentlige endringer og nye dokumentversjoner skal publiseres eller varsles på egnet måte og i henhold til avtale før de trer i kraft, slik at berørte parter får rimelig tid til å innrette seg.

Status- og valideringstjenester oppdateres etter behov, slik at brukersteder kan fastslå om en BankID er gyldig, suspendert eller tilbakekalt.

Bare autorisert personell kan publisere eller endre informasjon og dokumenter på selskapets nettsider. Publisering og endringer skal skje i samsvar med gjeldende prosedyrer for endringshåndtering og skal logges. Integriteten til publiserte dokumenter og tjenester skal beskyttes med egnede tekniske og organisatoriske tiltak.

Sensitiv informasjon, herunder detaljerte logger, interne prosedyrer og annen informasjon som ikke er ment for offentlig deling, skal lagres i sikre systemer og ikke gjøres offentlig tilgjengelig.



3 Identifisering og autentisering

3.1 Identitetskontroll

Før BankID utstedes til en søker, skal søkerens identitet kontrolleres i samsvar med kravene til eID på sikkerhetsnivå høyt. Identitetskontrollen gjennomføres av Stø eller av en autorisert registreringsenhet som opptrer på vegne av Stø. Stø beholder ansvaret for at kontrollen oppfyller gjeldende krav.

BankID utstedes bare til fysiske personer som oppfyller kravene for utstedelse. Søkeren skal være registrert i Folkeregisteret med et unikt identifikasjonsnummer, og de identitetsopplysningene som legges til grunn for BankID, skal kontrolleres mot Folkeregisteret eller annen autoritativ kilde der dette er relevant. Pseudonymer og anonym utstedelse er ikke tillatt for BankID på sikkerhetsnivå høyt.

Alder og rettslig handleevne

For å inngå avtale om BankID må søkeren være minst 12 år. For mindreårige under 18 år kreves samtykke fra verge. Dersom den mindreårige har flere verger, kreves samtykke fra samtlige. Fullmakter, samtykker eller annen dokumentasjon på vergemyndighet skal dokumenteres. BankID skal ikke utstedes dersom søkeren mangler nødvendig rettslig handleevne, er fratatt rettslig handleevne på en måte som er relevant for utstedelsen, eller er under vergemål på en måte som innebærer at BankID ikke skal brukes av søkeren alene.

Identitetsdokumenter og dokumentkontroll

Identitetskontrollen skal bygge på legitimasjonsbevis som er godkjent i henhold til norsk lov, herunder norsk nasjonalt ID-kort, pass eller andre identitetsdokumenter, samt tidligere utstedt og gyldig BankID på sikkerhetsnivå høyt.

Fysiske identitetsdokumenter skal kontrolleres i samsvar med etablerte prosedyrer. Der dokumenttypen og kontrollmetoden krever det, skal dokumentet leses elektronisk og kontrolleres mot relevante autoritative eller anerkjente kilder, herunder TOVE-systemet for norske pass og nasjonale ID-kort. Dersom elektronisk lesing eller nødvendig kildekontroll ikke kan gjennomføres der dette er påkrevd, skal identitetskontrollen avbrytes, og BankID skal ikke utstedes på grunnlag av den aktuelle kontrollen.

Identitetskontrollen skal dokumenteres. Registreringsenheten skal registrere hvilket legitimasjonsbevis som ble framlagt, hvilke kontroller som ble gjennomført, og resultatet av kontrollene. Dokumentasjon fra identitetskontrollen, herunder relevant identitetsdokumentasjon og nødvendige person- og kontaktopplysninger, skal lagres sikkert i samsvar med etablerte prosedyrer og gjøres tilgjengelig for Stø når det er nødvendig for revisjon, tilsyn, etterlevelseskontroll eller oppfølging av konkrete saker.

BankID utstedes ikke før søkerens identitet er tilstrekkelig kontrollert. Dersom identitetskontrollen ikke kan gjennomføres i samsvar med kravene til sikkerhetsnivå høyt, eller det foreligger uavklarte avvik, mistanke om falsk dokumentasjon, dobbeltregistrering eller andre forhold som kan svekke tilliten til identiteten, skal søknaden avslås, settes på vent eller eskaleres til manuell behandling.

Identitetsdokumenter må kunne knyttes til Folkeregisteret

For nye søkere må det framlagte identitetsdokumentet entydig knytte personen til et norsk fødselsnummer eller D-nummer i Folkeregisteret. For personer med D-nummer forutsetter utstedelse at identitets- og dokumentkontroll med personlig oppmøte er gjennomført hos Skatteetaten eller annen relevant myndighet, slik at identitetsgrunnlaget i Folkeregisteret viser at identiteten er kontrollert.

Personlig oppmøte eller godkjent elektronisk kontroll

Ved førstegangsutstedelse skal identitetskontroll gjennomføres ved personlig oppmøte hos en registreringsenhet, med mindre BankID-ordningen uttrykkelig tillater en elektronisk kontroll som gir tilsvarende sikkerhet. Elektronisk identitetskontroll kan bare benyttes i kontrollerte prosesser som er godkjent av Stø, for eksempel ved fornyelse eller ny utstedelse til samme fysiske person basert på en eksisterende gyldig BankID.

Godkjente elektroniske metoder og bruk av eksisterende eID

Der BankID-ordningen tillater det, kan et eksisterende gyldig elektronisk identitetsmiddel benyttes i kontrollerte prosesser for fornyelse eller ny utstedelse til samme fysiske person, forutsatt at de relevante identitetsattributtene bekreftes ved oppslag mot Folkeregisteret eller annen autoritativ kilde.

Kontroll mot autoritative kilder

Stø eller registreringsenheten skal kontrollere at identitetsattributtene som brukes ved utstedelse, er konsistente med opplysningene som er registrert om søkeren i Folkeregisteret. Kontrollen gjennomføres ved førstegangsutstedelse og der fornyelse eller ny utstedelse bygger på et eksisterende gyldig elektronisk identitetsmiddel.

Delegert identitetskontroll

Identitetskontroll som helt eller delvis utføres av en tredjepart på vegne av Stø, skal oppfylle de samme kravene som om Stø hadde gjennomført kontrollen selv. Stø skal ha avtaler, prosedyrer og kontrollmekanismer som sikrer at registreringsenheter og andre autoriserte parter oppfyller kravene til sikkerhetsnivå høyt.

3.2 Fornyelse og reaktivering

Fornyelse og reaktivering av BankID skal opprettholde samme sikkerhetsnivå som ved førstegangsutstedelse, og BankID skal fortsatt være knyttet til samme verifiserte fysiske person.

Fornyelse kan, der BankID-ordningen og gjeldende rett tillater det, bygge på en eksisterende gyldig BankID for samme fysiske person. Stø skal da kontrollere at relevante identitetsattributter fortsatt er korrekte ved oppslag mot Folkeregisteret eller annen autoritativ kilde.

Dersom fornyelse ikke kan bygge på en eksisterende gyldig BankID, skal sluttbrukeren gjennomgå ny identitetskontroll som oppfyller kravene til sikkerhetsnivå høyt.

Reaktivering kan bare skje når årsaken til suspensjonen er avklart eller ikke lenger foreligger, og vilkårene for reaktivering er oppfylt. Før reaktivering skal Stø eller registreringsenheten kontrollere at sluttbrukeren fortsatt er korrekt identifisert og har kontroll over BankID eller relevante autentiseringsfaktorer.

Nærmere regler om suspensjon, reaktivering og tilbakekalling framgår av kapittel 4.5, 4.6 og 4.7.

3.3 Varsling og håndtering av anmodninger om suspensjon eller tilbakekalling

Mistenker sluttbruker urettmessig bruk av sin BankID, mister kontrollen over BankID eller en tilhørende autentiseringsfaktor, eller av andre grunner har behov for at BankID suspenderes eller tilbakekalles, skal sluttbrukeren varsle Stø eller registreringsenheten uten ugrunnet opphold. Varsler som kan påvirke gyldigheten av BankID, skal mottas og håndteres raskt for å hindre misbruk eller begrense skade.



Stø som utsteder skal ha egnede prosedyrer for å motta og håndtere varsler fra sluttbrukere, registreringsenheter og andre autoriserte kilder om mistanke om misbruk, tap, kompromittering eller andre forhold som kan gi grunnlag for suspensjon eller tilbakekalling. Stø eller registreringsenheten kan iverksette rimelige tiltak for å bekrefte identiteten til den som varsler, eller på annen måte verifisere varselets troverdighet. Behovet for rask handling skal veies mot behovet for å unngå uriktige tiltak.

På grunnlag av et varsel, eller der sikkerhetshensyn, rettslige krav eller krav etter BankID-ordningen ellers tilsier det, kan Stø suspendere eller tilbakekalle BankID. Suspensjon, tilbakekalling og eventuell reaktivering gjennomføres av Stø i samsvar med etablerte operasjonelle prosesser. Dersom anmodningen kommer fra en registreringsenhet eller annen autorisert kilde, skal grunnlaget være tilstrekkelig dokumentert før tiltaket iverksettes, med mindre umiddelbar suspensjon eller tilbakekalling er nødvendig for å hindre misbruk eller begrense skade.

Nærmere regler om suspensjon, tilbakekalling, reaktivering og formidling av status framgår av kapittel 4.5 til 4.7.

4 Livsløpshåndtering av BankID

Dette kapittelet gir en oversikt over livsløpsprosessene for BankID, fra søknad og utstedelse til eventuell suspensjon eller tilbakekalling, og beskriver roller og ansvar i hver fase. Detaljerte operasjonelle prosedyrer er dokumentert i interne håndbøker og tekniske retningslinjer.

4.1 Søknad om BankID

Søknadsprosessen starter når søkeren ber om å få BankID, for eksempel i forbindelse med åpning av bankkonto, ved personlig oppmøte hos en registreringsenhet og/eller gjennom et elektronisk søknadsløp der dette er tillatt. Registreringsenheten innhenter nødvendige personopplysninger fra søkeren, herunder fullt navn, fødselsnummer og kontaktopplysninger. Dette skjer normalt som del av søknads- og identitetskontrollprosessen.

Søkeren må akseptere gjeldende BankID-vilkår ved søknadstidspunktet. Aksept kan gis ved fysisk eller elektronisk signatur eller registreres gjennom en autentisert handling.

Registreringsenheten vurderer om søknadsopplysningene er fullstendige og korrekte, og om søkeren oppfyller kravene for å få utstedt BankID.

Utstedelse og aktivering skjer ikke før identitetskontrollen som kreves etter kapittel 3.1, og alle relevante kontrolltrinn er gjennomført.

4.2 Behandling og godkjenning av søknaden

Etter at identitetskontrollen er gjennomført, behandler Stø anmodningen om utstedelse av BankID. Stø kontrollerer at registreringsenheten er autorisert, at anmodningen er sendt inn gjennom en godkjent og sikker kanal, og at de innsendte opplysningene er fullstendige og konsistente med kravene til utstedelse.

Støs systemer kan gjennomføre automatiserte kontroller av innsendte opplysninger, herunder kontroll av at fødselsnummeret har gyldig format, at identitetsattributtene er konsistente, og at søkeren ikke allerede har en aktiv BankID i strid med gjeldende krav. Manuelle kontroller kan gjennomføres ved avvik, usikkerhet eller som del av stikkprøvebasert kvalitetssikring.

Dersom anmodningen godkjennes, klargjøres BankID med korrekte identitetsopplysninger og attributter i samsvar med gjeldende krav, og Stø godkjenner utstedelsen. Godkjenningen kan gjennomføres gjennom automatiserte systemer som opptrer på vegne av Stø.

Dersom kravene for utstedelse ikke er oppfylt, skal søknaden avslås, settes på vent eller returneres til registreringsenheten for avklaring i samsvar med etablerte prosedyrer. Avvik, mangelfull dokumentasjon, mistanke om dobbeltregistrering eller andre forhold som kan påvirke tilliten til identiteten eller utstedelsen, skal være avklart før BankID utstedes.

4.3 Utstedelse av BankID

Etter godkjent anmodning om utstedelse oppretter Stø BankID og knytter den til sluttbrukerens verifiserte identitet og relevante identitetsattributter. BankID kan ikke tas i bruk før sluttbrukeren har gjennomført aktiveringsprosessen.

BankID utstedes med identitetsopplysninger, unik sluttbrukeridentifikator, gyldighetsperiode og sikkerhetsattributter i samsvar med gjeldende krav. Tekniske formater, profiler, sertifikatinnhold og kryptografiske parametere er beskrevet i kontrollert teknisk dokumentasjon.



BankID har en maksimal gyldighet på to år. Sluttbrukere varsles i forkant av utløp. For fortsatt bruk må BankID fornyes før utløp. Dersom BankID ikke fornyes før utløp, opphører den å være gyldig, og det kreves ny søknads- og utstedelsesprosess.

4.4 Levering og aktivering

BankID er et serverbasert elektronisk identifikasjonsmiddel. Den private nøkkelen og tilhørende sertifikat genereres og oppbevares i Støs sentrale infrastruktur og overføres ikke til sluttbrukeren. Sluttbrukerens kontroll over BankID etableres gjennom autentiseringsfaktorer som er knyttet til sluttbrukerens verifiserte identitet.

Ingen autentiseringsfaktor kan leveres til eller aktiveres av en sluttbruker uten at sluttbrukerens identitet er kontrollert på leveringstidspunktet. Aktivering kan gjennomføres på ulike måter avhengig av hvilken autentiseringsfaktor som benyttes. Aktivering basert på en OTP-enhet eller annen fysisk autentiseringsenhet krever personlig oppmøte og identitetskontroll før BankID kan tas i bruk. Aktivering av BankID-appen gjennomføres digitalt ved bruk av godkjent ID-kontroll i appen, som omfatter kontroll av identitetsdokument og sammenligning med ansiktsskanning av sluttbrukeren, herunder «liveness-sjekk».

Aktiveringsprosessen skal sikre at BankID knyttes til den personen den er utstedt til, og at ingen annen person får kontroll over BankID eller tilhørende autentiseringsfaktorer. Ved utskifting, fornyelse og reaktivering gjelder samme krav som ved første gangs utstedelse. BankID kan ikke tas i bruk før aktiveringen er fullført.

For OTP-enheter og andre fysiske autentiseringsenheter skal utstedelse, levering, aktivering, administrasjon, suspensjon og eventuell utskifting gjennomføres i samsvar med etablerte prosedyrer og gjeldende BankID-krav. Registreringsenheten skal dokumentere sin praksis for håndtering av slike enheter og gjøre dokumentasjonen tilgjengelig for Stø når det er nødvendig for revisjoner, tilsyn, etterlevelseskontroller eller oppfølging av konkrete saker.

Sluttbrukeren skal gjennomføre de foreskrevne aktiveringstrinnene før første bruk. Aktiveringen skal omfatte nødvendige kontroller for å bekrefte at det er rett sluttbruker som aktiverer BankID, og at ingen annen person får kontroll over BankID eller autentiseringsfaktorer.

Aktiveringen etablerer eller bekrefter sluttbrukerens autentiseringsfaktorer. Faktorer, aktiveringskoder og andre data som brukes i aktiveringsprosessen, skal etableres, overføres og lagres slik at de er beskyttet mot avsløring, kopiering og urettmessig bruk.

Dersom sluttbrukeren oppdager en feil, ikke får gjennomført aktiveringen, eller mener at en annen person kan ha fått kontroll over BankID eller en autentiseringsfaktor, skal BankID ikke tas i bruk, og forholdet skal rapporteres til Stø eller registreringsenheten (banken) uten ugrunnet opphold.

4.5 Suspensjon

Suspensjon innebærer at BankID deaktiveres midlertidig. Suspensjon kan benyttes når det er behov for å hindre bruk i en avgrenset periode, for eksempel ved mistanke om misbruk eller svindel, mistanke om at BankID brukes av en annen enn sluttbrukeren, tap av kontroll over BankID eller en tilhørende autentiseringsfaktor, eller mens en sikkerhets- eller svindelundersøkelse pågår.

Suspensjon gjennomføres av Stø i samsvar med etablerte operasjonelle prosesser. I den ordinære prosessen iverksettes suspensjon normalt på grunnlag av varsel fra sluttbrukeren eller anmodning fra registreringsenheten. Stø kan også suspendere BankID når sikkerhetshensyn, svindelforebyggende kontroller, rettslige krav eller andre begrunnede forhold knyttet til BankID tilsier det.

Når BankID suspenderes, skal sluttbrukeren varsles uten ugrunnet opphold i samsvar med etablerte prosedyrer, med mindre varsling må utsettes av sikkerhetsmessige, rettslige eller etterforskningsmessige grunner. Varselet skal opplyse om at BankID er suspendert og gi nødvendig informasjon om videre framgangsmåte.

Suspensjon skal være midlertidig og bare være så lenge grunnlaget for suspensjonen foreligger. BankID kan ikke brukes mens den er suspendert, og statusen «suspendert» skal framgå av status- og valideringstjenestene.

En suspendert BankID kan reaktiveres når årsaken til suspensjonen er avklart eller ikke lenger foreligger, og vilkårene for reaktivering er oppfylt. Før reaktivering skal Stø eller registreringsenheten kontrollere at grunnlaget for suspensjonen er håndtert, og at sluttbrukeren fortsatt er korrekt identifisert og har kontroll over BankID. Dersom BankID ikke kan reaktiveres innen 30 dager etter at den ble suspendert, skal den tilbakekalles. En BankID som er tilbakekalt kan ikke reaktiveres.

4.6 Tilbakekalling

Tilbakekalling innebærer at BankID deaktiveres permanent før utløp. En tilbakekalt BankID kan ikke reaktiveres eller gjenopprettes.

Stø kan tilbakekalle BankID når det foreligger grunnlag som tilsier at BankID ikke lenger skal være aktiv. Dette omfatter blant annet varsel fra sluttbrukeren eller sluttbrukerens rettslige representant, pålitelig informasjon om at sluttbrukeren er død, mistanke om misbruk eller svindel, tap av kontroll over BankID eller tilhørende autentiseringsfaktor, kompromittering av koder, passord eller andre hemmeligheter, brudd på BankID-vilkårene, uriktige eller utdaterte registrerte opplysninger, utstedelse på uriktig grunnlag, eller rettsavgjørelse, krav fra relevant myndighet eller annet rettslig krav.

Tilbakekalling kan gjennomføres umiddelbart når misbruk er avdekket, når det foreligger mistanke om at BankID brukes av en uvedkommende, eller når sikkerhetshensyn, rettslige krav eller krav etter BankID-ordningen tilsier det. Før tilbakekalling skal grunnlaget dokumenteres i samsvar med etablerte prosedyrer, med mindre umiddelbar tilbakekalling er nødvendig for å hindre misbruk eller begrense skade.

Sluttbrukeren skal uten ugrunnet opphold varsle Stø eller registreringsenheten dersom BankID er eller kan være kompromittert, dersom sluttbrukeren mister kontrollen over BankID eller en autentiseringsfaktor, eller dersom det ellers er behov for å sperre eller tilbakekalle BankID. Stø skal ha tilgjengelige kanaler for mottak og håndtering av slike varsler.

Når BankID tilbakekalles, skal status- og valideringstjenestene oppdateres slik at BankID vises som tilbakekalt. Brukersteder skal kunne fastslå tilbakekallingsstatus gjennom de relevante status- og valideringstjenestene.

Dersom sluttbrukeren har behov for BankID etter tilbakekalling, kreves ny søknad og ny utstedelse i samsvar med gjeldende krav for nyutstedelse av BankID.

4.7 Status- og valideringstjenester

Stø tilbyr status- og valideringstjenester som gjør det mulig å fastslå om en BankID er gyldig, suspendert, tilbakekalt eller ukjent. Tjenestene skal være tilgjengelige og robuste nok til å understøtte sikker bruk av BankID. Den tekniske gjennomføringen er beskrevet i kontrollert teknisk dokumentasjon.

Brukersteder som integrerer BankID-validering, bør konsultere den tekniske integrasjonsdokumentasjonen for opplysninger om endepunktene til valideringstjenesten, formater for forespørsler og svar, og kravet om signerte OCSP-forespørsler.



4.8 Opphør

Når sluttbrukerens BankID-brukeravtale avsluttes, opphører samtidig retten til å bruke BankID. Avslutning av avtalen påvirker ikke Støs plikt til å oppbevare informasjon og dokumentasjon i samsvar med kapittel 7, eller til å oppfylle øvrige plikter knyttet til en allerede utstedt BankID.

5 Fysiske, organisatoriske og operasjonelle kontroller

5.1 Fysiske sikkerhetskontroller

Stø beskytter datasentre og driftssteder som er en del av BankID-tjenesten, med fysiske sikkerhetstiltak.

BankID-systemene er plassert i sikrede datasentre med lagdelt adgangskontroll, og tilgang er begrenset til autorisert personell med sterk autentisering. Kritisk utstyr er beskyttet i definerte sikre soner, inn- og utpasseringer logges, og lokalene overvåkes med egnede sikkerhetstiltak. Fysiske sikkerhetstiltak inspiseres regelmessig for å kontrollere at kravene til fysisk sikkerhet og omgivelsessikkerhet er oppfylt.

5.2 Prosesskontroller og personellsikkerhet

Driften av BankID er underlagt krav til arbeidsdeling, betrodderoller, tilgangsstyring og personellsikkerhet. Kontrollene skal redusere risikoen for feil, misbruk og uautorisert påvirkning av prosesser som er kritiske for utstedelse, drift og forvaltning av BankID.

Kritiske oppgaver fordeles mellom ulike roller slik at én enkelt person ikke får full kontroll over sensitive prosesser. Dette gjelder blant annet kryptografiske operasjoner, endringer i sikkerhetskonsfigurasjon, bakgrunnssjekker, håndtering av revisjonslogger og andre sikkerhetskritiske handlinger. Der det er nødvendig, skal slike oppgaver utføres med tomannskontroll, flerpartskontroll eller tilsvarende sikkerhetstiltak.

Stø definerer hvilke roller og oppgaver som anses som betrodderoller, herunder sikkerhetsansvarlige, RA-ansvarlige, revisjonsansvarlige, systemadministratorer og systemoperatører. Personell i betrodderoller skal ha nødvendig kompetanse, være underlagt konfidensialitetsplikt og bare ha den tilgangen som er nødvendig for å utføre sine oppgaver.

Ansatte skal gjennomgå relevante bakgrunnssjekker før de tildeles betrodderoller. Stø gir nødvendig opplæring til personell som arbeider med BankID, slik at de er kjent med sikkerhetskrav, personvernplikter, konfidensialitet og prosedyrer for rapportering av hendelser.

Driftshåndbøker og sikkerhetsprosedyrer vedlikeholdes og gjøres tilgjengelige for autorisert personell. Etterlevelsen følges opp gjennom interne kontroller og periodiske revisjoner.

5.3 Kontinuitet og katastrofegjenoppretting

Stø har planer for virksomhetskontinuitet og beredskapsplaner for katastrofegjenoppretting for å håndtere driftsavbrudd. Kritiske deler av BankID-infrastrukturen er utformet slik at tjenesten kan opprettholdes ved feil. Kritiske data sikkerhetskopieres regelmessig og lagres sikkert atskilt fra det primære driftsstedet. Gjenoppretting testes periodisk.

Planene beskriver hvordan kritiske utstedelses- og valideringstjenester skal gjenopprettes ved alvorlig svikt, herunder bruk av en sekundær lokasjon eller reserveløsninger der det er nødvendig. Mål for gjenopprettingstid (RTO) og gjenopprettingspunkt (RPO) fastsettes i samsvar med relevante rettslige og forretningsmessige krav.

Stø har etablert prosedyrer for håndtering av sikkerhetshendelser. Hendelser klassifiseres etter alvorlighetsgrad og mulig innvirkning på BankID, sluttbrukere og brukersteder. Planene omfatter tiltak for å begrense skadeomfanget og for å undersøke hendelser, nødvendige kommunikasjonsprosedyrer, varsling der det kreves, og prosesser for utbedring og forbedring. Planer for virksomhetskontinuitet og hendelseshåndtering testes og vedlikeholdes regelmessig.



5.4 Terminering av ordningen

Stø har en termineringsplan for tilfeller der selskapet skal slutte å levere BankID, enten fordi tjenesten overføres til en annen leverandør, eller fordi BankID-ordningen termineres. Ved en planlagt terminering skal Stø gi tilstrekkelig varsel til sluttbrukere, brukersteder og relevante myndigheter.

Ved terminering skal Stø slutte å utstede nye BankID-er før tjenesten opphører, og så langt det er mulig legge til rette for en overgang til en alternativ løsning for brukerne. Stø skal oppbevare nødvendig informasjon og dokumentasjon i samsvar med kapittel 7 også etter avviklingen.

Stø skal avvikle tekniske funksjoner, nøkler, statusinformasjon og annet relevant støttemateriell på en ordnet måte. Brukersteder og andre berørte parter skal gis tilstrekkelig forhåndsvarsel, slik at de kan fase ut bruken av BankID på en ordnet måte.

5.5 Risiko- og sikkerhetsstyring

Stø håndterer risiko knyttet til BankID gjennom etablerte styringsprosesser, operasjonelle prosedyrer og sikkerhetskontroller. Risikostyringen skal oppfylle kravene til eID på sikkerhetsnivå høyt.

I samsvar med Kommisjonens gjennomføringsforordning (EU) 2015/1502 bygger sikkerhetsnivået på den samlede kvaliteten i identitetskontroll, forvaltning av elektroniske identitetsmidler, autentisering og organisatoriske kontroller. Risikostyringen skal derfor dekke hele livsløpet til BankID og være innarbeidet i alle relevante prosesser og kontroller.

Stø overvåker risikobildet løpende gjennom driftserfaring, sikkerhetshendelser, trusseletterretning og revisjonsfunn, og justerer kontroller og prosesser etter behov for å opprettholde sikkerhet, pålitelighet og etterlevelse.

6 Tekniske sikkerhetskontroller

6.1 Generelt

Stø etablerer og vedlikeholder tekniske sikkerhetskontroller for systemer og prosesser som understøtter utstedelse og drift av BankID. Kontrollene skal bidra til konfidensialitet, integritet og tilgjengelighet, og skal oppfylle kravene til eID på sikkerhetsnivå høyt.

Dette kapittelet beskriver de overordnede målene for de tekniske sikkerhetskontrollene. Detaljerte tekniske krav, spesifikasjoner og gjennomføring er beskrevet i kontrollert teknisk dokumentasjon.

6.2 Beskyttelse av sensitivt kryptografisk materiale

Stø beskytter sensitivt kryptografisk materiale mot urettmessig tilgang, bruk, endring og tap. Dette omfatter prosedyrer for generering, lagring, bruk, sikkerhetskopiering, utskifting, rotasjon og sletting. De tekniske detaljene er beskrevet i kontrollert teknisk dokumentasjon.

Kryptografisk materiale genereres og håndteres gjennom kontrollerte prosesser og med komponenter som oppfyller gjeldende sikkerhetskrav. Tilgang gis bare til autoriserte systemer og personell som trenger slik tilgang for å utføre sine oppgaver. Bruk og administrative handlinger logges, og særlig kritiske handlinger krever flerparts kontroll eller tilsvarende sikkerhetstiltak der det er nødvendig.

Nøkler som er nødvendige for kritiske BankID-funksjoner, sikkerhetskopieres bare der behovet er dokumentert. Sikkerhetskopier beskyttes mot urettmessig tilgang og kan bare brukes til gjenoppretting, kontinuitet eller andre formål som er særskilt godkjent etter etablerte prosedyrer. Kryptografisk materiale skiftes ut, roteres eller slettes i samsvar med etablerte prosedyrer, og tidligere dersom det oppstår forhold som kan svekke tilliten til materialet. Utfasing og sletting skal hindre etterfølgende bruk uten å svekke sikkerheten eller kontinuiteten i BankID.

6.3 System- og nettverkssikkerhet

Stø beskytter systemer og nettverk som understøtter BankID mot urettmessig tilgang, misbruk, skadevare og avbrudd. Kontrollene omfatter tilgangsstyring, sikker konfigurasjon, beskyttelse av kommunikasjonskanaler, system- og nettverksadskillelse, sårbarhetsoppfølging og overvåking.

Tilgang til sensitive BankID-systemer og tilhørende data gis bare til autoriserte brukere, systemer og prosesser som trenger slik tilgang for å utføre sine oppgaver. Brukere autentiseres med unike legitimasjonsdata, og administrativ tilgang er særskilt begrenset, logges og følges opp.

Systemer, servere og applikasjoner konfigureres og vedlikeholdes i samsvar med anerkjent sikkerhetspraksis. Standardkontoer og standardpassord endres, unødvendige tjenester deaktiveres, og sikkerhetsoppdateringer installeres uten ugrunnet opphold basert på risiko og kritikalitet.

BankID-infrastrukturen er segmentert slik at offentlig eksponerte tjenester, interne systemer og sikkerhetskritiske komponenter er tilstrekkelig atskilt. Kommunikasjonskanaler som overfører sensitive data, beskyttes med egnet kryptering og integritetsbeskyttelse.

Stø gjennomfører regelmessig sårbarhetsoppfølging og testing av systemer og nettverk. Funn vurderes og prioriteres basert på risiko, og nødvendige utbedringer gjennomføres i samsvar med etablerte prosedyrer.



Relevante system- og nettverkshendelser overvåkes for å oppdage avvik, misbruk og forhold som kan påvirke sikkerheten eller tilgjengeligheten til BankID. Kritiske forhold skal undersøkes og håndteres uten ugrunnet opphold.

6.4 Sikkerhet i livsløpet til systemer og komponenter

Tekniske sikkerhetskontroller anvendes gjennom hele livsløpet til systemer og komponenter som understøtter BankID. Dette omfatter sikker utvikling, konfigurasjon, vedlikehold, kontrollert endringshåndtering og sikker utskifting eller avvikling av systemer.

7 Logging, overvåking og oppbevaring av dokumentasjon

7.1 Revisjonslogging og overvåking

Stø fører og oppbevarer revisjonslogger for hendelser som er nødvendige for sikker drift, sporbarhet og etterlevelse i BankID-ordningen. Loggene brukes til sikkerhetsovervåking, hendelsesundersøkelser, revisjon, tilsyn og dokumentasjon av etterlevelse.

Loggingen omfatter blant annet hendelser knyttet til identitetskontroll, utstedelse, fornyelse, suspensjon, reaktivering, tilbakekalling og validering av BankID. Administrativ tilgang til kritiske systemer, bruk av sensitivt kryptografisk materiale, endringer i sikkerhetskonsfigurasjon og andre sikkerhetskritiske handlinger logges også. Det samme gjelder relevante sikkerhetshendelser og avvik, herunder mislykkede påloggingsforsøk, systemfeil som kan påvirke sikkerhetsfunksjoner og forsøk på urettmessig nettksttilgang.

Logger skal tidsstemples og beskyttes mot urettmessig tilgang, endring og sletting. Tilgang til logger gis bare til særskilt autoriserte personer og systemprosesser, og bruk av slik tilgang skal være sporbar.

Logger oppbevares så lenge det er nødvendig for sikkerhet, etterlevelse, revisjon, tilsyn og nødvendig dokumentasjon, og minst så lenge lov, forskrift eller krav etter BankID-ordningen krever.

Stø overvåker relevante loggdata for å oppdage avvik, misbruk og forhold som kan påvirke sikkerheten i BankID-ordningen. Kritiske forhold skal flagges, undersøkes og håndteres uten ugrunnet opphold. Loggene gjennomgås regelmessig for å kontrollere at driften skjer i samsvar med gjeldende krav, og gjennomgangene dokumenteres.

7.2 Arkivering

Stø arkiverer informasjon som er nødvendig for å dokumentere korrekt utstedelse, forvaltning og livsløpshåndtering av BankID, oppfylle etterlevelseskav og muliggjøre revisjoner, tilsyn og nødvendige undersøkelser.

Arkivet omfatter, innenfor rammene av gjeldende rett, relevante søknadsopplysninger, registrerte og verifiserte identitetsopplysninger, bekreftelser mot Folkeregisteret, dokumentasjon på aksept av sluttbrukervilkårene, unik sluttbrukeridentifikator og referanser til kontrollert identitetsdokumentasjon.

Stø arkiverer også informasjon om utstedelse, fornyelse, suspensjon, reaktivering, tilbakekalling, utløp og eventuell ny søknad. Der det er nødvendig for sikkerhet, etterlevelse eller tvisteløsning, kan valideringsforespørsler og svar på slike forespørsler også arkiveres.

Arkivert informasjon lagres sikkert og beskyttes mot urettmessig tilgang, endring og sletting gjennom egnede tekniske og organisatoriske tiltak, herunder tilgangskontroll, integritetsbeskyttelse og kryptering der det er relevant. Informasjonen oppbevares så lenge det er nødvendig for formålene den ble samlet inn for, og så lenge lov, forskrift eller krav etter BankID-ordningen krever.



8 Revisjon og egenerklæring

Stø sørger for at BankID-ordningen er underlagt de relevante revisjonene, vurderingene eller sertifiseringene som kreves etter lov, forskrift og gjeldende standarder, herunder Kommisjonens gjennomføringsforordning (EU) 2015/1502 slik den er gjennomført i norsk rett. Funn vurderes og følges opp med korrigerende tiltak eller forbedringstiltak der det er nødvendig. Relevant dokumentasjon og resultater gjøres tilgjengelig for kompetente myndigheter eller vurderingsorganer ved behov.

9 Andre forretningsmessige og juridiske forhold

9.1 Økonomisk ansvar

Støs økonomiske ansvar for BankID følger av gjeldende rett og de avtalene som regulerer tjenesten, herunder regler om ansvar ved feil i utstedelse, drift eller forvaltning av BankID.

Stø har økonomiske ressurser og forsikringsdekning som er egnet for virksomheten som leverandør av eID-tjenester på høyt sikkerhetsnivå. Dette omfatter alminnelig ansvarsforsikring eller særskilt dekning for digitale sikkerhetshendelser, systemsvikt eller sikkerhetsbrudd.

Eventuelle finansielle garantier som uttrykkelig er gitt til sluttbrukere eller brukersteder, framgår av relevante avtalevilkår i avtale med sluttbruker eller brukersted.

9.2 Konfidensialitet

Stø og Støs samarbeidspartnere, herunder registreringsenheter, fullmektiger og underleverandører, har etter inngåtte avtaler plikt til å beskytte konfidensiell informasjon som de får tilgang til i forbindelse med utstedelse, drift og forvaltning av BankID.

Konfidensiell informasjon omfatter blant annet personopplysninger om søkere og sluttbrukere, sensitive aktiveringsdata, vurderinger og dokumentasjon fra identitetskontroll, RA-vurderinger, systemkonfigurasjon, sikkerhetslogger, forretningssensitiv driftsdokumentasjon og annen informasjon som etter sin art eller etter avtale skal beskyttes.

Konfidensiell informasjon skal behandles og lagres sikkert. Tilgang gis bare til autoriserte personer som trenger informasjonen for å utføre sine oppgaver, og alt personell som får tilgang til slik informasjon, skal være underlagt konfidensialitetsplikt gjennom ansettelsesforhold, avtale eller annen bindende regulering.

Konfidensiell informasjon utleveres bare når det foreligger gyldig rettslig grunnlag, avtale, krav fra kompetent myndighet eller annen legitim og dokumentert grunn. Ved utlevering skal Stø påse at omfanget begrenses til det som er nødvendig, og at utleveringen håndteres på en kontrollert måte.

Opplysninger som etter sin art må formidles ved bruk av BankID, for eksempel nødvendige identitetsopplysninger og statusopplysninger, anses ikke som brudd på konfidensialitetsplikten når formidlingen skjer i samsvar med BankID-ordningen, gjeldende avtaler og relevant personvernlovgivning.

9.3 Svindelforebygging og enhets-/risikosignaler

For å beskytte BankID og forebygge kriminell virksomhet kan Stø identifisere den elektroniske enheten som BankID brukes fra, og vurdere signaler fra brukssituasjonen, som enhetens status, IP-adresse og avvik fra normalt miljø eller normal atferd. Brukersteder kan motta informasjon som angir risikonivået knyttet til å godta BankID fra en bestemt enhet i den aktuelle transaksjonen.

9.4 Personvern

Som eID-tilbyder har Stø et særlig ansvar for å beskytte personopplysninger som behandles i forbindelse med utstedelse, drift og bruk av BankID. Stø behandler personopplysninger i samsvar med gjeldende personvernlovgivning og de personvernprinsippene som gjelder for BankID-ordningen, formålsbegrensning, dataminimering, tilgangsstyring og tilpassede regler for oppbevaring.



Personopplysninger behandles bare når det foreligger et gyldig rettslig grunnlag, og ikke i større omfang enn nødvendig for utstedelse, forvaltning, autentisering, validering, sikkerhet, svindelforebygging, kundeservice, etterlevelse og tilhørende formål.

Sluttbrukerens personopplysninger utleveres bare til et brukersted eller en annen tredjepart når det foreligger et gyldig rettslig grunnlag, for eksempel sluttbrukerens samtykke, avtale, rettslig forpliktelse eller annet grunnlag etter gjeldende personvernlovgivning.

Personvernerklæringen for BankID beskriver hvilke personopplysninger som samles inn, formålene opplysningene behandles for, oppbevaringstiden, utlevering til tredjeparter og de registrertes rettigheter, herunder retten til innsyn og retting.

Personopplysninger oppbevares ikke lenger enn nødvendig. Personopplysninger i loggfiler kan likevel oppbevares så lenge det er nødvendig for å oppfylle rettslige krav eller ivareta pågående rettslige prosesser, og skal deretter slettes på en sikker måte.

Stø beskytter personopplysninger gjennom egnede tekniske og organisatoriske tiltak. Når Stø benytter tjenesteleverandører, reguleres plikter om personvern og konfidensialitet ved avtale og følges opp gjennom egnede kontrollaktiviteter.

9.5 Immaterielle rettigheter

Immaterielle rettigheter, varemerker, logoer og regler for merkevarebruk reguleres av separate merkevare- og lisensvilkår og relevante avtaler. Dette faller utenfor omfanget av dette dokumentet.

9.6 Erklæringer og garantier

Stø erklærer at BankID utstedes, forvaltes og driftes i samsvar med gjeldende krav, rettslige plikter og de prosedyrene som gjelder for BankID-ordningen. BankID er ment å formidle de identitetsopplysningene og det sikkerhetsnivået som følger av ordningen, innenfor de begrensningene som framgår av gjeldende avtaler, dette dokumentet og relevant teknisk dokumentasjon.

Stø gir ingen ytterligere garantier for BankID, herunder for at tjenesten er egnet for alle særskilte formål eller bruksmåter hos sluttbrukere eller brukersteder ut over det som følger av kravene til sikkerhetsnivå høyt og de avtalene som regulerer tjenesten.

Registreringsenheter som utfører identitetskontroll, registrering eller andre oppgaver på vegne av Stø, skal følge Støs prosedyrer, gjeldende standarder og relevante avtalevilkår. De skal sørge for at personell har nødvendig opplæring og kompetanse, beskytte sensitiv informasjon og bidra til etterlevelse av kravene som gjelder for BankID-ordningen.

Ved å akseptere BankID erklærer sluttbrukeren at opplysningene som gis ved registreringen, er korrekte, at BankID-vilkårene er lest og akseptert, og at BankID skal brukes og beskyttes i samsvar med disse vilkårene. Sluttbrukeren skal varsle Stø eller registreringsenheten uten ugrunnet opphold dersom BankID kompromitteres, kontrollen over BankID går tapt, eller registrerte opplysninger blir uriktige.

Ved å bruke BankID erklærer brukerstedet at BankID-integrasjonen og bruken av tjenesten skjer i samsvar med BankID-reglene, gjeldende veiledning, relevant teknisk dokumentasjon og de avtalene som regulerer brukerstedets tilgang til tjenesten. Dette omfatter blant annet å validere BankID-resultater der det er relevant, bare bruke BankID til tillatte formål, beskytte eget integrasjonsmiljø og rapportere mistanke om misbruk, svindel eller sikkerhetshendelser.

9.7 Ansvarsfraskrivelser og ansvarsbegrensninger

Støs ansvar overfor sluttbrukere, brukersteder, registreringsenheter og øvrige avtalepartnere reguleres av de avtaler som gjelder for de respektive partene, samt av ufravikelige lovkrav.

9.8 Varighet og opphør av praksiserklæringen

Dette dokumentet gjelder fra ikrafttredelsesdatoen og frem til det erstattes av en ny godkjent versjon, eller til BankID-ordningen slik den er beskrevet, avvikles.

Stø kan endre eller oppdatere dette dokumentet etter behov, i samsvar med reglene for forvaltning av denne praksiserklæringen i henhold til kapittel 1.4.3. Ved vesentlige endringer som kan påvirke sluttbrukere, brukersteder eller registreringsenheter, skal Stø formidle endringene på egnet måte, for eksempel ved publisering eller direkte varsel der dette er relevant.

Dersom Stø opphører å drifte BankID, eller dersom dette dokumentet erstattes som følge av at tjenesten overføres til en annen operatør, skal Stø sørge for nødvendig varsling og arkivering i samsvar med kapittel 5.4 og 7. Dersom Stø erstattes av en annen leverandør, skal relevante plikter og nødvendig dokumentasjon overføres på en kontrollert måte for å opprettholde tillit til og kontinuitet i BankID-ordningen.

9.9 Lovvalg og tvisteløsning

Støs drift av BankID er underlagt norsk rett.

Tvister knyttet til levering eller bruk av BankID skal i første omgang søkes løst i minnelighet, for eksempel direkte mellom sluttbrukeren eller brukerstedet og Stø, eller gjennom registreringsenhetens kundeservice der dette er relevant. Dersom tvisten ikke løses i minnelighet, kan den bringes inn for behandling i samsvar med gjeldende avtaler og gjeldende rett.

Sluttbrukere kan benytte de klage- og tvisteløsningsmekanismene som følger av sluttbrukeravtalen for BankID og gjeldende rett. Brukersteder skal følge de tvisteløsningsreglene som følger av, eller er henvist til i, de avtalene som regulerer brukerstedets tilgang til BankID.

Tvister skal behandles av norske domstoler.