Norwegian:

Avtalevilkår for PersonBankID og AnsattBankID - PDS

Denne Public Key Infrastructure Disclosure Statement (PDS) er strukturert ifølge standarden ETSI EN 319 411-1 vedlegg A. Dokumentet supplerer dokumentet BankID Trust Service Provider Statement.

Hensikten med dokumentet er å sammenstille hovedpunktene i Trust Service Provider Statement for Kunde og Sertifikatmottaker.

Avtalen vedlikeholdes både på engelsk og norsk språk. I tilfelle tvetydighet skal den norske versjonen gå foran.

Dokumenthistorikk:
Versjon 1.1 (21.05.2019): Norsk og engelsk tekst samlet. Oppdaterte lovreferanser. Godkjent av BankID Policy Board den 21.05.2019.

Versjon 1.0 (29.11.2018): Endelig versjon for publisering. Godkjent av BankID Policy Board den 29.11.2018.

1. Kontaktinformasjon til utsteder

SpareBank 1 Utvikling DA
Postboks 778 Sentrum
0106 Oslo

https://www.sparebank1.no

For sperring av BankID eller andre spørsmål om sertifikater, ta kontakt med utstedende bank, se kontaktinformasjon på https://www.sparebank1.no/nb/bank/privat/kundeservice.html.

English:

Terms and Conditions for Personal BankID and Employee BankID - PDS

This Public Key Infrastructure Disclosure Statement (PDS) is structured according to the standard ETSI EN 319 411-1 Annex A. This document is a supplement to the BankID Trust Service Provider Statement.

The purpose of this document is to summarise the key points of the Trust Service Provider Statement for the benefit of Subscribers and Relying Parties.

The agreement is maintained both in English and Norwegian language. In case of ambiguity, the Norwegian version shall be applied.

Document history:
Version 1.1 (21.05.2019): Norwegian and English text together. Updated legal references. Approved by BankID Policy Board on 21 May 2019.

Version 1.0 (29.11.2018): Final version for publishing document. Approved by BankID Policy Board on 29 Nov 2018.

1. Trust Service Provider contact info

SpareBank 1 Utvikling DA
Postboks 778 Sentrum
0106 Oslo

https://www.sparebank1.no

For revocation request or other certificate questions: Please contact the customer service at your bank, see list of contact info: https://www.sparebank1.no/nb/bank/privat/kundeservice.html.

2. Kort beskrivelse av tjenesten

Utstedelse av BankID som kvalifiserte sertifikater er regulert av bestemmelsene i lov om elektroniske tillitstjenester, som gjennomfører EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske signaturer (EU No 910/2014). Loven med tilhørende forskrifter er heretter benevnt eID-reglene. Disse stiller krav til utstedere, som må tilrettelegge systemer, regler og prosedyrer for å ivareta sikkerheten i sertifikatene. BankID er ett eller flere elektronisk(e) sertifikat(er) som en sertifikatholder (heretter benevnt Kunden) kan benytte for å lage elektroniske signaturer som skal sikre elektronisk meldingsutveksling, herunder elektronisk avtaleinngåelse. Sikring skjer ved at den elektroniske signaturen bekrefter avsenderens identitet, knytter meldingen til avsender og gjør det mulig å oppdage endringer i meldingen. PersonBankID er en avansert elektronisk signatur som oppfyller kravene i eID-reglene.

BankID kan benyttes som sikkerhetsanordning ved betalingstransaksjoner. Ansvar for tap som skyldes uautoriserte betalingstransaksjoner hvor PersonBankID er benyttet som personlig sikkerhetsanordning, reguleres av Finansavtalelovens § 35 og kontoavtale inngått mellom Kunde og kontobank.

AnsattBankID er et sertifikat som i tillegg bekrefter en knytning mellom en identifisert virksomhet (Juridisk person, heretter benevnt Kunden) og en entydig identifisert fysisk person innenfor denne virksomheten (heretter benevnt Brukeren) AnsattBankID blir brukt av Brukeren for tjenester eller oppdrag på vegne av Kunden.

Finansavtalelovens § 35 kommer ikke til anvendelse for AnsattBankID.

Bestemmelsene i denne avtalen gjelder for både PersonBankID og AnsattBankID. Der vilkår kun gjelder for en type BankID, fremgår det av avtalen.

Utsteder er registrert hos Nasjonal kommunikasjonsmyndighet (Nkom) som utsteder av kvalifiserte sertifikater og skal følge de regler som er fastsatt i eID-reglene.

Spørsmål og andre henvendelser vedrørende BankID rettes til Utsteder.

2. Certificate type, validation procedures and usage

Issuance of BankID as qualified certificates is governed by the provisions of the Act on electronic trust services, which implements the EU Regulation on electronic identification and trust services for electronic transactions in the internal marked ((EU) No 910/2014). This is referred to as the eID provisions throughout this document. The law with associated regulations imposes requirements on issuers who must arrange systems, rules and procedures to safeguard the security of the certificates. A BankID consists of one or more electronic certificates a Subscriber can use to create electronic signatures to secure electronic message exchanges and enter into contracts electronically. The electronic signature secures the message by confirming the sender's identity, linking the message to the sender and enables detection of any changes of the message. BankID is an advanced electronic signature that complies with the requirements of eID provisions.

BankID can be used as a security mechanism for payment transactions. Liability for loss resulting from unauthorised payment transactions where Personal BankID is used as a personal security mechanism, is regulated by the Finance Contracts Act article 35 and the account agreement between the Subscriber and the account bank.

Employee BankID is a certificate which in addition confirms a link between an identified organisation (legal person, referred to as the Subscriber) and a uniquely identified natural person within this organisation (referred to as the Subject). Employee BankID is used by the Subject for services or assignments on behalf of the Subscriber.

The Finance Contracts Act article 35 does not apply for the use of Employee BankID.

The provisions set forward in this agreement apply both for Personal BankID and Employee BankID. Where provisions only apply for one type of BankID, it will be stated explicitly.

Issuer has been registered with the Norwegian Communications Authority (Nkom) as issuer of qualified certificates and shall comply with the eID provisions.

All queries regarding BankID shall be directed to the Trusted Service Provider.

2.1 Hvem kan få BankID sertifikat

Utsteder kan avslå å utstede BankID når saklig grunn foreligger, så som mistanke om straffbare forhold rettet mot Utsteder eller hvor kundekontroll ikke lar seg gjennomføre.

PersonBankID

PersonBankID kan utstedes til fysiske personer.

AnsattBankID

AnsattBankID kan utstedes til personer som er ansatt hos eller som utfører oppgaver for virksomheter (privat eller offentlig virksomhet og forvaltning) som er registrert i Enhetsregisteret eller et tilsvarende offentlig register innenfor EØS-området

2.1 Eligibility for a BankID certificate

The Issuer has the right to refuse to issue a BankID provided it has factual reasons for such refusal, such as suspected criminal offences against the Issuer or where customer control cannot be carried out.

Personal BankID

Personal BankID can be issued to natural persons.

Employee BankID

Employee BankID can be issued to natural persons employed by or executing tasks for legal persons (private or governmental business) registered in Central Coordinating Register for Legal Entities ("Enhetsregisteret") or similar governmental register within the EEA area.

2.2 Priser og prisinformasjon

Kostnader ved å få utstedt, ha og bruke BankID fremgår av Utsteders gjeldende prisliste og/eller opplyses på annen egnet måte bl.a. på Utsteders hjemmeside på Internett.

Ved bruk av BankID som er lagret på SIM-kort, vil det kunne påløpe ekstra kostnader ved bruk av telenettet. Teleoperatørens priser for bruk av BankID på SIM-kort fremgår av den til enhver tid gjeldende prisliste på teleoperatørens hjemmeside på Internett og/eller opplyses på annen egnet måte.

2.2 Prices and price information

Charges for issuing, holding and using BankID are set out in the Issuer's current price schedules and/or specified by another appropriate means, such as on the Issuers home page.

When a BankID is used from a mobile telephone/SIM card, extra fees may be charged by the Subscriber's mobile network operator in addition to the BankID charges. The mobile network operator's fees for use of BankID on a mobile device should be specified in the current fee schedule on the provider's website.

2.3 Legitimasjonskontroll og krav til legitimasjonsdokumenter

eID-reglene stiller krav til utsteder om å forsikre seg om at sertifikatholders identitet er kontrollert og verifisert på en sikker måte.

Før det utstedes BankID skal brukeren legitimere seg og bekrefte riktigheten av oppgitte opplysningen. Slik legitimasjonskontroll skal skje ved Kundens eller Brukerens personlige fremmøte hos Utsteder eller en representant for denne, men mindre vedkommende Kunde eller Bruker allerede er identifisert ved personlige fremmøte gjennom eksisterende kundeforhold hos Utsteder.

Utsteder vil kreve at Kunden eller Brukeren i forbindelse med Utsteders legitimasjonskontroll fremlegger gyldig norsk pass, gyldig utenlandsk pass eller andre dokumenter som etter en risikobasert

2.3 Identity checking and identification requirements

eID provisions require issuers to ensure that the identity of the certificate holder is checked and verified in a secure manner.

Before the issuance of BankID, the Subject shall identify himself/herself and confirm the accuracy of the information provided. Such identification shall be by personal attendance with the Issuer or its representative unless the Subject already has been identified by personal attendance through existing customer relationship with the Issuer.

The Issuer will require the Subject, in connection with Issuer's verification of identity, to provide a valid Norwegian passport, a valid foreign passport or other documents, which based upon a risk-based assessment, is considered to be a valid identity document with an equivalent security level as a Norwegian passport.

vurdering anses som gyldig legitimasjon med samme sikkerhetsnivå som norsk pass.

Kunden eller Brukeren skal snarest mulig varsle Utsteder ved navn- og adresseendringer og endringer i andre opplysninger som er gitt Utsteder under dette avtaleforholdet.

AnsattBankID

Ved utstedelse av AnsattBankID skal Kunden være representert ved signaturberettiget eller en som har fått uttrykkelig fullmakt fra signaturberettighet til å inngå avtale om AnsattBankID på vegne av Kunden. Et enkeltpersonforetak skal være representert ved innehaveren av enkeltpersonforetaket eller en med eller en med fullmakt fra innehaver til å inngå avtale om AnsattBankID på vegne av enkeltpersonforetaket. Vedkommende som representerer Kunden skal oppgi fullt navn, adresse og fødselsnummer eller D-nummer, identifisere seg og bekrefte riktigheten av opplysningene. Vedkommendes rett til å inngå avtale skal dokumenteres.

Utstederen kan be om ytterligere opplysninger eller dokumentasjon, samt foreta nærmere undersøkelser om riktigheten av de avgitte opplysninger, fullmakter, med videre.

The Subject or Subscriber shall promptly notify the Issuer of any change of name or address or other information given to the Issuer in connection with this agreement.

Employee BankID

Upon the issuance of Employee BankID, the Subscriber shall be represented by signatory authorised person ("signaturberettiget") or a person with a dedicated authorisation from the signatory person to enter into an agreement for Employee BankID on behalf of the Subscriber. A sole proprietorship shall be represented by the owner of the proprietorship or with a authorisation from the owner to enter into an agreement for Employee BankID on behalf of the Sole Proprietorship. The person representing the Subscriber shall supply their full name, address and social security number ("fødselsnummer" or "D-nummer"), identify themselves and confirm the correctness of the information. Their right to enter into the agreement shall be documented.

The issuer can request further information or documentation, and conduct further investigations of the correctness of the information, authorisations etc.

2.4 Utlevering av BankID. Brukerdokumentasjon og sikkerhetsprosedyrer

Nødvendig brukerdokumentasjon og utstyr for bruk av BankID vil være tilgjengelig for eller bli utlevert til Kunden på anvist måte.

Informasjon og veiledning om prosedyrene for bruk, fornyelse og sperring av BankID vil fremgå av brukerdokumentasjonen som er tilgjengelig gjennom Utsteders nettsider eller Kundens nettbank der Kunden har nettbankavtale med Utsteder. Brukerdokumentasjonen vil også inneholde sikkerhetsprosedyrer, herunder rutiner for sikkerhetskopiering og informasjon om virusbeskyttelse samt eventuelle beløpsbegrensninger og grenser for Utsteders ansvar ved bruk av BankID.

Brukeren må gjøre seg kjent med dokumentasjonen før tjenesten tas i bruk og rette seg etter anvisningene. Brukeren må ikke gjøre endringer i BankID, programvare eller dokumentasjon.

Kunden må sammen med BankID benytte slik programvare, maskinutrustning eller det sikkerhetsutstyr som Utsteder spesifiserer. Utsteder kan stille nye krav til programvare, maskinutrustning

2.4 Delivery of BankID. User documentation and security procedures

Required user documentation and devices to use a BankID shall be made available for or delivered to the Subject in the designated manner.

Information and guidelines for usage, renewing and blocking BankIDs are set out in the user guide that can be accessed via the Issuer's website or online banking service to which the Subject subscribes. The user guide also contains descriptions of security procedures, including procedures for making security copies, and information about protection against viruses, any limits on amounts and limits on the Issuer's liability for use of BankID.

The Subject must familiarise himself/herself with the documentation before taking the service into use. The Subject may not alter the BankID, software or documentation.

The Subject must use BankID with the software, hardware or security devices specified by the Issuer. The Issuer can give new requirements if this is

eller sikkerhetsutstyr dersom dette er nødvendig av sikkerhetsmessige grunner eller ved nødvendige oppgraderinger av BankID.

AnsattBankID
For AnsattBankID er Kunden ansvarlig for at Brukerne gjøres kjent med disse reglene samt undertegner en erklæring om å ha mottatt programvare, brukerdokumentasjon, sertifikater, sikkerhetsprosedyrer og regler om hemmelighold av passord, brukernavn og lignende (jf vedlegg til denne avtale).

necessary for security reasons or needed upgrades of BankID.

Employee BankID
For Employee BankID, the Subscriber is responsible for ensuring the Subjects understand these rules and sign a declaration when receiving software, documentation, certificates, security procedures and rules on password secrecy, username and similar.

2.5 Anvendelsesområdet for BankID

BankID kan benyttes fra ulike elektroniske enheter som datamaskin, nettbrett, smarttelefon og lignende, for pålogging i nettbank og til identifisering og signering i forbindelse med elektronisk meldingsforsendelse, avtaleinngåelse og annen form for nettbasert elektronisk kommunikasjon med Utsteder og andre BankID brukersteder.

En BankID skal ikke benyttes som grunnlag for å få utstedt en fysisk eller en ny elektronisk legitimasjon.

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

Kunden må selv lagre/arkivere elektroniske meldinger/inngåtte avtaler sikret ved BankID.

AnsattBankID
For AnsattBankID skal Kunden påse at Brukere undertegner en erklæring om at AnsattBankID kun benyttes til tjenstlige oppgaver/oppdrag for Kunden, og at de ikke benyttes av ansatte og oppdragstakere til private gjøremål.

2.5 Area of application for BankID

BankID can be used with various electronic devices, such as a computer, tablet, smartphone or similar, to log in to an online banking service and as identification and signing in connection with sending electronic messages, entering into agreements and other forms of online communication with the Issuer and other BankID merchants.

A BankID may not be used as basis for issuing a physical or new electronic ID.

The Subscriber will be notified if the Issuer expands or limits the area of application for BankID. The area of application is described in more detail in the user documentation.

It is up to the Subscriber to save electronic messages/concluded contracts secured by BankID.

Employee BankID
For Employee BankID, the Subscriber must ensure the Subject signs a declaration ensuring Employee BankID is only used for work-related tasks for the Subject and not used for private purposes

3. Bruksbegrensninger

Dersom Kunden benytter BankID, tilhørende utstyr, programvare eller dokumentasjon på en måte som er i strid med denne avtalen, inkludert uautoriserte endringer eller manipulering av BankID eller programvare, kan Utstederen holde Kunden ansvarlig for tap lidd av Utsteder.

PersonBankID

3. Reliance limits

If the Subscriber uses BankID, associated devices/programs or documentation in a manner which violates the terms of this agreement, including unauthorised modification or manipulation of BankID or software, the Issuer may hold the Subscriber liable for any loss incurred by the Issuer.

Personal BankID

Med mindre Kunden opptrer grovt uaktsom eller forsettlig, vil Kundens ansvar mot Utstedere være begrenset til NOK 100.000,-.

AnsattBankID
Ingen beløpsbegrensning gjelder for bruk av AnsattBankID.

Unless the Subscriber is guilty of gross or wilful negligence, the Subscriber's liability towards the Issuer is limited to a maximum of NOK 100,000.

Employee BankID
No such limitation applies to the use of Employee BankID.

4. Kundens ansvar

4.1 Vern om passord og andre sikkerhetsprosedyrer

BankID er personlig og skal ikke overdras eller på annen måte overlates til eller brukes av andre enn Kunden eller Brukeren. Passord, personlige koder og andre sikkerhetsprosedyrer må ikke røpes for noen, heller ikke overfor politiet, Utsteder eller husstandsmedlemmer. Kunden og Brukeren skal benytte oppdatert programvare, herunder operativsystem, nettleserprogram og annen programvare for sikker kommunikasjon med nettstedet, samt antivirusprogramvare. For øvrig skal Kunden eller Brukeren følge Utsteders til enhver tid gjeldende sikkerhetsråd.

Når BankID benyttes som sikkerhetsanordning ved bruk av betalingsinstrumenter gjelder i tillegg finansavtalelovens § 34, første ledd: En kunde som har rett til å bruke et betalingsinstrument, skal bruke det i samsvar med vilkårene for utstedelse og bruk, og skal herunder ta alle rimelige forholdsregler for å beskytte de personlige sikkerhetsanordningene knyttet til betalingsinstrumentet så snart instrumentet er mottatt. I tillegg skal kunden uten ugrunnet opphold underrette institusjonen, eller den institusjonen har oppgitt, dersom kunden blir oppmerksom på tap, tyveri eller uberettiget tilegnelse av sikkerhetsanordningen, eller betalingsinstrumentet, eller på uautorisert bruk.

AnsattBankID
Fra det tidspunkt AnsattBankID er utlevert er Kunden ansvarlig for at AnsattBankID kun disponeres av den eller de personer som har bemyndigelse til å anvende AnsattBankID for utføring av tjenstlige oppgaver/oppdrag på vegne av Kunden.

4. Obligations of subscribers

4.1 Safeguarding the password and other security mechanisms

BankID shall not be transferred or entrusted to or used by anyone other than the Subject. Passwords, personal codes and other security mechanisms shall not be revealed to anyone, including the police, the Issuer or members of the Subject's household. The Subscriber must use updated software, including operating system, browser software and other software for secure communication with the site, as well as anti-virus software, and otherwise follow the Issuer’s security instructions.

When BankID is used as a security device for payment instruments, Section 34, first paragraph, of the Financial Agreement Act applies: A Subscriber who is entitled to use a payment instrument shall use it in accordance with the terms of issue and use and shall take all reasonable precautions to protect the personal security devices associated with the payment instrument as soon as the instrument is received. In addition, the Subscriber shall, without undue delay, notify the institution, or another party the institution has provided, if the Subscriber becomes aware of loss, theft or unauthorised acquisition of the security device, or payment instrument, or unauthorised use.

Employee BankID
From the time Employee BankID is delivered, the Subscriber is responsible Employee BankID only can be used by Subjects authorised to use BankID for performing work-related tasks for the Subscriber.

4.2 Melding om tap

Kunden må underrette Utsteder eller Utsteders utpekte medhjelper snarest mulig etter at Kunden eller Brukeren har fått kjennskap til eller mistanke om at BankID og/eller tilhørende passord og personlig kode er

4.2 Notice of loss or termination

The Subscriber shall notify the Issuer or the Issuer’s designated agent as soon as possible after having discovered or come to suspect that an unauthorised party has gained access to the BankID and/or learned

kommet bort eller at uvedkommende har fått kjennskap til passord/personlig kode. Kunden skal benytte de meldingsmuligheter Utsteder har stilt til disposisjon, og forøvrig bistå på en slik måte at BankID så raskt som mulig blir sperret. Kunden skal ikke anvende BankID etter at slik mistanke eller kunnskap har oppstått.

Ved slik melding skal Utsteder eller Utsteders medhjelper bekrefte overfor Kunden at meldingen er mottatt. Bekreftelsen skal blant annet inneholde en referanse til mottatt melding. Dersom Utsteder ikke kan dokumentere at meldingssystemet fungerte som det skulle innenfor det aktuelle tidsrom, skal Kundens forklaring vedrørende tapstidspunktet, samt når Utsteder eller Utsteders medhjelper ble forsøkt underrettet, normalt legges til grunn.

PersonBankID

For PersonBankID vil Kunden ikke bli belastet for Utsteders kostnader ved melding om tap og sperring av PersonBankID, med mindre det foreligger spesielle forhold på Kundens side, f.eks. gjentatte meldinger om tap. Utsteder kan imidlertid kreve vederlag for utstedelse av ny PersonBankID, så fremt tapet ikke skyldes forhold på Utsteders side.

AnsattBankID

For AnsattBankID skal Kunden skriftlig underrette Utstederen ved opphør av oppdrags- og ansettelsesforhold til Brukere av AnsattBankID, samt ved de tilfeller en Bruker ikke lenger har behov for et AnsattBankID for utføring av oppgaver og oppdrag for virksomheten. Slik underretting skal om mulig gis i god tid før forholdet inntrer.

For AnsattBankID skal Utstederen kreve at vedkommende som melder til Utstederen på vegne av Kunden, dokumenterer sin rett til å gi slik melding.

the password/personal code, or that these have been misplaced. The Subscriber shall use the reporting options the Issuer provides and otherwise help to ensure the BankID is blocked as soon as possible. The Subject must not use the BankID after such suspicion or discovery has been reported.

The Issuer or the Issuer's agent shall send the Subscriber confirmation that the notification has been received. Among other things, the confirmation shall contain a reference to the received notification. If the message is delayed or not received and the Issuer is unable to document the message system was functioning properly at the time in question, the Issuer shall normally accept the Subscriber's account of when the loss occurred and when he/she first tried to report this to the Issuer or the Issuer's agent.

Personal BankID

For Personal BankID, failing extraordinary circumstances on the Subscriber's behalf, the Subscriber will not be required to compensate the Issuer for costs incurred in connection with reporting the loss and blocking the Personal BankID. The Issuer may, however, demand payment for issuing a new Personal BankID, provided the loss is not attributable to circumstances on the Issuer's end.

Employee BankID

For Employee BankID, the Subscriber must in written form notify the Issuer if the employment or relation to the Subject is terminated, or if the Subject no longer has a need for Employee BankID. Such notification shall if possible be given in good time before this occurs.

For Employee BankID, the issuer can require the person notifying the Issuer on behalf of the Subscriber to document their right to do such notification.

5. Kontroll av sertifikatstatus

Hver gang et BankID sertifikat blir benyttet for enten autentisering eller signering, skal den som ønsker å stole på BankID verifisere sertifikatets gyldighet.

5.1 Sperring av BankID

eID-reglene stiller krav til at utstedere av BankID sertifikater skal ha systemer, regler og prosedyrer som gir utstedere adgang til å sperre (suspendere eller tilbakekalle) BankID sertifikatet for videre bruk dersom

5. Certificate status checking obligations of relying parties

Every time a BankID certificate is used for either authentication of signing purposes, the certificate status must be checked to verify it is valid

5.1 Blocking a BankID

The eID provisions require issuers of BankID certificates to have systems, rules and procedures in place to allow issuers to invalidate (suspend or revoke) a BankID certificate for further use if there are reasonable

det foreligger saklige grunner knyttet til sertifikatets sikkerhet, nøkler og tilhørende koder er kommet på avveie, at sertifikatet inneholder feilaktige opplysninger, jfr. punkt 4 eller at det foreligger mislighold, jf. pkt. 4.1. Utsteder vil i slike situasjoner umiddelbart sperre og tilbakekalle sertifikatet.

AnsattBankID
Sperring vil også kunne skje ved annen saklig grunn, blant annet ved opphør av ansettelsesforhold og oppdragsavtaler blant Brukere av AnsattBankID.

5.2 Kontroll av gyldig BankID (validering)
Utsteder vil påse at det blir etablert et system for gyldighetskontroll av alle BankID som er benyttet overfor Kunden og Brukere.

Det vil av hensyn til slik gyldighetskontroll bli ført et register over gyldige BankID samt BankID som er suspendert eller tilbakekalt (sperret). De registrerte opplysninger vil bli oppbevart i minst 10 år etter at gyldighetsperioden for et BankID er utløpt eller etter at det er tilbakekalt.

Utstedere av BankID vil utveksle opplysninger om gyldige og suspenderte/tilbakekalte BankID. Opplysningene vil bare benyttes for å kontrollere om BankID er gyldig og til formål som er forenlig med bruken av BankID.

6. Ansvar ved misbruk av Kundens BankID

6.1 Misbruk av PersonBankID
Dersom noen har handlet i tillit til disposisjoner gjort av uvedkommende som har misbrukt Kundens BankID, for eksempel inngått avtale med misbrukeren, vil disse etter alminnelige rettsregler kunne holde Kunden erstatningsansvarlig dersom misbruket er muliggjort ved forsettlig eller uaktsom handling eller unnlatelse fra Kundens side.

Dersom Utsteder har utvist uaktsomhet og dette er årsak til Kundens økonomiske tap som følge av andres misbruk av Kundens BankID som beskrevet i forrige avsnitt, er Utsteder erstatningsansvarlig.

6.2 Misbruk av AnsattBankID
Kunden er erstatningsansvarlig for disposisjoner som er foretatt av alle som har fått mulighet til å disponere

grounds regarding the security of the certificate, keys and associated codes have been compromised, if the certificate contains incorrect information, see section 4 or in case of misuse, see section 4.1. The Issuer will in such circumstances immediately invalidate the certificate.

Employee BankID
Invalidation can also be performed of other reasons, such as termination of employment or contract of users of Employee BankID.

5.2 Verification of the validity of BankIDs (validation)
The Issuer shall ensure procedures are in place for checking the validity of all BankIDs used in communication/transactions with the Subscriber or Subject.

For such validation, a record is kept of all valid BankIDs and BankIDs suspended or revoked (blocked). This information is kept for at least ten years after a BankID expires or is recalled.

BankID issuers exchange information about valid and suspended/revoked BankIDs. This information is only used to check if a BankID is valid, and for other purposes compatible with BankID use.

6. Limited warranty and disclaimer/Limitation of liability

6.1 Unauthorised use of Personal BankID
If someone has acted based on actions made by unauthorised persons who have misused the Subscriber's BankID by, for example, entered into an agreement with the unauthorised user, they will be able to keep the Subscriber liable if the unauthorised use is made possible by an intentional or negligent act or omission by the Subscriber.

If Issuer has been negligent and this is the reason for the Subscriber’s financial loss resulting from others’ misuse of the Subscriber’s BankID as described in the previous paragraph, the Issuer is liable.

6.2 Unauthorised use of Employee BankID
The Subscriber is responsible for usage conducted by anyone who has had the opportunity to use Employee

AnsattBankID utstedt til Brukere hos Kunden på grunn av forsettlig eller uaktsom handling eller unnlatelse fra Kundens eller Brukerens side.

Kunden er i forhold til Utstederen ansvarlig for at Brukerne er autorisert for å bruke AnsattBankID utstedt av Banken og at de personalopplysninger som oversendes Banken som grunnlag for utstedelse av AnsattBankID er korrekte.

Benytter Kunden og/eller Bruker AnsattBankID, programvare eller dokumentasjon i strid med denne avtale, herunder uberettiget endrer eller manipulerer sertifikatet eller programvare, kan Utstederen holde Kunden erstatningsansvarlig for Utstederens tap som følge av dette.

Kunden er i forhold til Utstederen ansvarlig for egne underleverandører. Kunden skal i avtale med eventuelle underleverandører pålegge disse ansvar for at leveransene tilfredsstiller kravene i denne avtalen og utfyllende bestemmelser gitt av Utstederen.

BankID issued to the Subscriber's Subjects based on wilfully or negligent actions or failure of the Subscriber or Subject.

The Subscriber is responsible to the Issuer to ensure Subjects are authorised to use Employee BankID and ensure personal information sent to the Issuer for issuing the Employee BankID is correct.

If the Subscriber or Subject of Employee BankID, software or documentation are used contrary to this agreement, including unauthorised changes or manipulation to the certificate or software, the Issuer can hold the Subscriber liable for losses.

The Subscriber is responsible for their subcontractors. The Subscriber shall require all subcontractors ensure their deliveries comply with requirements in this agreement and any supplementing provisions given by the Issuer.

6.3 Ansvar der Kunden feilaktig har stolt på en annens BankID

Utsteder er erstatningsansvarlig for direkte tap Kunden har lidt som følge av at Kunden på feilaktig grunnlag har stolt på en annens BankID, dersom Utsteder, noen Utsteder hefter for (for eksempel en underleverandør eller medhjelper) eller utsteder av det misbrukte sertifikatet, har opptrådt uaktsomt i forbindelse med utstedelse, bruk eller validering av den aktuelle BankID.

Ved følgende skadeårsaker må Utsteder godtgjøre at den eller andre som nevnt i første avsnitt, ikke har handlet uaktsomt (”omvendt bevisbyrde”):

a) BankID ble utlevert til uvedkommende,
b) de opplysninger som ble lagt inn i BankID ikke var korrekte på utstedelsestidspunktet,
c) BankID ikke inneholdt alle opplysninger som kreves i henhold til denne avtalen,
d) det ikke er benyttet forsvarlige produkter og systemer for utstedelse av BankID og fremstilling av digital signatur, eller
e) en tapsmelding eller tilbakekall av BankID ikke ble registrert på korrekt måte og det av denne grunn ble gitt uriktig svar på en gyldighetskontroll.

For indirekte tap som Kunden har lidd, er Utsteder ansvarlig dersom tapet skyldes grov uaktsomhet eller forsett fra Utsteders side.

6.3 Liability when the Subscriber mistakenly trusts another's BankID

The Issuer is liable for direct losses incurred by the Subscriber as a result of the Subscriber having mistakenly trusted another's BankID if the Issuer, someone for whom the Issuer is responsible (e.g. a sub-provider or agent) or issuer of a fraudulently used certificate, was guilty of negligence when issuing, use or validation of the BankID in question.

In the following cases the Issuer must prove that it or another entity specified in the preceding paragraph, is not guilty of negligence (”reverse burden of proof”):

a) The BankID was delivered to an unauthorised third party,
b) The BankID contained incorrect information when it was issued,
c) The BankID did not contain all the information required pursuant to this agreement,
d) The products and systems used to issue the BankID and produce digital signatures were inadequate, or
e) due to incorrect registration of a reported loss or recall of the BankID, the outcome of the validation was incorrect.

The Issuer shall only be liable for indirect losses suffered by the Subscriber if the Issuer is guilty of gross or wilful negligence.

Utsteder er likevel ikke erstatningsansvarlig for tap som skyldes at BankID har blitt brukt i strid med tydelige begrensninger i anvendelsesområde eller utover beløpsbegrensningen på NOK 100.000,-.

Utsteders ansvar kan begrenses eller falle helt bort dersom Kunden benytter BankID, programvare eller dokumentasjon i strid med denne avtale, herunder foretar uberettiget endring eller manipulering av BankID eller programvare.

Utsteders ansvar etter denne bestemmelse faller bort så langt Kunden har fått sitt tap dekket av andre, for eksempel av utsteder av det misbrukte sertifikat.

Notwithstanding, the Issuer shall not be liable for losses incurred as a result of the BankID having been used in violation of clear restrictions on use, or for transactions exceeding the upper limit of NOK 100,000.

The Issuer may have limited or no liability if the Subscriber uses the BankID, associated software/devices or documentation in violation of this agreement, which includes unauthorised modification or manipulation of the BankID or software.

The Issuer's liability shall be reduced by any compensation for loss the Subscriber receives from someone else, for example the issuer of a fraudulently used certificate.

6.4 Kundens ansvar overfor Utsteder ved sikkerhetsbrudd

Bruker Kunden PersonBankID, programvare eller dokumentasjon i strid med denne avtale, herunder uberettiget endrer eller manipulerer PersonBankID eller programvare, kan Utsteder holde Kunden erstatningsansvarlig for Utsteders tap som følge av dette. Med mindre Kunden har opptrådt forsettlig eller grovt uaktsomt er Kundens ansvar overfor Utsteder begrenset til NOK 100.000,-.

6.4 The Subscriber's liability towards the Issuer related to security breaches

If the Subscriber uses the Personal BankID, associated devices/software or documentation in a manner that violates the terms and conditions of this agreement, which includes unauthorised modification or manipulation of the Personal BankID or software, the Issuer may hold the Subscriber liable for any loss incurred by the Issuer. Unless the Subscriber is guilty of gross or wilful negligence, the Subscriber's liability towards the Issuer is limited to a maximum of NOK 100,000.

7. Gjeldende avtaler og policy

Det detaljerte policydokumentet Trusted Service Provider Statement (TSPS) finnes her: https://www.bankid.no/en/tsps_personal

7. Applicable agreements, CPS, CP

The detailed policy document Trusted Service Provider Statement (TSPS) can be found here: https://www.bankid.no/en/tsps_personal

7.1 Endring av avtalen og sikkerhetsprosedyrer

Er partene enige om det, kan avtalen endres. Endringen skjer i utgangspunktet på samme måte som ved inngåelse av ny avtale.

Utsteder kan likevel ensidig endre vilkårene med to ukers varsel i følgende tilfeller:

1) Dersom endringen ikke er til skade for Kunden
2) Endringer av fastsatte priser til skade for Kunden

Dersom forhold hos Kunden eller sikkerhetsmessige forhold gjør det nødvendig, kan Utsteder uten forhåndsvarsel begrense bruksområdet for BankID, senke beløpsmessige bruksbegrensninger og foreta andre endringer i sikkerhetsprosedyrer eller lignende.

7.1 Amendment of the agreement and security procedures

If the parties so agree, the agreement may be changed. The change shall be effectuated by means of the same medium used to enter into the agreement.

Notwithstanding, the Issuer is entitled to unilaterally change the terms and conditions, subject to two weeks' notice under the following circumstances:

1) If the change is not detrimental for the Subscriber
2) Changes of agreed prices, when such prices are detrimental for the Subscriber

If it is warranted by circumstances or security issues on the Subscriber's end, the Issuer may, without notice,

Utsteder skal snarest mulig etter endringen varsle Kunden om forholdet.

7.2 Opphør av avtalen

Kunden kan uten forhåndsvarsel si opp avtalen om BankID med mindre annet særskilt er avtalt.

Utsteder kan si opp avtalen med minst fire ukers varsel dersom det foreligger saklig grunn og det ikke er særskilt avtalt lengre oppsigelsesfrist. Grunnen til oppsigelsen skal opplyses. Utsteder kan med øyeblikkelig virkning heve avtalen ved vesentlig mislighold fra Kundens side. Grunnen til hevingen skal opplyses.

Ved opphør av avtalen eller Utsteder på annet saklig grunnlag forlanger det, skal Kunden straks makulere all programvare og dokumentasjon som Kunden har mottatt for bruk av BankID. BankID vil samtidig bli sperret og gjort ugyldig for videre bruk.

AnsattBankID

Ved tilbakekall eller ugyldiggjøring av alle AnsattBankID opphører avtalen med umiddelbar virkning.

limit the area of application for BankID, reduce limits on use, and change security procedures or the like. The Issuer shall notify the Subscriber as soon as possible after implementing such changes.

7.2 Termination of the agreement

Failing a contrary agreement, the Subscriber shall be entitled to terminate the BankID agreement with immediate effect.

The Issuer shall be entitled to cancel the agreement subject to four weeks' notice, provided it has factual reasons for such termination, and a longer notice period has not been agreed. The Issuer shall specify the reason for termination. The Issuer shall be entitled to terminate the agreement with immediate effect in the event of material default on the part of the Subscriber. The Issuer shall specify the reason for such termination.

Upon the termination of this agreement or if the Issuer for other sound reasons demands, the Subscriber shall promptly destroy all software and documentation the Subscriber has received for use of BankID. BankID will be invalidated for further use.

Employee BankID

Revocation or other types of invalidation of all Employee BankIDs, the agreement is terminated with immediate effect.

8. Personopplysninger

8.1 Behandling av personopplysninger

Utsteder vil i forbindelse med utstedelse og bruk av PersonBankID innhente og registrere opplysninger om Kunden og Brukeren. Slike personopplysninger innhentes direkte fra Kunden og Brukeren selv, fra Utsteders eget kunderegister og fra andre banker i forbindelse med bruken av BankID.

For å ivareta sikkerheten ved bruk av BankID og motvirke straffbare handlinger, kan Utsteder som ett av flere sikkerhetstiltak identifisere den datamaskin som Kunden anvender ved bruk av BankID, herunder brukeradferd og datamaskinens tilstand. Informasjon om datamaskinen, IP-adresse og eventuelle avvik fra normalt brukermiljø og brukeradferd, vil kunne anvendes for å motvirke og eventuelt følge opp straffbare handlinger rettet mot Kunden, Brukeren og/eller Utsteder. Brukerstedet vil kunne motta informasjon som indikerer hvilken risiko det er for at

8. Privacy policy

8.1 Personal information

The issuer will collect and store information about the Subscriber when BankID is issued and used. Such personal information will be gathered directly from the Subscriber or Subject, from the Issuer's own customer register and from other Issuers with use of BankID.

To safeguard the security of BankID use and prevent criminal offences, the Issuer may, as one of several security measures, identify the computer used by the Subject using BankID, including user behaviour and the state of the computer. Information about the computer, IP address and any deviations from the normal user environment and user behaviour may be used to prevent and possibly follow up criminal activity directed towards the Subject and / or Issuer. The BankID Merchant site may receive information indicating the risk of use of BankID may incur by an unjustified person (risk score). Such information will be

bruk av BankID kan være gjort av uberettiget person (risikoscore). Slik informasjon vil bli gitt til Utsteder eller til det brukersted som BankID er benyttet mot.

Personopplysningsloven av 20. juli 2018 nr. 38, som gjennomfører personvernforordningen (forordning (EU) 2016/679) om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (heretter benevnt personvernreglene), inneholder regler om registrering og annen form for behandling av personopplysninger. På denne bakgrunn har Utsteder utarbeidet Utsteders personvernregler.

8.2 Opplysninger i BankID. Utlevering av opplysninger til andre

BankID inneholder følgende opplysninger:

- Angivelse av sertifikatutsteder
- Opplysninger om Brukerens navn og fødselsdato. Kallenavn eller pseudonym skal ikke anvendes
- Unik identifikator for identifisering av Kunden
- Gyldighetsperiode for BankID
- Data som er nødvendig for fremstilling av Brukerens digitale signatur og verifisering av denne
- Sertifikatutsteders digitale signatur
- Data som entydig identifiserer det enkelte BankID (serienummer)
- Angivelse av BankID som kvalifisert sertifikat
- Angivelse av den bank som inngår avtale med Kunden

Ved bruk av BankID vil disse opplysningene inngå i meldingsutvekslingen og kan gjøres tilgjengelig for meldingsmottaker herunder brukersteder.

Andre opplysninger om Kunden eller Brukeren vil kun bli utlevert til meldingsmottaker herunder brukersteder så fremt Utsteder har lovbestemt opplysningsplikt eller det foreligger et uttrykkelig samtykke fra Kunden eller Brukeren.

PersonBankID

For å oppnå sikker identifisering av Kunden i forbindelse med Kundens bruk av PersonBankID, vil Utsteder for kontrollformål utlevere Brukerens fødselsnummer til brukersteder som har lovhjemmel til å registrere Brukerens fødselsnummer og som Brukeren enten har oppgitt fødselsnummer til i forbindelse med bruk av BankID eller som allerede har registrert Brukerens fødselsnummer.

AnsattBankID

given to the Issuer or the Merchant site where BankID is used.

The Personal Data Act of 20th of July 2018 nr. 38, which implements the EU General Data Protection Regulations ((EU) 2016/679) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, contains rules regarding registering and handling of personal data. These form the basis for the Issuer's general rules for handling customer data.

8.2 Information in the BankID. Delivery of information to others

A BankID contains the following information elements:

- The certificate issuer
- The Subject's name and date of birth. Aliases or pseudonyms may not be used.
- Unique identifier for confirming the Subject's identity
- Period of validity for the BankID
- Data required to produce and verify the Subject's digital signature
- The digital signature of the certificate issuer
- Unambiguous identifier of the individual BankID (serial number).
- Statement the BankID is a qualified certificate
- Specification of the bank that has entered into an agreement with the Subject.

When the BankID is used, this information will be included in the message exchange and can be accessed by the recipient of the message, including merchants.

Other Subscriber or Subject data will only be given to message recipients, including relying parties, when the Issuer has a statutory obligation to do so or the Subscriber or Subject has given his/her express consent.

Personal BankID

To ensure secure identification of the Subject when he/she uses BankID, for purposes of verification the Issuer will give the Subject's national ID number to merchants to which the Subject has given the same, or which have already lawfully registered it in their records.

Employee BankID

Employee BankID also includes

For AnsattBankID inneholder i tillegg

- Kundens organisasjonsnummer
- Angivelse av sertifikatholderen som Bruker av AnsattBankID

For AnsattBankID skal Kunden påse at Brukeren undertegner en erklæring som inneholder regler om Utsteders behandling av personopplysninger i forbindelse med bruk av AnsattBankID.

- Subscriber's organisational number
- Statement the Subject is using an Employee Certificate

For Employee BankID, the Subscriber shall ensure Subjects sign a declaration containing the Issuers handling of personal information related to use of Employee BankID.

9. Angrerett

Ingen refusjon blir gitt. Alle kjøp av sertifikater er endelig.

9. Refund policy

No refunds will be made. All certificate purchases are final.

10. Tvisteløsning

Avtalen er regulert av norsk lov.

Oppstår det tvist mellom Kunden og Utsteder for PersonBankID, kan Kunden bringe saken inn for Finansklagenemnda for uttalelse når nemnda er kompetent i tvisten og Kunden har saklig interesse i å få nemndas uttalelse.

10. Applicable law, complaints and dispute resolution

This agreement is regulated under the laws of Norway.

For Personal BankID, in the event of any dispute between the Subscriber and the Issuer pertaining to this agreement, the Subscriber may present the matter to the Norwegian Banking Complaints Board for an opinion in cases where the board is qualified to render such opinion and the Subscriber has good grounds for seeking the committee's opinion.

11. Utsteder og lisenser, tillitsmerker og revisjon

Denne utstederen (TSP) har blitt sertifisert for å være i overensstemmelse med sertifikatpolicy for EU Kvalifiserte Sertifikater for fysiske personer (QCP-n) etter eIDAS-forordningen.

Utstederen er på EU Trusted List, se Nkoms websider: https://www.tl-norway.no/TSL/NO_TSL.PDF

Revisjon av tredjepart har blitt utført av TÜVIT ifølge ETSI EN 319 403.

11. TSP and repository licenses, trust marks, and audit

The TSP has been certified to be conformant with the Certificate Policy for EU Qualified Certificate natural persons (QCP-n), that comply with the eIDAS regulations.

The TSP is on the EU Trusted List, see the Norway Communication Authority website https://www.tl-norway.no/TSL/NO_TSL.PDF

Third-party Audit was conducted by TÜVIT according to ETSI EN 319 403.