Norsk:

Public key infrastructure Disclosure Statement for PersonBankID - 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 og Avtale om BankID.

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

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

Dokumenthistorikk:

Versjon 1.3 (26.08.2022): Oppdatert som et enkeltstående dokument som er knyttet til «Avtale om BankID»

Versjon 1.2 (13.11.2020): Oppdatert 3. avsnitt i kapittel 2.4. Godkjent av BankID Policy Board den 13.11.2020.

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.

English:

Public key infrastructure Disclosure Statement for Personal 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 and BankID agreement.

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

Document history:

Version 1.3 (26.08.2022): Updated as a standalone document attached to BankID Agreement

Version 1.2 (13.11.2020): Updated 3rd paragraph in section 2.4. Approved by BankID Policy Board on 13 November 2020.

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. Kontaktinformasjon til utsteder

Eika Gruppen AS
Parkveien 61
0201 Oslo

https://www2.eika.no/eika-alliansen/eikagruppen

For sperring av BankID eller andre spørsmål om sertifikater, ta kontakt med utstedende bank på e-post eller telefon, eller Eika Servicesenter direkte på: +47 915 03 850.

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 Finansavtaleloven og kontoavtale inngått mellom Kunde og kontobank.

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.

1. Trust Service Provider contact info

Eika Gruppen AS
Parkveien 61
0201 Oslo

https://www2.eika.no/eika-alliansen/eikagruppen

For revocation request or other certificate questions the customer may contact their individual bank's customer service by mail or telephone, or Eika Service Centre directly: +47 915 03 850.

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 and the account agreement between the Subscriber and the account bank.

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 kan utstedes til fysiske personer registrert i det norske Folkeregisteret.

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 can be issued to natural persons registered in the National Population Register of Norway.

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, med 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 norsk Nasjonalt ID-kort, gyldig utenlandsk pass eller andre dokumenter som etter en risikobasert 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

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 Norwegian National ID-card 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.

The Subject or Subscriber shall promptly notify the Issuer of any change of name or address or other

andre opplysninger som er gitt Utsteder under dette avtaleforholdet.

information given to the Issuer in connection with this agreement.

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.

Brukeren må gjøre seg kjent med innholdet i sertifikatet og 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 eller sikkerhetsutstyr dersom dette er nødvendig av sikkerhetsmessige grunner eller ved nødvendige oppgraderinger av BankID.

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 Subject must familiarise himself/herself with the contents of the certificate and 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 necessary for security reasons or needed upgrades of BankID.

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.

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.

3. Bruksbegrensninger

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

3. Reliance limits

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

4. Kundens ansvar

4.1 Avtale om BankID

Kunden skal oppfylle alle vilkår i «Avtale om BankID». Denne avtalen kan finnes her: https://www.bankid.no/privat/personvern-og-regler/

4.2 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. 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 Finansavtaleloven.

4.3 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 kommet bort eller at uvedkommende har fått kjennskap til passord/personlig kode. Kunden skal benytte de meldingsmuligheter Utsteder har stilt til disposisjon, og for øvrig 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.

4. Obligations of subscribers

4.1 BankID agreement

The customer must fulfil all the obligations in the BankID agreement. Which can be found here: https://www.bankid.no/privat/personvern-og-regler/

4.2 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, and otherwise follow the Issuer’s security instructions.

When BankID is used as a security device for payment instruments the Financial Agreement Act applies.

4.3 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 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.

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.

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.

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.

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.

5. Kontroll av sertifikatstatus

Hver gang et BankID sertifikat blir benyttet, 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 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.

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.

5. Certificate status checking obligations of relying parties

Every time a BankID certificate is used, the certificate status must be checked to verify its validity.

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 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.

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.

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.

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. Ansvar ved misbruk av Kundens BankID

Ansvar for misbruk av kundens BankID følger norsk lovgivning.

6. Limited warranty and disclaimer/Limitation of liability

Limitations of liability are according to Norwegian law.

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

8. Personopplysninger

Banken din er behandlingsansvarlig, og vil behandle dine opplysninger i henhold til personvernreglene (GDPR). For mer opplysninger, se her www.bankid.no/privat/personvern-og-regler/

8. Privacy policy

Your bank is the data controller for your personal data and will process your personal data in accordance with the data protection rules and legislation (GDPR). For further information, see here www.bankid.no/en/private/protection-of-privacy-and-status/

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

PDSen 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 PDS 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.