SpareBank1 PDS Personal v1.0

BankID TSP documents

This Public Key Infrastructure disclosure statement - PDS, is structured according to ETSI EN 319 411-1 Annex A. This document is a supplement to and not a replacement for 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	Date	Changes	Approved by
1.0	29.11.2018	Final version for publishing document.	BankID Policy Board

1 Trust Service Provider contact info

Organisation name:	SpareBank 1 Banksamarbeidet DA
Organisation number:	986401598
Visiting address:	Hammerborggata 2, 0179 Oslo
Mailing address:	Postboks 778 Sentrum, 0106 Oslo
Contact person:	Mona Forsbakk Engebretsen
Website:	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 Certificate type, validation procedures and usage

Issuance of BankID certificates is governed by the provisions of the Electronic Signature Act, which implements the EU Electronic Signatures Directive. The law with associated regulations imposes requirements on issuers who must arrange systems, rules and procedures to safeguard the security of the certificates. Qualified certificates issued by the Trust Service Provider under BankID Scheme are issued in compliance with REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

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 the Electronic Signature Act § 3, No. 2.

Employee BankID is a certificate which in addition confirms a link between the Subscriber and a Subject, a uniquely identified natural person associated with the Subscriber. Employee BankID is used by the natural person for services or tasks on behalf of the Subscriber.

Specific for single issuer: Issuer has been registered with the Norwegian Communications Authority (Nkom) as issuer of qualified certificates and shall comply with the rules laid down in Act 15 June 2001 No. 81 on electronic signatures including the rules of liability in section 22.

Specific for Joint Issuer: It is the TSP which issues the Personal BankID with which the Issuer signs an agreement with its customers. The TSP is registered with the National Communications Authority (Nkom) as the issuer of qualified certificates and shall comply with the rules laid down in Act 15 June 2001 No. 81 on electronic signatures, including the rules of liability in section 22. These regulations come in addition to the responsibility Issuer has undertaken in accordance with the terms of this agreement. The certificate issuer's liability is limited to NOK 100,000.00. Issuer's liability is governed by clause 13 of the agreement.

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

2.1 Eligibility for a BankID certificate

Personal BankIDs can be issued to natural persons.

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 and has an account in the issuing bank. The business with the legal obligation is referred to as Subscriber, while the natural person identified in the certificate is referred to as Subject.

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.

2.2 Prices and price information

Charges for issuing, holding and using Personal BankIDs 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 Personal 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 Identity checking and identification requirements

The Electronic Signature Act Section 13 requires issuers to ensure that the identity of the certificate holder is checked and verified in a secure manner.

Upon 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.

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 by a Certificate of Registration from the Norwegian Register of Business Enterprises ("Firmaattest fra Foretaksregisteret"). The issuer can request further information or documentation, and conduct further investigations of the correctness of the information, authorisations etc.

As a basis for verification of the Subject's identity, the Subject shall provide the Issuer with identification in the form of a valid Norwegian passport, a document equivalent to a Norwegian passport or a foreign passport.

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.

2.4 Delivery of Personal 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 necessary for security reasons or needed upgrades of 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 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.

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

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 Reliance limits

If the Subscriber uses the Personal BankID, associated devices/programs or documentation in a manner which violates the terms of this agreement, including 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. No such limitation applies to the use of Employee BankID.

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 Subscriber or Subject in accordance with article 3 no. 2 of the Electronic Signature's Act. 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.

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 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.

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.

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.

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 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 Electronic Signature Act and associated regulations require issuers of BankID certificates to have systems, rules and procedures in place to allow issuers to 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 rejected or if the certificate contains incorrect information.

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 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 Liability in the event of unauthorised use of the Subscriber's BankID

6.1.1 Personal BankID is used for unauthorised debiting of the Subscriber's account

If the Subscriber suffers loss from Personal BankID being used with the unauthorised debiting of the Subscriber's account in the issuing bank, the liability of Issuer and Subscriber is governed by Section 35 of the Financial Agreement Act, cf. § 36 and 37 and by the Subscriber's agreement with its bank regarding the use of the applicable payment instrument.

6.1.2 Unauthorised use of BankID aside from debiting an account

If unauthorised use of the Subscriber's BankID in situations other than those mentioned above, the unauthorised person may claim to be the Subscriber and thus gain knowledge of Subscriber's information or attempt to enter into agreements on behalf of the Subscriber. 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.

Issuer is only responsible for the Subscriber's financial loss as a result of another's misuse of the Subscriber's BankID as described in the previous section, if the Issuer has shown negligence and this is the reason for the loss.

6.1.3 Employee BankID

The Subscriber is responsible for usage conducted by anyone who has had the opportunity to use Employee BankID issued to the Subscriber's Subjects based on wilfully or negligent actions or failure of the Subscriber og 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 og 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 deliveries to comply with requirements in this agreement and any supplementing provisions given by the Issuer.

Section 35 of the Financial Agreement Act does not apply for responsibilities between the parties for unauthorised access of the Subject's account at the Issuer.

6.2 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 latter having mistakenly trusted another’s BankID if the Issuer, someone for whom the Issuer is responsible (e.g. a sub-provider or agent) or another issuer was guilty of negligence in connection with the issuance, 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.

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 as specified in the certificate.

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.

6.3 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 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 Amendment of the agreement and security procedures

If the parties so agree, the agreement may be changed. The change shall be effected 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, 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 the Subscriber's relationship with the Issuer or if so demanded by the Issuer for other sound reasons, the Subscriber shall promptly destroy any software and documentation provided to enable the Subscriber to use the BankID. At such time, the BankID will be blocked and made invalid for further use.

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

The Norwegian Personal Data Act of 14 April 2000 contains rules regarding registering and handling of personal data. These form the basis for the Issuer's general rules for handling personal data (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. Nick names and pseudonyms may not be used. For Employee BankID this also includes Subscriber's name and Norwegian organisational number.
- 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).
- Confirmation that the BankID is a qualified certificate
- Specification of the Issuer that has entered into an agreement with the Subject.
- Specification of usage amount limits.

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.

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.

Other subject data will only be given to message recipients, including merchants, when the Issuer has a statutory obligation to do so or the Subject has given his/her express consent, in accordance with articles 8, 9 and 11 of the Personal Data Act and article 7 of the Electronic Signatures Act.

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 Refund policy

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

10 Applicable law, complaints and dispute resolution

This agreement is regulated by and shall be construed 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 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 and legal person (QCP-n/QCP-l), 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

The Third party Audit, conducted by TÜVIT according to ETSI EN 319 403.