BankID Rules

Established by Finance Norway Service Office following review by the Industry Board of Payment Systems and Infrastructure on 28th November 2013.

Document history

Version	Date	Changes	Approved by
1.0	15.03.2018	Updated	Bits

1. Scope and field of application

The rules apply to the issuing and processing of BankID.

BankID are electronic certificates that can be used by subjects to send and receive secure electronic messages to and from other subjects by verifying the identities of the parties (authentication), protecting the contents against change (integrity), attaching the message to a specific party (non-repudiation) and/or to hide the contents from unauthorised persons (encryption).

Issuance of BankID certificates is governed by the provisions of the Electronic Signatures Act, which implements the EU eIDAS Regulation. The Act and its associated regulations, including the Requirements Specification for PKI in the Public Sector, require issuers to provide appropriate systems, rules and procedures to safeguard certificate security.

The BankID Rules is a multilateral agreement setting out the rights and obligations of the participating entities in the BankID collaboration, including issuers of BankID certificates, BankID Norge AS and Bits AS (referred to as Bits).

The right to participate in the BankID collaboration is granted to entities authorized to operate payment services in Norway and which have the right to participate in interbank systems reported to the EFTA Surveillance Authority in accordance with EU Directive 98/26/EC, cf. the Payment Systems Act Chapter 4, and are affiliated to Bits through membership in the Finance Norway Service Office, or that have agreed to comply with "BankID Rules" following consent from Bits. Consent is dependent on payment of an affiliation fee. Entities are granted access based on fair, reasonable, non-discriminatory terms.

2. BankID Norge AS

BankID Norge AS maintains joint administrative, operational and business tasks in relation to BankID. All BankID related business performed by BankID Norge AS is performed in accordance with the agreement between Bits and BankID Norge AS.

All BankID related business performed by BankID Norge will be performed within the framework of BankID Rules and any other regulations stipulated by the Finance Norway Service Office and Bits pursuant to BankID Rules.

All BankID related business performed by BankID Norge shall comply with any currently applicable BankID security requirements, as defined and managed by Bits.

3. Issuing Level 1 Certificates and BankID

3.1 BankID Certificate Hierarchies

The Financial Services Service Office and The Norwegian Savings Bank Association Service Office have jointly established the top level in a trust hierarchy and issued a root certificate to themselves. Based on this root certificate and the associated keys, the Service Offices have issued Level 1 certificates to issuers of BankID.

As of 1st January 2010, FNO assumed all tasks and responsibilities as issuer and subject of the root certificate previously held by the Service Offices. From this date onward FNO was responsible for issuing Level 1 certificates to the issuers of BankID.

As of 1st January 2011, Finance Norway Service Office assumed all tasks and responsibilities as issuer and subject of the root certificate previously held by FNO. From this date onward the Finance Norway Service Office was in charge of issuing Level 1 certificates to the issuers of BankID.

As of 1st April 2016, Bits assumed the majority of tasks and responsibilities previously held by the Finance Norway Service Office.

The issuer of BankID is the entity signing BankID with a Level 1 certificate issued by either the Financial Services Service Office, The Norwegian Savings Bank Association Service Office, FNO or the Finance Norway Service Office. The BankID must show who the issuer is.

When a BankID is issued as a qualified certificate, the issuance and issuer's activities, tasks and responsibilities are also governed by the Electronic Signatures Act.

3.2 Issuance of Level 1 Certificate to Issuers of BankID

The Finance Norway Service Office will issue a Level 1 certificate to the participant and others (joint issuers) who have the right to issue BankID according to these rules. The Finance Norway Service Office may use BankID Norge AS to perform all or part of the processes involved in issuing the Level 1 certificate.

Prior to issuing a Level 1 certificate, the participant must submit a statement to the Finance Norway Service Office wherein the participant agrees to comply with BankID Rules. The statement must be signed by the CEO of the participating entity. If one or

more participants wishes to use a joint issuer, this must be made clear in the statement, and the statement must be jointly signed by the CEO of the joint issuer. When the statement has been approved, Bits will confirm the conditions for issuing a BankID are met, and send the confirmation to the participant, any joint issuers and BankID Norge AS.

Before a joint issuer receives a Level 1 certificate, the joint issuer must be approved by Bits in accordance with the rules in article 6.

Bits prepares a standard statement as mentioned in the second paragraph.

3.3 Who can issue BankID

BankID can be issued by participants who have agreed to comply with these Rules. In addition to participants, other entities may, by special permission from Bits pursuant to the rules in article 6, issue BankID on behalf of a participant or a group of participants. However, it is always the participant who enters into an agreement with BankID subscribers.

3.4 BankID subjects

BankID can be issued to

- Natural persons
- Natural persons who are employed by or perform services for a legal person (private or public business and administration) who is registered in the Central Coordinated Register for Legal Entities or a similar public register within the EEA, known as Employee BankID
- Legal persons (private or public business and administration) registered in the Central Coordinated Register for Legal Entities or a similar public register within the EEA

BankID cannot be issued to persons under 15 years old. BankID can still be issued to persons between 13 and 15 years, if guardian consent is provided.

BankID cannot be issued to persons who have partially or wholly lost the legal capacity to manage their own affairs.

3.5 BankID as a qualified certificate

BankID issued to natural persons shall comply with the requirements for qualified certificates pursuant to the Electronic Signatures Act, and issuers of BankID to natural persons will notify the Norwegian Communications Authority (Nkom) of the status as issuer of qualified certificates, cf. Regulation on voluntary self-declaration schemes for certificate issuers.

3.6 Use of BankID and similar schemes as the basis for issuing banking identity credentials

BankID shall not be issued to a natural person on the basis of a BankID issued by another participant or on the basis of other types of electronic credentials.

A BankID shall not be used as basis for issuance of physical or electronic credentials.

A Personal BankID which a participant has issued, or entered into an agreement about, can still be used by the same participant as a element required to issue identification instruments other than a BankID to customers.

4. Design of BankID. Requirements for physical and logical security

4.1 Definition of Certificate Policies
BankID Norge AS defines and administrates certificate policies for BankID.

4.2 Requirements to physical and logical security.
Bits is responsible for the definition of security requirements for BankID within the framework of these rules. Bits can make exceptions to their own requirements on a case-by-case basis, provided this is justified by fair, reasonable and non-discriminatory considerations.

Systems and other physical equipment used for BankID must conform to the requirements for physical and logical security defined by Bits. Bits has the right to check these requirements are met. Bits has the right to approve systems and other physical equipment. Approval should only be denied if this is based on just, reasonable and non-discriminatory terms.

Bits will develop and manage guidelines for the control and approval of systems or other physical equipment, as well as guidelines for allocation of costs of such inspection and approval.

5. Trademarks

A trademark or logo should always be used with, or be attached to, the certificate, so users and others who come into contact with the certificate can connect the certificate to the trademark and vice versa. Likewise, the trademark should, as far as possible, be associated with the use of the certificate, including being visible on merchants' sites to show subjects that BankID may be used.

BankID Norge AS has the rights to the trademark and determines its design and use.

If a participant or BankID Norge AS issues or enters into an agreement about an electronic certificate that is not a BankID, the issuer must ensure the certificate cannot be confused with a BankID.

6. Using a joint issuer or subcontractors for BankID services

6.1 Approval of joint issuers

A participant may only use a joint issuer to produce a BankID or deliver services related to BankID if the joint issuer is approved by Bits in accordance with the rules below. Approval may also be given in accordance with general rules. Bits may specify which joint issuers require approval in general, and in individual cases.

6.2 Terms for approval of joint issuer

Participants who use a joint issuer must control the joint issuer fully, either solely, or in partnership with other participants. If the joint issuer is a limited company, the company must be wholly owned by the participants who use the joint issuer. The provisions in this section do not apply if the joint issuer is a participant.

Participants who use a joint issuer must ensure that the joint issuer can fulfil the indemnity requirements of the Electronic Signatures Act, as well as cover any liability the joint issuer may incur under the Electronic Signatures Act or these Rules, including the agreement in the next paragraph. This requirement may be met through holding appropriate amounts of equity, or through ownership or guarantees/indemnity forms from the participant(s) who are using the joint issuer, or by insurance.

The participant must enter into an agreement with the joint issuer that governs rights and obligations, sets out the assignment of tasks, responsibilities and duration of the agreement, as well as any legal requirements.

6.3 Application for approval of joint issuer – change notification

Any application from collaborating participants for the approval of a joint issuer must as a minimum contain the following information:

a) The name, address and entity number of the joint issuer,
b) Ownership and participant relationships, board composition and general manager of the joint issuer,
c) Terms under which new participants can join and participate. If using a joint issuer is subject to membership, capital contributions and/or guarantees/indemnity forms, this must be explicitly stated.
d) A plan for the resolution of operational issues when a participant joins or leaves, including invalidating the relevant Level 1 certificate and issued BankIDs.
e) A plan for how the joint issuer is organized and run, including the distribution of tasks between the joint issuer and the participant, and
f) Measures to secure the ICT operations of the joint issuer, including whether the participant has ensured the joint issuer fulfils the requirements listed in The Financial Supervisory Authority's ICT Regulations.

Any agreement as mentioned in article 6.2, third paragraph, shall be attached to the application.

The application should be sent to Bits with a copy to the Finance Norway Service Office.

The cooperating participants or the joint issuer shall notify Bits of any significant change to the relationships mentioned in the first paragraph. The change can be implemented if Bits has not made any other decision within 4 weeks of the notification being received.

6.4 Declaration of subcontractors

Participants and approved joint issuers who use one or more subcontractors for the production of BankID or the delivery of services related to BankID, shall notify Bits about which subcontractors the participant or joint issuer uses.

The notification shall as a minimum contain the details of the subcontractor's name and entity number, the functions and tasks performed by the subcontractor, and other information about the subcontractors and their activities relevant to Bits' management and inspection of physical and logical security for BankID. Any changes affecting the submitted information must be reported to Bits without undue delay.

Bits sets out more detailed rules for the content of the notification, related documentation, submission routines, and the inspection, supervision and control of subcontractors. Bits may generally and in individual cases set out more specific rules for the safety and quality requirements that must be met by subcontractors.

Bits may prepare and publish an overview of registered subcontractors and establish routines for a simplified registration system.

6.5 Responsibility for the Banks' own subcontractors and joint issuers

BankID Rules and provisions issued pursuant to these apply irrespective of which subcontractors or joint issuers the participant uses, and the individual participant has a responsibility towards other participants to make sure subcontractor and joint issuer follow the rules.

When the participant enters into any agreements with subcontractors or joint issuers, they must ensure the agreement imposes compliance with the requirements set out in these rules and supplementary provisions provided by Bits.

7. BankID content

BankID must as a minimum contain the following:

a) Issuer's name
b) Subject's name
c) Validity period for BankID
d) Signature verification data for the subject
e) Issuer's digital signature
f) Data that uniquely identifies each individual BankID (serial number)

g) The name of the participant who enters into an agreement with the subject
h) Indication of BankID status as qualified certificate
i) Indication of any financial limits.

8. More details of BankID content

The issuer will be identified using a unique identifier.

The subject must be identified using the subject's name as it is appears in the bank's customer register, and a unique identifier defined by BankID Norge AS and approved by Bits. If the certificate is issued to a natural person, the subject's date of birth shall appear in the certificate.

The issuer's digital signature must be verifiable using a certificate issued by the service offices, FNO or the Finance Norway Service Office. Bits may set detailed rules for such certificates. Such rules may pertain to issuance, use, verification, revocation, liability, distribution of liability in case of compromise, and so on. BankID Norge AS issues certificates on the request of Bits.

9. Entering into agreements. Participant checks when issuing BankID

9.1 Entering into agreements

Before a BankID can be issued, the participant must enter into a written customer agreement with the subject regarding the use of the BankID. For Employee BankID, the participant enters into the customer agreement with the employer, or legal person, and the legal person collects a declaration from the employee, see article 10.1 and 10.4.

For issuing BankID to legal persons, participants may authorize BankID Norge AS or others to enter into the agreement with the subscriber on behalf of the Bank.

9.2 Personal Data

Personal data required to issue, use or invalidate a BankID may, pursuant to § 7 in the Electronic Signature Act, only be obtained directly from the subject, or with the subject's express consent. The information may only be used for purposes that comply with the Act, including statistical purposes, unless the subject has given his or her explicit consent that the information may be used for other purposes. The participant shall detail the purpose of the use of collected personal information in the customer agreement and inform the subject that the information will be disclosed to other subjects during use of BankID.

9.3 Verification and identification of subjects

Upon issuing BankID, participants must verify the identity of the subject, cf. the Electronic Signature Act § 13. The subject's identity shall be verified by personal attendance at the premises of a participant or a representative of the participant, unless

the subject has already been identified by personal attendance during the process of establishing the customer relationship.

9.4 Requirements for ID documents

The first time a BankID is issued to a natural person, the individual's identity will be verified on the basis of a valid Norwegian passport, a foreign valid passport or another identity document which, following a individual risk-based evaluation, is considered valid identification with the same security level as a Norwegian passport. There is no need to check the subject's passport when issuing a BankID if the subject's identity was verified with a passport during personal attendance in connection with the establishment of the customer relationship.

The requirement for identity verification by means of a passport may be waived if the participant is certain of the person's identity, and

- The subject established a customer relationship at a participating bank prior to March 1, 2007, or
- The requirement for identity verification by means of a passport will entail an unreasonable additional burden on the person concerned, due to age, health or other special circumstances.

If the requirement for passports can be waived, participants must instead submit another form of ID according to the requirements for physical ID documentation in the Money Laundering Act and associated regulations.

9.5 Complementary rules and recommendations

Bits may add additional rules on ID checks and identification of subjects, including holders of Employee BankID, in accordance with the rules in article 10.3.

Bits provides further guidance on understanding the rules at the start, including what is meant by Norwegian passports, documents equivalent to Norwegian passports, and foreign passports, and to what extent participants demand additional documentation for confirmation of foreign persons' identities and place of residence. Bits may also provide recommendations about how validation rules are applied.

10. Separate rules for Employee BankID

10.1 Scope etc.

Employee BankID must confirm a link between an identified entity (legal person) and a uniquely identified natural person (the user) within the entity.

Participants must enter into an agreement with the legal person for the use of Employee BankID prior to issuing such BankIDs. The agreement shall amongst other things include terms stating that Employee BankID should only be used by employees and contractors for official duties or assignments on behalf of the legal person.

10.2 Contents of Employee BankID
In addition to requirements as described in article 7, Employee BankID shall contain the legal person's name and Norwegian entity number.

Bits may approve an alternative unique identifier to the Norwegian entity number for legal persons that are not registered in Norway.

10.3 Identity validation
The participant shall ensure before Employee BankID agreements are entered into, the identities of the subscriber, subjects and a representative for the subscriber, are verified and validated. The identity validation must be based on personal attendance at the participant's premises or at the premises of a representative of the participant. The participant shall comply with the requirements for identity validation and documentation as set out in articles 9.3 to 9.5.

10.4 User statements
Participants shall, through the agreement with subscriber, ensure that the subscriber collects a statement from subjects regarding compliance with the usage and security rules for Employee BankID.

11. Identity validation when issuing a BankID to a legal person

Upon entering into a BankID agreement with a legal person, the legal person shall be represented by the signatory or someone who has been expressly authorized by the signatory to enter into a BankID agreement on behalf of the legal person. A sole proprietorship shall be represented by the proprietor of the sole proprietorship or a person authorized by the proprietor to enter into a BankID agreement on behalf of the sole proprietor.

The legal person and the natural person(s) who represent that legal person must be identified and verified in accordance with the provisions of the Act on Money Laundering.

12. Participants' mutual recognition of BankID

Participants who enter into BankID agreements according to these rules shall assume that any persons who use a BankID as identity validation, but where the agreement has been entered into with another participant, is the correct person unless the participant suspects that the rules have been violated, or that unauthorized persons are using the relevant BankID.

13. Invalidating and reactivating 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 invalidate (suspend or revoke) a certificate on reasonable grounds related to security,

or if keys and associated codes have been compromised or the certificate contains incorrect information.

When a BankID has been revoked, it cannot be reactivated. The participant may instead choose to suspend the BankID temporarily for up to 30 days. The participant can reactivate a suspended BankID before 30 days, provided the reason for the suspension is no longer present.

Participants shall ensure that appropriate procedures are in place for receiving and processing messages from their own subscribers/subjects who wish to invalidate a BankID.

If the BankID no longer contains the correct information or the participant becomes aware that the terms for issuing the BankID to a subject are no longer present, the participant shall revoke the BankID concerned.

14. Validation

The participant shall confirm or cancel the validity of a BankID if requested to by a subject with whom the participant has entered into a BankID agreement. Confirmation regarding BankIDs issued by other participants is given on the basis of information obtained from the participant concerned and on behalf of this participant.

Participants who are entering into a BankID agreement shall ensure that the agreement stipulates that merchants are required to make such validity requests.

At the request of another participant, participants shall confirm or disprove the validity of a BankID agreement into which the participant has entered.

A response to a request from a subject shall as a minimum contain:

- Information about whether a BankID is revoked or suspended;
- Information about whether the BankID is unknown.

In addition to this, BankID Norge AS may add other requirements for the validation request and the contents of the dialogue between subjects and merchants. Bits may also add requirements beyond the minimum if this is necessary to safeguard fair, reasonable, non-discriminatory security requirements.

15. Registration and use of certificate information and national identification number

15.1 Registration of Certificate Information

The participant shall establish, or ensure that a register is established for issued BankIDs. This register will serve as a basis for answering validation requests cf. article 14. As a minimum, the register shall contain information about the subject's name,

date of birth and unique identifiers. The register shall be continuously updated to record revoked and suspended BankIDs.

In addition to these requirements, Bits may add additional requirements for the issuers to register further information necessary for safeguarding security.

BankID Norge AS may set additional requirements for issuers' registration of information, including register content and operational quality, including response times, time-outs, uptime and updates.

15.2 Logging, archiving and retrieval

The participant shall establish satisfactory procedures for logging, archiving and retrieval of information in connection with issue, revocation, suspension and inquiries, or ensure that these are established.

The participant shall store certificate information as stated in article 15.1, first and second paragraphs, for a minimum of 10 years after the expiration or revocation of a BankID. Other recorded information (including validation requests and responses) shall be stored for as long as this is deemed necessary in view of the purpose of registering and storing the information.

Received and registered information may only be used for purposes that are consistent with this regulatory framework, including statistical purposes. BankID Norge AS may stipulate further requirements for information that should be registered, logged, archived and retrieved.

15.3 Registration and disclosure of national identification numbers

The participant shall register national identification numbers (11 digits) belonging to subjects to whom the participant has issued BankID. This registration assumes the subject has explicitly accepted that the national identification number can be disclosed to merchants to whom the subject has already disclosed the national identification number, or who are already legally keeping records of the national identification number.

National identification numbers can only be disclosed to merchants who can document the available certificate information in the BankID is insufficient to obtain secure identification of the subject, and who has already legitimately obtained the subject's national identification number. Each participant shall ensure that satisfactory procedures are established to verify that national identification numbers are only disclosed to merchants who meet these terms.

15.4 Data Processing Responsibility

The participant is responsible for processing personal information about subjects the participant has entered into a BankID agreement with. The participant is also

responsible for processing personal information received in accordance with these rules, from BankID Norge AS or the suppliers of BankID COI cf. article 25.

15.5 Duty to provide assistance and information exchange in connection with security incidents and abuse

In the event of security incidents or if a certificate no longer contains the correct information, participants who take part in message exchanges using BankID are obliged to assist other involved participants in preventing or limiting the extent of the incident or abuse, mapping the incident and its cause, and correcting any errors.

Insofar as fulfilment of such duty to provide assistance requires participants to obtain information about subject(s), such as IP addresses, validation information, or information about deviations and operational logs, it is expected that participants, BankID Norge AS or providers of BankID COI disclose such information without undue delay. The request for disclosure, specifying what information is required and the purpose of the disclosure must be documented.

Any distribution of personal data and other confidential information must be done securely in accordance with the Personal Data Protection Act and the requirements laid down by Bits.

16. Liability

If a participant, or a customer with whom the participant has entered into a BankID agreement, has suffered losses as a result of negligence with the issue, use or validation of a BankID they have acted in reliance on, on the part of a second participant or anyone this participant is liable for (such as a subcontractor or joint issuer), the second participant is liable for said losses.

For the following causes of damage, a participant must prove that there was no negligence on their part, or on the part of anyone for whom they were liable ("reverse burden of proof"):

a) A BankID was handed out to unauthorized persons;
b) The mandatory minimum information registered for a BankID was not correct at the time of issue;
c) A BankID did not contain all the information required according to these rules, cf. article 7;
d) A participant has not used appropriate products and systems for issuing BankIDs and creating digital signatures;
e) A participant failed to register its subscriber’s or subject’s loss notice, or invalidate BankIDs correctly, and therefore replied incorrectly to a validation request.

The participant is not liable for claims for damages caused by the certificate being used outside a specified scope clearly disclosed to the person who acts in reliance on the BankID.

The participant's liability according to the first and second paragraphs is in all cases limited to NOK 100.000 per transaction.

The participant is not liable for losses other participants suffer as a consequence of the participants or their customer using a BankID as the basis for issuing electronic certificates.

If a participant chooses to validate a BankID that a second participant has entered into an agreement about without performing the checks mentioned in article 13, the second participant is not liable for any losses resulting from this unless the participant can be held responsible for other reasons.

General rules for liability regulation between banks during payment processing will otherwise apply as appropriate.

If using BankID improperly created (e.g. fake BankID), and if the keys used for the creation of such BankID are owned by the Finance Norway Service Office, any losses should be covered by all participants in proportion to the number of BankID agreements they have entered into by the last year end before the date of the loss.

If BankID Rules are violated, this may result in sanctions under the General rules for liability regulation between banks during payment processing, insofar as they are appropriate. Bits may also impose a penalty if the violation means a significant security risk and risk of loss for other participants.

17. Loss of right to issue or enter into BankID agreements

A participant may lose the right to issue or enter into BankID agreements if the participant by gross negligence or deliberate breach, violates provisions within, or in accordance with these rules. General rules for liability regulation between banks during payment processing (§10) applies as appropriate during the evaluation period for the suspension or revocation of the participant's right to issue or enter into a BankID agreement, or in case of imposition of other penalties. The procedural and appeals rules in §§ 11-12 of the regulations likewise apply insofar as they are appropriate.

A participant who has entered into administration, or is subject to any other insolvency proceedings immediately loses the right to issue BankIDs or enter into BankID agreements. However, the participant may regain the right to issue BankIDs or enter into BankID agreements if the Administrator takes on all the participant's obligations and responsibilities according to these rules and other relevant regulations.

Bits can invalidate (suspend or revoke) a Level 1 Certificate if

- The recipient of the certificate loses the right to issue BankIDs or enter into BankID agreements, or ceases operations,

- Bits revokes approval of a joint issuer, or
- Changes in ownership, board composition, lack of equity, lack of security procedures or other reasons means a joint issuer no longer meets the necessary requirements.

If one of several participants using a joint issuer loses the right to enter into a BankID agreement or ceases to operate, Bits will determine if it is necessary to invalidate the Level 1 certificate.

If any participant loses the right to issue or enter into a BankID agreement pursuant to the provisions of this paragraph, all BankIDs the participant has issued or agreed on shall be invalidated without further decision. The same applies to BankIDs issued on the basis of a Level 1 certificate that is invalidated.

If a participant enters into administration or is subject to other insolvency proceedings, Bits may, at the request of the Norwegian Bank's Guarantee Fund, decide to postpone invalidating BankIDs issued by the relevant participant to natural persons, for up to three months. The Norwegian Banks' Guarantee Fund must then assume the participant's obligations and duties as issuer, including the liability arising from the Electronic Signatures Act and these BankID Rules.

18. Interpretation of the rules. Disputes

If a dispute arises between participants, or there are doubts about the interpretation or practice of these rules, any participant, and potentially Bits or BankID Norge AS, may bring the matter to the Contract Committee for a statement or decision. Detailed rules regarding treatment and decision making in the Committee are set out in the Regulations on dispute resolution.

19. Statistical information about BankID

The participants shall provide BankID Norge AS with an overview of the number of BankIDs they have issued at the end of each year. In addition to this, each participant is obliged to provide statistical information about the use of BankID according to further guidelines issued by BankID Norge AS.

Bits may retrieve information necessary to distribute liability under article 16, paragraph 8 from participants or BankID Norge AS on an annual basis.

20. When participants stop issuing BankID

A participant who no longer wishes to issue BankID or enter into BankID agreements shall immediately notify Bits, who will take the necessary measures so the participant can no longer issue BankID or enter into a BankID agreement.

A participant who stops issuing BankID shall, as long as there are subjects with valid BankID agreements previously issued by the participant, confirm the validity of such BankID and retain information about such BankID for at least 10 years after the last time the relevant BankID could have been used by the subject.

21. Termination of BankID

If a BankID is terminated, each participant is required to retain information about BankID agreements they have entered into and to be able to confirm the validity of such BankIDs for at least 10 years after the last time that BankID could have been used by the subject.

22. Suppliers of BankID COI

BankID Norge AS selects and enters into agreements with supplier(s) regarding operation, management and development of the joint operational activates in connection with BankID (BankID COI). BankID Norge AS defines the requirement for internal control and information security that has to be met by the supplier(s). The agreement with the supplier(s) shall also contain terms that comply with ICT Regulations and the rules of the Personal Data Act.

BankID Norge AS shall ensure that suppliers of BankID COI comply with the requirements in the Personal Data Act concerning processing of personal data, and that information is not disclosed or processed other than according to BankID Rules, or by written agreement with BankID Norge AS. The obligation of BankID Norge AS under this provision does not limit participants' data processing responsibilities according to the rules in article 13.4.

23. Changes

Bits may change these Rules with binding effect.

BankID Norge AS may propose changes to these Rules.

24. Glossary

Authenticate: To confirm the identity of the sender or recipient of an electronic document

BankID: One or more electronic certificates than can be used by one subject to secure electronic message exchange with another subject.

BankID COI: Common Operational Infrastructure that banks and joint issuers are obliged to use for part of their business related to BankID.

Merchant: Sole proprietorships and other legal persons (private or public business and administration) that have been issued with BankID for use in communication between the merchant and other subjects.

Bits: Bits AS

Joint issuer: A legal person who issues BankID on behalf of a group of participants and uses a Level 1 certificate for this purpose.

Where BankID Rules use the term participant, the rules also apply to the joint issuer as far as this is appropriate.

Valid BankID: A BankID that has not been revoked or suspended, and where the term of validity has not expired

Level 1 Certificate: Certificate issued by the Financial Services Service Office/The Norwegian Savings Bank Association Service Office, FNO or the Finance Norway Service Office, used to sign BankID issued to the customers of participating organisations.

Subject: Natural or legal person who has been issued with a BankID

Securing electronic message exchange: Verifying the identities of the parties (Authentication), protecting the contents against change (Integrity), attaching the message to a particular party (Non-repudiation) and/or hide the contents from unauthorised persons (Encryption).

Issue BankID: Sign BankID using the issuer's private key, corresponding to a public key in a Level 1 certificate issued by the Financial Services Service Office/The Norwegian Savings Bank Association Service Office, FNO or the Finance Norway Service Office.