



Stø – BankID Practice Statement

Version	v1.0 – English
Effective date	1 October 2026
Owner	Stø (issuer / BankID scheme operator / identity provider)
Contact	policy@sto.no
Scope	BankID (LoA High) issued by Stø

Document Control

Date	Version	Description of changes	Approved by
23. September 2026	V 1.0-EN		STØ IDLG Policy Board



Document Control	2
1 Introduction.....	5
1.1 Overview.....	5
1.2 Legal basis.....	5
1.3 Participants.....	5
1.3.1 Issuer	5
1.3.2 Registration authority (identity and registration services).....	5
1.3.3 End users.....	5
1.3.4 Relying parties	6
1.3.5 Other subcontractors	6
1.3.6 Trust anchor.....	6
1.3.7 Accessibility (universal design)	6
1.4 Use of BankID	6
1.4.1 Permitted use.....	6
1.4.2 Prohibited use	6
1.4.3 Administration of the Practice Statement.....	7
1.5 Definitions and abbreviations	7
2 Publication and repository responsibilities.....	9
2.1 Publication of scheme information	9
2.2 Publication frequency and control.....	9
3 Identification and authentication	10
3.1 Initial identity validation (identity verification of the applicant).....	10
3.1.1 Names and identity attributes.....	11
3.2 Renewal and reactivation	11
3.3 Notification and handling of requests for suspension or revocation.....	11
4 BankID lifecycle management	13
4.1 BankID application.....	13
4.2 Application processing and approval	13
4.3 Issuance of BankID	13
4.4 End user activation and confirmation.....	13
4.5 Suspension.....	14
4.6 Revocation.....	15
4.7 Status and validation services.....	15
4.8 Termination.....	16
5 Physical, organisational and operational controls	17
5.1 Physical security controls	17
5.2 Process controls and personnel security	17
5.3 Continuity and disaster recovery.....	17
5.4 Termination of the scheme.....	17

5.5	Risk management and security management	18
6	Technical security controls.....	19
6.1	General	19
6.2	Protection of sensitive cryptographic material	19
6.3	System and network security	19
6.4	System and component lifecycle security	20
7	Logging, monitoring and record retention	21
7.1	Audit logging and monitoring	21
7.2	Archiving	21
8	Audit and self-declaration	22
9	Other business and legal matters	23
9.1	Financial responsibility	23
9.2	Confidentiality	23
9.3	Fraud prevention and device/risk signals.....	23
9.4	Privacy	23
9.5	Intellectual property rights	24
9.6	Representations and warranties	24
9.7	Disclaimers and limitations of liability.....	25
9.8	Term and termination of the Practice Statement	25
9.9	Governing law and dispute resolution	25



1 Introduction

1.1 Overview

This document describes how Stø AS (“Stø”) issues and operates BankID as an electronic identification scheme at assurance level High (LoA High), in compliance with the eIDAS requirements as implemented in Norwegian law. The document also describes the governance of BankID, roles and responsibilities, the scope of the service and the overarching requirements for issuance, use, lifecycle management and oversight. Commercial terms, including pricing, brand and licensing terms, are governed by separate agreements and are not covered by this document.

This document does not cover other services provided by Stø that fall outside the BankID scheme, including digital identity verification solutions, trust services, KYC/AML services and similar.

1.2 Legal basis

The assurance level (LoA High) and the legal basis for BankID are based on eIDAS Regulation (EU) No 910/2014 and Commission Implementing Regulation (EU) 2015/1502 with its Annex, as implemented in Norwegian law.

Technical specifications, including PKI and cryptographic details, are described in separate supporting documents.

Annex 1 to this practice statement includes a table mapping each section of this practice statement to the specific requirements in accordance with Commission Implementing Regulation (EU) 2015/1502.

1.3 Participants

1.3.1 Issuer

Stø is a limited liability company registered under Norwegian law, with an established organisation and full operational capability in all areas relevant to the delivery of the services.

Stø is the sole issuer of BankID. No other party has the right to issue BankID. Stø is responsible for issuing, managing, suspending and revoking BankID, and for the overall operation of the service.

Stø is required to fulfil the obligations applicable to issuers of eID at assurance level High. This includes, among other things, operating and securing the systems that support issuance, providing mechanisms for status checking and validation, and maintaining continuity and security in the service.

1.3.2 Registration authority (identity and registration services)

Registration authorities (RAs) are legal persons that, pursuant to an agreement with Stø, may perform identity verification and registration tasks in connection with the issuance of BankID. A “BankID Agent” (BankID Fullmektig) or other authorised agents may perform RA functions, including verifying applicants’ identities, reviewing application information and submitting issuance requests. Legal persons performing such tasks on behalf of Stø are subject to corresponding audit and security requirements as Stø when performing tasks on behalf of the issuer. To ensure consistent practice, procedural guidelines have been drawn up for entities acting as registration authorities.

1.3.3 End users

End users are natural persons who are issued BankID following identity verification, registration and acceptance of the applicable terms and conditions. The end user shall protect their BankID identity means, including passwords and other secrets used in authentication. BankID is personal and may not be transferred to or used by others.

1.3.4 Relying parties

Relying parties are legal persons that accept BankID as an electronic identification means for natural persons and use the service to verify the end user's identity. Before a relying party may start using BankID, an agreement must be in place with Stø or an authorised contracting party, and the relying party must be identified and verified in accordance with established procedures. Checks may include business information, authority to represent, power of attorney or procuration, a certificate of incorporation or equivalent documentation, and an assessment of the legal basis where the relying party receives or process's national identity numbers or other identity information. The relying party shall comply with the applicable terms, technical requirements and security requirements for the use of BankID, including requirements for integration, validation of BankID results, protection of its own integration environment and reporting of misuse, fraud or security incidents. Stø or an authorised contracting party may suspend, revoke or terminate the relying party's access to BankID if the terms are no longer met, if there is suspicion of misuse or a security breach, or if this follows from the agreement, law or a requirement from the relevant authority.

1.3.5 Other subcontractors

Stø may use subcontractors and service providers for certain operational parts of the BankID service, such as technical infrastructure, data centre services or identity verification components. Such tasks are performed under Stø's authority and responsibility and are governed by contract. Stø shall ensure that providers meet the requirements for security, confidentiality, operations and compliance with applicable regulations. Stø retains overall responsibility for tasks performed by others.

1.3.6 Trust anchor

In BankID's trust hierarchy, the trust anchor is the ultimate authority. In the current BankID model, Finance Norway holds this role. The trust anchor function is part of the overall governance framework and does not affect Stø's role as the sole issuer of BankID.

1.3.7 Accessibility (universal design)

BankID shall be accessible to persons with disabilities and shall meet the relevant requirements of the Web Content Accessibility Guidelines (WCAG) where this is required by Norwegian law. Registration and issuance processes shall be non-discriminatory and shall address the relevant accessibility requirements.

1.4 Use of BankID

1.4.1 Permitted use

BankID is an eID for personal identification and authentication that may be used in online banking, public digital services through the national identity portal (ID-porten) and online stores that have entered into an agreement with Stø AS on the use of BankID as an eID at assurance level High.

1.4.2 Prohibited use

BankID shall not be used contrary to the BankID user agreement or in ways that could undermine the security of or trust in the service.



End users and relying parties shall not use BankID in ways that could undermine the integrity, reliability or privacy of the service. Such use may result in the revocation of BankID or other measures under agreements or applicable law.

1.4.3 Administration of the Practice Statement

This document is administered by Stø AS. Stø's Identity Policy Board, or a corresponding governing body within Stø, is responsible for reviewing, approving and maintaining the document. Significant changes shall be processed and formally approved through established governance processes.

Changes in standards or legal requirements, as well as new security or operational needs, may lead to changes in the company's practices and to the need for amendments to this document. Approved versions shall be published on the company's website together with a description of the changes.

Questions about this document may be directed to Stø using the contact details below.

Postal address: Stø AS, Postboks 9236 Grønland, N-0134 Oslo, Norway

Customer service and incident reporting: <https://bankid.no/en/help>

Policy enquiries: policy@stoe.no

1.5 Definitions and abbreviations

The following key terms and abbreviations apply to this document:

Term	Definition
Applicant	A natural person who applies for the issuance of BankID and has not yet been issued an electronic identification means.
Assurance level High	The highest level of assurance under eIDAS, providing very high confidence in the claimed identity of a person, requiring robust identity proofing and strong authentication mechanisms.
Authentication	The process of verifying the identity of an entity, confirming that the entity is who it claims to be, based on the use of an electronic identification means.
Authenticator	A mechanism or device used by the end user to authenticate, such as a mobile application, hardware token, or password, forming part of the electronic identification means.
Audit log	A chronological record of events and actions related to the issuance, management, and use of BankID, maintained for accountability, security, and compliance purposes.
BankID	The BankID scheme in Norway, issued by Stø at assurance level High.
Credential	The combination of identity data and authenticator issued to an end user, enabling authentication towards online services.
Data controller	The natural or legal person which determines the purposes and means of the processing of personal data, as defined in GDPR Art. 4(7).
eIDAS Regulation	Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market, which forms the regulatory basis for eID assurance levels and cross-border recognition within the EEA.

Electronic identification means	a material and/or immaterial unit containing person identification data and which is used for authentication for an online service.
End user	A natural person who has been issued BankID and is responsible for the correct use and protection of the identity means.
Expiry	The natural end of a BankID's validity period, after which the BankID can no longer be used and must be renewed or re-issued.
Identity proofing	The steps and procedures used to establish and validate the identity of an applicant before an electronic identification means is issued.
Identity verification	The process of confirming that a person's claimed identity corresponds to their real-world identity, carried out prior to issuance of BankID.
Issuance	The process of creating, binding, and delivering BankID to a verified end user, following successful identity proofing and registration.
Issuer / scheme operator	Stø AS, the legal entity responsible for issuing and operating the BankID scheme.
Level of Assurance (LoA)	A measure of the confidence in the identity verification and issuance process, as defined by eIDAS Regulation Art. 8. BankID is issued at assurance level High.
Personal data	Any information relating to an identified or identifiable natural person, as defined in the General Data Protection Regulation (GDPR) Art. 4(1).
Practice Statement (PS)	This document, which describes the company's practices and rules for the issuance and operation of BankID.
Reactivation	Lifting of a temporary suspension where the grounds for the suspension no longer exist and the scheme's conditions are met.
Registration authority (RA)	An entity delegated by Stø to perform identity verification, registration and certain lifecycle management tasks for BankID issuance and management, such as a BankID Agent or other authorised partner.
Relying party	An entity that relies on BankID for the identification or authentication of a user.
Renewal / Re-issuance	The process of issuing a new BankID to an end user following expiry or loss of an existing BankID, subject to applicable identity verification requirements.
Revocation	Permanent invalidation of a BankID before expiry.
Suspension	Temporary deactivation of a BankID's validity.
Validation	The process of determining whether a BankID is valid, suspended, revoked or unknown.



2 Publication and repository responsibilities

2.1 Publication of scheme information

Information, terms of use and publicly available documents about BankID are available on Stø's website, including this BankID Practice Statement, conditions and practices for end users and relying parties, terms for end users and relying parties, information necessary to validate BankID, contact information for customer service and incident reporting, and references to technical or operational documentation for use of the service, audits or supervision.

Minor changes are published on an ongoing basis without specific notice. Significant amendments and revised document versions shall be published prior to taking effect, in accordance with the notice periods specified in the respective agreements.

2.2 Publication frequency and control

When this document or other repository documents are updated, the latest approved version is published on the company's website without undue delay.

Status and validation services are updated as required, so that relying parties can determine whether a BankID is valid, suspended or revoked.

Only authorised personnel may publish or amend information and documents on the company's website. Publication and amendments shall take place in accordance with the applicable change management procedures and shall be logged. To prevent manipulation and misuse, the integrity of published documents is protected by digital signatures, secure web protocols and similar measures.

Sensitive information, such as detailed logs or procedures not intended for public sharing, is stored in secure systems. Such information shall not be exposed through publicly accessible websites or otherwise made available to the general public.

3 Identification and authentication

3.1 Initial identity validation (identity verification of the applicant)

Before BankID is issued to an applicant, Stø – either directly or through an authorised registration authority, such as a BankID Agent – carries out a thorough identity verification. The verification establishes the applicant's identity in accordance with the requirements for eID schemes at assurance level High.

BankID is issued only to natural persons who meet the requirements. This includes, among other things, that the person is registered in the National Population Register with a unique identification number and has accepted the applicable BankID user agreement.

Age and legal capacity

To enter into a BankID agreement, the person must be at least 12 years old. For minors between the ages of 12 and 18, consent of both guardians is usually required. If only one guardian receives the request for consents, the other guardian shall be informed and given the right to refuse and object to the issuance. Powers of attorney, consents or other documentation of guardianship authority shall be documented in accordance with established procedures. BankID shall not be issued if the applicant lacks the necessary legal capacity, has been fully or partially deprived of legal capacity, or is under a voluntary guardianship and BankID is not to be used by the end user alone.

Identity documents and document verification

Accepted proofs of identity are BankID at the required assurance level, a national identity card or a passport. Identity documents issued outside Norway may include Schengen identity cards, passports issued in the EU/EEA and passports issued outside the EU/EEA that are recognised by the Norwegian authorities.

Physical identity documents shall be verified in accordance with established procedures. Where the document type and verification method require it, the document shall be read electronically and checked against relevant authoritative or recognised sources, including the TOVE system for Norwegian passports and national identity cards. If electronic reading or necessary source verification cannot be completed where this is required, the identity verification shall be discontinued and BankID shall not be issued on the basis of the verification in question.

The identity verification shall be documented. The registration authority shall record which proof of identity was presented, which checks were carried out and the outcome of those checks. Documentation from the identity verification, including relevant identity documentation and the necessary personal and contact details, shall be stored securely by the registration authority in accordance with established procedures. The documentation shall be made available to Stø upon request where necessary for audits, supervision, compliance checks or the follow-up of specific cases. The information shall be retained and shared in accordance with applicable requirements regarding confidentiality, information security and personal data protection, as set out in Chapters 7 and 9.

BankID is not issued until the applicant's identity has been sufficiently verified. If the identity verification cannot be completed in accordance with the requirements for assurance level High – for example because the documentation is insufficient or suspected to be fraudulent – the application shall be rejected.

Identity documents must be linked to the National Population Register



For new applicants, the identity document presented must uniquely link the person to a Norwegian national identity number or D-number in the National Population Register. The applicant must be registered in the National Population Register with a unique identification number. For persons with a D-number, issuance requires that identity and document verification with in-person attendance has been completed at the Norwegian Tax Administration or another relevant authority, so that the identity basis in the National Population Register shows that the identity has been verified ("status kontrollert").

In-person attendance or approved electronic verification

For initial issuance, identity verification shall be performed by in-person attendance at a BankID Agent or another party acting on behalf of Stø. Electronic identity verification may only be used where the scheme expressly permits it, for example in connection with renewal or re-issuance to the same natural person based on an existing valid BankID identity means, or in digital activation processes specifically approved by Stø.

Approved electronic methods and use of existing eID

Where the scheme permits, an existing valid electronic identity means may be used in controlled processes for renewal or re-issuance to the same natural person, provided that the relevant identity attributes are confirmed by a lookup in the National Population Register.

Verification against authoritative sources

Stø or the delegated registration authority verifies that the identity attributes used for issuance are identical to the information registered for the applicant in the National Population Register. This verification is performed at initial issuance and where renewal or reactivation is based on an existing valid electronic identity means.

Delegated identity verification

Identity verification carried out wholly or in part by a third party on behalf of Stø shall meet the same requirements as if Stø had performed the verification itself. Stø retains full responsibility for ensuring that the verification is correctly performed and meets the requirements for assurance level High.

3.2 Renewal and reactivation

Renewal or reactivation of BankID shall maintain the same assurance level as the initial issuance, and BankID shall remain linked to the same verified natural person.

Where the BankID scheme and applicable law permit, an existing valid BankID may form the basis for renewal for the same natural person.

If renewal or reactivation of BankID cannot be based on an existing BankID, the end user shall undergo new identity verification meeting the requirements for assurance level High.

Where renewal or reactivation is based on the use of a valid electronic identity means, Stø shall confirm that the identity attributes are still correct by verifying identity data against the National Population Register.

3.3 Notification and handling of requests for suspension or revocation

If an end user suspects unauthorised use of BankID, loses control of the identity means or for other reasons needs BankID to be blocked, suspended or terminated, the end user shall notify their registration authority, for example the BankID Agent, without undue delay. Notifications that may affect the validity of BankID shall be received and handled promptly to prevent misuse.

The registration authority shall have appropriate procedures for receiving and handling notifications from end users regarding suspected misuse, loss, compromise or discontinuation of BankID. The registration authority may take reasonable steps to confirm the identity of the person giving notice or otherwise verify the credibility of the notification – the need for prompt action and the need to avoid incorrect measures must here be weighed against each other.

Based on a notification, or where security considerations, legal requirements or requirements under the BankID scheme otherwise so indicate, Stø may suspend or revoke BankID. Suspension, revocation and any permitted reactivation are carried out by Stø in accordance with established operational processes, normally at the request of the registration authority. Where the request comes from another authorised source – such as fraud checks, a court order or a substantiated internal security ground – Stø shall verify that the grounds for the measure are sufficiently documented before it is implemented.

Further rules on suspension, revocation, reactivation and communication of status are set out in Chapters 4.5 to 4.7.



4 BankID lifecycle management

This chapter provides an overview of the lifecycle processes for BankID, from application and issuance to any suspension or revocation, and describes roles and responsibilities in each phase. Detailed operational procedures are documented in internal manuals and technical guidelines.

4.1 BankID application

The application process begins when the applicant expresses a wish to obtain BankID, for example by opening a bank account, attending in person or completing an electronic application form. The registration authority collects the necessary personal information from the applicant, including full name, national identity number and contact details. This normally takes place in connection with the identity verification.

The applicant must accept the BankID terms and conditions at the time of application. Acceptance may be given by physical or electronic signature or recorded through an authenticated action. The registration authority assesses whether the application information is complete and correct and verifies that the applicant meets the requirements.

Issuance and activation do not take place until the identity verification required by Chapter 3.1 and all relevant verification steps have been completed.

4.2 Application processing and approval

After the identity verification has been completed, Stø processes the BankID request. Stø verifies that the registration authority is authorised, that the request was submitted over a secure channel and that the information submitted is complete. Stø's systems may automatically check certain fields, for example that the national identity number has a valid format and is not already linked to another active BankID at assurance level High in Stø's registries. Manual checks may be carried out in the event of discrepancies or as part of spot-check quality assurance.

If the request is approved, BankID is prepared with the correct identity information and attributes in accordance with the applicable requirements. Stø approves the issuance, where applicable through automated systems acting on behalf of Stø. Where there is suspicion of a duplicate identity or the documentation is insufficient, the application is placed on hold or returned to the registration authority for clarification.

4.3 Issuance of BankID

Following approval, Stø creates the BankID and links it to the end user's verified identity. BankID cannot be put into use until the end user has completed the activation process.

BankID is issued with identity information, validity and security attributes in accordance with the applicable requirements. Technical formats, profiles and cryptographic parameters are described in controlled technical documentation.

BankID has a maximum validity of two years. End users are notified in advance of expiry and must renew before it expires. If an end user does not renew before expiry, the BankID ceases to be valid and a new application and issuance process is required.

4.4 Delivery and activation

BankID is a server-based electronic identification means. The private key and associated certificate are generated and held in Stø's central infrastructure and are never transferred to the end user. Possession of the electronic identification means is therefore exercised as

exclusive control, obtained solely through an authentication factor bound to the end user's verified identity.

No authentication factor may be delivered to or activated by an end user without verification of that end user's identity at the point of delivery. BankID may be activated in different ways depending on which authentication factor is delivered. Activation based on the use of an OTP device, which constitutes a possession-based authentication factor within the meaning of Regulation (EU) 2015/1502, requires in-person attendance and identity verification before BankID can be put into use. Activation of the BankID app is carried out digitally using the ID check in the app; the ID check verifies the identity document and compares it with a facial scan of the end user, including liveness detection.

Accordingly, the electronic identification means is delivered into the possession of the person to whom it belongs and no other, since control of the means cannot be obtained except through an authentication factor whose delivery was itself conditional on verified identity. The same requirements apply to the replacement, renewal and reactivation of authentication factors as to first issuance. BankID cannot be put into use until activation has been completed.

For OTP devices and other physical authentication devices, issuance, delivery, activation, administration, suspension and any replacement shall be carried out in accordance with established procedures and the applicable BankID requirements. The BankID Agent shall document its practice for handling such devices and make the documentation available to Stø when necessary for audits, supervision, compliance checks or the follow-up of specific cases.

The end user shall complete the prescribed activation steps before first use. Activation shall include the necessary checks to confirm that it is the correct end user activating BankID, and that no other person obtains control of the end user's BankID or authentication factors.

Activation establishes the end user's knowledge-based authentication factor. That factor, and any activation codes or other data used to carry out the activation, shall be established, transmitted and stored so that they are protected against disclosure, copying and unauthorised use.

If the end user discovers an error, is unable to complete activation, or believes that another person may have obtained control of the end user's BankID or of an authentication factor, BankID shall not be put into use and the matter shall be reported to Stø or the issuing bank without undue delay.

4.5 Suspension

Suspension is a temporary blocking of BankID. Suspension may be used when there is a need to temporarily prevent use, for example in cases of suspected misuse or fraud, suspicion that BankID is being used by someone other than the end user, loss of control of the identity means, a misplaced code device, mobile phone or other relevant device, or while a security or fraud investigation is ongoing.

Initiation

Suspension is carried out by Stø in accordance with established operational processes. In the ordinary process, suspension is normally initiated based on a notification from the end user or a request from the registration authority, such as the BankID Agent. Stø may also suspend BankID when security considerations, fraud prevention checks, legal requirements or other substantiated circumstances relating to BankID so indicate.

When BankID is suspended, the end user shall be notified without undue delay in accordance with established procedures, unless notification must be deferred for security, legal or investigative reasons. The notification shall state that BankID is suspended and



provide the necessary information about next steps, including how the end user can contact the registration authority or customer support.

Duration

Suspension shall be temporary and shall only last as long as the grounds for suspension exist. BankID cannot be used while it is suspended, and the status “suspended” shall be reflected in BankID’s status and validation services.

Reactivation

A suspended BankID may be reactivated once the reason for the suspension has been resolved or no longer exists and the conditions for reactivation are met. Before reactivation, the registration authority or Stø shall verify that the grounds for the suspension have been addressed and that the end user is still correctly identified and has control of BankID. The verification shall be carried out in accordance with established procedures and may include authentication using a valid electronic identity means, security questions, verification against registered identity and contact details or new identity verification where necessary. Reactivation may only take place within 30 days of suspension. If BankID cannot be reactivated within that deadline, it shall be revoked. A revoked BankID cannot be reactivated.

4.6 Revocation

Revocation means that the agreement with the end user is terminated and BankID is deactivated before expiry. Grounds for revocation include:

Customer-initiated revocation; notification from the End User or the End User's legal representative of loss, compromise, suspected misuse, fraud, or other circumstances indicating that the BankID should no longer remain active; reliable information that the End User is deceased; suspicion that the BankID is being used by an unauthorised person; breach of the BankID Terms, including the disclosure of passwords, code devices or other security credentials; information demonstrating that data associated with the BankID is inaccurate or that the BankID was issued on an incorrect basis; or any court order, regulatory requirement or other legal obligation requiring suspension, revocation or termination of the BankID.

Revocation may be carried out immediately when misuse is discovered or there is suspicion that BankID is being used by an unauthorised person. If the end user suspects that codes, passwords, a code device or other secrets have been compromised, the end user shall contact the bank or another registration authority without undue delay to have their BankID revoked.

The status and validation services shall be updated so that the BankID is shown as revoked.

A revoked BankID cannot be reactivated or restored. If the end user needs BankID again after revocation, a new application and issuance is required.

4.7 Status and validation services

Stø provides status and validation services that make it possible to determine whether a BankID is valid, suspended, revoked or unknown. The services shall be available and robust enough to support the secure use of BankID. The technical implementation is described in controlled technical documentation.

Relying parties integrating BankID validation should consult the technical integration documentation provided for the validation service endpoint details, request and response formats, and the requirement for signed OCSP requests.

4.8 Termination

When the end user's BankID user agreement is terminated, the right to use BankID simultaneously ceases. Termination of the agreement does not affect Stø's obligation to retain information and documentation in accordance with Chapter 7 or to fulfil any other obligations relating to an already issued BankID.



5 Physical, organisational and operational controls

5.1 Physical security controls

Stø protects data centers and operating sites that form part of the BankID service with physical security measures.

BankID systems are located in secured data centers with layered access control, and access is limited to authorised personnel with strong authentication. Critical equipment is protected in defined secure zones, entries and exits are logged, and the premises are monitored with appropriate security measures. Physical security measures are inspected regularly to verify that the requirements for physical and environmental security are met.

5.2 Process controls and personnel security

The operation of BankID is subject to strict requirements for process controls and personnel security.

Critical tasks are distributed between different roles to prevent a single person from having full control over sensitive processes; cryptographic operations require dual-person audits, and audit logs are reviewed by personnel who were not involved in performing the logged activities. Stø defines which roles and tasks are considered trusted – including security officers, RA officers, Audit officers, system administrators and system operators– and grants these only the access necessary to perform their tasks. Employees shall undergo relevant background checks before being assigned trusted roles, and personnel in such positions shall be subject to confidentiality obligations and shall receive training in security rules and the handling of sensitive information. Stø provides regular training for all those who work in the operation of BankID, so that they are familiar with security requirements, data protection obligations and incident reporting procedures.

Operations manuals and security procedures are maintained and made available to authorised personnel. Compliance is monitored through periodic internal audits.

5.3 Continuity and disaster recovery

Stø has business continuity plans and disaster recovery contingency plans to handle operational disruptions. Critical parts of the BankID infrastructure are designed so that the service can be maintained in the event of failure. Critical data is backed up regularly and stored securely separately from the primary operating location. Recovery is tested periodically.

The plans describe how critical issuance and validation services are to be restored in the event of serious failure, including the use of a secondary location or fallback solutions where necessary. Recovery time objectives (RTO) and recovery point objectives (RPO) are set in accordance with the relevant regulatory and business requirements.

Stø has established procedures for handling security incidents. Incidents are classified according to severity and possible impact on BankID, end users and relying parties. The plans include measures to limit the scope of damage from and to investigate incidents, the necessary communication procedures, notification where required and processes for remediation and improvement. Business continuity and incident management plans are tested and maintained regularly.

5.4 Termination of the scheme

Stø has a termination plan for cases where the company is to cease delivering BankID, either because the service is transferred to another provider or because the BankID scheme

is discontinued. In the event of a planned termination, Stø shall provide sufficient notice to end users, relying parties and relevant authorities.

Upon termination, Stø shall cease issuing new BankIDs before the service is discontinued and, where possible, facilitate a transition to an alternative solution for users. Stø shall retain the necessary information and documentation in accordance with Chapter 7 even after wind-down.

Stø shall terminate technical functions, keys, status information and other relevant supporting material in an orderly manner. Relying parties and other affected parties shall be given sufficient advance notice so that they can phase out their use of BankID in an orderly fashion.

5.5 Risk and security management

Stø manages risks related to BankID through established governance processes, operational procedures and security controls. Risk management shall meet the requirements for eID at assurance level High.

In line with Commission Implementing Regulation (EU) 2015/1502, the assurance level is based on the overall quality of identity verification, management of electronic identity means, authentication and organisational controls. Risk management shall therefore cover the entire BankID lifecycle and be embedded in all relevant processes and controls.

Stø monitors the risk landscape on an ongoing basis through operational experience, security incidents, threat intelligence and audit findings, and adjusts controls and processes as needed to maintain security, reliability and compliance.



6 Technical security controls

6.1 General

Stø establishes and maintains technical security controls for systems and processes that support the issuance and operation of BankID. The controls shall contribute to confidentiality, integrity and availability and shall meet the requirements for eID at assurance level High.

This chapter describes the overarching objectives of the technical security controls. Detailed technical requirements, specifications and implementation are described in controlled technical documentation.

6.2 Protection of sensitive cryptographic material

Sensitive cryptographic material shall be protected against unauthorised access and use. Stø has established procedures for creation, storage, use, backup, replacement and deletion. The technical details are described in controlled technical documentation.

The material shall be created through controlled processes and with components that meet the applicable security requirements. Access is granted only to authorised systems and personnel who need it to perform their tasks. Use is logged, and particularly critical actions shall require multi-party control or equivalent security measures where necessary.

Keys necessary for critical BankID functions shall be backed up only where the need is documented. The backups shall be protected against unauthorised access and used exclusively for recovery or equivalent continuity measures.

Cryptographic material shall be replaced, rotated or deleted in accordance with established procedures, or earlier if circumstances arise that could undermine confidence in the material. Decommissioning and deletion shall prevent subsequent use without compromising the security or continuity of BankID.

6.3 System and network security

Stø protects systems and networks that support BankID against unauthorised access, misuse and disruption. The controls include access management, protection of communication channels, necessary system segregation and monitoring of system and network activity.

Access to sensitive BankID systems and associated data is strictly controlled. Users are authenticated with unique credentials and are granted only the access they need to perform their tasks. Administrative access is particularly restricted and logged.

Servers and applications are configured in accordance with recognised security practices. Default accounts and passwords are changed, unnecessary services are disabled and security patches are applied without undue delay.

The infrastructure is segmented so that publicly exposed services are separated from internal systems. Firewalls, intrusion detection, intrusion prevention and continuous monitoring protect the network against unauthorised access and anomalous activity. Sensitive data transfers are encrypted.

Systems are protected against malware and other relevant threats. Stø conducts regular vulnerability scans, prioritises and remediates findings based on risk and carries out periodic penetration testing.

Critical systems and security incidents are monitored continuously. Alert procedures shall ensure that security personnel are promptly made aware of possible incidents so that they can be investigated and handled without undue delay.

6.4 System and component lifecycle security

Technical security controls are applied throughout the lifecycle of systems and components that support BankID. This includes secure development, configuration, maintenance, controlled change management and secure replacement or decommissioning of systems.



7 Logging, monitoring and record retention

7.1 Audit logging and monitoring

Stø keeps and retains audit logs for events that are important for the secure operation, traceability and compliance of the BankID scheme. The logs are used for security monitoring, incident investigations and documentation of compliance with the applicable requirements.

Logging covers, among other things, events related to identity verification, issuance, renewal, suspension, reactivation and revocation of BankID. Administrative access to critical systems, use of sensitive cryptographic material and other security-critical actions are also logged. Security events – such as failed login attempts, system errors that may affect security functions, attempts at unauthorised network access and other relevant anomalies – are also covered.

Logs shall be timestamped and protected against unauthorised access, modification and deletion. Access to logs is granted only to specifically authorised persons and system processes.

Logs are retained for as long as required under statute and regulations.

Stø monitors relevant log data to detect anomalies, misuse and matters that may affect the security of the BankID scheme. Critical matters shall be flagged, investigated and handled without undue delay. Logs are reviewed regularly to verify that operations are conducted in accordance with the applicable requirements, and the reviews are documented.

7.2 Archiving

Stø archives information necessary to document the correct issuance and management of the scheme, to meet compliance requirements and to enable audits, supervision and necessary investigations.

The archive may, where relevant and permitted under applicable law, include application information, registered and verified identity data, confirmations against the National Population Register, documentation of acceptance of end user terms, a unique end user identifier and a reference to controlled identity documentation.

Stø also archives information on issuance, renewal, suspension, reactivation, revocation, expiry and any new application. Where necessary, validation requests and responses to such validation requests may also be archived.

Information is stored securely and protected with appropriate measures, including access control and encryption where relevant. Information is retained for as long as necessary for the purposes for which it was collected, and for as long as required under law, regulations or requirements under the BankID scheme.

8 Audit and self-declaration

Stø ensures that the BankID scheme is subject to the relevant audits, assessments or certifications required by law, regulation and applicable standards, including Commission Implementing Regulation (EU) 2015/1502 as implemented in Norwegian law. Findings are assessed and followed up with corrective or improvement measures where necessary. Relevant documentation and results are made available to competent authorities or assessment bodies where required.



9 Other business and legal matters

9.1 Financial responsibility

Stø assumes financial responsibility to the extent required under applicable law or the agreement for the BankID service.

Stø shall have sufficient financial resources or insurance coverage appropriate for a provider of eID services at high assurance level. This may include general liability insurance or specific insurance against digital security incidents covering possible losses resulting from system failure or security breaches.

Any financial guarantees expressly given to end users or relying parties are set out in the relevant contractual terms.

9.2 Confidentiality

Stø and Stø's partners, including registration authorities/agents and subcontractors, are bound by contractual duty of confidentiality in respect of confidential information they access in connection with the operation of BankID.

Confidential information is stored securely, and access is granted only to persons who need such access to perform their tasks. All personnel are bound by confidentiality obligations by virtue of their employment or contractual relationship.

Stø complies with applicable data protection legislation, including the GDPR and Norwegian data protection rules, when processing personal data about end users. Personal data collected during the issuance of BankID is used only for that purpose and associated operational purposes, including security monitoring, customer service and regulatory compliance. The data is not used for other purposes without consent or another legal basis. Further information about the processing, retention and the rights of data subjects is set out in the BankID privacy policy.

Stø only discloses confidential information where required by law – for example pursuant to a court order or a specific statutory provision – or where the data subject has expressly consented. In the event of legally required disclosure, Stø shall ensure that only the necessary information is disclosed and that the disclosure is logged.

Identity information stored in the identity means, such as the end user's name and expiry date, must by its nature be shared using the service. The same applies to aggregated or anonymised statistics that do not identify individuals. When the legal base allows for it, personal identifiers are shared with a relying party requesting it.

9.3 Fraud prevention and device/risk signals

To protect BankID and prevent criminal activity, Stø may identify the electronic device from which BankID is used and assess signals from the usage situation, such as device status, IP address and deviations from normal environment or behavior. Relying parties may receive information indicating the risk level associated with accepting BankID from a particular device in the relevant transaction.

9.4 Privacy

As an eID provider, Stø has a particular responsibility to protect personal data. Stø processes personal data in accordance with applicable data protection legislation, including the GDPR.

The end user's personal data shall only be disclosed to a BankID relying party or service when the end user has given consent, or where another valid legal basis exists.

The BankID privacy policy describes the personal data collected, such as name, national identity number, contact details and usage logs, as well as the purposes for which the data is processed, the retention period and the rights of data subjects.

Personal data is not retained longer than necessary. Personal data in log files may however be retained for as long as necessary for regulatory compliance or ongoing legal proceedings and shall thereafter be deleted securely.

End users have the right to access their own data and to request the correction of data that is inaccurate.

Stø protects personal data through technical measures, such as encryption and pseudonymisation, and organisational measures, such as training and data handling procedures.

Stø adheres to data protection principles including data minimisation, purpose limitation, role-based access and tailored retention rules. Personal data is processed only when a valid legal basis exists and not beyond the extent necessary for issuance, operations, security, fraud prevention, customer service, compliance and associated purposes. When Stø uses service providers, data protection and confidentiality obligations are regulated by contract and monitored through appropriate control activities.

9.5 Intellectual property rights

Intellectual property rights, trademarks, logos and rules for brand use are governed by separate brand and licence terms and relevant agreements. This falls outside the scope of this document.

9.6 Representations and warranties

Stø declares that the company will operate BankID with reasonable care, in compliance with applicable requirements and legal obligations. Stø warrants that BankID identity means that are issued can be relied upon for the information and assurance level they are intended to convey, within the applicable limitations.

Stø does not give any further warranties, for example that BankID meets all specific needs of a relying party beyond what follows from the requirements for assurance level High.

Participating registration authorities, such as partner banks/agents, warrant that they follow Stø's procedures and the applicable standards when performing identity verification and other tasks on behalf of Stø. They shall also ensure that personnel have the necessary training and competence, protect sensitive information and contribute to compliance.

By accepting a BankID identity means, the end user declares that the information provided during registration – including name and personal details – is true and accurate, that they have read and accepted the BankID terms, including rules on correct use, the prohibition on sharing the identity means and the obligation to promptly report problems, and that they will promptly notify Stø or their registration authority if BankID is compromised or associated information becomes incorrect, for example upon a change of name.

By using BankID, relying parties declare that they will use BankID integrations in accordance with BankID's rules and applicable guidance. At a high level, this means they shall validate the BankID result before relying on it, use the service only for permitted purposes, protect their own integration environment and report suspected misuse, fraud or security incidents affecting their use of BankID. Detailed integration requirements are set out in separate controlled documentation and relevant contractual terms.



This includes carrying out appropriate validation of BankID, including status checks where relevant pursuant to Chapter 4.7, assessing whether a particular transaction or use case is suitable for accepting BankID at assurance level High, and avoiding use of BankID in prohibited ways, as set out in Chapter 1.5.2.

9.7 Disclaimers and limitations of liability

Stø's liability towards end users, relying parties and other contractual parties is governed by the respective agreements applicable to those parties and by mandatory law.

9.8 Term and termination of the Practice Statement

This document applies from the effective date stated in the document control and remains in force until it is replaced by a new approved version or until the BankID scheme as described is discontinued.

Stø may amend or update this document as required, following the change control process in Chapter 1.5. In the event of significant changes that may affect end users or relying parties, Stø shall communicate this in an appropriate manner, for example by publication or direct notification to registration authorities.

If Stø ceases to operate BankID, or the document is replaced because the service is transferred to another operator, Stø shall ensure the necessary notification and archiving in accordance with Chapters 5.4 and 7. If Stø is replaced by another provider, obligations and documentation shall be transferred in a controlled manner to maintain trust and continuity for users.

9.9 Governing law and dispute resolution

Stø's operation of BankID is subject to Norwegian law.

Disputes concerning the delivery or use of BankID should in the first instance be attempted to be resolved amicably, for example directly between the end user or relying party and Stø, or through the registration authority's customer service. If the dispute is not resolved amicably, it may be pursued further under the applicable agreements and Norwegian law. End users may use the dispute resolution mechanisms described in the BankID end user agreement, while relying parties follow the dispute resolution rules referred to in their contracts.

Disputes are normally resolved by a Norwegian court unless otherwise agreed. This document is prepared in English, and Norwegian law applies to questions of interpretation.