



PKI DISCLOSURE STATEMENT

Stø AS

Qualified Certificates and
Qualified Timestamps

Version 1.1.1
Effective date 11.11.2025

PUBLIC



Table of contents

1. Definitions	3
2. Introduction.....	5
3. Trust Service Provider contact information	6
4. Certificate Type, Validation Procedures and Usage	6
5. Reliance Limit	7
6. Obligations of Subscribers.....	7
7. Certificate Status Checking Obligations of Relying Parties.....	7
8. Limited Warranty and Disclaimer/Limitation of Liability	7
9. Applicable agreements and policy	7
10. Privacy Policy	8
11. Applicable Law, Complaints, and Dispute Resolution	8
12. TSP and repository licenses, trust marks, and audit	8



1. Definitions

Authentication: An electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.

Stø: Stø AS is the Trust Service Provider, and a Norwegian company with business registration number 927 611 929.

BankID: A brand belonging to Stø AS which can be used for electronic identity or trust services. Examples are BankID Signing and BankID Timestamping

Certificate (Public key Certificate): A data sequence containing the Subscriber's public key along with other information, which cannot be falsified as the information is signed with a CA's private key.

eIDAS: 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.

Electronic identification (eID): A material and/or immaterial unit containing person identification data which is used for authentication for an online service.

ETSI: European Telecommunications Standards Institute.

Issuing bank: A bank operating in Norway or other party authorized to issue BankID Certificates.

Public Key Infrastructure (PKI): Infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.

Qualified: When the term is used in conjunction with one or more Trust Service(s) it reflects that the particular Service(s) are meeting the requirements for qualified Trust services set forth in eIDAS.

Qualified Signature Creation Device: Computer hardware and software used for creating an electronic signature evaluated and certified according to ISO/IEC 15408 [1] to a protection profile suitable for fulfilling the requirements laid out under Annex II of eIDAS.

Relying Party: Entity (natural and legal person, systems, devices) accepting signatures and signed Time stamps based on Certificates issued by BIDBAX Signing Services.

Signing Service: The service provided by BIDBAX related to signing application to create a digital signature value on behalf of a signer/Subscriber, issuing of a Qualified signature Certificate and Qualified Time stamping for electronic signing purposes.

Subscriber: Natural person being the creator of an electronic signature, identified in a Certificate as the holder of the private key associated with the public key given in the Certificate.



Terms and Conditions: The standard terms and conditions for the Signing Service entered between Stø and the Subscriber.

Time Stamps: Data in electronic form which binds other electronic data to a particular time establishing evidence that this data existed at that time.

Trust Service: Electronic service which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services.

Trust Service Provider: A natural or a legal person who provides one or more Services as defined in eIDAS.



2. Introduction

This document serves as the Public Key Infrastructure disclosure statement (PDS), which is required by European standard ETSI EN 319 411-1. Its purpose is to summarize and present the key points from the Trust Service Practice Statement (TSPS) for Stø AS Qualified Certificates and Qualified Time stamps. The goal is to make this information more accessible and comprehensible for our Subscribers and Relying Parties.

This document is a supplement to the Terms & conditions.

Document history:

Version	Date	Changes	Approved by
1.0	25.11.2024	Approved version for publishing	BankID BankAxept AS ID Policy Board
1.1.	17.09.2025	Adjusted with Stø as new company name	Stø ID Policy Board
1.1.1	11.11.2025	Adjusted with	Stø ID Policy Board



3. Trust Service Provider contact information

Contact information for Stø AS a Qualified Trust Service Provider (QTSP).

Name: Stø AS
Location: Biskop gunneriusgate 14a
Postal address: Postboks 9236 Grønland, 0134 OSLO
Website: www.bankid.no
Customer Support: [Hjelp \(bankid.no\)](http://Hjelp.bankid.no)

For customer support or other Certificate questions please contact the bank that has issued your eID. Contact information may be found on the respective Issuing bank's websites or on their online bank (netbank).

4. Certificate Type, Validation Procedures and Usage

Stø issue Qualified Certificates for electronic signatures to natural persons as part of the Signing Service. These Certificates are granted based on Authentication using an existing eID. The identity of the individual is verified through eID means that adhere to eIDAS Article 24(1)(b), ensuring equivalence to physical presence and meeting the requirements for eID level of assurance (LoA), specifically High or Substantial. Currently, the only eID being accepted by Stø within the Signing Service is Norwegian BankID.

The private keys associated with these Qualified Certificates are exclusively utilized for Qualified electronic signatures. A Qualified Time Stamp provided by Stø will be included in the electronic signatures.

These certificates are short-term, with a validity period of 15 minutes, certifying a one-time private key generated and used within a QCSD (Qualified Certificate Service Provider) as part of the Signing Service.

Electronic signatures will be produced using a Qualified Signature Creation Device. The Qualified Signature Creation Device will be operated by Stø following the successful Authentication of the Subscriber.

All signatures will be time stamped by Stø's Qualified Time stamping service. This is handled implicitly within the Signing Service and will not require any specific attention from the Subscriber.



5. Reliance Limit

The Qualified Certificates issued by Stø are short-term Certificates that shall only be used for Qualified electronic signatures according to Regulation (EU) No 910/2014, and as defined in this document, the TSPS and the Terms and Conditions.

Certificate registration data and event logs are maintained by the Stø for a minimum of 7 years after certificate expiration date.

6. Obligations of Subscribers

The Subscribers' obligations when using the Signing Service are regulated in the Terms and Conditions.

7. Certificate Status Checking Obligations of Relying Parties

Every time an eID is used for signing purposes, the Qualified signature Certificate status must be checked to verify it is valid.

Stø shall ensure that procedures are in place for checking the validity of all signature certificates.

The Qualified signature Certificates are only valid for a short period of time after issuance. It is therefore not established a public revocation service for the signature Certificates.

All parts of the Signing service are available 24/7/365. Event logs for usage of BankID are retained for ten years after the BankID certificates expiry date.

8. Limited Warranty and Disclaimer/Limitation of Liability

Stø' and Subscribers' liability and limitation of liability is regulated in the Terms and Conditions.

9. Applicable agreements and policy

The detailed policy document, Trust Service Practice Statement (TSPS), and applicable Terms and Conditions are published on BankID' website and can be found here:

[Documentation qualified signatures](#)



The TSPS documents address all requirements of the applicable policy to Stø's Trust Services.

The embedded Time Stamping Service issues Qualified Time stamps according to Regulation (EU) No 910/2014: {ITU-T(0) IDENTIFIED-ORGANIZATION(4) ETSI(0) ID-TST-PROFILE(19422) ID-ETSI-TSTS(1) ID-ETSI-TSTS-EUQCOMPLIANCE (1)}.

The identifier for BTSP: the best practices policy for time-stamp. This is the policy Stø's Trust Services will follow:

itu-t(0) identified-organization(4) etsi(0)time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)

10. Privacy Policy

Personal data of the Subscriber is processed according to EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("GDPR") and data protection law in Norway. Stø provide the applicable privacy policy available to Subscribers in the BankID app or on the BankID website:

[Privacy, Terms and Regulations](#)

11. Applicable Law, Complaints, and Dispute Resolution

This document and applicable agreements shall be performed and interpreted in accordance with Norwegian law.

Any complaints from Subscribers related to the Signing Service shall be directed to the Subscribers Issuing bank. Contact information may be found on the respective bank's websites or in their online bank (Nettbank).

If a complaint from a Subscriber cannot be resolved and a dispute should arise concerning the interpretation or legal effects of this document or applicable agreements and policies, an attempt shall be made to resolve the dispute through negotiations. If such negotiations are not successful, each party may submit the dispute to the ordinary courts. The legal venue is Oslo District Court.

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

Stø is a Qualified Trust Service Provider (QTSP) and issues Qualified signature Certificates and Qualified Timestamping according to eIDAS Regulation.

Stø is registered as a QTSP on the European trusted list and on the Norwegian trusted list. Stø has been certified to be conformant with the certificate policies for EU Qualified Certificate for natural persons with a Qualified Signature Creation Device, as well as for Qualified Time stamping.

[eIDAS Dashboard](#)

Third party audits are conducted annually by an accredited conformity assessment body according to ETSI EN 319 403.