Stø AS Identity Proofing Service Provider Practice Statement

Version: 1.0

Date: 2026-03-24

This document constitutes the Practice Statement (PS) for the Identity Proofing Service from Stø AS, describing the practices and policies governing the provision of its identity proofing service component.

Contents

Document History

Version	Date	Changes	Approved by
1.0	2026-03-24	Initial version	

1 Introduction

This document describes the practices established by Stø AS for the Identity Proofing Service (hereinafter referred to as “The Service”).

Stø AS is a Norwegian Trust Service Provider (TSP). Since May 4th, 2025 Stø AS has been the name of the company formerly known as BankID BankAxept AS. Stø AS is ISO/IEC 27001:2022 [10] certified company.

The name BankID BankAxept AS may still be used in referenced documents. Future versions will incorporate the name change.

This Practice Statement (PS) specifies the procedures, activities and rules implemented in order to fulfil the role as an Identity Proofing Service Provider (IPSP) operating an Identity Proofing Service Component (IPSC) providing fully automated remote identity proofing services in accordance with ETSI TS 119 461 [7].

This document provides a Trust Service Practice Statement (TSPS) and an Identity Proofing Service Practice Statement (IPSPS) for the Identity Proofing Service provided by Stø AS and is structured according to, and complies with, the policy statement requirements defined in ETSI TS 119 461 [7].

1.1 Overview

Stø AS Identity Proofing Service is a fully automated unattended remote identity proofing process supporting the identity proofing of trust service subjects for use by trust services from both qualified and non-qualified trust service providers (TSPs) according to the Regulation (EU) No 910.2014 (eIDAS regulation) [i.1]. The service can also be provided to actors that are not TSPs with their own identity proofing requirements. The Service only supports identity proofing of natural persons.

The service supports use cases as defined by in ETSI TS 119 461 [7] Section 9.2.3.4; Annex C Section C.2.4; and Annex C Section C.3.4.

By acting in this capacity, The Service provides an Extended Level of Identity-Proofing (LoIP) of qualified trust service subjects applicable to all relevant ETSI trust service standards, including enabling TSPs to issue qualified certificates based on verified identity information that satisfies the assurance level requirements of the amended eIDAS Regulation and applicable national legislation.

In accordance with Article 24(1) of the amended eIDAS Regulation (EU) No 910/2014 [i.1], a TSP may verify the identity of a natural person or a legal person either directly or by relying on a third party. ETSI TS 119 461 [7]**,** the technical specification for the policy and security requirements for trust service components providing identity proofing of trust service subjects, states:

> *The identity proofing service component (IPSC) can be an integral part of the Trust Service Provider's (TSP) service provisioning, but the service component can also be the task of a specialized Identity Proofing Service Provider (IPSP) acting as a subcontractor to the TSP.*

This document is structured into nine sections. Not all sections and subsections are relevant to the specific service components provided by The Service.

1.2 Document name and identification

The name of this document is:

“Stø AS identity proofing service provider practice statement”.

Stø AS as an IPSP claims conformance to ETSI TS 119 461 [7] via the following identity proofing policy OID:

itu-t(0) identified-organization(4) etsi(0) IDENTITY-PROOFING-policies(19461) policyidentifiers(1) extended(2)

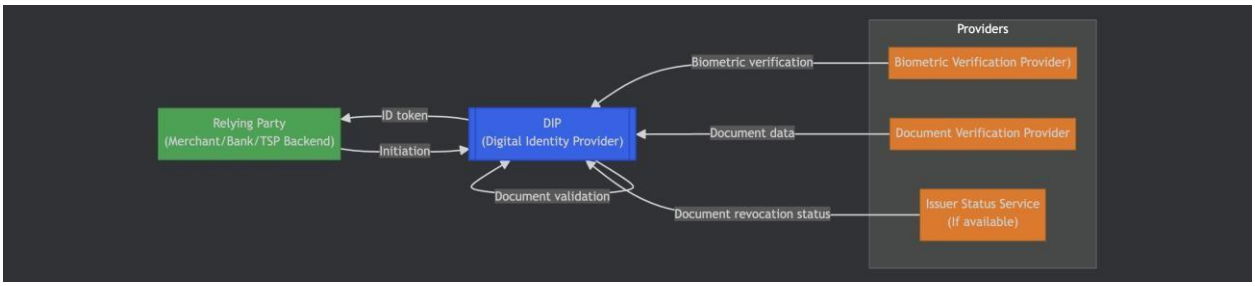
1.2.1 Conventions

The structure (headings and subheadings) in this IPSPS is organised in accordance with recommendations in ETS TS 119 461 [7].

In the present document “shall”, “shall not”, “should”, “should not”, “may”, “need not”, “will”, “will not”, “can” and “cannot” are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules [11].

1.3 Participants

The Stø AS Identity Proofing Service is based on a fully automated unattended remote identity proofing architecture.



1.3.1 Trust Service Provider

Trust Service Provider is an entity adhering to eIDAS Regulation Article 3 (19) and (20). Where a commercial agreement exists, a TSP is the consumer of DIP service and has a contractual relationship with Stø.

1.3.2 Applicant

A natural person whose identity is to be proven.

1.3.3 Subscriber

A natural person bound by an agreement with a trust service provider to any subscriber obligation.

1.3.4 Other Participants

1.3.4.1 Document Verification Provider

Document Verification Provider is an external IPSC, maintaining their own ETSI TS 119 461 compliant Trust Service Practice Statement (TSPS) and holding their own eIDAS and ETSI certifications. The provider is audited and assessed against the eIDAS regulation and ETSI standards. This service is outside the scope of the present document.

The Document Verification Provider is responsible for performing authoritative evidence collection and validation relating to digital identity documents as set out in ETSI 119 461 sections 8.2.3 and 8.3.2.

1.3.4.2 Biometric Verification Provider

The Biometric Verification Provider is an external IPSC, maintaining their own ETSI TS 119 461 compliant Trust Service Practice Statement (TSPS) and holding their own eIDAS and ETSI certifications. The provider is audited and assessed against the eIDAS regulation and ETSI standards. This service is outside the scope of the present document.

The Biometric Verification Provider is responsible for performing automated face biometrics as set out in ETSI 119 461 section 8.4.3.

1.3.4.3 Public Cloud Provider

The underlying infrastructure is provided through Microsoft Azure, which is ISO/IEC 27001 certified.

1.4 Policy administration

For details related to policy and practices administration and responsibilities, please see [9] section 1.5.

1.5 Definitions and abbreviations

1.5.1 Definitions

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.2], ETSI TS 119 461 [7] and the following apply:

NOTE: Where a definition is copied from a referenced document this is indicated by inclusion of the reference identifier number at the end of the definition.

Applicant	A natural person whose identity is to be proven.
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. [i.1]

1.5.2 Abbreviations

APCER	Attack Presentation Classification Error Rate
BPCER	Bonafide Presentation Classification Error
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
DORA	Digital Operational Resilience Act [i.6]
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
FAPI	Financial-grade API
FAR	False Acceptance Rate

FRR	False Rejection Rate
FSA	Financial Supervisory Authority of Norway
ICAO	Internation Civil Aviation Organization
IPSC	Identity Proofing Service Component
IPSP	Identity Proofing Service Provider
ISMS	Information Security Management System
LoA	Level of Assurance
LoIP	Level of Identity Proofing
NDPA	Norwegian Data Protection Authority
NKOM	Norwegian Communications Authority
OIDC	OpenID Connect
OIDC4IA	OpenID Connect for Identity Assurance
PAD	Presentation Attack Detection
SOC 2	System and Organization Controls 2
SSDLC	Secure Software Development Life Cycle
TSP	Trust Service Provider

1.6 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

1.6.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ETSI EN 319 401 (V3.1.1 2024-06): “ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers”

[2] ISO/IEC 19795-1:2021: “Information technology — Biometric performance testing and reporting Part 1: Principles and framework”

[3] ISO/IEC 30107-3: “ISO/IEC 30107-3:2023 Information technology — Biometric presentation attack detection Part 3: Testing and reporting”

[4] ICAO Doc 9303 part 10: "Machine Readable Travel Document - Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)".
[5] ISO/IEC 15408:2022: "Information technology -- Security techniques -- Evaluation criteria for IT security".
[6] ISO/IEC 19989-3:2020: “Information security — Criteria and methodology for security evaluation of biometric systems Part 3: Presentation attack detection”
[7] ETSI TS 119 461 (v2.1.1): “Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects”.
[8] Privacy policy for BankID app: https://bankid.no/en/privacy-policy-for-bankid-app
[9] Stø AS Trust Services Practice Statement
[10] ISO/IEC 27001:2022: “Information security, cybersecurity and privacy protection — Information security management systems — Requirements” [11] ETSI Drafting Rules (EDRs), accessed 29.02.2024: https://portal.etsi.org/Services/editHelp/How-to-start/ETSI-Drafting-Rules

1.6.2 Informative references

[i.1] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[i.2] ETSI TR 119 001 (v1.2.1): "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".
[i.3] ENISA: "Methodology for Sectoral Cybersecurity Assessments", EU Cybersecurity Certification Framework, September 2021.
[i.4] 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 and repealing Directive 1999/93/EC, consolidated version: 18/10/2024.
[i.5] ETSI EN 319 411-1 (v1.5.1): “Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements”
[i.6] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

1.7 Notations

Text that is outside text boxes is the applicable policy requirement. Each requirement is identified with the following syntax:

In brackets: <6 digits>/<3 letters>-<clause number>

- The 6 digits reflect the standard stating the requirement.
- The 3 letters refer to type of requirement.
- The clause number reflects the clause number in the referred standard.

Text contained inside orange coloured text boxes details the practices employed by Stø AS to meet the applicable policy requirements.

1.8 General provisions

a) **(119 461/OVR-5-01):** The requirements specified in ETSI EN 319 401 [1], clause 5 shall apply.

See below letters b) – f)

b) **(119 401/REQ-5-01)**: The TSP shall carry out a risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues.

See [9], section 2 a)

c) **(119 401/REQ-5-02)**: The TSP shall select the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.

See [9], section 2 b)

d) **(119 401/REQ-5-03)**: The TSP shall determine all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the trust service practice statement (see clause 6).

See [9], section 2 c)

e) **(119 401/REQ-5-04)**: The risk assessment shall be regularly reviewed and revised.

See [9], section 2 d)

f) **(119 401/REQ-5-05)**: The TSP's management shall approve the risk assessment and accept the residual risk identified.

See [9], section 2 e). In addition:

Stø AS management will approve the risk assessment and accept the residual risks identified.

g) **(119 461/OVR-5-02)**: The IPSP's risk assessment shall be updated yearly.

Stø AS performs yearly reviews of risk assessments and authors required updates as needed.

h) **(119 461/OVR-5-03)**: The IPSP's risk assessment shall cover relevant risks related to identity proofing and at least:
   a. An assessment of the risks related to identity fraud; and
   b. An assessment of the risks related to information systems security.

Stø AS ISMS has defined a risk management policy mandating regular risk assessments. The risk management policy considers risks related to identity proofing including risks related to identity fraud and information systems security.

i) **(119 461/OVR-5-04)**: The IPSP's risk assessment shall be updated if an identity proofing process is changed.

Stø AS ISMS has a defined risk management policy mandating the risk assessment is updated when identity proofing processes are changed.

j) **(119 461/OVR-5-05)**: The IPSP shall have a documented and effective procedure for threats intelligence that ensures that the IPSP's service is adapted to new threats.

Stø AS has threat intelligence procedures in place based on ENISA report “Methodology for sectoral cybersecurity assessments” [i.3]

k) **(119 461/OVR-5-06)**: The IPSP's risk assessment shall be updated according to findings from the threats intelligence procedure.

Stø AS ISMS has a defined risk management procedure in place which includes updating the risk assessment in accordance with findings from the threats intelligence procedure.

l) **(119 461/OVR-5-07)** [CONDITIONAL]: If the Baseline LoIP is claimed, the risk assessment shall consider at least attackers with moderate attack potential.

Not applicable; The Service does not make a claim to Baseline LoIP.

m) **(119 461/OVR-5-08)**: If the Extended LoIP is claimed, the risk assessment shall consider at least attackers with high attack potential.

Stø AS ISMS has a defined risk management procedure in place which includes considering risks from attackers with high attack potential.

n) **(119 461/OVR-5-09)**: Based on findings from the threats intelligence procedure and changes to the risk assessment, the need for training of personnel shall be assessed and training be carried out if needed.

Stø AS carries out regular assessment of the need for training personnel and training is performed as and when needed.

o) **(119 461/OVR-5-10)**: The IPSP shall state in its practice statement goals for quality and security in terms of resilience to false acceptance and false rejection of applicants and perform regular testing of the performance against these goals.

Stø AS sets out goals for quality and security of The Service in terms of resilience to false acceptance and false rejection of applicants that are in line with industry best practices. Regular testing of the performance of the product is carried out with both automated and manual testing against these goals.

2 Policies and practices

2.1 Identity proofing service practice statement

a) **(119 461/OVR-6.1-01)**: The requirements specified in ETSI EN 319 401 [1], clause 6.1 shall apply.

See [9] section 3.1 with subsections, section 3.12 of the present document, and letters below.

b) **(319 401/REQ-6.1-03X)**: The TSP shall have a statement of the practices and procedures used to address all the requirements of the applicable trust service policy as identified by the TSP.

See [9] section 3.1 letter c).

c) **(319 401/REQ-6.1-04)**: The TSP's trust service practice statement shall identify the obligations of all external organizations supporting the TSP's services including the applicable policies and practices.

This document in combination with the Stø TSPS document [9] identifies the obligations to be adhered to by all external organizations (listed under section 1.3.4 of the present document) to which any task has been outsourced. Such requirements obligations are detailed in the outsourcing contract.

d) **(319 401/REQ-6.1-05X)**: The TSP shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to demonstrate conformance to the trust service policy.

See [9] section 3.1 letter e).

e) **(319 401/REQ-6.1-09X)** [CONDITIONAL]: When the TSP intends to make changes in its practice statement that might affect the acceptance of the service by the subject, subscriber or relying parties, it shall give due notice of changes to subscribers and relying parties.

See [9] section 3.1 letter i)

f) **(119 461/OVR-6.1-02)**: An IPSP claiming compliance with the present document shall identify in its practice statement the use cases for which compliance is claimed.

The Service claims compliance with the following use cases as set out in ETSI TS 119 461 [7] relating to use case for automated operation; use case for issuing of qualified certificate according to Article 24.1 of the original eIDAS regulation relating to identity proofing by other identification means; and use case for issuing of qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, and 24.1b of the amended eIDAS regulation relating to identity proofing by other identification means.

g) **(119 461/OVR-6.1-03)**: Identification of use cases for which compliance is claimed shall be by reference to specific parts of clause 9 and/or Annex C of the present document.

The Service claims compliance with the following use cases as set out in ETSI TS 119 461 [7] sections 9.2.3.4; C.2.4; and C.3.4.

2.2 Terms and conditions

a) **(119 461/OVR-6.2-01)**: The requirements specified in ETSI EN 319 401 [1], clause 6.2 shall apply.

The obligations relating to terms and conditions fall onto the QTSP to provide to the applicant before initiation of the identity proofing process in accordance with Section 4.1 letter a) of the present document.

2.3 Information and security policy

a) **(119 461/OVR-6.3-01)**: The requirements specified in ETSI EN 319 401 [1], clause 6.3 shall apply.

See [9] section 3.3.

b) **(319 401/REQ-6.3-04X)**: The TSP shall establish procedures to notify of important changes in the provision of the trust service to the appropriate parties in accordance with business requirements and relevant laws and regulations, including changes in the provision of trust services and the intention to cease on its provision.

The Service is subject to the change-management procedures established by the internal Change Advisory Board (CAB). All changes must be reviewed and approved by the CAB prior to implementation. The CAB shall notify all relevant parties, including the relying TSPs, and shall fulfil all applicable reporting obligations in accordance with the relevant legislative and regulatory frameworks, including DORA [i.6], as well as the requirements set by supervisory authorities such as the FSA, NKOM, and the NDPA.

3 Identity proofing service management and operation

3.1 Internal organization

a) **(119 461/OVR-7.1-01)**: The requirements specified in ETSI EN 319 401 [1], clause 7.1 shall apply.

See [9] section 4.1.

3.2 Human resources

a) **(119 461/OVR-7.2-01)**: The requirements specified in ETSI EN 319 401 [1], clause 7.2 shall apply.

See below letters b) – t).

b) **(319 401/REQ-7.2-01X)**: The TSP shall ensure that all personnel and contractors apply information security in accordance with the established information security policy, topicspecific policies and procedures of the TSP.

Stø AS ensures that all personnel and contractors follow the established information security policy and all related procedures through mandatory training, documented responsibilities, and enforced adherence as a condition for system access.

c) **(319 401/REQ-7.2-02)**: The TSP shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding cybersecurity and personal data protection rules as appropriate for the offered services and the job function.

See [9] section 4.2 letter b).

d) **(319 401/REQ-7.2-03X)**: The TSP shall identify at least one person responsible for network and information security and reporting to top management.

The Service has designated a Security Officer as the person responsible for network and information security, ensuring direct reporting to top management and oversight of compliance with all security policies and procedures.

e) **(319 401/REQ-7.2-04X)**: TSP's personnel should be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two.

See [9] section 4.2 letter c).

f) **(319 401/REQ-7.2-05X)**: This should include regular (at least every 12 months) updates on new threats and current security practices.

See [9] section 4.2 letter d).

g) **(319 401/REQ-7.2-06X)**: Appropriate disciplinary sanctions shall be applied to personnel violating TSP's policies or procedures.

See [9] section 4.2 letter e).

h) **(319 401/REQ-7.2-07X)**: Information security roles and responsibilities, as specified in the TSP's information security policy, shall be documented in job descriptions or in documents available to all concerned personnel and allocated accordingly.

See [9] section 4.2 letter f).

i) **(319 401/REQ-7.2-08X)**: Trusted roles, on which the TSP's operation is dependent, shall be clearly identified.

See [9] section 4.2 letter g).

j) **(319 401/REQ-7.2-09X)**: TSP's personnel (both temporary and permanent) shall have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege (see clause 7.1.2), determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.

See [9] section 4.2 letter h).

k) **(319 401/REQ-7.2-10X)**: Where appropriate, job descriptions shall differentiate between general functions and TSP's specific functions. These should include skills and experience requirements.

See [9] section 4.2 letter i).

l) **(319 401/REQ-7.2-11X)**: Personnel shall exercise administrative and management procedures and processes that are in line with the TSP's information security management procedures.

See [9] section 4.2 letter j).

m) **(319 401/REQ-7.2-12X)**: Managerial personnel shall possess experience or training with respect to the trust service that is provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

See [9] section 4.2 letter k).

n) **(319 401/REQ-7.2-13X)**: All TSP's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSP's operations.

See [9] section 4.2 letter l).

o) **(319 401/REQ-7.2-14X)**: Trusted roles shall include roles that involve the following responsibilities:
    a. **Security Officers**: Overall responsibility for administering the implementation of the security practices.
    b. **System Administrators**: Authorized to install, configure and maintain the TSP's trustworthy systems for service management.
    c. **System Operators**: Responsible for operating the TSP's trustworthy systems on a day-to-day basis. Authorized to perform system backup.
    d. **System Auditors**: Authorized to view archives and audit logs of the TSP's trustworthy systems.

The Service defines trusted roles that include Security Officers responsible for administering security practices, System Administrators authorized to install, configure and maintain the trustworthy systems, System Operators responsible for daily operation and system backups, and System Auditors authorized to review archives and audit logs.

p) **(319 401/REQ-7.2-15X)**: TSP's personnel shall be formally appointed to trusted roles by senior management responsible for security.

See [9] section 4.2 letter n).

q) **(319 401/REQ-7.2-16X)**: Trusted roles shall be accepted by the appointed person to fulfil the role.

See [9] section 4.2 letter o).

r) **(319 401/REQ-7.2-17)**: Personnel shall not have access to the trusted functions until the necessary checks are completed.

See [9] section 4.2 p).

s) **(319 401/REQ-7.2-18X)** [CONDITIONAL]: When personnel are working remotely, TSP shall implement cybersecurity measures to protect information accessed, processed or stored outside the TSP's premises.

When personnel work remotely, the Stø AS enforces the ISMS Remote Working Policy supported by endpoint management, DLP protection and other ISMS-mandated controls to ensure that all information accessed, processed or stored outside Stø AS premises remains secure.

t) **(319 401/REQ-7.2-19X)**: TSPs allowing remote working activities shall issue a topicspecific policy on remote working that defines the relevant cybersecurity conditions and restrictions.

Stø AS has an ISMS Remote Working Policy that defines the relevant cybersecurity conditions and restrictions.

3.3 Asset management

a) **(119 461/OVR-7.3-01)**: The requirements specified in ETSI EN 319 401 [1], clause 7.3 shall apply.

See below.

b) **(319 401/REQ-7.3.1-01)**: The TSP shall ensure an appropriate level of protection of its assets including information assets.

See [9] section 4.3.1 a).

c) **(319 401/REQ-7.3.1-02X)**: The assets provided through a supply chain shall be protected as specified in clause 7.14.

Stø AS ensures that all assets obtained through the supply chain are protected in accordance with clause ETSI TS 319 401 [1] clause 7.14 by enforcing ISMS-mandated supplier security controls, including rigorous vendor assessments, contractual security requirements, and continuous monitoring of supply-chain–related risks.

d) **(319 401/REQ-7.3.2.01X)**: The TSP shall maintain an accurate inventory of assets as a prerequisite for effective technical vulnerability management and shall assign a classification consistent with the risk assessment.

Stø AS maintains an accurate and continuously updated asset inventory, classified in accordance with the risk assessment, as a prerequisite for effective technical vulnerability management and in alignment with the ISMS Asset Inventory requirements.

e) **(319 401/REQ-7.3.2-02X)**: For asset, or group of assets, the inventory shall contain, when applicable:
    a. a unique asset ID;
    b. an asset description;
    c. the asset owner;
    d. the asset location;
    e. the asset type (e.g. software, hardware, services, facilities, HVAC systems, personnel, physical records);
    f. the type of information processed or/stored in the asset and its information classification;
    g. the date and version of the asset's last update or patch;
    h. the classification level of the asset; and
    i. the asset's end of life.

Stø AS maintains an asset inventory and contains, where applicable, the above information.

f) **(319 401/REQ-7.3.2-03X)**: The TSP shall assign a classification level to each asset, or group of assets, based on requirements for protecting confidentiality, integrity, authenticity and availability, and in accordance to its risk assessment and business value.

Stø AS assigns classification levels to each asset in the asset inventory as per the organisation's ISMS.

g) **(319 401/REQ-7.3.2-04X)**: The TSP shall assure that the availability requirements of each asset, or group of assets, classified are aligned with the delivery and recovery objectives as described in the business and disaster recovery plan.

Stø AS ensures that the availability requirements for each asset, or asset group, are aligned with defined delivery and recovery objectives by mapping asset availability classifications to the Business Continuity Plan and Disaster Recovery Plan and validating this alignment through the ISMS asset inventory and continuity management processes.

h) **(319 401/REQ-7.3.2-05X)**: The TSP shall conduct periodic reviews of the classification levels of the assets.

Stø AS conducts periodic reviews of asset classification levels as part of its ISMS Asset Management processes to ensure that classifications remain accurate, risk-appropriate and aligned with current operational and security requirements.

i) **(319 401/REQ-7.3.2-06X)**: The TSP shall identify, document and implement rules for the acceptable use of and procedures for handling information and other associated assets.

Stø AS identifies, documents and enforces rules for acceptable use and handling of information and associated assets in accordance with the ISMS Standard for Information Classification and Asset Management.

j) **(319 401/REQ-7.3.2-07X)**: The TSP shall implement and document procedures in case of change or termination process of, internal and external personnel, contractors or other third parties in order to include the return of all previously issued physical and electronic assets owned by or entrusted to the TSP.

Stø AS has implemented and documented offboarding procedures for internal and external personnel, contractors and third parties to ensure that, upon change or termination, all

previously issued physical and electronic assets owned by or entrusted to Stø AS are returned in accordance with the established ISMS offboarding process.

k) **(319 401/REQ-7.3.3-01X)**: All storage media shall be managed through its life cycle of acquisition, use, transportation and disposal in accordance with the TSP's classification scheme and handling requirements.

Stø AS manages all storage media throughout its lifecycle covering acquisition, use, transportation and secure disposal in accordance with the ISMS classification and handling requirements, supported by contractual protections with internal and external personnel, contractors and other third parties, enforced full-disk encryption on all managed endpoints, and mandatory encryption of external media when connected to Stø AS devices.

l) **(319 401/REQ-7.3.3-02X)**: Storage media used within the TSP's systems shall be securely handled to protect storage media from damage, theft, unauthorized access and obsolescence.

See [9] section 4.3.2 letter b).

m) **(319 401/REQ-7.3.3-03X)**: Storage media management procedures shall protect against obsolescence and deterioration of storage media within the period of time that records are required to be retained.

See [9] section 4.3.2 letter c).

3.4 Access control

a) **(119 461/OVR-7.4-01)**: The requirements specified in ETSI EN 319 401 [1], clause 7.4 shall apply.

See below.

b) **(319 401/REQ-7.4-01)**: The TSP's system access shall be limited to authorized individuals.

See [9] section 4.4 a).

c) **(319 401/REQ-7.4-02X)**: The TSP shall administer user access of operators, administrators and other privileged accounts and system auditors applying the principle of "least privileges" when configuring access privileges. In particular:

See [9] section 4.4 letter b).

d) **(319 401/REQ-7.4-03X)**: The TSP shall provide setting up specific accounts to be used for administrative purposes like installation, configuration, management or maintenance.

Stø AS provides dedicated administrative accounts for installation, configuration, management and maintenance activities, with their creation and use controlled through the Privileged Identity Management (PIM) solution, enforced approval workflows, and the responsibilities defined in the trusted roles framework.

e) **(319 401/REQ-7.4-04X)**: Privileged accounts shall be used only if the privileges are necessary for the specific activity.

Stø AS ensures that privileged accounts are used only when the elevated rights are strictly required for the specific activity, with all privileged access governed through Privileged Identity

Management (PIM) with approval flows, which enforces justification, time-bound elevation and change-management approval in accordance with the trusted-roles framework.

f) **(319 401/REQ-7.4-05X)**: Strong identification, authentication and authorisation procedures shall be used for privileged accounts.

Stø AS enforces strong identification, authentication and authorisation for all privileged accounts, applying MFA, role-based access controls and secure credential practices in alignment with the ISMS Identity and Access Management Policy, which mandates rigorous security controls for all systems handling privileged access.

g) **(319 401/REQ-7.4-06X)** [CONDITIONAL]: Where appropriate, the TSP shall ensure that users and devices are authenticated by multi-factor or continuous authentication mechanisms, such as secure voice, video and text, before accessing the TSP's network and ITS information systems, depending on the classification of the systems to be accessed.

See above letter f).

h) **(319 401/REQ-7.4-07X)**: The TSP shall review access rights to privileged and administrator accounts at planned intervals, and access rights shall be modified based on organisational changes. The result of the review, including the necessary changes of access rights, shall be documented.

See above letter f).

i) **(319 401/REQ-7.4-08X)**: The TSP shall ensure that access permissions are modified accordingly upon termination of employment or change of function.

See section 3.3 letter j) of the present document.

j) **(319 401/REQ-7.4-09X)**: Access to information and application system functions shall be restricted in accordance with the access control policy.

Stø AS restricts access to information and application system functions in accordance with the access control policy, ensuring that write-access is limited to users in approved trusted roles, with the Security Officer responsible for overseeing and approving such access in line with ISMS least-privilege requirements.

k) **(319 401/REQ-7.4-10X)**: The TSP's system shall provide sufficient computer security controls for the separation of trusted roles identified in TSP's practices, including the separation of security administration and operation functions. Particularly, use of system utility programs shall be restricted and controlled.

Stø AS enforces strict computer security controls to maintain separation of all trusted roles including clear separation of administration from operational functions and restricts and monitors the use of system programs in accordance with ISMS-mandated access control and trusted-role requirements.

l) **(319 401/REQ-7.4-11X)**: TSP's personnel shall be identified and authenticated before using critical applications related to the service.

See [9] section 4.4 letter f).

m) **(319 401/REQ-7.4-12X)**: TSP's personnel shall be accountable for their activities.

See [9] section 4.4 letter g).

n) **(319 401/REQ-7.4-13X)**: Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) or storage media (see clause 7.3.2) being accessible to unauthorized users.

See [9] section 4.4 letter h).

3.5 Cryptographic controls

a) **(119 461/OVR-7.5-01)**: The requirements specified in ETSI EN 319 401 [1], clause 7.5 shall apply.

See below.

b) **(319 401/REQ-7.5-01X)**: Appropriate security controls shall be in place for the management of any cryptographic keys, cryptographic algorithms, and cryptographic devices throughout their lifecycle.

All cryptographic keys used by The Services are generated, stored and used within HSMs.

Critical cryptographic keys are managed by HSMs certified in accordance with ISO/IEC 15408 with assurance level EAL 4+ and ISO 19790. Other cryptographic keys are stored according to their criticality, at least in key vaults using HSMs conforming to FIPS 140-2, level 2.

Established management practices, operations and security controls are in line with vendors recommendations for maintaining the operational requirements in line with the HSMs certification.

When cryptographic keys are backed up, the backups will be encrypted by a key protected by equivalent security controls to the key to be backed up.

3.6 Physical and environmental security

a) **(119 461/OVR-7.6-01)**: The requirements specified in ETSI EN 319 401 [1], clause 7.6 shall apply.

The underlying infrastructure is provided through Microsoft Azure, which is ISO/IEC 27001 and SOC 2 certified. The physical access to the components of The Service is managed by Microsoft Azure. The cloud provider has gone through The Service's procurement process.

3.7 Operation security

a) **(119 461/OVR-7.7-01)**: The requirements specified in ETSI EN 319 401 [1], clause 7.7 shall apply.

See below.

a) **(319 401/REQ-7.7-01)**: The TSP shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

See [9] section 4.7 a).

b) **(319 401/REQ-7.7-02)**: An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project

undertaken by the TSP or on behalf of the TSP to ensure that security is built into IT systems.

See [9] section 4.7 b).

c) **(319 401/REQ-7.7-03)**: Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies the TSP's security policy.

See [9] section 4.7 c).

d) **(319 401/REQ-7.7-04)**: The procedures shall include documentation of the changes.

See [9] section 4.7 d).

e) **(319 401/REQ-7.7-05)**: The integrity of TSP's systems and information shall be protected against viruses, malicious and unauthorized software.

See [9] section 4.7 letter e).

f) **(319 401/REQ-7.7-06X)**: Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of services.

See [9] section 4.7 letter f).

g) **(319 401/REQ-7.7-07X)**: The TSP shall specify and apply procedures for ensuring that:
a) security patches are applied within a reasonable time after they come available;
b) security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and
c) the reasons for not applying any security patches are documented.

Stø AS ensures that security patches are applied within a reasonable timeframe, deferred only when they introduce greater risk and fully documented when not applied, with all software releases governed by ISMS change management processes including pre-release security testing while infrastructure patching is handled under third parties' contractual obligations for platform security and maintenance.

h) **(319 401/REQ-7.7-08X)**: The TSP shall establish, document, implement, monitor, and review configurations, including security configurations, of hardware, software, services and networks.

Stø AS establishes, documents, implements, monitors and reviews security configurations for software, services and networks through formally approved design documents validated by Security Officers and network experts and governs all configuration changes through the ISMS Change Management Board to ensure secure and consistent implementation.

i) **(319 401/REQ-7.7-09X)**: The TSP shall monitor configurations with a comprehensive set of system management tools.

Stø AS monitors the configurations of systems with a comprehensive set of system

management tools.

j) **(319 401/REQ-7.7.10X)**: The TSP shall review configurations on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed.

Stø AS conducts regular configuration reviews at intervals defined by the ISMS to verify configuration settings, evaluate password strengths and assess system activities, etc with the

Security Officer responsible for overseeing the reviews and the Audit Officer ensuring independent verification and documentation of the outcomes.

3.8 Network security

a) **(119 461/OVR-7.8-01)**: The requirements specified in ETSI EN 319 401 [1], clause 7.8 shall apply.

See letters c) – w) of the present section.

b) **(119 461/OVR-7.8-02)**: The information system making the identity proofing decision shall be logically or physically separated from non-critical information systems at the IPSP.

Critical systems supporting The Service are in secured network zones with controlled perimeter protection providing logical separation of the non-critical information systems from the information system making the identity proofing decision.

c) **(319 401/REQ-7.8-01)**: The TSP shall protect its network and systems from attacks.

See [9] section 4.8 letter a).

d) **(319 401/REQ-7.8-02)**: The TSP shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services.

The Service segments its systems in networks and zones based on risk assessments considering functional and logical relationships between trustworthy systems and services. The Service is segregated into two logical zones, the secure zone and the high-secure zone. Low to medium risk systems are placed in the secure zone, whilst systems integral to the overall security of the services are placed in the high secure zone.

e) **(319 401/REQ-7.8-03)**: The TSP shall apply the same security controls to all systems co-located in the same zone.

See [9] section 4.8 letter c).

f) **(319 401/REQ-7.8-04)**: The TSP shall restrict access and communications between zones to those necessary for the operation of the TSP.

See [9] section 4.8 letter d).

g) **(319 401/REQ-7.8-05)**: The TSP shall explicitly forbid or deactivate not needed connections and services.

See [9] section 4.8 letter e).

h) **(319 401/REQ-7.8-06)**: The TSP shall review the established rule set on a regular basis.

See [9] section 4.8 letter f).

i) **(319 401/REQ-7.8-07)**: The TSP shall keep all systems that are critical to the TSP's operation in one or more secured zone(s) (e.g. Root CA systems see ETSI EN 319 411-1 [i.5])

See [9] section 4.8 letter g).

j) **(319 401/REQ-7.8-08)**: The TSP shall separate dedicated network for administration of IT systems and TSP's operational network.

See [9] section 4.8 letter h).

k) **(319 401/REQ-7.8-09X)**: The TSP shall logically separate administration systems and networks from other information systems and networks.

Stø AS ensures the logical separation and isolation between production systems and networks from other information systems networks.

l) **(319 401/REQ-7.8-10)**: The TSP shall separate the production systems for the TSP's services from systems used in development and testing (e.g. development, test and staging systems).

See [9] section 4.8 letter j).

m) **(319 401/REQ-7.8-11X)**: The TSP shall establish communication between distinct trustworthy systems only through trusted channels that are isolated using logical, cryptographic or physical separation from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

See [9] section 4.8 letter k).

n) **(319 401/REQ-7.8-12)**: If a high level of availability of external access to the trust service is required, the external network connection shall be redundant to ensure availability of the services in case of a single failure.

See [9] section 4.8 letter l).

o) **(319 401/REQ-7.8-13)**: The TSP shall undergo or perform a regular vulnerability scan on public and private IP addresses identified by the TSP and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

See [9] section 4.8 letter m).

p) **(319 401/REQ-7.8-14X)**: The vulnerability scan requested by **REQ-7.8-13** should be performed once per quarter.

See [9] section 4.8 letter n).

q) **(319 401/REQ-7.8-15X)**: The TSP shall protect its network and information systems against malicious and unauthorised software by means of malware detection and removal software, which is updated at least on a daily basis.

Stø AS protects its network and information systems from malicious and unauthorised software by means of malware detection and removal software, updated on a daily basis, in accordance with the organisation’s ISMS.

r) **(319 401/REQ-7.8-16X)**: The TSP shall regularly update its malware detection and repair software.

Stø AS ensures that the malware detection and repair software is regularly updated in accordance with the organisation’s ISMS.

s) **(319 401/REQ-7.8-17X)**: The TSP shall undergo a penetration test on the TSP's systems at set up and after infrastructure or application upgrades or modifications that the TSP determines are significant.

See [9] section 4.8 letter o).

t) **(319 401/REQ-7.8-18X)**: The penetration test requested by REQ-7.8-17X should be performed at least once per year.

See [9] section 4.8 letter p).

u) **(319 401/REQ-7.8-19X)**: The TSP shall record evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

See [9] section 4.8 letter q).

v) **(319 401/REQ-7.8-20X)**: Controls (e.g. firewalls) shall protect the TSP's internal network domains from unauthorized access including access by subscribers and third parties.

See [9] section 4.8 letter r).

w) **(319 401/REQ-7.8-21X)**: Firewalls should also be configured to prevent all protocols and accesses not required for the operation of the TSP.

See [9] section 4.8 letter s).

3.9 Vulnerabilities and incident management

a) **(119 461/OVR-7.9-01)**: The requirements specified in ETSI EN 319 401 [1], clause 7.9 shall apply.

See sections 3.9.1, 3.9.2, 3.9.3, 3.9.4, 3.9.5 of the present document.

b) **(119 461/OVR-7.9-02)**: Reporting obligations according to ETSI EN 319 401 [1] REQ7.9.2-02X and clause 7.9.3 shall be fulfilled as required by the identity proofing context and the obligations of the TSPs relying on the IPSP's service.

See [9] section 4.9. In addition, The Service complies with reporting obligations as mandated by relevant legislative frameworks for network and information security incidents, including supervisory authorities and CSIRTs.

3.9.1 Monitoring and logging

a) **(319 401/REQ-7.9.1-01X)**: The TSP shall establish mechanisms to detect potential security incidents and to respond accordingly by implementing tools and processes to enable continuous monitoring and logging of activities on the entity's network and information systems.

Stø AS has established mechanisms to detect potential security incidents by ensuring 24/7 monitoring of its networks and information systems by SOC teams using appropriate security tools, supported by defined incident response plans and continuously updated detection rules aligned with ETSI requirements and the evolving threat landscape.

b) **(319 401/REQ-7.9.1-02X)**: Monitoring activities should take account of the sensitivity of any information collected or analysed.

See [9] section 4.9 letter b).

c) **(319 401/REQ-7.9.1-03X)**: Abnormal system activities that indicate a potential security violation, including intrusion into the TSP's network, shall be detected and reported as alarms.

See [9] section 4.9 letter c).

d) **(319 401/REQ-7.9.1-04X)**: The TSP shall maintain, document and regularly review logs which shall include:
    a. outbound and inbound network traffic;
    b. activities regarding user administration and permission management, access (including privileged access) to systems and applications;
    c. activities performed with administrator accounts;
    d. assess or changes to critical configuration files and backups;
    e. security relevant logs;
    f. use and performance of system resources;
    g. physical access to facilities, where appropriate;
    h. access and use of network equipment and devices; and
    i. environmental events, where appropriate.

Stø AS maintains, documents and regularly reviews all required log sources including network traffic, user and permission administration, privileged activity, configuration changes, security-relevant events, system resource usage and network-device activity with 24/7 monitoring of defined events to ensure timely detection and response.

e) **(319 401/REQ-7.9.1-05X)**: The TSP's systems shall be monitored including the monitoring or regular review of audit logs to identify evidence of malicious activity implementing automatic mechanisms to process the audit logs and alert personnel of possible critical security events.

See [9] section 4.9 letter i).

3.9.2 Incident response

a) **(319 401/REQ-7.9.2-01X)**: The TSP shall establish incident response procedures including containment, eradication and recovery.

Stø AS has established incident response procedures covering containment, eradication and recovery, implemented in accordance with the ISMS Standard for Incident Management, ensuring that security incidents are handled systematically and effectively.

b) **(319 401/REQ-7.9.2-02X)**: The TSP shall comply with reporting obligations as mandated by relevant legislative frameworks for network and information security incidents, including supervisory authorities and CSIRTs.

Stø AS complies with reporting obligations in conformance with relevant legislative frameworks including eIDAS [i.1], DORA [i.6], and as set out by supervisory authorities such as FSA, NKOM, and NDPA.

c) **(319 401/REQ-7.9.2-03X)**: TSPs shall inform stakeholders about incidents according to agreed communication plans.

Stø AS informs stakeholders about incidents according to agreed communication plans as set out in the organisation’s internal global communication plan.

d) **(319 401/REQ-7.9.2-04X)**: The TSP shall establish and maintain effective communication plans that include incident categorisation, well-defined escalation procedures, and standardised reporting protocols.

Stø AS establishes effective communication plans in the internal global communication plan, and maintains standard for incident management, which defines incident categorisation and well-defined escalation procedures, and standardised reporting protocols.

e) **(319 401/REQ-7.9.2-05X)**: The TSP shall ensure that personnel possess the necessary competencies to proficiently detect and respond to security incidents.

Stø AS ensures that personnel possess the competencies necessary to effectively detect and respond to security incidents by employing skilled SOC analysts hired based on demonstrated expertise, assessed through security-focused interviews, and continuously kept up to date on the evolving threat landscape.

f) **(319 401/REQ-7.9.2-06X)**: The TSP shall create and maintain comprehensive documentation throughout the incident detection and response process.

Stø AS creates and maintains comprehensive documentation throughout the incident detection and response process in accordance with the ISMS Standard for Incident Management.

g) **(319 401/REQ-7.9.2-07X)**: The TSP shall establish clear interfaces between the incident handling and business continuity management functions to ensure a coordinated and cohesive response during incidents.

Stø AS maintains clear interfaces between incident handling and business continuity management by ensuring coordinated processes and communication flows defined in the company-wide Business Continuity Plan (BCP) and Crisis Management Plan, enabling unified escalation, decision-making and response during incidents.

h) **(319 401/REQ-7.9.2-08X)**: The TSP shall test and review regularly and after incidents roles, responsibilities and appropriate procedures.

Stø AS tests and reviews roles, responsibilities and relevant procedures on a regular basis at minimum annually and after major changes in the structure to ensure they remain effective, up-to-date and aligned with current operational and security requirements.

i) **(319 401/REQ-7.9.2-09X)**: The TSP shall address any critical vulnerability not previously addressed by the TSP, within a period of 48 hours after its discovery.

See [9] section 4.9 letter j).

j) **(319 401/REQ-7.9.2-10X)**: For any vulnerability, given the potential impact, the TSP shall [CHOICE]:
   - create and implement a plan to mitigate the vulnerability; or
   - document the factual basis for the TSP's determination that the vulnerability does not require remediation.

See [9] section 4.9 letter k).

k) **(319 401/REQ-7.9.2-11X)**: Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.

See [9] section 4.9 letter l).

l) **(319 401/REQ-7.9.2-12X)**: The TSP shall appoint trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures.

See [9] section 4.9 letter f).

3.9.3 Reporting

a) **(319 401/REQ-7.9.3-01X)**: The TSP shall establish procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.

See [9] section 4.9 letter g).

In addition:

- QTSPs within 24 hours after identifying security breach impacting any of their subscribers

Subcontractors are obligated to notify Stø AS of any security breaches or loss of integrity as soon as possible in compliance with Stø AS' outsourcing policy.

b) **(319 401/REQ-7.9.3-02X)**: Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the TSP shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

Stø AS notifies TSPs in line with 3.9.3 a) allowing them to provide timely notifications to any affected applicants.

c) **(319 401/REQ-7.9.3-03X)**: The TSP shall establish a simple procedure allowing its staff, contractors and customers to report possible network and information security incidents.

Stø AS has established a simple procedure for reporting potential network and information security incidents through clearly documented and regularly updated intranet guidance, an external notification channel for customers and third parties, and reporting workflows embedded into the ISMS Secure Software Development Lifecycle (SSDLC) to ensure consistent and timely escalation.

d) **(319 401/REQ-7.9.3-04X)**: The TSP shall communicate the reporting procedure to its contractors and customers and shall train its staff to follow the reporting procedure and to address the appropriate point of contact.

Stø AS communicates the reporting procedure to contractors and customers and trains staff to follow it, supported by regular meetings and defined contact points in supplier, contractor and customer contracts.

3.9.4 Event assessment and classification

a) **(319 401/REQ-7.9.4-01X)**: The TSP shall analyse the reported events and assess their severity.

Stø AS events are analysed as per the priority matrix and classified accordingly as part of the internal incident management policy.

b) **(319 401/REQ-7.9.4-02X)**: The TSP shall be capable to reassess and reclassify events based on new inputs.

Stø AS ensures that the incidents priority and handling actions are updated as new information becomes available.

3.9.5 Post-incident reviews

a) **(319 401/REQ-7.9.5-01X)**: The TSP shall keep itself informed about technical vulnerabilities of all information systems it uses.

Stø AS keeps itself informed about technical vulnerabilities affecting all information systems it uses by following the ISMS Vulnerability Management Standard, Risk Management Standard, Penetration Testing Standard ensuring continuous monitoring, assessment and prioritization of newly identified vulnerabilities.

b) **(319 401/REQ-7.9.5-02X)**: The TSP shall evaluate the TSP's exposure to such vulnerabilities and take appropriate measures.

Stø AS evaluates exposure to vulnerabilities and takes appropriate measures following the assessment and prioritisation of newly identified vulnerabilities. See above for relevant ISMS standards.

c) **(319 401/REQ-7.9.5-03X)**: The TSP shall identify the root cause of an incident and shall conduct a post-incident review possibly resulting in measures mitigating the risk of the recurrence of similar incidents.

Stø AS identifies the root cause of incidents and performs post-incident reviews in accordance with the ISMS Problem Management Standard, which mandates formal root-cause analysis (RCA) and the implementation of measures to mitigate the risk of similar incidents recurring.

d) **(319 401/REQ-7.9.5-04X)**: The TSP shall ensure that each past incident led to a postincident review.

Stø AS ensures that every incident results in a post-incident review in accordance with the ISMS Problem Management process, which mandates documented root-cause analysis and follow-up actions.

3.10 Collection of evidence

a) **(119 461/OVR-7.10-01)**: The requirements specified in ETSI EN 319 401 [1], clause 7.10 shall apply.

See [9] section 4.10 and below.

b) **(119 401/REQ-7.10-01)**: The TSP shall record and keep accessible for an appropriate period of time, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

The Service has established audit logging procedures ensuring that all relevant information to ensure secure operation of The Service and providing evidence in case of legal proceedings.

Evidence of the identity proofing process is stored in accordance with Section 3.10 of the present document in compliance with all retention obligations as set out by the identity proofing context.

c) **(119 401/REQ-7.10-02)**: The confidentiality and integrity of current and archived records concerning operation of services shall be maintained.

Evidence of the identity proofing process is stored in accordance with Section 3.10 of the present document in compliance with all retention obligations as set out by the identity proofing context.

d) **(119 401/REQ-7.10-03)**: Records concerning the operation of services shall be completely and confidentially archived in accordance with disclosed business practices.

Evidence of the identity proofing process is stored in accordance with Section 3.10 of the present document in compliance with all retention obligations as set out by the identity proofing context.

e) **(119 401/REQ-7.10-04)**: Records concerning the operation of services shall be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.

See [9] section 4.10. letter d).

f) **(119 401/REQ-7.10-05)**: The precise time of significant TSP's environmental, key management and clock synchronization events shall be recorded.

See [9] section 4.10. letter e).

g) **(119 401/REQ-7.10-06)**: The time used to record events as required in the audit log shall be synchronized with UTC at least once a day.

See [9] section 4.10. letter f).

h) **(119 401/REQ-7.10-07)**: Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the TSP's terms and conditions (see clause 6.2).

The Service requires that the TSP includes this information within their terms and conditions.

i) **(119 401/REQ-7.10-08)**: The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

Evidence of the identity proofing process is stored in accordance with Section 3.10 of the present document in compliance with all retention obligations as set out by the identity proofing context.

3.11 Business continuity management

a) **(119 461/OVR-7.11-01)**: The requirements specified in ETSI EN 319 401 [1], clause 7.11 shall apply.

See sections 3.11.1, 3.11.2, and 3.11.3 of the present document.

b) **(119 461/OVR-7.11-02)**: Processes for crisis management according to ETSI EN 319 401 [1], REQ-7.11.3-01X shall be as required by the identity proofing context and the obligations of the TSPs relying on the IPSP's service.

The Service extends the process defined under [9] section 4.11 to address obligations to relying TSPs based on the identity proofing context.

3.11.1 General

a) **(319 401/REQ-7.11.1-01X)**: The TSP shall define and maintain a continuity plan to enact in case of a disaster.

See [9] section 4.11 letter a).

b) **(319 401/REQ-7.11-1-02X)**: In the event of a disaster, including compromise of a private signing key or compromise of some other credential of the TSP, operations shall be

restored within the delay established in the continuity plan, having addressed any cause for the disaster which may recur (e.g. a security vulnerability) with appropriate remediation measures.

See [9] section 4.11 letter b).

3.11.2 Back up

a) **(319 401/REQ-7.11.2-01X)**: The TSP shall maintain backup copies of information and sufficient resources, including facilities, network and information systems as well as personnel in accordance with risk assessment and business continuity plan.

Stø AS maintains backup copies of information and ensures sufficient facilities, network, system and personnel resources in line with the risk assessment and Business Continuity Plan, supported by the relevant ISMS policies including the ISMS Risk Management Policy and SSDLC requirements for resilient service design.

b) **(319 401/REQ-7.11.2-02X)**: The TSP shall define backup plans taking into account at least the following:
   a. recovery times;
   b. assurance of the backup copies' completeness and accuracy (including configuration data and information stored in cloud service environment);
   c. storage of backup copies at a safe location or locations which are outside the network of the system backed up and are at sufficient distance to escape any damage from a disaster at the main site;
   d. physical/environmental and logical controls for backup copies in accordance with their information classification level; and
   e. processes for restoring information from backup copies (including approval processes).

Stø AS defines and maintains backup plans that address recovery times, completeness and accuracy of backup copies (including cloud-hosted data and configurations), secure storage in geographically distributed data centers and regions, classification-aligned controls, and approved processes for restoring information.

c) **(319 401/REQ-7.11.2-03X)**: The TSP shall perform integrity check on the backup copies.

Stø AS performs integrity checks on backup on a regular basis.

d) **(319 401/REQ-7.11.2-04X)**: The TSP shall test at planed (sic) intervals the recovery of backup copies and redundancies and shall take corrective actions in case of findings. The results of these tests shall be documented.

Stø AS tests the recovery of backup copies and redundancies at planned intervals, at minimum yearly, documents the results, and implements corrective actions whenever findings are identified.

3.11.3 Crisis management

a) **(319 401/REQ-7.11.3.-01X)**: The TSP shall establish processes for crisis management addressing at least:
   a. roles and responsibilities in crisis situations;
   b. mandatory and voluntary communications between the TSP and relevant competent authorities, and
   c. appropriate controls for maintaining network and information security in crisis situations.

Stø AS has processes in place for crisis management, including definition of roles and responsibilities, mandatory and voluntary communications between Stø and relevant competent authorities, and appropriate controls for maintaining network information security in accordance with the company-wide business continuity plan.

b) **(319 401/REQ-7.11.3-02X)**: The TSP shall implement a process for managing and making use of information received from National CSIRT or, where applicable, competent authorities useful for crisis management.

Stø AS maintains a process for handling information received from the National CSIRT and relevant authorities, with threat-intelligence updates regularly received by the SOC team and communicated to the CISO who holds a seat on the Crisis Management Board to support informed crisis-management decisions.

c) **(319 401/REQ-7.11.3-03X)**: The TSP shall test and review, at planned intervals or in the post-incident review process, its crisis management plan.

Stø AS performs yearly reviews of its crisis management plan in conformance with the company-wide business continuity plan.

3.12 Termination and termination plans

a) **(119 461/OVR-7.12-01)**: The requirements specified in ETSI EN 319 401 [1], clause 7.12, excluding REQ-7.12-11, shall apply.

See below. In accordance with The Service’s termination plan.

b) **(119 401/REQ-7.12-01)**: Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the TSP's services, and in particular continued maintenance of information required to verify the correctness of trust services shall be provided.

See [9] section 4.12 letter a). In addition:

The Service will supply relying QTSPs with evidence of applicable identity proofing processes that are obtained under the obligations set out in ETSI TS 119 461 section 8.5.2.

c) **(119 401/REQ-7.12-02)**: The TSP shall have an up-to-date termination plan.

See [9] section 4.12 letter b).

d) **(119 401/REQ-7.12-03)**: Before the TSP terminates its services, the TSP shall inform the following of the termination: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties, TSPs and relevant authorities such as supervisory bodies.

See [9] section 4.12 letter c). In addition:

This includes:

- All of The Service's relying QTSPs
- The Service's conformance assessment body

e) **(119 401/REQ-7.12-04)**: Before the TSP terminates its services, the TSP shall make the information of the termination available to other relying parties.

See [9] section 4.12 letter d).

f) **(119 401/REQ-7.12-05)**: Before the TSP terminates its services, the TSP shall terminate authorization of all subcontractors to act on behalf of the TSP in carrying out any functions relating to the process of issuing trust service tokens.

See [9] section 4.12 letter e).

g) **(119 401/REQ-7.12-06)**: Before the TSP terminates its services, the TSP shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period, unless it can be demonstrated that the TSP does not hold any such information.

See [9] section 4.12 letter f).

h) **(119 401/REQ-7.12-07)**: Before the TSP terminates its services, the TSP's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.

See [9] section 4.12 letter g).

i) **(119 401/REQ-7.12-08)**: Before the TSP terminates its services, where possible TSP should make arrangements to transfer provision of trust services for its existing customers to another TSP.

The Service, where possible, will supply relying QTSPs with evidence of applicable identity proofing processes that are retained under the obligations set out in ETSI TS 119 461 section 8.5.2.

j) **(119 401/REQ-7.12-09)**: The TSP shall have an arrangement to cover the costs to fulfil these minimum requirements in case the TSP becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

Stø AS has in place a combination of funds and insurance arrangements covering potential damage reflected in the applicable Subject/Signer terms and conditions.

Funds are set aside to cover the cost of a termination, including continued storage of mandatory data.

k) **(119 401/REQ-7.12-10)**: The TSP shall state in its practices the provisions made for termination of service. This shall include:
    a. notification of affected entities; and
    b. where applicable, transferring the TSP's obligations to other parties.

See [9] section 4.12 letter j). In addition:

The Service will supply relying QTSPs with evidence of applicable identity proofing processes that are retained under the obligations set out in ETSI TS 119 461 section 8.5.2.

l) **(119 401/REQ-7.12-11)**: The TSP shall maintain or transfer to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period.

See [9] section 4.12 letter k).

3.13 Compliance

a) **(119 461/OVR-7.13-01)**: The requirements specified in ETSI EN 319 401 [1], clause 7.13 shall apply.

See below.

b) **(119 401/REQ-7.13-01)**: The TSP shall ensure that it operates in a legal and trustworthy manner.

See [9] section 4.13 letter a).

c) **(119 401/REQ-7.13-02)**: The TSP shall provide evidence on how it meets the applicable legal requirements.

See [9] section 4.13 letter b).

d) **(119 401/REQ-7.13-03)**: Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities, where feasible.

Stø AS maintains conformation with WCAG AA accessibility guidelines for its mobile application ensuring availability to persons with disabilities.

e) **(119 401/REQ-7.13-04)**: Applicable standards on accessibility such as ETSI EN 301 549 [i.6] should be taken into account.

See [9] section 4.13 letter d).

f) **(119 401/REQ-7.13-05)**: Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

See [9] section 4.13 letter e).

3.14 Supply chain

a) **(119 461/OVR-7.14-01)**: The requirements specified in ETSI EN 319 401 [1], clause 7.14 shall apply.

See sections 3.14.1, 3.14.2, 3.14.3 of the present document.

3.14.1 Supply chain policy

a) **(119 401/REQ-7.14-01X)**: The TSP shall identify and implement processes and procedures to address security risks associated with the use products and services provided by suppliers, including the ICT supply chain.

Stø AS identifies and implements processes and procedures to address security risks associated with supplier-provided products and services, including the ICT supply chain, through the organization's vendor-selection procurement process, associated policies and ISMS-aligned vendor and risk assessments.

b) **(119 401/REQ-7.14-02X)**: The TSP shall define, document and implement processes and procedures to manage the information security risks associated with the use of supplier's products or services.

Stø AS defines and documents processes and procedures to manage the information security risks associated with suppliers in the ISMS-aligned vendor and risk assessments and associated procurement policy documents.

c) **(119 401/REQ-7.14-03X)**: The supply chain policy shall identify and communicate the TSP's role in the supply chain.

Stø AS identifies and communicates its role in the supply chain through clearly defined responsibilities embedded in supplier and vendor contracts, ensuring all parties understand their obligations in the delivery chain.

d) **(119 401/REQ-7.14-04X)**: The supply chain policy shall define criteria for selecting and contracting suppliers or service providers. Criteria shall include:
   a. the ability of the supplier or service provider to meet the cybersecurity specifications, risks and classification levels of the TSP's services, systems or products delivered by the supplier or service provider;
   b. the ability of the TSP to diversify sources of supply and to limit vendor lock-in; and
   c. the results of the coordinated security risk assessments of critical supply chains.

Stø AS defines supplier selection and outsourcing criteria that ensure providers can meet the cybersecurity, risk and classification requirements of our services, support diversification to reduce vendor lock-in, covered through the tech strategy and the Procurement and Outsourcing Policy which incorporates coordinated supply-chain risk assessments and ongoing vendor evaluation into the overall vendor-risk-assessment process.

3.14.2 Supply chain procedures and processes

a) **(119 401/REQ-7.14.2-01X)**: Processes and procedures shall be defined and implemented to manage information security risks associated with the information and communication technologies products and services supply chain.

Stø AS identifies and implements processes and procedures to address information security risks associated with supplier-provided products and services, through the organization's vendor-selection procurement process, associated policies and ISMS-aligned vendor and risk assessments. Supported by Stø's ISMS "Standard for Leverandørstyring" and in "Rutine for Utvidet Leverandørstyring"

b) **(119 401/REQ-7.14.2-02X)**: TSP shall define information security requirements to apply to ICT product or service acquisition.

Stø AS has a defined set of information security requirements for ICT product and service acquisition in the internal ISMS security policy, this security policy is made available to suppliers.

c) **(119 401/REQ-7.14.2-03X)**: TSP shall require that ICT services suppliers propagate the TSP's security requirements throughout the supply chain if they sub-contract for parts of the ICT service provided to the TSP.

Stø AS requires that suppliers must propagate the security requirements as defined in the ISMS security policy throughout the supply chain wherever sub-contracted services are in place. Supported by ISMS policy as with 3.14.2 a)

d) **(119 401/REQ-7.14.2-04X)**: TSP shall require that ICT products suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased or acquired from other suppliers or other entities.

Stø AS requires that suppliers must propagate the security requirements as defined in the ISMS security policy to any components purchased or acquired from other suppliers or entities. Supported by ISMS policy as with 3.14.2 a)

e) **(119 401/REQ-7.14.2-05X)**: TSP shall request that ICT products suppliers provide information describing the software components used in products.

Stø AS requires that all ICT product suppliers provide up-to-date and accurate documentation describing the software components used in the supplied products, as mandated in the Technical Application Control requirements and contractually required as part of supplier agreements.

f) **(119 401/REQ-7.14.2-06X)**: TSP shall request that ICT products suppliers provide information describing the implemented security functions of their product and the configuration required for its secure operation.

Stø AS requires that all ICT product suppliers provide up-to-date and accurate documentation describing to the security functions of their product including best practice and secure integration guidelines relating to the product, as mandated in the Technical Application Control requirements and contractually required as part of the supplier agreements.

g) **(119 401/REQ-7.14.2-07X)**: TSP shall implement a monitoring process and acceptable methods for validating ICT products and services conform to stated cybersecurity requirements.

Stø AS ensures that regular operational meetings are held with suppliers and places clear requirements on them to meet their obligations, risk assessments, certifications and other agreed relevant activities as part of the supplier agreements. Supported by ISMS policy as with 3.14.2 a)

h) **(119 401/REQ-7.14.2-08X)**: TSP shall implement a process for identifying and documenting product or service components that are critical for maintaining functionality.

Stø AS identifies and documents product and service components critical to maintaining functionality through the service-classification process, the onboarding process to Command Center and the ISMS Secure Software Development Lifecycle (SSDLC), ensuring that critical dependencies are understood, tracked and protected.

i) **(119 401/REQ-7.14.2-09X)**: TSP shall obtain assurance that critical components and their origin can be traced throughout the supply chain.

Stø AS places requirements on suppliers that they have full control over their supply chain and origins as part of the supplier agreements.

j) **(119 401/REQ-7.14.2-10X)**: TSP shall obtain assurance that the delivered ICT products are functioning as expected without any unexpected or unwanted features.

Stø AS places requirements on suppliers that their products are tested to ensure they meet expected quality and functionality requirements without unexpected or unwanted features; this is further verified by ensuring all changes first go through change control procedures and testing in test environments before being released to production environments.

k) **(119 401/REQ-7.14.2-11X)**: TSP shall implement processes to ensure that components from suppliers are genuine and unaltered from their specification.

Stø AS requires that software is obtained only from officially agreed distribution channels.

l) **(119 401/REQ-7.14.2-12X)**: TSP shall define rules for sharing of information regarding the supply chain and any potential issues and compromises among the TSP and its suppliers.

Stø AS defines rules for sharing supply chain related information and any identified issues or compromises with suppliers, ensuring that all such exchanges follow the ISMS Information Classification and Handling Standard to guarantee secure and appropriate communication.

m) **(119 401/REQ-7.14.2-13X)**: TSP shall implement specific processes for managing ICT component life cycle and availability and associated security risks.

The Service defines its own Lifecycle Management (LCM) process relating to The Service's applicable assets defined in the asset registry.

n) **(119 401/REQ-7.14.2-14X)**: TSP shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

Stø AS ensures that regular operational meetings are held with suppliers and places clear requirements on suppliers to raise any changes to information security practices and service delivery. Any relevant module certifications of subcontractors are monitored to ensure ongoing and uninterrupted certification is in place.

o) **(119 401/REQ-7.14.2-15X)**: The TSP shall define, implement and communicate to all relevant interested parties topic-specific policies on the use of cloud services and on how the TSP intends to manage information security risks associated with them.

Stø AS maintains an Interested Parties and Compliance Requirements policy and recognises its shared obligations in relation to managing information security risks in collaboration with cloud service providers.

3.14.3 Responsibility, third parties agreements and SLA

a) **(119 401/REQ-7.14.3-01X)** [CONDITIONAL]: When the TSP makes use of other parties, including trust service component providers, to provide parts of its service through subcontracting, outsourcing or other third party arrangements, it shall maintain overall responsibility for conformance with the supply chain policy, its information security policy and the requirements defined in the trust service policy.

When Stø AS uses third parties, including trust-service component providers, to deliver parts of its service, it maintains full responsibility for meeting all trust-service, security and compliance requirements by selecting suppliers based on strict criteria such as relevant ETSI certification, and where such certification is not held the trust-service component provider will be audited as part of our service.

b) **(119 401/REQ-7.14.3-02X)**: The TSP shall define the outsourcers' liability and ensure that outsourcers are bound to implement any controls required by the TSP.

Stø AS defines the suppliers' liability and ensures outsourcers are bound to implement any controls required in supplier agreements.

c) **(119 401/REQ-7.14.3-03X)**: These processes and procedures shall include:
   a. those to be implemented by the TSP;
   b. those the TSP requires the supplier to implement for the commencement of use of a supplier's products or services; and
   c. those the TSP requires the supplier to implement for the termination of use of a supplier's products and services.

Stø AS ensures that supplier agreements cover processes and procedures that must be implemented by The Service, those required to implement for the commencement of use of the product or service, and for the termination of the use of the products or services.

d) **(119 401/REQ-7.14.3-04X)**: The TSP shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements to ensure that there is clear understanding between the TSP and the supplier regarding both parties' obligations to fulfil relevant information security requirements.

Stø AS ensures that supplier agreements, where applicable, include documented agreements and contractual relationships where the provisioning of service involves subcontracting, outsourcing, or other third party arrangements; this covers both parties' obligations to fulfil relevant information security requirements.

e) **(119 401/REQ-7.14.3-05X)** [CONDITIONAL]: When the TSP makes use of a trust service component provided by another party it shall ensure that the use of the component interface meets the requirements as specified by the trust service component provider.

Stø AS ensures that all component interface integration requirements as documented by the supplier are met.

f) **(119 401/REQ-7.14.3-06X)** [CONDITIONAL]: When the TSP makes use of a trust service component provided by another party it shall ensure that the security and functionality required by the trust service component meet the appropriate requirements of the applicable policy and practices.

Stø AS ensures that when trust-service components are provided by third parties, their security and functionality meet all applicable policy and practice requirements by verifying that the supplier's ETSI or other relevant certifications are valid, or where such certifications are not held by conducting dedicated audits as part of our trust-service oversight.

g) **(119 401/REQ-7.14.3-07X)**: The TSP shall include in their services agreements "Service level agreements" and/or auditing mechanisms ensuring that direct suppliers and service providers, including cloud computing providers, take appropriate security measures addressing the TSP's security requirements aligned with the TSP's risk assessment.

Stø AS includes service-level agreements and auditing mechanisms where applicable in service contracts to ensure that direct suppliers and service providers, including cloud providers, implement appropriate security measures aligned with Stø AS's security requirements and risk assessments.

h) **(119 401/REQ-7.14.3-08X)**: Compliance with TSPs security policies and requirements shall be considered in the selection process of any direct supplier or service provider as part of the procurement process.

Stø AS' Procurement and Outsourcing Policy ensures that security polices and requirements as set out in the relevant ISMS polices are considered in the selection process of any direct supplier or service provider.

i) **(119 401/REQ-7.14.3-09X)**: Applicable TSPs security policies and requirements and (sic) shall be included in contracts with direct suppliers or service providers.

Stø AS ensures applicable security policies and requirements are included in supplier contracts and agreements.

j) **(119 401/REQ-7.14.3-10X)**: The TSP shall review the supply chain policy and monitor, review, evaluate and manage changes in the cybersecurity practices of direct suppliers or service providers at planned intervals or after an incident related to the provision of services from direct suppliers or service providers.

Stø AS ensures that regular operational meetings are held with suppliers and places clear requirements on suppliers to raise any changes to supply chain policy and cybersecurity practices. Suppliers must alert us of any incidents related to the provision of the services as set out in contractual agreements.

k) **(119 401/REQ-7.14.3-11X)**: The TSP shall establish and maintain a register of suppliers and their agreements to track where the TSP information is managed and/or archived.

Stø AS maintains a register of suppliers and their agreements through its centralised contract-management system, enabling full tracking of where Stø AS information is managed and/or archived.

l) **(119 401/REQ-7.14.3-12X)**: The TSP shall regularly review, validate and update its registry of suppliers and their agreements to ensure that they are still valid, fit for purpose, and include the relevant information security clauses.

Stø AS regularly reviews, validates and updates its registry of suppliers and their agreements to ensure they remain valid, fit for purpose and include the required information-security clauses, supported by the central contract-management system where each contract has an assigned responsible employee and designated signatory.

4 Identity proofing service requirements

4.1 Initiation

a) **(119 461/INI-8.1-01X)**: The applicant shall be informed of, and shall actively accept before the identity proofing process is started, the purpose of the identity proofing and the related terms and conditions as required by the identity proofing context.

Stø AS identity proofing service agreements oblige TSPs to inform applicants and obtain active acceptance of the identity proofing purpose, and terms and conditions before the proofing process is started as required by the identity proofing context.

b) **(119 461/INI-8.1-02X)**: If alternative identity proofing processes are available to achieve the purpose of the identity proofing, the applicant should be allowed to select which of the alternative processes to use.

Stø AS identity proofing service does not offer any alternative identity proofing processes.

c) **(119 461/INI-8.1-03X)**: The applicant shall receive clear guidance regarding how the identity proofing process will be carried out, regarding the identity information that will be collected, regarding what data is kept and for how long, regarding the evidence that the applicant is required to present, and regarding any tool that the applicant is required to use.

The Service provides a user friendly software application to perform the identity proofing process. The applicant is provided with clear guidance of how the process will be carried out with automated guidance and instructions. The applicant is required to agree to the identity information that will be collected, how it is kept and for how long in the privacy statement presented to the applicant.

d) **(119 461/INI-8.1-04)**: The identity proofing process, or at least one process if alternative processes are available, shall be available to persons with disabilities in accordance with the applicable legislation

Stø AS maintains conformation with WCAG AA accessibility guidelines for its mobile application ensuring availability to persons with disabilities.

4.2 Attribute and evidence collection

4.2.1 General requirements

a) **(119 461/COL-8.2.1-01X)**: Mandatory and optional identity attributes to collect shall be defined for each identity proofing context.

All supported identity proofing contexts define both mandatory and optional identity attributes to be collected.

b) **(119 461/COL-8.2.1-01A)**: All mandatory attributes for a specific identity proofing context shall be collected.

The Service requires that all mandatory identity attributes are collected; if mandatory identity attributes cannot be collected, the identity proofing process fails.

c) **(119 461/COL-8.2.1-02)**: The identity attributes collected shall provide unique identification of the applicant for the identity proofing context.

The Service provides unique identification of the applicant for the identity proofing context.

d) **(119 461/COL-8.2.1-03X)**: The identity attributes collected shall be validated by use of one or more authoritative evidence and optionally one or more supplementary evidence.

The Service collects and validates identity attributes from digital identity documents as the source of authoritative evidence. Evidence validation is carried out in accordance with ETSI 119 461 [7] Section 8.3.2

e) **(119 461/COL-8.2.1-04)**: The evidence collected shall meet the requirements of the identity proofing context.

The Service validates collected evidence meets the requirements of the identity proofing context.

f) **(119 461/COL-8.2.1-05)**: The evidence shall be issued by entities trusted in the identity proofing context.

Each identity proofing context declares trusted issuers. If the evidence does not meet the requirements it is rejected and the proofing session is ended.

g) **(119 461/COL-8.2.1-06X)**: The identity proofing practice statement shall identify a list of the identity proofing use cases supported, the authoritative and optionally supplementary evidence that shall be trusted, and, as far as possible, the identity proofing contexts supported.

The list of supported use cases can be found in section 2.1 of the present document.

The Service supports digital identity documents as the authoritative source of evidence.

The Service supports identity proofing contexts relating to:

- Identity proofing
- Identity proofing for qualified and non-qualified TSPs

Each identity proofing context can be customised during the initiation phase by making use of the OIDC4IA compliant interface exposed by The Service.

h) **(119 461/COL-8.2.1-07)**: The freshness of the identity attributes obtained from evidence shall be evaluated against the freshness requirements of the identity proofing context.

Each identity proofing context asserts requirements against issue date or expiry date (as available) to ensure freshness requirements that meet the context's needs. If the evidence does not meet the requirements of the context it is rejected, and the proofing session is ended.

4.2.2 Attribute collection

4.2.2.1 Attribute collection for natural person

[CONDITIONAL] If the applicant is a natural person, the requirements in the present clause apply.

a) **(119 461/COL-8.2.2.1-01X)**: The identity proofing practice statement shall identify for each identity proofing context supported, the means used to collect identity attributes for a natural person.

All supported identity proofing contexts collect identity attributes for a natural person from digital identity documents.

b) **(119 461/COL-8.2.2.1-02)**: The following attributes shall at a minimum be collected if the applicant is a natural person:
   a) family name(s), first name(s), which should be current names;
   b) further information as needed to uniquely identify the applicant as a natural person in the identity proofing context.

The Service ensures that family name(s), first name(s), and further information to uniquely identify an applicant are collected from the digital identity document in accordance with requirement COL-8.2.1-02

c) **(119 461/COL-8.2.2.1-02A)**: The outcome of the identity proofing process may be a pseudonymous identity.

The Service does not support pseudonymous identities.

d) **(119 461/COL-8.2.2.1-03)**: The attributes to collect shall be as determined by the identity proofing context.

The Service allows per identity proofing context declaration of required attributes allowing attribute collection to be determined by the identity proofing context.

e) **(119 461/COL-8.2.2.1-04)**: The identity proofing process shall not collect identity attributes that are not included in the result of the identity proofing, except when such attributes are required for attribute and evidence validation and/or binding to applicant.

The Service only collects attributes that are returned in the identity proofing result except where required for the validation and binding to applicants.

4.2.2.2 Attribute collection for legal person

[CONDITIONAL] If the applicant is a legal person, the requirements in the present clause apply.

The Service does not support attribute collection for legal persons.

4.2.2.3 Attribute collection for natural person representing legal person

[CONDITIONAL] If the applicant is a natural person representing a legal person, the requirements in the present clause apply.

The Service does not support attribute collection for natural persons representing legal persons.

4.2.3 Use of physical or digital identity document evidence

[CONDITIONAL] If physical and/or digital identity documents are used as evidence, the requirements in the present clause apply.

a) **(119 461/COL-8.2.3-01X)**: An identity document used as evidence shall be in physical or digital form.

The Service requires the use of digital identity documents for identity attribute collection.

b) **(119 461/COL-8.2.3-02X)**: A document used as authoritative evidence shall contain a face photo and/or other information that can be used to uniquely identify the applicant when compared with the applicant's physical appearance.

The Service only support digital identity documents which contain a face photo.

c) **(119 461/COL-8.2.3-03X)**: For each identity proofing context supported, a list of the identity documents that are accepted shall be identified by the identity proofing practice statement.

The Service supports reading of digital identity documents by way of NFC with supported documents containing NFC chips and compliant implementations of the specification set out in ICAO 9303 part 10 [4].

d) **(119 461/COL-8.2.3-04X)** [CONDITIONAL]: If physical identity documents are used as authoritative evidence, only passports, national identity cards and other official identity documents that according to the identity proofing context offer the same or higher reliability of the identity shall be accepted, where the judgement on comparable reliability shall be based on an assessment of the security features and issuance process of the other identity document towards the security features and issuance process of passport and/or identity card.

Not applicable. Physical identity documents are not supported as authoritative evidence.

e) **(119 461/COL-8.2.3-05X)** [CONDITIONAL]: If a physical identity document is used as evidence, the IPSP shall verify that the document is presented in its original form.

Not applicable. Physical identity documents are not supported as evidence.

f) **(119 461/COL-8.2.3-06X)** [CONDITIONAL]: If digital identity documents are used as authoritative evidence, only eMRTD digital identity documents according to ICAO 9303 part 10 [4] and other digital documents that according to the identity proofing context offer the same or higher reliability of the identity shall be accepted, where the judgement on comparable reliability shall be based on an assessment of the security features and issuance process of the other identity document towards the security features and issuance process required by ICAO 9303 part 10 [4].

The Service only supports eMRTD digital identity documents according to ICAO 9303 part 10 [4] and other digital documents that offer the same or higher reliability of the identity.

g) **(119 461/COL-8.2.3-07)** [CONDITIONAL]: If required attributes to be collected cannot be validated by the identity document, these attributes shall be collected from other sources and validated, including assessing that the attributes are bound to the applicant, by use of other authoritative sources in accordance with the identity proofing context.

If The Service is unable to collect required attributes from the identity document, the identity proofing process will result in failed identity proofing.

4.2.4 Use of existing eID means as evidence

[CONDITIONAL] If existing eID means for authentication is used as evidence, the requirements in the present clause apply.

The Service does not support use of eID means as evidence.

4.2.5 Use of existing digital signature means as evidence

[CONDITIONAL] If an existing digital signature means with a supporting certificate is used as evidence, the requirements in the present clause apply.

The Service does not support use of existing digital signature means as evidence.

4.2.6 Use of trusted register as supplementary evidence

[CONDITIONAL] If a trusted register is used as supplementary evidence, the requirements in the present clause apply.

The Service does not support use of trusted register as supplementary evidence.

4.2.7 Use of proof of access as supplementary evidence

[CONDITIONAL] If proof of access is used as supplementary evidence, the requirements in the present clause apply.

The Service does not support proof of access as supplementary evidence.

4.2.8 Use of documents and attestations as supplementary evidence

[CONDITIONAL] If documents and attestations are used as supplementary evidence, the requirements in the present clause apply.

The Service does not support use of documents and attestations as supplementary evidence.

4.2.9 Evidence collection for natural person representing legal person

[CONDITIONAL] If the applicant is a natural person purporting to represent a legal person, the requirements in the present clause apply.

The Service does not support evidence collection for natural person representing legal person.

4.3 Attribute and evidence validation

4.3.1 General requirements

a) **(119 461/VAL-8.3.1-01X)**: All necessary identity attributes shall be validated to the required reliability by an authoritative source.

The Service validates all necessary identity attributes and evidence collected from the digital identity document using the document's cryptographic signature and hash-tables in accordance with requirement VAL-8.3.2-00.

b) **(119 461/VAL-8.3.1-02)**: Evidence of the identity proofing process shall be collected and secured supporting requirements in clause 8.5.2 of the present document.

The Service logs and stores evidence of the identity proofing process in an anonymised fashion.

c) **(119 461/VAL-8.3.1-03X)**: The handling of differences in encoding of identity attributes between different evidence or between evidence and attributes collected from other sources than evidence shall be specified in the practice statement.

The Service provides the identity attributes as-is.

Digital identity documents may impose constraints on the character set, length and format of names – this may sometimes result in truncation of attributes. These are aligned with relevant standards and are provided "as-is" in identity attributes for the applicant.

d) **(119 461/VAL-8.3.1-04X)**: The handling of differences in name attributes between different evidence or between evidence and attributes collected from other sources than evidence shall be specified in the practice statement.

The Service does not use other sources of evidence than the provided digital identity document; as such no differences between sources is handled.

e) **(119 461/VAL-8.3.1-05)**: The identity proofing process shall verify that the evidence is of a type accepted according to the identity proofing context.

The Service allows for identity proofing contexts to define specific evidence criteria (eg: document types, issuers, etc). Evidence is evaluated against these rules and the identity proofing session is closed if the presented evidence is not acceptable according to the identity proofing context.

f) **(119 461/VAL-8.3.1-06X)**: The identity proofing process shall verify that the issuer of evidence is trusted according to the identity proofing context.

See section 4.3.1 e) of the present document; The Service also maintains a trust list for signing certificates of digital identity document issuers and only documents with trusted root certificates are accepted by the system; the identity proofing context can further narrow these trusted issuers.

g) **(119 461/VAL-8.3.1-07)** [CONDITIONAL]: If the evidence has an explicit validity period, the identity proofing process shall verify that the time of the identity proofing is within this validity period.

The Service evaluates the validity period both by assessing the validity period of the signing certificate and the stated issue and/or expiry date of the authoritative evidence where provided; the identity proofing context can further narrow these requirements.

h) **(119 461/VAL-8.3.1-08X)**: The identity proofing process shall verify the authenticity and integrity of the evidence, i.e. that the evidence is genuine and presented in its original form.

The Service verifies the authenticity and integrity of the evidence, specifically digital identity documents, by using various security features of the document. See section 4.3.1 i) of the present document.

i) **(119 461/VAL-8.3.1-10X)**: The IPSP shall for all accepted evidence document the security features that are to be verified.

The Service makes use of security features made available by digital identity documents when validating and accepting evidence. Various security features are checked where practically available including Passive Authentication and Active Authentication.

j) **(119 461/VAL-8.3.1-11X)**: The identity proofing process shall whenever practically possible verify that the evidence is valid at the time of the identity proofing.

See section 4.3.2 d) of the present document.

k) **(119 461/VAL-8.3.1-12)**: Validation of evidence shall be done in an environment controlled by the actor responsible for the identity proofing process.

The Service controls the environment in which evidence is validated; in that the evidence is validated by servers under control of The Service and does not rely on client applications to perform validation checks.

4.3.2 Validation of digital identity document

[CONDITIONAL] If a digital identity document is used as authoritative evidence, the requirements in the present clause apply.

a) **(119 461/VAL-8.3.2-00)**: Successful validation of a digital identity document shall imply that the identity document as evidence is validated and that the identity attributes conveyed from the identity document are validated.

The Service uses validation of the digital identity document as implied validation of the document as evidence and validation of the identity attributes conveyed from the identity document.

b) **(119 461/VAL-8.3.2-01)** [CONDITIONAL]: If the digital identity document is used in a remote identity proofing process, the data from the identity document shall be transferred to an environment controlled by the actor responsible for the identity proofing process in a manner that ensures authenticity, integrity, and confidentiality of the document content.

The Service transfers data from the identity document to the environment controlled by the Service by means of TLS 1.2 or newer ensuring the authenticity, integrity and confidentiality of the data.

c) **(119 461/VAL-8.3.2-02)**: The digital identity document shall only be accepted if the issuer's digital signature on the document is successfully validated.

The Service only accepts digital identity documents where the issuer’s digital signature on the document is successfully validated.

d) **(119 461/VAL-8.3.2-03)** [CONDITIONAL]: If an online status service to confirm the document's validity exists and is practically available, the process shall use this service to verify that the document is currently valid.

The Service integrates with issuers’ online status services where practically available. Where the Service is unable to obtain a result or does not have an integration, the TSP must verify whenever practical the evidence is valid at the time of the identity proofing.

e) **(119 461/VAL-8.3.2-04X)** [CONDITIONAL]: If the digital identity document is required to be read from a chip embedded in a physical identity document, the identity proofing process shall protect against injection into the process, by the applicant or an external attacker, of a copy of a digital identity document that has previously been obtained and stored by the attacker.

The Service protects against injection into the process by the applicant or an external attacker of a copy of the digital identity document that has previously been obtained by requiring applicants to use software that is approved for the identity proofing process; namely a smartphone application. Protections are also put in place as per 4.3.1 i) of the present document.

f) **(119 461/VAL-8.3.2-04A)** [CONDITIONAL]: If the digital identity document is required to be read from a chip embedded in a physical identity document, in case of an interruption of the identity proofing process for any reason (e.g. loosing internet connection), if the identity proofing process is resumed, the identity document shall be reread from the chip.

The Service does not allow applicants to resume interrupted identity proofing sessions; applicants must restart the identity proofing process and represent their digital identity document to be able to successfully complete an identity proofing process.

g) **(119 461/VAL-8.3.2-05)**: Information obtained from the digital identity document shall be recorded as needed for binding to applicant and to evidence the identity proofing process.

The Service records information from the identity document as needed to for binding to the applicant and for evidence of the identity proofing process. This typically includes document issuer, validity period and document numbers.

h) **(119 461/VAL-8.3.2-06)**: The face photo contained in the digital identity document shall be extracted to enable binding to applicant.

The Service extracts the photo contained in the digital identity document to enable binding to the applicant for use in automated biometric verification.

4.3.3 Validation of physical identity document

[CONDITIONAL] If a physical identity document is used as authoritative evidence, the requirements in the present clause apply.

The Service does not support use of a physical identity document as authoritative evidence.

4.3.4 Validation of eID means

[CONDITIONAL] If authentication by use of an existing eID means is used as evidence, the requirements in the present clause apply.

The Service does not support authentication by use of an existing eID means as evidence.

4.3.5 Validation of digital signature with certificate

[CONDITIONAL] If a digital signature with certificate is used as evidence, the requirements in the present clause apply.

The Service does not support use of a digital signature with certificate as evidence.

4.3.6 Validation of trusted registers

[CONDITIONAL] If a trusted register is used as supplementary evidence in an identity proofing process, the requirements in the present clause apply.

The Service does not support use of trusted registers.

4.3.7 Validation of proof of access

[CONDITIONAL] If proof of access is used as supplementary evidence in an identity proofing process, the requirements in the present clause apply.

The Service does not support use of proof of access as supplementary evidence.

4.3.8 Validation of documents and attestations

[CONDITIONAL] If documents and attestations are used as supplementary evidence in an identity proofing process, the requirements in the present clause apply.

The Service does not support use of documents and attestations as supplementary evidence.

4.4 Binding to applicant

4.4.1 General requirements

a) **(119 461/BIN-8.4.1-01X)**: The identity proofing process shall verify that the applicant is the legitimate holder of the authoritative evidence.

The Service ensures that the applicant is the legitimate holder of the evidence by means of biometric face matching of the applicant to the trusted reference image extracted from the digital identity document's embedded chip which has been validated as per section 4.3.

b) **(119 461/BIN-8.4.1-02X)**: The identity proofing process shall verify that the authoritative evidence is in the possession of the applicant.

The Service verifies the authoritative evidence is in the possession of the applicant by requiring the evidence is validated at the time of the identity proofing.

The evidence is also bound to the applicant by biometric identification means as per Section 4.4.1 a) of the present document.

4.4.2 Capture of face image of the applicant

[CONDITIONAL] If the applicant is a natural person, and an identity document is used as evidence, and the identity proofing process is carried out remotely, the following requirements apply.

a) **(119 461/BIN-8.4.2-01)**: A video stream of the applicant's face shall be captured.

The Service captures a video stream of the applicant's face.

b) **(119 461/BIN-8.4.2-01A)**: The video recording shall use frame rate and resolution of sufficient quality for the identity proofing process.

The Service captures a video stream is captured with frame rate and resolution at sufficient quality for the identity proofing process.

c) **(119 461/BIN-8.4.2-02X)**: The video capture process shall apply presentation attack detection means to ensure that the video stream is of a live person present in front of the camera at the time of the identity proofing.

The Service applies passive presentation attack detection methods by way of capturing skin reflections from the use of random light patterns to ensure that the video stream is of a live person present in front of the camera at the time of identity proofing.

d) **(119 461/BIN-8.4.2-02A)**: The video capture process shall happen at the time of the identity proofing.

The Service ensures the video capture process happens at the time of the identity proofing by way of capturing skin reflections from the use of random light patterns.

e) **(119 461/BIN-8.4.2-03X)**: The video stream capture shall apply means to detect artificially generated or manipulated face appearance.

The Service's biometric verification service is FIDO certified against attacks using artificially generated or manipulated face images.

f) **(119 461/BIN-8.4.2-04)** [CONDITIONAL]: If the video stream is captured on the applicant's device, the identity proofing process shall ensure that the video stream is transmitted to an environment controlled by the actor responsible for the identity proofing process in a manner that ensures authenticity, integrity, and confidentiality of the video stream.

The Service transfers the video stream to the environment controlled by The Service by means of TLS 1.3 or newer ensuring the authenticity, integrity and confidentiality of the data.

g) **(119 461/BIN-8.4.2-04A)**: The identity proofing process shall apply biometric injection attack prevention and detection means to ensure that neither the applicant nor an external attacker can undetectably inject into the process a previously recorded or artificially generated video stream

The Service applies biometric injection attack prevention and detection by mandating the use of the approved software application to perform the identity verification process. The integrity of the software application is controlled by the necessary means corresponding to the latest threat intelligence information.

h) **(119 461/BIN-8.4.2-04B)** [CONDITIONAL]: If the identity proofing targets Baseline LoIP, the biometric injection attack detection means shall be tested by an accredited laboratory according to TS 18099 [5] level Substantial (level 2) at the latest before the end of 2026.

Not applicable; The Service does not target Baseline LoIP.

i) **(119 461/BIN-8.4.2-04C)** [CONDITIONAL]: If the identity proofing targets Extended LoIP, the biometric injection attack detection means shall be tested by an accredited laboratory according to TS 18099 [5] level High (level 3) at the latest before the end of 2026.

The Service’s biometric verification provider is FIDO certified by an accredited laboratory according to TS 18099 level High (level 3).

j) **(119 461/BIN-8.4.2-04D)**: Evaluation of biometric injection detection means by an accredited laboratory according to TS 18099 [5] shall be repeated at least every second year.

The Service’s biometric verification service has evaluation of biometric injection detection means by an accredited laboratory according to TS 18099 [5] is repeated at least every second year.

k) **(119 461/BIN-8.4.2-05X)** [CONDITIONAL]: If face biometrics is used for binding to applicant, at least one image of sufficient quality for binding to applicant shall be captured integral to the video capturing or be extracted from the video stream.

The Service captures at least one image of sufficient quality for binding to the applicant is captured during the binding process.

l) **(119 461/BIN-8.4.2-05A)** [CONDITIONAL]: If face biometrics is used for binding to applicant, and a face image of the applicant is captured in the process, the face image shall have a resolution of sufficient quality for the identity proofing process.

The face image captured of the applicant is of sufficient quality for the identity proofing process.

m) **(119 461/BIN-8.4.2-05B)**: The conditions (e.g. lighting conditions, reflections, sharpness) of video and images shall be assessed, and video and images shall be rejected if they are not suited for binding to applicant, with an instructions to the applicant to repeat the process under better conditions.

If lighting conditions are not suitable, or other issues such as darkened glasses, or no face is found in the video stream, then the applicant must repeat the biometric verification process.

n) **(119 461/BIN-8.4.2-05C)**: There shall be an upper limit on the number of retries before the process is aborted with failed result.

Applicants may not have more than 5 attempts at the binding process, otherwise the identity proofing process is aborted and the session is closed in a failed state.

o) **(119 461/BIN-8.4.2-05D)**: The IPSP shall in its practice statement state goals for APCER (attack presentation classification error rate) and BPCER (bona fide presentation classification error rate) values that are at least at the level of industry best practice and that the service shall aim to achieve.

Test results for the PAD of The Service achieves APCER and BPCER at the level of industry best practice. The Service will keep aiming to achieve this standard.

p) **(119 461/BIN-8.4.2-05E)**: The IPSP shall keep its APCER and BPCER goals updated based on its threats intelligence procedure.

The Service keeps the APCER and BPCER goals up to date.

q) **(119 461/BIN-8.4.2-06X)**: The PAD means and APCER and BPCER rates shall be systematically tested in accordance with ISO/IEC 30107-3 [3] against updated reference data sets and against the goals set by the IPSP.

The video stream capture applies PAD measures in compliance with ISO/IEC 30107-3 [3].

r) **(119 461/BIN-8.4.2-07X)**: The PAD means shall be evaluated by an accredited laboratory according to ISO/IEC 19989-3 [6] at the latest before the end of 2026.

The PAD means will be evaluated by an accredited laboratory according to ISO/IEC 19989-3 [6] before the end of 2026.

s) **(119 461/BIN-8.4.2-07A)**: Evaluation of PAD means by an accredited laboratory according to ISO/IEC 19989-3 [6] shall be repeated at least every second year.

Evaluation of PAD means by an accredited laboratory according to ISO/IEC 19989-3 [6] is repeated at least every second year.

t) **(119 461/BIN-8.4.2-08X)**: Test results for the PAD shall achieve an APCER as defined by ISO/IEC 30107-3 [3] in accordance with the goal stated in the practice statement.

Test results for the PAD achieves an APCER as defined by ISO/IEC 30107-3 [3].

u) **(119 461/BIN-8.4.2-09X)**: Test results for the PAD should achieve BPCER as defined by ISO/IEC 30107-3 [3] in accordance with the goal stated in the practice statement.

Test results for the PAD achieves an BPCER as defined by ISO/IEC 30107-3 [3].

4.4.3 Binding to applicant by automated face biometrics

[CONDITIONAL] If binding to applicant is by automated face biometrics, the following requirements apply.

a) **(119 461/BIN-8.4.3-01X)**: The process shall provide a reliable, automated comparison between face image(s) extracted from the identity document presented by the applicant and face image(s) captured according to the requirements of clause 8.4.2 of the present document.

The Service uses a face matching algorithm that has achieved a FIDO alliance certification for face biometry identification. This program is the premier certification to assess the performance and usability of remote identity verification systems based on facial biometrics. This is done in accordance with all requirements in section 8.4.2 of [7].

b) **(119 461/BIN-8.4.3-02X)**: Data capture and preliminary data quality assessment may be done in equipment controlled by the applicant.

The applicants use with an NFC-enabled device (eg: smartphone) in conjunction with The User Application to perform data capture.

c) **(119 461/BIN-8.4.3-03)**: Biometric signal processing, comparison, data storage, and decision shall be carried out in an environment controlled by the actor responsible for the identity proofing process.

An IPSP subcontractor is contracted to provide these services and are bound by our control contractually and through close cooperation.

d) **(119 461/BIN-8.4.3-05A)**: The IPSP shall in its practice statement state goals for False Acceptance Rate (FAR) and False Rejection Rate (FRR) values that are at least at the level of industry best practice and that the service shall aim to achieve.

The test results for the biometric face recognition show a FAR (false acceptance rate) and FRR (false rejection rate) at the level of industry best practice. The Service will keep aiming to achieve this standard.

e) **(119 461/BIN-8.4.3-05B)**: The IPSP shall keep its FAR and FRR goals updated based on its threats intelligence procedure.

The Service keeps the FAR and FRR goals up to date.

f) **(119 461/BIN-8.4.3-06X)**: The biometric algorithms and technologies applied shall be systematically tested in accordance with ISO/IEC 19795-1 [2] against updated reference data sets and against the goals set by the IPSP.

The biometric algorithms and technologies applied conforms with ISO/IEC 19795-1 [2].

g) **(119 461/BIN-8.4.3-07X)**: Test results for the biometric face recognition shall achieve FAR in accordance with the goal stated in the practice statement.

The test results for the biometric face recognition show a FAR (false acceptance rate) at the level of industry best practice.

h) **(119 461/BIN-8.4.3-08X)**: Test results for the biometric face recognition should achieve False Rejection Rate (FRR) in accordance with the goal stated in the practice statement.

The test results for the biometric face recognition show a FRR (false rejection rate) at the level of industry best practice.

i) **(119 461/BIN-8.4.3-09X)**: The biometric face recognition should apply means to detect morphed photos in identity documents.

The biometric face recognition applies means to detect morphed photos in identity documents.

4.4.4 Binding to applicant by manual face verification

[CONDITIONAL] If manual binding of the applicant to an identity document is used, the following requirements apply.

The Service does not support manual binding of the applicant to an identity document.

4.4.5 Binding to applicant for legal person and natural person representing legal person

[CONDITIONAL] If the applicant is a legal person or a natural person representing a legal person, the following requirements apply.

The Service does not support applicants representing a legal person.

4.5 Issuing of proof

4.5.1 Result of the identity proofing

a) **(119 461/ISS-8.5.1-01)**: The result of the identity proofing shall be delivered securely to the trust service provider, regarding the authenticity, integrity, and confidentiality of the result.

The identity proofing result is sent to the TSP using connections secured with up to date TLS standards and validated with TLS certificates. This guarantees authenticity, integrity and confidentiality of the result. Further, the data delivered to the TSP is signed with our signing certificate allowing for an added layer of trust.

b) **(119 461/ISS-8.5.1-02)**: The result of the identity proofing process shall convey the LoIP achieved by the identity proofing process for the identity attributes required for the unique identification of the applicant in the identity proofing context.

The Service only supports Extended LoIP. The act of sending a success response conveys implicitly that the identity proofing process has reached Extended LoIP.

4.5.2 Evidence of the identity proofing process

In this clause, the term "evidence" means audit information for the identity proofing process as such, and not authoritative or supplementary evidence as in other clauses of the document.

a) **(119 461/ISS-8.5.2-01)**: Evidence of the identity proofing process shall be gathered and retained in compliance with the identity proofing context.

Audit logs are retained as evidence of the process, including information that can be used to validate the identity verification process with re-presentation of the document

b) **(119 461/ISS-8.5.2-02X)**: The evidence of the identity proofing process shall document the authoritative and supplementary evidence used in the identity proofing process and the issuer or source of that evidence.

The document number and the issuer of the authoritative evidence used in the identity proofing process is saved in the evidence of the identity proofing process. The Service does not support use of supplementary evidence.

The document number is stored by way of a non-reversable cryptographic hash, allowing verification of per-session data via zero-knowledge proof. Document issuer is kept without being hashed.

c) **(119 461/ISS-8.5.2-03)**: The evidence of the identity proofing process should completely document the identity proofing process.

The service stores evidence of the complete process, apart from any special categories of PII in accordance with our data privacy statement [8].

d) **(119 461/ISS-8.5.2-04)**: Evidence of the identity proofing process shall be retained for the necessary retention time given by the identity proofing context.

Evidence of the identity proofing process is stored with retention periods defined by the identity proofing context and by the TSP.

e) **(119 461/ISS-8.5.2-05)**: The evidence of the identity proofing process shall be stored in a tamper-proof way.

The integrity of the evidence of the identity proofing process is maintained through encryption, access controls, and tamper-proof storage.

f) **(119 461/ISS-8.5.2-05A)**: The time of completion of the identity proofing process shall be part of the evidence.

The Service stores the completion time of the identity proofing process as a part of the evidence.

g) **(119 461/ISS-8.5.2-06)**: The evidence of the identity proofing process shall be stored in a way that guarantees the confidentiality of the information.

The confidentiality of the evidence of the identity proofing process is maintained through encryption and access controls. Appropriate authorisation scheme for accessing the information is implemented as per our security policy.

h) **(119 461/ISS-8.5.2-07)**: The evidence of the identity proofing process shall be stored in a way that ensures the possibility to search, retrieve, and re-verify the identity proofing result.

Evidence of the proofing process is stored in a way that is searchable (by means of the proofing process identifier, or supplied reference value, or timestamp). The evidence can be retrieved from the store and reverified given the original digital identity document is re-presented or data from it is provided for verification.

i) **(119 461/ISS-8.5.2-08)**: At the end of the retention time defined by ISS 8.5.2-04, the evidence of the identity proofing process and all personal data on the applicant shall be deleted.

The evidence of the identity proofing process and all personal data on the applicant is deleted at the end of retention time defined by ISS-8.5.2-04 [7].

5 Use cases for identity proofing to Baseline and Extended LoIP

5.1 Introduction, compliance with the present document, general requirements for all use cases

a) **(119 461/USE-9.1-01X)**: To be compliant with the present document, an identity proofing process shall conform to at least one of the use cases in clause 9 or Annex C of the present document for Baseline LoIP or Extended LoIP.

The identity proofing process supported by The Service conforms to the use case in clause 9.2.3.4 of [7], Annex C.2 and Annex C.3.

b) **(119 461/USE-9.1-01A)**: Compliance with the claimed use cases and the claimed LoIP from the present document should be assessed by an independent, accredited conformity assessment body.

The compliance with the claimed use cases and the claimed LoIP as per USE-9.1-01X of [7] is assessed by an independent, accredited conformity assessment body.

c) **(119 461/USE-9.1-02X)**: The requirements in the following clauses of the present document shall apply to all use cases: • clause 5 (operational risk assessment);
• clause 6 (policies and practices);
• clause 7 (identity proofing service management and operation);
• clause 8.1 (initiation);
• clause 8.2.1 (attribute and evidence collection general requirements);
• clause 8.3.1 (attribute and evidence validation general requirements); • clause 8.4.1 (binding to applicant general requirements); and
• clause 8.5 (issuing of proof).

The Service conforms to the requirements listed under USE-9.1-02X of [7].

5.2 Use cases for identity proofing of natural person

5.2.1 Use cases using an identity document with physical presence of the applicant

[CONDITIONAL] If the identity proofing is based on the applicant's physical presence, the following requirements apply.

The Service does not support identity proofing based on the applicant's physical presence.

5.2.2 Use cases using an identity document for attended remote identity proofing

[CONDITIONAL] If the identity proofing is based on the remote presence of the applicant with online communication with a registration officer, the following requirements apply.

The service does not support identity proofing with a registration officer.

5.2.3 Use cases using an identity document for unattended remote identity proofing

5.2.3.1 General requirements

[CONDITIONAL] If the identity proofing is based on the remote presence of the applicant with unattended online communication, the following requirements apply.

a) **(119 461/USE-9.2.3.1-01)**: The applicant shall receive automated guidance throughout the identity proofing process.

Applicants are provided automated guidance through the process by instructions and animations throughout the process in The User Application.

b) **(119 461/USE-9.2.3.1-02)**: The automated process' handling of deviations from expected results or expected behaviour of the applicant shall be specified, including the conditions where the identity proofing process shall be aborted, and the information to convey to the applicant when an identity proofing process is aborted.

Applicants are informed by The User Application when the process has failed. The circumstances under which IPSP sessions will fail are well documented internally.

c) **(119 461/USE-9.2.3.1-03)**: Attribute collection shall be according to the requirements of clause 8.2.2.1 of the present document.

Attribute collection is performed in accordance with clause 8.2.2.1 of [7].

d) **(119 461/USE-9.2.3.1-04)**: The process shall use at least one digital or physical identity document as authoritative evidence.

The service requires identity proofing using one and only one digital identity document to be used as authoritative evidence.

e) **(119 461/USE-9.2.3.1-05)**: Collection of evidence shall be according to the requirements in clause 8.2.3 of the present document.

Collection of evidence is performed in accordance with clause 8.2.3 of [7].

f) **(119 461/USE-9.2.3.1-06)**: The capture of the face image of the applicant shall be according to the requirements in clause 8.4.2 of the present document.

The capture of the applicant's face image is done in accordance with clause 8.4.2 of [7].

g) **(119 461/USE-9.2.3.1-07)**: The identity proofing may use trusted registers and/or proof of access and/or documents and attestations as supplementary evidence.

See clause 4.2.1 d) of the present document.

h) **(119 461/USE-9.2.3.1-08)**: The identity proofing may use additional digital or physical identity documents as supplementary evidence.

See clause 4.2.1 d) of the present document.

i) **(119 461/USE-9.2.3.1-09)**: The identity proofing may use existing eID means as supplementary evidence.

See clause 4.2.1 d) of the present document.

j) **(119 461/USE-9.2.3.1-10)**: The identity proofing may use existing digital signature means as supplementary evidence.

See clause 4.2.1 d) of the present document.

5.2.3.2 Use case for manual operation (Baseline LoIP only)

[CONDITIONAL] If the identity proofing is based on the remote presence of the applicant with unattended online communication, and validation of evidence is manual using a physical identity document, and binding to applicant is by manual face verification, then the following requirements apply.

The Service does not support binding to applicant by manual face verification.

5.2.3.3 Use case for hybrid manual and automated operation

[CONDITIONAL] If the identity proofing is based on the remote presence of the applicant with unattended online communication, and validation of evidence is either automated using a digital identity document or combined automated and manual for physical identity document, and binding to applicant is either by manual face verification or a combination of manual face verification and face biometrics, then the following requirements apply.

The service does not support hybrid operation with a physical identity document or a manual face verification in any use case.

5.2.3.4 Use case for automated operation

[CONDITIONAL] If the identity proofing is based on the remote presence of the applicant with automated online communication, and validation of evidence is automated using a digital identity document, and binding to applicant is by automated face biometrics, then the following requirements apply.

a) **(119 461/USE-9.2.3.4-01X)**: At least one digital identity document shall be used as authoritative evidence.

The service requires identity proofing using one and only one digital identity document to be used as authoritative evidence.

b) **(119 461/USE-9.2.3.4-02)**: Evidence validation shall be according to the requirements in clause 8.3.2 of the present document.

See clause 4.3.2 of the present document.

c) **(119 461/USE-9.2.3.4-03)**: Binding to applicant shall be according to the requirements in clause 8.4.3 of the present document.

See clause 4.4.3 of the present document.

5.2.4 Use case for identity proofing by authentication using eID means

[CONDITIONAL] If the identity proofing is based on authentication using eID means, the following requirements apply.

The Service does not support identity proofing based on authentication using eID means.

5.2.5 Use case for identity proofing using digital signature with certificate

[CONDITIONAL] If the identity proofing is based on the use of a digital signature with a certificate, the following requirements apply.

The Service does not support identity proofing based on the use of a digital signature with a certificate.

5.3 Use case for identity proofing of legal person

[CONDITIONAL] If identity proofing is of a legal person, the following requirements apply.

The Service does not support identity proofing of a legal person.

5.4 Use case for identity proofing of natural person representing legal person

[CONDITIONAL] If identity proofing is of a natural person representing a legal person, the following requirements apply.

The Service does not support identity proofing of a natural person representing a legal person.

5.5 Use cases for additional identity proofing to enhance an identity proven by use of an eID from Baseline LoIP to Extended LoIP

[CONDITIONAL] If the applicant is a natural person, including a natural person representing a legal person, and the identity of the applicant has been proven to Baseline LoIP by means of authentication using an eID, and an enhancement to Extended LoIP is required, the following requirements apply.

The Service does not support additional identity proofing to enhance an identity from Baseline LoIP to Extended LoIP

6 Use cases for identity proofing for EU qualified trust services (119 461/Annex C)

6.1 (C.1) Introduction

Use cases for identity proofing for EU qualified trust services applies to The Service.

6.2 (C.2) Use cases for issuing of qualified certificate according to Article 24.1 of the original eIDAS regulation

6.2.1 (C.2.1) Use case for identity proofing by physical presence of the applicant

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate according to Article 24.1 of the original eIDAS regulation [i.1], and identity proofing is done by physical presence according to letter a of this Article, the following requirements apply.

The Service does not support identity proofing done by physical presence.

6.2.2 (C.2.2) Use case for identity proofing by authentication using eID means

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate according to Article 24.1 of the original eIDAS regulation [i.1], and identity proofing is done by authentication using eID means according to letter b of this Article, the following requirements apply.

The Service does not support identity proofing by authentication using eID means.

6.2.3 (C.2.3) Use case for identity proofing by certificate of qualified electronic signature or qualified electronic seal

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate according to Article 24.1 of the original eIDAS regulation [i.1], and identity proofing is done by the certificate of a qualified electronic signature or qualified electronic seal according to letter c of this Article, the following requirements apply.

The Service does not support identity proofing by certificate of qualified electronic signature or qualified electronic seal

6.2.4 (C.2.4) Use case for identity proofing by other identification means

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate according to Article 24.1 of the original eIDAS regulation [i.1], and identity proofing is done by other identification means according to letter d of this Article, the following requirements apply.

a) **(119 461/QTS-C.2.4-01)** [CONDITIONAL]: If attended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements of clause 9.2.2.1 of the present document shall apply.

The Service does not support attended remote identity proofing.

b) **(119 461/QTS-C.2.4-02)** [CONDITIONAL]: If attended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements of either clause 9.2.2.2 or 9.2.2.3 of the present document shall apply.

The Service does not support attended remote identity proofing.

c) **(119 461/QTS-C.2.4-03)** [CONDITIONAL]: If unattended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements of clause 9.2.3.1 of the present document shall apply.

See clause 5.2.3.1 of this document.

d) **(119 461/QTS-C.2.4-04)** [CONDITIONAL]: If unattended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements of either clause 9.2.3.2 or 9.2.3.3 or 9.2.3.4 of the present document shall apply.

See clause 5.2.3.4 of this document.

e) **(119 461/QTS-C.2.4-05)**: The identity proofing method shall be recognized at national level by the EU Member State in which the qualified trust service provider is registered.

The identity verification method is self-declared to NKOM (regulating body) as a method for delivery and binding of authenticator means on an eID of level assurance high.

QTSPs are obliged to obtain recognition at a national level with the Member State in which it resides.

f) **(119 461/QTS-C.2.4-06)**: The identity proofing method shall in terms of reliability provide equivalent assurance of the identity proofing to physical presence as determined at national level by the EU Member State in which the qualified trust service provider is registered.

The identity proofing method in terms of reliability provides equivalent assurance of the identity proofing to physical presence as determined at national level by Norway.

QTSPs are obliged to clarify the recognition in the Member State in which it resides.

g) **(119 461/QTS-C.2.4-07)**: The fulfilment of requirement QTS-C.2.4-06 shall be confirmed by a conformity assessment body.

The requirements under QTS-C.2.4-06 are assessed by a conformity assessment body.

6.2.5 (C.2.5) Use case for identity proofing of legal person

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate according to Article 24.1 of the original eIDAS regulation [i.1], and identity proofing is of a legal person, the following requirements apply.

The Service does not support identity proofing of a legal person.

6.2.6 (C.2.6) Use case for identity proofing of natural person representing legal person

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate according to Article 24.1 of the original eIDAS regulation [i.1], and identity proofing is of a natural person representing a legal person, the following requirements apply.

The Service does not support identity proofing of a natural person representing a legal person.

6.3 (C.3) Use cases for issuing of qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, and 24.1b of the amended eIDAS regulation

6.3.1 (C.3.1) Use case for identity proofing by physical presence of the applicant

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, or 24.1b of the amended eIDAS regulation [i.4], and identity proofing is done by physical presence according to letter d of Article 24.1a and/or letter e of Article 24.1b, the following requirements apply.

The Service does not support identity proofing by physical presence.

6.3.2 (C.3.2) Use case for identity proofing by authentication using eID means

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, or 24.1b of the amended eIDAS regulation [i.4], and identity proofing is done by authentication using eID means according to letter a of Article 24.1a and/or letter a of Article 24.1b, the following requirements apply.

The Service does not support identity proofing by authentication using eID means.

6.3.3 (C.3.3) Use case for identity proofing by certificate of qualified electronic signature or qualified electronic seal

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, or 24.1b of the amended eIDAS regulation [i.4], and identity proofing is done by the certificate of a qualified

electronic signature or qualified electronic seal according to letter b of Article 24.1a and/or letter b of Article 24.1b, the following requirements apply.

The Service does not support identity proofing by certificate of qualified electronic signature or qualified electronic seal.

6.3.4 (C.3.4) Use case for identity proofing by other identification means

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, or 24.1b of the amended eIDAS regulation [i.4], and identity proofing is done by other identification means according to letter c of Article 24.1a and/or letter d of Article 24.1b, the following requirements apply.

a) **(119 461/QTS-C.3.4-01)** [CONDITIONAL]: If attended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements for Extended LoIP of clause 9.2.2.1 of the present document shall apply.

The Service does not support attended remote identity proofing.

b) **(119 461/QTS-C.3.4-02)** [CONDITIONAL]: If attended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements for Extended LoIP of clause 9.2.2.3 of the present document shall apply.

The Service does not support attended remote identity proofing.

c) **(119 461/QTS-C.3.4-03)** [CONDITIONAL]: If unattended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements for Extended LoIP of clause 9.2.3.1 of the present document shall apply.

See clause 5.2.3.1 of the present document.

d) **(119 461/QTS-C.3.4-04)** [CONDITIONAL]: If unattended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements for Extended LoIP of either clause 9.2.3.3 or clause 9.2.3.4 of the present document shall apply.

See clause 5.2.3.4 of the present document.

e) **(119 461/QTS-C.3.4-05)** [CONDITIONAL]: If identity proofing is done by enhancing an identity proofing for Baseline LoIP using eID as authoritative evidence, the requirements of clause 9.5 of the present document shall apply.

The Service does not support enhancing an identity proofing for Baseline LoIP using eID as authoritative evidence.

f) **(119 461/QTS-C.3.4-06)** [CONDITIONAL]: If identity proofing is done by enhancing an identity proofing for Baseline LoIP using eID as authoritative evidence, ...

The Service does not support enhancing an identity proofing for Baseline LoIP using eID as authoritative evidence.

g) **(119 461/QTS-C.3.4-07)**: Identity proofing for any further attributes additional to the unique identity of the person shall be either according to the requirements of one of the clauses C.3.1, C.3.2, C.3.3, or C.3.4 of the present document, or by means of qualified electronic attestation of attributes, or by means of supplementary evidence that

according to the identity proofing context is regarded as authoritative evidence according to the requirements of clauses 8.2.6 and 8.3.6 (trusted register), and/or clauses 8.2.7 and 8.3.7 (proof of access), and/or clauses 8.2.8 and 8.3.8 (documents and attestations) of the present document.

Identity proofing for any further attributes additional to the unique identity of the person is done according to the requirements of C.3.4 of [7].

h) **(119 461/QTS-C.3.4-08)**: The conformity of the identity proofing method with the requirements of this clause C.3.4 of the present document shall be confirmed by a conformity assessment body.

The requirements under clause C.3.4 are assessed by a conformity assessment body.

6.3.5 (C.3.5) Use case for identity proofing of legal person

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, or 24.1b of the amended eIDAS regulation [i.4], and identity proofing is of a legal person, the following requirements apply.

The Service does not support identity proofing of a legal person.

6.3.6 (C.3.6) Use case for identity proofing of natural person representing legal person

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, or 24.1b of the amended eIDAS regulation [i.4], and identity proofing is of a natural person representing a legal person, the following requirements apply.

The Service does not support identity proofing of a natural person representing a legal person.

6.4 (C.4) Use case for qualified electronic registered delivery services according to Article 44 of the amended eIDAS regulation

The Service does not support this use case.