Fourthline

Certificate Practice Statement

Document Information

Document ID	FL-QTSP-CPS1
OID	1.3.6.1.4.1.55012.3.2.1
Version	1.3
Classification	Public
Registered on	28/01/2026
Business Owner	IT Security Team
Status	Final

Version Overview

Version	Date	Description
0.9	27.01.2026	Draft submitted for registration
1.0	11.03.2026	First published version
1.1	30.03.2026	OCSP profile update
1.2	24.04.2026	CA profile update
1.3	27.08.2026	Participants and Assessments update

Table of Contents

1. Introduction

1.1. Overview

The Certification Practice Statement (CPS) is a document that describes the requirements and practices that **Fourthline Trust Services AB** (hereafter "Fourthline Trust Services", "Fourthline", "we", "our") follows to manage and use Certificates, in acting as a Trust Service Provider. This document follows the framework specified in RFC 3647.

This Certification Practice Statement distinguishes between qualified and non-qualified certificate services provided under this PKI:

- Qualified – Certificates issued in accordance with Regulation (EU) No 910/2014 (eIDAS) and applicable ETSI standards, intended for use cases requiring a defined level of legal assurance and regulatory compliance.
- Non-Qualified – Certificates issued outside the scope of eIDAS qualification, intended for authentication, electronic signatures, or other trust services where qualified status is not required.

Fourthline distinguishes separate Certification Authorities, pursuant to the scenarios above:

- Root CA: issues and validates the subordinate CAs
- QCP CA: subordinate CA that issues and validates certificates under eIDAS qualified status

1.2. Document Name and Identification

The name of this document is the Certificate Practice Statement of certificates issued by Fourthline Trust Services AB. This document serves to the purpose of practice statement for the issuance of qualified electronic certificates and the management of remote QSCD. The OID for this document is 1.3.6.1.4.1.55012.3.2.1.

The Certificate Policies applicable to this document, as defined in ETSI EN 319 411-1 and ETSI EN 319 411-2, are the following:

- Qualified electronic certificates for natural persons
    - QCP-n-qscd – 0.4.0.194112.1.2

The Server Signing Application Service Policies applicable to this document, as defined in ETSI TS 119 431-1, are the following:

- Normalized SSAS Policy
    - NSP – 0.4.0.19431.1.1.2

This document goes into effect upon its publishing. It loses its validity upon its replacement or when being succeeded by an updated version.

1.3. PKI Participants

This section lists and describes the entities that participate in the Fourthline PKI qualified according to the eIDAS regulation.

1.3.1. Certification Authorities

Certification Authorities (CA) are the entities that issue certificates. In this document, the term CA refers to the trusted infrastructure, key material, and associated processes from which certificates are issued and signed.

Fourthline follows a two-tier CA structure. The first tier consists of the Root CA, and the second tier consists of subordinate CAs that issue certificates following the practices in this document.

The Root CA serves the purpose to issue and sign the subordinate CA certificates. Root CA functions are provided by a third party (see 1.3.5, Other participants), who manages and operates the CA independently from Fourthline Trust Services, while conforming to the requirements from EN 319 401 and EN 319 411-1.

The subordinate CAs owned and controlled by Fourthline are hosted and operated by the trustworthy systems service provider (see 1.3.5, Other participants) on behalf of Fourthline within the controlled trust service environment. Fourthline retains exclusive authority for all CA decisions regarding these subordinate CAs, including certificate issuance, renewal and revocation (where applicable), and ensures that all sensitive CA operations are performed only upon authorization from Fourthline systems in accordance with documented procedures.

1.3.2. Registration Authorities

Registration authorities (RA) are the entities that establish enrollment procedures for end-user certificate applicants, perform identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates (where applicable), and approve applications for renewal or re-keying certificates on behalf of a CA.

Fourthline B.V. acts as the Registration Authority. Under the oversight and control of Fourthline Trust Services, the RA is responsible for:

- Verifying the identity of certificate applicants to the level of assurance required by the certificate policy
    - Qualified certificates require eIDAS Level of Assurance "High"
- Validating certificate requests and binding verified identities to their public keys
- Maintaining records of identity verification, certificate requests, and key usage

Identity verification is performed using Fourthline B.V. remote identity verification solutions, which are ETSI TS 119 461 compliant. The solutions provide an interface for Applicants and Relying Parties to participate in authentication, signature creation, and other PKI-related processes.

1.3.3. Subscribers

Subscribers are the individuals to whom Fourthline has issued a certificate. A subscriber may be the Subject in the Certificate. A Subscriber is considered an Applicant until their identity is verified, and a Certificate is issued.

Prior to issuing a Certificate, the Subscriber must agree to the Terms and Conditions supplied by Fourthline. Subscribers are subject to the requirements and provisions in this CPS and the Terms and Conditions.

1.3.4. Relying Parties

Relying Parties (RP) are natural or legal entities that use and verify certificates issued by Fourthline, according to this document. RPs rely upon the accuracy of, the binding between the subject public key distributed via that certificate and the identity and/or other attributes of the subject contained in that certificate.

1.3.5. Other Participants

1.3.5.1. Trustworthy Systems Service Provider

Be Invest International SA (hereafter “Be Ys”, “CA host”, “TSA host”) is a provider of trusted computing solutions. Be Ys acts as the host and administrator of the public key infrastructure, including the CA and TSA, as well as the secure cryptographic hardware.

The secure cryptographic hardware is responsible for generating, storing, and protecting cryptographic. This device functions as a remote Qualified Signature Creation Device (QSCD) for QCP-n-qscd certificates. The cryptographic hardware and signature activation modules meet the qualifications required to operate as a QSCD.

Cryptomathic Signer SAM

- **Assurance Package:** EAL4 augmented with AVA_VAN.5
- **Protection Profile Conformance**: EN 419 241-2:2019
- **Certificate Number**: NSCIB-CC-2300116-01

Ultimaco Cryptoserver CP5

- **Assurance Package**: EAL4 augmented with AVA_VAN.5
- **Protection Profile Conformance**: EN 419 221-5:2018
- **Certificate Number**: NSCIB-CC-2300142-01

Fourthline integrates this QSCD into the controlled trust service environment and maintains overall responsibility for its operation. Fourthline oversees the provision and functioning of all relevant components within a tamper-protected environment and implements additional controls to identify and mitigate risks arising from QSCD operations.

While the cryptographic hardware and supporting interfaces are supplied and maintained by a third party, Fourthline governs the authorization, creation, and activation of signature keys. The Subscriber retains sole control over the activation of their cryptographic keys during qualified signature generation.

1.4. Certificate Usage

1.4.1. Acceptable Use

Certificates may be used for purposes designated by:

- The certificate type and applicable certificate policy OID
- Key usage and extended key usage extensions in the certificate
- The applicable legal and regulatory framework

Qualified certificates issued under this CPS are intended for creating qualified electronic signatures and comply with ETSI EN 319 412-2. They shall not be used for encryption or confidentiality purposes.

1.4.2. Prohibited Use

Certificates shall not be used for any purpose not designated by the type of the certificate, associated usage policy, and/or key extensions.

Certificates issued in the context of this policy shall not be used to attest the reputation, credibility, or safety of the Subscriber, or their obedience and respect of, or compliance with, any laws. Certificates only represent the verification of the information contained therein during issuance, in accordance with this document.

Additionally, non-qualified certificates shall not be used in contexts that require a qualified certificate. The subscriber and the relying party are responsible for ensuring that the correct type of certificate is requested according to its intended use.

1.5. Policy Administration

The organization responsible for administering this document is:

Fourthline Trust Services AB
Östermalmstorg 1,
114 42 Stockholm
Sweden
security@fourthline.com

Questions, queries and other communication should be addressed to Fourthline in written or electronic form. Additional contact information is available in the Fourthline website: https://www.fourthline.com

The person(s) who determine the suitability of this document are the Security Officers within Fourthline. Members of this role act according to the results and recommendations of approved independent auditors. The security officers are responsible for considering and actioning the results of the corresponding audits.

Changes to this document must be approved by the management board of Fourthline Trust Services. The CPS is reviewed after major process changes or at least annually, as part of the internal audit and is adapted if

necessary.

1.6. Definitions and Acronyms

1.6.1. Definitions

Term	Definition
Applicant	An individual who has initiated a certificate application. In the case of qualified certificates, the individual has not yet been verified to the required level of assurance for certificate issuance
Certificate Authority (CA)	The entity responsible for issuing, managing, revoking, and renewing certificates, and for all functions associated with the Public Key Infrastructure (PKI)
Certificate Policy (CP)	A document that describes the requirements and practices that the CA follows to manage and use certificates
Certificate Practice Statement (CPS)	A document that describes the requirements and practices that a Trust Service Provider follows to manage and use certificates
Certificate Revocation List (CRL)	A list of certificates that have been revoked before their scheduled expiration date
Certification Authority	See Certificate Authority
Distinguished Name (DN)	A name format using X.500 naming conventions that uniquely identifies entities in certificates
Level of Assurance (LoA)	The degree of confidence in the identity verification process, with three levels under eIDAS: low, substantial, and high
Multi-Factor Authentication (MFA)	A security mechanism that requires users to provide two or more independent verification factors to gain access to a system, application, or resource.
Public Key Infrastructure (PKI)	A set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store, and revoke certificates and manage public key encryption
Qualified Certificate	A certificate issued in accordance with Regulation (EU) No 910/2014 (eIDAS) and applicable ETSI standards, intended for use cases requiring a defined level of legal assurance and regulatory compliance
Qualified Electronic Certificate (QEC)	A certificate issued by a qualified trust service provider that can be used to create a qualified electronic signature once the client's identity is verified to an appropriate standard
Qualified Electronic Signature (QES)	An electronic signature that complies with the eIDAS Regulation, providing a high level of assurance equivalent to a handwritten signature
Qualified Signature Creation Device (QSCD)	A secure cryptographic device responsible for generating, storing, and protecting cryptographic keys that meets requirements of CEN EN 419 241-2
Qualified Trust Service Provider (QTSP)	A licensed organization that can issue qualified electronic certificates and create qualified electronic signatures, which must comply with eIDAS regulations

Registration Authority (RA)	The entity that establishes enrollment procedures, performs identification and authentication of certificate applicants, and initiates revocation requests on behalf of a CA
Relying Party (RP)	Natural or legal entities that use and verify certificates issued by the CA according to the CPS
Root CA	The top-level certification authority that issues and validates intermediate CAs
Subscriber	An individual to whom the CA has issued a certificate; considered an Applicant until identity is verified and a certificate is issued
Trust Service Provider (TSP)	An entity responsible for the operation of trust services including certificate issuance and management

1.6.2. Acronyms

Acronym	Definition
CA	Certification Authority
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DORA	Digital Operational Resilience Act (Regulation (EU) 2022/2554)
eIDAS	electronic Identification, Authentication and Trust Services (Regulation (EU) No 910/2014)
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
HSM	Hardware Security Module
ISMS	Information Security Management System
LoA	Level of Assurance
NIS2	Network and Information Security Directive 2 (Directive (EU) 2022/2555)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy
QEC	Qualified Electronic Certificate
QES	Qualified Electronic Signature
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
RA	Registration Authority

RP	Relying Party
SIEM	Security Information and Event Management
SOC 2	Systems and Organization Control 2
TSP	Trust Service Provider
UTC	Coordinated Universal Time

2. Publication and Repository Responsibilities

2.1. Repositories

Fourthline operates a public HTTPS repository available on https://pki.fourthline.com.

The repository contains:

- published CA certificates
- current and previous CPS documents
- information related to certificate revocation
- terms and conditions for qualified trust services
- privacy and data protection policies or statements

This repository has an availability target of 99.5% during business hours.

2.2. Publication of certificate information

Fourthline publishes CA certificates, CRLs, OCSP services, and policy documentation through its public repository.

Certificate status information is available through CRL and OCSP services as specified in the certificate profiles (Section 7). The locations of CRLs and OCSP responders are documented in the Authority Information Access extension of issued certificates.

Fourthline issues certificates with short validity periods aligned to specific transaction use cases. Due to these short lifetimes, certificates typically expire before standard revocation procedures can complete. Relying parties must verify the validity period of the certificate, as well as the certificate status.

Subscriber certificates issued to end-entities are not published in these repositories, in accordance with GDPR data minimization principles. Certificates used for remote electronic signatures are included in the signed document(s). Relying Parties are responsible for distribution of the signed document(s) to the Subscribers.

2.3. Time or frequency of publication

Certificate Revocation Lists are published every 24 hours, with each CRL having a maximum validity period of 7 days from issuance. OCSP responders provide real-time responses with maximum 24-hour validity periods and 5-second response time under normal operating conditions.

CA certificates that support trust services are published within 24 hours of issuance.

The CPS is reviewed, updated and published following the process and timelines defined in section 9.12.

2.4. Access controls on repositories

The information repositories listed in section 2.1 are available publicly on a read-only basis over encrypted transport channels.

Access to the repositories for publishing and managing the information therein is restricted to authorized personnel only, and protected using strong authentication, role-based access, and context-based authorization.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of names

All certificates issued by Fourthline use a Distinguished Name (DN) in the Subject field of the Certificate. Specific DN construction rules, mandatory and optional attributes, and encoding requirements are defined in the Certificate Profiles (Section 7).

Qualified certificates for natural persons comply with ETSI EN 319 412-2 regarding subject Distinguished Name structure and mandatory attributes.

3.1.2. Need for names to be meaningful

Names in the certificates must identify the Subscriber as a specific natural person. Fourthline uses the full legal name of the Applicant from the valid and verified identity proof provided. The name of the Applicant becomes the name of the Subscriber when the identity verification reaches the required level of assurance. Additionally, names are presented in a form that Relying Parties can interpret.

3.1.3. Anonymity or pseudonymity of subscribers

Fourthline does not issue anonymous certificates for subscribers.

For qualified certificates, the legally verified name of the subscriber must be included in the subject DN. Pseudonyms may be included as an additional identifier in the pseudonym attribute field but cannot replace the legal name.

For non-qualified authentication certificates, pseudonymous identifiers may serve as the primary subject identifier where appropriate, insofar as it is allowed by the certificate policy.

3.1.4. Rules for interpreting various name forms

Distinguished Names use standard X.500 naming conventions. Individual names used in the certificate Subject include the encoded and transliterated representation of the legal names, in conformance with international identity document standards.

3.1.5. Uniqueness of names

Each certificate issued by Fourthline contains a unique Subject DN.

End-entity certificates achieve uniqueness through the serialNumber attribute, which contains a unique subscriber identifier. This allows to disambiguate certificates issued for the same subscriber on different occasions, or to distinguish applicants that share the same name. Fourthline performs an additional uniqueness check that verifies that the serial numbers used in subject DNs are never reused.

Multiple certificates may be issued to the same subscriber with different certificate policy OIDs, key pairs, or validity periods.

3.1.6. Recognition, authentication, and role of trademarks

Fourthline does not validate or assert any rights related to trademarks, trade names, or service marks in connection with the Subject DN. Subscribers warrant that they possess rights to use names provided. Relying parties are responsible for assessing any potential trademark implications outside the scope of the certificate's identity information.

3.2. Initial Identity Validation

Fourthline uses a remote process to perform the identification and authentication of Applicants. The identity validation process is supported by identity verification solutions provided by the RA, compliant with ETSI TS 119 461.

3.2.1. Method to Prove Possession of Private Key

Subjects using a remote electronic signature process supported by a QSCD may either provide their own device or use the remote QSCD. Under the present CPS, Fourthline operates a remote QSCD.

3.2.1.1. Subjects Using Remote QSCD (Fourthline-Operated)

For qualified electronic signatures and other scenarios where the Qualified Signature Creation Device (QSCD) is operated remotely by Fourthline, the key pair is generated exclusively within the remote QSCD environment in accordance with ETSI TS 119 431-1 and ETSI TS 119 431-2.

The private key is generated inside a certified QSCD that meets the requirements of CEN EN 419 241-2. The Subscriber never has direct access to, or possession of, the private key material at any time. Key generation occurs only after the successful authentication of the applicant's identity in accordance with eIDAS Article 24 and ETSI EN 319 411-2. The key pair is cryptographically bound to the verified legal identity of the Subscriber.

Use of the private key remains under the sole control of the Subscriber through a secure protocol which is detailed further in Section 6.

3.2.2. Authentication of Organization Identity

Not applicable. Fourthline does not issue certificates to legal persons or organizations.

3.2.3. Authentication of Individual Identity

Fourthline verifies the identity of each natural person prior to issuing a qualified certificate, in accordance with eIDAS Article 24 and ETSI EN 319 411-2. Identity verification ensures that the Subscriber is uniquely and unambiguously identified, and that the identity information included in the certificate is accurate. Since the identity of the individual is strongly bound to the certificate and the usage of the corresponding private key, the authentication of the individual is subject to achieving a level of assurance required by the usage of the key.

3.2.3.1. Remote Identity Verification

Identity verification is performed through a remote identification process that provides a level of assurance equivalent to in-person verification, in accordance with ETSI TS 119 461.

The remote identity verification process includes:

- Capture and verification of an official identity document using the device camera, including checks to confirm authenticity and integrity.
- Live capture of facial biometrics (still image or short video sequence) performed by the applicant using their device camera.
- Consistency checks between the identity document, biometric data, and applicant-provided information.
- Fraud-prevention controls, including detection of replay attacks, presentation attacks, and document manipulation.

Fourthline validates and records the following mandatory attributes: full legal name, date of birth, document type and issuing authority, document number and expiry date, and nationality (where available). Additional attributes may be collected to support the identity verification process.

A unique identifier is assigned to each Subscriber to ensure unambiguous identification. Verified identity attributes are bound to the certificate request following successful authentication.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for Routine Re-key

Fourthline does not support certificate re-key operations for end entities. Certificates issued under this policy are single-use and short-lived, with validity periods designed to match the specific transaction for which they are issued (for example, signature creation). Once a certificate is used for its intended purpose, it expires shortly thereafter and cannot be re-keyed.

Subscribers requiring certificates for new transactions must undergo a new certificate issuance process, following the enrolment and verification procedures defined in Section 3.2.

3.3.2. Identification and Authentication for Re-key After Revocation

Not applicable. Fourthline does not support re-key operations and does not provide a revocation process. Certificates cannot be re-keyed following revocation. Subscribers must request new certificate issuance following the standard enrollment and verification procedures defined in Section 3.2.

3.4. Identification and Authentication for Revocation Requests

Not applicable. Fourthline issues validity-assured certificates to end-entities. Under the present document, these certificates have very short validity periods (up to 24 hours). Additionally, certificates are issued and used for a single purpose only, following the consent of the subscriber. End-entity certificates typically expire before standard revocation processes can complete. Therefore, Fourthline does not facilitate a revocation request process for end-entities.

The revocation of intermediate CA certificates shall follow internal Fourthline procedures, including the authentication and change management requirements.

3.4.1. Entities Allowed to Request Revocation

Not applicable. Fourthline may accept certificate revocation requests under exceptional circumstances from the following entities:

- The TSP or RA, upon detection of certificate compromise or fraudulent issuance
- Competent authorities with legal basis

3.4.2. Authentication Level Requirements

Not applicable for end-entity certificates. Revocation of intermediate CA certificates shall follow internal Fourthline procedures, including the authentication and change management requirements.

3.4.3. Revocation Request Channels

Not applicable for end-entity certificates. Revocation of intermediate CA certificates shall follow internal Fourthline procedures, including the authentication and change management requirements.

3.4.4. Processing Timeline

Not applicable. Exceptional revocation requests shall be processed according to the requirements of the event that necessitates it.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

A certificate application may only be submitted by an individual whose identity will be bound to the Certificate. Applications are initiated when an Applicant engages with Fourthline for the identity verification process, in the context of providing a remote electronic signature.

Fourthline and the Registration Authority (RA) are responsible for:

- Collecting identity evidence and data supporting the application
- Verifying the authenticity, accuracy, and validity of the information submitted
- Ensuring that the Applicant provides explicit consent for certificate issuance, key generation within a QSCD, and the use of the certificate
- Binding verified identity attributes to the certificate application.

Applicants must provide valid identity proofs required by the applicable certificate policy. Identity verification processes are conducted with the aim to identify the subject to the level of assurance required by the certificate policy. Records are stored and retained as defined in Section 5.5.

4.2. Certificate Application Processing

4.2.1. Validation of Information

Fourthline verifies all identity evidence and submitted information to the level of assurance required by the applicable Certificate Policy.

The identity verification process is carried out in accordance with Section 3.2 and confirms that:

- The Applicant is the person represented in the identity proofs provided
- Identity attributes from the applicant which are added in the certificate comply with the certificate profile in Section 7
- The verification of the identity reaches the level of assurance required by the applicable Certificate Policy
- The Applicant provided explicit consent for certificate issuance and key creation

Fourthline evaluates integrity and fraud-prevention signals to ensure a reliable binding between the Applicant and the certificate request.

4.2.2. Authorization for Key Generation in QSCD

After successful identity verification to the level of assurance required by the Certificate Policy, Fourthline authorizes the creation of the key pair within the certified remote QSCD operating under Fourthline responsibility. The private key remains within the tamper-protected environment.

All authorization requests to the CA and QSCD components occur through mutually authenticated, secured channels in Fourthline's controlled trust service environment.

4.2.3. Approval or Rejection

Fourthline approves an application only when all necessary verification, authorization, and consent conditions have been successfully met. Applications are rejected where identity evidence is insufficient or inconsistent, where verification requirements are not fulfilled, or where fraud indicators are present.

Rejected applications cannot be modified and must be resubmitted as new applications if the Applicant wishes to obtain a certificate.

4.2.4. Processing Times

Fourthline aims to process certificate applications promptly, generally within 24 hours, subject to the completeness and quality of the identity evidence provided. Applicants or relying parties may be notified when delays arise due to additional checks or verification requirements.

4.3. Certificate Issuance

Fourthline issues certificates under the Certificate Policies applicable to its subordinate CAs, including:

- QCP-n-qscd

Certificates issued by the CA use a certificate serial number which is computed with a random value. This ensures the serial numbers are unique and protected from forgery.

Certificate issuance and usage of private keys follow a controlled, auditable process that ensures the integrity of identity binding and the correct application of certificate profiles.

4.3.1. Issuance Authorization

Fourthline authorizes certificate issuance only when:

- Identity verification has been satisfactorily completed for the Subscriber
- Explicit Subscriber consent has been recorded
- The type of certificate requested and its corresponding certificate policy are appropriate to the context of the request

All certificate issuance instructions originate from authorized Fourthline systems using mutually authenticated channels to the CA components integrated into Fourthline's trust service environment.

4.3.2. Certificate Construction

Certificates are constructed by the CA infrastructure using the profiles defined in Section 7, including:

- Subject Distinguished Name attributes drawn from verified identity data
- a unique subscriber identifier encoded in the serialNumber attribute
- the appropriate Certificate Policy OID
- required extensions such as Key Usage, Extended Key Usage, and QC Statements for qualified certificates.

Fourthline ensures that certificate profiles are applied consistently and that all mandatory fields and extensions are present. The inclusion of a unique subscriber identifier ensures the uniqueness of the Subject DN in the certificate.

4.3.3. Key Generation in QSCD

The issuance of QCP-n-qscd certificates follows that:

- The key pair of the subject is generated in a QSCD certified against EN 419 221-5.
    - The algorithms and key strengths applied are reflected in the certificate profile
- The Subscriber's private key remains within the QSCD in the tamper-proof environment
- The activation of the private key – under the sole control of the subject – is controlled by a signature activation module certified against EN 419 241-2.

4.3.4. Certificate Signing

Certificates are signed using CA private keys stored in secure cryptographic modules forming part of the CA infrastructure under Fourthline's governance. Access to CA signing operations is strictly controlled and occurs only upon authorization by Fourthline.

4.3.5. Notification mechanisms

Relying parties receive the issued certificates through obtaining the document(s) signed with them, via the available interfaces of Fourthline services for qualified electronic signatures. Relying Parties may additionally

obtain CA certificates, certificate chains, and status information from the endpoints referenced in the Authority Information Access extension of the certificate, or from the information provided in the public repositories detailed in Section 2. Publication and Repository Responsibilities.

End-entity certificates are not directly delivered to subscribers as part of the software applications or services provided by Fourthline. Relying parties should facilitate to the subscriber a copy of the material signed with the subscriber certificates, when the certificate is successfully used to provide a qualified electronic signature.

Subscribers may request from Fourthline a copy of the certificate issued on their behalf, provided that:

a. The subscriber successfully completed the identity validation
b. A certificate was generated as a result of the successful identification

Subscribers shall make a request in email form to the address stated in Section 1.4. Policy Administration, containing at minimum the following information:

1. The full name used in the certificate application,
2. The name of the business partner through whose services the certificate is being applied for,
3. The timestamp or narrowest approximate time range when the identity verification was conducted,
4. A copy of the identity document used during the identity proofing.

Fourthline may request a copy or confirmation of any additional information that was requested at the time of identity validation, such as e-mail address, phone number, physical address, in order to unambiguously identify the Applicant during the identity proofing as the Subject of the certificate.

Fourthline shall return the issued public certificate to the Subscriber in a response email upon completing the validation.

4.4. Certificate Acceptance

Certificate acceptance is implicit and occurs when Fourthline has confirmed explicit consent from the Subscriber for certificate issuance, and the Subscriber uses the certificate for its intended purpose (e.g., executing a signature within the QSCD).

Fourthline records all relevant authorization and usage events as evidence of acceptance.

4.5. Key Pair and Certificate Usage

The private key of the subject is created and used in a QSCD certified against EN 419 221-5.

Fourthline ensures that Subscribers retain sole control over the use of their private keys. This is enforced through a signature activation module and associated controls conforming with TS 119 431-1. Private key use can only occur following authenticated, explicit authorization from the Subscriber. The relevant provisions for the Signature Activation Protocol that ensures this control are detailed in Section 4.5.1. Activation of the private key of the subject is managed by a signature activation module certified against EN 419 241-2.

The signature activation module ensures that the subject has sole control over the private key. The private key of the subject is only used for signing or sealing.

4.5.1. Subscriber Use of Private Key

Subscribers may use their private keys only in accordance with:

- The certificate policy under which the certificate was issued
- The permitted Key Usage and Extended Key Usage fields
- The Terms and Conditions and applicable legal requirements.

The Subscriber cannot extract, copy, or export private key material. For qualified certificates issued according to QCP-n-qscd, the private key is stored and used exclusively within the remote QSCD under Fourthline responsibility.

Since Fourthline operates a remote electronic signature process using a remote QSCD, Fourthline ensures the Subscriber has sole control over usage of the private key. This control is maintained through:

- Verifying the identity of the subscriber to the required level of assurance
    - Qualified certificates require reaching eIDAS Level of Assurance “High”
- Cryptographically binding the device session to the identity of the subscriber
- Collecting consent for the usage of the key for explicit purposes only, as confirmed by the Subscriber

This control is maintained through the continuity of the authenticated session of the user, and through integrity-protected session management mechanisms. The activation of the subscriber private key for the use consented to by the Subscriber follows the protocol described in Section 6.4.

4.5.2. Relying Party Usage

Relying Parties who use the certificates issued by Fourthline are responsible for ensuring that qualified certificates are used only where qualified signatures are legally required or appropriate. In addition, RPs must validate the certificates issued by Fourthline using the means and information provided by Fourthline.

Fourthline provides sufficient information to support relying party validation, including access to CA certificates, and certificate chain information. Relying Parties are responsible for verifying:

- the certificate policy,
- the intended usage of the certificate,
- the validity period

4.6. Certificate Renewal

Fourthline does not support certificate renewal.

Certificates issued in accordance with this CPS are short-lived and tied to a specific transaction or workflow. When a certificate expires or a new certificate is required, relevant parties must initiate a new certificate issuance process. This process includes identity verification as required by the applicable Certificate Policy.

4.7. Certificate Re-key

Fourthline does not support certificate re-key operations.

Key pairs associated with certificates are generated exclusively within the QSCD for each request, and new certificates always require the creation of new keys (and key material).

4.8. Certificate Modification

Certificate modification is not supported.

Certificates issued under this CPS cannot be altered after issuance. Any changes to identity attributes, certificate policy, or usage require a new certificate to be issued according to the procedures in this document.

4.9. Certificate Revocation and Suspension

Due to the short lifetime of certificates issued according to the present document, Certificates may expire naturally before the revocation process completes and takes effect. The certificate revocation status endpoints are implemented to support long-term validation of certificates. In exceptional cases when Fourthline should revoke a certificate, the status is reflected (as applicable) in CRL and OCSP services as defined in the Certificate Profile.

Fourthline does not support the suspension of certificates.

4.10. Certificate Status Services

Fourthline provides certificate status through CRL and OCSP services, as defined in the Certificate Profiles.

Due to the limited validity period of certificates, status information will typically indicate validity and expiration. Nevertheless, revocation status remains available throughout the validity lifetime of certificate records to support long-term validation.

4.11. End of Subscription

A Subscriber's relationship with Fourthline ends when one of the following conditions is met:

- The certificate expires or is revoked
- The associated transaction or workflow is completed

Given the short-lived nature of certificates, subscription typically ends when the certificate expires.

4.12. Key Escrow and Recovery

The CA and remote signing services do not support key escrow.

5. Management, Operational, and Physical Controls

Fourthline operates an Information Security Management System (ISMS). Physical security, personnel security, access control, logging, and records management controls are implemented according to the ISMS framework. Sub-contracted functions, including the CA and TSA hosting, and RA supporting systems operate under ISO 27001 certified ISMSs. Fourthline oversees the qualifications of the service providers to ensure the requirements for management, operational and physical controls conform to EN 319 401.

Additional controls specific to qualified trust service operations supplement the ISO 27001 baseline and are described below.

5.1. Physical Security Controls

The CA and remote QSCD systems are hosted in ISO 27001 certified data centers located in the European Union. The data center enforces strict physical access control in accordance with the requirements of clause 6.4.2 of EN 319 411-1. The data center protects the CA systems in accordance with clause 7.6 of EN 319 401 and clause 6.4.2 of EN 319 411-1.

The RA systems are hosted in third-party data centers in the European Union. The hosting provider provides multi-zone redundancy within the same region with automated failover between the data centers. Data centers are certified to ISO 27001 and SOC 2 standards, ensuring consistent physical and environmental security controls across all hosting locations.

Fourthline maintains oversight of data center provider compliance through contractual service level agreements, periodic audit rights, and annual vendor risk assessments as defined in the Supplier Management Policy. The supplier review process includes mitigation actions to minimize the risks and consequences of non-conformities in these providers.

5.2. Procedural Controls

Fourthline has established trusted roles and procedural controls to ensure secure and accountable operation of trust services. Role definitions, responsibilities, and segregation requirements pertaining to the provision of trusted services are documented and maintained as part of the Information Security Management System.

5.2.1. Trusted Roles

Fourthline has defined the following trusted roles for QTSP operations:

Security Officer: Responsible for administering and enforcing security policies and practices, corresponding to ETSI EN 319 401 requirements. The Security Officer establishes and maintains the ISMS, approves security controls, authorizes security-relevant activities, owns risk assessments and incident reviews, and ensures eIDAS compliance. The Security Officer is organizationally independent from operational and administrative roles and cannot act as System Administrator, Operator, or Auditor.

System Administrator: Installs, configures, and maintains trustworthy systems supporting QTSP services. Administrators deploy, harden, patch, and upgrade systems, maintain availability and backups, and implement approved security controls. Administrators cannot issue certificates, approve issuance, or modify audit logs. All administrative actions are logged.

System Operator: Responsible for day-to-day operation of QTSP systems. Operators monitor operational status, execute approved procedures, support system-driven identification and registration operations, and escalate anomalies. Operators cannot change system configurations or security parameters. Given Fourthline's exclusive use of short-lived and validity-assured certificates, System Operators do not operate, monitor, or publish revocation-based certificate status mechanisms.

System Auditor: Provides independent oversight by reviewing audit logs and system records. Auditors review logs, verify compliance with procedures and segregation of duties, prepare audit reports, escalate violations, and support external conformity assessments. The System Auditor function is organizationally and

operationally independent with read-only access to logs and archives. Audit logs are protected against modification and deletion.

Identity Validation Role: Fourthline does not establish a separate Registration Officer role as certificate issuance decisions are fully automated and policy-driven. Identity verification and validation are performed through automated processes supported by qualified identification systems. Dedicated personnel at Fourthline perform manual review in escalated cases (exception handling, risk-based escalation, quality assurance, suspected fraud). Identity validators confirm the completeness and integrity of identification evidence.

Revocation Function: Not applicable. Fourthline does not establish a dedicated Revocation Officer role as the QTSP exclusively issues short-lived and validity-assured certificates that reach the end of the validity period before revocation requests can be validated, authenticated, processed, and enforced, in alignment with ETSI EN 319 411-1. Any emergency or security-driven certificate invalidation is performed under the oversight of the Security Officer.

5.2.2. Number of Persons Required per Task

Critical security-sensitive operations require the involvement of at least two authorized persons (dual control/four-eyes principle). Depending on the operation, this may involve either two different trusted roles or two persons holding the same trusted role. Examples of operations requiring dual control include:

- Configuration of cryptographic algorithms (requires two Security Officers)
- Activation of CA private keys for certificate signing operations (requires involvement of multiple authorized personnel at the hosting provider facilities)
- Approval of material changes to security policies (requires Security Officer and management approval)

These controls are enforced through technical access restrictions, role-based access control, and procedural safeguards. Compliance with dual-control requirements is subject to regular audit and review.

5.2.3. Identification and Authentication for Each Role

Personnel performing trusted roles must be identified and authenticated before accessing systems or performing sensitive functions. Authentication mechanisms include:

- Multi-factor authentication (MFA) for access to administrative systems, CA infrastructure, and audit systems
- Role-based credentials and role-based authorization permissions for everyone
- Context-based authorization policy decisions
- Access logging and real-time analysis of authentication events

Authentication credentials and the configuration of access control systems are managed according to the access management procedures, with the aim to minimize the risks of misuse of user accounts, credentials, and authorization. The procedures stipulate minimum authentication strength requirements and other security policies to be applied during authentication and authorization.

5.2.4. Roles Requiring Separation of Duties

To prevent conflicts of interest and single points of failure, Fourthline enforces segregation of duties:

- Security Management and Operations: The Security Officer does not perform operational or administrative tasks. Security policy approval is separated from implementation.
- System Administration and System Operation: Administrator and Operator functions are logically separated. An individual may hold multiple roles organizationally, but technical and procedural controls ensure only one role can be exercised at any given time using separate accounts and access rights.
- Audit Independence: System Auditors do not perform operational, administrative, or security management tasks. Audit activities are independent of the functions being audited.
- Identity Validation vs. Certificate Issuance: personnel performing identity validation do not have authority to approve or deny certificate issuance. Certificate issuance decisions are enforced

automatically by the system based on policy rules, ensuring no single individual can override the automated decision.

Additional to the segregation of roles, a four-eyes principle ensures that a single individual does not perform conflicting duties within the same case or process (e.g., requestor and approver).

5.3. Personnel Security Controls

Fourthline ensures that the personnel involved in the provision of trusted services meets the security requirements and expectations stipulated for their roles.

Personnel performing trusted roles receive access to relevant policies, procedures, and operational documentation necessary to perform their assigned functions. This includes the Information Security Policy Framework, operational procedures for their specific role, incident reporting channels, and guidance on regulatory compliance obligations.

5.3.1. Qualifications, Experience, and Clearance Requirements

Personnel performing trusted roles must possess appropriate qualifications, experience, and reliability for their assigned responsibilities. Trusted roles require expertise in information security, PKI operations, identity verification, and regulatory compliance as appropriate to the specific role function. Management personnel responsible for security-sensitive areas demonstrate relevant professional experience and maintain current knowledge of applicable standards and regulations.

5.3.2. Background Check Procedures

Background checks are performed for personnel assigned to trusted roles prior to granting access to security-sensitive systems or functions. The scope and depth of background screening is commensurate with the sensitivity and criticality of the role. Personnel may not access trusted functions or systems before required checks are completed. Background check procedures follow applicable employment law requirements and data protection regulations.

5.3.3. Training Requirements

Personnel performing trusted roles receive training appropriate to their assigned responsibilities. Training covers information security awareness, PKI operations, relevant ETSI standards, regulatory requirements, operational procedures, and incident reporting channels. Security Officer and System Administrator roles require specialized training in cryptographic operations, security risk management, and compliance frameworks. Identity validation personnel receive training in document authentication, fraud detection, biometric verification, and applicable identity proofing standards including ETSI TS 119 461. All personnel must demonstrate understanding of their security responsibilities before performing trusted functions.

5.3.4. Retraining Frequency and Requirements

Personnel assigned to trusted roles participate in annual refresher training to maintain current knowledge of security threats, regulatory changes, procedural updates, and evolving fraud patterns. Additional training is provided when material changes occur to systems, processes, policies, or regulatory requirements affecting their role responsibilities. Training completion is documented and verified by the Security Officer.

5.3.5. Job Rotation Frequency and Requirements

Not stipulated. Job rotation is not a mandatory control given the specialized nature of trust service roles and the relatively small size of operational teams. Segregation of duties and dual control requirements provide appropriate risk mitigation without requiring systematic job rotation.

5.3.6. Sanctions for Unauthorized Actions

Personnel who violate security policies, fail to follow operational procedures, or perform unauthorized actions are subject to disciplinary measures in accordance with employment policies and applicable labor law. Sanctions may include retraining requirements, access restrictions, reassignment of duties, or termination of

employment depending on the severity and impact of the violation. Material security violations are investigated by the Security Officer and escalated to management as appropriate.

5.3.7. Independent Contractor Requirements

External contractors and service provider personnel performing trusted roles must meet the same competence, reliability, and training requirements as internal personnel. Contractor access to systems and data is governed by written agreements specifying adherence to security policies, confidentiality obligations, and acceptable use requirements. Contractor access rights are reviewed periodically and revoked promptly upon completion of contracted services.

5.4. Audit Logging Procedures

Fourthline logs security-relevant events across systems that provide or support trust service operations. Audit logging procedures comply with ETSI EN 319 401 clause 7.10 requirements for trust service providers.

5.4.1. Types of Events Recorded

The following system information is logged:

- Security events,
- Configuration changes,
- Policy changes,
- Access attempts, and
- CA key life-cycle events.

The following registration information is logged:

- Applicant name (legal name)
- Document type and issuing authority
- Identity document identifier
- Repository location for the electronic copies of identity data
- Identity of the Registration Authority receiving and processing the application
- Terms and Conditions and other legal documents consented to by the applicant

Audit log entries are recorded and protected in accordance with EN 319 401 and EN 319 411-1.

5.4.2. Log Processing

Fourthline operates centralized audit collection using a dedicated Security Information Events Management (SIEM) system for aggregation, analysis, and alerting. The system operates independently from operational systems to prevent log modification or deletion. Logs are collected from RA systems, supporting infrastructure, and external service provider systems where contractually required. The system includes automated anomaly detection, event correlation, and real-time security incident alerting.

Logs are processed continuously through automated monitoring using the SIEM for real-time analysis and alerting. Manual review occurs weekly (at minimum) for operational monitoring and monthly for comprehensive security reporting. Logs supporting trust service operations are additionally reviewed annually for external conformity assessments.

Audit logs are retained for a minimum of seven years following the event, in accordance with eIDAS requirements and ETSI EN 319 401 clause 7.10. Logs supporting qualified trust services may be retained longer where required by law.

All systems synchronize time with Coordinated Universal Time (UTC) at least daily, in accordance with ETSI EN 319 401 clause 7.10. Accurate time stamps are essential for audit log integrity, certificate validity verification, and non-repudiation of trust service operations.

Fourthline stipulates no requirements to notifying the entity that caused the event. Personnel are informed through security awareness training that their activities are subject to audit logging. Individual notification may occur when an audit log review identifies policy violations or security incidents requiring investigation.

5.4.3. Log Retention

Audit logs are protected through solutions that provide tamper-evident, append-only storage mechanisms with cryptographic integrity protection. Access is restricted to System Auditors with read-only permissions. Administrative modification or deletion is prevented through technical controls. Logs are encrypted at rest and in transit. Backup copies are maintained in geographically separate locations with the same protection controls.

Records retained in the SIEM benefit from the built-in high availability and durability of the system hosted on a globally distributed infrastructure with automatic replication across availability zones. Logs retained in the SIEM system are continuously available for analysis, compliance verification, and forensic investigation without requiring manual backup procedures. Log integrity is maintained through the inherent data protection mechanisms including encryption at rest and in transit provided by the solution.

5.4.4. Vulnerability Assessment

Regular vulnerability assessments are performed on systems supporting trust service operations. Penetration testing is performed when systems are set-up, after significant changes, or at minimum once a year following a schedule.

Critical vulnerabilities are remediated within reasonable timeframes based on severity – the exact fix timelines and risk indicators are documented in the Vulnerability Management Process. Where immediate remediation is not possible, mitigations are applied to reduce the risk, or documented exceptions are recorded to accept the risks.

5.5. Records Archival

Fourthline archives records necessary for demonstrating compliance with trust service obligations and providing evidence for legal proceedings. The retention and protection periods follow the technical security controls for data backup and archival.

5.5.1. Types of Records Archived

Fourthline archives the following types of records to support the provision of trusted services:

- identity verification evidence, such as government-issued identity documents, biometric data, and identity proofing outcomes
- certificate lifecycle records, such as certificate signing requests, issued certificates with subscriber Distinguished Names and certificate policy OIDs, certificate delivery confirmations,
- subscriber agreements, such as terms and conditions, and consent records for certificate issuance and signature creation

Other records of events may be archived to support information security. The record types and their retention period are selected based on a risk assessment, and reviewed annually for accuracy, relevance, and completeness.

Records are stored electronically in encrypted object storage with commensurate access controls and role-based authorization.

5.5.2. Retention Periods

Audit logs regarding operations related to subscriber keys issued on behalf of individuals and managed by the CA are retained for a minimum of 7 years.

Registration information related to certificate requests and issuance workflows are retained for 10 years.

Identity verification evidence and certificate issuance records supporting qualified electronic signature certificates are retained for 10 years after certificate expiration to support legal evidence requirements for signatures with long-term legal effect and to enable validation of signatures beyond the cryptographic validity period of certificates.

Other security-relevant audit logs are retained for up to 2 years to support the management of information security.

Records may be retained longer where required by applicable law, or for ongoing legal or regulatory proceedings.

All suppliers, processors, and subcontractors processing data on behalf of the QTSP in relation to identity verification, certificate issuance, validation, revocation, or associated audit records shall be subject to the same data retention periods defined in this CPS.

5.5.3. Protection and Access

Archived records are stored in encrypted formats with access restricted to authorized personnel on a need-to-know principles. Records are protected against tampering through cryptographic integrity controls and immutable storage mechanisms. Access to archived records is logged and monitored.

Authorized personnel retrieve archived records through controlled access procedures requiring authentication and authorization verification. Requests from supervisory authorities, conformity assessment bodies, or legal proceedings are processed through designated security and/or compliance personnel.

5.5.4. Backup and Availability

Archived records are backed up through automated daily processes with verification of backup integrity. Backup archives are stored in geographically separate locations from primary archives to ensure resilience against localized disasters. Backup restoration procedures are tested annually.

Archive systems operate with appropriate redundancy and geographic distribution to ensure long-term availability and maintain readability throughout the retention period despite technological changes.

5.5.5. Timestamping

Critical records include trusted time stamps synchronized with UTC. Certificate issuance events, identity verification completion, subscriber authorization events, and significant administrative actions include accurate time stamps for audit and non-repudiation purposes, ensuring temporal integrity of archived evidence.

5.6. Key Changeover

Fourthline engages the creation of a new key (and associated public certificate) for a CA under circumstances such as the following:

- the CA certificate approaches its natural expiration
- the CA private key requires revocation following a security event (for example, compromise of the private key, or proven weakness of the underlying algorithm)
- the legal entity identified in the CA certificate undergoes material change
- any other events acknowledged by the Security Officer as requiring a re-key

Key changeover is performed through a formal key ceremony procedure, that stipulates the secure generation of key material within a certified Hardware Security Module, the presence of multiple parties for its authorization and oversight, and the creation of the appropriate PKI certificate.

The key changeover process allows for both the expiring and the new private keys to exist, however only one key is used for signing certificates at a time. The expiring CA may remain in place only to process certificate status information for certificates issued within its infrastructure until its certificate expires.

Fourthline publishes the new CA public certificate in the Repository as described in Section 2. Advance notice of the changeover timeline is provided to stakeholders for planned key expiration or algorithm deprecation, except in cases of key compromise or security incidents requiring immediate action.

The impact of CA key changeover on subscribers is minimal due to the nature of validity-assured certificates. Certificates issued immediately before CA key changeover remain valid until their natural expiration. Subscribers requesting new certificates following the transition automatically receive certificates signed by the new CA key without requiring any action.

5.7. Compromise and Disaster Recovery

5.7.1. Incident Management

Fourthline operates incident management procedures compliant with ISO 27001 and DORA requirements. Security incidents affecting trust service operations are detected through automated monitoring using SIEM systems with real-time alerting.

Incidents are classified by priority and severity based on impact to trust service operations and subscribers. Response procedures assign roles and responsibilities through an on-call rotation system with escalation to the Security Officer for major incidents.

Major ICT-related incidents are reported to the management body and competent authorities within required timeframes. All incidents are documented with root cause analysis to prevent recurrence.

The CA and TSA host is ISO 27001 certified and has established vulnerability and incident management policies and procedures for:

- Monitoring,
- Information security incident management planning and preparation,
- Assessment and decision on information security events,
- Response to information security incidents,
- Learning from information security incidents,
- Collection of evidence, and
- Information security event reporting.

Incidents are reported in accordance with NIS2.

5.7.2. CA Private Key Compromise

In the event of suspected or confirmed compromise of a CA private key, Fourthline immediately activates emergency response procedures. The response to this event follows incident handling processes outlined in 5.7.1. Fourthline ensures that the compromised CA is deactivated promptly, and stakeholders are notified of the revocation through the repository channels defined in Section 2.

Where the security of the cryptographic algorithms used in the CA are compromised, Fourthline engages an off-schedule update to the CA keys. The timeline of the update is dictated by the risk and severity of the event, with critical events resulting in priority or immediate key changeover.

A new CA key pair is generated through the key ceremony procedures described in Section 5.6.

5.7.3. Business Continuity and Disaster Recovery

Fourthline maintains business continuity and disaster recovery plans compliant with ISO 27001 and DORA requirements. Plans are designed to restore trust service operations after disasters including physical facility failures, prolonged power outages, cyber-attacks, data center failures, and infrastructure provider outages.

Recovery procedures prioritize restoration of identity verification and certificate issuance capabilities. Recovery time objectives are established based on the criticality of affected functions.

Business continuity plans are tested annually with results documented and deficiencies addressed. Plans are updated following incidents, tests, and material changes to infrastructure or operations. The Security Officer maintains oversight of business continuity preparedness and coordinates with infrastructure providers to ensure recovery capabilities remain effective.

The CA and TSA host has additionally established business continuity policies and procedures for:

- Information backup,
- Information security during disruption, and
- ICT readiness for business continuity.

5.8. CA or RA Termination

Fourthline maintains an up-to-date termination plan in accordance with ETSI EN 319 401 clause 7.12 and ENISA Guidelines on Termination of Qualified Trust Services. The termination plan addresses both voluntary cessation of services and involuntary termination due to business failure, regulatory action, or other circumstances requiring service discontinuation.

If termination becomes necessary, Fourthline will notify all affected parties in advance in accordance with the Service Termination Plan. Fourthline will provide notice within the timeframes defined in that plan to allow affected parties to take appropriate action, and will communicate as early as reasonably possible based on the circumstances of the termination.

If Fourthline terminates trust services, all required archival records will be transferred to a designated custodian, which will act as the responsible party for maintaining required evidence. The details of the custodian or the method to select the custodian are documented in the termination plan (see 9.8. Terms and Termination).

Fourthline will ensure that all CA private keys are securely destroyed so they cannot be used after the service ends. Any agreements with infrastructure providers that support the CA operations will also be terminated. Fourthline keeps financial provisions in place to cover the costs of an orderly termination.

Finally, Fourthline will coordinate with the relevant supervisory bodies as required to ensure the termination is compliant, transparent, and properly documented.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

The CA keys are created and maintained in certified cryptographic modules located in a physically protected environment. CA key pair generation and certification is undertaken by dedicated personnel under dual control. The CA key algorithms and parameters can be seen in Section 7.1, "Certificate Profiles".

The CA only issues certificates to subject keys that are managed by the TSP. The subject keys managed by the TSP are created and maintained in a certified QSCD. See also Section 4.5, "Key Pair and Certificate Usage".

Fourthline conducts a yearly re-assessment of the certifications attained by the QSCD operator. The process includes validation of the results of independent audits supporting the certifications, and mitigation actions to reduce the risks to acceptable levels for Fourthline. The termination plan detailed in Section 5.8 includes provisions to follow should the remote QSCD operator and/or hosting provider fail to meet the required certifications.

The public certificates for the CA are published in the repository as dictated in Section 2. Relying parties may obtain these certificates from the repository.

The key pairs for End-entity certificates are only created following successful identity verification to the level of assurance required by the certificate policy. If the Applicant identity does not reach the required level of assurance, the Applicant cannot become a Subscriber, and therefore a key pair is not generated.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

The CA keys are used in certified cryptographic modules located in a physically protected environment. The cryptographic modules are operated in compliance with the certification of the cryptographic modules. Backup and recovery of CA keys is handled by dedicated personnel.

Usage of the CA keys is subject to the purpose of the CA. Certificate-issuing CAs use the private key to issue entity certificates. The private key of these CAs can only be activated through programmatic interfaces that require mutual authentication from pre-registered entities and from specific locations. The process to activate the key to issue an end-entity certificate includes controls to prevent this usage unless the end-entity is sufficiently verified.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Public certificates for Fourthline CAs are published in the repository detailed in Section 2.

CA certificates remain published and accessible for the duration of their validity period, and an additional retention period to enable verification of signatures created before CA termination. For qualified CAs, certificates remain available for 10 years following the last certificate issued by that CA to support long-term signature verification requirements.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

CA certificates have validity periods appropriate to their position in the certificate hierarchy and the cryptographic algorithms used. Certificate-issuing CAs typically have validity periods of 5-10 years.

Fourthline may re-key CAs before certificate expiration based on cryptographic strength assessments, usage volume, or security policy requirements.

6.4. Activation Data

The CA keys are protected by a cryptographic module. The activation of the CA keys require authentication towards the cryptographic module. Activation of the Root CA to issue a subordinate CA certificate is performed by the Root CA provider, following strict protocols for requesting, authenticating, validating, securing and auditing the process, conformant to EN 319 411-1.

Subscriber keys are activated following a key activation protocol. For qualified certificates, the protocol requires subscribers' identities to achieve eIDAS Level of Assurance "High" in accordance with ETSI TS 119 461 (identity proofing requirements) within the same session where the subscriber consents to the usage of the private key.

The subscriber authenticates through security mechanisms that cryptographically bind the identity verification to the signature authorization, ensuring the person who completed identity verification is the same person authorizing signature creation. Subscribers must provide explicit consent for the usage of the key to provide a qualified electronic signature for a specific document (or set thereof).

6.5. Computer Security Controls

The CA, TSA, and remote QSCD systems are hosted in an ISO 27001 certified data center. Access control follows best practices based on "least privileges" and strong authentication. All systems are kept in physically and logically protected environments (see also Section 5.1, "Physical Security Controls"). Attempts to access the systems are logged and monitored.

Systems used to support TSP operations implement security controls compliant with ISO 27002. These systems operate in a physically and logically segregated environment with limited access, following strict just-in-time access controls and separation of duties.

Security controls for the systems and software are audited through independent testing at minimum annually and following major modifications, including vulnerability scanning and penetration testing where appropriate.

Test and production environments are separated to prevent unauthorized changes or disruptions to operational systems.

Systems are protected against malware through endpoint protection, network security controls, and regular security updates.

6.6. Life Cycle Security Controls

6.6.1. Change and Defect Management

The CA, TSA, and remote QSCD systems are hosted in an ISO 27001 certified data center. Change management is implemented in accordance with ISO 27002 recommendations.

Systems supporting trust service operations implement life cycle security controls compliant with ETSI EN 319 401 clause 7.7 and ISO 27002. Changes to software, hardware, firmware components, systems, or security parameters are performed in a controlled manner following documented change management procedures. Change control procedures apply to system configurations, application code, infrastructure definitions, and security parameters affecting trust service operations.

Security requirements are analyzed during system design and specification phases to ensure security is embedded throughout the development lifecycle. Changes are subject to approval from roles whose functions are independent from the implementation.

Test and production environments are separated to prevent unauthorized changes or disruptions to operational systems. Changes are tested in non-production environments before deployment. Rollback procedures and responsibilities are defined for aborting changes or recovering from unsuccessful implementations.

Security updates are applied within reasonable timeframes based on a risk assessment, unless applying the update would cause negative effects to the operation of the systems. Exceptions are documented to either accept the risk, or to implement compensating controls to partially reduce the risks.

6.6.2. Capacity Management

Fourthline ensures that the systems operating to provide trusted services meet the contracted or forecasted capacity demands. This is achieved through practices such as (but not limited to) fault-tolerant designs, high-availability architectures, real-time alerting, dynamic capacity allocation, performance testing, and failover and recovery process documentation.

Systems are further designed to identify, and alert or respond to changes in capacity of dependent systems, where appropriate. Dependencies are identified and documented for the required functioning of system components and monitored for availability.

When the provided capacity fails to meet the required and established targets, Fourthline follows an incident management and fault recovery process (as applicable to the situation), to restore available capacity within the acceptable time frames.

6.6.3. Supplier Management

Fourthline follows a supplier management process to identify, assess, and minimize risks to security, availability, operations for the provision of trusted services. Critical suppliers or those providing a substantial concentration of ICT services to Fourthline are reviewed annually, including validation of any operating certifications and independent audit results provided. Where possible, Fourthline aims to reduce the concentration of ICT services provided by third parties, and additionally maintains exit plans, to avoid the risks of single-vendor lock-in.

Ongoing monitoring of the contracted SLAs ensures that the third-party services operate within the agreed parameters. Fourthline monitors critical functions in real or near-real time through service information channels provided by the supplier, or through direct evaluation and measurement, as appropriate.

6.7. Network Security Controls

The CA, TSA, and remote QSCD systems are hosted in an ISO 27001 certified data center. Network security controls are implemented in accordance with ISO 27002 recommendations.

Systems supporting trust service operations implement network security controls compliant with ETSI EN 319 401 clause 7.8 and ISO 27002. Network infrastructure is segmented into security zones based on the criticality of functions and data classification. Communication between zones is restricted to necessary operations with firewall rules reviewed at least annually, and every six months for systems supporting critical functions.

All network connections between trust service components use encrypted channels, using latest industry standard recommendations. Administrative access to systems requires multi-factor authentication over dedicated secure channels, and following just-in-time access controls subject to review and approval. Network access controls prevent and detect unauthorized connections to trust service networks, with only authorized devices meeting security requirements permitted to establish connections.

Test and production environments are separated to prevent unauthorized changes or disruptions to operational systems. Network architecture and security design are reviewed annually to identify potential vulnerabilities. Firewall rules and other network filters are designed and implemented following through change management procedures with roles and responsibilities clearly defined.

Systems are protected against network-based attacks through intrusion detection, DDoS mitigation, and continuous monitoring for anomalous network activities. Network traffic is monitored for security events with automated alerting through a SIEM system. Vulnerability scanning and penetration testing include network security assessments as described in Section 6.5.

6.8. Timestamping

Qualified time stamps are issued in accordance with the Best Practice Time Stamp Policy as set out in EN 319 421. Time-stamping services are provided by the TSA hosting provider, operating ISO 27001 certified infrastructure. The TSA maintains accurate time synchronization with Coordinated Universal Time (UTC) to ensure the reliability of timestamps.

Time stamps are applied to signed documents to support long-term validation of qualified electronic signatures, particularly where signatures must maintain legal evidentiary value beyond the validity period of the signing certificate or where cryptographic algorithms may be deprecated over time.

7. Certificate and CRL Profiles

Fourthline maintains certificate profiles, Certificate Revocation List (CRL) profiles, and Online Certificate Status Protocol (OCSP) response profiles for the CAs and certificates covered by this CPS.

Certificate profiles specify the structure, content, and encoding of certificates issued under this CPS, including mandatory and optional fields, extensions, and their values. Profiles comply with applicable ETSI standards including ETSI EN 319 412-2 for qualified certificates issued to natural persons.

7.1. Certificate Profile

This section defines the X.509 v3 certificate profiles. Certificate profiles specify the structure of the Distinguished Name, mandatory and optional attributes, certificate extensions, cryptographic algorithms, and validity periods. Where applicable, the profiles include the values used in the certificate, or an indication of how Fourthline formats the value used in the certificate.

7.1.1. Subordinate CA Certificate Profile

Field	Detail	Value
Version		2
Signature Algorithm		sha256WithRSAEncryption
Serial Number		55:41:7d:0b:19:31:2c:5a:b5:99:1b:34:d3:d7:40:af:a4:a4:d7:83
Issuer	commonName	LC ROOT CA
	organizationName	BE INVEST International S.A.
	organizationIdentifier	VATLU-29222134
	countryName	LU
Issuer SerialNumber		0e:f2:63:c1:63:d3:b2:bd:ff:f6:78:da:bf:b8:dc:2d:eb:b9:3a:c1
Validity	notBefore	
	notAfter	notBefore + 10 years
Subject	commonName	Fourthline QCP CA 01
	organizationName	Fourthline Trust Services AB
	organizationIdentifier	NTRSE-5595552505
	countryName	SE
Subject Public Key Info		ansip521r1
Extensions	keyUsage	KeyCertSign crlSign
	extendedKeyUsage	OCSPSigning
	BasicConstraints	Critical
		CA

7.1.2. Subject Certificate Profile

Field	Detail	Value
Version		2
Signature Algorithm		ecdsa-with-SHA512
Issuer	commonName	Fourthline QCP CA 01
	organizationName	Fourthline Trust Services AB
	organizationIdentifier	NTRSE-5595552505
	countryName	SE
Subject	commonName	*String with the legal name of the Subscriber as verified through the official identity document. Transliteration may be applied.*
	givenName	*String with the given name of the Subscriber*
	surname	*String with the surname of the Subscriber*
	organizationName	*Empty or not included for QCP-n-qscd certificates*
	organizationIdentifier	*Empty or not included for QCP-n-qscd certificates*
	countryName	*ISO 3166-1 alpha-2 codes*
	serialNumber	*UUID that links the certificate to the verified identity in the signing session*
Validity	notBefore	*Time of issuance*
	notAfter	*Calculated as* notBefore *+ 24h*
Subject Public Key Info		ansip521r1
Extensions	keyUsage	nonRepudiation
	certificatePolicies	QCP-n-qscd
	cRLDistributionPoints	http://crl.fourthline.com/fourthlineca.crl
	QcStatements	QcCompliance QcSSCD QcType=esign QcPDS=https://pki.fourthline.com/PDS.pdf
	authorityInfoAccess	id-ad-caIssuers= https://pki.fourthline.com/CA/FourthlineQCPCA01.cer id-ad-ocsp= http://ocsp.fourthline.com
	id-etsi-ext-valassured-ST-certs	

7.2. CRL Profile

This section defines the profiles for Certificate Revocation Lists. These specify the primary attributes that identify the respective CRL.

7.2.1. End-Entity Certificate Revocation List

The certificate revocation list conforms to RFC 5280.

Property	Value
Version	2
Signature Algorithm	ecdsa-with-SHA512
Issuer	Fourthline QCP CA 01
Extensions	CRLNumber
	Authority Key Identifier

7.3. OCSP Profile

The OCSP responder conforms to RFC 6960.

Property		Value
Version		1
Distribution point		http://ocsp.fourthline.com/
Subject	commonName	FOURTHLINE OCSP {nn}
	organization	Fourthline Trust Services AB
	organizationIdentifier	NTRSE-5595552505
	countryName	SE

The **commonName** in the OCSP certificate subject uses an incremental numeric counter, such as 01, 02, 03, etc. represented in the profile by the symbol {nn}.

Since Fourthline only issues short-term certificates, there is no revocation management service available to Subscribers. The CRL and OCSP endpoints are maintained to support long-term validation of issued certificates.

8. Compliance Audit and Other Assessment

Fourthline Trust Services AB undergoes audits and assessments to verify conformity with different requirements, regulations, and standards.

8.1. Topics Covered and Assessment Methodology

The scope of assessments includes, but is not limited to:

- Compliance with **eIDAS Regulation** and applicable delegated and implementing acts
- Conformance with relevant **ETSI standards** (i.e. EN 319 401, EN 319 411-1/-2 etc, as applicable to the trust services provided)
- Effectiveness of organizational, procedural, and technical security controls
- Certificate lifecycle management, key management, and cryptographic controls
- Incident management, business continuity, and disaster recovery arrangements
- Personnel security, access control, and segregation of duties
- Data protection and privacy controls, where applicable
- Industry and information security standards such as ISO 27000-series
- Implementation standards and best practices such as OWASP ASVS or WCAG 2

Assessments are performed using recognized assurance frameworks and methodologies accepted by supervisory bodies, including ETSI-based conformity assessments and equivalent audit schemes applicable to trust service providers.

Additional technical security assessments are conducted, both by internal specialists (independent from the implementation) and accredited external parties, to validate the implementation of security controls. See also 5.4.4. Vulnerability Assessment.

8.2. Frequency of Assessment

Compliance audits and other assessments are performed under the following conditions:

- Pre-operational assessment prior to the commencement of services, including trust services as required for initial qualification
- Regular periodic assessments, at least on an annual basis, or at intervals mandated by the competent supervisory authority or as defined through the result of risk analysis
- Ad-hoc or extraordinary assessments triggered by:
    - Significant changes to the trust service, system architecture, or security model
    - Major incidents, security breaches, or suspected compromise affecting trust services
    - Requests from the competent supervisory body

The results of assessments are documented, reviewed by management, and used as input for corrective and preventive actions where required.

8.3. Identity and Qualifications of Assessors

Audits and conformity assessments are conducted by qualified and competent assessors who:

- Are accredited or recognized for performing assessments against the applicable standards and requirements, such as eIDAS, ETSI or ISO
- Possess demonstrable expertise in trust services, information security, and cryptographic systems, as required by the requirements or standards under assessment
- Meet the professional, ethical, and independence requirements defined by the applicable accreditation or supervisory framework

8.4. Independence of the Assessor

Fourthline ensures that the individuals or entities performing audits and assessments to validate the compliance or conformity of standards, remain independent and impartial with regards to the methodology followed and the results.

The assessors performing compliance, conformity, or accreditation audits or assessments with regulatory standing, are independent from Fourthline Trust Services AB and are not involved in the design, implementation, or operation of the assessed trust services. Independence is ensured through:

- Organizational and legal separation between the assessor and the assessed entity
- Absence of conflicts of interest
- Compliance with accreditation and professional conduct requirements

Assessors of internal requirements and standards are maintained independent from the implementation under assessment through organizational role segregation. Where the internal organization does not allow for a skilled specialist to validate internal compliance, at least one responsible individual independent from the design or implementation is selected to review and accept the assessment outcomes.

8.5. Additional Testing

Fourthline provides the capability to allow third parties to check and test all certificate types it issues. This capability extends to independent auditors, conformity assessors, and integrating business partners acting as relying parties.

Where certificates issued on the production environment are used for testing, the following controls apply, based on which party conducts or supports the test and the upload of the document for which a signature will be requested:

a. Testing conducted by Fourthline. Where Fourthline controls the document upload step, a blank document is provided to the application for signing. No legal rights or obligations may be derived from a signature created in this manner.
b. Testing conducted by a business partner. Where an integrating business partner conducts testing on the Production environment using credentials that grant authorization to upload documents to sign, the partner is required to submit only blank documents or documents bearing an explicit disclaimer stating that no legal rights or obligations may be derived from the resulting signature. This requirement is communicated to business partners as part of the integration agreement governing access to Fourthline's Production environment.

Fourthline shall not be liable for legal obligations arising from a qualified electronic signature created in the production environment during testing where a business partner submitted a legally valid document in violation of this requirement. Business partners bear sole responsibility for ensuring that documents submitted during testing carry no legal effect. See Section 1.4 for the acceptable use of certificates.

9. Other Business and Legal Matters

This section addresses general business, legal, and contractual matters applicable to the provision of trust services under this document. Where relevant, detailed terms may be further specified in associated agreements (e.g. subscriber, relying party, or partner agreements).

9.1. Fees

Fees for trust services, if applicable, are defined in separate commercial agreements.

9.2. Financial Responsibility

Fourthline Trust Services AB maintains adequate financial and organizational resources to support the continuous and secure operation of its trust services.
Where required by applicable law or regulation, appropriate insurance coverage or equivalent financial safeguards are maintained to cover potential liabilities arising from trust service operations.

9.3. Confidentiality of Business Information

Confidential business information exchanged between participants is treated as confidential and protected against unauthorized disclosure.
Such information is disclosed only as required for the performance of trust services, by law, or under applicable contractual or regulatory obligations.

9.4. Privacy of Personal Information

Personal data is processed in accordance with applicable data protection laws, including GDPR.
The applicable privacy notice or privacy policy governs the collection, use, retention, and disclosure of personal data related to trust services.

9.5. Intellectual Property Rights

Intellectual property rights relating to this document, certificates, systems, software, trademarks, and documentation remain with their respective owners.
No rights are transferred except as explicitly stated in applicable agreements or licenses.

9.6. Representations and Warranties

Representations and warranties applicable to subscribers, relying parties, or other participants are defined in relevant agreements and are consistent with this document.

9.7. Limitations of Liability

Limitations of liability, including exclusions of certain types of damages and any liability caps, are defined in applicable agreements and subject to mandatory legal requirements.
Nothing in this document limits liability where such limitation is prohibited by law.

9.8. Term and Termination

This document remains in force until amended or withdrawn. Termination conditions for participants or services, including suspension or revocation of certificates, are defined in this document and applicable agreements. The remaining provisions to handle the termination of trust services are outlined in the Service Termination Plan.

9.9. Individual notices and communications with participants

Legally relevant notices between participants must be provided in writing or through other agreed and verifiable communication channels, as specified in applicable agreements.

9.10. Amendments

This document may be amended from time to time. Non-material changes may take effect without prior notice, while material changes affecting assurance levels are communicated in advance where required.

9.11. Dispute Resolution Procedures

Disputes arising from this document, or related agreements are handled in accordance with dispute resolution mechanisms defined in applicable agreements or by law.

9.12. Governing Law

This document is governed by the laws of the jurisdiction in which Fourthline Trust Services AB is established, unless otherwise required by applicable regulation.

9.13. Compliance with Applicable Law

All participants are required to comply with applicable laws and regulations relevant to trust services, including those related to cryptography, security, and data protection.

9.14. Miscellaneous Provisions

Standard contractual provisions, including assignment, severability, and waiver clauses, may be included in applicable agreements and apply consistently with this document.

9.15. Other Provisions

Additional terms or obligations not explicitly covered elsewhere in this document may be specified in applicable agreements or supplementary policies.