Fourthline

PKI Disclosure Statement

March 2026

Document Information

Document ID	FL-QTSP-PDS1
Version	1.0
Classification	Public
Registered on	17/03/2026
Business Owner	IT Security Team
Status	Final

Version Overview

Version	Date	Redactor	Action / Changes
1.0	11.03.2026	IT Security Team	Final draft for review

Table of Contents

1. Contact Information

a. **Name**: Fourthline Trust Services AB
b. **Location**: Stockholm, Sweden
c. **Address**: Östermalmstorg 1, 114 42 Stockholm
d. **Website**: https://www.fourthline.com
e. **PKI Documentation**: https://pki.fourthline.com
f. **Email**: security@fourthline.com

2. Certificates

2.1. Qualified Certificate for Natural Person using a remote Qualified Signature Creation Device

a. **Certificate Policy**: Contained in the Certificate Practice Statement, section 1.2.
    i. **Name**: QCP-n-qscd
    ii. **Identifier**: OID 0.4.0.194112.1.2
    iii. **Description**: This certificate policy is defined in accordance with ETSI EN 319 411-1 and ETSI EN 319 411-2 for qualified electronic certificates for natural persons. Certificates are issued for creating qualified electronic signatures that have the same legal effect as a handwritten signature pursuant to Article 25(2) of the eIDAS Regulation
b. **Certificate Description**: Qualified certificates issued under this policy enable subscribers to create Qualified Electronic Signatures (QES) using a remote Qualified Signature Creation Device (QSCD). The certificates:
    - Are issued to natural persons for electronic signature purposes
    - Comply with ETSI EN 319 412-2 certificate profiles
    - Have a validity period limited to 24 hours
    - Are managed by Fourthline Trust Services AB as a Qualified Trust Service Provider listed on the EU Trusted List and Swedish Trusted List maintained by the Swedish Post and Telecom Authority (PTS)

    The subordinate CAs are hosted and operated by the trustworthy systems service provider on behalf of Fourthline within the controlled trust service environment. The secure cryptographic hardware functions as a remote Qualified Signature Creation Device (QSCD) for QCP-n-qscd certificates.
c. **Validation Procedure**: Subscribers undergo identity verification at eIDAS Level of Assurance "High". Identity verification is performed by Fourthline B.V. acting as Registration Authority using ETSI TS 119 461 compliant remote identity verification solutions. The validation process includes:
    i. Verifying the identity of certificate applicants to the level of assurance required by the certificate policy
    ii. Validating certificate requests and binding verified identities to their public keys
    iii. Maintaining records of identity verification, certificate requests, and key usage
d. **Usage Restrictions**: Qualified certificates issued under this policy shall not be used for any purpose not designated by the type of the certificate, associated usage policy, and/or key extensions. Restrictions indicate that these certificates
    i. **SHALL** be used exclusively for creating qualified electronic signatures
    ii. **SHALL NOT** be used for encryption or confidentiality purposes
    iii. **SHALL** be used personally and exclusively by the subscriber
    iv. **SHALL** only be used for lawful purposes

3. Reliance Limits

a. **Certificate Use**: Certificates are only for use with electronic signatures, as stated in section 6.2 of the Terms & Conditions agreed to by the subscriber. A QES created using the QES Services has the same legal effect as a handwritten signature pursuant to Article 25(2) eIDAS.
b. **Retention Period**: Records and evidence relating to the identification process and the issuance and management of qualified electronic certificates, including related personal data, are retained for a period of at least 10 years from the date of issuance of the qualified electronic certificate. The retention periods that apply to other categories of data under this scheme are outlined in the Privacy Statement, section 9.

4. Subscriber Obligations

a. Subscribers must comply with the obligations contained in the Certificate Practice Statement, section 4.5.1, and the Terms & Conditions, section 7.
b. **Secure Cryptographic Device**: Subscribers agree to and must use the remote Qualified Signature Creation Device (QSCD) provided through the secure cryptographic hardware operated within the controlled trust service environment. The secure cryptographic hardware is responsible for generating, storing, and protecting cryptographic keys.
c. **Certificate Acceptance**: Prior to issuing a Certificate, the Subscriber must agree to the Terms and Conditions supplied by Fourthline. The Terms and Conditions require explicit agreement from the user, according to section 1.3, and further state that accepting the agreement extends to accepting the creation of a certificate bearing the verified identity of the user, for creating a qualified electronic signature, in section 6.1.
d. **Certificate Usage**: Subscribers are subject to the requirements and provisions in the Certificate Practice Statement and the Terms and Conditions

5. Relying Party Obligations

a. **Certificate Validation**: relying parties may validate a QES using standard electronic signature validation processes, following the indications on the Terms and Conditions, section 8.2. Such validation includes verification of:
    i. The integrity of the signed data
    ii. The qualified electronic certificate used to create the signature
    iii. The status and validity of the certificate at the time of signature creation
    iv. The qualified trust service provider status of Fourthline Trust Services, as indicated in the European Union Trusted List
b. **Certificate Status**: The qualified electronic certificates issued by Fourthline Trust Services are **short-lived** (less than 24 hours validity period). As a result, validation of a QES does not require checking certificate revocation information as the validity of the certificate is assured for its limited lifetime. Fourthline Trust Services nevertheless publishes certificate revocation information in accordance with applicable trust service requirements. Certificate status information is available through:
    i. Certificate Revocation Lists (CRL) published in the repository (see Certificate Practice Statement, section 2)
    ii. Online Certificate Status Protocol (OCSP) services (see Certificate Practice Statement, section 7.3)

6. Limitation of Liabilities

a. **Warranties**: refer to the Terms and Conditions, section 4.1, and Certificate Practice Statement, section 9.6.
b. **Disclaimers**: refer to the Terms and Conditions, section 5.2.
c. **Limitation of Liabilities**: refer to the Terms and Conditions, section 10.
d. **Insurance programs**: addressed in the Certificate Practice Statement, section 9.2.

7. Agreements, Policies and Statements

a. **Terms and Conditions**:
   i. Name: Terms and Conditions QES Services
   ii. Reference: https://pki.fourthline.com/pdf/T&Cs.pdf
b. **Certificate Practice Statement**:
   i. Name: Certificate Practice Statement
   ii. Identifier: 1.3.6.1.4.1.55012.3.2.1
   iii. Reference: https://pki.fourthline.com/pdf/CPS-v1.0.pdf
c. **Certificate Policy**:
   i. Name: QCP-n-qscd
   ii. Identifier: 0.4.0.194112.1.2
   iii. Standard: ETSI EN 319 411-1 and ETSI EN 319 411-2

8. Privacy Policy

a. **Description**: Fourthline Trust Services acts as a Qualified Trust Service Provider (QTSP) under the eIDAS Regulation and processes personal data in connection with the provision and operation of Qualified Electronic Signature services.
b. **Data Collection**: the full reference of data collected through this service is specified in the Privacy Policy, section 2. Personal data processed may include the following:
   i. Name and surname of the subscriber
   ii. Identity attributes required under eIDAS for certificate issuance
   iii. Identity proofs required under eIDAS for the target level of assurance (or references to identity proofs in supporting systems)
c. **Retention Period:** the retention periods that apply to each category of data under this scheme are outlined in the Privacy Statement, section 9.
c. **Reference**: https://pki.fourthline.com/pdf/privacy-statement.pdf

9. Refund Policy

Subscribers do not pay any fees associated with the QES services. Any fees are borne by the relevant Business Partner or other third party. Therefore, no specific refund policy for subscribers is applicable. Refer to the Terms and Conditions, section 9.1.

10. Legal Matters

a. **Complaints and Disputes**: If a subscriber has a complaint relating to the QES Services, they may submit it by contacting Fourthline Trust Services using the contact details and process provided in the Terms and Conditions, section 14. (See
b. **Legal system or Jurisdiction**: The agreement is governed by and interpreted in accordance with the laws of Sweden**.** Legal matters are defined in the Terms and Conditions, section 13.

11. Licensing and Certification

11.1. Certification

a. **Qualified Trust Service Provider Status**: Fourthline Trust Services AB is a Qualified Trust Service Provider (QTSP) under Regulation (EU) No 910/2014 (eIDAS), as updated by Regulation (EU) 2024/1183.
b. **Supervisory Body**: Swedish Post and Telecom Authority (Sw. Post- och telestyrelsen) - PTS

c. **Trust List References**:
    i. EU Trusted List: https://esignature.ec.europa.eu/efda/tl-browser/
    ii. Swedish Trusted List (PTS): https://pts.se/internet-och-telefoni/betrodda-tjanster/Kvalificerade-tillhandahallare/

11.2. Conformance

a. **Certification to Certificate Policy**: Fourthline Trust Services has been certified to be conformant with the following, through audits conducted in accordance with section 8 of the Certificate Practice Statement:
    i. ETSI EN 319 411-1 (General requirements for Trust Service Providers issuing certificates)
    ii. ETSI EN 319 411-2 (Requirements for trust service providers issuing EU qualified certificates)
    iii. Certificate Policy OID: 0.4.0.194112.1.2 (QCP-n-qscd)