PKI Disclosure Statement (PDS)

This document details the policies and procedures that govern the Scrive Certified Trust Services (SCTS). Together with the Certificate Policy (CP) and the SCTS trust service practice statement (TPS), it describes the policies and procedures related to the SCTS in compliance with the eIDAS regulation. The statements herein may include links to relevant CP/CPS clauses.

Introduction

The SCTS, operated by Scrive AS, provides seamless and secure issuance of short-term qualified certificates for signing documents. The service is provided as a qualified trust service in the EU/EEA, subject to the supervision of the eIDAS supervisory body in Norway.

TSP contact information

Scrive AS operates the SCTS in Oslo, Norway. The organization administering the policy document is the Scrive TSP Squad.

General Policy Contact: pki@scrive.no

Questions or Complaints regarding SCTS: support@scrive.com

Address: Scrive AS – Møllergata 6-8, 0179, Oslo, Norway

The SCTS does not provide a certificate revocation service for certificates created through the SCTS. This is due to the certificates' single-use nature and limited lifetime of 15 minutes, which makes revocation not practically feasible.

Certificate type, validation procedures and intended use

The SCTS issues advanced and qualified certificates with a short-term validity of 15 minutes. Certificates are designed for single use for signing one specific document or object and are then discarded.

Intended Use

Certificates are issued to natural persons for electronic identification of end-users, content commitment (non-repudiation) signing, and strong authentication.

Validation Procedures

Identity is verified in connection with every signing occasion using nationally recognized electronic identification means (eID) or other approved ID Proofing Services. The eID means supported include Swedish BankID. Identities are derived from European eIDs issued at substantial or high assurance levels.

Certificate Policy (CP)

Certificates are issued according to the identifiers NCP+ for advanced certificates and QCPNCQ-n-QSCD for qualified certificates.

The OID for the Qualified Subject CA Profile

QCP-n-qscd (Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)policy-identifiers(1) qcp-natural-qscd (2)).

Relying on the certificate

Reliance on the certificate is subject to the limitations of liability set out in this PDS and the SCTS Terms, which limit Scrive's liability for direct damages to NOK 100,000 per loss-making event. Records and data related to the operation of the trust services are archived for a retention period of at least 10 years to meet statutory requirements and provide supporting evidence.

Obligations of subscribers

Subscribers undertake the following obligations upon using the SCTS:

- To provide Scrive with complete and accurate information as part of the identification verification process.
- To protect their devices, eID, id cards, passport, and passwords used in connection with the SCTS from unauthorized access and to not share them with anyone else.
- To make every reasonable effort to protect their devices from malware and other cyber threats.

- If devices, eID, or passwords are compromised, the subscriber is obliged to immediately change passwords, report the incident to the police or relevant authorities, and revoke the compromised item.

- If fraudulent activity within the SCTS is suspected, the subscriber must immediately report this to Scrive and any relying parties.

Verification obligations of the relying party

Relying parties must perform the following checks before relying on a digital certificate:1

- Check the Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) response to confirm that SCTS has not revoked the certificate.

- For qualified certificates, check the EU Trusted List (EUTL) to confirm that the SCTS Qualified Certificate issuer service is still a valid Qualified Trust Service.

- Qualified electronic signatures created in the SCTS can be validated through readily available means such as the DSS Demonstration Web App and qualified validation services.

Limitations of liability

Scrive AS, as a QTSP, limits its liability for direct damages resulting from a failure to provide the SCTS in accordance with the eIDAS Regulation or the SCTS Terms.

Liability is limited to NOK 100,000 per loss-making event, and is maximized at the applicable limit specified in the user's license terms.

Scrive is not liable for any special, incidental, indirect, statutory, exemplary, punitive, or consequential damages.

Scrive assumes no liability for damages arising from the user’s failure to comply with their obligations, unavailability or faults in third-party services or products used by the user, or events arising from Force Majeure.

Liability is presumed under the eIDAS Regulation unless Scrive proves that the damage occurred without its intention or negligence.

Claims for damages must be brought no more than twelve (12) months after the loss-making event occurred.

Applicable agreements, certification practice statement (CPS) and certificate policy (CP)

The SCTS Terms and Conditions, the Certification Policy (CP), and the SCTS Trust Service Practice Statement (TPS) form an integral part of the agreement. This PDS and related certificate profiles are published at https://pki.scrive.eu/. All subscribers accept the service terms and conditions before the certificate creation request is signed. Scrive reserves the right to modify, amend, and supplement the SCTS Terms. Scrive is entitled to transfer all rights and obligations under these SCTS Terms to another legal entity.

Privacy policy

Scrive acts as the data controller of the personal data within the SCTS, even when it may operate as a data processor in an originating application.

All data processing takes place in accordance with the EU General Data Protection Regulation (GDPR). Processed data may include first name, last name, date of birth, personal identification number, unique identifiers, document hashes, the certificate, and signing metadata.

Scrive implements strict access controls and encryption, and requires third-party services (eIDs, remote QSCD providers, etc.) to adhere to the same confidentiality standards.

Scrive is required to retain certain sets of data for 10 years from each time the SCTS is used, and will delete data after a maximum of 11 years following each signing process.

Scrive's general privacy notice is available at https://www.scrive.com/privacy-notice

Refund policy

The SCTS are typically offered in a B2B setting for remuneration, where one legal entity acquires the right to use the service. Therefore, fees and potential refunds for the services are governed by the applicable license terms of the entity that acquired the right to use the service.

Applicable law, complaints and resolution of disputes

The SCTS Terms are governed by the substantive laws of Norway. Scrive also complies with eIDAS, GDPR, and local implementations in Norway and Sweden.

Parties shall initially attempt to resolve any dispute through good faith negotiations. If not resolved, disputes shall be finally settled by arbitration administered by the SCC Arbitration Institute in Oslo. If the user is a consumer and arbitration is not admissible by law, Oslo District Court shall have exclusive jurisdiction.

Complaints

Questions or complaints regarding the SCTS can be directed to support@scrive.com.

Trust marks and certificates

Scrive AS is a Qualified Trust Service Provider (QTSP) in the EU/EEA, subject to the supervision of the Norwegian Communications Authority (NKOM).

Scrive AS is ISO 27001 certified. The trust service system undergoes an annual internal audit and is evaluated by a conformity assessment body at least once every 24 months to certify compliance with the eIDAS regulation and supporting standards.