Trust Service and Certification Practice Statement (TS/CPS) for Scrive Certified Trust Services

Version 1.4

Date 15 May 2026

Scrive AS
OSLO

scrive.

Ownership and version history

QTSP management board at Scrive AB

Date/revision	Author	Changelog
15 May 2026	Antti Kettunen, Linus Kilander Xu, Nicolai Rasmussen	Version 1.4 Added Trusted Roles & complaints procedure descriptions. Added more descriptive Termination Plan activities, personnel controls and identity verification sections. Replaced CRL references with OSCP.
31 Mar 2025	Björn Hesthamar	Version 1.3 Added support for certificate re-keying Added CertificateProfile version 1.3
4 Oct 2024	Björn Hesthamar	Version 1.2 Removed references to Norwegian BankID and issuing of certificates to Norwegian subjects. Amended ISO certification status.
2 Jul 2024	Björn Hesthamar	Version 1.1
14 Jun 2024	Björn Hesthamar	First published version 1.0
12 Jun 2024	Björn Hesthamar	Second draft 0.2
4 Apr 2024	Björn Hesthamar	First draft 0.1

scrive.

Introduction

Purpose

This trust service practice statement (TPS) describes policy and procedures that the Scrive Certified Trust Service is bound to. This policy is in compliance with relevant laws and regulations, including but not limited to the eIDAS regulation (EU) 910/2014.

Document Structure

Policy Administration

Policy Approval and Modification

This document is versioned and outlines the policy's applicability based on the issuance dates of certificates over a specified time interval. The information in this practice statement is compiled from TSP internal documentation.

The SCTS management body approves the Trust Service and Certification Practice Statement and certificate profiles.

All revisions that are implemented in SCTS are subject for such approval.

When Scrive plans to change its practice statement in a way that could affect how the service is accepted by the subject, subscriber, or relying parties, it publishes the updated practice statement, and notifies the supervisory body without delay.

Policy publication

This document and related certificate profiles are published at https://pki.scrive.eu/

Organisation administering the document

This document is administered by the Scrive TSP Squad. Please contact at pki@scrive.no.

scrive.

Introduction to Scrive Certified Trust Services

The Scrive Qualified Electronic Signature (QES) service provides a seamless and secure way for users of Swedish BankID to obtain a short-term qualified certificate and sign documents within the Scrive signing flow. This service ensures that your electronic signatures are legally binding and recognized across the EU.

How to Use Scrive QES Service

1. Review the Document - Begin by reviewing the document in the Scrive interface as you normally would. Ensure that all the information is correct before proceeding. This is done in the normal Scrive eSign service, outside of the Scrive Trust Service

2. Initiate Signing Process - If you decide to sign the document sent to you, click the "Continue to Sign" button at the bottom of the page. This will forward you to the **Scrive QES Trust Service interface**.

3. Accept Terms and Conditions - In the Scrive QES interface, you will be prompted to accept the Terms and Conditions for the Scrive QTSP (Qualified Trust Service Provider) signing service. Please read through these terms carefully and select the checkbox to accept.

4. Identification and Signing Process

For Swedish BankID Users

- A QR code will appear on the screen. Scan this QR code with your BankID app as you normally would.
- In the BankID app, you will see a text including the name of the document and the transaction number. You are prompted to ask if you would like to sign the document. Click "Sign" to proceed.
- The Scrive QES service will then create your Qualified Certificate. The Certificate is only valid for 15 minutes.
- The Scrive QES uses your “sign-click” as intent to sign and signs the document with your Qualified Certificate.
- The Qualified Certificate is then discarded.

5. Completion - After completing the signing process you will be forwarded back to the signed document in the Scrive eSign interface. A confirmation message will indicate that the document has been successfully signed.

By following these straightforward steps, you can easily and securely sign documents using the Scrive QES service with your Swedish BankID. This service ensures that your electronic signatures are compliant with EU regulations, providing peace of mind and legal certainty.

About Short-Term Qualified Certificates

Short-term qualified certificates are a crucial component of the Scrive QES service, providing an additional layer of security and trust for electronic signatures. These certificates are designed for single-use, meaning they are issued for signing one specific document only and cannot be reused for any other document.

The qualified short-term certificates created by the Scrive QES signing Trust Scrive are based on the information obtained from Swedish BankID. Each certificate is used for one identification and one signature only. The certificate expires immediately after the document is signed or after 15 minutes, whichever comes first.

The nature of short-term qualified certificates ensures that each signing instance is uniquely authenticated and secured. Due to their single-use and time-limited nature, there is no

opportunity for revocation. The brief validity period is sufficient to complete the signing process but does not extend long enough to necessitate revocation procedures. This characteristic enhances the efficiency and security of the signing process, ensuring that each transaction is both secure and streamlined.

In summary, short-term qualified certificates offer a robust and efficient means of ensuring document integrity and signer authenticity, perfectly suited for the fast-paced needs of modern digital transactions.

General Provisions

Overview of TSP Services

Scrive AS operates qualified and non-qualified trust services, Scrive Certified Trust Services (SCTS), in Norway. Scrive AS have contracted Scrive AB to provide infrastructure, development and service operations for SCTS, for the issuance of advanced and qualified certificates in order to provide advanced and qualified signatures as a service.

This document outlines the policies and procedures established to manage qualified certificates in compliance with the eIDAS Regulation.

Trust services

Scrive offers a comprehensive suite of services designed to manage the document lifecycle, including eSigning, eArchiving, and document offboarding. This document specifically addresses the PKI-based trust services provided by Scrive AS in accordance with the eIDAS regulation. Scrive's trust services are integrated into other Scrive services and may also be provided independently to third parties in the future.

Scrive trust services are typically offered in a B2B setting for remuneration where one legal entity acquires the right to use the trust service and invite signatories (natural persons) to have short term validity advanced and qualified certificates issued for single use advanced or qualified electronic signatures (AdES or QES). The certificates are managed by SCTS in the role of (Q)TSP on behalf of the certificate subject for the sole purpose of creating document or object signatures based on a DTBS/R. The DTBS/R is only released by the service on the condition that the private key for the certificate was successfully destroyed after successfully creating the signed DTBS/R.

Scrive trust services issue both advanced and qualified certificates with short-term validity, aligned with the eIDAS regulation. The advanced and qualified signing service share the same code base and operational principles but are operated as separate instances. The qualified instance of the service is audited by a conformity assessment body. Issued certificates are managed by a remote Qualified Signature Creation Device (QSCD) and enable natural persons to sign documents in services that integrate with Scrive trust services. Natural persons who possess the eIDs used for identity proofing can be issued an advanced or qualified certificate for document signing purposes.

Certificates are requested as a part of a user entering a signing flow in order to digitally sign a document with an advanced or a qualified certificate. The certificate issued is of short term validity (15 minutes) and will be used only once for signing one object. Then the certificate is then discarded and the private key destroyed.

scrive.

PKI Participants

Certification Authority

As a Certificate Authority, SCTS provides advanced and qualified certificates for use within its trust services. SCTS will:

- Follow the guidelines set out in this document (or any other disclosed CA business practices), which may be periodically updated,
- Issue and make available certificates quickly, as specified in this document,
- Revoke a certificate when a valid request is made by an authorised person, this is however not applicable for short term validity certificates,
- Make OCSP responder available, adhering to the relevant Certificate Policy and the details in this document,
- Enable subscribers to use their certificates for content commitment as described in this document,
- Without undue delay inform subscribers, relying parties and applicable authorities of any breaches of security or loss of integrity that are likely to adversely affect a natural or legal person to whom the trust service has been provided,

Certificate Subject

Natural person that will sign an object or document using a certificate created by the SCTS in relation with the service terms and conditions.

Relying parties

Before relying on the information in a digital certificate, relying parties must check the Online Certificate Status Protocol (OCSP) response to confirm that SCTS has not revoked the certificate. The location of the OCSP is specified in the certificate itself.

For qualified certificates (QC) before relying on the information in a digital certificate, relying parties must check the EU Trusted List to confirm that the SCTS Qualified Certificate issuer service is still a valid Qualified Trust Service. The trust anchor for the validation of the certificate shall be identified in a service digital identifier of the Scrive QTSP record.

Certificate usage

Permitted usage

Certificates outlined in this Trust Service Practice Statement are issued to subscribers for the purposes of electronic identification of end-users, content commitment (non-repudiation) signing and strong authentication.

Certificates are managed by SCTS on behalf of the user and can only be used to sign DTBS/R that is provided to the SCTS.

Prohibited usage

Applications utilising certificates issued under this Trust Service Practice Statement must adhere to the key usage purposes specified in the "Key Usage" extension field of the certificate.

The Scrive CA Service Signing Keys, which are used to generate subscriber certificates and issue revocation status information, must not be employed for any purposes other than those specified.

Compliance with Standards

Standards that are part of conformity assessment

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

- General Policy Requirements for Trust Service Providers (ETSI EN 319 401)
- Policy and security requirements for Trust Service Providers issuing certificates;
    - Part 1: General requirements (ETSI EN 319 411-1)
    - Part 2: Requirements for trust service providers issuing EU qualified certificates (ETSI EN 319 411-2)

Standards that are used for reference

- Certificate Profiles;
    - Part 1: Overview and common data structures (ETSI EN 319 412-1)
    - Part 2: Certificate profile for certificates issued to natural persons (ETSI EN 319 412-2)
    - Part 5: QCStatements (ETSI EN 319 412-5)
- Policy and security requirements for trust service providers;
    - Part 1: TSP service components operating a remote QSCD / SCDev (ETSI TS 119 431-1)

Certification Practice Statement for Scrive Certified Trust Services

Publication and repository responsibilities

Public certificates are made available to subscribers and subjects in the signed object or document. Public certificates are made available to relying parties as part of the signed object or document.

Terms and conditions are made publicly available on https://pki.scrive.eu/, this link is also included in the certificate.

Identification and Authentication

Identity Validation

Scrive's QES service is used by natural persons either as individuals or as representatives of organisations. Although businesses are a key customer group, the signing certificates are used to identify only natural persons, without connecting the natural person to a legal person they may represent. The identification of the legal person or the signatory affiliation with the legal person are not reflected in the certificate. For this purpose, Identity Verification includes only the scenario, where the signatory is a natural person, and is both the subscriber and the subject.

Identity verification is done based on Swedish BankID means under *Swedish eID (Svensk e-legitimation)* ,notified to eIDAS Substantial Level of Assurance.

SCTS does not support issuing certificates on behalf of another natural person other than the natural person identified in the certificate subject . It is always the subscriber that applies to have the certificate issued and it takes place after successful verification of the certificate creation request. The SCTS does only support issuance of certificates to the identity returned by the eID and therefore does not support issuance of certificates to pseudonyms of that identity.

scrive.

Certificate Life-Cycle operational requirements

Certificate Application

A user applies for a certificate at the time of accepting a request to sign a document. The application is generated and fulfilled by the service as the user signs the certificate application request. In accordance with ETSI TS 119 431-1 LNK-6.2.2-07.

The eID is validated and it is ensured that it was not expired, not revoked and not suspended at the time when the certificate creation request was issued. This ensures that the information in the identity and other attributes of the certificate subject are correct at the time of requesting certificate issuance. It also ensures that the request is attested by the correct source (the eID).

Certificate application processing

When a certificate creation is requested, the signatory is directed to the chosen eID endpoint (Swedish BankID) to sign the certificate creation request. The session with the eID is securely protected and verified, ensuring that the resulting signed payload originates from these eID endpoints. For the current version of the service, the eID must provide a level of assurance rated as *substantial* or higher.

This requirement, combined with the policy of issuing one certificate per signature, ensures sole control over the certificates and ability to sign.

The certificate application is processed to make sure that it is uniquely linked to the browser session that is established for the purpose of facilitating certificate issuance and electronic signing on behalf of the certificate subject. The signed data from the eID provider is independently verified by two separate functions, where one is managing the certificate issuance at the remote QSCD and one is managing the usage of certificates within the QSCD. If any of these services fails to validate the incoming certificate application, the certificate will either not be created or not used within the maximum lifetime of 15 minutes.

Certificate Issuance

Certificates are automatically issued when a subject has requested the creation of a certificate. The subscriber identification data is determined by the identification proofing service or European eIDAS compliant eID on level of assurance *substantial* or *high*. The certificate serial number is unique. Certificates are not issued that will have a validity beyond the CA certificate. Certificates are issued according to the identifiers NCP+ for advanced certificates and QCP-n-QSCD for qualified certificates.

Certificate Acceptance

All subscribers to the service accept the service terms and conditions before the certificate creation request is signed. Certificates are created in accordance with the associated Certificate Profile and populated with information that the certificate subject has already approved as part of accepting the eID that was previously issued in their name.

Key pair and certificate usage

Sole control of the private key is established through session management and single time use of the certificate for signing purposes. Only a certificate issued to a specific subject can be used to electronically sign a document or object in the same session. The private keys of the certificate will only be used in accordance with the limitations described in this document and the service terms and conditions. The private key of the certificate is maintained under subject sole control as ensured by the independent verification of eID means to enable use of the issued certificate.

scrive.

Certificate Renewal

The service does not support certificate renewal due the single use and short 15 minute lifetime of issued certificates.

Certificate Re-keying

The service uses re-keying if issuing a new certificate within an existing certificate validity period for the same subject. Apart from this automatic functionality the service does not support certificate re-keying.

Certificate Modification

The service does not support certificate modification due the single use and short 15 minute lifetime of issued certificates.

Certificate Suspension and Revocation

The Service does not support subject initiated certificate suspension and revocation due the single use and short 15 minute lifetime of issued certificates.

Certificate status services

An OCSP responder is made available and updated with issued, revoked or suspended certificates.

End of subscription

The service subscription is limited to the lifetime of the certificate and it is automatically terminated when the private key of the certificate is deleted, when the certificate validity lapses or when the certificate is first used to sign a document or object electronically.

Key escrow and recovery

The service does not support key escrow or recovery due the single use and short 15 minute lifetime of issued certificates.

Scrive CA Profile

		Scrive Advanced CA	Scrive Qualified CA
Field	**Details**	**Value**	
Version		2	
Serial Number		Unique integer determined by the CA	
Signature Algorithm		sha256WithRSAEncryption	
Issuer	*countryName*	FR	
	organizationName	ALMERYS	
	organizationalUnitName	0002 432701639	
	commonName	ALMERYS ROOT CA	
Validity		10 years	
Subject	*countryName*	NO	
	organizationName	Scrive AS	
	commonName	Scrive AS eSign CA Adanac	Scrive AS eSign CA Aceymac
Subject Public Key Info		RSA/4096	
Extensions	*basicConstraints*	critical=true value='true'	
	subjectKeyIdentifier	Not Critical value='SHA1 of subject public key'	
	authorityKeyIdentifier	critical=false value='SHA1 of issuer public key'	
	keyUsage	critical=true value=keyCertSign (5) and cRLSign (6)	
	authorityInformationAccess	critical=false value accessMethod=id-ad-calssuers accessLocation=:URL=http://pki.scrive.eu/CA/almerysrootca.cer	
	cRLDistributionPoints	http://pki.scrive.eu/CA/almerysrootca.crl	
Signature Algorithm		sha256WithRSAEncryption	

scrive.

Scrive Subject CA Profile

		Scrive Advanced Subject CA	Scrive Qualified Subject CA
Field	**Details**	**Value**	
Version		2	
Serial Number		Unique integer determined by the CA	
Signature Algorithm		sha256WithRSAEncryption	
Issuer	*countryName*	NO	
	organizationName	Scrive AS	
	commonName	Scrive AS eSign CA Adanac	Scrive AS eSign CA Aceymac
Validity		15 minutes	
Subject	*countryName*		
	organizationName	(optional)	
	commonName		
	givenName		
	surName		
	serialNumber	SerialNumber as per ETSI EN 319 412-1 semantics Identifier for natural persons and will follow either: ● Swedish PNOSE for Swedish personal number (national civic registration number)	
Subject Public Key Info		ECC/P256	
Extensions	*basicConstraints*	critical=true value=true	
	subjectKeyIdentifier	critical=false value='SHA1 of subject public key'	
	authorityKeyIdentifier	critical=false value='SHA1 of issuer public key'	
	keyUsage	critical=true value=contentCommitment(1)	
	certificatePolicies	critical=false value=NCP+(itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2))	critical=false value=QCP-n-qscd (Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2))
	qcStatements-2	Not applicable	critical=false value=esi4-qcStatement-1, esi4-qcStatement-6, QCType=id-etsi-qctesign, esi4-qcStatement-4,

			semanticsIdentifier: id-etsi-qcs-semanticsId-Natural, nameRegistrationAuthorities= https://pki.scrive.eu/ id-etsi-qcs-semanticsId-Natural, nameRegistrationAuthorities= https://pki.scrive.eu/ value=etsi-qcStatement-LimitValue: 100000 NOK, etsi-qcStatement-RetentionPeriod: 10 years, etsi-qcStatement-QcPDS: https://pki.scrive.eu/
	authorityInformationAccess	critical=false value accessMethod=id-ad-calssuers accessLocation=:URL= https://pki.scrive.eu/CA/a/scrive-signingsubca.cer	critical=false value accessMethod=id-ad-calssuers accessLocation=:URL= https://pki.scrive.eu/CA/q/scrive-signingsubca.cer
		value accessMethod=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL = http://a.ocsp.scrive.eu/	value accessMethod=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL = http://a.ocsp.scrive.eu/
Signature Algorithm		sha256WithRSAEncryption	

Facility, Management, and Operational Controls

General

Scrive AS is ISO 27001 certified and has a certified information security management system (ISMS). All assets are systematically managed in accordance with the ISMS. Risk assessment is performed and risks are systematically and periodically re-assessed.

Physical Security Controls

Scrive employs data centres and hosting facilities that adhere to strict standards with regard to physical security controls. Hosting locations are ISO 27001 certified and employ access controls, restricted areas, alarm and monitoring, access authorisations, visitor policies and regular audits.

Procedural controls

SCTS procedural controls involve rigorous security requirements analysis during system development, documented change control procedures, and systems hardening. These controls ensure that security is integrated into IT systems from the outset and maintained throughout their lifecycle.

Trusted Roles

The SCTS has assigned key people to Trusted Roles, who are responsible for the primary operational duties of the trust service. The following roles are set in the SCTS organization:

- **TSP Security Officer** holds overall responsibility for administering and overseeing the implementation of security practices within the Scrive QTSP/QES Service Scope. The Security Officer ensures that security controls, operational practices, and risk management measures are implemented and maintained in accordance with eIDAS and ETSI requirements.
- **TSP System Auditor** is authorized to review archives and audit logs of the TSP's trustworthy systems. The role is responsible for reviewing system activities, verifying adherence to approved procedures, and monitoring compliance with applicable standards.
- **TSP System Administrator** is authorized to install, configure, and maintain the TSP's trustworthy systems for service management.
- **TSP System Operator** is responsible for day-to-day operation of the TSP's trustworthy systems.
- **Registration and Revocation Officer** is responsible for managing certificate registration and revocation processes.
- **Validation Specialist** is responsible for performing validation activities required under applicable certificate policies, and ensuring compliance with identity and certificate profile requirements
- **Lead Developer** is responsible for the technical direction of QTSP/QES service development, ensuring that development practices support security and compliance requirements and coordinating implementation of approved changes.
- **Developer** is responsible for Implementation of software components within the QTSP/QES scope, secure coding practices and supporting validation and compliance requirements.

Personnel controls

Scrive has documented various personnel controls, including separation of duties and responsibilities across different locations and services within the organisation to prevent unauthorised access and enhance security.

The SCTS is designed so that key functions of the service are distributed between Scrive AS and its subcontractors. The obligations and responsibilities of each party in producing the SCTS are agreed and documented clearly. By separating key functions and data processing activities across different trusted services, we mitigate the risk of unauthorized tampering or alteration of critical data. The division of duties and data across multiple trusted services helps to safeguard sensitive information from unauthorized access or disclosure. This ensures that sensitive data remains protected from unauthorized parties, reinforcing the trustworthiness of our service provision.

Logging & monitoring

Scrive maintains comprehensive logging and monitoring to ensure the high performance, security, and legal integrity of its digital signature services. By centralizing data from diverse system layers, the infrastructure provides visibility into application health and user transactions while maintaining compliance with regulatory standards.

Logging is divided into three primary categories:

- **Diagnostic & Application Logs:** These logs capture the behavior and performance of internal software components to facilitate troubleshooting and optimization. They include detailed records of web traffic (e.g. tracking request sizes, status codes, and response times) to monitor the health of public-facing interfaces.
- **Transaction Event Logs:** Designed for legal compliance, these logs provide an immutable, chronological "single source of truth" for electronic signature processes. They record every critical step of a transaction, including creation requests, signatory interactions, and identity verification responses from external providers.

- **Infrastructure & Audit Logs:** These logs provide a detailed trail of system-level activity to ensure security and accountability.
    - **System Access:** Tracking user logins and the execution of privileged commands across servers.
    - **Configuration Changes:** Monitoring modifications to application settings and deployment statuses.
    - **Security Events:** Recording all interactions with central management interfaces, including resource access and internal system requests.
    - **Network Traffic:** Providing granular visibility into internal network flows to assist with security analysis and connectivity debugging.

Scrive employs monitoring of the production environment, including continuous checks on server clock synchronization, and threat detection that identifies suspicious behavior, such as configuration changes.

Records archival

Records and data related to the operation of the trust services are archived following regulatory requirements, with strict measures to ensure data integrity and confidentiality. The retention period is compliant with statutory obligations, and is set at 10 years.

Compromise and disaster recovery

Disaster recovery and complete redeployment of the service is tested every quarter. The Scrive trust service is transactional in nature, and certificates are of short term validity and never re-used for signing a document.

Business Continuity Management (BCM) and Disaster Recovery (DR) plans ensure the continuous operation and quick recovery of services during disruptions. The BCM strategy, aligned with ISO/IEC 27001 standards, focuses on maintaining the operational integrity of the Scrive Certified Trust Service (SCTS) and protecting critical internal and customer data through reliable backup processes.

The DR approach includes regular, secure backups of all production systems, stored offsite with encryption. These backups are retained in compliance with regulatory requirements and tested regularly to ensure they can be restored efficiently. We aim for an 8-hour Recovery Time Objective (RTO) and a 24-hour Recovery Point Objective (RPO), ensuring minimal data loss and downtime.

Scrive AS adopts a hybrid and cloud-first approach to enhance operational resilience. This strategy allows employees to work remotely or from alternative locations if primary facilities are unavailable. Any loss of information assets is promptly addressed with appropriate risk assessments and actions. This comprehensive BCM and DR framework supports the reliability and resilience of our services, maintaining trust among our stakeholders.

Certification Authority or Registration Authority Termination

SCTS have taken measures to implement a termination plan that ensures a smooth winding down of operations with minimal side effects for subscribers, certificate subjects and relying parties.

If the decision is taken to terminate the qualified trust services, the actions described below will be taken.

1. The supervisory body will be notified at least 60 days prior to the effective termination.
2. Customers, subscribers, resellers, and subcontractors will be notified at least 30 days prior to the effective termination.
3. All services used for certificate and signature issuance will be terminated no later than the termination date.
4. All currently issued and valid certificates will be revoked prior to the termination.

5. All cryptographic material used for the service will be erased or destroyed to make recovery impossible.
6. All relevant information concerning issued certificates and received data is archived for 10 years.
7. Certificate Revocation Lists will be kept accessible at pki.scrive.eu to allow for the validation of signatures created before termination.
8. If Scrive AS is unable to carry out points 6 and 7, a custodian will be appointed for which prior financial arrangements have been made for the required operation.

Technical security controls

Technical security controls at SCTS include logical access control, network segmentation, and firewalls to restrict access to necessary endpoints. Systems are isolated to protect against unauthorised access and to ensure data integrity.

Key pair generation and installation

Key generation and management are performed using trustworthy systems supporting server signing, certified devices and protocols to ensure security. The system employs Qualified Signature Creation Devices (QSCD) for subject certificate key management and HSMs for infrastructure key management.

Private key protection and cryptographic module engineering controls

Private keys are protected through rigorous cryptographic module engineering controls, ensuring that keys are generated, stored, and handled securely to prevent unauthorised access.

Other aspects of key pair management

The management of keys involves ensuring their integrity and security throughout their lifecycle, from generation to destruction after their single use within a 15-minute validity period. Issued cryptographic keys for Qualified Certificates are managed in a certified Qualified Signature Creation Device (QSCD). The management of the QSCD is done by a third party QTSP on behalf of Scrive AB. Key generation and storage for supporting services (infrastructure and encryption at rest of databases) is done in HSMs.

Activation data

SCTS relies on the validation of signed eID digests for signature activation.

Computer Security controls

Computer security for SCTS involves separate administrative and operational networks, hardened systems, and regular security assessments to mitigate risks and enhance the security posture. Different components of the Scrive Trust Service are separated into different security zones based on security profile. Interzone communication is kept to a bare minimum on a protocol level. Internet facing systems are hardened and separated by firewalls and load balancers enabling full segmentation between zones. The QSCD is utilised in accordance with vendor specifications.

Life cycle security controls

Life cycle security controls include the integration of security practices into all phases of system development and operational processes, from initial design to deployment and maintenance. Risk assessments are used to focus security efforts. It is ensured that the QSCD certification is valid at all times of service operation.

Operational Security Controls

Operational security controls include continuous monitoring, incident response protocols, and network security measures to safeguard the infrastructure and services from potential threats. Scrive AS trust services are monitored 24/7 by on-call engineers that manage resources and raise incidents based on system performance. Internet facing systems are hardened and separated by firewalls and load balancers enabling full segmentation between zones.

Separation of duties

The service is partitioned into two separate services each deployed at different locations under separate internal ownership and management within the (Q)TSP. These two services operate independently, without mutual trust, to verify eID-session authenticity and the advanced or qualified subject certificate creation request (signed data from eID) that is created when a subject expresses the intent to sign a document. The Remote-QSCD will only process requests that have been independently verified and validated by both services.

Logical Access Control

- The systems are segmented into networks or zones based on risk assessment. This segmentation considers the functional, logical, and physical relationships between trustworthy systems and services.
- Access and communications between zones are restricted to those necessary for the operation of the TSP (Trust Service Provider). Firewalls are implemented between each network zone to restrict access to only necessary endpoints.
- Separated administrative network plane. The network for administration of IT systems is separate from the operational network. For example, administrative functions of the Scrive EC environment are hosted in a separate infrastructure project on a separate management network.
- The production systems are separated from development and testing systems. For instance, the production network is connected to a separate virtual router that has no routing capabilities towards the staging environment.
- Communication between distinct trustworthy systems is established only through trusted channels that are isolated using logical, cryptographic, or physical separation. These channels ensure endpoint identification and protection of channel data from modification or disclosure.
- Firewalls and network policies are configured to prevent all protocols and accesses not required for the operation of the TSP. For example, network policies are used to restrict traffic to specifically allowed endpoints on a per Pod basis.
- For high availability, the external network connection is redundant to ensure service availability in case of a single failure.
- The established rule set is reviewed regularly, and the system undergoes regular vulnerability scans and penetration tests to identify and address potential security issues.

QSCD management

If the QSCD status is modified before the end of the validity period SCTS will take measures to ensure that a replacement QSCD can be put to use. If a smooth transition can not be ensured, SCTS will temporarily terminate services that depend on a QSCD. Any valid certificates depending on the QSCD during such a transition will be revoked.

Service development controls

- Security requirements analysis is conducted during the design and requirements specification phase of any systems development project undertaken by the TSP or on behalf of the TSP. This ensures that security is integrated into IT systems from the outset.
- Change control procedures are applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies the TSP's security policy. Changes are documented.

- Deployed systems are hardened and only components that are strictly necessary for the provisioning and operation of the services are part of the deployed systems.
- Client computers as well as all environments and networks used for producing and managing software and services are monitored and managed by Scrice IT.

Monitoring and Detection

System activities related to access, use, and service requests are continuously monitored. Any abnormal activities indicating potential security violations, such as intrusions, are detected and reported as alarms. SCTS monitors events like the start-up and shutdown of logging functions and the availability and utilisation of necessary services within the network.

Response and Mitigation

Upon detection of a potential security incident, SCTS responds promptly and in a coordinated manner to minimise the impact. Trusted personnel are appointed to follow up on critical security alerts and ensure relevant incidents are reported in accordance with established procedures.

Incident Reporting

SCTS has established procedures to notify appropriate parties of any security breach or loss of integrity that significantly impacts the trust service or personal data. Notifications are to be made within 24 hours of identifying the breach. If the incident adversely affects any natural or legal person, they must also be notified without undue delay.

Handling Vulnerabilities

Any critical vulnerabilities not previously addressed by SCTS are to be mitigated within 48 hours of discovery. A plan to address each vulnerability is created, or a rationale is documented if the vulnerability does not require remediation.

Documentation and Communication

All incidents and their resolutions are documented. A report is maintained, ready for submission at short notice, containing details such as the incident's occurrence, detection, affected services, personal data impacted, and countermeasures taken. Ongoing communication with SCTS Management Body is maintained throughout the incident response process.

Authority Reporting

Incidents are reported to the relevant authorities (e.g., Nkom in Norway) as soon as possible and no later than 24 hours after detection. Reports include detailed information as specified by regulatory guidelines. If necessary, the TSP Management Body signs the incident report before submission, but speed of reporting takes precedence over obtaining signatures.

Complaints procedure

The SCTS has a documented complaints procedure. The complaints procedure starts when a Customer Support Agent receives an issue and categorizes it as a formal complaint regarding the service. The TSP Security Officer oversees the process, which involves notifying key stakeholders (including Legal and Product Manager) for a detailed analysis and decision on validity. If valid, TSP Squad develops and implements a resolution plan to achieve a timely and documented closure, with a focus on continuous improvement.

Support information can be found at https://www.scrive.com/contact/.

Risk Management

Risks associated with the trust services are managed in line with Scrive ISMS. Flagged decisions and actions within the service's management and operations are assessed, monitored, and reviewed annually. This systematic review ensures that operational risk for the trust service remains low and under control.

scrive.

Compliance Audit Procedures and frequency

The trust service system undergoes an annual internal audit and is evaluated by a conformity assessment body at least once every 24 months. The purpose of these audits is to certify that the system complies with the requirements set forth in the eIDAS regulation and its supporting standards. Scrive AS is also ISO 27001 certified with a re-certification audit every third year and two consecutive surveillance audits in the intervening years.

Legal and Regulatory Considerations

Compliance with Laws

The eIDAS and local implementations in Norway and Sweden. General Data Protection Regulation and local implementations in Norway and Sweden.

Liability

Scrive AS, as a Qualified Trust Service Provider (QTSP), limits its liability for the Scrive Certified Trust Services (SCTS) in accordance with the eIDAS Regulation and these terms. Scrives liability for direct damages resulting from a failure to provide the SCTS shall not exceed NOK 100,000 per loss-making event, subject to the applicable limit specified in the user's licence terms. This liability does not extend to 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, issues with third-party services or products, or events beyond Scrives reasonable control (Force Majeure). Claims for damages must be brought within twelve months of the loss-making event. In cases of intentional acts or gross negligence, this limitation does not apply.

Scrives liability is presumed under the eIDAS Regulation unless it can demonstrate that the damage occurred without its intention or negligence. Users are advised to ensure compliance with their obligations and the requirements of the SCTS to mitigate any potential risks.

Code of conduct

In addition to subject specific policies and procedures, all employees of Scrive are bound by Scrive’s Code of Conduct, which includes principles regarding:

- Environment & Sustainability: Complying with applicable legislation, integrating sustainability, choosing eco-friendly subcontractors, and minimising waste and energy consumption.
- Ethics: Maintaining a culture of ethical conduct, with a commitment from senior leaders and all employees to uphold honesty, integrity, and ethical practices in all business activities.
- Labor & Human Rights: Respecting and promoting human rights in accordance with the UN Guiding Principles, prohibiting child and forced labour, and ensuring fair treatment and non-discrimination.
- Anti-Money Laundering and Anti-Bribery & Anti-Corruption: Complying with laws against money laundering and terrorist financing, prohibiting transactions that facilitate these activities, and maintaining a zero-tolerance policy towards bribery and corruption.
- Data Protection: Complying with data protection legislation, including GDPR, through dedicated teams, regular training, and adherence to privacy and security policies.
- Subcontractors: Conducting due diligence and ensuring subcontractors are assessed and approved according to Scrive's Sourcing Policy.
- Sanctions & Export Control: Complying with EU, US, UK, and UN sanctions and export controls, ensuring neither Scrive nor its customers are subject to sanctions.

- Standards & Certifications: Committing to international standards and certifications such as the UN Global Compact, EcoVadis, and ISO 27001 to uphold sustainability, security, and ethical practices.

Privacy and Confidentiality

Data Protection and confidentiality

Scrive AS, as a Qualified Trust Service Provider (QTSP) under the eIDAS Regulation, ensures compliance with data protection standards for both subjects and relying parties of the Scrive Certified Trust Services (SCTS). Personal data is processed in accordance with the EU General Data Protection Regulation (GDPR). Scrive acts as the data controller within the SCTS, even when operating as a data processor in originating applications. Processed data includes names, identification numbers, digital identifiers, document hashes, and signing metadata. Third-party services are used for identity verification and other supportive roles, with adherence to data protection standards. All collected data is retained for at least 10 years to meet statutory requirements, with measures in place to protect this data from unauthorised access and cyber threats. Relying parties are assured that SCTS processes maintain the integrity and confidentiality of electronic signatures and associated data.

Confidentiality Obligations

Scrive AS ensures the confidentiality of both the subject and relying parties within the Scrive Certified Trust Services (SCTS). All personal data processed, including names, identification numbers, and digital identifiers, is handled in accordance with the EU General Data Protection Regulation (GDPR). Scrive implements strict access controls and encryption measures to protect this data from unauthorised access and cyber threats. Third-party services involved in provisioning of the service are required to adhere to the same confidentiality standards. Scrive also commits to limiting data access to only those parties necessary for providing the SCTS and retains data for the legally required duration, ensuring it is securely deleted thereafter. These measures collectively ensure that the confidentiality of all parties involved is maintained throughout the data processing lifecycle.