Agency for Digital Government

DEN DANSKE STAT

Management of remote QSCD Practice Statement

Version: 1.0

Author: Danish Agency for Digital Government, Den Danske Stat

Date: 27-01-2026

Den Danske Stat Trust Services

Table of contents

Changelog

Version	Dato	Change description
1.0	27-01-2026	Created to reflect that with the amendment to the eIDAS regulation management of remote QSCD is qualified trust service.

1. Introduction

Den Danske Stat provides management of remote qualified signature creations device (QSCD) and qualified seal creations device as a qualified trust service. From this point forward only the term signature is used.

The qualified trust service is provisioned according to [eIDAS] and [CIR 2025/1567] which reference [ETSI TS 119 431-1] as the required standard used by qualified trust service providers operating a remote QSCD.

2. References

Term	Reference
[eIDAS]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[CIR 2025/1566]	COMMISSION IMPLEMENTING REGULATION (EU) 2025/1566 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards for the verification of the identity and attributes of the person to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued.
[CIR 2025/1567]	Commission Implementing Regulation (EU) 2025/1567 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the management of remote qualified electronic signature creation devices and of remote qualified electronic seal creation devices as qualified trust services.
[CIR 2015/1502]	COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
[Notification]	Reference to OJEU on MitID being as eID means under the notified scheme for level of assurance substantial and high: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202405468&qid=1731325587133
[ETSI EN 319 401]	ETSI EN 319 401, Electronic Signatures and Trust Infrastructures (ESI) General Policy Requirements for Trust Service Providers. v3.2.0, June 2025, ETSI ESI. **https://www.etsi.org/standards**
[ETSI TS 119 431-1]	ETSI TS 119 431-1, Electronic Signatures and Infrastructures (ESI) Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev, v1.3.1, December 2024, ETSI ESI. **https://www.etsi.org/standards**
[GRPS]	Den Danske Stat Practice Statement on General Security Requirements for Trust Service Providers.
[Profile]	Den Danske Stat Certificate Profile.
[CEN EN 419 241-1]	CEN EN 419 241-2, Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements, CEN, 2018.
[CEN EN 419 241-2]	CEN EN 419 241-2, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing, CEN, 2019.

Term	Reference
[CEN EN 419 221-5]	CEN EN 419 221-5, Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services, CEN, 2018.
[ETSI TS 119 461]	ETSI TS 119 461, Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects, v2.1.1, February 2025, ETSI ESI. **https://www.etsi.org/standards**
[NSIS]	National Standard for Identiteters Sikringsniveauer (NSIS), Agency for Digital Government, version 2.1, June 2024. https://digst.dk/it-loesninger/standarder/nsis/
[MitID IdV]	Certificate(s) for MitID and MitID Erhverv meeting requirements in [ETSI TS 119 461] for Extended LoIP.
[QSCDs]	List of certified qualified signature creation devices. **https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd**
[ALGO]	European Cybersecurity Certification Group, Sub-group on Cryptography: 'Agreed Cryptographic Mechanisms' published by the European Union Agency for Cybersecurity. https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en

3. Definitions and abbreviations

For definitions, terms, symbols, abbreviations and notations the reader is directed to the references, in particular [ETSI EN 319 401], [ETSI TS 119 431-1] and [CEN EN 419 241-1].

4. General concepts

4.1. General policy concepts

This document is part of several practice statements provided by Den Danske Stat. In particular the document [GRPS], which describes how Den Danske Stat meets general policy requirements for trust service providers as stated in [ETSI EN 319 401]. This document follows the same convention as the other practice statements for the services offered by Den Danske Stat and reference the [GRPS] for general practice considerations. As such this document can focus on the service specific topics related to [ETSI TS 119 431-1].[ETSI TS 119 431-1]

The management of a remote qualified signature creation device is part of other qualified trust services offered by Den Danske Stat as a qualified trust service provider under the eIDAS regulation [eIDAS].

This document is organised as [ETSI TS 119 431-1] with same [ETSI TS 119 431-1][ETSI TS 119 431-1]clause numbers, to aid the reader knowing the standard. Since this service is to follow the policy EUSPv2 described in [ETSI TS 119 431-1], chapter 7 of the standard is not applicable. Instead, the Annex from the standard appears as chapter 7 in this document.

4.2. Void

This section is added to have the same numbering as [ETSI TS 119 431-1].

4.3. SSAS applicable documentation

4.3.1. SSAS practice statement

In Commission Implementing Regulation [CIR 2025/1567], the EU Commissions supplements requirements in [ETSI TS 119 431-1]. These additional requirements are valid from August 19, 2027. Den Danske Stat QTSP however, already meets the requirements: OVR-6.1-04, OVR-6.8.5-02 and OVR-A.3-02.

4.3.2. SSAS policy

See clause 5.2 for information on the policy used by the TSP for management of a remote qualified signature creation device.

4.3.3. Terms and conditions

See clause 6.8.4 for terms and conditions.

4.3.4. SSAS component services

In [ETSI TS 119 431-1] the SSAS component is divided into a series of sub-components for the purpose of classifying requirements. For Den Danske Stat SSAS the relevant sub-components are:

- Signing key generation service: generates signing keys in the remote qualified signature creation device and produces a proof of possessions. The proof of possession, being a certification signing request is provided to the QTSPs certificate generation service.
- Certificate linking service: establishes a verifiable association between a certificate generated by the certificate generation service of the QTSP and the specific corresponding key within the remote qualified signature creation device.
- eID means linking service: links an eID means references with the corresponding signing keys in order to provide sole control
- Signature activation service: collects and verifies signature activation data and activates the corresponding signing key within the remote qualified signature creation device to create a single digital signature.
- Signing key deletion service: destroys signing keys in a way that ensures that the signing keys cannot be used anymore.

The SSAS used several identity providers for providing it's services.

- MitID and MitID Erhverv are conformity assessed,[MitID IdV], to meet the requirements in [ETSI TS 119 461] for identity verification on Extended LoIP and is used to issue qualified certificates and OCES certificates.
- For Local IdPs which are conformity assessed to meet the requirements in [ETSI TS 119 461] for identity verification on Extended LoIP they are used to issue qualified certificates and OCES certificates.
- For Local IdPs which are audited/conformity assessed to meet requirements in [NSIS] they are used to issue OCES certificates and create advanced signatures.

The subject attributes which the SSAS receives from an identity provider must be protected in integrity with a cryptographic key which is protected and used within a cryptographic module.

The SSAS does not provision any eID means but relies on existing eIDs through the NemLog-in Broker. The NemLog-in Broker uses either MitID as eID or a Local IdP for subject authentication. Once the user has been authenticated, MitID Business is consulted for specific subject attributes associated to potential organizations.

The system is prepared for adding other identity providers. In this case, the identity providers are checked to meet the applicable requirements in the regulation [eIDAS].

In the future other eIDs may be added to the solution. For instance, this could be eID Gateway[1] or Digital Identity Wallets.

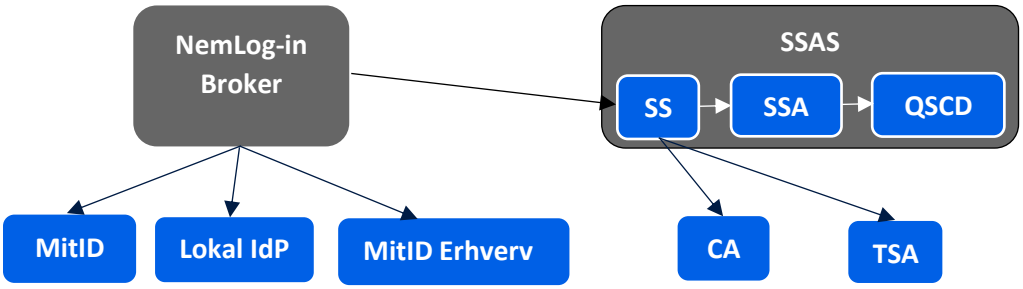
SSAS comprises of:

- Signing service (SS)

[1] https://digitaliser.dk/eid-gateway

- Server signing application (SSA)
- Qualified Signature Creation Device (QSCD)

The SSAS leverage of the of identity providers and PKI.



5. General provisions on practice statement

5.1. Practice statement requirements

Consult [GRPS] clause 6.1 for general considerations on practice statement.

See clause **Fejl! Henvisningskilde ikke fundet.** on the use of cryptographic algorithms.

5.2. SP Name and identification

The TSP conforms to the EU SSAS policy, [ETSI TS 119 431-1], identified by:

itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd-v2 (4)

5.3. Participants

5.3.1. SSASP

For general concerns on participants, consult the [GRPS], clause 4.2.

5.3.2. Subscriber and signer

For general concerns on subscriber and subject, consult the [GRPS], clause 4.2.

6. Trust Service Provider practice

6.1. Publication and repository responsibilities

Den Danske Stat provides a repository with applicable practice statements and terms and conditions for use of its services.

The terms and conditions are made available to the subject for every signing or seal key created by the SSAS. The subject is required to approve them before the key is generated.

The repository is made publicly and internationally available 24/7 at **https://www.ca1.gov.dk/**

Den Danske Stat may limit international availability without notice for cyber security reasons.

6.2. Signing key initialization

6.2.1. Signing key generation

The SSAS uses a cryptographic device certified against [CEN EN 419 221-5] with a SAM certified against [CEN EN 419 241-2]. Both standards describe Common Criteria protection profiles meeting EAL 4 augmented by AVA_VAN.5. The cryptographic device is dedicated to the Signer Server Application.

The initialisation of the cryptographic device, preparation of the SAM and the SSAS initialisation is conducted under dual control in the secure room facilities using appropriate procedures.

All private and secret keys are generated by HSM.

The algorithms for key generation and usage supported by the SAM is described in the manufacturers Security Target. The SSAS is configured to only support the use of Elliptic Curve Cryptography on the NIST recommended curve P-256 with ECDSA with SHA256 as signature algorithm. Change of signature algorithm can be conducted through administrative procedures.

Cryptographic keys are stored outside the cryptographic module. When keys are outside the module, they are protected in confidentiality and integrity by the cryptographic module and always encrypted by internal keys within the module.

The discrete logarithm problem on the NIST recommended curve P-256 is a recommended scheme [ALGO].

The signature keys for the SSAS are only used in one session for one signature operation and lifetime, see [Profile], of signing key is not a concern. Pre-generated keys are not used. All signature keys are using the same configuration of the SAP and SAD.

All subject certificates used by the SSAS are issued by the Den Danske Stat certification service.

The signature flow ensures that the subject is presented with the document to be signed and approves the signature operation.

The signature flow ensures that the subject is presented with the document to be signed and approved signature operation.

6.2.2. eID means or identity linking

MitID has been notified [Notification] to the EU Commission to meet the requirements in regulation [eIDAS] and [CIR 2015/1502] for assurance level substantial and high. In addition the registration process of MitID has been conformity assessed to meet the requirements in [ETSI TS 119 461] for extended LoIP, which by [CIR 2025/1566] meets the requirement for identity validation for issuing advanced and qualified certificates for natural persons.

MitID Erhverv has been audited to meet the requirements in [NSIS] for assurance level substantial. This covers the requirements in [CIR 2015/1502]. In addition the registration process of MitID Erhverv has been conformity assessed to meet the requirements in [ETSI TS 119 461] for extended LoIP, which by [CIR 2025/1566] meets the requirement for identity validation for issuing advanced and qualified certificates for natural persons associated to a legal person and for issuing advanced and qualified certificates to legal persons.

When using the rQSCD it is always linked to the eID means. The SSAS uses a similar approach to reference the subject at the eID as for certificate subject serial number [Profile].

The SAM used by SSAS is conformant to protection profile [CEN EN 419 241-2]. In the protection profile, the Security Functional Requirement FDP_ACF.1/Signing describes that only a key which is assigned to the intended user can be used for signing.

The NemLog-in Broker uses cryptographic modules to protect keys used to authenticate the entity towards the SSAS. MitID uses cryptographic modules to protect keys used to authenticate the entity towards the NemLog-in Broker. Local IdPs, which are conformity assessed to meet the requirements in [ETSI TS 119 461], use a cryptographic module to protect keys used to authenticate the entity towards the NemLog-in Broker.

6.2.3. Certificate linking

When the SSAS requires a key pair for a signing, the SSA requests the SAM to generate a key pair, assign it to the signer and generate a certificate signing request (CSR). The CSR is returned to the SSAS and from there it is submitted to the CA for certificate issuing. The issued certificate is returned to the SSAS which then sends it to the SAM which links the certificate to the signing key.

As pr. the design of the flow, signature keys cannot be used before they are linked with a certificate.

The linking of the certificate and the signing key is enforced by the SAM.

6.2.4. eID means provision

The SSASP does not provide any eID means.

6.3. Signing key life-cycle operational requirements

6.3.1. Signature activation

The SSAS requires a subject to be authenticated by an eID before a key pair is generated for the subject, a certificate is issued and a signature created. See clause **Fejl! Henvisningskilde ikke fundet.** on how the SSAS uses an eID means.

The use of eIDs which meet the requirements in [CIR 2015/1502] with assurance level at least substantial ensures communication protocols resistant against attackers with at least moderate attack potential. In addition to the communication protocol, the protection of the electronic identification means is carried out such that it can be assumed to be under sole control of the person to whom it belongs.

The communication between the SIC and the SAM is encrypted.

The Server Signing Application uses a SAM certified against [CEN EN 419 241-2] which provides assurance that only the legitimate signer can access own signing key. Access to other objects than signing keys is only permitted for system operators. The SAM verifies the SAD prior to the signature operation and enforces that a signature operation is only carried out on the supplied DTBS/R ([CEN EN 419 241-2], FDP_ACF/Signing).

The SAD used by Den Danske Stat only contains the (one) DTBS/R, which is linked to the document to be signed. The SAD is not stored by the SSAS after the signature operation is completed.

6.3.2. Signing key deletion

Signing keys can only be used for one signature operation signing one DTBS/R. The signing key is automatically deleted when the signature session is completed which is well before the expiration, see [Profile], of the public key certificate.

The SSAS does not provide a mechanism for the user to delete a signing key as it only exists during the signing session.

Den Danske Stat has backup and recovery procedures for its systems, including backup of the SSAS and the cryptographic keys it manages. It is practically not feasible to delete individual signing keys from backup.

6.3.3. Signing key backup and recovery

The SSAS stores all private and secret keys encrypted in a database. The keys are encrypted by a key which remains in a cryptographic device. Private or secret keys are not exported from the SSAS.

Backup, storage and restoration of any backup including keys persisted in the cryptographic module are performed by authorized personnel.

Den Danske Stat has backup and recovery procedures for its systems, which are designed to meet the service availability requirements.

6.4. Facility, management, and operational controls

6.4.1. General

See [GRPS] clauses 5, 6.3 and 7.3 on general considerations on facility, management and operational controls.

6.4.2. Physical security controls

See [GRPS] clause 7.6 for general considerations on physical security controls.

6.4.3. Procedural controls

See [GRPS] clause 7.4 for general considerations on procedural controls.

Every administrator of the Server signing application has an asymmetric key pair, which is used to sign administration commands send to Server signing application, which uses the SAM to verify these commands before any action can take place. For commands which require two administrators, two signatures on the command are required. The key pair is generated and persisted on a smart card and requires a user chosen password to be activated.

The administrator logs on to the smart card to activate the key pair for signing commands. There are no limitations on how many commands that can be signed. If the card is extracted from the reader, credentials are required to activate that key pair again. There is a session timeout of one hour between the administration client and the Signer server.

The smart cards used by administrators to log on to the Server signing application administration client keeps a counter of failed password attempts. When the counter exceeds 5, the smart card is locked and can't be unlocked. For the administrator with the locked card to get access the Administration Client, the administrator should be enrolled again and provided with a new smart card.

6.4.4. Personnel controls

See [GRPS] clause 7.2 for general considerations on personnel controls.

6.4.5. Audit logging procedures

See [GRPS] clause 7.10 for general considerations on audit logging procedures.

The SSAS uses a Server Signing Application which audit log includes the following items:

- System events. System initialization. Server start-up and shut-down.
- Administrator user events. Creation, management, and destruction of administrator users, including failed operations.
- Authentication events. Administrator users signing in and out of the administration client. Authentication of administrator users by verification of command signature. Failed authentication attempts.
- System management. Modification of configuration and system settings. Administration of system keys, policy administration, management of IdP, and failed management operations are logged as well.

- Events pertaining to the logs. Failure of MAC check to verify audit log consistency. Log purge and export for audit and usage logs.

The Server Signing Application audit records includes:

- Date and time of event;
- Type of event (server or user);
- Identity of the entity (e.g. user, administrator, process) responsible for the action;
- Success or failure of the audited event.

The Server Signing Application stores audit records in the database, which can only be accessed by authorized persons.

The Server Signing Application appends audits records and chains the elements, such that removal and modification can be detected by the server. It is supported that audit records can be archived to an external media and then deleted from the database.

In case the Server Signing Application does not have access to the database, all administrative and service calls to the server will fail.

The audit records are protected with a cryptographic value, such that any modification can be detected. The integrity of the audit records within the database can be verified through the Administration Client.

The log entries never contain data that can be used for retrieving sensitive data and does not include sensitive security parameters.

Server Signing Application is connected to the same time source as Den Danske Stat qualified time stamping service.

The Server Signing Application provides search using filters which allow specification of a search criteria. Only administrations who are authorized may use the search function.

Den Danske Stat logs all events related to security.

6.4.6. Records archival

See [GRPS] clause 7.10 for general considerations on Records archival.

Audit records can be exported to external media. Before exporting, the log entries are validated for integrity by the Server Signing Application. The exported entries are saved to an UTF-8 encoded text file including header and tab-delimiter. A hash (SHA-256) is calculated and shown on the screen when the export is completed. The hash is protecting the exported log - any changes to the exported file will cause further hash verification to fail.

Each log entry contains basic information about the event that occurred such as description and time stamp.

Den Danske Stat retains audit logs for at least 10 Years.

6.4.7. Key changeover

Den Danske Stat changes infrastructure keys based on a risk-based approach.

6.4.8. Compromise and disaster recovery

See [GRPS] clauses 7.9 and 7.11 for general considerations on compromise and disaster recovery.

6.4.9. SSASP service termination

See [GRPS] clause 7.12 for general considerations on service termination.

6.5. Technical security controls

6.5.1. Systems and security management

The SSAS supports both privileged and non-privileged roles. Each role has different privileges. The trusted roles include security officers, admins, operators and auditors performing critical activities following pre-defined and approved procedures.
The SSAS supports the following non-privileged role:

- The Signer is designated the subject of the certificate and is authorized through the provision of Signature Activation Data (SAD) to sign documents etc.

Signature requests are provisioned through the SAP from the SIC to the SAM. The SAM manages the certificates and key-pair on behalf of the Signer. The SSAS is designed to receive DTBS/R request from the user through the SAP and forwards the requests and responses to the SAM.
The SSAS is managed and operated under the TSP trusted roles regime and dual control preventing privileged users from having more than one role at the time and not allowing privileged user to take any roles alone. Following the TSP trusted roles regime credentials are only assigned to roles and qualified Individuals allowed to assume the role when on-site and under dual control.

In the SSAS the privileged user and non-privileged users use two different authentication schemes. Privileged user uses the administration interface and uses an approach where each administrative request is signed by a key controlled by the privileged user.

Non-privileged user, signers, use the SAP to authorize a signature operation.

The role configuration of the SSAS is designed to ensure that privileges for the different roles are not mixed. This is enforced by the SAM used by the SSAS and explained in the Security Target provided by the SAM certification.

6.5.2. Systems and operations

The SSA manufacturer has provided the necessary instructions for the development of a local operational handbook for the SSA. The SSA instance is deployed in a clustered set-up only physically accessible from inside a secure environment or through the SSAS through a network connection. Scheduled backups of

configuration and the Cryptographic Modules are stored inside secure room on NFS files system. Instead of Antivirus/Anti malware the applications are protected from access via Firewall rules, and can only be operated within the secure room.

The documentation provided by the SSAS manufacturer includes the required

- Installation Guidance;
- Administration Guidance;
- User Guidance.

The SSAS uses a NTP connection to a timeserver, which is the same as the QTSPs Time Stamp Authority.

6.5.3. Computer security controls

See [GRPS] clause 7.4 for general considerations on computer security controls.

Audit and usage logs are written to splunk which is monitored for abnormal behaviour.

6.5.4. Life cycle security controls

See [GRPS] clauses 7.7 and 7.14 for general considerations on life cycle security controls.

6.5.5. Network security controls

See [GRPS] clause 7.8 for general considerations on network security controls.

6.6. Complaince audit and other assessment

See [GRPS] clause 7.13 for general considerations on compliance.

No policy requirement.

6.7. Other business and legal matters

6.7.1. Fees

No policy requirement.

6.7.2. Financial responsibility

See [GRPS] clause 7.1 for general considerations on financial responsibility.

No policy requirement.

6.7.3. Confidentiality of business information

No policy requirement.

6.7.4. Privacy of personal information

See [GRPS] clause 7.13 for general considerations on privacy of personal information.

6.7.5. Intellectual property rights

No policy requirement.

6.7.6. Representations and warranties

No policy requirement.

6.7.7. Disclaimers of warranties

See clause 6.7.6.

6.7.8. Limitations of liability

Limitations on liability are covered in the terms and conditions as per clause 6.8.4.

6.7.9. Indemnities

No policy requirement.

6.7.10. Term and termination

No policy requirement.

6.7.11. Individual notices and communications with participants

No policy requirement.

6.7.12. Amendments

No policy requirement.

6.7.13. Dispute resolution procedures

No policy requirement.

6.7.14. Govering law

Not in the scope of the present document.

6.7.15. Compliance with applicable law

See [GRPS] clause 7.13 for general considerations on compliance with applicable law.

6.7.16. Miscellaneous provisions

No policy requirement.

6.8. Other provisions

6.8.1. Organizational

See [GRPS] clause 7.1 for general considerations on organizational.

6.8.2. Additional testing

No policy requirement.

6.8.3. Disabilities

See [GRPS] clause 7.13 for general considerations on disabilities.

6.8.4. Terms and conditions

See [GRPS] clause 6.2 for general considerations on terms and conditions.

7. Specific requirements related to Regulation (EU) 2024/1183

7.1. SSASP as a Qualified TSP

This section specifies generally applicable policy and security requirements used for Den Danske Stat for managing the remote QSCD.

7.2. Policy name and identification

See clause **Fejl! Henvisningskilde ikke fundet.**.

7.3. General requirements

This practice statement covers all requirements in [ETSI TS 119 431-1] for the NSP policy.

The SSAS uses a qualified signature creation device, which has been certified to meet the requirements in [CEN EN 419 241-2] and appears on the list of remote qualified signature creation devices managed by a QTSP [QSCDs]. The configuration and management of the device follow the manufacturer's guidelines. The certification report has not identified any special requirements.

7.4. Signing key generation

See clause **Fejl! Henvisningskilde ikke fundet.** on Signer's signing key generation.

Se clause 7.3 on operation according to the guidance documentation.

7.5. Signature activation

See clause **Fejl! Henvisningskilde ikke fundet.** on Signer's signing key generation and protection.

See clause 7.3 on operation according to the guidance documentation.

The SSAS relies on evidence from the identity providers, MitID or Lokal IdP. Authenticator factors are provided between the user and the identity provider and not through the SAP. It is only evidence that authentication has taken place which is provided from the identity provider including the level of assurance and attributes related to the subject. The information is protected in integrity and confidentiality. The communication between the user and the identity provider is protected against replay and bypass, and since messages are encrypted, protection against forgery is ensured.

The SAP is an encrypted protocol, which resists against replay, forgery and bypass. The SAD is protected in integrity such that any modification will be detected by the SAM. The communication between the browser

and SAM is encrypted and provides protection as such against eavesdropping, hijacking and man-in-the-middle. Standard techniques are used to protect against replay.

7.6. Signature activation data management

The SAD is only issued after the user is authenticated by an NSIS audited identity provider. The assurance level for the authentication must be at least substantial.

The SAD is generated by the NemLog-in Broker and provisioned to the signer's environment, where it is collected and provisioned to the SAM through the SAP.

The SAD includes the DTBS/R and elements to identify the signer within the SSAS. The SAD is protected with a digital signature such that it can't be modified during transmission. The digital signature is verified by the SAM as described in [CEN EN 419 241-2], FDP_ACF.1/Signing step 1 which requires the SAD to be verified in integrity.

7.7. eID means linking

See clause 4.3.4 regarding the use of eIDs by the SSAS.