CPS- PRACTICE STATEMENT
MSG MYSAVEID GMBH QUALIFIED TRUST SERVICES

Dokumenteninformationen

Version:	1.0
Datum der Version:	13.06.2024
Status:	☐ in Bearbeitung seit: ☐ vorgelegt am: ☒ akzeptiert/abgeschlossen
Classification:	öffentlich
Language:	<Englisch>
Autor:	Christoph Thiel
Name oft the file:	PRACTICE STATEMENT MSG MYSAVEID GMBH QUALIFIED TRUST SERVICES
Englischer Titel:	PRACTICE STATEMENT MSG MYSAVEID GMBH QUALIFIED TRUST SERVICES
Contact person:	Karsten Treiber
Effective date:	With the official certification of the BNetzA
Last review date:	13.06.2024
Next review date	13.06.2025

Dokumentenhistorie

Datum	Version	Änderungsgrund	Bearbeiter (Kürzel)
02.01.2024	V0.8	Erste Fassung	NB, TS, PK, CT
13.06.2024	V0.9	Angepasste Version	NB
13.06.2024	V1.0	Akzeptiert	KTR

Inhalt

1 Introductions

This document, hereinafter referred to as the “Policy and Practice Statement” or short “CPS” is used by msg mySaveID GmbH (hereinafter “mySaveID”) to provide qualified, trusted services comprising:

1. the issuance of **public key qualified certificates for electronic signatures and seals**, including registration of **subscribers and subjects**, certification of public keys
2. the **revocation** of certificates and online status information
3. generating and managing electronic signature creation data on behalf of the Subject (signatory)
4. processing certificate subjects' data for certificate issuance, other trust services, and provision of eID means.

mySaveID is a reliable service provider respecting:

a) The Act on Trust Services and Electronic Identification of 5 September 2016 (Journal of Laws of 2016, item 1579), hereinafter the “Trust Services Act”
b) Regulation (EU) No 2024/1183 of the European Parliament and of the Council of 20 May 2024, hereinafter the “eIDAS 2.0”
c) 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, hereinafter the “eIDAS”
d) Vertrauensdienstegesetz (VDG) vom 18. Juli 2017 (BGBl. I S. 2745) ((German Trust Services Act)
e) Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter the “GDPR”
f) Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), Stand: zuletzt geändert durch Art. 10 G v. 23.6.2021 I 1858; 2022 I 1045 (German Federal Data Protection Act)
g) Appropriate Executive (implementing) provisions to these above regulations.

The structure and contents of this document complies with the RFC 3647 Internet standard “Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practice Framework”.

This Policy also fulfils the role of the Certification Practice Statement.

It fulfills also the requirements of the:

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

4. ETSI TS 119 432: "Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation".
5. ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
6. ETSI TS 119 431-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation"
7. ETSI TR 119 411-4: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 4: Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2"
8. ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
9. ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".
10. ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for certificates issued to natural persons".
11. ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for certificates issued to legal persons"
12. EN 419 241-1: "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements", produced by CEN
13. EN 419 241-2: "Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing", produced by CEN.
14. EN 419 221-5: " Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services",

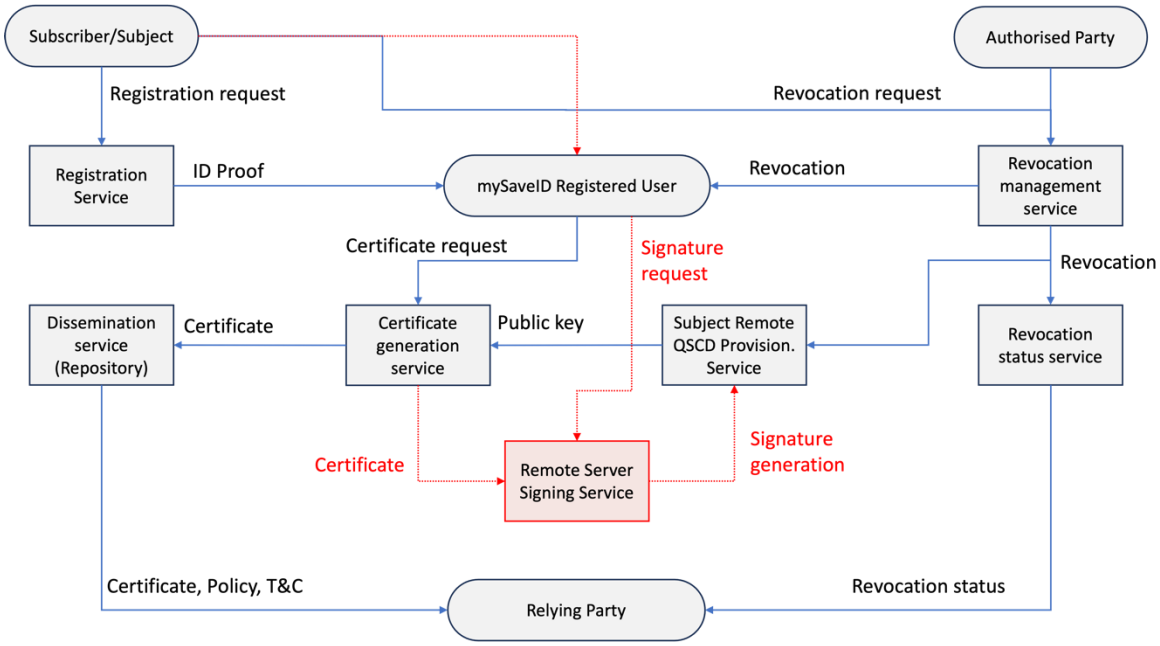
In order to provide services as a trust service provider, mySaveID uses services of other companies of the msg group of companies. In particular, mySaveID has outsourced the technical data center operation and the functional operation of the mySaveID application for the trust services to msg services GmbH. Data center and services are certified according to ISO 27001 and ISO 27017. There are contractual regulations for coordinated incident management and disaster recovery. Also mySaveID uses the services of an external certified certified identification service provider” (of the AUTHADA is) by the BSI

All suppliers used by mySaveID for providing trust services have been obliged by mySaveID to fulfill the requirements of this policy as well as to comply with the security and data policies and requirements of mySaveID. This includes also all other parties, including trust service component providers, to provide parts of its service through subcontracting, outsourcing or other third party arrangements. In any case mySaveID as TSP maintains overall responsibility for meeting the requirements defined in the trust service policy.

1.1 Overview

This policy covers the provision of qualified trust service issuance in accordance with eIDAS.

The following diagram shows the mySaveID Qualified Trust Service components – general overview:



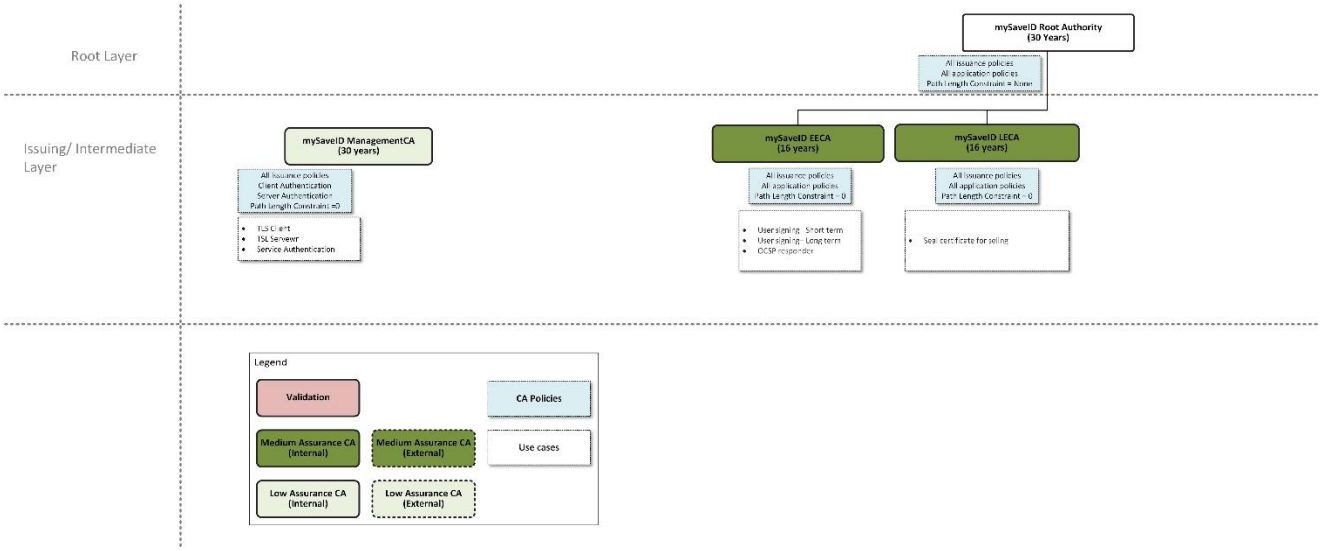
The trust services provided by mySaveID are logically broken down into the following component services for the purposes of addressing requirements stated in clause 4.3 of ETSI EN 319 411-1. 1

- **Registration service**: verifies the identity and if applicable, any specific attributes of a subject. The result of this service is identity proof creating an entry in the catalog of mySaveID registered users.
- **Certificate generation service**: creates and signs certificates based on the identity and other attributes verified and stored in the catalog of mySaveID registered users. This includes key generation.
- **Dissemination service**: disseminates certificates to subjects, and if the subject consents, makes them available to relying parties. This service also makes available the TSP's terms and conditions, and any published policy and practice information, to subscribers and relying parties.
- **Revocation management service**: processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the revocation status service.

- **Revocation status service**: provides certificate revocation status information to relying parties and other components.
- **Remote QSCD Subject device provision service**: manages QSCD on behalf of the subject, generates keys and creates signatures.

This subdivision of services is only for the purposes of clarification of practice statement and trust service policy and places no restrictions on any subdivision of an implementation of the TSP's services.

The following diagram represents the PKI hierarchy of mySaveID:



Certificates issued by mySaveID are compliant with the EU- qualified policies QCP-N, QCP-L, QCP-N-QSCD, QCP-L-QSCS.

1.2 Document Name and Identification

The full name of this document is „Practice Statement – mySaveID Qualified Trust Services". This document is available in an electronic version at:

- https://mysaveid.de/repository

The CPS can be identified by any party through the following OID:

1.3.6.1.4.1. 61029.1.1

1.3 PKI Participants

The eIDAS is a European Union regulation that establishes a framework for electronic signatures, electronic identification, and other trust services provided by trust service providers. Services described by the present document fulfill the requirements of the eIDAS regulation to all participants described below:

- Certification authorities

- Registration authorities
- Subjects and subscribers
- Relying parties
- Supervisory body
- Other participants
- Customer od the TSP mySaveID

The Service Provider mySaveID provides its services in accordance with the principle of nondiscrimination.

1.3.1 Certification authorities

Certification authorities (CAs) are operated by the trust service provider (TSP) and issue certificates and revocation lists.

There are the following root certification authorities of mySaveID (Root CAs):

- mySaveID Root Authority

CA Certificate	
Parameter	**Value**
proper name / naming convention	mySaveID Root Authority
Key size	4K
signature algorithm	SHA256RSA
Validity period of the certificate	30 years
subject	CN = mySaveID Root Authority, O = mySaveID GMBH, 2.5.4.97 = HRB-127516, C = DE
basic constraints	Subject Type=CAPath Length Constraint=1
key usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Distribution points	n/a
CRL distribution points	n/a

The Root CA are physically decoupled as a USB device and stored in a safe in the high-security room with dual access control. There it is only activated (physically isolated from the normal operations) when required to generate new certificates for the operating CAs.

There are the following operational certification authorities of mySaveID (CAs):

- mySaveID EECA
  The certification authority issues both personal certificates for natural persons and certificate revocation lists.

CA Certificate	
Parameter	**Value**
proper name / naming convention	mySaveID EECA
Key size	4K
signature algorithm	SHA256RSA
Validity period of the certificate	16 years
subject	CN = mySaveID EECA, O = mySaveID GMBH, 2.5.4.97 = HRB-127516, C = DE
basic constraints	Subject Type=CAPath Length Constraint=0
key usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Distribution points	n/a
CRL distribution points	n/a

- mySaveID LECA
  The certification authority issues certificates for legal persons and certificate revocation lists.

CA Certificate	
Parameter	**Value**
proper name / naming convention	mySaveID LECA
Key size	4K
signature algorithm	SHA256RSA
Validity period of the certificate	16 years
subject	CN = mySaveID EECA, O = mySaveID GMBH, 2.5.4.97 = HRB-127516, C = DE
basic constraints	Subject Type=CAPath Length Constraint=0

key usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Distribution points	n/a
CRL distribution points	n/a

Depending on their features, the certificates generated by the operational CAs can be assigned to the requirements of the different policies (certification level) within EN 319 411-2:

- QCP-n-qscd – EU qualified certificates issued to a natural person with private key related to the certified public key in a QSCD.
- QCP-l-qscd – EU Qualified certificates issued to legal person with private key related to the certified public key in a QSCD.

Since key generation, key storage and certificate management is handled by mySaveID in the systems and secure hardware modules of mySaveID and no secure cryptographic devise for the subscriber and / or subject is required all obligations specified for NCP in ETSI EN 319 411-1 apply.

The list of CAs above can be expanded in the next version of the present document.

Before expiration of a CA certificate which is used for signing subject keys (for example as indicated by expiration of CA certificate), in case of continuing with the service, the CA generates a new certificate for signing subject key pairs and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA certificate.

1.3.2 Registration authorities

mySaveID uses an internal face to face registration service and external identification proofing service providers as the Registration Authority Service.

The Registration Authority performs the following functions:

- collecting and accepting certificate applications, terms of provision of trust services, accepted by Subscribers,
- verification of subscribers' identity,
- Identifies the person who finally submitted a request in accordance with the rules and procedures established by mySaveID.
- Verification of the subject's identity shall be at time of registration by appropriate means. The collection of evidence may include the copy of personal data, such as ID or passport.
- mySaveID shall collect and validate either direct evidence or an attestation from an authorized source, of the identity and if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation.

- Certifies the veracity and admissibility of a submitted electronic request for qualified certificate.
- Notifies the users for issued qualification certificate.
- Performs approval of requests for continuing the effect of a qualified certificate on behalf of mySaveID.

Certificate request may be:

1. submitted at the time of registration of the subject or
2. for already registered subjects anytime during validity of identity proof stored in mySaveID register.

1.3.3 Subjects and subscribers and Client

msg mySaveID enters into two types of contractual relationships, one with the natural person (also referred to as User) and one with the legal entity (also referred to as Client). The respective contractual relationship results from the explicit acceptance of the contractual terms and conditions (GTC). In general, any legal entity (fulfilling the legal German and European requirements and following the terms and conditions as well as this CPS) may be a client of msg mySaveID. The contractual relationship with the natural person is normally established when a legal entity invites the persons associated with the organization (e.g. employees) or his client (natural person paid for by the legal entity) to mySaveID. A client (legal entity) is paying for msg mySaveID GmbH services.

Subscriber is identified in a certificate as the holder of the private key, subscriber can be:

- a natural person;
- a legal person (that can be an Organization or a unit or a department identified in association with an Organization).

Subject describes the end users of the certificates, subjects can be:

- a natural person;
- a natural person identified in association with a legal person (authorized representatives);
- a legal person (for seal certificates).

Organizations willing that their employes or customers should be able to get certificates issued by mySaveID and be able to sign documents using the trust services of mySaveID could do it by means of their authorized representatives.

As described above, before a contractual relationship is entered into, mySaveID is informed of the conditions and obligations relating to the use of the certificate and the natural person or legal person must expressly agree to this. mySaveID records the agreements with the natural persons and legal person accordingly.

To avoid any conflicts of interests, the subscriber and the mySaveID are separate entities. The only exceptions are certificates that a mySaveID issues for itself (as a legal person) or natural persons belonging to it (as a subject). Certificates that mySaveID issues for itself or persons

belonging to it (as a subject) are requested, validated and handled according to the TSP's defined processes for the selected type of certificates.

1.3.4 Relying parties

Relying party means a natural person or legal entity who relies on the trust services of mySaveID and electronic identification means provided by mySaveID.

The relying party using the certificate in order to verify an electronic signature or seal is liable for verifying the current status of the certificate. This decision must be made by the relying party each time when the certificate is to be used for verifying an electronic signature (seal) or authentication of websites. Information included in a qualified certificate (for instance certificate type, object identifiers of the certificate policy, content of keyUsage field) should be used by the relying party for the assessment whether the certificate was used in line with its declared designation.

Obligations of relying parties are listed in chapter 4.5.2 of the Policy.

1.3.5 Other participants

mySaveID uses subcontractors and service providers, such as specialized data centers, for reliable and secure colocation and operation of server and network equipment, providers of identity proofing services, IT services and others. mySaveID is a part of the .msg Group. Companies in the .msg Group may be providers of services for mySaveID.

When working with subcontractors and providers, mySaveID has a documented agreement and contractual relationship in place with them which (among other things) requires them to strictly follow the procedures and policies of mySaveID, in accordance with this Policy and Practice as well as the information security and privacy policy and requirements of mySaveID. This is regulated in the contracts with them and regularly reviewed by mySaveID.

All suppliers used by mySaveID for providing trust services have been obliged by mySaveID to fulfill the requirements of this policy as well as to comply with the security and data policies and requirements of mySaveID. This includes also all other parties, including trust service component providers, to provide parts of its service through subcontracting, outsourcing or other third party arrangements. In any case mySaveID as TSP maintains overall responsibility for meeting the requirements defined in the trust service policy. Details are regulated in the Guideline for suppliers and service providers (Richtlinie Lieferanten und Dienstleister). When selecting suppliers, mySaveID uses the Guideline for suppliers and service providers (Richtlinie Lieferanten und Dienstleister).

When the TSP makes use of a trust service component provided by another party (e.g. identity providers) it ensures (by reviews and tests) that the use of the component interface meets the requirements as specified by the trust service component provider. The TSP also ensures (by reviews and tests) that the security and functionality required by the trust service component are meeting the appropriate requirements of the applicable policy and practices.

Regardless of this, parts of the TSP concerned with certificate generation and revocation management are independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services in conformance with the applicable certificate policies.

1.4 Certificate Usage

mySaveID Root CA issues certificates for operational CAs indicated above.

mySaveID operational CAs issues certificates for electronic signatures and electronic seals. Qualified certificates are issued to the subjects and subscribers who previously had to accept the terms of provision of trust services by mySaveID and the rules of this Policy and Practice Statement.

Every qualified certificate issued by the mySaveID operational CA provides of indication that it is a qualified certificate.

There are the following types of qualified certificates and their applicability:

1. **Personal**

   Qualified certificates for qualified electronic signatures - certificate contains at least: name of the country, name of the subject and serial number of the certificate.

2. **Professional (with additional data)**

   Qualified certificate for qualified electronic signatures - certificates are used by individuals who are employees or representatives of organizations, institutions, enterprises, or by the representatives of other individuals; the certificate contains at least: the name of the country, name of the subject, name of the entity and serial number of certificate.

3. **Electronic Seal**

   Qualified certificates for qualified electronic seals - certificates are issued to legal persons. Qualified certificate for electronic seal includes at least: the name of the country, the name of the legal entity (subject) and its registration number, common name, and serial number.

1.4.1 Appropriate certificate uses

Personal certificates use is restricted to creation of qualified electronic signatures by the natural person and its validation by relying parties.

Professional certificates use is restricted to creation of qualified electronic signatures by the natural person associated with legal person and its validation by relying parties.

Electronic seal certificates use is restricted to creation of qualified electronic seals by the legal person and its validation by relying parties.

1.4.2 Prohibited certificate uses

Certificate usage is restricted by using certificate extensions on key usage and extended key usage. Any usage of the Certificate inconsistent with these extensions is not authorised. Certificates are not authorised for use for any transactions above the designated reliance limits that have been indicated in the mySaveID Warranty Policy.

Certificates do not guarantee that the subject is trustworthy, operating a reputable business or that the equipment into which the Certificate has been installed is free from defect, malware or virus.

Certificates issued under this policy may not be used:

- Where prohibited by the law
- Qualified Certificates for Electronic Signatures should only be used by natural persons whereas Certificates for Electronic Seals should only be used by legal persons.
- For any application or mechanism where issues with the certificate could cause a safety risk (e.g. human or environmental risk)

Unauthorized use of Certificates may result in the voiding of warranties offered by mySaveID to Subjects, Subscribers and their Relying Parties.

1.5 Practice Statement Administration

1.5.1 Organization responsible for administrating the document

mySaveID is in charge of managing the Policy (including the approval of amendments etc.).

Each amendment to the Policy, except for those replacing obvious clerk or style errors, must be approved by the management board of mySaveID in the new version of the Policy. The version valid at a certain time has a current status.

Each version is valid until a new version is approved and published in the repository (see also Section 1.5.4).

The management board is responsible and ensures that the practices of this Policy and other policies of mySaveID are implemented.

1.5.2 Contact

All correspondence regarding trust services must be addressed to:

CEO of msg mySaveID GmbH (member of the management board,)

msg mySaveID GmbH GmbH
Amelia-Mary-Earhart-Straße 14,
60549 Frankfurt am Main

Email: info@mysaveid.de
Phone number: +49 69 580045-4000

1.5.3 Entities determining the validity of the principles contained in the document

The mySaveID team (including management board of mySaveID) is responsible for evaluating the timeliness and usefulness of the Policy and other documents concerning PKI services, provided by mySaveID, as well as the compatibility between these documents.

All inquiries and comments concerning the contents of these documents should be directed to the address in chapter 1.5.2.

1.5.4 Approval procedures

The Management Board of mySaveID approves the Policy. Upon an approval, the document receives the valid status indicating the date of entering into force. It is published in the repository no later than on the same date.

Before the approval comments on suggested modifications may be submitted by the affected parties within 14 working days of their announcement (as presented in chapter 9.12). After this deadline, if there are no significant reservations to the substantive content of the proposed changes, the Management Board of mySaveID may approve the Policy which becomes valid with the validity date indicated in it.

All changes made in the document are recorded in the history of the document.

The approved Policy is published and communicated to:

- employees
- relying parties
- subjects and subscribers
- other parties defined in 1.3.5.

The Policy is in effect from the date indicating the beginning of its validity until the publication of the next valid version. https://mysaveid.de/en_GB/repository

1.6 Definitions and Acronyms

Definitions and abbreviations used in this document are at the end of it.

2 Publication and Repository Responsibilities

2.1 Repository

The Repository is a public collection of documents concerning designed for external parties (subscribers, relying parties) which is available 24/7 and published at: https://mysaveid.de/en_GB/repository .

The public registry of mySaveID is a repository where current and previous version of electronic documents are located. The repository contains:

- Trust service provider certificates (Certificates of the root CA and of the operating CA, see chapter 1.3.1)
- Test certificates for all certificate types that the TSP issues for subjects to provide the capability to allow third parties to check and test them
- Other (see chapter 2.2).

2.2 Information published by mySaveID

The information published by mySaveID includes documents describing:

- This Policy
- Terms & Conditions for mySaveID Qualified Trust Services connected to the certificates (English and German)
- Certificates Revocation Lists (CRLs) and Certification Authority Revocation List (CARL)
- Additional information, such as notifications
- PKI Disclosure Statement (PDS)
- Conformity Assessment Report (CAR)

https://mysaveid.de/en_GB/repository

2.3 Frequency of publication

CRLs are generated and published automatically, while other information each time upon their updating or amending.

2.4 Access to publication

mySaveID has implemented logical and physical mechanisms protecting against unauthorized adding, removing and modifying of the information published in the repository.

3 Identification and Authentication

Within identification and authentication mySaveID meets applicable data protection legislation. mySaveID fulfills the data protection requirements of the GDPR and the German Federal Data Protection Act. Compliance is ensured in particular by the data protection officer. Corresponding technical and organizational measures and complied data protection principles are described in the guideline for data protection and information security. The same applies to the suppliers and providers of mySaveID. An data processing agreement according the legal requirements has been concluded with them.

3.1 Naming

3.1.1 Type of names

The certificates generally contain information regarding the issuer and the subscriber and/or the subject. In line with the [X.509] standard, these names are given as distinguished name.

3.1.2 Meaningful names required

The distinguished name used is unambiguous within this trust services.

All the values in the Subject information section of a Certificate are meaningful.

Mandatory data in the certificate enabling unambiguous identification of the subscriber has been pointed out in section 3.1.4.

3.1.3 User anonymity

Anonymity or pseudonymity of Subject is not allowed.

3.1.4 Rules for different names interpretation

The interpretation of names of fields included in certificates complies with ETSI TS 119 412-1 and ETSI EN 319 412 (Part: 2,3,4,5). The attributes of the distinguished name (DN components) of certificates are interpreted as follows:

DN component	**Interpretation**
G (given name)	*Given name(s)* of the natural person - According to the proof used for identification
SN (surname)	*Surname* of the natural person - According to the proof used for identification
CN (common name)	*Common name:* The following variants are used: - Natural persons without a pseudonym: “Surname, name used”. - Legal entities: Official name of the organization (company, public authority, association, etc.), if necessary, reduced to a meaningful name if the maximum number of 64 characters is exceeded.

serialNumber	*Serial number*: number to ensure unambiguity of the name (typically the application number with some random component). Other product-specific uses of the field are possible.
O (organization)	*Official name of the subscriber or full name of the organization* (including legal form) to which the subject belongs or to which he or she is otherwise affiliated (company, public authority, association, etc.) according to the proof of existence, consistent with the national or other applicable identification practices.
OU (organization unit)	*Organization unit* (department, division or other unit) of the organization
OrgID (organization identifier)	*Unambiguous organization number of the organization*. tax identification number, register number in the national commercial register or local identifier, recognizable on the European Union's level according to point 5.1.4 ETSI TS 119 412-1
C (country)	The notation of the *country* to be stated corresponds to [ISO 3166] and is set up as follows: • If an organization O is listed in the DistinguishedName, the organization's place of business in the register determines the entry in the certificate. • If no organization O is entered, the country is listed that was transmitted as the nationality of the subscriber during the identification process.
E-mail	The e-mail address of the applicant (optional)
Street	Postal address Street
Locality	Postal address City
State	Postal address (Federal) state
PostalCode	Postal address Postal code

Qualified certificates for natural persons include, as a minimum, the subject DN components: "commonName", "countryName", "serialNumber" as well as "GivenName" and "Surname".

Qualified certificates for legal entities include, as a minimum, the subject DN components: "commonName", "countryName", "serialNumber" and "organizationName" as well as "organizationIdentifier". It is not necessary to use all the DN components mentioned here.

Further components can be added. Additional DN components must comply with [RFC 5280], [RFC 6818] and [ETSI EN 319 412].

3.1.5 Uniqueness of the names

Subject's distinguished name is compiled according to the profile described in the Certificate Profile. mySaveID does not issue Certificates with an identical Common Name (CN), Serial Number (S) for different subjects. In addition to the application number, the serial number contains a random component.

3.1.6 Names verifications and disputes in this regard

Subjects may not request Certificates with any content that infringes the intellectual property rights of a third party. mySaveID does not require that an subject's or subscriber's right to use a trademark be verified. mySaveID reserves the right to revoke any certificate that is involved in a dispute.

3.2 Initial Identity Validation

mySaveID verifies the identity of the subscriber and subject and checks if certificate requests are accurate, authorized, and complete according to the collected evidence or attestation of identity.

mySaveID collects and validates all evidence and attestations from an appropriate and authorized source, of the identity and any specific attributes of registered subjects. mySaveID collects only evidence of identity sufficient to satisfy the requirements of the intended use of the certificate.

mySaveID uses an internal face to face registration service and external identification proofing service providers as the Registration Authority Service and verifies and authenticates the subject's identity and other attributes before including these attributes in the Certificate.

The subjects are prohibited from using names in their Certificate that infringe upon the intellectual property rights of others. mySaveID does not verify whether a subject has intellectual property rights in the name appearing in the Certificate request or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any Domain Name, trademark, trade name or service mark. mySaveID reserves the right, without liability to any subject, to reject an application because of such a dispute. mySaveID RAs authenticate the requests of parties wishing to revoke Certificates.

mySaveID records all the information from the verification process of the subject's identity, including specific attributes of the subject, reference numbers on the documentation used for verification, and limitations on documentation validity.

mySaveID keeps record of all changes in the register of the users.

mySaveID ensures that registration inspector is not allowed to verify own identity during identification and authentication process described in this chapter.

3.2.1 Method to prove possession of key

Registration processes are conducted by Registration Authorities. Once a registration is completed, the Subject's key pair is generated by mySaveID Subject Remote QSCD Provision

Service. Subject's key is generated in remote QSCD (HSM held by mySaveID on behalf of the Subject).

3.2.2 Authentication of legal person

Authentication of legal person is done according to statements indicated in chapter 3.2.4.

3.2.3 Authentication of Natural person

mySaveID provides an internal register of all subjects (Users). The register is an accurate database used for the issuance of subject certificates and provisioning identification means. All subjects included in the register are verified at the time of registration using Registration Service.

The natural person's identity and specific attributes of the person are verified with one of the methods (eIDAS 2.0; Article 24; 1a) described in the following table.

a.	Identification via eID checked according to BSI-K-TR-0565-2023	eID from AUTHADA GmbH by using the electronic proof of identity in accordance with § 18 PAuswG
d.	By the physical presence of the natural person;	Based on a face-to-face meeting in a common physical location where the applicant presents the necessary evidence e.g. identification documents, and the operator confirms the identity based on that evidence

Natural persons are checked either directly by the physical presence of the person or indirectly using means with equivalent assurance to physical presence. The evidence is provided of:

a) full name including surname and given names consistent with the national identification practices.
b) date and place of birth, reference to a nationally recognized identity document.

A Registration Authority (RA) collects the data necessary for identity proofing and verification of the Subject. This data is stored in the register of mySaveID users. The register of mySaveID users is the trusted source of identity data submitted to CA.

Where physical ID documents are used for the applicant identification, the RA service fulfills related requirements under German Law:

- relevant provisions of Vertrauensdienstegesetz (VDG).

The exchange of Identification data by a remote connection or other type of telecommunications (see case b, above) is protected by authentication and encryption. The identification data is integrity-protected.

For the implementation of AUTHADA GmbH and its use, mySaveID follows the implementation guidelines provided by AUTHADA GmbH.

3.2.4 Authentication of a natural person representing legal entity

Natural person identity validation is performed according to practices defined in 3.2.3

Natural person in the association with legal person are checked either directly by the physical presence of the person or indirectly using means with equivalent assurance to physical presence.

The evidence of the natural person identified in the association with legal person is provided:

a) full name, including surname and given names, consistently with the national or other applicable identification practices of the subject.
b) date and place of birth, reference to a nationally recognized identity document, or other attributes of the subscriber which can be used to, as far as possible, distinguish the person from others with the same name.
c) full name and legal status of the associated legal person or other organizational entity (e.g., the subscriber);
d) any relevant existing registration information (e.g., company registration) of the associated legal person or other organizational entity identified in association with the legal person, consistent with the national or other applicable identification practices.
e) affiliation of the natural person to the legal person consistent with national or other applicable identification practices.
f) the association between the legal person and any organizational entity identified in association with this legal person that would appear in the organization attribute of the certificate, consistent with the national or other applicable identification practices.
g) approval by the legal person and the natural person that the subject attributes also identify such organization.

Also evidence of the full name of the legal person consistent with the national or other applicable identification practices is provided.

The exchange of Identification data by a remote connection or other type of telecommunications (see case b, above) is protected by authentication and encryption. The identification data is integrity-protected.

3.2.5 Unconfirmed information

Non-verified Subjects information is not allowed in the Certificate.

3.2.6 Criteria of interoperability

No stipulation.

3.3 Identification and Authentication for Re-key Requests

Re-key request are not allowed in mySaveID practices.

3.4 Identification and Authentication for Revocation Requests

Certificate revocation request may be submitted by the Subscriber and/or Subject via individual account available for mySaveID registered users. In this case, subject's authentication involves re-entering account credentials.

Certificate revocation request may also be submitted by the subject via direct contact with mySaveID according to data contact in 1.5.2. In this case, the subject's authentication is based on providing basic identity data checked against register of mySaveID users. Then, the revocation request is forwarded to Registration Officers. Registration Officers calls the phone number provided in the request and during the conversation verifies the identity and verifies if the person can revoke the certificate of the subject.

The access by the registration / revocation officer requires multi-factor authentication on attempts to modify revocation status information.

mySaveID may perform full identity proofing validation according to 3.2.3.

mySave ID may also perform revocation on behalf of Subject or by the Subscriber in accordance with the CPS.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

mySaveID maintains the register of the users (subscribers and subjects). Only registered subscribers (together with registered users) of mySaveID can submit a certificate application.

4.1.2 Enrollment process and responsibilites

The registered subscriber has to invite a user and to unlock for him the option to be able to sign with the services of mySaveID. (You can imagine that step as a prerequest for certificate for the user.)

Registered and authenticated mySaveID's user can then finalise a request remotely for certificate with mySaveID account.

As a result of this request, the certificate issuance procedure is started.

Generally, the application process includes the following steps:

- Submitting a request for a Certificate type and appropriate application information (both by subscriber and by subject).
- Confirmation any applicable fees.
- Validation if subject's data stored in mySaveID register fulfills requirements of present Policy (i.e. if the identification is valid and fullfills the requirements of a qualified trust service provider)
- Automatic generation of a suitable Key Pair based on remote QSCD under mySaveID control on behalf of the Subject.
- Certificate generation and acceptance by subject.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

mySaveID verifies the identity of the subscriber and subject and checks if certificate requests are accurate, authorized, and complete according to the collected evidence or attestation of identity.

Registration processes are conducted by Registration Authorities. mySaveID provides an internal register of all subscribers and subjects (Users) and level of assurance electronic identification means assigned to the subject. The register is an accurate database used for the issuance of subject certificates.

All subjects included in the register are verified at the time of registration using Registration Service and level of assurance is assigned to the mySaveID user account. Detailed initial identity validation is described in chapter 3.2 of Practice Statement.

After having an account, users of mySaveID are authenticated with two-factor authentication methods. Information about level of assurance of authentication method is collected in mySaveID user account.

4.2.2 Approval or Rejection of Certificate Applications

The acceptance or rejection of a Subscriber and subject application is determined by the CA. Subject applications will be approved if they meet the requirements in this Policy and CPS.

mySaveID shall reject applications for certificates where validation of all items cannot successfully be completed. This also includes any identification of discrepancies between the data in the application and the data stored in the mySaveID user register.

If any additional data are required, mySaveID conducts the initial validation process according to CPS to extend mySaveID user account with these data. The data exchange is done via encrypted communication if registered service is an external.

4.2.3 Time to Process Certificate Applications

mySaveID makes every effort to ensure that on receiving the application for a certificate, the CA examines the application and issues a certificate as soon as possible.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

After verifying that the Subjects identification data in the certificate request matches the identification data in the register of mySaveID users, the mySaveID certificate generation service automatically issues the corresponding certificates.

Certificates of the root CA and the operating CAS are generated as part of the key ceremony (cf. section 6.1.1).

4.3.2 Notification to Subjects and Subscribers by the CA of issuance of a certificate

Subject and Subscriber, whose data is included in the certificate application, are informed about certificate issuance. mySaveID will be notified of the issuance of the certificate using the method agreed in the contract with the Subscriber.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

Once the Subject confirms the Subscriber Agreement with the Terms and Conditions and verifies accuracy of data in the certificate, the certificates are deemed as accepted. The consent and acceptance are logged.

To avoid this being an open-ended stipulation, the mySaveID may set a time limit by when the Certificates shall be accepted, otherwise the Subscriber will have to start the process from the beginning.

4.4.2 Publication of the certificate by the CA

mySaveID does not publish valid Subject Certificates (of natural or legal persons) to any other party (except the subject itself).

Regardless of this, mySaveID publishes in its repository (see section 2.1) test certificates for all certificate types that the TSP issues for subjects to provide the capability to allow third parties to check and test them. The corresponding subject name of the test certificates clearly indicate that they are for testing purposes.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber and/or subject private key and Certificate usage

Subscribers and subjects are entitled to use their private keys exclusively for those applications which are in conformity with the types of use stated in the certificate. They are required to use the Certificate and Private Key lawfully and in accordance with:

- this Policy and CPS
- the Terms and Conditions [AGB].

The remote signature system technically excludes the signature with expired certificates. Subscriber can use the signing key pair for signing using various signature formats.

mySaveID hosts, secures, and manages certificates and corresponding Private Keys in a conformant HSM/QSCD.

4.5.2 Relying party public key and Certificate usage

The relying party is required to use the Certificate and Public Key lawfully and in accordance with:

- This Policy and CPS;
- the Terms and Conditions [AGB].

The certificates issued by mySaveID can be used by all relying parties. However, they can only be relied upon if:

1. the certificates are used in line with the types of use shown there (key use, extended key use, restricting extensions, if applicable).
2. all other precautionary measures determined in agreements or otherwise were taken (see documents in the mySaveID repository) and if any restrictions in the certificate as well as any application-specific measures were taken by the relying party and found to be compatible.

3. the verification of the certificate-chain is carried out successfully right through to the trusted root certificate. This is done, to validate the trust status of the PKI (e.g. EU Trusted List according to eIDAS.
4. it is verified that the certificate is not listed as revoked on the associated Certificate Revocation List (CRL), or the status of the certificates is checked via the Online Certificate Status Protocol (OCSP) and the outcome is positive (i.e. a third party can determine via the OCSP status query that mySaveID has issued the requested certificate.). If the check mechanism from point 3 did not work, the existence and validity of a certificate can be checked via the Online Certificate Status Protocol (OCSP).

4.6 Certificate Renewal

Renewal of Certificates for end entities is not allowed.

Before expiration of a CA certificate which is used for signing subject keys (for example as indicated by expiration of CA certificate), in case of continuing with the service, a new CA certificate has to be generated and distributed in accordance with the present document.

mySaveID applies all necessary actions to avoid disruption to the operations of any entity that may rely on the CA certificate.

The operations should be performed with a suitable interval between certificate expiry date and the last certificate signed to allow all parties that have relationships with the TSP (subjects, subscribers, relying parties, CAs higher in the CA hierarchy, etc.) to be aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions. This does not apply to a TSP which will cease its operations before its own certificate-signing certificate expiration date.

4.7 Certificate Re-key

Certificate Re-Key initiated by the Subject or Subscriber is considered to be a new application and processed accordingly. Certificate re-key is not allowed.

4.8 Certificate Modification

Modification is not allowed. Each application is processed as a new application and is performed according to chapter 4.1. The process of modifying the data in the certificate means creating a new certificate based on the identity confirmed by mySaveID.

Each application is processed as a new application and is performed according to chapter 4.1.

4.9 Certificate Revocation

4.9.1 Circumstances for revocation

Revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated validity period. Prior to revoking a certificate, the Operational CA verifies that the revocation request was made by either the Subscriber or Subject. The Operational CA should revoke a certificate if one or more of the following circumstances occurs:

- the subject or subscriber requests revocation using the mySaveID App or Site;
- the subject notifies that the original certificate request was not authorised and does not retroactively grant authorisation;
- MySaveID obtains a report that the Subject's Private Key corresponding to the Public Key in the certificate suffered a key compromise or no longer complies with the requirements;
- MySaveID obtains a report that the certificate was misused;
- the Subscriber has violated one or more of its obligations under the Terms and Conditions [AGB];
- Subject made any change (e.g. surname change) in the information contained in the certificate;
- the Certificate was not issued in accordance with the CPS and/or this policy;
- MySaveID obtains a report that a Certificate is no longer compliant with Policy under which it has been issued;
- MySaveID determines that any of the information appearing in the certificate is inaccurate or misleading;
- mySaveID's right to issue certificates is revoked or terminated;
- MySaveID obtains a report of a possible compromise of the Private Key of the CA used for issuing the certificate;
- revocation is required by the CPS;
- the technical content or format of the certificate presents an unacceptable risk to Relying Parties;
- MySaveID is made aware that CA Certificates has been compromised;
- MySaveID receives a report if cryptographic suites used in CA Certificates have been deemed non secure.

A revocation request requiring revocation at a future date (e.g. subject's planned cessation from his/her duties at a certain date), is not supported.

Certificates whose remaining validity period is less than 24 hours may not be revoked.

4.9.2 Who can request revocation

The Subject or Subscriber can request revocation of the Subject's Certificates at any time.

RA may request revocation of the Subject's certificates or submit a report of an event related to revocation based on Subject's application.

CA may request revocation for any of the reasons listed in the Section 4.9.1 of this Policy.

Supervisory Body can request a revocation or submit a report of events that may cause revocation for a Subject's or CA's certificates at any time.

Relying Parties and other third parties may submit reports informing mySaveID of reasonable cause to revoke the certificate.

When an entity requesting certificate revocation is not an owner of this certificate (i.e. the subscriber), a certification authority has to:

- check whether the requester is authorized to request the revocation (e.g. acts as a subscriber's requester)
- submit notification to the subject about revocation or initiation of revocation process.

4.9.3 Procedure for revocation request

Certificate revocation request may be submitted by the subject via individual account available for mySaveID registered users. In this case, subject's authentication involves re-entering account credentials and results in automatic revocation.

Certificate revocation request may also be submitted by the subject via direct contact with mySaveID according to data contact in 1.5.2. In this case, the subject's authentication is based on providing basic identity data checked against register of mySaveID users. Then, the revocation request is forwarded to Registration Inspectors. Registration Inspector calls the phone number provided in the request and during the conversation verifies the identity and verifies if the person can revoke the certificate of the subject.

mySaveID may perform full identity proofing validation according to 3.2.3.

Subscribers, relying parties, and other third parties may submit a request according to data contact in 1.5.2.

mySaveiD will record each request for revocation and authenticate the source, taking appropriate action to revoke the certificate if the request is authentic and approved.

4.9.4 Revocation request grace period

The subject or subscriber is solely responsible for ensuring that they or a person authorized to request revocation on their behalf immediately request revocation as soon as reasons for revocation of the respective certificate become known.

4.9.5 Time within which CA must process the revocation request

All revocation requests for end entity certificates, both those generated automatically via user accounts and those initiated by mySaveID itself, must be processed within a maximum of 24 hours of receipt.

The mySaveID shall process revocation requests as follows:

- Before the next CRL is published, if the request is received two or more hours before regular periodic CRL issuance,
- By publishing it in the CRL following the next CRL, if the request is received within two hours of the regularly scheduled next CRL issuance.

Once a decision has been taken to process revocation it is processed immediately and made available via OCSP with a maximum delay of 60 minutes.

4.9.6 Revocation checking requirement for relying parties

Prior to relying on the information listed in a certificate, a relying party shall confirm the validity of each certificate in the certificate path, including checks for certificate validity, issuer-

to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each certificate in the chain.

4.9.7 CRL issuance frequency (if applicable)

Every certification authority being a part of mySaveID issues separate Certificate Revocation List.

Every Certificate Revocation List is updated at least every 24 hours. Regular updates after revocation within a few minutes.

A Certification Authority Revocation List (CARL) is generated at least once a year with a nextUpdate of at most 1 year after the issuing date.

After a root CA certificate has been revoked a new CARL (Certification Authority Revocation List) is generated.

4.9.8 Maximum latency for CRLs (if applicable)

Each CRL is published without undue delay as soon as it is created (usually this is done automatically within a few minutes).

4.9.9 On-line revocation/status checking availability

mySaveID provides real-time certificate status verification service. This service is carried out on the basis of OCSP described in RFC6960. Using OCSP, it is possible to acquire certificate status information without requiring CRL.

OCSP response times are generally no longer than 10 seconds under normal network operating conditions. mySaveID updates information provided via an OCSP every few minutes.

If the OCPS responder receives a request for status of a certificate that has not been issued then the responder will not respond with a "good" status as per clause 2.2 of IETF RFC 6960. The CA monitors such requests concerning non-issued certificates on the responder as part of its security response procedures to check if this is an indication of an attack.

4.9.10 On-line revocation checking requirements

Relying parties must check revocation information of a certificate on which they wishes to rely.

For the status of subject certificates:

mySaveID updates information provided via an OCSP every few minutes. OCSP responses have a maximum expiration time of seven days.

For the status of subordinate CA certificates:

mySaveID updates information provided via an OCSP at least every twelve months and within maximum 24 hours after revoking a subordinate CA certificate.

4.9.11 Other forms of revocation advertisements available

No stipulation

4.9.12 Special requirements related to key compromise

No stipulation

4.9.13 Circumstances for suspension

No stipulation

4.9.14 Who can request suspension

No stipulation

4.9.15 Procedure for suspension request

No stipulation

4.9.16 Limits on suspension period

No stipulation

4.10 Certificate Status Services

4.10.1 Operational Characteristics

mySaveID provides a Certificate status service either in the form of a CRL distribution point or an OCSP responder or both in the certificates. OCSP certificate status request services are accessible over HTTPS. The current CRL is published in the repository and available through CRL distribution point over HTTPS.

The formats and protocols of the services are described in sections 7.2 and 7.3 of this policy. The system time of the OCSP responder is synchronized daily using the DCF77 time signal and reliable time servers (NTP) on the Internet.

The URL of the OCSP service and CRL distribution point are included in the certificate.

Since TSP is managing the subject's private key it assures that the certificate is valid at the time of use of the private key.

Revocation status information is made available beyond the validity period of the certificate.

If CRLs are provided, revoked certificates are not removed from the CRL after they have as long as the HSM have their qualified Status we use it for the operation as TSP. If the HSM loose the qualified Status mySaveID shut down the system at the latest with the termination of QSCD-Status. If valid certificates exist at this time, they will be revoked.expired.

If CRLs are provided and the TSP decides or is required to terminate a CRL, the TSP issues and publishes at the corresponding CRL Distribution Point a last CRL with a nextUpdate field value as defined in ETSI EN 319 411-1 [2], clause 6.3.9.

If CRLs are provided, the TSP preserves the integrity and the availability of the last CRL at least for the period specified in the CPS as requested in CSS-6.3.10-12.

If CRLs are provided, the TSP will issue a last CRL until all certificates in the scope of the CRL are either expired or revoked.

If OCPS is provided, the OCPS responder uses the ArchiveCutOff extension as specified in IETF RFC 6960 [i.9], with the archiveCutOff date set to the CA's certificate "notBefore" time and date value.

If OCPS is provided and the CA's certificate is about to expire, the TSP computes a last OCPS answer for each and every issued certificate (whether revoked or not), with the "nextUpdate" field set to "99991231235959Z".

Since TSP is managing the subject's private key it assures that the certificate is valid at the time of use of the private key.

4.10.2 Service Availability

mySaveID maintains an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by mySaveID.

Validation services for qualified electronic signatures and qualified electronic seals are available 24/7 (without any planned outages).

4.10.3 Operational Features

No stipulation.

4.11 End of Subscription

The end of the subscription occurs in the following cases:

- subject certificate validity period has expired and subscriber/subject has not taken action to update or modify his/her key,
- subject's certificate was revoked.

4.12 Key Escrow and Recovery

CA Private Keys are never escrowed. mySaveID does not offer key escrow services to Subjects.

4.12.1 Key escrow and recovery policy and practices

Key escrow and recovery are not supported.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 Management, Operational, and Physical Controls

mySaveID It operates an integrated management system for information security and privacy (based on ISO 27001:2022 and ISO/IEC 27701) whose scope includes in particular all processes and procedures of its offered trust services but also business issues. This management system includes the information security and privacy policy and describes its documentation, implementation and maintenance, including security controls and operating procedures for TSP's facilities, systems and information assets that provide the services. The management board of mySaveID approves this management system and thereby also the security and privacy policy.

Any changes that will impact on the level of security and privacy provided has to be approved by the management bord of mySaveID.

The security and privacy policy is published and communicated by the TSP to all employees who are impacted by it in the intranet.

Moreover, mySaveID retains overall responsibility for conformance with the procedures prescribed in its information security policy, even when the TSP's functionality is undertaken by outsourcers. Changes to the information security policy are communicated to third parties, where applicable. This includes subscribers, subjects, relying parties, assessment bodies, superviory body or other regulatory bodies. mySaveID obliges these third parties to comply with the specifications and requirements of this Policy and the information security and privacy policy and checks this regularly,

The following sections describes the general practices for supervision over physical and operational controls used by msg mySaveID GmbH.

The basis for establishing controls is the formal risk management process (including risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues) of mySaveID as well as the inventory of all information assets (in the scope of the trust services) that is maintained by mySaveID. mySaveID assigns a classification consistent with the risk assessment to the assets.

Risk management process is regularly reviewed and revised. mySaveID Management Board approves the risk assessment and accept the residual risk identified. Also the management board of mySaveID triggers a review of the controls and possible changes to the TSP at least every 6 months.

5.1 Physical Security Controls

The basic goal of physical security measures is to guarantee that assets are not lost, damaged, or compromised, and that business operations are not disrupted. Based on risk assessment, mySaveID selects security measures and monitors their effectiveness.

mySaveID uses trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

5.1.1 Premises

ICT systems used to provide mySaveID trust services are located in two independent fire areas in a remote location (data center). The premises are owned by msg group company, provided under agreement. The premises are in the scope of an ISMS operated by the msg group company that is certified according to ISO 27001 with ISO 27017.

5.1.2 Physical access

The mySaveID and its suppliers and providers control physical access to components of the mySaveID's system whose security is critical to the provision of its trust services by:

- 24/7 monitoring operated by security guards
- CCTV, alarm system
- creating security zones
- access limitation to authorized individuals (trusted roles)
- internal procedures for personnel
- every entry and exit is logged.

The issuing of the cards and the logging of entries and exits is handled by msg group. The recorded data is stored for 90 days.

Visitors to areas occupied by mySaveID may access this area only if they are escorted by the authorized personnel of mySaveID.

An important aspect of protection is the creation of security zones, with a specific designation of a perimeter with a high level of security. In the highest security perimeter, mySaveID stores Root CA systems and HSM devices used, among others, for certificate generation and revocation management services. It is required a double access (dual control) to this area.

The access to the area of operators and administrators is limited and is administered using a smart-card system and access control.

5.1.3 Power and air conditioning

The premises with critical components are powered by two independent sources. In case of power line failure, the system switches to emergency power source (UPS and power generators).

The air-conditioning maintains a constant air temperature for the normal operation of the technological system.

The operation environment in the computer systems area (Administrator and operators area) is monitored continuously.

5.1.4 Water exposure

Humidity and water detecting sensors are installed in the server room. These sensors are integrated with the security system of mySaveID building. The guards and employees of mySaveID are trained and required in case of possible incidents to immediately inform the relevant services, the security officer, and the system administrator.

5.1.5 Fire prevention and protection

The server room is equipped with fire control system, activated automatically in the case of fire detection in monitored area. Fire prevention and protection system installed in room complies with local standards and regulations for fire safety.

5.1.6 Media storage

Media used within the TSP's systems are securely handled to protect media from damage, theft, unauthorized access and obsolescence. In order to achieve this mySaveID has been implemented an Information Security and Privacy Policy including also requirements for handling and classification of information and media.

All media containing software, data backups, archives or auditing information are stored in a special premise with implemented access control. mySaveID has a policy that prohibits the removal of carriers without authorization (e.g. maintenance process).

In addition to that, data backups and archives are stored in different area than the server room. Management procedures are in place to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

Sensitive data are protected against being revealed through re-used storage objects (e.g. deleted files) by unauthorized users. mySaveID has been implemented an Information Security and Privacy Policy with requirements for classification of information.

5.1.7 Waste disposal

The mySaveID has implemented a procedure for information destruction and waste disposal.

Paper and electronic media containing any relevant information about the mySaveID trust service, after the expiry of the period determined in retention policy, are destroyed in special shredding devices.

Hardware security modules are reset and securely erased according to manufacturer’s recommendations before reuse.

5.2 Procedural Controls

mySaveID ensures the performance of organizational securities by specifying the following:

a) roles that may be performed by one or more individuals in the trust services, including job scription,
b) ban of cumulation of specified roles,
c) the scope of obligations and responsibilities of individuals performing specific roles,
d) number of individuals necessary for the performance of specific tasks,
e) identification and verification of personnel.

5.2.1 Trusted roles

Security roles and responsibilities are specified in the TSP's information security policy and documented in job descriptions or in documents available to all concerned personnel.

The functions allocation is implemented in such a way as to minimize the risk of compromising, confidential information leakage or the emergence of a conflict of interests.

Trusted roles on which the security of the TSP's operation is dependent are named by the management board of mySaveID. A detailed allocation of the functions and responsibilities of the personnel is stipulated by the management board of mySaveID including job descriptions, staffing plan and the relevant internal operating procedures.

The following trusted roles which are manned with one or more individuals are identified and applied by mySaveID (complying with the requirements of ETSI EN 319 401 and CEN TS 419 261):

Role	Tasks/area of responsibility	Qualification
Manager of mySaveID (Management Board)	• Responsible for correct management of mySaveID trust services and electronic identification systems, determines directions of development of certification authority, responsible to manage Certification Policy and Practice Statement,	Relevant degree, at least three years of professional experience as Manager of an organization, experience in the field of trust services
Incident Manager	• Responsible for the organisational and technical process and the response to identified or suspected security incidents or operational disruptions.	Relevant specialised training or relevant degree
Registration Officer	• Responsibility for the verification of information required for the issuance of certificates and the approval of certification requests.	Relevant specialised training, relevant knowledge in the field of document verification
Revocation Officer	• Responsibility for changing the status of certificates before the certificates and authorisations expire.	Relevant specialised training, relevant knowledge in the field of document verification
Security Officer	• Preparing and participating in the development, implementation and application of security policies for the use of information systems used in the provision of trust services. • Implementation of the provisions of the policies of the trust services (e.g. CPS, TSP) • Supervision of the actions of the system administrators in accordance with the existing regulations. • Initiating and monitoring the process of generating keys and shared secrets. • Participation in the internal control process. Control of the execution of security processes. • Assignment of rights in the area of security and user access rights	Relevant degree at least three years of professional experience in the field of structural, technical and procedural safety

System Administrator	• Responsibility for the installation, configuration and maintenance of trusted systems and networks for the provision of trust services • Management of system support rights • Replacement of hardware and software components • Monitoring • Creation of backups • Restoration of backups • Analysing hardware and software requirements • Procurement processes	Relevant specialised training
System Auditor/ Audit Inspector	• Responsibility for reviewing event logs (in particular checking their integrity) and conducting internal audits to verify the compliance of a certification body's operations with the Practice Statement. • Authorisation to view archives and audit logs of trusted systems.	Relevant specialised training, auditor training
System Operator	• Standard operation of the mySaveID systems and application for the provision of trust services, in particular in relation to the High Protected Environment • Control of operations in the managed environment • Creation of backup copies and transfer of current copies and archives to external locations	Relevant specialised training
Data Protection Officer	• supervision over the compliance with requirements set forth in the GDPR resp. German Federal Data Protection Act	Relevant education, experience as Data protection Officer
Key ceremonie Roles, i.e. different roles for attendees of a key signing ceremony	• Responsibility for the successful execution of the key ceremony. Details are described in the plan and script oft he key ceremmonies.	

The appointment of (trusted) roles are accepted by the management board of mySaveID. Conversely, every person who is assigned a role must accept it in a recognizable, documented manner. The same applies to the change or replacement of roles.

5.2.2 Four-eyes principle

The four-eyes principle is the minimum requirement for particularly security-critical operations. This is ensured by technical and organizational measures, such as access authorization and verification of knowledge. When validating subject, it is ensured that an experienced validation specialist is called upon and works according to the four-eyes principle. Security-critical systems used for certificate issuance are generally protected by multi-factor authentication.

5.2.3 Identification and authentification for each role

The mySaveID staff is subject to identification and authentication of personality in the following situations:

- inclusion on the list of persons allowed to access mySaveID locations,
- inclusion on the list of persons allowed to physically access system and network resources of mySaveID,
- issuance of confirmation authorizing to perform the assigned role,
- assignation of an account and a password in mySaveID information system.

Every confirmation and assigned account:

- has to be unique and directly assigned to a specific person,
- cannot be shared with any other person,
- has to be restricted to function (arising from the role performed by a specific person) carried out solely by means of available mySaveID system software, operating system and controls.

Operations performed in mySaveID that require access through shared network resources are protected with implemented mechanisms of strong authentication and encryption of transmitted information.

Before being allowed to access any security-critical applications, the employee concerned must have been successfully authenticated. Only authorized and identified employees may access security-critical areas. Event logs enable the identification of employees who performed past actions; these employees are accountable for their acts.

5.2.4 Roles Requiring Separation of Duties

Every user of mySaveID system is assigned only the rights arising from the user's role and related responsibility.

The presented roles may be joined in limited scope, modified or denied. Chairman of the Management Board, Security Officer role and Audit Inspector are separated from other roles.

Access to software supervising operations performed by mySaveID is granted solely to the individuals whose responsibility and obligations arise from the acted role of the system administrator.

5.3 Personnel Security Controls

Personnel of mySaveID exercises administrative and management procedures and processes that are in line with the TSP's information security and privacy management procedures.

5.3.1 Qualifications, experience and clearances

mySaveID executes hiring, qualification and continuous training process according to its policies and routines. mySaveID staff are provided relevant and timely training and have the experience and competence required to carry out the duties specified in role descriptions and employment contracts. mySaveID defines a hiring process and continuous training process in the operational and security procedures.

mySaveID employees are required to:

- Demonstrate that they have not been convicted of intentional crime;
- Adhere to confidentiality clauses as part of their employment;
- Remain neutral with regards to financial or commercial interests that could constitute liabilities for personnel or mySaveID (“conflict of interest”).

Trusted Roles are further required to:

- Not participate in any activity regarding the issuing of certificates in his/her name or legal representative of him/her;
- Remain neutral and objective with regards to any interests conflicting with Trust Services operations.

Personnel in Trusted Roles are obliged to follow all required procedures without exceptions as defined in Practice Statement.

Managerial personnel possess experience or training with respect to the trust service that is provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

The senior executive, senior staff and staff in trusted roles, of the TSP concerned with certificate generation and revocation management are required to be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

5.3.2 Personnel testing procedures

Each new mySaveID employee, performing a trusted role is tested by mySaveID:

- to confirm previous employment.
- for verification of recommendations.
- to confirm the educational degree.
- to verify the certificate of conviction.
- to verify the identity document.

In cases where the requested information is not available (for example, due to an applicable law), mySaveID uses other legal methods, allowing the collection of the necessary information.

mySaveID may reject the application related to the implementation of the trusted role or act against a person who is already employed and performs a trusted role if it is established that:

- It was misled by an applicant or employee with respect to the above required data.
- receives highly unfavorable or not very reliable recommendations from previous employers.
- obtains information about any criminal record of the applicant or its employee has been sentenced by an enforced and valid judgment of court.

In case of occurrence, the further steps are carried out in accordance with the mySaveID safety procedures and applicable law.

5.3.3 Training requirements

In addition to strict requirements on competence and experience at the time of hiring, mySaveID employees undergo regular training. It is key that all personnel have adequate training and necessary experience for the duties specified in the role description and employment contract and maintain the necessary competency over time. Training includes:

- Regulations, procedures and documentation related to the occupied position.
- Responsibilities arising from roles and tasks performed in the system.
- Procedures performed upon system failure of the Certification Authority's activities.
- Information security policies.
- Procedures and security controls implemented by a Certification Authority
- Personal Data Protection.
- Trainings in Cybersecurity.

5.3.4 Retraining Frequency and requirements

Trainings described in chapter 5.3.3 must be repeated or supplemented always in situation when significant modification to mySaveID or its registration authority operation is executed.

5.3.5 Job rotation frequency and sequency

The Practice Statement does not imply any requirements in this field.

5.3.6 Sanctions for unauthorized actions

Personnel are bound by contractual employment obligation to carry out their duties according to internal rules.

mySaveID has routines for disciplinary actions. Disciplinary actions for unauthorized actions may include warning, role change or termination depending on the severity of the unauthorized action. Further disciplinary actions are to be consulted with mySaveID management.

5.3.7 Contracts with the personnel

Independent contractors and their personnel are subject to the same privacy protection and confidentiality conditions as mySaveID personnel. Under a signed contract, the persons or consultants are subject to the same verification procedure as the mySaveID employees.

mySaveID has provided penalties in the contracts in case that such personell is violating TSP's policies or procedures.

5.3.8 Documentation available to Personnel

Management of mySaveID provides their personnel with access to the following documents:

- Trust Service Policy,
- Practice Statement,
- Crypto Concept,
- extracts from documentation corresponding to performed role, including emergency procedures,
- range of responsibilities and obligations associated with the acted role in the system.

5.4 Audit Logging and monitoring Procedures

For the efficient management and operation of mySaveID, all events having a significant impact on the security and reliability of the technological system, the control over the personnel and users, and the impact on the safety of the qualified certification services, are recorded. This is also applies to the supplier and providers of mySaveID, which are obligated and controlled by mySaveID.

mySaveID logs all events relating to the life-cycle of certificates as all events relating to certificates generation and dissemination.

Where applicable, the event logs are created automatically. If it cannot be created automatically, the record is stored on paper. The audit logs/logging files created are permanently analysed for important security and operationally relevant events. Furthermore, mySaveID checks the audit logs/logging files for suspicious and unusual activities as a result of irregularities and faults. mySaveID monitors all relevant logs/systems and an alert would be raised as soon as there is an incidents.

5.4.1 Types of events recorded

Every activity, critical for mySaveID security, is recorded in event logs and archived. Archives are stored in the manner to prevent it from modification or forgery.

mySaveID stores records of every activity generated by any software component within the system. Such entries are divided into three separate categories:

- **system** - when new or additional software is installed; upon startup of systems and applications; in successful attempts to launch and access to hardware and software PKI-components (Public Key Infrastructure of the systems); generation and management of the key pairs and certificates for the CA
- **errors** - record contains information about errors on the level of network protocols and on the level of application modules,
- **audits -** record contains information associated with providing trust services, for example: registration and certificate request, certificate acceptance, certificate and CRL issuance, creation of signatures or seals, etc.

Especially, for the audit logs all registration information including the following are recorded:

- type of document(s) presented by the subscriber / subject to support registration;
- record of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable;
- storage location of copies of applications and identification documents, including the subscriber agreement;
- identity of entity accepting the application;
- method used to validate identification documents, if any.

There are no specific choices in the subscriber agreement.

Detailed list of recorded events depends on the certification policy of certificates issued or confirmed by a specific certification authority or a registration authority.

Audit trail records contain:

- The identification of the operation
- The data and time of the operation (The time used to record events as required in the audit log is synchronized with UTC at least once a day. see section 6.8)
- The identification of the certificate, involved in the operation
- The identification of the person that performed the operation
- A reference to the request of the operation

Only authorized persons from the mySaveID personnel have access to the information in the records.

5.4.2 Frequency of processing log

Processing logs is scheduled at regular intervals depending on the type of log. Policy related to frequency and work procedure related to a particular logs, is detailed in internal documentation.

Audit logs are reviewed periodically for any evidence of malicious activity and following each important operation.

5.4.3 Retention time for Records

Retention period for audit logs are unlimited (according to VDG).

Event logs of IT systems are stored for at least three months. Video recordings of persons and recordings of administrative activities are stored for a period of 90 days. The system time for the archival system is synchronized daily using the DCF77 time signal and reliable time servers (NTP) on the Internet.

5.4.4 Protection of records

Audit log is stored in a dedicated storage within mySaveID infrastructure. Logs are signed and the signature is validated when auditing logs. The access to the audit log is given to a person who does not have operational access to mySaveID Service hardware or software.

An event log may be reviewed solely by the security officer, system administrator or an audit inspector. Access to the event log is configured in such a way that:

- only authorized persons (i.e. auditors and personnel defined above) have the right to read log entries,
- only the security officer may archive or erase files (after their archive) containing registered events,
- it is possible to detect every violation of integrity; it assures that the records do not contain gaps or forged entries,
- no entity has the right to modify the contents of the journal.

mySaveID ensures that the time used to record events as required in the audit log is synchronised with UTC at least once a day.

Also the privacy of subject information is maintained.

5.4.5 Backups of records

Backup copies of entries in the system logs are kept and reliably stored. The mySaveID's procedures require event logs to undergo backup in accordance with an approved schedule.

5.4.6 Audit log accumulation system

Automated audit data is generated and recorded at the application, network and operating system level. Non-electronically generated audit data is recorded by Trusted Roles.

mySaveID ensures mechanism which do not allow for switching off the logging function of mySaveID CA.

5.4.7 Notification system to event-Causing

mySaveID systems (and systems provide and operated by supplier or other providers) are being monitored 24/7/365 days by system operators and by automatic solutions. In the case of activities having an impact on the system security, the security officer and the system administrator are automatically notified (alarmed). In the other cases, the notification is addressed only to the system administrator.

Information transmission to authorized persons about critical – from the point of view of the system security – situations is carried out by other, appropriately secured, means of communication, for example, mobile phone, electronic mail or physically.

5.4.8 Vulnerability assessment

This Policy requires performing vulnerability assessment analysis of every application and information system on public and private IP addresses identified by the TSP and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report. This also applies for subcontractors and service providers of mySAveID, such as specialized data centers,

for reliable and secure colocation and operation of server and network equipment, providers of identity proofing services, IT services and others.

Requirements for analysis may be also determined by an external institution, authorized to carry out external or internal audit.

Scan of vulnerabilities are held four times a year and provides a reliable report. Process of vulnerability assessment at mySaveID is established based on requirements from ISO 27001. The System Administrator is responsible for this process.

The issues found in Vulnerability assessment are documented as tickets scheduled and prioritized. Following the priority the resulting are implemented as needed.

5.5 Records Archival

5.5.1 Types of archives

mySaveID archives all data and files related to:

- the registration information
    - All documents and data used in the process of identity verification are subjected to archiving
- the system security;
- all requests submitted by users;
- the whole user information;
- all keys and certificates used by the Certification Authorities and the Registration Authority;
- and the whole correspondence between mySaveID and the users.
- Information about the certificate life cycle

mySaveID keeps archives in a retrievable format. It could be paper and electronic carrier.

5.5.2 Retention period of archives

During the operation of msg mySaveID GmbH, the archived data (in paper form and electronically) is archived in accordance with the requirements of VDG § 16.4 and stored over the validity period of the certificates.

5.5.3 Protection of archive

Electronic archive is stored in a dedicated storage within mySaveID infrastructure. Paper archive is stored in a special safe.

Access to the archive have only authorized persons performing trusted roles in mySaveID.

The media holding the archive data and the applications required to process the archive data are maintained to ensure that the archive data can be accessed for the time period required.

5.5.4 Backup archives procedures

The archive is backed up in order to protect data and to enable restoring the system after a failure and stored in a secure safe. Detailed procedures of performing backup copies are regulated by internal policies.

5.5.5 Requirements for time-stamping the archives

The Archives containing audit records are time-stamped by a qualified time-stamping service..

5.5.6 Archive storage

The archive data collecting system is a mySaveID internal system.

5.5.7 Archival information access and verification procedures

Access to the archive is only available to authorized mySaveID employees after a successful authentication and confirmation of access rights.

To verify the integrity of archived information, data may be periodically tested and verified against original data (if still accessible in the system). This activity may be carried out solely overseen by the security inspector and should be recorded in the event logs.

If any damages or modifications to original data are detected, the damages are to be removed as promptly as possible.

5.6 Key Changeover

The key exchange procedure refers to Certification authority keys used for signing certificates, and seals, CRLs. The exchange of keys of certification authorities is performed in the manner ensuring keeping the agreed minimum certificates validity period. Before the expiry of the certificate of a certain authority a new, independent public key infrastructure is created under which a new pair of keys and a certificate of the new Certification authority is generated. Until the expiry of the old certification authority's certificate, both authorities operate. The new Certification authority takes over the role of the expiring one, performs all activities related with servicing certificates: generating, suspending and revoking certificates, generating CRL. The expiring certification authority processes only revoking and suspending certificates issued within its own infrastructure and generate CRLs until its operating activity ceases (the certificate expires).

A new Certification authority's certificate is published in the repository (chapter 2). Information on changing keys may be published in the mass media.

5.7 Compromise and Disaster Recovery

This chapter describes procedures carried out by mySaveID in abnormal situations (including natural disasters) to restore a guaranteed service level. Such procedures are executed in accordance with the accepted plan disclosed in Disaster Recovery Plan.

5.7.1 Incident and compromise handling procedures

All information about possible incidents are communicated to the Security Officer of mySaveID who assigns the performance of activities under the procedures developed.

- These procedures are designed to analyze the intensity of an attack or failure, investigate the incident, to minimize its effects and eliminating it in the future. By this mySaveID acts in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security.
- If necessary, in the case of mySaveID private key compromise or other corruption events appropriate steps must be taken with the Disaster Recovery Plan including.

This also applies to suppliers and service providers of mySaveID which have been obliged by mySaveID to define their own roles for incident management, to staff them appropriately and to inform mySaveID of any relevant incidents via contractually agreed channels.

At least once a year mySaveID tests the effectiveness of the procedures.

The incidents can be submitted using either internal or external submission forms (mySaveID website with contact form), or as an email to support@msg.com or even by the contact phone number. The response time by the Incident Evaluation Team is determined by the severity of the incident but is no longer than 24 hours on working days. The objective of Incident Management is the immediate response and recovery of availability and the continuous protection of mySaveID certificate services.

mySaveID has established procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.

In case of private CA key compromise mySaveID will additionally:

- Indicate that mySaveID Certificates and validity information issued using this CA may no longer be valid via information on the website and a press release;
- Revoke any CA certificate that has been issued for the compromised TSP when a TSP is informed of the compromise of another CA.
- Inform the Supervisory Body regarding a certificate revocation so that the National Trusted List can also be updated accordingly;
- Inform all affected Subjects and Relying parties.

In case of algorithm or associated parameters become insufficient for its remaining intended usage mySaveID will additionally:

- Schedule a revocation of any affected mySaveID Certificates;
- Inform all affected Subscribers and Relying parties.

Any critical vulnerability (e.g. the algorithms, or associated parameters, used by the TSP or its subscribers become insufficient for its remaining intended usage) is addressed no later than 48 hours after its discovery; the vulnerability is remediated, or a mitigation plan is created and implemented to reduce the impact of vulnerability or a decision has been made and documented that remediation is not required. In the event of an emergency, mySaveID will inform all the Subjects and Relying Parties immediately (or at least within 24 hours of the crisis

committee's decision) of the emergency situation and proposed solution through public information communication channels. mySaveID will inform without undue delay but in any event within 24 hours after having become aware of it, the Supervisory Body and, where applicable, other relevant bodies as national CERT of any breach of security or loss of integrity that has a significant impact on the mySaveID certificate services provided.

If a data breach is likely to involve personal data and is likely to result in high risk to the rights and freedoms of the natural person, mySaveID will notify the natural or legal person of the breach of security or loss of integrity without undue delay. mySaveID will also notify the relevant Authorities (Supervisory Authority, Data Protection Authority) without undue delay, but at least within 24 hours after initial discovery of the personal data breach.

Any provider or supplier has to notify mySaveID about a data breach that is likely to involve personal data without undue delay to.

5.7.2 Incidents, related to failures in hardware, software and/or data and attacks

All information about corruption of computing resources, software and/or data are communicated to the Security Officer who assigns the performance of activities under the procedures developed. This also applies to suppliers and service providers of mySaveID which have been obliged by mySaveID to define their own roles for incident management, to staff them appropriately and to inform mySaveID of any relevant incidents via contractually agreed channels.

These procedures are designed to analyze the intensity of an attack, investigate the incident, to minimize its effects and eliminating it in the future. By this mySaveID acts in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security.

If necessary, in the case of mySaveID private key compromise or other corruption events appropriate steps must be taken with the Disaster Recovery Plan including.

5.7.3 Private key compromise procedures

mySaveID key compromise is handled according to internal Incident Management documentation and considered to be a disaster. In case of a CA's key compromise the revocation status of the CA certificate is published via the open accessible repository as well via a dedicated message (email) to all subscribers and subjects. The disaster recovery plan includes that all subject certificates are revoked.

5.7.4 Business Continuity Management

mySaveID has developed a Business Continuity Plan which is periodically tested and maintained up-to-date and which shall be adopted in case of an accident. This document governs the preparation and processes to ensure the preservation of the mySaveID activity. The aim is to achieve continuity in the company's operations and business protection when there are major disruptions of normal commercial operations.

mySaveID Business Continuity Plan includes at least:

- The conditions for activating the plan.
- Emergency procedures.

- Resumption procedures.
- A maintenance schedule for the plan.
- The responsibilities of the individuals.
- Recovery time objective (RTO).
- Regular testing of contingency plans.
- What constitutes an acceptable system outage and recovery time.
- How frequently backup copies of essential business information and software are taken.
- The distance of recovery facilities to the mySaveID's main site

All suppliers and providers are obliged also to develop a Business Continuity Plan fulfilling the contractual requirements given by mySaveID.

In case of an accident and failure of critical components of the technological system, including hardware, software or compromising of a private key of mySaveID, the operations are resumed within the delay period established in the continuity plan. The reasons for the accident are analyzed, suitable measures for its elimination are undertaken and measures are defined to prevent its recurrence.

The security policy, followed by mySaveID, takes into consideration the following threats influencing the continuity of the services provided:

- physical corruption to the computer system of mySaveID, including network resources corruption – this threat addresses corruptions originating from random situations,
- software and application malfunction, rendering data inaccessible – such corruptions address operating system, users' applications and execution of malicious software, for example viruses, worms, Trojan horses,
- loss of important network services, associated with mySaveID interests. It primary addresses power cuts and damages of the network connections,
- corruption of a part of the network, used by mySaveID to provide its services – the corruption may imply obstruction for the customers and denial (unintended) of services.
- compromise, loss or suspected compromise of a CA's private key as a disaster.

To prevent or limit the losses of the above threats, as an adequate security policy, mySaveID undertakes the following:

- all Subjects and relying parties shall be informed as quickly as possible and in a way best suited to the existing situation;
- regular creation and archiving copies of all components of the mySaveID infrastructure, stored in a well-protected and safe place;
- periodic creation of a backup copy of the database, including all filed requests, issued, renewed, and revoked certificates. Backup copies are archived and stored in a well-protected and safe place;
- periodic creation of a backup copy of data necessary to resume CA operations, stored in safe places (different fire zones), suitable to allow the TSP to timely go back to operations in case of incident/disasters.
- periodic creation of a backup copy of each server;

- periodic testing of backup copies.
- mySaveID private keys are divided in accordance with the security procedures and by secret sharing. They are kept by trusted individuals in a safe and protected place; the replacement of resources is done in a way allowing the recovery of the most recent data.

Backup facilities are provided and monitored. Backups are made on a daily basis and after changes. Backups are stored in a different fire zone. Back-up arrangements are regularly tested to ensure that they meet the requirements of business continuity plans.

The system recovery procedures are tested on each component of the mySaveID IT system at least once a year. These tests are part of the internal audit. Any change in the system requires the consent and acceptance by the security administrator. In every post-disaster system recovery, the system administrator together with Security Officer performs the following:

- If risk analysis identifies information requiring dual control for management, for example keys, then dual control is applied to recovery;
- changes all previously used passwords;
- removes all access rights to the system resources;
- changes all codes and PIN numbers associated with the physical access to the facilities and system components;
- if the recovery from the accident involves reinstallation of the operating system and utility software, all IP addresses in the system and its subnets are changed;
- Review analysis of the disasters causes.

To perform the system recovery, the System Operator requires approval from the System Administrator.

5.8 TSP Termination

5.8.1 Termination plan

mySaveID has an up-to-date termination plan for ensuring an orderly winddown because of cessation of the company operations.

When the services are terminated, mySaveID shall notify customers, certificate holders and third parties, including relying third parties and the competent supervisory authority (BNetzA Federal Network Agency), of the discontinuation of the qualified certification services. All certificates issued by the CAs concerned which are still valid are revoked. The private CA keys concerned, including backup copies, are destroyed in such a way that private keys cannot be recovered.

mySaveID will publish final CRLs as described in section 4.10.1

In the event of scheduled discontinuation of its operations, mySaveID shall notify customers and subscribers, certificate holders and third parties, including relying third parties and the competent supervisory authority (BNetzA Federal Network Agency), of the discontinuation of the qualified certification services at least 90 days in advance.

In addition, all further contractual relationships with third parties concerning the provision of trust services by mySaveID shall be terminated upon discontinuation.

The certificate databases together with the revocation information and the repository (TSP, CPS and CA certificates) are transferred to the Federal Network Agency in accordance with sec. 16 (1) VDG.

mySaveID declares to maintain documents and data resulting from the content of the CPS and the Policy and data required to verify the correctness of the Trust Services, including documents and data for a indefinite period of time.

Funding to cover the Efforts of the orderly cessation of operations is secured. mySaveID GmbH has an appropriate assurance from msg systems ag for the fulfillment of these minimum requirements.

6 Technical security controls

The descriptions contained in this section refer to the trust services that are referred to in this CPS and which are under the control of mySaveID.

[ETSI 319 401] REQ-7.7-01 The TSP shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

6.1 Key pair generation and installation

6.1.1 Key pair generation

CA keys and keys for service certificates (e.g. used by revocation and registration services) are generated in a “FIPS 140-2 Level 3” OR a CC-evaluated (according to Protection Profile EN 419 211-5) hardware security module (HSM). The HSM is located in the high-security area of the TSP. The mentioned keys are generated during a planned structured key ceremony.

The key ceremony takes place according to defined procedures. Depending on the CA, the key ceremony is performed by trusted roles in the presence of the security officer and, if necessary, under the supervision of an independent third party. The activities during the key ceremony are checked and recorded using a checklist. During key generation, the enforcement of the role concept and thus the 4-eyes principle is enforced by the voluntary entry of the activation data for signature generation of the CA certificate. The number of personnel authorized to carry out CA key pair generation is kept to a minimum and be consistent with the TSP's practices.

The definition of the key ceremony indicates, at least, the following:

- roles participating in the ceremony (internal and external from the organization);
- functions to be performed by every role and in which phases;
- responsibilities during and after the ceremony; and
- requirements of evidence to be collected of the ceremony.
- The TSP shall produce a report proving that the ceremony, as in GEN-6.5.1-11 above, was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured.

"This report shall be signed

- For root CA: by the trusted role responsible for the security of the TSP's key management ceremony (e.g. security officer) and a trustworthy person independent of the TSP's management (e.g. Notary, auditor) as witness that the report correctly records the key management ceremony as carried out.
- For subordinate CAs: by the trusted role responsible for the security of the TSP's key management ceremony (e.g. security officer) as witness that the report correctly records the key management ceremony as carried out. "

CA key pair and subject key pair generation is performed using an algorithm as specified in ETSI TS 119 312 [i.10] for the signing purposes.

Whenever CA keys are generated, an independent auditor is present if necessary or, following key generation, the auditor can use a video recording in order to verify that the key generation process was carried out correctly. Furthermore, the creation of CA keys and, if applicable, service certificates will be documented depending on the policy level.

CA keys, including keys used by revocation and registration services, are generated securely and the private key are kept secret.

Subscriber and subject keys are generated and stored by the TSP. The keys are generated with the help of an CC-evaluated (according to Protection Profile EN 419 211-5) hardware security module (HSM) in the secure environment of the trust service provider and in accordance with the requirements of [EN 319 411-1] and [EN 319 411-2] and future access to private key is managed by Entrust Signature Activation Module which is a software component that interacts with the Cryptographic Module (CM) in order to implement a Signature Activation Module (SAM) according to the European Standards. Private subscriber and subject keys can be transferred from the cryptographic module only by the trust service provider. The key will never leave the module in a non-encrypted form.

QCP-n-qscd, QCP-l-qscd: The TSP uses qualified signature/ seal creation devices only and, as long as the qualified certificates issued are valid, monitors the status of the corresponding qualified signature/ seal creation device within the meaning of [EN 319 411-2].

As long as the HSM have their qualified Status we use it for the operation as TSP. If the HSM loose the qualified Status mySaveID shut down the system at the latest with the termination of QSCD-Status. If valid certificates exist at this time, they will be revoked.

mySaveID monitors the validity period of the QSCDs used. It is ensured that no certificates are issued that have a validity period that is longer than the validity period of the QSCD or, alternatively, it is ensured that the certificates are revoked when the validity of the QSCD expires.

6.1.2 Private key delivery to subscriber or subject

The private keys are not delivered to the subscriber and subject. The private keys remain in the secured area of the TSP as long as they are used and are only used within a secure cryptographic device (HSM) of mySaveID. The TSP ensures that the subject has sole control (or if the subject is a legal person, "control") over its private key.

6.1.3 Public key delivery to certificate issuer

The TSP does not accept any public keys from external bodies.

6.1.4 CA public key delivery to relying parties

The CA public key is contained in the CA certificate. This certificate is available to the subscriber and subject for download. The CA and service certificates are available from the public repository that is also pointed in end entity certificates as part of Authority Information Access (AIA) in an X.509 v3 certificate extension.

The root CA certificate is included in the trusted list of the national Supervisory authority.

6.1.5 Key sizes

The keys of all certification authorities of mySaveID are RSA keys and have 4096 bits. Keys of the subscribers and subjects are RSA keys and have at least 2048 RSA bits.

6.1.6 Public key parameters generation and quality checking

Public key generating parameters meet the requirements specified in the ETSI EN 319 401, ETSI EN 319 411 and ETSI TS 119 312 norms in their latest applicable version.

6.1.7 Key usage purposes

Private root CA keys are exclusively used to sign CA certificates, service certificates (e.g. OCSP service certificates) and certificate revocation lists. Same for other private CA keys are used to sign CA certificates, service certificates, subscriber and subject certificates and certificate revocation lists (see 7.1.2).

The subscriber and subject keys may only be used for the types of use stated in the certificate. The types of use are defined in the keyUsage and extKeyUsage fields in the certificate and may be restricted by further extensions.

The operating CAs will not use the CA private signing keys beyond the end of their life cycle.

The use of CA's private key is be compatible with the hash algorithm, the signature algorithm and signature key length used for generating certificates, in line with current practice of mySaveID.

6.2 Private key protection and cryptographic module engineering

6.2.1 Cryptographic module standards and controls

Throughout their entire life cycle (including delivery and storage), the modules are protected against manipulation by suitable technical and organizational controls. The CA keys are protected by an HSM that was evaluated according to FIPS 140-2 Level 3. Also the service, subscriber and subject keys are protected by HSMs meeting the requirements for a qualified signature creation device within the meaning of the eIDAS Regulation.

6.2.2 Private key (n out of m) multi-person control

The cryptographic module on which the service, CA and subscriber and subject keys are stored is located in the secure environment of the trust service provider. Two authorized persons are needed to activate the respective private key and to access the private subscriber and subject keys.

6.2.3 Private key escrow

The TSP does not offer escrow of private subscriber and subject keys.

6.2.4 Private key backup

A backup of the private CA keys exists. A CA key backup must be carried out at the HSM by two persons authorized for this activity and takes place in the secure environment of the trust

service provider. The backup system is subject to the same requirements and backup measures as the productive system.

Service keys stored on a smart card are not secured. Availability is ensured by providing several service keys on redundant smart cards.

Recovery of private keys also requires two authorized persons. Further copies of the private CA keys do not exist.

6.2.5 Private key archival

Private CA and subscriber and subject keys are not archived.

6.2.6 Private key transfer into or from a cryptographic module

Transfers of private CA keys to or from the HSM are limited to backup and recovery purposes. Adherence to the 4-eyes principle is compulsory. Private CA keys exported to/imported from another HSM are protected by encryption.

Private subscriber and subject keys can be transferred from the cryptographic module only by the trust service provider. The key will never leave the module in a non-encrypted form.

6.2.7 Private key storage on cryptographic module

The private keys for CA and service certificates are contained in encrypted form in the HSM.

Subscriber and subject keys are encrypted with the help of an HSM according to ETSI TS 119 431-1 and contained in a database of the TSP.

6.2.8 Method of activating private key

The private CA and service keys can only be activated according to the 4-eyes principle, by the authorized roles and for the permitted types of use (keyCertSign, cRLSign).

Private subscriber and subject keys are activated by the end-entity using the authentication features and for the permitted types of use. It is the subscriber's and subject's responsibility to protect its authentication credentials.

6.2.9 Method of deactivating private key

The private keys for CA and service certificates are deactivated by termination of the connection between the HSM and the application by the Trusted Roles provided for this purpose.

Subscriber and subject keys are deactivated as soon as they have been used once.

6.2.10 Method of destroying private key

When the scheduled useful life of the private CA keys expires, these keys are deleted by the trusted roles provided for this purpose. Useful life is determined in accordance with ETSI TS 119 312. This is accomplished by deleting the private key on the HSM and simultaneous deleting of the backups on data media. When the HSM is shut down, the private keys in the device are deleted. When files containing the private subscriber and subject key are deleted, the private key is then also destroyed.

Service keys stored on smart cards are deleted by destroying the card.

6.2.11 Cryptographic module rating

The TSP operates suitable hardware-based and software-based key generators according to [EN 319 421] or [EN 319 411-1] and [EN 319 411-2].

Signature creation data managed by mySaveID on behalf of subscriber or subject are generated in a qualified electronic signature and seal creation devices (QSCD) which meets the requirements specified in Annex II of eIDAS.

mySaveID monitors the validity period of the QSCDs used. It is ensured that no certificates are issued that have a validity period that is longer than the validity period of the QSCD or, alternatively, it is ensured that the certificates are revoked when the validity of the QSCD expires.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public service, CA and subscriber and subject keys are archived in the form of the certificates generated. Public CA keys are stored for at least 10 years.

6.3.2 Certificate operational periods and key pair usage periods

The term of validity of the service and CA keys and certificates is variable and shown in the certificate. The maximum possible validity period totals 30 years. The term of validity of the subscriber and subject keys and certificates is variable and shown in the certificate. The maximum possible validity period totals 36 months. In any case the operating CAs do not issue certificates whose lifetime exceeds that of the CA's signing certificate.

6.4 Activation data

6.4.1 Activation data generation and installation

The activation data of the service and CA keys is requested by the smart card or HSM. Adherence to the 4-eyes principle is compulsory.

The authentication feature is generated by the subscriber and subject and closely linked to the subscriber and subject within the scope of identification.

The second authentication factor is generated by the TSP and transferred to the end-entity via a separate channel (SMS). Validation is if selective and corresponding for user private key can be activated used for signing is under the control of Signature Activation Module.

6.4.2 Activation data protection

The activation data of the service and CA keys is made up of two secrets with one authorized employee each knowing one of these. Only authorized employees can access the activation data.

The subscriber is responsible for protecting his or her authentication features.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

mySaveID administer user access of operators, administrators and system auditors. Also, the administration includes user account management and timely modification or removal of access.

The TSP's system access is limited to authorized individuals

6.5.1 Specific computer security technical requirements

mySaveID ensures that the TSP's system components are secure and correctly operated, with an acceptable risk of failure.

The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. The TSP's components include the following security mechanisms:

- Require authenticated logins for trusted role;
- Provide discretionary access control with least privilege;
- Provide security audit capability (protected in integrity);
- Require use of strong password policy;
- Require use of cryptography for session communication;
- Require trusted path for identification and authentication;
- Provide means for malicious code protection (e.g. viruses);
- Provide means to maintain software and firmware integrity;
- Provide domain isolation and partitioning different systems and processes;
- Provide self-protection for the operating system
- For accounts capable of directly causing certificate issuance, Issuing CA shall enforce multifactor authentication.

6.5.2 Computer security rating

No stipulation

6.6 Life Cycle Technical Controls

6.6.1 System development controls

The system development controls for mySaveID are as follows:

- An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by mySaveID.
- The software will be approved by the Security Officer and shall originate from a trusted source.
- The hardware and software are dedicated to performing CA activities. There are no other applications, hardware devices, network connections, or component software installed which are not part of the CA operation.

- New versions of software are tested in a testing environment of the appropriate service and their deployment is conducted according to documented change management procedures.
- Changes to systems are documented.
- Control of the cryptographic modules creation includes requirements imposed on design, manufacture and delivery of cryptographic modules. mySaveID does not define its own requirements in that matter.
- All hardware will be inspected during commissioning process to ensure conformity to supply, and no evidence of tampering found. Hardware security modules are subject to special commissioning process.

6.6.2 Security management controls

Security controls are implemented within information security and privacy management system of mySaveID, including all workstations for guaranteeing the integrity of software and configurations, as well as for detecting fraudulent software and restricting its spread.

Current configuration of mySaveID system, as well as any modifications and updates to its system are recorded and controlled and protected against viruses, malicious and unauthorized software.

A formal change configuration process is used for installation and on-going maintenance (including patches) of mySaveID systems. Security patches are applied within a reasonable time after they come available; security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; in that case the reasons for not applying any security patches are documented.

Capacity demands are monitored and projections of future capacity requirements are made to ensure that adequate processing power and storage are available.

6.6.3 Life cycle security controls

mySaveID policies, assets and practices for information security are regularly reviewed by a Security Officer reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness. The implemented controls are also verified as part of the risk assessment procedure.

The evaluation of the security controls is verified using various methods, such as: penetration tests, configuration audits, internal audits.

This Policy requires undergoing a penetration test on the TSP's systems at set up and after infrastructure or application upgrades or modifications that the TSP determines are significant. mySaveID records evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

This also applies for subcontractors and service providers of mySaveID, such as specialized data centers, for reliable and secure colocation and operation of server and network equipment, providers of identity proofing services, IT services and others.

6.7 Network Security Controls

mySaveID uses subcontractors and service providers, such as specialized data centers, for reliable and secure colocation and operation of server and network equipment and networks. mySaveID has defined requirements and security controls to protect the internal network domains from unauthorized access. The mentioned subcontractors and service providers have to fulfill the requirements which is controlled on a regular base by mySaveID.

mySaveID's TSP networks are divided into several logically separated segments:

- High security zone (protected area of the certification authority including the key servers, certificate issuance servers and HSMs (high security moduls)) with no direct Internet access
- Normal security zone based on ISO 27001 controls including:
    - Operators workstations
    - Administrators workstations
    - DMZ area with frontend systems

For each segment, a security policy has been implemented in the context of physical and organizational security measures.

All parts of the network are protected by firewall whose rules are approved by mySaveID to prevent all protocols and accesses not required for the operation of the TSP. Also the TSP's internal network domains is protected from unauthorized access including access by subscribers and third parties by it.

mySaveID ensures that only the protocols needed for mySaveID services are allowed through the firewall. Each of the above area have a separate traffic policy filtering policy. Access to the administrative interfaces of IT equipment is not directly accessible from the public Internet. For the most critical tasks a separate workstation is used.

The front-end systems which are in a DMZ are protected by a firewall and TLS offload servers.

The security of mySaveID's internal network and external connections is constantly monitored to prevent all access to protocols and services not required for the operation of the Trust Services.

At least once a year, penetration tests covering mySaveID systems are conducted. In addition, mySaveID runs at four vulnerability scans per year (one per 3 months). Both types of tests are performed by a professional service provider. The issues found in penetration tests are documented as tickets scheduled and prioritized. Following the priority the resulting are implemented as needed.

All mySaveID system accounts and user permissions are reviewed according to access control policy and at the request of mySaveID executives. Any system, services and network accounts that are not used are blocked or deactivated. TSP configures all CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

All external network connections to the mySaveID system are secured with the TLS protocol.

Any changes in mySaveID network devices require the prior approval of Security Officer. The change is implemented only after verification by the administrator who did not take a direct part in creation of changes.

6.7.1 Network Security

mySaveID has introduced and implemented procedures and measures to secure, manage and control networks and network devices to protect information in systems and applications.

The following applies to the protection of data and information in networks and to the protection of networked services:

- Responsibilities, rules and procedures for the management of networks are defined.
- The rules and procedures ensure that data and information are protected against loss of confidentiality and integrity during transmission over the network.
- Administrative activities and network activities that are relevant to information security are logged and monitored.
- Unused connection options are explicitly prohibited or deactivated.
- systems used for administration of the security policy implementation are not used for other purposes.

6.7.2 Security of Network services

Security mechanisms, quality of service and service requirements of network services are identified, implemented, and monitored to ensure security in the use of network services.

The following applies to the security of information in networks:

- The amount of bandwidth provided, the required security measures (e.g. availability, encryption, authentication) and the troubleshooting resources meet the respective business requirements. Since there is required a high level of availability of external access to the trust service, the external network connection for subscribers and sujects as well as relying parties are redundant (provided by the supplier of mySaveID) to ensure availability of the services in case of a single failure.
- Data and information transmitted via public networks are encrypted.
- The end devices, the server infrastructure and the test network are separated into separate network zones. Also mySaveID separates dedicated network for administration of IT systems and TSP's operational network.
- Network zones are configured using packet filters so that only services, protocols and applications that are actually required, including the permitted source and destination addresses, are enabled.
- An Internet firewall is operated between the internal network of msg mySaveID GmbH and the Internet or other networks.
- Unused services are prohibited or deactivated.
- The following measures apply to the Internet firewall:
    - It is managed by a central set of rules.
    - The Internet firewall filters both incoming and outgoing network traffic and only allow enabled applications or protocols between permitted source and destination addresses.

- All successful and blocked connections, including the volume of data transferred, is logged for at least 90 days and allow detailed analysis.
- Only services that are necessary are activated.
- For liability reasons and for the prosecution of criminal acts, logging is carried out with user assignment.

6.7.3 Segregation of Networks

Groups of information services, users and information systems are separated in the networks to divide the network into security boundaries and control traffic between them based on business requirements and on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services. Cryptographic mechanisms and logical or physical separation are used to establish trusted channels for the communication between distinct trustworthy systems and to provide assured identification of its end points and protection of the channel data from modification or disclosure.

mySaveID keeps all systems that are critical to the TSP's operation (e.g. certificate generation and revocation management services) in one or more secured zone(s) (e.g. Root CA is physically decoupled as a USB device and stored in a safe in the high-security room Room. The active HSMs and SCDs are located in a seperated High Protection Environment in the Data Center).

Any parts of the premises shared with other organizations shall be outside the perimeter of the certificate generation and revocation management services.

There is also a separation of the production systems from the Dev / Test Systems.

To protect the availability of the entire network, different network zones are separated according to function and trustworthiness. The following measures apply:

- Networks are separated either by physical separation or by logical separation with VPN or VLAN segmentation.
- Communication between the network zones is controlled and monitored by firewalls.
- Information processing equipment that has a non-recoverable vulnerability must be operated in a separate network zone.

Access to secure zones and high security zones is only granted to trusted roles.

6.8 Time synchronization

All mySaveID components (also those of suppliers and providers) are regularly synchronized with a reliable time service synchronized with UTC at least once a day. mySaveID uses NTP source clocks to establish the correct time for:

- Initial validity time of a CA Certificate.
- Revocation of a CA Certificate.
- Posting of CRL updates.
- Issuance of Subject end entity Certificates.
- Records of Events

Clock adjustments are auditable events.

mySaveID also uses for archiving external time-stamping service which has been qualified. mySaveID ensures making a cyclical review of this service (status of QTSP and heartbeat) every 24 hours.

7 Certificate and CRL Profiles

The certificates issued by the CAs of the mySaveID meet the requirements of the ITU [X.509], IETF [RFC 5280] and IETF [RFC 6818] standards, as well as ETSI [ETSI EN 319 412].

Profiles of certificates and CRLs are issued in line with norms of ETSI TS 119 412-1 and ETSI EN 319 412 (Parts 2,3,4,5).

7.1 Certificate Profile

7.1.1 Version number

Certificates are issued in X.509v3.

7.1.2 Certificate extensions

CA certificates contain the following critical extensions (“mandatory field”):

Extension	OID	Parameter
keyUsage	2.5.29.15	*keyCertSign, cRLSign*
basicConstraints	2.5.29.19	*Ca=TRUE, (pathLenConstraint)*

CA certificates can include the following non-critical extensions (“optional”):

Extension	OID	Parameter
authorityKeyIdentifier	2.5.29.35	160-bit SHA-1 hash of the issuer key
cRLDistributionPoints	2.5.29.31	Address(es) of the CRL issuing authority/authorities

Further extensions can be added; they must comply with [X.509], [RFC 5280], [RFC 6818], [ETSI EN 319 412] and [ETSI-ALG] or they must be described in a referenced document.

Subscriber and/or subject certificates contain the following critical extensions:

Extension	OID	Parameter
keyUsage	2.5.29.15	*nonRepudiation*

Subscriber and/or subject certificates can include the following non-critical extensions:

Extension	OID	Parameter
authorityKeyIdentifier	2.5.29.35	160-bit SHA-1 hash of the issuer key
subjectKeyIdentifier	2.5.29.14	160-bit SHA-1 hash of the subject public key
cRLDistributionPoints	2.5.29.31	CRL issuing authority as an http and,if applicable, ldap link

authorityInfoAccess	1.3.6.1.5.5.7.1.1	*accessMethod=OCSP* *{1.3.6.1.5.5.7.48.1},* *accessLocation {…}*[12] *accessMethod= caIssuer* *{1.3.6.1.5.5.7.48.2},* *accessLocation {…}*
certificatePolicies	2.5.29.32	OIDs of the CPs supported *cpsURI*
qcStatements	*1.3.6.1.5.5.7.1.3*	**QCP-l-qscd:** esi4-qcStatement-1 {0 4 0 1862 1 1}; esi4-qcStatement-4 {0 4 0 1862 1 4}; esi4-qcStatement-5 {0 4 0 1862 1 5}; esi4-qcStatement-6 {0 4 0 1862 1 6}; id-etsi-qct-eseal {0 4 0 1862 1 6 2} ; **QCP-n-qscd:** esi4-qcStatement-1 {0 4 0 1862 1 1}; esi4-qcStatement-2 {0 4 0 1862 1 2}; esi4-qcStatement-4 {0 4 0 1862 1 4}; esi4-qcStatement-5 {0 4 0 1862 1 5}; esi4-qcStatement-6 {0 4 0 1862 1 6}; id-etsi-qct-esign {0 4 0 1862 1 6 1} ;

Further extensions can be added; they must comply with [X.509], [RFC 5280], [RFC 6818], [ETSI EN 319 412] and [ETSI-ALG] or they must be described in a referenced document.

The list of QSCDs in Germany is made publicly available on the website of the Federal Network Agency (BNetzA). mySaveID monitors the QSCD certification status of the QSCDs it uses. If the QSCD certification status of the QSCDs used is shorter than the regular certificate validity periods, customers will be informed in advance and the certificates will be issued with a shorter certificate validity period from the critical point in time.

However, if a certificate is mistakenly issued on a QSCD with a certificate expiry date that is valid beyond the valid QSCD certification status, the subject/ subscriber will be informed in advance and the certificate will be revoked no later than by the expiry date of the QSCD.

If the TSP becomes aware of changes that affect the validity of the certificate, for instance, because the supervisory body has withdrawn the QSCD certification status, all affected certificates with “esi4-qcStatement-4” according to ETSI EN 319 412-5 and which are affected by this change of the affected QSCD certification status will be revoked. The subjects concerned and, if applicable, subscribers will be informed of this.

mySaveID applies no size limit regarding IETF RFC 5280 in naming attributes.

7.1.3 Algorithm Object Identifiers

The following signature algorithms are currently used in CA and subscriber and/or subject certificates and in time stamps:

- sha256 with RSA encryption with OID 1.2.840.113549.1.1.11

7.1.4 Name forms

In the subject (here: name of the subject/subscriber) and issuer (name of the issuer) fields, names are assigned according to [X.500] or [X.509] as DistinguishedName. The attributes described in section 3.1.4 can be assigned. Coding is carried out as UTF8 string or PrintableString for the C (Country) attribute.

7.1.5 Name constraints

“NameConstraints” is not used.

7.1.6 Certificate Policy Object Identifier

“CertificatePolicies” can contain the OID of CPS supported.

We fulfil the requirements of our CPS and the ETSI Policies:

0.4.0.194112.1.2 natural person

0.4.0.194112.1.3 legal person

7.1.7 Usage of Policy Constraints Extension

“PolicyConstraints” is not used.

7.1.8 Policy qualifier syntax and semantic

“PolicyQualifiers” can be used.

7.1.9 Processing Semantics for Critical Certificate Extensions

In service, CA and subscriber and subject certificates, the CertificatePolicies extension is not critical. Subscribers and relying parties are free to decide whether this extension is evaluated.

7.2 CRL Profile

7.2.1 Reason for Revocation

7.2.1.1 CA certificates

For revoked CA certificates, mySaveID states the reason for revocation in the reasonCode entry in the CRL. If an entry is required, mySaveID uses one of the following CRLReasons according to RFC 5280, section 5.3.1, which best matches the revocation reason:

- keyCompromise (1),
- cACompromise (2),
- affiliationChanged (3),
- superseded (4) or
- cessationOfOperation (5).

7.2.1.2 Subscriber and/or subject certificates

The subscriber/ subject must select a revocation reason. If the subscriber/subject selects unspecified (0), the reasonCode entry in the CRL remains empty. mySaveID uses one of the following CRLReasons according to RFC 5280, section 5.3.1:

- unspecified (0)
- keyCompromise (1),
- affiliationChanged (3),
- superseded (4) or
- cessationOfOperation (5)

The TSP subsequently enters the following revocation reason as a CRL reason if the subscriber violates the agreed terms and conditions:

- privilegeWithdrawn (9).

If there is evidence that a key has been compromised, but the subscriber failed to document this correctly in the CRLReason, the TSP will then set this value to “keyCompromise”. If the TSP determines that the certificate private key was compromised before the revocation date specified in the CRL entry for that certificate, the TSP will then correct the revocation date. This backdating is an exception and does not usually apply.

7.2.2 Version number

The CRL list profile is compliant with the X.509 V2 standard.

7.2.3 CRL and CRL Entry Extensions

Revocation entries remain in the associated revocation lists after the respective certificate validity has expired.

Certificate revocation lists can contain the following non-critical extensions:

Extension	**OID**	**Parameter**
cRLNumber	2.5.29.20	Number of the certificate revocation list
authorityKeyIdentifier	2.5.29.35	160-bit SHA-1 hash of the issuer key
expiredCertsOnCRL	2.5.29.60	The extension is used only for **QCP-n-qscd, QCP-l- qscd,**
reasonCode	2.5.29.21	If this field is shown, then a CRLReason is used according to section

Revoked certificates are not remove from the CRL revoked certificates after they have expired. after they have expired.

7.3 OCSP Profile

mySaveID provides an on-line certificate status verification service based on OCSP (Online Certificate Status Protocol) in accordance with RFC 6960. The service is provided in the authorized responder mode (Authorized Responder). Responses of the responder are authenticated with a special certificate issued for that purpose by the CA mySaveID EECA.

In addition to RFC 6960, the OCSP responder also supports positive information. (“Certificate is authentic and valid”).

The OCSP responder delivers the following replies:

- “good” if the responder identifies the certificate as not revoked,
- “unknown”if the responder cannot identify the status of the certificate and
- “revoked” if the responder identifies the certificate as revoked.

The “nextUpdate” field is set. The difference between the nextUpdate field and the thisUpdate is at least eight hours, however, it does not exceed 24 hours.

Revocation status information is made available beyond the validity period of the certificate.

The OCPS responder uses the ArchiveCutOff extension as specified in IETF RFC 6960 [i.9], with the archiveCutOff date set to the CA's certificate "notBefore" time and date value.

If OCPS is provided and the CA's certificate is about to expire, the TSP computes a last OCPS answer for each and every issued certificate (whether revoked or not), with the "nextUpdate" field set to "99991231235959Z".

7.3.1 Version number

Responses of the OCSP services generated by the OCSP server are compliant with RFC 6960. The version corresponds to version v1.

7.3.2 OCSP extensions

The OCSP server response contains the OCSP Nonce Extension (OID 1.3.6.1.5.5.7.48.1.2) that contains a phrase linking the query with the response. The value in the OCSP response is the same as the phrase in the query. The purpose of using the phrase is to prevent replay attacks on the OCSP server. Responses of the OCSP server do not contain private extensions.

This dedicated responder shall contain id-pkix-ocsp-nocheck extension.

Responses of the OCSP server do not contain private extensions.

8 Compliance Audit and Other Assessment

The mySaveID management carries out constant operational control for the accurate execution of the instructions, procedures and policies. The audits conducted in mySaveID concern the information data processing and key procedures management.

8.1 Frequency or circumstances of assessment

The conformity of information systems, policies, practices, facilities, personnel, and assets of mySaveID are assessed by a CAB pursuant to the eIDAS regulation, ETSI Standards and relevant national law (see Section 1)

Conformity is assessed at least every 2 years and when any major change is made to Trust Service operations.

mySaveID's internal auditor carries out internal reviews and audits on a rolling yearly schedule.

8.2 Qualification of auditors

mySaveID's CAB is accredited according to ISO/IEC 17065 as profiled by ETSI EN 319 403 and in particular against the requirements defined in the eIDAS Regulation. The CAB is competent to carry out conformity assessments of Qualified Trust Service Providers and its services.

8.3 Auditor's relationship with mySaveID

mySaveID has selected an auditor/assessor who is completely independent from mySaveID.

8.4 Audit scope

The CAB audits all parts of the information system used to provide Trust Services.

The audit by the Conformity Assessment Body covers the entire mySaveID operation for the provision of qualified certification services and implementation of all standards and standardization documents related to Regulation (EU) No 910/2014:

- Documentation;
- Archives;
- Information data related to the issuance and management of qualified certificates;
- Physical and information security and reliability of the technological system and management;

The scope of internal audits includes:

- Verification of the provider's activity and its compliance with the Certificate Policy and Certification Practice Statement;
- comparison of the practices and procedures outlined in this document with their practical realization in the implementation of the mySaveID operation;
- verification of the activity of the Registration Authority;
- other circumstances, facts and activities related to the mySaveID infrastructure.

8.5 Actions Taken as a Result of Deficiency

Where the CAB identifies deviations or non-compliance in the assessment, the Supervisory Body requires mySaveID to remedy these to fulfil requirements within a time limit set by the Supervisory Body. mySaveID makes efforts to stay compliant and fulfil all requirements of the deficiency on time. mySaveID management is responsible for implementing a corrective action plan. mySaveID assesses the deviations or non-compliance items and prioritizes appropriate actions to be taken. If any deviations relate to the protection of personal data, the Supervisory Body shall inform the data protection authority.

8.6 Communication of results

The results of the performed internal and external audits are properly kept in the mySaveID archive.
The certification document received by the Conformity Assessment Body are published on mySaveID's website www.mySaveID.de.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate prices

Remuneration for the services described in this document is laid down in the price list or the respective agreement.

9.1.2 Prices for access to certificates

Certificate requests in the repository service are free of charge.

9.1.3 Prices for revocation or status information

Revocation and the retrieval of status information are free of charge. Revoked certificates are not replaced.

9.1.4 Prices for other services

If offered, refer to the price list or the respective agreement. If the acquisition or temporary loan of hardware or software, especially card readers, has been agreed, this will be deemed compensated by payment of the agreed prices, including the required simple user license.

9.1.5 Rules for cost refunds

The respective agreements with the customer or the General Terms and Conditions [AGB] apply.

9.2 Financial Responsibility

9.2.1 Insurance cover

mySaveID has the means and the financial stability required to operate trust services in a suitable manner. The TSP meets the requirement pursuant to Article 24 (2) lit. c (eIDAS) in conjunction with section 10 of the German Trust Services Act (VDG, Vertrauensdienstgesetz) and, with a view to damage pursuant to Article 13, has taken out liability insurance pursuant to section 10 VDG (€250,000 for each case of damage caused by a liability-triggering event).

9.2.2 Other resources for maintaining operations and compensation for damage

No stipulation.

9.2.3 Insurance or warranty for end users No stipulation

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Definition of confidential business data

The confidentiality of information can be agreed to unless this is already defined in applicable law.

9.3.2 Business data not treated as confidential

All information in issued and published certificates as well as the data referred to in section 0 is deemed to be public.

9.3.3 Responsibilities for the protection of confidential business data

In certain cases, the TSP can be obliged to employ suitable technical and organizational measures to protect data provided to it and deemed to be confidential business data against disclosure and illicit access, and further not to use such data for other unintended purposes or to disclose it to third parties only in as far as such obligation does not violate the law. As part of organizational measures, the employees working for the TSP will be obliged to maintain confidentiality regarding the data in as far as permitted by law.

9.4 Privacy of Personal Information

Processing of personal data is carried out in accordance to GDPR regulation and Bundesdatenschutzgesetz (BDSG). Appropriate technical and organizational measures are described in the information security and data privacy policy and taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

9.5 Intellectual Property Rights

9.5.1 TSP

The applicability and content of copyrights and other IP rights are based on the general statutory provisions.

9.5.2 Subscriber

The subscriber undertakes to comply with intellectual property rights in the application and certificate data.

9.6 Representations and Warranties

9.6.1 mySaveID’s obligations

mySaveID does:

- Provides its services consistent with the requirements and the procedures defined in this CPS and according to the policies under which this CPS is created.
- Provides the service in compliance with eIDAS regulation and related legal acts and standards.
- Provides publicly available repository of relevant documents and information.

- complies with and exacts the procedures described in the present document,
- issued certificates contain accurate data that were actually at the time of their confirmation,
- issued certificates do not contain any mistakes resulting from negligence or procedure violence by the people confirming applications for certificate issuance or issuing certificates,
- it does not copy or store private keys of its subscribers, except for private keys stored in HSM devices,
- protect the integrity and confidentiality of personal data and information acquired as part of service provisioning and not subject to publication.
- inform the Conformity Assessment Body and National Supervisory Body of any changes to a public key used for the provision Trust Services.
- within 24 hours after having become aware of it, notify the Supervisory Body of any breach of security or loss of integrity that has a significant impact on the Trust Service provided.
- within 72 hours after initial discovery, notify the German Authority for Privacy Protection of any personal data breach.
- where the breach of security or loss of integrity or personal data breach is likely to adversely affect a natural or legal person to whom the Trusted Service has been provided, notify the natural or legal person of the breach without undue delay.
- preserve all the documentation, records and logs related to Trust Services according to chapter 5.4 and 5.5.
- have the financial stability and resources required to operate in conformity with this CPS.
- hires employees who possess a knowledge, a qualifications and an experience appropriate to providing trust services.

mySaveID further warrants that it has documented contracts with its subcontracting and outsourcing partners.

mySaveID has defined in these contracts liabilities and ensured that partners are bound to implement any requirements and controls required by mySaveID.

9.6.2 Registration Authorities obligations and warranties

mySaveID uses an internal face to face registration service and external identification proofing service providers as the Registration Authority Service.

mySaveID ensures that registration service used to register users of mySaveID meets the level of assurance equivalent to physical presence in remote identification as set forth in German national state-of-the-art legislation conformant to eIDAS.

In case of external identification proofing services, mySaveID ensures that those services are provided equivalent assurance in terms of reliability to the physical presence. The equivalence is proven by Certification Accredited Body with audit against ETSI EN 319 411-2 or ETSI TS 119 461.

9.6.3 Subjects and Subscribers' obligations and warranties

Subject and Subscriber are committed:

- to comply with the terms and conditions of the trust services provided by mySaveID,
- to state true data in applications submitted to a registration authority,
- to immediately inform mySaveID about any errors, defects or changes in the certificate,
- to protect the credentials necessary for the use of the mySaveID Services and for signature creation against misuse, loss, disclosure, manipulation or unauthorized use, neither communicating nor disclosing them to third parties, and maintaining sole control of them,
- to take all the measures needed to prevent unauthorized use of mySaveID account.
- to treat the loss or revelation of credentials necessary for the use of the mySaveID Services and for signature creation (revealing it to an unauthorized person) as the loss or revelation of the private key (revealing it to an unauthorized person),
- to discontinue using the revoked or expired certificate,
- to stop using mySaveID services as soon as he/she become aware that the mySaveID system as such has been compromised.
- to start without any reasonable delay a procedure of revocation in the case of security violation (or security violation suspicion) of their private keys,
- to use qualified certificate and the corresponding private keys only for the purpose stated in the certificate and in accordance with the aims and restrictions stated in Practice Statement and Trust Service Policy.

9.6.4 Relying Party Obligations and warranties

If the Relying party verifies qualified signatures or qualified seals, it is obliged to use for verification software or service compliant with standards and the following requirements:

- verify if the certificate that supports the signature or seal was, at the time of signing, a qualified certificate for electronic signature issued according to the preset document;
- verify if a qualified mySaveID trust service issued the qualified certificate and the certificate was valid at the time of signing;
- verify if the signature validation data corresponds to the data provided to the relying party;
- verify if the integrity of the signed data has not been compromised.

The relying party shall protect the private data of the subject included in the certificate.

The relying party should not use for validation unknown or unprotected systems provided by a third party.

9.6.5 Representations and warranties of other participants

Any service providers appointed by the mySaveID must comply with this practice statement as well as the information and privacy policies of mySaveID. Service providers whose employees support the operation of the TSP must fulfill additional contractual requirements that guarantee monitoring and control by mySaveID.

9.7 Warranty Disclaimer

9.7.1 TSP's disclaimer

The agreements entered into and the General Terms and Conditions [AGB] apply.

The TSP expressly does not assume any liability, especially for damage that is caused by the use or non-use of certificates without certification or by incorrect use of electronic signatures for which the customer is liable. Any impairment of the functioning of the certificate storage medium, which results from using unsuitable hardware or software, falls under the customer's sphere of risk.

9.8 Limitations of Liability

9.8.1 Limitations of Liability

mySaveID is liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under eIDAS Regulation.

The intention or negligence of a qualified trust service provider is presumed unless that qualified trust service provider proves that the damage referred to above occurred without the intention or negligence of that qualified trust service provider.

Furthermore, the respective agreements, if any, and the General Terms and Conditions [AGB] apply.

9.8.2 Liability for slight negligence

Notwithstanding section 9.8.1, msg mySaveID GmbH's liability in the case of slightly negligent breaches of duty are limited to the direct average damages that are foreseeable and typical for the type of goods and the certification and trust services. This is defined by mySaveID to be an aggregate maximum sum of EUR 100,000 for all claims of the customer.This also applies in the case of any slightly negligent breaches of duty on the part of legal representatives or vicarious agents. msg mySaveID GmbH is not liable to entrepreneurs for any slightly negligent violation of insignificant contractual obligations.

9.8.3 No limitation of liability in special cases

The aforesaid limitation of liability does not apply to product liability claims by the customer. Furthermore, the limitation of liability does not apply to physical injury, damage to health or death of the customer caused by reasons for which msg mySaveID GmbH is responsible. Section 9.8.1remains unaffected by the foregoing.

9.8.4 Liability for identification

The issuing of certificates only confirms that the required proof of identity or proof of legitimization was properly and verifiably submitted to mySaveID at the time of application in accordance with the applicable statutory regulations in Germany and within the scope of the verification options available by msg mySaveID GmbH. In as far as the customer performs the required identity verification on the basis of the verification options with msg mySaveID GmbH, the customer will adhere to msg mySaveID GmbH's requirements for identity verification. In the event that the customer violates such requirements, the customer will indemnify and hold harmless mySaveID with regard to any resultant claims raised by third parties.

9.8.5 Customer's liability

The subscriber and/or subject is liable for any damage which mySaveID may suffer as a result of incorrect information in the certificate caused by the subscriber and/or subject, and as a result of the incorrect use of electronic signatures for which the subscriber and/or subject is responsible. The subscriber and/or subject is also liable for any damage which results from the authorized or unauthorized use of the services rendered by if and to the extent that the subscriber and/or subject is responsible for such damage.

9.9 Indemnities

9.9.1 Claims by the TSP against subscribers

In the event that the customer demands correction of the information specified in its order, the customer will be obliged to bear the costs of such correction on the basis of the agreed prices in as far as the customer was responsible for the incorrect information in the order form, for instance, due to faulty transmission for which the customer is responsible. Furthermore, the respective agreements, if any, and the General Terms and Conditions [AGB] apply.

9.9.2 Claims by the subscriber against the TSP

Agreements, if any, and the General Terms and Conditions [AGB] apply. The customer will only be entitled to offset against claims which are uncontested or have been recognized by a court of law. The customer will only be entitled to exercise a right of retention due to counterclaims resulting from this contractual relationship. Furthermore, the respective agreements, if any, and the General Terms and Conditions [AGB] apply.

9.10 Amendments

9.10.1 Procedure for amendment

This Policy is reviewed at least annually and may be reviewed more frequently. All changes are reviewed and approved by the mySaveID before insertion to public. Changes to this Policy are indicated by appropriate numbering.

mySaveID will post appropriate notice on its web sites of any major or significant changes to this CPS as well as any appropriate period by when the revised Policy is deemed to be accepted.

Modification proposals may be submitted by regular mail or electronic mail for the contract addresses of mySaveID. Suggestions propositions should describe modifications, their scope and justifications and means of contact the person requesting modification.

9.10.2 Notification mechanism of and comment period

Information about every significant modification is submitted to every affected party.

After notification in advance, comments on suggested modifications may be submitted by the affected parties within 14 working days of their announcement.

The only items not requiring notification in advance apply to amendments resulting from implementation of editorial modifications, amendments to the contact information of the person responsible for the document management and changes not having a real impact on considerable group of individuals.

9.10.3 Circumstances under which OID must be changed

No stipulation

9.11 Dispute Resolution Procedures

Complaints regarding adherence to or implementation of this CPS should be submitted in writing to the TSP (msg mySaveID GmbH). If the matter has not been resolved within four weeks after the complaint was submitted, the following applies: Any legal relations between msg group companies, mySaveID and third parties who derive legal relations under this CPS are subject to the laws of the Federal Republic of Germany, barring the United Nations Convention on Contracts for the International Sale of Goods.

9.12 Governing Law and Place of jurisdiction

mySaveID ensures that it operates in a legal and trustworthy manner: (see also Chapter 5 and Subchapters).

This CPS is subject to the laws of the Federal Republic of Germany and the laws of the European Union. Any legal relations between mySaveID and the customer are subject to the laws of the Federal Republic of Germany. The UN Convention on Contracts for the International Sale of Goods is excluded.

The TSP mySaveID, as a company under private law, is subject to the General Data Protection Regulation, the Federal Data Protection Act and the laws of the Federal Republic of Germany.

The place of jurisdiction for any legal disputes is Frankfurt am Main in as far as the customer is a merchant, a legal entity under public law or a special fund under public law, or if the customer does not have a place of general jurisdiction in the Federal Republic of Germany. mySaveID is entitled to enforce its rights at the general place of jurisdiction for the customer. An exclusive place of jurisdiction, if any, will not be affected by the foregoing provision.

9.13 Miscellaneous Provisions

9.13.1 Completeness

The following documents are the subject matter of the applicable agreements involving PKI entities:

- Agreement and application documents

- The General Terms and Conditions [AGB] valid at the time of application or any valid version included
- The CPS in effect at the time of application
- In the case of qualified certificates, the PKI user information valid at the time of application

9.13.2 Differentiation

No stipulation.

9.13.3 Partial invalidity

In the event that one or more of the provisions of this CP are invalid, the validity of the remaining provisions will not be affected by such invalidity.

9.14 Other provisions

9.14.1 Conflicting provisions

The provisions contained in section 9.13.1 are final. They are applicable in relation to each other in the order in which they are enumerated in section 9.13.1 with subordinate effect.

9.14.2 Compliance with export laws and regulations

mySaveID particularly hereby rejects any terms and conditions of the customer, which would involve mySaveID in a boycott that exceeds the applicable statutory EU and UN penalty provisions or would cause mySaveID to make any declarations in this regard.

Right to refuse performance, termination, rescission, disclaimer

In the event that the deliveries or services to be rendered by mySaveID require prior export or import authorization of any government and/or state authority, or in the event that the delivery or service is otherwise restricted or prohibited due to national or international laws, mySaveID is entitled to suspend performance of its obligation to render such deliveries or services or to make payments until such authorization has been granted or such restriction or prohibition has been cancelled. In the event that the delivery or service depends on the granting of export or import authorization and such authorization is not granted, mySaveID will be entitled to terminate or withdraw from the contract at any time. mySaveID will not be held liable if delivery is delayed for any one or more of the reasons listed in this section or if delivery cannot be effected at all due to export regulations unless mySaveID acted intentionally or with gross negligence. The same applies in cases of justified withdrawal or termination.

Undertaking

By accepting the offer, or at the latest by accepting the delivery or service, the customer guarantees that it will not conduct any business with the goods which breaches applicable statutory export regulations and, in particular, that it will perform any further deliveries, transfers or exports of the delivered goods solely in compliance with the applicable statutory export control regulations. The customer undertakes to also impose the above regulations on its customers.

Exclusion of participants

The customer undertakes to ensure that no persons, organizations or institutions are involved in the handling of the contract or will be supported by the contract who/which are listed in the sanction lists of the EU and of the United Nations (in particular, Council Regulation (EC) No 881/2002, Council Regulation (EC) No 2580/2001, Council Regulation (EU) No 753/2011). The foregoing also applies to persons, organizations or institutions named in the sanctions lists of other governments (in particular, the US Denied Persons List, US Entity List, US Specially Designated Nationals List, US Debarred List) in as far as these do not unilaterally go beyond the UN or EU sanctions. The customer further guarantees that neither it nor any of its shareholders are listed on such a list, and that it is not under the control of or a partner of any person or corporate body found on such lists. In the event that the customer or any of its shareholders, or a person or corporate body that the customer is a partner of, is added to a sanctions list during the term of this contract, the customer will be obliged to immediately notify mySaveID in this regard. mySaveID will in such case also be entitled at any time to cancel or withdraw from the contract without the customer being entitled to any claims as a result thereof. Violation against export control laws mySaveID and the customer agree that effective export control by the customer is an important prerequisite for performance of the agreement. mySaveID and the customer will therefore always consider a breach of export control regulations in conjunction with mySaveID products to be a severe violation of the interests of mySaveID. The foregoing is also applicable in the case of any violations committed by third parties. In such case, mySaveID will be entitled to terminate the contract for cause or to withdraw from the contract. The customer is obliged to indemnify and hold harmless mySaveID with regard to any resultant third-party claims for damages. The customer is obliged to compensate mySaveID for other costs and damage, whether tangible or intangible, including, in particular, penalties and fines, which are incurred due to failure to observe the obligations listed in section 9.14.2. Furthermore, the respective agreements, if any, and the General Terms and Conditions [AGB] apply.

9.14.3 Accessibility for persons with disabilities

The trust services provided by mySaveID are made accessible for persons with disabilities, where feasible, taking into account standard EN 301 549. Especially, mySaveID setups of alternative ways to reach the same objectives (e.g. a dedicated support line that persons with disabilities may call if they experience difficulties with the mySaveID Web-Application delivering so that they may be guided efficiently).

9.14.4 Notification of Stage 2 audit and Changes

mySaveID submits the Stage 2 audit with the BNetzA one month in advance and gives the BNetzA the opportunity to take part in it. In addition, mySaveID informs the BNetzA about planned changes to the service.

10 Appendix

10.1 Definitions and Acronyms

auditor: person who assesses conformity to requirements as specified in given requirements documents

authentication: provision of assurance that a claimed characteristic of an entity is correct [SOURCE: ISO 27002:2022]

Certificate Policy (CP): named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

Certificate Revocation List (CRL): signed list indicating a set of certificates that have been revoked by the certificate issuer

certificate: public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it

Certification Authority (CA): authority trusted by one or more users to create and assign certificates

Certification Authority Revocation List (CARL): revocation list containing a list of CA-certificates issued to certification authorities that have been revoked by the certificate issuer

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6

High security zone: specific physical location of the security zone (see ETSI EN 319 401 clause 7.8) where the Root CA key is held

incident handling: any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident

incident: any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems

information security breach: compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed [SOURCE: ISO 27002:2022]

Practice Statement (CPS): statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates (present document)

Publicly-Trusted Certificate (PTC): certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software

Registration Authority (RA): entity that is responsible for identification and authentication of subjects of certificates mainly

registration officer: person responsible for verifying information that is necessary for certificate issuance and approval of certification requests

relying party: natural or legal person that relies upon an electronic identification or a trust service

revocation: permanent termination of the certificate's validity before the expiry date indicated in the certificate

risk: potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of that incident

root CA: certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s)

secure cryptographic device: device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user

secure zone: area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of the systems used by the TSP

short-term certificate: certificate whose validity period, i.e. the period of time from notBefore through notAfter, inclusive, is shorter than the maximum time to process a revocation request as specified in the Practice Statement

subject: entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

subordinate CA: certification authority whose Certificate is signed by the Root CA, or another Subordinate CA

subscriber: legal or natural person bound by agreement with a trust service provider to any subscriber obligations

- the creation, verification and validation of certificates for website authentication; or the preservation of electronic signatures, seals or certificates related to those services
- the creation, verification, and validation of electronic signatures, electronic seals or electronic time-stamps, electronic registered delivery services and certificates related to those services, or

trust anchor: entity that is trusted by a relying party and used for validating certificates in certification paths

trust service policy: set of rules that indicates the applicability of a trust service to a particular community and/or class of application with common security requirements

Trust Service Provider (TSP): entity which provides one or more trust services

trust service: means electronic services normally provided for remuneration by the Trust Services Provider which consists of:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time-stamps, electronic registered delivery services and certificates related to those services, or

- the creation, verification and validation of certificates for website authentication; or the preservation of electronic signatures, seals or certificates related to those service

vulnerability: weakness of an asset or control that can be exploited by one or more threats [SOURCE: ISO 27002:2022]

EU Qualified Certificate: Qualified Certificate as specified in Regulation (EU) No 910/2014

Qualified electronic Signature/Seal Creation Device (QSCD): As specified in Regulation (EU) No 910/2014

10.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CA	Certification Authority
CARL	Certification Authority Revocation List
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DIS	DIssemination Services
FIPS	Federal Information Processing Standard
LCP	Lightweight Certificate Policy
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PDF/A	Portable Document Format/Archive
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PTC	Publicly-Trusted Certificate
RA	Registration Authority
SDP	Subject Device Provisioning
SSL	Secure Socket Layer
TLS	Transport Layer Security
TLS/SSL	Transport Layer Security/Secure Socket Layer protocol
TSP	Trust Service Provider
UTC	Coordinated Universal Time