PKI Disclosure Statement of the msg mySaveID GmbH certification and trust services

This document provides users of the qualified trust services offered by msg mySaveID GmbH, the trust service provider of the msg Group, about the general conditions for the trust service provided.

Document information

Version:	1.0
Date	13.06.24
Status:	☐ in Bearbeitung seit: 02.01.2024 ☐ vorgelegt am: ☒ akzeptiert/abgeschlossen/accepted
Classification	interner Gebrauch
Language:	<English>
Autor:	Christoph Thiel
Dateiname:	MYSAVEID_PDS
German Title:	PKI Disclosure Statement der msg mySaveID GmbH Zertifizierungs- und Vertrauensdienste
Translation:	German
Category (Level):	Directive
Contact person:	Karsten Treiber
Effective date:	13.06.2024
Next review date:	13.06.2025

Dokumentenhistorie

Datum	Version	Änderungsgrund	Bearbeiter (Kürzel)
02.01.2024	V0.8	Erste Fassung/First version	NB, TS, PK, CT
11.06.2024	V0.9	Erweiterte Fassung	NB
13.06.24	V1.0	Akzeptierrt	KTR

Content

1. Introduction

This PKI-Disclosure-Statement (PDS) fulfils the publication requirement specified under European standard ETSI EN 319 411-1, regarding the certification service offered by Qualified Trust Service Provider msg mySaveID GmbH, ("QTSP" or "CA" hereinafter) and is intended to provide applicants for the service with technical information necessary for its use. Regulation (EU) No. 2024/1183 of 20 May 2024 and the (EU) No. 910/2014 of 23 July 2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, is referred to hereinafter as the "eIDAS Regulation". The present document accompanies the Terms and Conditions of service and constitutes an integral part of the msg mySaveID GmbH contract documentation. The publication of this PDS does not replace the publication of the Certification Practice Statement (CPS) or Terms and Conditions (AGB), which provides more detailed information and is available on the msg mySaveID GmbH website at the following link: https://www.mySaveID.de/repository/.

1. Contact details

Your trust service provider (TSP):

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

Email: info@mysaveid.de

Phone number: +49 69 580045-4000

3. Revocation of certificates

- Revocation requests can be submitted via the msg mySaveID GmbH web application if the party applying for revocation can unambiguously authenticate itself to the interface using the agreed access data. In addition, a revocation can be requested (in writing) via the contact options.
- If you want to revoke your own certificate log in to the mySaveID web application (https://id.mySaveID.de/), go to your user profile and revoke your certificate under the "Signature" menu item.
- If your certificate contains further information (such as a company name) involving third parties, these are then also authorized to have your certificate revoked. Revocation by third parties authorized to revoke certificates takes also place via the online interface.

The revocation request submitted via the online interface will be immediately executed. Retroactive revocation is generally not possible. Temporary revocation or suspension of certificates is not offered. A certificate, once revoked, cannot be restored, i.e. the revocation process is final and irreversible.

4. Qualified trust services

Types of qualified trust services offered

Trust service	Applicable policies
Creation of qualified certificates for natural persons on a High Security Module (HSM) at the TSP	▪ ETSI 319 411-2 QCP-n-qscd ▪ Certification Practice Statement and Trusted Service Policy of the msg mySaveID GmbH
Creation of qualified certificates for legal entities on a High Security Module (HSM) at the TSP	▪ ETSI 319 411-2 QCP-l-qscd ▪ Certification Practice Statement and Trusted Service Policy of the msg mySaveID GmbH

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.

msg mySaveID GmbH as a qualified trust service provider holds a certificate of conformity with the above-stated policies for the above-mentioned services.

The certificates can be used for applications which are compatible with the types of use shown in the certificate (key use and extended key use). Relying parties are solely responsible for their acts.

The rules of the Certification Practice Statement and of the Terms and Conditions (AGB) of msg mySaveID GmbH also apply.

Msg mySaveID GmbH also provides remote electronic signature services on Qualified Electronic Signature Creation Devices (QSCDs), generating and managing keys and certificates for the signatory.

Possible restrictions in qualified certificates and archiving period

Trust service	Possible restrictions	Archiving period
Creation of qualified certificates for natural persons on a High Security Module (HSM) at the TSP	Certificate restrictions, if any, are shown in the certificate itself (for instance, test certificates, monetary limit).	The German Trusted Services Act (Vertauensdienstegesetz) in conjunction with the German Trust Services Regulation (Vertrauensdiensteverordnung) requires permanent storage of certificate data.
Creation of qualified certificates for legal entities on a High Security Module (HSM) at the TSP		

Msg mySaveID GmbH also provides remote electronic signature services on Qualified Electronic Signature Creation Devices (QSCDs), generating and managing keys and certificates for the signatory.

The validity period of every certificate is stated in the selfsame certificate and can vary from to three years and three months maximum. It is forbidden to use the certificate outside of the limits and settings specified in the CPS and in contracts, and at all events in breach of the limits of usage and value (key usage, extended key usage, user notice) indicated in the certificate. Event logs connected with the issue of certificates are preserved in the compliant data storage System of informatic documents of mySaveID, for an unlimited time from the date of expiration of the certificate.

Information on the legal effect

The legal effect of the electronic signature, seal and time stamp is defined in Regulation (EU) No 910/2014 of the European Parliament and of the Council, in short: eIDAS Regulation.

Sec. 13 (1) No. 3 of the German Trust Services Act (VDG, Vertrauensdienstegesetz), i.e. of the law implementing the eIDAS Regulation, stipulates that the trust service provider must inform the public pursuant to Sec. 13 (1) VDG of the legal effect of the qualified trusted services offered. We would like to inform you in the following section of the legal effect of our qualified trust services.

Legal effect of the electronic signature and the electronic seal

A qualified electronic signature has the same legal effect as a hand-written signature (Art. 25 eIDAS Regulation). A qualified electronic signature based on a qualified certificate issued in a Member State is recognized as a qualified electronic signature in all other Member States.

Pursuant to sections 126 and following of the German Civil Code [§§ 126 ff BGB], the legal "qualified electronic signature" has the same effect as a hand-written signature under civil law if

the signed document additionally bears the signatory's name ("electronic form") and if such electronic form is not explicitly ruled out by law.

The legal effect of a qualified seal certificate is determined in the eIDAS regulation as follows:

Presumption of the integrity of data and of the accuracy of the stated source of the data with which the qualified electronic seal is associated (see Art. 35 (2) eIDAS Regulation).

Section 371a of the German Code of Civil Procedure [§ 371a ZPO] Evidentiary value of electronic documents

The provisions concerning the evidentiary value of private instruments are analogously applicable to private electronic documents which are provided with a qualified electronic signature. The prima-facie evidence of authenticity of a statement available in electronic form which is based on the verification of the qualified electronic signature according to Article 32 of the eIDAS Regulation (EU) Nr. 2024/1183 and the (EU) No 910/2014 can only be questioned by facts which cast serious doubt on whether the statement was made by the person responsible for this.

This means that anyone who can use your sign-me account, i.e. has access to your login data and the second authentication factor, i.e. your mobile phone, can trigger a signature in your name.

Any electronic signature generated using your digital signature key is generally deemed to be yours if your certificate was valid at the time it was generated and if there are no facts which disprove the presumption that you deliberately generated the electronic signature.

5. Obligations of subscribers

The subscriber and/or subject must abide by the clauses in the CPS and TSP and the Terms and Conditions (AGB) of service, and in particular, must:

- read and understand the terms and conditions (AGB) and any additional informative documentation,
- state true data in applications submitted to a registration authority,
- immediately inform msg mySaveID GmbH about any errors, defects or changes in the certificate,
- protect the credentials necessary for the use of the msg mySaveID GmbH 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,
- take all the measures needed to prevent unauthorized use of msg mySaveID GmbH account.
- treat the loss or revelation of credentials necessary for the use of the msg mySaveID GmbH 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),
- discontinue using the revoked or expired certificate,
- stop using msg mySaveID GmbH services as soon as he/she become aware that the msg mySaveID GmbH system as such has been compromised.
- start a procedure of revocation in the case of security violation (or security violation suspicion) of their private keys,

- 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.

In the event that the subscriber and/or subject violates the above obligations, msg mySaveID GmbH is entitled to have the qualified certificate revoked without replacement.

Responsibility for the procurement and utilization of an internet connection and of all the requisite tools (hardware and software) lies with the applicant.

6. Validity status of certificates

All parties relying on information contained in certificates must check that the certificates are not suspended or revoked. Information on the status of certificates is available by consulting the list of revoked certificates (CRL) published by the CA at the URL indicated on the certificate or through the OCSP service.

7. Important documents

The documents CPS, TSP, Disclosure Statements and General Terms and Conditions (AGB) as well as all published CA certificates are linked in the msg mySaveID GmbH repository: https://www.mySaveID.de/repository

8. General Information

Complaint and arbitration procedure

Should you have any problems or questions which you cannot settle with our support on an amicable basis, you can refer the case to the Federal Network Agency as your contact partner for complaints and arbitration; furthermore, you can also obtain details of such proceedings from the Federal Network Agency.

Applicable law

Any legal relationships arising from this contract shall be subject to the laws of the Federal Republic of Germany. The applicability of the United Nations Convention on Contracts for the International Sale of Goods shall be excluded.

Place of jurisdiction

The legal venue for any legal disputes shall be Frankfurt am Main 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. msg mySaveID GmbH may also assert its rights at the customer's place of general jurisdiction. Any exclusive jurisdiction shall remain unaffected by the present agreement.