

PKI Disclosure Statement der msg mySaveID GmbH Zertifizierungs- und Vertrauensdienste

Dieses Dokument informiert die Nutzer der von der msg mySaveID GmbH, dem Vertrauensdiensteanbieter der msg-Gruppe, angebotenen qualifizierten Vertrauensdienste über die allgemeinen Bedingungen für den erbrachten Vertrauensdienst.

Dokumenteninformationen

Version:	1.0
Datum der Version:	13.06.24
Zustand:	<input type="checkbox"/> in Bearbeitung seit: 02.01.2024 <input type="checkbox"/> vorgelegt am: <input checked="" type="checkbox"/> akzeptiert/abgeschlossen
Vertraulichkeitsstufe/Klassifizierung:	internal use
Sprache:	<Deutsch>
Autor:	Christoph Thiel
Dateiname:	MYSAVEID_PDS
Englischer Titel:	PKI Disclosure Statement of the msg mySaveID GmbH certification and trust services
Übersetzung:	In Vorbereitung
Kategorie (Level):	Richtlinie
Ansprechpartner:	Karsten Treiber
Datum des Inkrafttretens:	13.06.2024
Nächstes Reviewdatum	13.06.2025

Dokumentenhistorie

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

Inhalt

Inhalt.....	II
1. Einführung	3
2. Kontaktangaben	3
3. Revozierung/Widerruf von Zertifikaten	3
4. Qualifizierte Treuhanddienste.....	1
Arten der angebotenen qualifizierten Treuhanddienste	1
Mögliche Einschränkungen bei qualifizierten Zertifikaten und Archivierungszeitraum	2
Informationen über die Rechtswirkung	2
Rechtswirkung der elektronischen Signatur und des elektronischen Siegels	2
371a der deutschen Zivilprozessordnung [§ 371a ZPO] Beweiskraft elektronischer Dokumente..	3
5. Pflichten der Abonnenten	3
6. Gültigkeitsstatus der Zertifikate	4
7. Wichtige Dokumente.....	4
8. Allgemeine Informationen	4
Beschwerde- und Schlichtungsverfahren.....	4
Anwendbares Recht	5
Ort der Gerichtsbarkeit	5

1. Einführung

Dieses PKI-Disclosure-Statement (PDS) erfüllt die Veröffentlichungspflicht nach der europäischen Norm ETSI EN 319 411-1 für den von der Qualified Trust Service Provider msg mySaveID GmbH (im Folgenden "QTSP" oder "CA") angebotenen Zertifizierungsdienst und dient dazu, Antragstellern die für die Nutzung des Dienstes erforderlichen technischen Informationen zur Verfügung zu stellen. Die Verordnung (EU) Nr. 2024/1183 vom 20. Mai 2024 und der (EU) Nr. 910/2014 vom 23. Juli 2014 des Europäischen Parlaments und des Rates über elektronische Identifizierungs- und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, wird im Folgenden als "eIDAS-Verordnung" bezeichnet. Das vorliegende Dokument begleitet die Allgemeinen Geschäftsbedingungen und ist Bestandteil der Vertragsunterlagen der msg mySaveID GmbH. Die Veröffentlichung dieser PDS ersetzt nicht die Veröffentlichung des Certification Practice Statements (CPS) bzw. der Allgemeinen Geschäftsbedingungen (AGB), die detaillierteren Informationen enthalten und auf der Website der msg mySaveID GmbH unter folgendem Link verfügbar sind: <https://www.mySaveID.de/repository/>.

2. Kontaktangaben

Ihr Vertrauensdiensteanbieter (TSP):

msg mySaveID GmbH
Amelia-Mary-Earhart-Straße 14
60549 Frankfurt am Main
E-Mail: info@mysaveid.de

Rufnummer: +49 69 580045-4000

3. Revozierung/Widerruf von Zertifikaten

- Über die Webanwendung der msg mySaveID GmbH können Widerrufsansprüche gestellt werden, wenn sich der Antragsteller mit den vereinbarten Zugangsdaten eindeutig an der Schnittstelle authentifizieren kann. Darüber hinaus kann ein Widerruf auch über die Kontaktmöglichkeiten (schriftlich) angefordert werden.
- Wenn Sie Ihr eigenes Zertifikat widerrufen möchten, melden Sie sich in der mySaveID-Webanwendung (<https://id.mySaveID.de/>) an, gehen Sie zu Ihrem Benutzerprofil und widerrufen Sie Ihr Zertifikat unter dem Menüpunkt "Signatur".
- Enthält Ihr Zertifikat weitere Informationen (z.B. einen Firmennamen), an denen Dritte beteiligt sind, so sind diese ebenfalls berechtigt, Ihr Zertifikat zu sperren. Die Sperrung durch Dritte, die zur Sperrung von Zertifikaten berechtigt sind, erfolgt ebenfalls über die Online-Schnittstelle.

Der über die Online-Schnittstelle übermittelte Widerrufsanspruch wird sofort ausgeführt. Eine rückwirkende Sperrung ist grundsätzlich nicht möglich. Eine vorübergehende Sperrung oder Aussetzung von Zertifikaten wird nicht angeboten. Ein einmal gesperrtes Zertifikat kann nicht wiederhergestellt werden, d.h. der Sperrvorgang ist endgültig und unumkehrbar.

4. Qualifizierte Treuhanddienste

Arten der angebotenen qualifizierten Treuhanddienste

Vertrauensdienst	Anwendbare Politiken
Erstellung von qualifizierten Zertifikaten für natürliche Personen auf einem Hochsicherheitsmodul (HSM) im TSP	<ul style="list-style-type: none"> ▪ ETSI 319 411-2 QCP-n-qscd ▪ Certification Practice Statement und Trusted Service Policy der msg mySaveID GmbH
Erstellung von qualifizierten Zertifikaten für juristische Personen auf einem Hochsicherheitsmodul (HSM) beim TSP	<ul style="list-style-type: none"> ▪ ETSI 319 411-2 QCP-l-qscd ▪ Certification Practice Statement und Trusted Service Policy der msg mySaveID GmbH

Da die Schlüsselgenerierung, die Schlüsselspeicherung und die Zertifikatsverwaltung von mySaveID in den Systemen und sicheren Hardwaremodulen von mySaveID durchgeführt werden und kein sicheres kryptografisches Gerät für den Teilnehmer und/oder das Subjekt erforderlich ist, gelten alle für NCP in ETSI EN 319 411-1 festgelegten Verpflichtungen.

Die msg mySaveID GmbH verfügt als qualifizierter Vertrauensdiensteanbieter über eine Konformitätsbescheinigung zu den oben genannten Richtlinien für die oben genannten Dienste.

Die Zertifikate können für Anwendungen verwendet werden, die mit den im Zertifikat angegebenen Nutzungsarten (Schlüsselverwendung und erweiterte Schlüsselverwendung) vereinbar sind. Die auftraggebenden Parteien sind für ihre Handlungen allein verantwortlich.

Im Übrigen gelten die Regelungen des Certification Practice Statements und der Allgemeinen Geschäftsbedingungen (AGB) der msg mySaveID GmbH.

Die Msg mySaveID GmbH bietet auch Fernsignaturdienste auf qualifizierten Signaturerstellungseinheiten (QSCDs) an, indem sie Schlüssel und Zertifikate für den Unterzeichner erzeugt und verwaltet.

Mögliche Einschränkungen bei qualifizierten Zertifikaten und Archivierungszeitraum

Vertrauensdienst	Mögliche Einschränkungen	Archivierungszeitraum
Erstellung von qualifizierten Zertifikaten für natürliche Personen auf einem Hochsicherheitsmodul (HSM) im TSP	Eventuelle Einschränkungen des Zertifikats sind im Zertifikat selbst angegeben (z. B. Testzertifikate, Geldbetragsgrenze).	Das deutsche Vertrauensdienstegesetz in Verbindung mit der Vertrauensdiensteverordnung schreibt eine dauerhafte Speicherung der Zertifikatsdaten vor.
Erstellung von qualifizierten Zertifikaten für juristische Personen auf einem Hochsicherheitsmodul (HSM) beim TSP		

Die msg mySaveID GmbH bietet auch Fernsignaturdienste auf qualifizierten Signaturerstellungseinheiten (QSCDs) an, indem sie Schlüssel und Zertifikate für den Unterzeichner erzeugt und verwaltet.

Die Gültigkeitsdauer eines jeden Zertifikats ist im Zertifikat selbst angegeben und kann zwischen drei Jahren und drei Monaten variieren. Es ist verboten, das Zertifikat außerhalb der im CPS und in den Verträgen angegebenen Grenzen und Einstellungen und auf jeden Fall unter Verletzung der im Zertifikat angegebenen Nutzungs- und Wertgrenzen (Schlüsselverwendung, erweiterte Schlüsselverwendung, Benutzerhinweis) zu verwenden. Die Ereignisprotokolle im Zusammenhang mit der Ausstellung von Zertifikaten werden im konformen Datenspeichersystem der informatischen Dokumente von mySaveID aufbewahrt, und zwar auf unbegrenzte Zeit ab dem Ablaufdatum des Zertifikats.

Informationen über die Rechtswirkung

Die Rechtswirkung der elektronischen Signatur, des Siegels und des Zeitstempels ist in der Verordnung (EU) Nr. 2024/1183 und der (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates, kurz: eIDAS-Verordnung, festgelegt.

13 Abs. 1 Nr. 3 des Vertrauensdienstegesetzes (VDG), d.h. des Gesetzes zur Umsetzung der eIDAS-Verordnung, sieht vor, dass der Vertrauensdiensteanbieter die Öffentlichkeit gemäß § 13 Abs. 1 VDG über die Rechtswirkung der angebotenen qualifizierten Vertrauensdienste informieren muss. Wir möchten Sie im Folgenden über die Rechtswirkung unserer qualifizierten Vertrauensdienste informieren.

Rechtswirkung der elektronischen Signatur und des elektronischen Siegels

Eine qualifizierte elektronische Signatur hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift (Art. 25 eIDAS-VO). Eine qualifizierte elektronische Signatur, die

auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruht, wird in allen anderen Mitgliedstaaten als qualifizierte elektronische Signatur anerkannt.

Die gesetzliche "qualifizierte elektronische Signatur" hat gemäß §§ 126 ff BGB die gleiche Wirkung wie eine handschriftliche Unterschrift im Zivilrecht, wenn das signierte Dokument zusätzlich den Namen des Unterzeichners trägt ("elektronische Form") und eine solche elektronische Form nicht ausdrücklich gesetzlich ausgeschlossen ist.

Die Rechtswirkung eines qualifizierten Siegelzertifikats ist in der eIDAS-Verordnung wie folgt festgelegt:

Vermutung der Integrität der Daten und der Richtigkeit der angegebenen Quelle der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist (siehe Art. 35 (2) eIDAS-Verordnung).

371a der deutschen Zivilprozessordnung [§ 371a ZPO] Beweiskraft elektronischer Dokumente

Die Bestimmungen über die Beweiskraft privater Urkunden sind auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, analog anwendbar. Der Anscheinsbeweis der Echtheit einer in elektronischer Form vorliegenden Erklärung, der auf der Überprüfung der qualifizierten elektronischen Signatur nach Artikel 32 der eIDAS-Verordnung (EU) Nr. 2024/1183 und die (EU) Nr. 910/2014 beruht, kann nur durch Tatsachen in Frage gestellt werden, die ernsthafte Zweifel daran begründen, dass die Erklärung von der dafür verantwortlichen Person abgegeben wurde.

Das bedeutet, dass jeder, der Ihr sign-me-Konto nutzen kann, d.h. Zugriff auf Ihre Anmeldedaten und den zweiten Authentifizierungsfaktor, d.h. Ihr Mobiltelefon, hat, eine Signatur in Ihrem Namen auslösen kann.

Jede elektronische Signatur, die mit Ihrem Signaturschlüssel erzeugt wurde, gilt in der Regel als Ihre Signatur, wenn Ihr Zertifikat zum Zeitpunkt der Erzeugung gültig war und keine Tatsachen vorliegen, die die Vermutung widerlegen, dass Sie die elektronische Signatur absichtlich erzeugt haben.

5. Pflichten der Abonnenten

Der Abonnent und/oder das Subjekt muss sich an die Klauseln in den CPS und TSP sowie an die Allgemeinen Geschäftsbedingungen (AGB) des Dienstes halten, und zwar insbesondere an:

- die Allgemeinen Geschäftsbedingungen (AGB) und alle zusätzlichen Informationsunterlagen gelesen und verstanden haben,
- die Angabe wahrheitsgemäßer Daten in den bei einer Registrierungsbehörde eingereichten Anträgen,
- die msg mySaveID GmbH unverzüglich über Fehler, Mängel oder Änderungen des Zertifikats zu informieren,
- die für die Nutzung der Dienste der msg mySaveID GmbH und für die Signaturerstellung erforderlichen Zugangsdaten vor Missbrauch, Verlust, Offenlegung, Manipulation oder unberechtigter Nutzung zu schützen, sie Dritten

weder mitzuteilen noch offenzulegen und die alleinige Kontrolle darüber zu behalten,

- alle erforderlichen Maßnahmen zu ergreifen, um eine unbefugte Nutzung des Kontos der msg mySaveID GmbH zu verhindern.
- den Verlust oder die Offenlegung von Zugangsdaten, die für die Nutzung der Dienste der msg mySaveID GmbH und für die Signaturerstellung erforderlich sind, wie den Verlust oder die Offenlegung des privaten Schlüssels zu behandeln (Offenlegung gegenüber einem Unbefugten),
- das widerrufen oder abgelaufene Zertifikat nicht mehr zu verwenden,
- die Nutzung der Dienste der msg mySaveID GmbH einzustellen, sobald er/sie Kenntnis davon erlangt, dass das System der msg mySaveID GmbH als solches kompromittiert wurde.
- im Falle einer Sicherheitsverletzung (oder des Verdachts auf eine Sicherheitsverletzung) ihrer privaten Schlüssel ein Widerrufsverfahren einleiten,
- ein qualifiziertes Zertifikat und die zugehörigen privaten Schlüssel nur für den im Zertifikat angegebenen Zweck und in Übereinstimmung mit den in der Praxiserklärung und der Vertrauensdienstrichtlinie genannten Zielen und Einschränkungen zu verwenden.

Verstößt der Zertifikatnehmer bzw. das Subjekt gegen die vorgenannten Verpflichtungen, ist die msg mySaveID GmbH berechtigt, das qualifizierte Zertifikat ersatzlos zu sperren.

Die Verantwortung für die Beschaffung und Nutzung eines Internetanschlusses und aller erforderlichen Tools (Hard- und Software) liegt beim Antragsteller.

6. Gültigkeitsstatus der Zertifikate

Alle Parteien, die sich auf die in den Zertifikaten enthaltenen Informationen verlassen, müssen überprüfen, ob die Zertifikate nicht ausgesetzt oder widerrufen wurden. Informationen über den Status von Zertifikaten sind in der Liste der gesperrten Zertifikate (CRL) verfügbar, die von der CA unter der auf dem Zertifikat angegebenen URL oder über den OCSP-Dienst veröffentlicht wird.

7. Wichtige Dokumente

Die Dokumente CPS, TSP, Disclosure Statements und Allgemeine Geschäftsbedingungen (AGB) sowie alle veröffentlichten CA-Zertifikate sind im Repository der msg mySaveID GmbH verlinkt: <https://www.mySaveID.de/repository>

8. Allgemeine Informationen

Beschwerde- und Schlichtungsverfahren

Sollten Sie Probleme oder Fragen haben, die Sie mit unserer Unterstützung nicht gütlich regeln können, können Sie sich an die Bundesnetzagentur als Ihren Ansprechpartner für Beschwerden und Schlichtung wenden; außerdem können Sie sich bei der Bundesnetzagentur auch über ein solches Verfahren informieren.

Anwendbares Recht

Für alle Rechtsbeziehungen, die sich aus diesem Vertrag ergeben, gilt das Recht der Bundesrepublik Deutschland. Die Anwendbarkeit des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf ist ausgeschlossen.

Ort der Gerichtsbarkeit

Gerichtsstand für alle Rechtsstreitigkeiten ist Frankfurt am Main, soweit der Kunde Kaufmann, eine juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen ist oder keinen allgemeinen Gerichtsstand in der Bundesrepublik Deutschland hat. msg mySaveID GmbH kann ihre Rechte auch am allgemeinen Gerichtsstand des Kunden geltend machen. Ein etwaiger ausschließlicher Gerichtsstand bleibt von dieser Vereinbarung unberührt.