**Zentrum für sichere Informationstechnologie – Austria**
**Secure Information Technology Center – Austria**

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: +43 1 503 19 63–0
Fax: +43 1 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: +43 316 873-5514
Fax: +43 316 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

# QSEE-BESCHEINIGUNG DER BESTÄTIGUNGSSTELLE GEM. § 7 ABS. 1 SVG[1] IVM ART. 30 ABS. 3 LIT. B EIDAS-VO[2]

## Qualifizierte Signatur- und Siegelerstellungseinheit (QSEE) Trust2Go, Version 1.0

Antragstellerin:
e-commerce monitoring GmbH
Redtenbachergasse 20
1160 Wien

**Referenznummer A-SIT-VIG-20-105**

**QSEE-Bescheinigung gültig ab:**
Siehe Datum der qualifizierten elektronischen Signatur

## 1. Beschreibung der zu bescheinigenden Komponente

Das hiermit bescheinigte Produkt Trust2Go der *e-commerce monitoring GmbH* ist eine qualifizierte elektronische Signatur- und Siegelerstellungseinheit (QSEE). Bei der Verwendung qualifizierter Zertifikate werden qualifizierte elektronische Signaturen und qualifizierte elektronische Siegel gemäß Verordnung (EU) Nr. 910/2014 (eIDAS) erstellt, wodurch die in der Verordnung definierte rechtliche Anerkennung erreicht wird. Die QSEE wird in der geschützten Umgebung in Rechenzentren des qualifizierten Vertrauensdiensteanbieters (VDA) betrieben, worin der physische Zugang zur QSEE restriktiv auf autorisierte, privilegierte Personen eingeschränkt ist. An Benutzerinnen und Benutzer der QSEE erfolgt keine Auslieferung physischer Komponenten, da die QSEE die jeweiligen Signatur- oder Siegelerstellungsdaten verwaltet.

Teilkomponenten:

Der Aufbau der QSEE und ihrer Umgebung folgt dem Konzept eines Trustworthy Systems Supporting Server Signing (TW4S) aus EN 419 241-1. Sie besteht somit aus zwei Teilkomponenten:

[1] Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG, BGBl. I Nr. 50/2016 vom 8. Juli 2016 idF BGBl. I Nr. 27/2019 vom 29. März 2019)

[2] Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

dem Signaturaktivierungsmodul (SAM) und dem Hardware Security Modul (HSM). Das SAM ist eine Softwarekomponente auf dem HSM und steuert als Endpunkt des Signaturaktivierungsprotokolls (SAP) die Aktivierung der Signaturschlüssel (bzw. Siegelschlüssel) sowie die Auslösung der Signatur- oder Siegelerstellungsfunktionen. Das HSM ist für die Ausführung der kryptografischen Operationen und die Schlüsselverwaltung zuständig. Derzeit werden ausschließlich HSM vom Typ „Thales Luna K7 Cryptographic Module“[3] mit der Firmware Version 7.7.0 unterstützt. Das eingesetzte HSM wird gemäß seiner Common Criteria Zertifizierung[4] und den Trust2Go Sicherheitsvorgaben betrieben.

Diese beiden Komponenten (SAM und HSM) bilden den zu bescheinigenden Bereich. Weitere notwendige und optionale Komponenten des Systems, wie zum Beispiel die Serversignatur-anwendung (SSA) oder clientseitige Komponenten, sowie die Prozesse zur Identifikation, Registrierung und Zertifikatsausstellung sind nicht Teil dieser Bescheinigung.

Erzeugung der Signatur- und Siegelerstellungsdaten:

Im Zuge der Registrierung erzeugt die QSEE für die jeweilige Person ein kryptografisch miteinander verknüpftes Schlüsselpaar. Der private Schlüssel dieses asymmetrischen Schlüsselpaares stellt die Signatur- bzw. Siegelerstellungsdaten (SCD[5]) dar, wohingegen der öffentliche Schlüssel die Signatur- bzw. Siegelvalidierungsdaten (SVD[6]) ergibt. Die SCD werden eindeutig und ausschließlich an die jeweilige Benutzerin bzw. den jeweiligen Benutzer sowie die Komponenten des VDA[7] gebunden, sowohl logisch, durch Zuweisung, als auch kryptografisch, durch Verschlüsselung mit einem Wrapping-Key. Die Erzeugung des Schlüsselpaares erfolgt im manipulationsgeschützten und nach Common Criteria EAL4+[8] zertifizierten HSM.

Im Anschluss signiert das HSM eine Zertifikatsanfrage für den öffentlichen Schlüssel (SVD) und leitet sie an die verbundene Certification Authority (CA) zur Zertifikatsausstellung weiter. Die Prozesse und Komponenten der Zertifizierung sind nicht Teil dieser Bescheinigung.

Speicherung der Signatur- und Siegelerstellungsdaten:

Die Speicherung der SCD erfolgt im sogenannten Scalable Key Storage (SKS), einem Mechanismus des HSMs zur Erweiterung des für die Schlüsselspeicherung verfügbaren Speichers. Um dies zu erreichen werden die SCD nicht im HSM intern gespeichert, sondern verschlüsselt mit dem SKS Master Key (SMK) – einem vom HSM generierten, nicht exportierbaren Schlüssel – in einer Datenbank abgelegt, wodurch die SCD zwar außerhalb des HSM gelangen, jedoch durch die Verschlüsselung nicht dessen sichere Umgebung verlassen. Die so gesicherten SCD werden zusätzlich noch mit zwei weiteren Faktoren gesichert, einerseits mit dem Passwort der SSA und andererseits mit dem AktivierungsPIN[9] der Benutzerin bzw. des Benutzers. Das dabei entstandene SIM[10]-Key-Objekt wird in der Datenbank gespeichert.

Die SCD verlassen das HSM somit niemals in unverschlüsselter oder ungeschützter Form. Auf diese Weise können die SCD nur durch die Kombination von SAM und HSM verwendet werden. Alle Operationen zur Erzeugung, Verwendung und Zerstörung der SCD werden mit den zertifizierten Sicherheitsfunktionen des HSM implementiert.

[3] Thales Luna K7 Cryptographic Module, Firmware Version: 7.7.0 mit Boot Loader Versionen 1.1.1, 1.1.2 oder 1.1.4, Hardware Versionen: 808-000048-002, 808-000066-001, 808-000069-001, 808-000070-001 und 808-000073-001, Hersteller: Thales (ehem. Gemalto bzw. SafeNet), 20 Colonnade Road, Suite 200, Ottawa, ON K2E 7M6, Canada

[4] TÜV Rheinland Nederland B.V.: Certificate CC-20-195307, Thales Luna K7 Cryptographic Module Abrufbar: https://www.commoncriteriaportal.org/files/epfiles/CC-20-195307.pdf [Letzter Zugriff: 17.6.2022]

[5] SCD – Signature Creation Data

[6] SVD – Signature Validation Data

[7] Server Signing Application (SSA) und Signature Activation Module (SAM)

[8] EAL – Evaluation Assurance Level

[9] PIN – Persönliche Identifikationsnummer (Personal Identification Number)

[10] SIM – Secure Identity Management (ein Feature der Thales Luna K7 HSMs)

Signatur- und Siegelerstellung:

Für die Signaturerstellung ist zuerst die Auswahl eines gültigen und geeigneten Zertifikates, das der Benutzerin bzw. dem Benutzer zugewiesen wurde, notwendig. Für die Identifizierung als die dem Zertifikat zugewiesene Person ist die Kenntnis des ersten Authentifizierungsfaktors, einem Passwort („AktivierungsPIN“), erforderlich. Dieser Faktor wird von der SSA überprüft und im Positivfall die Abfrage des zweiten Faktors gestartet. Hierzu stehen zwei Verfahren zur Auswahl:

- SMS[11]-TAN[12]: Die SSA generiert eine transaktionsspezifische TAN und sendet sie per SMS an die bei der Registrierung gespeicherte Mobilfunknummer. Der Authentifizierungsvorgang gilt als positiv abgeschlossen, wenn die idente TAN wieder an die SSA retourniert wird.
- AuthenticationApp: In der verknüpften mobilen Applikation erscheint eine Aufforderung zur Bestätigung der Transaktion. Diese kann durch die im mobilen Betriebssystem eingestellte Authentifizierungsart (PIN, Gesichtserkennung oder Fingerabdruck) erteilt werden.

Bei positiver Rückbestätigung des zweiten Faktors sendet die SSA die SAD[13] mit einer Signaturanfrage zum SAM. Das SAM prüft die SAD und aktiviert nach erfolgreicher Prüfung den entsprechenden Signaturschlüssel im HSM. Hierzu wird das SIM-Key-Objekt aus der Datenbank in das HSM geladen und mit den durch die SAD erhaltenen Schlüssel entschlüsselt. Der übergebene Hashwert wird vom HSM signiert und die dazu verwendeten SCD anschließend wieder aus dem HSM gelöscht. Die erstellte Signatur wird zurück an die SSA und weiter an den Client zur weiteren Verarbeitung gesendet. Zusätzlich wird sie auch in der Datenbank samt Protokolleinträgen gespeichert.

Die Siegelerstellung erfolgt analog zur Signaturerstellung, nur dass diese keinen zweiten Faktor zur Aktivierung der Siegelerstellungsdaten erfordert.

[11] SMS – Short Message Service
[12] TAN – Transaction Authentication Number
[13] SAD – Signature Activation Data

## 2. Erfüllung der Anforderungen der eIDAS-VO

Die QSEE erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach Artikel 29 Abs. 1[14] eIDAS-VO,
- Anforderungen nach Artikel 39 Abs. 1[15] eIDAS-VO,
- Anforderungen nach Anhang II eIDAS-VO (Abs. 1 lit. a[16],b[17],c[18],d[19], Abs. 2[20], Abs. 3[21], Abs. 4 lit a[22], b[23])

Die QSEE ist daher in folgenden Kategorien bescheinigt:

- Komponenten und Verfahren zur Erzeugung von Signatur- und Siegelerstellungsdaten,
- Komponenten und Verfahren zum Speichern von Signatur- und Siegelerstellungsdaten,
- Komponenten und Verfahren zur Verarbeitung der Signatur- und Siegelerstellungsdaten

## 3. Gültigkeitsdauer der QSEE-Bescheinigung

Die Gültigkeit dieser QSEE-Bescheinigung ist bis auf Widerruf durch A-SIT aufrecht. A-SIT führt bei Beauftragung eine kontinuierliche Evidenthaltung und ein Monitoring hinsichtlich der Sicherheit der eingesetzten Produkte und Verfahren sowie der kryptografischen Algorithmen und Parameter durch. Mit der Ausstellung dieser QSEE-Bescheinigung ist ein Monitoring für zwei Jahre verbunden. Der Widerruf erfolgt sofern die Sicherheit der eingesetzten Produkte und Verfahren sowie der

---

[14] *Qualifizierte elektronische Signaturerstellungseinheiten müssen die Anforderungen des Anhangs II erfüllen.*

[15] *Artikel 29 gilt sinngemäß für die Anforderungen an qualifizierte elektronische Siegelerstellungseinheiten.*

[16] *Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass die Vertraulichkeit der zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten angemessen sichergestellt ist.*

[17] *Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten praktisch nur einmal vorkommen können.*

[18] *Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten mit hinreichender Sicherheit nicht abgeleitet werden können und die elektronische Signatur bei Verwendung der jeweils verfügbaren Technik verlässlich gegen Fälschung geschützt ist.*

[19] *Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten vom rechtmäßigen Unterzeichner gegen eine Verwendung durch andere verlässlich geschützt werden können.*

[20] *Qualifizierte elektronische Signaturerstellungseinheiten dürfen die zu unterzeichnenden Daten nicht verändern und nicht verhindern, dass dem Unterzeichner diese Daten vor dem Unterzeichnen angezeigt werden.*

[21] *Das Erzeugen oder Verwalten von elektronischen Signaturerstellungsdaten im Namen eines Unterzeichners darf nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt werden.*

[22] *Unbeschadet des Absatzes 1 Buchstabe d dürfen qualifizierte Vertrauensdiensteanbieter, die elektronische Signaturerstellungsdaten im Namen des Unterzeichners verwalten, die elektronischen Signaturerstellungsdaten ausschließlich zu Sicherungszwecken kopieren, sofern folgende Anforderungen erfüllt sind: a) Die kopierten Datensätze müssen das gleiche Sicherheitsniveau wie die Original-Datensätze aufweisen.*

[23] *Unbeschadet des Absatzes 1 Buchstabe d dürfen qualifizierte Vertrauensdiensteanbieter, die elektronische Signaturerstellungsdaten im Namen des Unterzeichners verwalten, die elektronischen Signaturerstellungsdaten ausschließlich zu Sicherungszwecken kopieren, sofern folgende Anforderungen erfüllt sind: Es dürfen nicht mehr kopierte Datensätze vorhanden sein als zur Gewährleistung der Dienstleistungskontinuität unbedingt nötig.*

kryptografischen Algorithmen und Parameter nicht mehr dem Stand der Technik entsprechen bzw. kein weiteres Monitoring beauftragt wird.

# 4. Einsatzbedingungen

Die Gültigkeit dieser QSEE-Bescheinigung ist an die im Folgenden angeführten Einsatzbedingungen gebunden. Diesen ist in geeigneter Weise der Wirkung nach zu entsprechen und es sind die getroffenen Maßnahmen

- durch das Sicherheits- und Zertifizierungskonzept des Vertrauensdiensteanbieters sicherzustellen,
- in der Belehrung der Benutzerin bzw. des Benutzers entsprechend zu übernehmen
- und deren Wirkung im Wege der Beaufsichtigung (iSv Artikel 20 eIDAS-VO) sicherzustellen.

(1) Die eindeutige Zuordnung und die sichere Beendigung der Benutzersession sowie die Vertraulichkeit und Integrität der Autorisierungscodes und die Integrität der zu signierenden bzw. zu besiegelnden Daten bei der Übertragung von der Benutzerin bzw. vom Benutzer zur QSEE im Zuge des Auslösevorgangs sind in der Systemumgebung der QSEE sicherzustellen und daher nicht Teil der QSEE-Bescheinigung[24]. Es ist sicherzustellen, dass die Benutzerin bzw. der Benutzer darüber informiert sind, dass ihre im Zuge der Auslösung der Signatur bzw. des Siegels verwendeten Komponenten (Mobiltelefon, Webbrowser etc.) geeignet abgesichert sein müssen.

(2) Die QSEE darf nur von einem qualifizierten Vertrauensdiensteanbieter betrieben werden.

(3) Der qualifizierte Vertrauensdiensteanbieter muss die QSEE in einer geschützten Umgebung betreiben, dabei ist insbesondere zu gewährleisten:

- Beschränkung des physischen Zugangs zur QSEE auf autorisiertes, vertrauenswürdiges und geprüftes Personal
- Schutz vor Verlust und Diebstahl der QSEE und der außerhalb dieser gespeicherten Assets
- Maßnahmen zur Erkennung und zur Verhinderung von Manipulationsversuchen (einschließlich Zugriffe auf Seitenkanäle, Zugriffe auf Verbindungen zwischen physisch separierten Komponenten der QSEE oder Teile der Hardware-Appliance)
- Schutz gegen die Möglichkeit von Attacken beruhend auf kompromittierender Abstrahlung (z.B. elektromagnetischer Abstrahlung) gemäß dem für die Betriebsumgebung ermittelten Risiko
- Schutz vor unautorisierten Änderungen an der Software und Konfiguration der QSEE sowie der Hardware-Appliance
- Äquivalentes hohes Schutzniveau für alle Teilkomponenten (einschließlich für zu Sicherungszwecken verwendete Komponenten)

(4) Komponenten der Signatorin bzw. des Signators, die Schwachstellen oder ungeeignete Methoden zur Benutzer/innen-Authentifizierung aufweisen, dürfen bei der Signaturauslösung nicht verwendet werden können.

(5) Das HSM muss unter Einhaltung des 4-Augen-Prinzips (dabei muss mindestens eine Person die Rolle „HSM Security Officer“ innehaben) initialisiert und dabei in den „FIPS 140-2 approved mode“ geschalten werden.

(6) Das HSM muss gemäß seiner Common Criteria EAL4+ Zertifizierung initialisiert und betrieben werden.

(7) Elektronische Signatur- bzw. Siegelerstellungsdaten dürfen zu Sicherungszwecken nur soweit kopiert werden als zur Gewährleistung der Dienstleistungskontinuität unbedingt nötig.

[24] Entsprechend Erwägungsgrund 56 der eIDAS-VO.

(8) Nur die in Kapitel 5 gelisteten kryptografischen Algorithmen und Parameter dürfen für die Erstellung von qualifizierten elektronischen Signaturen oder qualifizierten elektronischen Siegeln verwendet werden.

## 5. Algorithmen und zugehörige Parameter

Zur Erstellung von qualifizierten elektronischen Signaturen bzw. qualifizierten elektronischen Siegeln werden von der QSEE die kryptografischen Algorithmen

- RSA[25]SSA-PKCS1-v1_5 nach PKCS#1 v2.2 (RFC 8017)
  mit Schlüssellängen von 2048, 3072 oder 4096 Bit,
- RSASSA-PSS[26] nach PKCS#1 v2.2 (RFC 8017)
  mit Schlüssellängen von 2048, 3072 oder 4096 Bit und
- ECDSA[27] nach FIPS[28] PUB 186-4 und den NIST[29]-Kurven P-256, P-384 oder P-521
  mit Länge der Parameter p, q von 256, 384 oder 512 Bit,

verwendet.

Für die Berechnung der Hashwerte werden folgende Hashfunktionen unterstützt[30]:

- SHA[31]-256, SHA-384 und SHA-512 nach ISO[32]/IEC[33] 10118-3 bzw. FIPS 180-4

## 6. Prüfstufe und Mechanismenstärke

Die QSEE verwendet ausschließlich Hardware Security Module (HSM) des folgenden Typs:

- Thales Luna K7 Cryptographic Module, Firmware Version 7.7.0

Für diesen HSM-Typ mit der Firmware-Version 7.7.0 liegt das Common Criteria Zertifikat von TÜV Rheinland Nederland B.V. mit der Zertifikatsnummer CC-20-195307 vor. Das Zertifikat wurde am 06.10.2020 ausgestellt und ist für fünf Jahre bis zum 06.10.2025 gültig. Es bescheinigt dem HSM eine erfolgreiche Evaluierung nach Common Criteria Version 3.1, Revision 5, Evaluation Assurance Level EAL4, erweitert um ALC_FLR.2[34] und AVA_VAN.5[35] und konform zum Schutzprofil EN 419 221-5:2018: *Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services*.

Da keine Normen für die Sicherheitsbewertung vorliegen, die durch die Kommission im Wege von Durchführungsrechtsakten festgelegt wurden, wurde das QSEE-Bescheinigungsverfahren gemäß Art. 30 Abs. 3 lit. b eIDAS-VO durchgeführt und die Gleichwertigkeit des Sicherheitsniveaus wurde von der Bestätigungsstelle nach dem Stand der Technik beurteilt.

Die QSEE widersteht in ihrer vorgesehenen Einsatzumgebung Angreifern mit hohem Angriffspotenzial.

[25] RSA – Rivest Shamir Adleman
[26] PSS – Probabilistic Signature Scheme
[27] ECDSA – Elliptic Curve Digital Signature Algorithm
[28] FIPS – Federal Information Processing Standards
[29] NIST – National Institute of Standards and Technology
[30] Die Berechnung des Hashwertes erfolgt in der Systemumgebung der QSEE.
[31] SHA – Secure Hash Algorithm
[32] ISO – International Organization for Standardization
[33] IEC – International Electrotechnical Commission
[34] ALC_FLR.2 – Flaw reporting procedures
[35] AVA_VAN.5 – Advanced methodical vulnerability assessment

Die dieser QSEE-Bescheinigung zu Grunde liegenden Prüfungsergebnisse sind im Prüfbericht unter der Referenznummer A-SIT-VIG-20-105 dokumentiert.

**Unterschrift:**

A-SIT Zentrum für sichere Informationstechnologie – Austria

Wien, (Datum siehe el. Signatur)

| | |
|---|---|
| **Unterzeichner** | DI Herbert Leitold |
| **Datum/Zeit-UTC** | 2022-07-12T18:19:34+02:00 |
| **Prüfinformation** | Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at |

DI Herbert Leitold, Gesamtleiter