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. ART. 30 ABS. 3 LIT. B EIDAS-VO[1]

Qualifizierte Signatur- und Siegelerstellungseinheit (QSEE) der D-Trust sign-me, Version 7.4

Antragsteller:
D-Trust GmbH
Kommandantenstraße 15
10969 Berlin

QSEE-Bescheinigung ausgestellt am: 12.04.2021
Referenznummer A-SIT-VIG-20-081

1. Beschreibung der zu bescheinigenden Komponente

Das Produkt „D-Trust sign-me“ von der D-Trust GmbH[2] ist eine qualifizierte elektronische Signatur- bzw. Siegelerstellungseinheit (QSEE). Die QSEE bietet die Funktionalität zur Erstellung von Fernsignaturen bzw. Fernsiegeln.

Teilkomponenten:

Die qualifizierte Signatur- und Siegelerstellungseinheit (QSEE) *D-Trust sign-me* (Version 7.4) besteht aus einer Hardware-Appliance mit dem Software-Modul *sign-me SAM* (SAM – Signature Activation Module) und einem Hardware-Security-Modul (HSM) vom Typ Utimaco CryptoServer CP5 Se1500 LAN v5. Das SAM-Modul implementiert das Signature-Activation-Protocol (SAP) zur Auslösung der Signatur- oder Siegeloperation. Das HSM dient zur Durchführung der kryptografischen Operationen. Das eingesetzte HSM wird gemäß der Common Criteria Zertifizierung in Verbindung mit dem Security Target beim Vertrauensdiensteanbieter (VDA) D-Trust betrieben.

Beide Komponenten der QSEE werden im geschützten Bereich des qualifizierten Vertrauensdiensteanbieters (VDA) D-Trust – dem sogenannten *Trust Center* – betrieben. Der physische Zugang zum Trust Center ist restriktiv auf autorisierte und privilegierte Personen gemäß einem Rollenkonzept beschränkt.

[1] 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

[2] Anmerkung: Die D-Trust GmbH ist ein Tochterunternehmen der Bundesdruckerei GmbH

Erzeugung der Signatur- und Siegelerstellungsdaten:

Die QSEE unterstützt sowohl Signaturen bzw. Siegel mit „Kurzzeitzertifikaten“[3] als auch mit „Langzeitzertifikaten“[4].

Die Anmeldung für eine erstmalige Registrierung zum Signatur- bzw. Siegelerstellungsdienst erfolgt bei einer Registrierungsstelle. Die Registrierung erfolgt entweder direkt über den VDA oder mittels delegierter Authentifizierung bei vertrauenswürdigen Dritten – z.B.: Identity-Providern, Registration-Authorities. Im Rahmen dieser erstmaligen Registrierung eines Benutzers oder einer Benutzerin durch eine Registrierungsstelle, kann eine vertrauenswürdige Applikation (über die sign-me API[5]) beim SAM die Erzeugung des entsprechenden kryptografisch miteinander verknüpften SCD[6]/SVD[7]-Schlüsselpaars innerhalb des geschützten HSMs anfordern. Ausgeliefert wird der Evaluierungsgegenstand (EVG) (i.e., SAM und HSM) zum VDA in einer geschützten Form. Anschließend fordert die vertrauenswürdige Applikation die Bindung des SCD/SVD-Schlüsselpaars an den Benutzer bzw. die Benutzerin an. Der Zugriff für die Erstellung und die Zuordnung der SCD wird vom SAM gesteuert. Danach generiert das HSM die Signatur- bzw. Siegelerstellungsdaten und verbindet diese mit einer im EVG erzeugten key-ID.

Speicherung der Signatur- und Siegelerstellungsdaten:

Nachdem innerhalb des HSM das SCD/SVD-Schlüsselpaar generiert wurde, werden diese gemeinsam mit einer key-ID in einer verschlüsselten Datenstruktur (keyblob) durch einen nur im HSM verfügbaren Schlüssel verschlüsselt abgespeichert. Dadurch ist die Anwendung der Signatur- bzw. Siegelerstellungsdaten nur innerhalb des HSM bzw. der jeweiligen Backup-Instanz des HSM, welche ein äquivalentes Sicherheitsniveau aufweist, möglich. Wenn das HSM die Erzeugung spezifischer Autorisierungsdaten für ein SCD/SVD-Schlüsselpaar anfordert, werden diese Autorisierungsdaten erzeugt und mit dem SCD/SVD-Schlüsselpaar verbunden. Anschließend wird ein Zertifikatsrequest erzeugt und das qualifizierte Zertifikat wird durch die Certification Authority (CA) eines qualifizierten VDA ausgestellt[8]. Die SCD verlassen das HSM 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.

Signatur- bzw. Siegelerstellung:

Die Prozesse für die Signatur- und für die Siegelerstellung sind äquivalent. Ein Benutzer bzw. eine Benutzerin kann eine Signatur- bzw. eine Siegelerstellung nur über vertrauenswürdige Applikationen (sign-me SSA) und nicht über einen direkten Zugriff auf die QSEE anfordern. Die Kommunikation zwischen diesen externen Komponenten und der Remote-QSEE verwendet das Signature Activation Protocol (SAP) und setzt eine Authentifizierung voraus.

Die Authentifizierung nach SCAL2[9] gemäß EN 419 241-1 wird auf eine von drei verschiedenen Arten durchgeführt. Entweder erfolgt die Authentifizierung ausschließlich direkt durch das SAM, oder indirekt durch das SAM in Verbindung mit einem externen Service zur Authentifizierung. Dieses externe Service stellt eine Assertion aus, die vom SAM geprüft wird. Die dritte Möglichkeit umfasst eine Kombination des direkten Authentifizierungsschemas mit dem indirekten Authentifizierungsschema. In jedem Fall wird die Authentifizierung für eine Signatur- bzw. Siegelerstellung als 2-Faktor-Authentifizierung gemäß SCAL2 durchgeführt.

[3] Kurzzeitzertifikate werden in der Regel nur für eine oder kurzzeitig für mehrere Signatur(Siegel)-Aufträge verwendet und die Signatur- bzw. Siegelerstellungsdaten werden anschließend gleich wieder zerstört.
[4] D.h. mit persistenten Signatur- bzw. Siegelerstellungsdaten.
[5] API – Application Programming Interface
[6] SCD – Signature Creation Data
[7] SVD – Signature Verification Data
[8] Anmerkung: Die Prozesse zur Identifikation, Registrierung und Zertifikatsausstellung sind nicht Gegenstand dieser QSEE-Bescheinigung
[9] SCAL2 – Sole Control Assurance Level 2

Ein Benutzer bzw. eine Benutzerin, welche die Signatur bzw. die Erstellung eines Siegels für ein oder mehrere Dokumente (d.h.: mehrere DTBS[10]) anfordert, interagiert mit der Signer Interaction Component (SIC). Bei der SIC handelt es sich um eine Applikation oder um ein Partnersystem das sowohl eine gesicherte TLS[11]-Verbindung als auch den Empfang der Authentifizierungsfaktoren unterstützt und für welches der Schutz gegen Schadsoftware gefordert wird. Wenn der Benutzer bzw. die Benutzerin eine Signatur- bzw. Siegelerstellung initiiert, werden die DTBS oder mehrere DTBS über die „sign-me API" an die SSA übertragen. Danach initiiert die SSA gemeinsam mit dem SAM den Signaturprozess im Auftrag des authentifizierten Benutzers bzw. der authentifizierten Benutzerin. Zu diesem Zweck wird ein Uniform Resource Locator (URL) für den Signatur- bzw. Siegelerstellungsprozess erstellt.

Ein – beispielsweise durch Benutzername und Passwort-Kombination – authentifizierter Benutzer bzw. eine authentifizierte Benutzerin ruft den URL auf und kann anschließend die zu signierenden Daten über die SSA darstellen und prüfen. Die SSA berechnet die Hash-Darstellung (DTBS/R) der zu signierenden Daten. Als zweiter Authentifizierungsfaktor können ein SMS-TAN-Verfahren oder eine App gewählt werden:

- Eine SMS-TAN besteht aus einem 6-stelligen Zufallswert und ist höchstens 5 Minuten gültig. Die TAN wird vom SAM über einen eigenen Kanal übertragen.
- Wird als zweiter Authentifizierungsfaktor die sign-me App ausgewählt, dann erhält der Benutzer bzw. die Benutzerin eine Benachrichtigung per Push-Notification mit der Aufforderung die jeweilige Operation zu bestätigen. Dazu ist die Eingabe einer App-PIN erforderlich, die im Zuge der App-Registrierung festgelegt wurde.

Die SSA überprüft für die Erstellung einer Signatur bzw. eines Siegels die Authentifizierungsfaktoren und ruft das SAM der QSEE auf. Das SAM überprüft die SAD und die DTBS/R. Wenn die Überprüfung erfolgreich ist, autorisiert das SAM die Verwendung der Signatur- bzw. Siegelschlüssel im HSM zum Signieren des DTBS/R durch den Benutzer bzw. die Benutzerin. Der Signatur- bzw. Siegelschlüssel wird anschließend geladen und aktiviert[12]. Mit dem Signatur- bzw. Siegelschlüssel werden die DTBS/R verschlüsselt und dadurch die Signatur bzw. das Siegel erzeugt. Danach wird die Signatur bzw. das Siegel an die SCA zurückübermittelt und an die DTBS angehängt.

2. Erfüllung der Anforderungen der eIDAS-VO

Die QSEE erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach Artikel 29 Abs. 1[13] eIDAS-VO,
- Anforderungen nach Artikel 39 Abs. 1[14] eIDAS-VO,

[10] DTBS – Data to be Signed
[11] TLS Transport Layer Security
[12] Die Generierung der Signatur- bzw. Siegelschlüssel erfolgt (wenn diese nicht schon bereits vorhanden sind) nach Erteilung eines Signaturauftrages bereits vor Erstellung der Signaturaktivierungsdaten, sofern der Identifizierungszustand des Signators / der Signatorin im System dies zulässt.
[13] *Qualifizierte elektronische Signaturerstellungseinheiten müssen die Anforderungen des Anhangs II erfüllen.*
[14] *Artikel 29 gilt sinngemäß für die Anforderungen an qualifizierte elektronische Siegelerstellungseinheiten.*

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

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 laufende 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 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,

---

[15] *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.*

[16] *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.*

[17] *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.*

[18] *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.*

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

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

[21] *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.*

[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: Es dürfen nicht mehr kopierte Datensätze vorhanden sein als zur Gewährleistung der Dienstleistungskontinuität unbedingt nötig.*

- in der Belehrung der Benutzerin bzw. des Benutzers entsprechend zu übernehmen
- und deren Wirkung im Wege der Aufsicht sicherzustellen.

(1) Die eindeutige Zuordnung und die sichere Beendigung der Benutzer/innen-Session 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[23]. 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 (Mobilfunkgerät, 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 privilegiertes und autorisiertes 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 elektromagnetischer Abstrahlung
- 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) Elektronische Signatur- bzw. Siegelerstellungsdaten dürfen zu Sicherungszwecken nur soweit kopiert werden, als zur Gewährleistung der Dienstleistungskontinuität unbedingt nötig.

(5) Die HSMs müssen gemäß ihrer Common Criteria EAL4+ -Zertifizierung unter Einhaltung des 4-Augen-Prinzips initialisiert und betrieben werden.

(6) Externe Authentifizierungsmechanismen, die zur Authentifizierung eines Benutzers verwendet werden, um eine qualifizierte elektronische Signatur oder ein qualifiziertes elektronisches Siegel zu erstellen, müssen einem Authentifizierungsmittel entsprechen, das der EG-Durchführungsverordnung 2015/1502 für ein substanzielles oder höheres Sicherheitsniveau entspricht[24].

5. Algorithmen und zugehörige Parameter

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

- RSASSA-PKCS1-v1_5 oder RSASSA-PSS nach FIPS PUB 186-4 und RFC 8017 mit Schlüssellängen von 2048, 3072 und 4096 Bit oder
- ECDSA mit den Kurven P-256 und P-521 nach FIPS PUB 186-4

verwendet.

[23] Entsprechend Erwägungsgrund 56 der eIDAS-VO.

[24] DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

Zur Berechnung des Hashwertes wird der Algorithmus SHA[25]-256, SHA-384 bzw. SHA-512 nach NIST[26] FIPS 180-4 sowie SHA3-256/384/512 nach NIST FIPS 202 verwendet.

6. Prüfstufe und Mechanismenstärke

Zum verwendeten Hardware Security Modul Utimaco CryptoServer CP5 Se1500 LAN v5 (Version: Se1500 5.1.0.0) liegt das Common Criteria Zertifikat von TÜV Rheinland Nederland B.V mit der Nr. CC-19-222073 vor. Das Common Criteria Zertifikat wurde erstmalig ausgestellt am 19.12.2018 bzw. erneuert am 14.3.2019 und ist bis 19.12.2023 gültig. Das Zertifikat weist dem Hardware Security Modul eine erfolgreiche Evaluierung nach Common Criteria Version 3.1, Evaluation Assurance Level EAL4+, erweitert um AVA_VAN.5[27], nach.

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.

Die dieser QSEE-Bescheinigung zu Grunde liegenden Prüfungsergebnisse sind im Prüfbericht unter der Referenznummer A-SIT-VIG-20-081 dokumentiert.

Unterschrift

A-SIT Zentrum für sichere Informationstechnologie – Austria

Wien, (Datum siehe el. Signatur)

SIGNATURINFORMATIONEN	**Unterzeichner**	Reinhard Posch
	Datum/Zeit-UTC	2021-04-12T15:55:39+02:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.	

Prof. DI Dr. Reinhard Posch, Gesamtleiter

[25] SHA – Secure Hash Algorithm
[26] NIST – National Institute of Standards and Technology
[27] AVA_VAN.5 – Advanced methodical vulnerability assessment