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

A-SIT

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

A-8010 Graz, Inffeldgasse 16a
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

KONFORMITÄTSBEWERTUNGSBERICHT I.S.D. ARTIKELS 20 DER VERORDNUNG (EU) NR. 910/2014 (EIDAS)

Vertrauensdiensteanbieter

e-commerce monitoring GmbH

Qualifizierter Vertrauensdienst

GLOBALTRUST QUALIFIED

Nr.: A-SIT-CONF-REP-VIG-17059

Version 1.0, 30.06.2017

Dieser Konformitätsbewertungsbericht dient i.S.d. Artikels 20 der Verordnung (EU) Nr. 910/2014 (eIDAS) zur Vorlage an eine Aufsichtsstelle. Nur das vollständige und unveränderte Dokument gilt als Konformitätsbewertungsbericht. Dieser darf nur unter Berücksichtigung der Vertraulichkeitsbestimmungen und nur in vollständiger Form (außer bei diesbezüglicher Zustimmung durch die Konformitätsbewertungsstelle A-SIT) weitergegeben oder vervielfacht werden.

Akkreditierte Konformitätsbewertungsstelle

Inhalt

A. Konformitätsbewertungsaussage

Die Konformitätsbewertungsstelle Zentrum für sichere Informationstechnologie – Austria (A-SIT) bescheinigt hiermit dem Vertrauensdiensteanbieter

e-commerce monitoring GmbH, Redtenbachergasse 20, 1160 Wien

für den qualifizierten Vertrauensdienst

- GLOBALTRUST QUALIFIED

alle erforderlichen Anforderungen der Verordnung (EU) Nr. 910/2014 (eIDAS) zu erfüllen.

Wien, (Datum siehe el. Signatur)

SIGNATURINFORMATIONEN	**Unterzeichner**	Reinhard Posch
	Datum/Zeit-UTC	2017-06-30T09:33:39+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, technischer Leiter der Konformitätsbewertungsstelle

B. Grundlagen der Konformitätsbewertung

Rechtliche Grundlage

Das „Zentrum für sichere Informationstechnologie – Austria“ (A-SIT) ist eine durch das BMWFW gem. ÖVE/ÖNORM EN ISO/IEC 17065 akkreditierte Konformitätsbewertungsstelle i.S.d. Artikel 3 Z 18 der Verordnung (EU) Nr. 910/2014 (eIDAS).

Konformitätsbewertungsanforderungen

Die Konformitätsbewertungsanforderungen sind in der *„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“* definiert. Es wurden die für Aussteller elektronischer Identifizierungsmittel laut eIDAS maßgeblichen Anforderungen sowie europäischen Normen herangezogen:

- Artikel 15 (Zugänglichkeit für Personen mit Behinderungen)
- Artikel 19 (Sicherheitsanforderungen an Vertrauensdiensteanbieter)
- Artikel 24 (Anforderungen an qualifizierte Vertrauensdiensteanbieter)
- Artikel 28 (Qualifizierte Zertifikate für elektronische Signaturen)
- Anhang I (Anforderungen an qualifizierte Zertifikate für elektronische Signaturen)
- ETSI EN 319 401 V2.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 V1.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 V2.1.1 (2016-02), 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

Konformitätsbewertungsgegenstand

Der Konformitätsbewertungsgegenstand ist definiert durch folgende Informationen des Vertrauensdiensteanbieters und der angebotenen Vertrauensdienste:

Vertrauensdiensteanbieter	
Name	e-commerce monitoring GmbH
Adresse	Redtenbachergasse 20, 1160 Wien
VAT	AT-U54992708

Vertrauensdienst GLOBALTRUST QUALIFIED		
Certificate Policy	GLOBALTRUST® Certificate Policy, Version 2.0	
Certificate Policy OID	1.2.40.0.36.1.1.8.1	
Zertifikate[1]		
Root-CA „GLOBALTRUST”	CN: GLOBALTRUST QUALIFIED 1	Seriennummer: 1a29229c888b31ba479f67a55

[1] Nur Zertifikate, die zum Zeitpunkt der Ausfertigung dieses Berichts gültig waren, sind angeführt

Root-CA „GLOBALTRUST 2015”	CN: GLOBALTRUST 2015 QUALIFIED 1	Seriennummer: 166578fb0eb1e07ead2fc7a55

Ablauf der Konformitätsbewertung

e-commerce monitoring GmbH hat am 22.05.2017 einen Antrag auf Durchführung einer Konformitätsbewertung nach Artikel 20 der Verordnung (EU) Nr. 910/2014 (eIDAS) gestellt.

Die Konformitätsbewertung wurde vom 23.05.2017 bis 29.06.2017 durch Daniel Konrad durchgeführt. Vor-Ort-Audits wurden am 07.06.2017 und 21.06.2017 in den Büroräumlichkeiten der e-commerce monitoring GmbH und in einem vom VDA genutzten Rechenzentrum durchgeführt.

Die Konformitätsbewertungsentscheidung erfolgte am 30.06.2017 durch Prof. DI Dr. Reinhard Posch.

C. Detailbericht

Beschreibung des qualifizierten Vertrauensdienstes

Diese Konformitätsbewertung behandelt den folgenden vom VDA angebotenen qualifizierten Vertrauensdienst:

- ***GLOBALTRUST QUALIFIED:***

  Im Dienst GLOBALTRUST QUALIFIED werden an natürliche Personen qualifizierte Zertifikate für elektronische Signaturen ausgestellt. Die Signaturerstellungsdaten der Signatoren müssen sich in einer qualifizierten elektronischen Signaturerstellungseinheit (QSCD) befinden. Als QSCDs werden ausschließlich Signaturkarten genutzt.

Ergebnisse der Konformitätsbewertung

Im Folgenden werden die für diese Konformitätsbewertung relevanten eIDAS-Artikel aufgelistet und bewertet. Dafür wurden die Bestimmungen der ETSI-Standards ETSI EN 319 401 [VIG-17-059_03], ETSI EN 319 411-1 [VIG-17-059_04] und ETSI EN 319 411-2 [VIG-17-059_05] geprüft und auf Basis der Tabelle A.1 im Anhang A des ETSI EN 319 411-2 [VIG-17-059_05] den eIDAS-Artikeln zugeteilt.

Artikel 15 - Zugänglichkeit für Personen mit Behinderungen

Soweit möglich werden Vertrauensdienste und zur Erbringung solcher Dienste verwendete Endnutzerprodukte Personen mit Behinderungen zugänglich und nutzbar gemacht.

Betrifft: ETSI EN 319 401 [VIG-17-059_03] clause 7.13 b)

Anforderungen erfüllt.

Sowohl eine Registrierung für die angebotenen Vertrauensdienste, deren Benutzung als auch das Sperren oder Widerrufen der Zertifikate ist barrierefrei bzw. barrierearm möglich. Die Registrierung ist persönlich im barrierefrei erreichbaren Büro möglich oder auf elektronischem Wege.

Die Verwendung der Zertifikate zum Signieren kann mit diversen – auch barrierefreien – Programmen durchgeführt werden. Eine Sperre oder das Widerrufen eines Zertifikates kann telefonisch, online, per Fax, E-Mail, oder schriftlich beantragt werden. Somit ist die Zugänglichkeit und Nutzbarkeit für Personen mit Behinderungen grundsätzlich gegeben.

Artikel 19 - Sicherheitsanforderungen an Vertrauensdiensteanbieter

(1) Qualifizierte und nichtqualifizierte Vertrauensdiensteanbieter ergreifen geeignete technische und organisatorische Maßnahmen zur Beherrschung der Sicherheitsrisiken im Zusammenhang mit den von ihnen erbrachten Vertrauensdiensten. Diese Maßnahmen müssen unter Berücksichtigung des jeweils neuesten Standes der Technik gewährleisten, dass das Sicherheitsniveau der Höhe des Risikos angemessen ist. Insbesondere sind Maßnahmen zu ergreifen, um Auswirkungen von Sicherheitsverletzungen zu vermeiden bzw. so gering wie möglich zu halten und die Beteiligten über die nachteiligen Folgen solcher Vorfälle zu informieren.

Betrifft: ETSI EN 319 401 [VIG-17-059_03], clauses 5, 6.3, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10, 7.11, 7.12, ETSI EN 319 411-1 [VIG-17-059_04], clauses 6.4, 6.5, ETSI EN 319 411-2 [VIG-17-059_05] clauses 6.4, 6.5

Anforderungen erfüllt.

Um Risiken erkennen und abschätzen zu können hat e-commerce monitoring eine Risikoanalyse durchgeführt. Der VDA orientiert sich dabei am BSI Standard „Risikoanalyse auf der Basis von IT Grundschutz“ (BSI 100-3). Die Risikoanalyse und die auf Basis dieser Analyse getroffenen Sicherheitsmaßnahmen sind in der „GLOBALTRUST Certificate Security Policy“ dokumentiert [VIG-17-059_10]. Die Sicherheitsinfrastruktur wird laufend überprüft und angepasst.

Alle wichtigen Einrichtungen sind ausreichend physisch gesichert. Weiters wird nur geschultes und geübtes Personal, nach ausgearbeiteten und vorgegebenen Rollen eingesetzt. Sollten dennoch unvorhergesehene Ereignisse eintreffen, steht ein Notfallplan bereit, der ein rasches Wiederherstellen der Normalsituation erleichtert. Sollten externe Personen oder Stellen von einem Sicherheitsvorfall betroffen sein, werden diese unverzüglich benachrichtigt.

(2) *Qualifizierte und nichtqualifizierte Vertrauensdiensteanbieter melden der Aufsichtsstelle und wo zutreffend anderen einschlägigen Stellen wie etwa der für Informationssicherheit zuständigen nationalen Stelle oder der Datenschutzbehörde unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme von dem betreffenden Vorfall, jede Sicherheitsverletzung oder jeden Integritätsverlust, die bzw. der sich erheblich auf den erbrachten Vertrauensdienst oder die darin vorhandenen personenbezogenen Daten auswirkt.*

Wenn sich die Sicherheitsverletzung oder der Integritätsverlust voraussichtlich nachteilig auf eine natürliche oder juristische Person auswirken, für die der Vertrauensdienst erbracht wurde, so unterrichtet der Vertrauensdiensteanbieter auch diese natürliche oder juristische Person unverzüglich über die Sicherheitsverletzung oder den Integritätsverlust.

Betrifft: ETSI EN 319 401 [VIG-17-059_03], clauses 7.9, 7.11, ETSI EN 319 411-1 [VIG-17-059_04], clause 6.4.8

Anforderungen erfüllt.

Die internen im Betriebshandbuch [VIG-17-059_11] dokumentierten Verfahrungsanweisungen sehen vor, bei sicherheitsrelevanten Ereignissen (insbesondere Kompromittierung von Schlüsseln) die Aufsichtsstelle sowie betroffene Personen und Stellen unverzüglich zu informieren. Weiters werden – so weit möglich – unverzüglich Maßnahmen eingeleitet, um den Schaden für die Betroffenen zu minimieren, zum Beispiel Widerrufen eines Zertifikates im Falle einer Kompromittierung.

Artikel 24 - Anforderungen an qualifizierte Vertrauensdiensteanbieter

(1) *Bei der Ausstellung eines qualifizierten Zertifikats für einen Vertrauensdienst überprüft der qualifizierte Vertrauensdiensteanbieter anhand geeigneter Mittel und im Einklang mit dem jeweiligen nationalen Recht die Identität und gegebenenfalls die spezifischen Attribute der natürlichen oder juristischen Person, der das qualifizierte Zertifikat ausgestellt wird.*

Die Informationen nach Unterabsatz 1 werden vom qualifizierten Vertrauensdiensteanbieter im Einklang mit dem nationalen Recht entweder unmittelbar oder unter Rückgriff auf einen Dritten wie folgt überprüft:

a) *durch persönliche Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person oder*

b) *aus der Ferne mittels elektronischer Identifizierungsmittel, für die vor der Ausstellung des qualifizierten Zertifikats eine persönliche Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person gewährleistet war und die die Anforderungen gemäß Artikel 8 hinsichtlich der Sicherheitsniveaus „substanziell“ oder „hoch“ erfüllen, oder*

c) *durch ein Zertifikat einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels, das gemäß Buchstabe a oder b ausgestellt wurde, oder*

d) *durch sonstige Identifizierungsmethoden, die auf nationaler Ebene anerkannt sind und gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten. Die gleichwertige Sicherheit muss von einer Konformitätsbewertungsstelle bestätigt werden.*

Betrifft: ETSI EN 319 411-1 [VIG-17-059_04], clauses 6.2.2, 6.2.3, ETSI EN 319 411-2 [VIG-17-059_05] clause 6.2.2

Anforderungen erfüllt.

Qualifizierte Zertifikate werden nur für natürliche Personen ausgestellt. Die Prüfung der Identität einer natürlichen Person wird mit einem der beiden folgenden Verfahren durchgeführt:

- durch eine persönliche Registrierung in einem Registrierungsbüro gemäß lit. a.
- mit der Identifizierungsmethode „Post-Zustellung eigenhändig mit Rückschein, nicht an Postbevollmächtigte“, welche in der Bestätigung mit der Referenznummer A-SIT-VIG-17-059A gemäß lit. d bestätigt wurde.

(2) *Für qualifizierte Vertrauensdiensteanbieter, die qualifizierte Vertrauensdienste erbringen, gilt Folgendes:*

b) *Sie beschäftigen Personal und gegebenenfalls Unterauftragnehmer, das bzw. die über das erforderliche Fachwissen, die erforderliche Zuverlässigkeit, die erforderliche Erfahrung und die erforderlichen Qualifikationen verfügt bzw. verfügen, in Bezug auf die Vorschriften für die Sicherheit und den Schutz personenbezogener Daten angemessen geschult worden ist und Verwaltungs- und Managementverfahren anwendet, die den anerkannten europäischen oder internationalen Normen entsprechen.*

Betrifft: ETSI EN 319 411-1 [VIG-17-059_04], clause 6.4.4

Anforderungen erfüllt.

Das Personal von e-commerce monitoring verfügt über technische (HTL oder FH) oder juristische Ausbildung. Neue Mitarbeiterinnen und Mitarbeiter werden durch erfahrenes Personal eingeschult, die Schulungsmaßnahmen werden dokumentiert. Die Zuverlässigkeit des Personals wird durch Vorlage einer Strafregisterbescheinigung vor einer Anstellung überprüft. Die Mitarbeiterinnen und Mitarbeiter werden zur Einhaltung der Datensicherheitsbestimmungen gemäß der bestehenden Gesetze und Standards vertraglich verpflichtet. Über Stellenbeschreibungen sind die Pflichten, Zugriffsrechte und Kompetenzen der Mitarbeiterinnen und Mitarbeiter festgelegt.

c) *Sie verfügen in Bezug auf das Haftungsrisiko für Schäden gemäß Artikel 13 über ausreichende Finanzmittel und/oder schließen eine angemessene Haftpflichtversicherung nach nationalem Recht ab.*

Betrifft: ETSI EN 319 401 [VIG-17-059_03], clause 7.1.1 c), ETSI EN 319 411-1 [VIG-17-059_04], clause 6.8.2

Anforderungen erfüllt.

Der VDA verfügt über eine Haftpflichtversicherung und Eigenkapitalausstattung, die den Bestimmungen des mittlerweile außer Kraft getretenen § 2 SigV entspricht. Diese beinhalten eine Haftpflichtversicherung mit einer Mindestversicherungssumme von 700 000 Euro, die zumindest drei Versicherungsfälle im Jahr deckt und Eigenmittel oder ein eingezahltes Nennkapital von mindestens 300 000 Euro.

d) *Sie unterrichten Personen, die einen qualifizierten Vertrauensdienst nutzen wollen, klar und umfassend über die genauen Bedingungen für die Nutzung des Dienstes, einschließlich Nutzungsbeschränkungen, bevor sie vertragliche Beziehungen zu dieser Person eingehen.*

Betrifft: ETSI EN 319 401 [VIG-17-059_03] clause 6.2, ETSI EN 319 411-1 [VIG-17-059_04], clauses 6.1 c), d), e), f), 6.3.4 a), b), c), 6.9.4

Anforderungen erfüllt.

Im Zuge der Registrierung müssen bevor die Registrierung abgeschlossen ist und der Dienst verwendet werden kann, der Erhalt und die Anerkennung der allgemeinen Informationen zur Nutzung des Dienstes und zum Einsatz qualifizierter Zertifikate [VIG-17-059_05], sowie die Anerkennung der Certificate Policy [VIG-17-059_08] und des Certificate Practice Statements [VIG-17-059_08] durch den Zertifikatswerber bestätigt werden. Alle Informationen sind öffentlich und dauerhaft auf der Webseite des Vertrauensdienstes (www.globaltrust.eu) verfügbar. Die ausgestellten Zertifikate beinhalten eine URL zur jeweils gültigen Anwendungsvorgabe. Einschränkungen bei der Nutzung der Dienste werden unter http://www.globaltrust.eu/limitation.html veröffentlicht. Dies beinhaltet auch etwaige sicherheitstechnische Beschränkungen, die während der Nutzung des Dienstes auftreten können.

e) *Sie verwenden vertrauenswürdige Systeme und Produkte, die vor Veränderungen geschützt sind und die technische Sicherheit und Zuverlässigkeit der von ihnen unterstützten Prozesse sicherstellen.*

Betrifft: ETSI EN 319 401 [VIG-17-059_03], clauses 7.4 a), f), 7.5, 7.7, 7.8, ETSI EN 319 411-1 [VIG-17-059_04], clause 6.5, ETSI EN 319 411-2 [VIG-17-059_05], clause 6.5

Anforderungen erfüllt.

Die IT-Systeme des VDA laufen in von Dritten betriebenen Hochsicherheitsrechenzentren mit entsprechendem physischen Schutz. Es werden beispielsweise Perimeterschutz, Personenkontrollsysteme, Überwachung und Aufzeichnung bzw. Protokollierung relevanter Vorgänge durchgeführt. Ebenso sind Maßnahmen getroffen worden bzw. Vorgänge definiert für den Fall von unvorhergesehenen Ereignissen (z.B. Stromausfall, Naturgewalten, Ausfall eines Rechenzentrums). Da in den Hochsicherheitsrechenzentren keine räumliche Trennung von IT-Systemen anderer Kunden vorgesehen ist, hat der VDA zusätzliche Überwachungsmechanismen (Öffnungssensor mit Alarmierung, eigene Videoüberwachung) in den Racks implementiert. [VIG-17-059_10]

Die verwendeten Systeme verwenden Software-Eigenentwicklungen des VDA, die auf vertrauenswürdigen Krypto-Bibliotheken (OpenSSL und Bouncycastle) aufgebaut sind. Alle relevanten Systeme werden einer regelmäßigen Integritätsprüfung unterzogen. [VIG-17-059_10].

Die verwendeten QSCDs zur Generierung und Verwaltung der Signaturerstellungsdaten der Signatoren (zum Zeitpunkt der Konformitätsbewertung: CardOS V5.3 QES, V1.0) sowie die HSMs zur Generierung und Verwaltung der Siegelerstellungsdaten des VDA (zum Zeitpunkt der Konformitätsbewertung: Luna PCI-E 3000, Luna PCI 1200, LunaSA 5.4.1) verfügen über die geforderten Bescheinigungen, Bestätigungen bzw. Zertifizierungen und werden entsprechend den darin definierten Einsatzbedingungen eingesetzt.

f) *Sie verwenden vertrauenswürdige Systeme für die Speicherung der ihnen übermittelten Daten in einer überprüfbaren Form, so dass*

i) diese nur mit Zustimmung der Person, auf die sich die Daten beziehen, öffentlich abrufbar sind,

ii) nur befugte Personen Daten eingeben und gespeicherte Daten ändern können,

iii) die Daten auf ihre Echtheit hin überprüft werden können.

Betrifft: ETSI EN 319 401 [VIG-17-059_03], clauses 7.4 a), f), 7.5, 7.7, 7.8, ETSI EN 319 411-1 [VIG-17-059_04], clauses 6.4.3, 6.4.6, 6.5, ETSI EN 319 411-2 [VIG-17-059_05], clause 6.5

Anforderungen erfüllt.

Die Veröffentlichung von Zertifikaten einer Person im Verzeichnisdienst erfolgt nur nach deren Zustimmung im Rahmen der Registrierung. Durch ein Rollenkonzept wird sichergestellt, dass nur befugte Personen die für sie vorgesehenen Rechte besitzen. Ein Zugriff zur Ausstellung von Zertifikaten bzw. zum Veröffentlichen von Zertifikats-Widerrufen ist nur im 4-Augen-Prinzip durch Anmeldung zweier Zertifizierer/innen mittels Mehrfaktor-Authentifizierung möglich.

Die generelle Personalpolitik stellt darüber hinaus sicher, dass Mitarbeiterinnen und Mitarbeiter über ausreichende Qualifizierung verfügen sowie sensibilisiert und vertrauenswürdig sind.

Dokumentationsdaten mit Archivierungserfordernissen werden mit einem Zeitstempel oder einer anderen geeigneten Form der elektronischen Signatur versehen, wodurch eine Prüfung auf Echtheit ermöglicht wird. [VIG-17-059_08] ,[VIG-17-059_09], [VIG-17-059_10]

g) *Sie ergreifen geeignete Maßnahmen gegen Fälschung und Diebstahl von Daten.*

Betrifft: ETSI EN 319 401 [VIG-17-059_03] clauses 5, 6.3, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10, 7.11, 7.12, ETSI EN 319 411-1 [VIG-17-059_04], clauses 6.4, 6.5, ETSI EN 319 411-2 [VIG-17-059_05], clauses 6.4, 6.5

Anforderungen erfüllt.

Der VDA hat eine Risikoanalyse beruhend auf dem BSI Standard „Risikoanalyse auf der Basis von IT Grundschutz“ (BSI 100-3) durchgeführt. Auf dieser Grundlage wird vom VDA ein Informationssicherheitsmanagementsystem (ISMS) betrieben, in dessen Rahmen umfangreiche Sicherheitsmaßnahmen definiert sind, um Fälschungen bzw. Diebstahl von Daten zu verhindern. Das ISMS des VDA ist in der Certificate Security Policy [VIG-17-059_10] dokumentiert. Es werden sowohl organisatorische Maßnahmen (Einsatz geeigneten Personals, Definition aller vorhandenen Rollen inklusive ihrer Zuständigkeiten und Verantwortungen, Ausschluss etwaiger Unvereinbarkeiten) als auch physische (Betrieb der IT-Systeme in Hochsicherheitsrechenzentren) und technische (laufende Integritätsüberprüfung der Systeme, netzwerktechnische Segmentierung, Einsatz von Firewalls, sicherheitsrelevante Systeme werden in separaten Bereichen betrieben) getroffen.

h) *Sie zeichnen alle einschlägigen Informationen über die von dem qualifizierten Vertrauensdiensteanbieter ausgegebenen und empfangenen Daten auf und bewahren sie so auf, dass sie über einen angemessenen Zeitraum, auch über den Zeitpunkt der Einstellung der Tätigkeit des qualifizierten Vertrauensdiensteanbieters hinaus, verfügbar sind, um insbesondere bei Gerichtsverfahren entsprechende Beweise liefern zu können und die Kontinuität des Dienstes sicherzustellen. Die Aufzeichnung kann in elektronischer Form erfolgen.*

Betrifft: ETSI EN 319 401 [VIG-17-059_03], clause 7.12, ETSI EN 319 411-1 [VIG-17-059_04], clauses 6.2.2 g), 6.3.4 e), 6.3.8 a), 6.4.5 c), 6.4.6, 6.4.9

Anforderungen erfüllt.

Alle relevanten Maßnahmen, Entscheidungen, Vereinbarungen, Anweisungen etc. werden durch den VDA beleghaft (schriftlich, Eintragungen in Datenbanken, elektronische Protokollaufzeichnungen der eingesetzten Systeme, E-Mails) dokumentiert. Die Dokumente werden elektronisch oder handschriftlich signiert bzw. wird deren Integrität durch Zeitstempel gesichert. Die Protokolle und historische Versionen werden in einem beschränkt zugänglichen Archivsystem aufbewahrt. Alle den Betrieb des Dienstes betreffenden Ereignis- und Zertifizierungsdienstprotokolle (Ausstellungs-, Sperr-, Entsperr- und Widerrufs-Protokoll für Zertifikate) werden 35 Jahre aufbewahrt. [VIG-17-059_08]

Soweit Ausdrucke aufbewahrt werden (Papierausdrucke, Hardcopies) werden sie in versperrbaren Räumlichkeiten aufbewahrt. Elektronisch archivierte Dokumente werden in gängigen Datenformaten aufbewahrt, unter anderem in Plain-Text, XML, PDF (inkl. PDF/A), TIFF, JPG, GIF,

PNG etc.), von denen auch in Zukunft eine einfache Darstellbarkeit und Lesbarkeit erwartet werden kann. Sofern absehbar ist, dass bestimmte Formate in Zukunft nicht mehr lesbar sind, erfolgt zeitgerecht eine Konvertierung in zukunftssichere Formate. [VIG-17-059_08]

i) *Sie verfügen über einen fortlaufend aktualisierten Beendigungsplan, um die Dienstleistungskontinuität nach den von der Aufsichtsstelle gemäß Artikel 17 Absatz 4 Buchstabe i geprüften Vorgaben sicherzustellen.*

Betrifft: ETSI EN 319 401 [VIG-17-059_03], clause 7.12, ETSI EN 319 411-1 [VIG-17-059_04], clause 6.4.9

Anforderungen erfüllt.

Der VDA hat in seiner Certificate Policy [VIG-17-059_08] einen allgemeinen Plan für die Einstellung seiner Tätigkeiten definiert. Dieser sieht eine unverzügliche Anzeige der Einstellung bei der Aufsichtsstelle sowie die Information aller Signatoren sowie etwaiger Dritter, mit denen der VDA Vereinbarungen getroffen hat, vor. Der VDA versichert, alle Anstrengungen zu unternehmen, damit eine minimale Abwicklung der angebotenen Dienste, insbesondere die Verbreitung des Widerrufsstatus und die weitere Archivierung der gesetzlich notwendigen Unterlagen von einem Dritten vorgenommen werden kann. Im Betriebshandbuch [VIG-17-059_11] des VDA sind die einzelnen Schritte, die bei Einstellung der Tätigkeiten durchzuführen sind, definiert.

j) *Sie stellen eine rechtmäßige Verarbeitung personenbezogener Daten gemäß der Richtlinie 95/46/EG sicher.*

Betrifft: ETSI EN 319 401 [VIG-17-059_03], clause 7.13 c), ETSI EN 319 411-1 [VIG-17-059_04], clause 6.8.4

Anforderungen erfüllt.

e-commerce monitoring verpflichtet sich, alle im Rahmen der Vertrauensdienste erhaltenen personenbezogenen Informationen vertraulich zu behandeln und nur für Zwecke des Vertrauensdienstes sowie für Verständigungszwecke im Zusammenhang mit den Dienstleistungen des VDAs zu verwenden.

Bei einer Registrierung über Webformular wird die Übertragung der Daten durch ausreichende Verschlüsselung gesichert. Eine Übertragung und Verarbeitung personenbezogener Daten ist erst nach der Zustimmung des Betroffenen gestattet. Das Personal ist gemäß der aktuellen Datenschutzbestimmungen geschult und zur Geheimhaltung verpflichtet. [VIG-17-059_08]

k) *Sie erstellen im Falle qualifizierter Vertrauensdiensteanbieter, die qualifizierte Zertifikate ausstellen, eine Zertifikatsdatenbank und halten sie auf dem neuesten Stand.*

Betrifft: ETSI EN 319 411-1 [VIG-17-059_04], clause 6.1

Anforderungen erfüllt.

Die Zertifikatsdatenbank wird vom VDA auf einem eigenen Datenbankserver betrieben. Jedes Zertifikat ist eindeutig identifizierbar und enthält den aktuellen Gültigkeitsstatus. Bei Registrierung, Sperre oder Widerruf von Zertifikaten erfolgt unmittelbar eine Aktualisierung der Datenbank.

(3) *Beschließt ein qualifizierter Vertrauensdiensteanbieter, der qualifizierte Zertifikate ausstellt, ein Zertifikat zu widerrufen, so registriert er den Widerruf in seiner Zertifikatsdatenbank und veröffentlicht den Widerrufsstatus des Zertifikats zeitnah und in jedem Fall innerhalb von 24 Stunden nach Erhalt des Ersuchens. Der Widerruf wird sofort nach seiner Veröffentlichung wirksam.*

Betrifft: ETSI EN 319 411-1 [VIG-17-059_04], clause 6.2.4

Anforderungen erfüllt.

Der Widerruf eines Zertifikats wird von befugten Mitarbeiter/innen direkt über die Zertifikatsdatenbank vorgenommen. Es müssen sich zwei Mitarbeiter/innen mittels Token im 4-Augen-Prinzip anmelden. Der Vorgang wird protokolliert und das Protokoll mit einer elektronischen Signatur versehen. Das Zertifikat scheint danach umgehend in der Widerrufsliste auf. Der VDA garantiert, dass ein Widerruf innerhalb einer maximal zulässige Zeitdauer zwischen Einlangen des Widerrufs bzw. der Sperre und der Durchführung jedenfalls kleiner als 24 Stunden ist. [VIG-17-059_08]

Die Aktualisierung der Widerrufsdienste erfolgt an Werktagen, ausgenommen Samstag, von 9 bis 17 Uhr spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes. Außerhalb dieser Zeit erfolgt die Sperre jedenfalls innerhalb von sechs Stunden. [VIG-17-059_08] Die OCSP-Responder überprüfen die CRL jede Minute auf Aktualität, d.h. eine in der Widerrufsliste veröffentlichte Sperr- bzw. Widerrufsinformation ist binnen längstens einer Minute auch über OCSP verfügbar.

(4) *Im Zusammenhang mit Absatz 3 stellen qualifizierte Vertrauensdiensteanbieter, die qualifizierte Zertifikate ausstellen, den vertrauenden Beteiligten Informationen über den Gültigkeits- oder Widerrufsstatus der von ihnen ausgestellten qualifizierten Zertifikate zur Verfügung. Diese Informationen werden zumindest auf Zertifikatsbasis jederzeit und über die Gültigkeitsdauer des Zertifikats hinaus automatisch auf zuverlässige, kostenlose und effiziente Weise bereitgestellt.*

Betrifft: ETSI EN 319 411-1 [VIG-17-059_04], clause 6.3.10, ETSI EN 319 411-2 [VIG-17-059_05] clause 6.3.10

Anforderungen erfüllt.

e-commerce monitoring stellt für seine Vertrauensdienste Gültigkeits- und Widerrufsinformationen sowohl über das Online Certificate Status Protocol (OCSP) als auch über eine Widerrufsliste (CRL) bereit. Diese beiden Dienste sind 24/7 online und kostenlos verfügbar. Die Verfügbarkeit der Sperr- und Widerrufsdienste wird vom VDA einer laufenden Betriebsüberwachung unterzogen. Die URLs zu den Diensten sind als Attribute in den Zertifikaten vermerkt (Authority Information Access: OCSP – http://ocsp.globaltrust.eu; X509v3 CRL Distribution Points: http://service.globaltrust.eu/static/globaltrust-qualified-1.crl bzw. http://service.globaltrust.eu/static/globaltrust-qualified-2015-1.crl). Die Widerrufsliste enthält alle jemals widerrufenen Zertifikate. Das Entfernen eines Zertifikates aus dieser Liste ist nicht möglich. [VIG-17-059_08], [VIG-17-059_11]

Artikel 28 - Qualifizierte Zertifikate für elektronische Signaturen

(3) *Qualifizierte Zertifikate für elektronische Signaturen können zusätzliche fakultative spezifische Attribute enthalten. Diese Attribute dürfen die Interoperabilität und Anerkennung qualifizierter elektronischer Signaturen nicht berühren.*

Betrifft: ETSI EN 319 411-1 [VIG-17-059_04] clause 6.6.1 i), ii)

Anforderungen erfüllt.

Die Zertifikate entsprechen dem X509v3 Format. Neben den Pflichtfeldern werden sowohl Standard-Zertifikatserweiterungen als auch individuelle Zertifikatserweiterungen verwendet. Alle Felder und Erweiterungen halten sich an die Vorgaben der diesbezüglichen Norm ETSI EN 319 412-2 [VIG-17-059_06]. Als individuelle Erweiterung wird unter der OID 1.2.40.0.36.4.1.3 die Seriennummer der Signaturerstellungseinheit in das Zertifikat aufgenommen. Des Weiteren kann optional die Zugehörigkeit zu einer Behörde oder Berufsgruppe (Notare, Rechtsanwälte, Ziviltechniker) in das Zertifikat aufgenommen werden („E-Government OID“). [VIG-17-059_11] Der Gesamtaufbau der Zertifikate sowie die inkludierten Erweiterungen folgen strikt dem Strukturaufbau des X.509-Standards, eine Störung der Interoperabilität oder Anerkennung der Signaturen ist somit ausgeschlossen.

(4) *Wird ein qualifiziertes Zertifikat für elektronische Signaturen nach der anfänglichen Aktivierung widerrufen, ist es ab dem Zeitpunkt des Widerrufs nicht mehr gültig und sein Status darf unter keinen Umständen rückgängig gemacht werden.*

Betrifft: ETSI EN 319 411-1 [VIG-17-059_04] clause 6.3.9 b)

Anforderungen erfüllt.

Bei Widerruf eines Zertifikates wird es auf die öffentlich und ständig erreichbare Widerrufsliste (CRL) gesetzt. Ein widerrufenes Zertifikat wird nicht mehr von der Liste genommen.

Anhang I - Anforderungen an qualifizierte Zertifikate für elektronische Signaturen

Qualifizierte Zertifikate für elektronische Signaturen enthalten Folgendes:

a) *eine Angabe, dass das Zertifikat als qualifiziertes Zertifikat für elektronische Signaturen ausgestellt wurde, zumindest in einer zur automatischen Verarbeitung geeigneten Form;*

b) *einen Datensatz, der den qualifizierten Vertrauensdiensteanbieter, der die qualifizierten Zertifikate ausstellt, eindeutig repräsentiert und zumindest die Angabe des Mitgliedstaats enthält, in dem der Anbieter niedergelassen ist, sowie*

- *bei einer juristischen Person: den Namen und gegebenenfalls die Registriernummer gemäß der amtlichen Eintragung;*
- *bei einer natürlichen Person: den Namen der Person;*

c) *mindestens den Namen des Unterzeichners oder ein Pseudonym; wird ein Pseudonym verwendet, ist dies eindeutig anzugeben;*

d) *elektronische Signaturvalidierungsdaten, die den elektronischen Signaturerstellungsdaten entsprechen;*

e) *Angaben zu Beginn und Ende der Gültigkeitsdauer des Zertifikats;*

f) *den Identitätscode des Zertifikats, der für den qualifizierten Vertrauensdiensteanbieter eindeutig sein muss;*

g) *die fortgeschrittene elektronische Signatur oder das fortgeschrittene elektronische Siegel des ausstellenden qualifizierten Vertrauensdiensteanbieters;*

h) *den Ort, an dem das Zertifikat, das der fortgeschrittenen elektronischen Signatur oder dem fortgeschrittenen elektronischen Siegel gemäß Buchstabe g zugrunde liegt, kostenlos zur Verfügung steht;*

i) *den Ort der Dienste, die genutzt werden können, um den Gültigkeitsstatus des qualifizierten Zertifikats zu überprüfen;*

j) *falls sich die elektronischen Signaturerstellungsdaten, die den elektronischen Signaturvalidierungsdaten entsprechen, in einer qualifizierten elektronischen Signaturerstellungseinheit befinden — eine geeignete Angabe dieses Umstands, zumindest in einer zur automatischen Verarbeitung geeigneten Form.*

Betrifft: ETSI EN 319 411-1 [VIG-17-059_04], clause 6.6.1, ETSI EN 319 411-2 [VIG-17-059_05] clause 6.6.1 a) & b)

Anforderungen erfüllt.

Die qualifizierten Zertifikate sind entsprechend dem Standard X.509 v3 aufgebaut, alle darin enthaltenen Attribute sind somit auch automatisch verarbeitbar. In der Certificate Policy werden die

möglichen Attribute und deren Inhalte aufgelistet. Durch die Angabe der Zertifikatserweiterung *id-etsi-qcs-QcCompliance* mit dem Wert 1 werden die Zertifikate als qualifizierte Zertifikate deklariert. Mit der Zertifikatserweiterung *id-etsi-qcs-QcSSCD* wird die Verwendung einer qualifizierten elektronischen Signaturerstellungseinheit in einer automatisch verarbeitbaren Form angegeben. [VIG-17-059_08], [VIG-17-059_11]

Um den ausstellenden VDA der Zertifikate festzuhalten, werden dessen Name (O=e commerce monitoring GmbH), Herkunftsland (C=AT) sowie die Bezeichnung der Zertifikate (CN=GLOBALTRUST QUALIFIED 1 bzw. CN=GLOBALTRUST 2015 QUALIFIED 1) als Attribute festgehalten.

Der Name des Unterzeichners wird im Zertifikat festgehalten, allfällige Pseudonyme sind so gesondert gekennzeichnet eingetragen, dass sie nicht mit Vor- bzw. Familiennamen, offiziellen Firmen- oder Organisationsbezeichnungen verwechselt werden können. Im Subject-Feld ist eine innerhalb des VDA eindeutige Seriennummer angegeben.

Weiters sind Beginn und Ende der Zertifikatsgültigkeit sowie eine eindeutige Seriennummer des Zertifikats gespeichert. Zur Validierung der Signatur wird der öffentliche Schlüssel des Unterzeichners samt verwendeten Parametern eingetragen.

In der Zertifikatserweiterung cRLDistributionPoints wird eine URL festgehalten, unter der die diesbezügliche Widerrufsliste geführt wird. Weiters werden in der Zertifikatserweiterung *authorityInfoAccess* URLs zum Onlinestatusprotokoll (OCSP) und Ausstellerzertifikat (CA-Issuer) gespeichert.

Als kryptografische Verfahren werden bei der Zertifikatsausstellung RSA mit 4096 Bit und SHA256 als Hashverfahren eingesetzt. Die Schlüssel des VDA werden in geeigneten HSMs generiert und verwahrt. Damit werden die Anforderungen für fortgeschrittene elektronische Siegel erfüllt.

D. Anhang – Unterlagen

VIG-17-059_NN	Erhalten am	Typ	Beschreibung	Revision	Status
VIG-17-059_01	2017-03-21	Elektronisch	Antrag		Endgültig
VIG-17-059_02		Elektronisch	Verordnung (EU) Nr. 910/2014 (eIDAS)		Endgültig
VIG-17-059_03		Elektronisch	ETSI EN 319 401 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers	V2.1.1	Endgültig
VIG-17-059_04		Elektronisch	ETSI EN 319 411-1 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements	V1.1.1	Endgültig
VIG-17-059_05		Elektronisch	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	V2.1.1	Endgültig
VIG-17-059_06		Elektronisch	ETSI EN 319 412-2 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons	V2.1.1	Endgültig
VIG-17-059_08	2017-06-22	Elektronisch	GLOBALTRUST® Certificate Policy	V 2.0 vom 22. Juni 2017	Endgültig
VIG-17-059_09	2017-06-22	Elektronisch	GLOBALTRUST® Certificate Practice Statement	V 2.0 vom 22. Juni 2017	Endgültig
VIG-17-059_10	2017-06-22	Elektronisch	GLOBALTRUST® Certificate Security Policy	V 2.0b vom 22. Juni 2017	Endgültig
VIG-17-059_11	2017-06-22	Elektronisch	GLOBALTRUST® Service – Betriebs-Handbuch (Auszüge)	V 1.0c vom 19. Juni 2017	Endgültig
VIG-17-059_12	2017-06-07	Papier	[CQinfo] Information zum Einsatz qualifizierter Zertifikate GLOBALTRUST® qualified	V 1.0	Endgültig