powered by e-commerce monitoring gmbh

public / öffentlich
Endfassung

[CQINFO-WEB] Information zum Einsatz qualifizierter Serverzertifikate GLOBALTRUST® SERVER QUALIFIED Version v1.0

Inhalt

Editorial note: This document has been provided with an qualified signature. The date of signature can deviate from the date of the start of the validity of this document for different legal and organisational reasons. The signature does not give information about the start of the validity of the document, but confirms the integrity of the content.

Redaktioneller Hinweis: Das vorliegende Dokument ist mit einer qualifizierten Signatur versehen. Das Datum der Signatur kann aus verschiedenen rechtlichen und organisatorischen Gründen vom Datum des Gültigkeitsbeginns des Dokuments abweichen. Die Signatur gibt keine Auskunft über den Gültigkeitsbeginn des Dokuments, sondern bestätigt nur die Unversehrtheit des Inhalts.

1. ALLGEMEINES

Die vorliegende Erstinformation wendet sich an Zertifikatswerber, Signatoren und sonstige Dritte, soweit sie ein rechtliches Interesse an den GLOBALTRUST®-Zertifikatsprodukten haben.

Das vorliegende Dokument kann unter http://www.globaltrust.eu/static/general-web.pdf abgerufen werden und ist mit einer qualifizierten elektronischen Signatur (iS eIDAS-VO) versehen.

Weiterführende Informationen können beim Vertrauensdiensteanbieter (VDA)
e-commerce monitoring GmbH angefordert werden oder können auf der Website
http://www.globaltrust.eu/certificate-policy.html eingesehen werden.

2. REFERENZEN

Im Zusammenhang mit der vorliegenden Erstinformation wird auf folgende Dokumente in der jeweils gültigen Fassung verwiesen:

[GCP] GLOBALTRUST® Certificate Policy (public, OID-Nummer: 1.2.40.0.36.1.1.8.1, http://www.globaltrust.eu/static/globaltrust-certificate-policy.pdf)

[GCPS] GLOBALTRUST® Certificate Practice Statement (public, OID-Nummer: 1.2.40.0.36.1.2.3.1, http://www.globaltrust.eu/static/globaltrust-certificate-practice.pdf)

[eIDAS-VO] 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, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&rid=1

[ETSI 319 412] ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles Part 1-5, https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx

[CABROWSER-EV] CA/Browser-Forum Guidelines For The Issuance And Management Of Extended Validation Certificates, https://cabforum.org/extended-validation/

3. VERWENDETE BEGRIFFE

Im Zusammenhang mit der vorliegenden Information werden folgende Begriffe gemäß GLOBALTRUST® Certificate Policy verwendet:

Auszug aus der [GCP] GLOBALTRUST® Certificate Policy Abschnitt "1.6 Definitionen und Kurzbezeichnungen "

Elektronische Signatur
Daten in elektronischer Form im Sinne EU Signaturverordnung [eIDAS-VO], die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.

fortgeschrittene elektronische Signatur
Eine elektronische Signatur, die folgende Anforderungen erfüllt:
a) sie ist ausschließlich dem Unterzeichner zugeordnet;
b) sie ermöglicht die Identifizierung des Unterzeichners;
c) sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;
d) sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

qualifizierte elektronische Signatur
Elektronische Signatur die folgende Anforderungen erfüllt:
- alle Anforderungen der fortgeschrittenen elektronischen Signatur,
- die auf einem qualifizierten Zertifikat beruht und
- von einer sicheren Signaturerstellungseinheit (SSCD) erstellt wird.

Zertifikat
Eine elektronische Bescheinigung, mit der Signaturprüfdaten einem Signator zugeordnet werden und die Identität dieses Signators, der von ihm vertretenen juristischen Person oder einem von ihm oder der von ihm vertretenen juristischen Person kontrollierten System bestätigt wird.

qualifiziertes Zertifikat für elektronische Signaturen
Ein Zertifikat, das zur Erstellung elektronischer Signaturen dient und das dem Stand der Technik ausgestellt wurde und insbesondere die Anforderungen der [eIDAS-VO] Anhang I erfüllt und von einem Zertifizierungsdiensteanbieter (VDA) bereitgestellt wird, der die Anforderungen der [eIDAS-VO] erfüllt.
Der Inhalt folgt [ETSI EN 319 412]. Die Laufzeit des qualifizierten Zertifikats für elektronische Signaturen ist auf Grund der rechtlichen Vorgaben auf maximal 5 Jahre limitiert und kann vom VDA auf Grund geänderter rechtlicher Rahmenbedingungen oder anderer wichtiger Gründe jederzeit verkürzt werden.

qualifiziertes Serverzertifikat
Ein Zertifikat, das zur Websiteauthentifizierung dient und das dem Stand der Technik ausgestellt wurde und insbesondere die Anforderungen der [eIDAS-VO] Anhang IV sowie [CABROWSER-EV] erfüllt und von einem Zertifizierungsdiensteanbieter (VDA) bereitgestellt wird, der die Anforderungen der [eIDAS-VO] erfüllt.
Der Inhalt folgt [ETSI EN 319 412] sowie [CABROWSER-EV] Die Laufzeit des qualifizierten Serverzertifikats ist auf Grund der rechtlichen Vorgaben auf maximal 825 Tage limitiert und kann vom VDA auf Grund geänderter rechtlicher Rahmenbedingungen oder anderer wichtiger Gründe jederzeit verkürzt werden.

qualifiziertes Zertifikat
Kann entweder als qualifiziertes Zertifikat für elektronische Signaturen oder als qualifiziertes Serverzertifikat ausgestellt werden und enthält einen Hinweis auf die Certificate Policy unter der das Zertifikat ausgestellt wurde und die es eindeutig als qualifiziertes Zertifikat kennzeichnet.
Die Kodierung des Subjects erfolgt gemäß UTF-8 wenn Umlaute/Sonderzeichen enthalten sind, printableString kann verwendet werden, wenn Umlaute/Sonderzeichen nicht enthalten sinnd.
Das Subject kann folgende Einträge enthalten: countryName (verpflichtend), localityName (verpflichtend), stateOrProvinceName (optional), organizationName (sofern Zertifikat für eine Organisation ausgestellt wird), organizationalUnitName (optional), commonName oder pseudonym oder givenName (eines ist verpflichtend), title (optional), serialNumber (verpflichtend), businessCategory (verpflichtend, nur bei qualifizierten Serverzertifikaten), jurisdictionLocalityName

und/oder jurisdictionStateOrProvinceName und/oder jurisdictionCountryName (nur bei qualifizierten Serverzertifikaten, Einsatz gemäß [CABROWSER-EV]) Jedes Feld kann nur für jene Einträge verwendet werden, für das es gemäß der anzuwendenden Standards und Normen definiert ist.

Weitere Angaben im Zertifikat:

- X509v3 Key Usage: critical Digital Signature und bei qualifizierten Serverzertifikaten zusätzlich. Key Encipherment
- X509v3 Extended Key Usage: critical TLS Web Server Authentication und/oder TLS Web Client Authentication
- CA Issuers - URI:http://service.globaltrust.eu/static/globaltrust-NN-**-der.cer
- X509v3 CRL Distribution Points: Full Name: URI:http://service.globaltrust.eu/static/globaltrust-NN-**.crl
- OCA - URI:http://OCA-NN-**.globaltrust.eu
- X509v3 Certificate Policies: Policy: 1.2.40.0.36.1.1.##.1
- CPS: http://www.globaltrust.eu/certificate-policy.htm Policy: 0.4.0.1456.1.1 (qualifizierte Zertifikate für elektronische Signaturen) oder 0.4.0.194112.1.4 (qualifizierte Serverzertifikate) und 2.23.140.1.1 (qualifizierte Serverzertifikate, wenn auch EV)
- 1.2.40.0.36.4.1.3: [Seriennummer der Signaturerstellungseinheit als ASN1 OCTET STRING]
- qcStatements:
- id-etsi-qcs-QcCompliance (OID 0.4.0.1862.1.1),
- id-etsi-qcs-QcLimitValue: QcEuLimitValue (OID 0.4.0.1862.1.2) (optional)
- id-etsi-qcs-QcRetentionPeriod: QcEuRetentionPeriod (OID 0.4.0.1862.1.3) (optional)
- id-etsi-qcs-QcSSCD (OID 0.4.0.1862.1.4)
- id-etsi-qcs-QcType (OID 0.4.0.1862.1.6)
- id-etsi-qct-web (OID 0.4.0.1862.1.6.3)
- Verwaltungseigenschaft (OID 1.2.40.0.10.1.1.1): Verwaltungskennzeichen (optional)
- Dienstleistereigenschaft (OID 1.2.40.0.10.1.1.2): NULL (optional)
- Organwaltereigenschaft (OID 1.2.40.0.10.3.4): Verwaltungskennzeichen (optional)
- Eigenschaft zur Signatur von elektronischer Vollmachten (OID 1.2.40.0.10.1.7.2): NULL (optional)
- weitere OID-Einträge sofern im Einklang mit den Bestimmungen zu qualifizierten Zertifikaten (optional)
- verwendeter Signature Algorithm: SHA2 (sha256WithRSAEncryption oder höher)

4. BETRIEBSVORAUSSETZUNGEN DES VDA

Die Zertifizierungstätigkeit des VDA unterliegt der Aufsicht der Telekom-Control-Kommission (TKK) bzw. Rundfunk und der Telekom Regulierungs-GmbH (RTR-GmbH) beide A-1060 Wien, Mariahilfer Straße 77-79. Kontaktdaten der Aufsichtsstelle finden sich unter https://signatur.rtr.at/

Die Tätigkeit des VDA wurde mit 29. Juni 2015 gemäß Bescheid A 4/2014-36 akkreditiert. Seit 1. Juli 2016 erfolgt die Tätigkeit gemäß eIDAS-Verordnung

Angaben zum VDA und seiner Zertifizierungsdienste sind bei der Aufsichtsstelle unter https://www.signatur.rtr.at/de/vd/Zertifizierungsdiensteanbieterdetails%3Fanbieter=ecm.html abrufbar.

Die Erbringung der Zertifizierungsdienste erfolgt auf Basis folgender Dokumente in der jeweils gültigen Fassung:

- [GCPS] GLOBALTRUST® Certificate Practice Statement (public, OID-Nummer: 1.2.40.0.36.1.2.3.1, http://www.globaltrust.eu/static/globaltrust-certificate-practice.pdf)
- [GCP] GLOBALTRUST® Certificate Policy (public, OID-Nummer: 1.2.40.0.36.1.1.8.1, http://www.globaltrust.eu/static/globaltrust-certificate-policy.pdf)
- [GCSP] GLOBALTRUST® Certificate Security Policy (non public)

Sonstige, nicht durch die Bestimmungen der Zertifizierungsdienste geregelten wirtschaftliche Bedingungen, insbesondere Konditionen und Zahlungsmodalitäten können den Allgemeinen Geschäftsbedingungen des VDA entnommen werden (http://www.e-monitoring.at/static/agb.pdf).

5. SICHERHEITSKONZEPT

Das Sicherheitskonzept des VDA ist vollständig in [GCP] GLOBALTRUST® Certificate Policy beschrieben.

1. ALLGEMEINE SICHERHEITSANGABEN

Auszug aus der [GCP] GLOBALTRUST® Certificate Policy Abschnitt "6. Technische Sicherheitsmaßnahmen":

Die Betriebsinfrastruktur des Betreibers wird regelmäßig überprüft und an geänderte Anforderungen angepasst. Im Falle einer Änderung der [GCSP] GLOBALTRUST® Certificate Security Policy erfolgt eine Mitteilung an die zuständigen Aufsichtsstellen.

Der technische Betrieb erfolgt beim Betreiber oder in den Räumen ausreichend qualifizierter Vertragspartner. Die aktuellen Vertragspartner sind vollständig dokumentiert und können der Aufsichtsbehörde jederzeit bekannt gegeben werden. Alle Vertragspartner sind an die Wahrung der Datensicherheit im Sinne dieser Policy, des [DSG 2000], der Signaturbestimmungen und sonstiger zutreffender rechtlicher Bestimmungen und technischen Standards vertraglich insoweit gebunden, als es die ihnen übertragene Tägigkeit betrifft.

Der Betreiber verwendet zur Erbringung seiner Zertifizierungsdienste und zur Abwicklung der internen (administrativen) Geschäftsprozesse soweit technisch möglich, sicherheitstechnisch erforderlich und wirtschaftlich sinnvoll Signatur- und Kryptographieschlüssel.

2. SPEZIFISCHE SICHERHEITSANGABEN

Auszug aus der [GCP] GLOBALTRUST® Certificate Policy Abschnitt "5. Anforderungen Standort, Management und Betrieb":

Der VDA ist für die Gestaltung und Dokumentation aller Prozesse im Rahmen der Zertifizierungsdienste verantwortlich; dies gilt auch für die an Vertragspartner ausgelagerten Dienste. Die Aufgaben und zugeordneten Verantwortlichkeiten der Vertragspartner sind klar geregelt, weiters sind Kontrollen zur Überprüfung der ordnungsgemäßen Tätigkeit eingerichtet.

Die Verfügbarkeit der zentralen Zertifizierungsdienste
- *Verbreitung der VDA-Zertifikate,*
- *Sperr- und Widerrufsmanagement und*
- *Verbreitung des Widerrufsstatus*

erfolgt durch redundante Systemkomponenten und unterliegt einer laufenden Betriebsüberwachung. Angestrebt wird die Verfügbarkeit dieser zentralen Zertifizierungsdienste von 99,9% auf Monatsbasis. Gemessen wird die Verfügbarkeit durch Aufzeichnungen aus der Betriebsüberwachung. Diese Aufzeichnungen werden zumindest für die Dauer eines Jahres bereit gehalten und erlauben jedenfalls Beginn und Ende von Ausfällen zu erkennen.

Alle betrieblichen Abläufe sind dokumentiert und unterliegen der [GCP] GLOBALTRUST® Certificate Policy, der [GCSP] GLOBALTRUST® Certificate Security Policy und dem jeweils anzuwendenden [GCPS] GLOBALTRUST® Certificate Practice Statement.

Die Zertifizierungsdienste werden ausschließlich in geeigneten Räumlichkeiten erbracht. Die Details sind in der [GCSP] GLOBALTRUST® Certificate Security Policy geregelt. Die Geschäftsführung des VDA entscheidet, an welchem Ort die Zertifizierungsdienste stattzufinden haben, dabei werden die Vorgaben der [GCSP] GLOBALTRUST® Certificate Security Policy beachtet.

Es ist sicher gestellt, dass der Zutritt zu Räumlichkeiten, in denen sicherheitskritische Funktionen ausgeübt werden, beschränkt ist und die Risken einer physischen Beschädigung von Anlagen minimiert sind.

Insbesondere gelten folgende Sicherheitsmaßnahmen:
1. *Der Zugriff zu den Geräten, in denen Zertifizierungs- und Widerrufsdienste erbracht werden, ist auf autorisiertes Personal beschränkt. Die Systeme, welche Zertifikate ausstellen, sind vor Gefährdung durch Umweltkatastrophen baulich geschützt.*
2. *Es werden Maßnahmen ergriffen, um den Verlust, die Beschädigung oder die Kompromittierung von Anlagen und die Unterbrechung des Betriebes zu verhindern.*

Stromversorgung und Klimanalage sind in ausreichender Kapazität verfügbar. Die Auswahl des Standortes der zertifizierungskritischen Komponenten erfolgt unter Bedachtnahme der Unwahrscheinlichkeit einer Gefährdung durch Wasser. Es sind ausreichende Vorkehrungen zum Brandschutz getroffen.

Backups werden entfernt vom Betriebsstandort der zertifizierungskritischen Komponenten aufbewahrt und gesichert.

Die Erbringung der Zertifizierungsdienste (insbesondere Antragstellung, Ausstellung, Ablauf und Widerruf von Zertifikaten) erfolgt unter strikter Trennung von administrativen und technischen Tätigkeiten. Für den Betreiber kommen organisatorische Maßnahmen zur gesicherten Betriebsführung zentrale Bedeutung zu. Zu diesen zentralen allgemeinen Maßnahmen gehören:
a) 4-Augen-Prinzip bei kritischen Prozessen
b) motivierte Mitarbeiter
c) klare und eindeutige Aufgabenverteilung
d) umfassende Dokumentation des betrieblichen Geschehens
e) kollegialer Informationsaustausch im Rahmen eines institutionalisierten Zertifizierungs-Ausschusses

Kritische Prozesse unterliegen dem 4-Augenprinzip. Die beteiligten Personen werden dokumentiert. Im Zuge der Zertifizierungsdienste authentifizieren sich die Mitarbeiter eindeutig, erfolgt zwischenzeitlich ein Log-Out, erfolgt eine Re-Authentifizierung. Alle vergebenen Authentifikationskennzeichen werden eindeutig und einmalig vergeben.

Alle im Zusammenhang mit Zertifizierungsdiensten tätigen Mitarbeiter, dies sind insbesondere jene Mitarbeiter, die die Bestellungen von Signaturprodukten verwalten, den technischen Betrieb betreuen und die Neu- und Weiterentwicklung der Zertifizierungsprodukte durchführen weisen die erforderliche Fachkenntnis auf. Die Systemadministratoren und sonstige mit Zertifizierungsaufgaben betraute Personen werden zur Einhaltung der Datensicherheitsbestimmungen gemäß der bestehenden Gesetze und Standards vertraglich verpflichtet.

- *Für die Mitarbeiter des VDAs sind klare Stellenbeschreibungen ausgearbeitet, in denen die Pflichten, Zugriffsrechte und Kompetenzen dargelegt sind.*
- *Alle Leitungsfunktionen sind mit Personen besetzt, die über Erfahrung mit der Technologie elektronischer Signaturen und Verschlüsselungen verfügen.*
- *Der VDA beschäftigt keine Personen, die strafbare Handlungen begangen haben, welche sie für eine vertrauenswürdige Position ungeeignet erscheinen lassen.*
- *Bei sicherheitsrelevante Funktionen und Verantwortlichkeiten wir darauf geachtet, dass keine Interessenskonflikte bzw. Unvereinbarkeiten entstehen.*

Weiters haben alle Mitarbeiter eine verbindliche Erklärung bezüglich ihrer Unbescholtenheit abzugeben, wobei der Umfang der Erklärung auf Grund gesetzlicher Bestimmungen auf bestimmte strafbare Sachverhalte beschränkt werden kann. Nicht zu berücksichtigen sind Verurteilungen die nach einschlägigen Bestimmungen als getiligt, aufgehoben oder gelöscht anzusehen sind.

Die Mitarbeiter werden mit Zertifizierungsaufgaben ausschließlich nach ausreichender Einschulung betraut.

Der Betreiber kann sich für alle seine Zertifizierungsdienste (vollständig oder teilweise) Dienstleister bedienen. In diesem Fall werden die für den jeweiligen Zertifizierungsdienst gültigen Anforderungen vollständig dem Dienstleister überbunden. Dienstleister werden sorgfältig ausgewählt und zur Einhaltung der für ihre Tätigkeit anwendbaren Bestimmungen verpflichtet.

Die Verantwortung für die ordnungsgemäße Erbringung der Zertifizierungsdienste bleibt in jedem Fall beim VDA.

Die zum Betrieb der Zertifizierungsdienste erforderlichen Dokumente und Prozesse werden nachweislich den Mitarbeitern zur Kenntnis gebracht.

Folgende Ereignisse unterliegen besonderen Dokumentationen:

- *Außergewöhnliche Betriebssituationen (inkl. Wartungen, Systemausfälle, ..) werden durch das Überwachungssystem dokumentiert und können bei Bedarf durch zusätzliche Anmerkungen und Erklärungen ergänzt werden. Die Überwachungsdaten werden regelmäßig signiert und archiviert.*
- *Alle im Zuge der Zertifikatserstellung relevanten Ereignisse werden protokolliert. Das sind insbesondere alle Ereignisse die den Lebenszyklus von ausgestellten Zertifikaten sowie Cross-Zertifikate betreffen.*
- *Alle Ereignisse die den Antrag auf neue Zertifikate, den Antrag auf Verlängerung von Zertifikaten oder die Bestätigung von Anträgen betreffen, werden dokumentiert.*

Dem Betriebspersonal stehen Monitoring-Instrumente zur Verfügung, die laufend den Betriebsstatus anzeigen. Diese Monitoring-Instrumente werden laufend aktuellen Anforderungen und betrieblichen Erfahrungen angepasst und optimiert.

Die Überwachungsfrequenz orientiert sich an den betrieblichen Anforderungen der einzelnen Prozesse und ist intern dokumentiert. Es erfolgt bei Bedarf eine Anpassung.

Die Aufbewahrungszeit für Aufzeichnungen die für Audits erforderlich sind, ist jedenfalls so lange, bis ein Audit durchgeführt und bestätigt wurde. Davon unberührt sind allenfalls längere gesetzliche oder vertragliche Aufbewahrungszeiten.

Die Dokumentation der Sicherheitsvorkehrungen, von Störfällen und besonderen Betriebssituationen erfolgt in statischen Dateiformaten bzw. in Dateiformaten ohne dynamische Elemente, werden mit einem Zeitstempel oder einer anderen geeigneten Form der elektronischen Signatur versehen.

Archive der Überwachungsaufzeichnungen werden entfernt vom Betriebsstandort der zertifizierungskritischen Komponenten aufbewahrt und gesichert. Die erforderlichen Maßnahmen sind in der [GCSP] GLOBALTRUST® Certificate Security Policy geregelt.

Die Zertifizierungsdienste wurden einer Risikoanalyse unterzogen, die Ergebnisse und die erforderlichen Maßnahmen sind in der [GCSP] GLOBALTRUST® Certificate Security Policy dokumentiert.

Alle relevanten Maßnahmen, Entscheidungen, Vereinbarungen, Anweisungen usw. werden beleghaft dokumentiert. Als "beleghaft" werden alle Aufzeichnungsformen verstanden, die eine zuverlässige spätere Rekonstruktion der Dokumentation erlaubt, insbesondere sind dies schriftliche Aufzeichnungen (inkl. Ausdrucke), Eintragungen in entsprechende, dafür vorgesehene Datenbanken, elektronische Protokollaufzeichnungen der eingesetzten Systeme oder E-Mails.

Abhängig von den individuellen Anforderungen können diese Dokumente elektronisch oder handschriftlich signiert sein oder es kann die Integrität durch andere Maßnahmen, wie Zeitstempel gesichert sein.

Protokolle und historische Versionen werden in einem beschränkt zugänglichen Archivsystem aufbewahrt. Die Aufbewahrungszeit ist, sofern nicht im jeweils anzuwendenden [GCPS] GLOBALTRUST® Certificate Practice Statement anders vermerkt, die Dauer von 35 Jahren ab Erstellung des Dokuments/Eintreten des Ereignisses.

Für Unterlagen, die für qualifizierte Zertifikate von Bedeutung sind, gilt jedenfalls die gesetzlich vorgesehene Mindestaufbewahrungszeit. Alle archivierten Unterlagen sind mit Zeitangaben versehen, die sich auf das dokumentierte Ereignis beziehen.

Abhängig von den betrieblichen Anforderungen können diese Dokumente elektronisch oder handschriftlich signiert sein oder es kann die Integrität durch andere Maßnahmen, wie Zeitstempel gesichert sein.

Der Wechsel eines Schlüssels beim Betreiber wird zeitgerecht geplant und unterliegt allen erforderlichen Audits. Vom Wechsel betroffene Dritte werden zeitgerecht über einen geplanten Wechsel informiert.

Als Katastrophenszenario ("worst case") wird die Kompromittierung eines Zertifizierungsschlüssels angesehen. Für diesen Fall wird der VDA die Aufsichtsstelle, die Signatoren, die auf die Verlässlichkeit der Zertifizierungsdienste vertrauenden Personen und ggf. andere Zertifizierungsdiensteanbieter und Einrichtungen, mit denen einschlägige Vereinbarungen bestehen, davon unterrichten und mitteilen, dass die Widerrufs- und Zertifikatsinformationen nicht mehr als zuverlässig anzusehen sind.

Zertifikate und Widerrufslisten werden als nicht mehr gültig gekennzeichnet. Den Signatoren werden mit Hilfe eines neu generierten sicheren Zertifizierungsschlüssels neue Zertifikate ausgestellt.

Der Betreiber hat Vorkehrungen für den Fall des Ausfalls einzelner Betriebskomponenten getroffen. Die Zertifizierungsdienste werden dann statt im Normalbetrieb (volle Funktionalität ist vorhanden) im Ausfallsbetrieb (Teilfunktionalitäten sind vorhanden) betrieben.

Für alle zentralen Komponenten des Zertifizierungsbetriebes existiert eine Risikoanalyse die in der [GCSP] GLOBALTRUST® Certificate Security Policy beschrieben ist. Im Rahmen der Risikoanalyse sind auch die Verfahren zur Wiederherstellung des Normalbetriebs nach Kompromittierung von Ressourcen beschrieben.

Der VDA zeigt die Einstellung der Tätigkeit - sofern vorgesehen - unverzüglich der Aufsichtsstelle an und stellt sicher, dass eine eventuelle Beeinträchtigung ihrer Dienstleistungen sowohl gegenüber Signatoren als auch gegenüber allen auf die Zuverlässigkeit der Dienste vertrauenden Parteien möglichst gering gehalten wird.

Über die Einstellung werden außerdem alle Signatoren sowie etwaige Dritte, mit denen der VDA relevante Vereinbarungen geschlossen hat, informiert. Alle beim VDA vorhandenen privaten Schlüssel werden aus dem Verkehr gezogen.

In diesem Fall werden weiters Anstrengungen unternommen, damit eine minimale Abwicklung der angebotetenen Dienste, insbesondere die Verbreitung des Widerrufsstaus, und die weitere Archivierung von gesetzlich notwendigen Unterlagen von einem Dritten vorgenommen werden kann.

6. EIGENSCHAFTEN DER QUALIFIZIERTEN SERVERZERTIFIKATE

Der VDA bietet qualifizierte Serverzertifikate in der in der [eIDAS-VO] definierten Variante an.

Qualifizierte Zertifikate werden nur eindeutig identifizierten Personen ausgestellt.

Die Identitätsprüfung kann durch persönliche Anwesenheit des Antragstellers und Vorlage geeigneter amtlicher Personaldokumente erfolgen. Sie kann auch im Fernverfahren durch Vorabübermittlung von gut lesbaren Kopien geeigneter amtlicher Personaldokumente erfolgen. Im zweiten Fall erfolgt statt der Identitätsprüfung im ersten Schritt eine Plausibilitätsprüfung der übermittelten Unterlagen, die Identitätsprüfung erfolgt bei Aushändigung der Unterlagen zum qualifizierten Zertifikat durch entsprechend autorisierte Personen.

Auszug aus eIDAS Art. 3

„Zertifikat für die Website-Authentifizierung" ist ein Zertifikat, das die Authentifizierung einer Website ermöglicht und die Website mit der natürlichen oder juristischen Person verknüpft, der das Zertifikat ausgestellt wurde.

„Qualifiziertes Zertifikat für die Website-Authentifizierung" ist ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat für Website-Authentifizierung, das die Anforderungen des Anhangs IV erfüllt.

Auszug aus [CABROWSER-EV]:
„Provide a reasonable assurance to the user of an Internet browser that the Web site the user is accessing is controlled by a specific legal entity identified in the EV Certificate[…]"

„enable the encrypted communication of information over the Internet between the user of an Internet browser and a Web site.[…]"

„Make it more difficult to mount phishing and other online identity fraud attacks using Certificates;"

7. PFLICHTEN DES SIGNATORS

Auszug aus der [GCP] GLOBALTRUST® Certificate Policy Abschnitt "4.5.1 Subscriber private key and certificate usage / Nutzung des privaten Schlüssels und des Zertifikates durch den Signator":

Der VDA bindet den Signator vertraglich an die Einhaltung der nachfolgend angeführten Verpflichtungen.
Dem Antragsteller werden alle Vertragsbedingungen auf der Website des VDA zugänglich gemacht. Gleichzeitig mit dem Absenden des Bestellformulars bestätigt er deren Kenntnisnahme und Akzeptanz.
Die dem Signator auferlegten Verpflichtungen umfassen:

1. *Die Angabe vollständiger und korrekter Informationen in Übereinstimmung mit den Anforderungen dieser Policy insbesondere anlässlich des Vorgangs der Registrierung.*
2. *Die Prüfung der Korrektheit aller Angaben im Zertifikat auf deren Korrektheit unmittelbar nach erfolgter Zustellung*
3. *Die Aufbewahrung des privaten Schlüssels in einer Hardware-Einheit, zu der der Signator den alleinigen Zugriff hat (z.B. verschlüsseltes Abspeichern des privaten Schlüssels mittels Passwort, Signatur-PIN bzw. Passphrase, spezielle Signaturerstellungseinheiten, die das Auslesen des privaten Schlüssels verhindern oder wesentlich erschweren).*
   Im Fall einfacher Signaturen, wie zum Beispiel GLOBALTRUST® CLIENT, sind auch Zutrittsbeschränkungen und organisatorische Maßnahmen, die den Zugang zum Computer beschränken der den Schlüssel und das Zertifikat enthält, als ausreichende Sicherheitsmaßnahmen im Sinne dieser Policy zu verstehen.
4. *Im Falle der Selbstgenerierung des privaten Schlüssels werden geeignete sichere Verfahren angewandt, die eine ausreichende Zufallsqualität bei der Schlüsselerzeugung gewährleisten, insbesondere sind dies ausdrücklich dafür vorgesehene Hardwarekomponenten, wie HSM-Module oder Softwarekomponenten, die es erlauben durch Systemereignisse die Zufallsqualität zu erhöhen (insbesondere Angabe von Dateien mit Zufallszahlen, Durchführen von Mausbewegungen oder Tastaturanschlägen während der Schlüsselgenerierung). Der VDA behält sich vor, vom Signator vollständige Auskunft über den Schlüsselgenerierungsvorgang zu verlangen und bei Bedenken bezüglich der Zufallsqualität des Schlüssels einen Zertifizierungsantrag abzulehnen. Ungeeignete Schlüsselverfahren werden auf der Website des Betreibers bekannt gemacht und dürfen nicht verwendet werden.*
5. *Die Anwendung entsprechender Vorsicht, um den unbefugten Gebrauch des privaten Schlüssels zu verhindern.*
6. *Die Verwendung von Serverzertifikaten ausschließlich auf Geräten, die über die im Zertifikat eingetragenen Adressen (bei X.509v3 in der subjectAltName-Erweiterung) erreichbar sind.*

7. *Die unverzügliche Benachrichtigung des Betreibers, wenn vor Ablauf der Gültigkeitsdauer eines Zertifikats eine oder mehrere der folgenden Bedingungen eintreten:*
   - *Der private Schlüssel oder dessen Aktivierungsdaten gingen verloren.*
   - *der private Schlüssel des Signators oder dessen Aktivierungsdaten wurden möglicherweise kompromittiert,*
   - *die alleinige Kontrolle über den privaten Schlüssel ging verloren,*
   - *die im Zertifikat beinhalteten Informationen sind inkorrekt oder haben sich geändert,*
8. *Die unverzügliche vollständig Außerbetriebnahme des Schlüssels, sobald er Kenntnis über dessen Kompromitierung erhält .*
9. *Die unverzügliche vollständig Außerbetriebnahme des Zertifikats, wenn ihm vom Betreiber eine Kompromitierung des CA-Schlüssels zur Kenntnis gebracht wird.*
10. *Die sichere Verwahrung des Schlüssels liegt in der ausschließlichen Verantwortung des Signators.*
11. *Ungültige Schlüssel sind zu vernichten, dies gilt auch für auf Signaturerstellungeinheiten gespeicherte Schlüssel. Eine geeignete Vernichtung besteht auch in der Retournierung der Signaturerstellungseinheit an den Betreiber mit dem Auftrag die ungültigen Schlüssel zu vernichten.*
12. *Der Signator hat den Nutzer signierter Dateien in geeigneter Weise auf seine Pflichten im Sinne dieser Policy hinzuweisen. Er darf keine Vereinbarungen abschließen oder Erklärungen gegenüber Dritten abgeben, die im Widerspruch zu dieser Policy, den anzuwendenden Standards, den gültigen rechtlichen, insbesondere gesetzlichen Bestimmungen oder dem GLOBALTRUST® Certificate Practice Statement stehen.*
13. *Im Falle der Ausgabe qualifizierter Zertifikate für elektronische Signaturen gelten folgende Einschränkungen:*

Das Schlüsselpaar darf ausschließlich für die Erstellung elektronischer Signaturen eingesetzt werden. Alle weiteren dem Signator bekanntgegebenen Einschränkungen der Schlüsselverwaltung sind ebenfalls zu beachten.

Das Zertifikat darf nur für elektronische Signaturen verwendet werden, die mit der dem Zertifikat zugehörigen SSCD erstellt wurden.

14. *Im Falle der Kompromitierung eines CA- oder des Signator-Schlüssels hat der Signator die Anweisungen des VDA innerhalb von 48 Stunden auszuführen. Diese Zeitspanne kann verkürzt werden, wenn spezifische Sicherheitsrisken zu erwarten sind. In diesem Fall wird der Signator von der verkürzten Reaktionszeit telefonisch, per E-Mail oder auf sonstige geeignete Weise verständigt.*
15. *Der Signator akzeptiert, dass der VDA ein Zertifikat im Falle der Mißachtung der Bestimmungen dieser Policy, anderer mit dem Signator geschlossenen Vereinbarungen oder im Falle der Zertifkatsverwendung für kriminelle oder betrügerische Aktivitäten jederzeit widerrufen kann. Ein Kostenersatz für aus diesen Gründen widerrufene Zertifikat oder daraus resultierten Schäden gebührt nicht.*

Sofern der Signator über einen automatisierten Vorgang Zertifikate im Rahmen eines ihm zugewiesenen Sub-Zertifikates ausstellen kann, dürfen Einträge von E-Mail-Adressen, Domain Namen und IP-Adressen lediglich einem vorab definierten und von einer Registrierungsstelle geprüften und vereinbarten Bereich entstammen.

8. *HAFTUNG DES VDA*

Auszug aus der [GCP] GLOBALTRUST® Certificate Policy Abschnitt "9. Regelungen für sonstige finanzielle und geschäftliche Angelegenheiten":

Der VDA hat eine Haftpflichtversicherung bei einem Versicherungsunternehmen mit ausreichender Bonität, die den gesetzlichen Anforderungen entspricht abgeschlossen. Die abgeschlossene

Versicherung ist intern dokumentiert.

Der VDA stellt keine Versicherung für Endnutzer zur Verfügung, die Gewährleistung erstreckt sich auf den in die GLOBALTRUST® Certificate Policy zugesicherten Eigenschaften. Davon nicht berührt oder beschränkt sind Gewährleistung aufgrund gesetzlicher Bestimmungen.

Der VDA erfüllt alle Auflagen nach den jeweils geltenden österreichischen und europäischen Datenschutzbestimmungen. Sofern nicht anders geregelt gelten die Bestimmungen des österreichischen Datenschutzgesetzes in der geltenden Fassung auf Basis der Datenschutzrichtlinie der Europäischen Union EG/46/95 oder der ihr nachfolgenden Regelung der Europäischen Union.

Der VDA kommt allen erforderlichen Informations-, Aufklärungs- und Zustimmungspflichten der anzuwendenden Datenschutzbestimmungen nach.

Der VDA haftet
- *in seinem Verantwortungsbereich für die Einhaltung dieser Policy, insbesondere für die darin festgelegten Maßnahmen zur prompten Veröffentlichung von Sperr- und Widerrufslisten und die Einhaltung der in der Policy genannten Sperr- und Widerruf-Standards.*
- *dafür, dass Antragsteller, Signatoren und Nutzer von Signaturen, Zertifikaten und öffentlicher Schlüssel über ihre Verpflichtungen zur Beachtung der Policy in Kenntnis gesetzt wurden. Der Nachweis der Kenntnisnahme ist jedenfalls erbracht, wenn die vom VDA ausgegebenen Zertifikate eindeutige Verweise auf die Dokumentationsstellen für die anzuwendende Policy enthalten.*
- *dafür, dass die im Zertifikat enthaltenen Daten des Antragstellers zum Zeitpunkt der Ausstellung des Zertifikats überprüft wurden und keine Abweichungen der Daten gegenüber den Prüfverzeichnissen und den vorgelegten Dokumenten festgestellt wurden. Die Prüfmaßnahmen sind in dieser Policy dokumentiert, die verwendeten Prüfverzeichnisse ergeben sich aus der Art des Antragstellers und können sachlich und regional unterschiedliche Quellen umfassen. Welche Quellen für welche Antragsteller verwendet werden, wird im Detail im Rahmen der VDA-internen Prozessdokumentation geregelt.*
- *dafür, dass Hinweisen einer fehlerhaften Identitätsprüfung durch eine Registrierungsstelle oder anderen von der VDA autorisierten Personen und Stellen in jedem Fall nachgegangen wird und Zertifikate ohne ausreichende Identifikation des Signators nicht freigegeben oder bei Zweifel einer ordnungsgemäßen Identitätsprüfung unverzüglich widerrufen werden.*
- *dafür, dass ein qualifiziertes Zertifikat zu den Signaturerstellungsdaten der Signaturerstellungseinheit passt, sofern diese vom VDA erstellt wurde. Andernfalls dafür, dass der Signator zum Zeitpunkt der Ausstellung eines qualifizierten Zertifikates im Besitz des SSCD war.*

Der VDA gewährleistet Schadenersatz für nachgewiesene Schäden, die er zu verantworten hat.

9. BEDINGUNGEN BEI DER VERWENDUNG VON ZERTIFIKATEN

Auszug aus der [GCP] GLOBALTRUST® Certificate Policy Abschnitt "4.5.2 Nutzung des öffentlichen Schlüssels und des Zertifikates durch Nutzer":

Elektronische Signaturen die Zertifikate verwenden, die vom VDA herausgegeben wurden, sind nur im Rahmen dieser Policy gültig. Als elektronische Signatur in diesem Sinne sind auch die vom VDA erbrachten Zeitstempel zu verstehen. Nutzer von Zertifikaten und elektronisch signierten Informationen inklusive Zeitstempel müssen folgende Prüfschritte beachten:
- *die Überprüfung wird in dem Umfang dokumentiert als dies zur Sicherung rechtlicher Sachverhalte erforderlich ist,*

- *verbindliche Rechtsgeschäfte mit einem Wert von mehr als 100.000,- Euro erfordern eine qualifizierte Signatur*
  der Nutzer der elektronischen Signatur hat die Prüfung jedenfalls schriftlich zu dokumentieren und die Prüfung hat unabhängig voneinander durch zumindest zwei Personen zu erfolgen,
- *ist die Überprüfung eines Zertifikates zu einer elektronischen Signatur nicht möglich, liegt es in der alleinigen Verantwortung des Nutzers, ob er die Gültigkeit der Signatur anerkennt, eine Haftung des VDA oder Dritter ist ausdrücklich ausgeschlossen,*
- *Beachtung der im Zertifikat (inkl. Verweis auf die anzuwendende Certificate Policy) oder in den veröffentlichten Geschäftsbedingungen dargelegten Einschränkungen in der Nutzung bzw. Gültigkeit des Zertifikats (insbesondere Beachtung von Betragsobergrenzen, bis zu denen die Signatur gültig ausgestellt wird). Gemäß dieser eingetragenen Einschränkungen und Obergrenzen beschränkt sich auch die Haftung des VDA.*
- *Sämtliche Vorkehrungen die in Vereinbarungen oder anderswo verordnet wurden, müssen eingehalten werden.*

Der Nutzer nimmt zur Kenntnis, dass auf Grund des raschen Fortschritts der kryptographischen Technik und der raschen Steigerung der Leistungsfähigkeit von Computersystemen Signaturen und Schlüssel unsicher werden können, auch wenn zum Zeitpunkt der Ausstellung der Signatur von der Sicherheit des Signaturverfahrens ausgegangen werden konnte. Es wird daher dringend empfohlen die Website des VDA zum Thema Limits zu konsultieren, um allfällige Beschränkungen in der Gültigkeit von Signaturen und Zertifikaten erkennen zu können, die sich nicht durch Widerruf- und/oder Zertifikatsinhalt darstellen lassen. Dies gilt insbesondere bei Signaturen älteren Datums, jedenfalls bei Signaturen, die länger als 12 Monate zurück liegen.

Bestehen Zweifel an der Gültigkeit des Zertifikats, insbesondere wenn die bereitgestellten Abfragemöglichkeiten zu Sperr- und Widerrufsstatus nicht verfügbar sind, ist mit dem VDA direkt Kontakt aufzunehmen. Es werden dann geeignete Maßnahmen zur Klärung der Gültigkeit des Zertifikats gesetzt.

Der VDA registriert alle erbrachten Zeitstempel. Bestehen Zweifel an der Gültigkeit eines Zeitstempels kann der VDA feststellen, ob der Zeitstempel zu einem bestimmten Dokument tatsächlich mit seinem Service erbracht wurde. Dazu ist es ausreichend den Hash-Wert des zu prüfenden Dokuments an den VDA zu senden. Der Nutzer erhält auf diesem Weg Auskunft ob und wenn ja, wann ein Zeitstempel zu diesem Hash-Wert angefordert wurde.

10. NÜTZLICHE LINKS

1. Impressum / allgemeine rechtliche Informationen zum VDA (inkl. Missbrauchsmeldung)
   - http://www.globaltrust.eu/impressum.html
   - http://www.globaltrust.eu/abuse.html

2. öffentliche Übersicht über die anzuwendenden Policies
   - http://www.globaltrust.eu/certificate-policy.html

3. Produktübersicht (inkl. für qualifizierte Zertifikate geeignete Produkte, Zeitgenauigkeit der Zeitstempeldienste)
   - http://www.globaltrust.eu/produkte.html

4. Limits/Vorgaben bei Einsatz / Ausstellung von Zertifikaten
   - http://www.globaltrust.eu/limitation.html

5. Verzeichnisdienst
   - http://www.globaltrust.eu/directory.html

6. Sperre und Widerruf
   - http://www.globaltrust.eu/revocation.html

7. Anerkennung Root-CA durch Dritte
   - http://www.globaltrust.eu/thirdparty.html

8. Reports zur Verfügbarkeit der Zertifizierungsdienste (inklusive Zeitstempeldienste)
   - http://www.globaltrust.eu/auditreport.html

9. Online-Hilfe / Online-Support
   - http://www.globaltrust.eu/support.html

10. Zertifizierungspartner
    - http://www.globaltrust.eu/partner.html

11. Nachrichtenübersicht
    - http://www.globaltrust.eu/news.html

11. GÜLTIGKEIT DES DOKUMENTS

Stand: 25. Juni 2019
Dokumentenkurztitel: [CQINFO-WEB]
Dokumententitel: Information zum Einsatz qualifizierter Serverzertifikate GLOBALTRUST® SERVER QUALIFIED Version v1.0
OID-Nummer: 1.2.40.0.36.1.2.6.1
Herausgeber: e-commerce monitoring GmbH
Kontakt bei allgemeinen Fragen zu elektronischen Zertifikaten und elektronischer Signatur:
support@globaltrust.eu ☎ +43/01/5320944, Fax +43/01/5320974
Informationen zu GLOBALTRUST®-Zertifikatsprodukten: http://www.globaltrust.eu