

[CQINFO] Information zum Einsatz qualifizierter Zertifikate für elektronische Signaturen und elektronische Siegel gemäß Artikel 24 Abs 2 eIDAS-VO

Autor: Daniel Zens

Version 5.0 / 9. August 2022

OID-Number/Nummer: OID-Nummer: 1.2.40.0.36.1.2.5.1

Online-Publikation: <https://service.globaltrust.eu/static/general-de.pdf>

Policy Online: <https://www.globaltrust.eu/certificate-policy.html>

Contact: <https://www.globaltrust.eu/impressum.html>

Limits: <https://globaltrust.eu/limitations>

Suspension(Sperre) / Revocation(Widerruf): <https://www.globaltrust.eu/revocation.html>

© e-commerce monitoring GmbH 2022

Editorial note: This document has been provided with a 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 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.

Copyright note: The document is subject to copyright and is only made available in the context of certification services. An additional application, full or partial transmission to a third party or the publication of the document by a third party requires the prior consent of the author(s) and the CA

Urheberrechtshinweis: Das Dokument unterliegt dem Urheberrecht und wird nur im Rahmen der Zertifizierungsdienste zur Verfügung gestellt. Eine darüber hinaus gehende Verwendung, eine vollständige oder auszugsweise Übermittlung an Dritte oder die Veröffentlichung des Dokuments durch Dritte bedarf der vorherigen Zustimmung des Autors/der Autoren und des Vertrauensdiensteanbieters.

1. BEVOR SIE STARTEN

Qualifizierte Signatur ist die zentrale Technik der Informationsgesellschaft um rechtsgültige Vereinbarungen zu schließen. Gehen Sie daher mit den bereitgestellten Mitteln und Informationen besonders sorgfältig um. Ihre qualifizierte Signatur ist mit Bargeld vergleichbar, verwahren Sie alle Informationen dazu in vergleichbarer Weise.

Smartcard, Password (im Falle einer Karten-basierten qualifizierten Signatur) oder Benutzerkennung, TransportPIN, AktivierungsPIN, Mobiltelefon und Bestätigungscode (im Falle einer Cloudbasierten qualifizierten Signatur) beschreiben die Identität des Signators und erlauben dem Inhaber rechtlich verbindliche Verträge im Namen des Signators abzuschließen.

Der Signator muss daher alle zumutbaren Maßnahmen treffen, die einen Diebstahl der Informationen und Objekte und damit einen Identitätsdiebstahl verhindern oder soweit erschweren, dass der Identitätsdiebstahl unwahrscheinlich ist.

Dazu gehört insbesondere die sorgfältige Verwahrung aller physischer Komponenten, die Wahl ausreichend komplexer Passwörter und PINs, die Geheimhaltung aller persönlicher Informationen, das Vermeiden von Computerfunktionen, die vertrauliche Informationen speichern, wie Autocomplete-Funktionen, Passwortspeicherung in Textdateien, Niederschreiben von Passwörtern und Vergleichbares.

2. EINFÜHRUNG

Die vorliegende Information bezieht sich auf alle Produkte der e-commerce monitoring gmbh die zur Ausstellung qualifizierter Zertifikate für elektronische Signaturen und elektronische Siegel vorgesehen sind. Die Information wendet sich an Zertifikatswerber, Signatoren und sonstige Dritte, soweit sie ein rechtliches Interesse an den GLOBALTRUST-Produkten haben.

Qualifizierte Zertifikate werden unter den Bezeichnungen GLOBALTRUST QUALIFIED und TRUST2GO® (ohne den Zusatz „ADVANCED AATL“) angeboten. Alle anderen Dienste wie insbesondere qualifizierte Zeitstempeldienste, qualifizierte Zertifikate zur Website-Authentisierung und sonstige nicht-qualifizierte Dienste, sind nicht Gegenstand dieses Dokuments.

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

3. KONTAKTINFORMATION

Firmenname: e-commerce monitoring GmbH
Firmensitz: A-1160 Wien, Redtenbachergasse 20
Büroadresse: A-1020 Wien, Handelskai 388 Top 621 (Eingang Wehlstraße 299)
UID: ATU54992708
Handelsgericht Wien FN 224536a Gesellschaft mit beschränkter Haftung
Geschäftsführer: Dr. Hans G. Zeger

Website: <https://globaltrust.eu>

Email-Adresse: info@globaltrust.eu

Tel +43/01/5320944

Fax +43/01/5320974

Eine Bereitschaftshotline für Widerrufe wird dem Signator im Zuge der Antragsbearbeitung bekannt gegeben.

4. KONFORMITÄTSBewERTUNG DES VDA

Der VDA ist als qualifizierter Vertrauensdiensteanbieter gemäß eIDAS und dem österreichischen Vertrauensdienstgesetz in der Vertrauensliste der europäischen Union eingetragen. Der Betrieb erfolgt unter Aufsicht der Telekom-Control-Kommission/RTR GmbH. Der VDA unterliegt einer jährlichen Konformitätsbewertung durch akkreditierte Stellen. Der Betrieb der Vertrauensdienste erfolgt in ISO-27001-zertifizierten Rechenzentren.

Konformitätsbewertungsbescheinigungen und sonstige Zertifizierungen werden auf der Website des VDA veröffentlicht.

5. ANWENDBARES RECHT

Alle in diesem Dokument beschriebenen Vertrauensdienste werden gemäß österreichischem Signatur- und Vertrauensdienstegesetz¹ inkl. Signatur- und Vertrauensdiensteverordnung sowie der EU Signaturverordnung (eIDAS²) erbracht. Die technische Umsetzung erfolgt gemäß ETSI-Standard ETSI EN 319 401³, ETSI EN 319 411-1⁴, ETSI EN 319 411-2⁵, die Erweiterungen für die Ausgabe qualifizierter Zertifikate gemäß ETSI EN 319 412⁶ oder vergleichbarer gleichwertiger Standards. Weiters werden die Anforderungen ETSI TS 119 421 über Fernsignaturen und EN 419221 über den Betrieb serverbasierter Signatordienste angewendet.

Das Vertragsverhältnis zwischen VDA und Antragsteller umfasst:

- den Antrag / die Bestellung
- dieses Dokument
- die [GCP] GLOBALTRUST Certificate Policy (public, OID-Nummer: 1.2.40.0.36.1.1.8.1, <https://www.globaltrust.eu/static/globaltrust-certificate-policy.pdf>)
- das [GCPS] GLOBALTRUST Certificate Practice Statement (public, OID-Nummer: 1.2.40.0.36.1.2.3.1, <https://www.globaltrust.eu/static/globaltrust-certificate-practice-statement.pdf>)
- die [GCSP] GLOBALTRUST Certificate Security Policy (non public)

¹ Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG) BGBl. I Nr. 50/2016 siehe <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009585>

² VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, siehe <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0910>

³ EN 319 401 General Policy Requirements for Trust Service Providers http://www.etsi.org/deliver/etsi_en/319400_319499/319401/

⁴ EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1 General Requirements http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/

⁵ EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/

⁶ ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles Part 1-5, <https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx>

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

6. IDENTIFIZIERUNG DES ZERTIFIKATSWERBERS

Qualifizierte Zertifikate für elektronische Signaturen werden nur eindeutig identifizierten natürlichen Personen ausgestellt. Qualifizierte Zertifikate für elektronische Siegel werden nur an geprüfte Organisationen ausgestellt, wobei eine zeichnungsberechtigte natürliche Person als Verantwortlicher identifiziert wird.

Die Identitätsprüfung natürlicher Personen kann durch persönliche Anwesenheit und Vorlage geeigneter amtlicher Personaldokumente oder im Fernverfahren wie insbesondere Postident- oder Videoidentverfahren erfolgen.

Sofern Dritte in die Identifizierung eingebunden sind, werden die für den jeweiligen Zertifizierungsdienst gültigen Anforderungen vertraglich vollständig dem Dritten überbunden. Die Verantwortung für die ordnungsgemäße Erbringung der Zertifizierungsdienste bleibt in jedem Fall beim VDA.

7. RECHTSWIRKUNG DER VERWENDETEN SIGNATURVERFAHREN

Qualifizierte elektronische Signatur

Die Rechtswirkungen einer qualifizierten elektronischen Signatur ergeben sich aus § 4 Abs. 1 Signatur- und Vertrauensdienstegesetz (SVG)

(1) Eine qualifizierte elektronische Signatur erfüllt das rechtliche Erfordernis der Schriftlichkeit im Sinne des § 886 ABGB. Andere gesetzliche Formerfordernisse, insbesondere solche, die die Beziehung eines Notars oder eines Rechtsanwalts vorsehen, sowie vertragliche Vereinbarungen über die Form bleiben unberührt.

(2) Letztwillige Verfügungen können in elektronischer Form nicht wirksam errichtet werden. Folgende Willenserklärungen können nur dann in elektronischer Form wirksam abgefasst werden, wenn das Dokument über die Erklärung die Bestätigung eines Notars oder eines Rechtsanwalts enthält, dass er den Signator über die Rechtsfolgen seiner Signatur aufgeklärt hat:

1. Willenserklärungen des Familien- und Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind;

2. eine Bürgschaftserklärung (§ 1346 Abs. 2 ABGB), die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit abgegeben wird.

(3) Bei Rechtsgeschäften zwischen Unternehmern und Verbrauchern sind Vertragsbestimmungen, nach denen eine qualifizierte elektronische Signatur nicht das rechtliche Erfordernis der Schriftlichkeit erfüllt, für Anzeigen oder Erklärungen, die vom Verbraucher dem Unternehmer oder einem Dritten abgegeben werden, nicht verbindlich, es sei denn, der Unternehmer beweist, dass die Vertragsbestimmungen im Einzelnen ausgehandelt worden sind oder mit dem Verbraucher eine andere vergleichbar einfach verwendbare Art der elektronischen Authentifizierung vereinbart wurde.

In anderen EU-Mitgliedstaaten ist die Signatur gemäß eIDAS anzuerkennen. Die Signatur hat dort die Rechtswirkung wie eine handschriftliche Unterschrift nach jeweiligem nationalem Recht.

Qualifiziertes elektronisches Siegel

Die Rechtswirkung eines qualifizierten elektronischen Siegels ergibt sich aus Art 35 eIDAS-VO:

(1) Einem elektronischen Siegel darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in einer elektronischen Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Siegel erfüllt.

(2) Für ein qualifiziertes elektronisches Siegel gilt die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist.

(3) Ein qualifiziertes elektronisches Siegel, das auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruht, wird in allen anderen Mitgliedstaaten als qualifiziertes elektronisches Siegel anerkannt.

8. PFLICHTEN DES SIGNATORS

Die dem Signator auferlegten Verpflichtungen umfassen:

- ☒ Die Angabe vollständiger und korrekter Informationen in Übereinstimmung mit den Anforderungen dieser Policy insbesondere anlässlich des Vorgangs der Registrierung.
- ☒ Soweit zur Verwendung des privaten Schlüssels eine Mobiltelefonnummer erforderlich ist, hat der Signator eine Telefonnummer bekanntzugeben und zu verwenden, über die er allein verfügt.
- ☒ Die Prüfung der Korrektheit aller Angaben im Zertifikat auf deren Korrektheit unmittelbar nach erfolgter Zustellung
- ☒ Die Vergabe eines von der Transportsicherung abweichenden Passworts/PIN.
- ☒ Die Aufbewahrung des privaten Schlüssels in einer Hardware-Einheit, zu der der Signator den alleinigen Zugriff hat
- ☒ Der Signator hat alle ihm übergebenen Komponenten, Informationen und Verfahren zur Verwendung des privaten Schlüssels unter seiner alleinigen Kontrolle zu behalten und vor dem Zugriff durch unbefugte Dritte zu schützen.
- ☒ Die Anwendung entsprechender Vorsicht, um den unbefugten Gebrauch des privaten Schlüssels zu verhindern.
- ☒ Die unverzügliche vollständige Außerbetriebnahme des Schlüssels, sobald er Kenntnis über dessen Kompromittierung erhält.
- ☒ Ungültige Schlüssel sind zu vernichten, dies gilt auch für auf Signaturerstellungseinheiten gespeicherte Schlüssel. Eine geeignete Vernichtung besteht auch in der Retournierung der Signaturerstellungseinheit an den Betreiber mit dem Auftrag die ungültigen Schlüssel zu vernichten.
- ☒ 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 QSCD erstellt wurden.

Der Signator benachrichtigt den Betreiber unverzüglich über folgende Vorfälle:

- ☒ Die Transportsicherung (zB der TransportPIN) der Signaturerstellungseinheit nicht verwendbar ist
- ☒ Der private Schlüssel oder dessen Aktivierungsdaten verloren gingen
- ☒ Das Mobiltelefon verloren oder gestohlen wird oder sonst abhanden kommt, sofern ein Mobiltelefon als Komponente zur Signaturauslösung verwendet wird
- ☒ Der private Schlüssel des Signators oder dessen Aktivierungsdaten möglicherweise kompromittiert wurden
- ☒ Die alleinige Kontrolle über den privaten Schlüssel ging verloren
- ☒ Die im Zertifikat beinhalteten Informationen inkorrekt sind oder sich geändert haben

Der Signator nimmt zur Kenntnis dass:

- ☒ Im Fall des Verlustes seines Passwortes keine Möglichkeit der Rekonstruktion auf Seiten des Betreibers bestehen und daher eine Neuausstellung des privaten Schlüssels und eines Zertifikates erforderlich sind und die Kosten in diesem Fall vom Signator zu tragen sind
- ☒ Dass fünf Falscheingaben des Passwortes zu einer Sperre seines Accounts führen, die nur aufgehoben wird, wenn der Signator glaubhaft machen kann, dass er die Falscheingaben persönlich verursacht hat

9. SIGNATURPRODUKTE UND –VERFAHREN

Zur Erstellung und Prüfung von qualifizierten elektronischen Signaturen und Siegeln empfiehlt der VDA entweder spezielle Produkte und Verfahren oder stellt diese zur Verfügung stellen. Der Signator ist verpflichtet, ausschließlich empfohlene oder bereitgestellte Produkte und Verfahren unter Beachtung etwaiger Einsatzbedingungen zu verwenden.

Die Aufzählung hat demonstrativen Charakter, weitere Produkte werden laufend auf der Website des VDA (⇒ <http://globaltrust.eu/produkte.html>) veröffentlicht.

Geeignete Signaturerstellungseinheiten für die qualifizierte Mobilsignatur TRUST2GO®

Typ: remote-QSCD-Gesamtsystem

Bestätigungsstelle: A-SIT (AT)

Bestätigung: AIT VIG A-SIT-VIG-20-105 (<https://www.a-sit.at/downloads/1909>)

Ausgestellt: 12.07.2022

Zertifizierung: § 7 ABS. 1 SVG IVM ART. 30 ABS. 3 LIT. B EIDAS-VO

Signatursuite:

- RSASSA-PKCS1-v1_5 nach PKCS#1 v2.2 (RFC 8017) mit Schlüssellängen von 2048, 3072 oder 4096 Bit,
- RSASSA-PSS nach PKCS#1 v2.2 (RFC 8017) mit Schlüssellängen von 2048, 3072 oder 4096 Bit und
- ECDSA nach FIPS PUB 186-4 und den NIST29-Kurven P-256, P-384 oder P-521 mit Länge der Parameter p, q von 256, 384 oder 512 Bit,

Hashfunktionen:

- SHA31-256, SHA-384 und SHA-512 nach ISO32/IEC33 10118-3 bzw. FIPS 180-4

Geeignete Signaturerstellungseinheiten für qualifizierte Signaturen:

Produkt: Atos CardOS v5.3

Typ: Smartcard

Bestätigungsstelle: A-SIT (AT)

Bestätigung: A-SIT-1.108 Sichere Signaturerstellungseinheit CardOS V5.3 QES, V1.0

(http://www.a-sit.at/de/bestaetigungsstelle/bescheinigungen_sigg/veroeffentlichungen.php)

Ausgestellt: 08.08.2014

Zertifizierung: Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5

Signatursuite:

- ECDSA12 nach ANSI X 9.62 bzw. ISO/IEC 15946-2 mit Längen der Parameter p, q von 256 oder 384 Bit. Es werden die Kurven P-256 bzw. P-384 nach FIPS PUB 186-4 sowie brainpoolP256r1 bzw. brainpoolP384r1 nach RFC 5639 unterstützt.

Hashfunktion: SHA-2

Geeignete Kartenlesegeräte (Cardreader)

Eine Bestätigung ist für den Betrieb eines Kartenlesegeräts nach den österreichischen Signaturbestimmungen nicht zwingend erforderlich, kann aber bei der Auswahl zuverlässiger Geräte hilfreich sein. Auf Anfrage testet GLOBALTRUST gewünschte Kartenlesegeräte und stellt eine Bestätigung aus, unter welchen Bedingungen sie für GLOBALTRUST-Smartcards geeignet sind. Grundsätzlich sind alle Cardreader, die ISO 7816 unterstützen für die Verwendung von GLOBALTRUST-Smartcards geeignet.

Geeignete Signaturerstellungssoftware

Die Spezifikation eines Formats für zu signierende Daten muss allgemein verfügbar sein und sicherstellen, dass die signierten Daten sowohl bei der Signaturerstellung als auch bei der Signaturprüfung zweifelsfrei und mit gleichem Ergebnis darstellbar sind. Können in einem Format dynamische Änderungen kodiert werden, so dürfen jene Elemente, die dynamische Änderungen hervorrufen können, nicht verwendet werden.

Produkt: e-Sign Agent

Dokumentenformate: pdf

Signaturformate: Adobe (pdf)

Anmerkung: Kostenlose Software direkt von GLOBALTRUST

Download Windows: <https://service.globaltrust.eu/static/eSignAgent.msi>

Dokumentation: <https://service.globaltrust.eu/static/trust2go-benutzer.pdf>

10. WIDERRUF UND SUSPENSION, MISSBRAUCHSMELDUNG

Der VDA stellt folgende Möglichkeiten zur Verfügung:

(a.) Suspension/Sperre

Die Gültigkeit eines Zertifikates wird vorläufig ausgesetzt, kann manuell oder automatisiert ausgelöst werden und ist maximal für 10 Tage gültig

(b.) Revocation/Widerruf

Führt zum vorzeitigen ungültig Erklären eines Zertifikates. Re-Aktivierung ist ausgeschlossen.

Die Tatsache der Sperre oder des Widerrufs eines Zertifikates ist öffentlich verfügbar. Die Nutzung des Verzeichnis- und Widerrufsdienstes ist kostenlos und anonym möglich.

Elektronische Unterschriften, die vor Widerruf oder Sperre ausgestellt wurden, behalten ihre Gültigkeit.

Anträge auf Widerruf sollten so rasch als möglich via <https://www.globaltrust.eu/revocation.html> übermittelt werden. Alternativ können Widerrufe auch per email an revocation@globaltrust.eu oder telefonisch beantragt werden. In jedem Fall ist eine ausreichende Berechtigung zum Widerruf nachzuweisen, zum Beispiel durch online-Authentisierung.

Gründe für den Widerruf sind insbesondere:

- Verlangen des Antragstellers
- Der ursprüngliche Zertifikatsantrag war nicht hinreichend autorisiert
- Privater Schlüssel wurde kompromittiert wurde oder entspricht nicht mehr den aktuellen technischen Anforderungen
- Komponenten, Informationen und Verfahren zur Verwendung des privaten Schlüssels wurden kompromittiert
- Missbräuchliche Verwendung des Zertifikats
- Signator ist nicht länger rechtlich befugt, eine im Zertifikat eingetragene Bezeichnung zu verwenden
- Der Betreiber erhält Kenntnis von einer signifikanten Änderung bezüglich der im Zertifikat eingetragenen Informationen.
- Es werden Gründe bekannt, die den technischen Inhalt oder das Format des Zertifikates zu einem inakzeptablen Sicherheitsrisiko machen.

(c.) Deaktivierung

Auf Antrag des Signators oder durch den Betreiber kann anstelle einer Sperre oder eines Widerrufs auch nur eine Deaktivierung des 2. Authentisierungsverfahrens vorgenommen werden, wenn der private Schlüssel nicht kompromittiert ist, aber sonstige Bedenken im Signaturablauf bestehen (Verlust des Mobiltelefons, ...).

(d.) Meldung von Missbrauch

Bei zertifikatsbezogenen Problemen, zum Beispiel bei Verdacht auf Missbrauch, kann sich jeder Beteiligte an abuse@globaltrust.eu oder telefonisch mit dem Betreiber in Verbindung setzen.

11. HAFTUNG DES VDA

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

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 Signaturerstellungseinheiten 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.

12. NÜTZLICHE LINKS

1. Impressum

- <https://globaltrust.eu/impressum>

2. öffentliche Übersicht über die anzuwendenden Policies, Veröffentlichung anwendbare Stamm- und Zwischenzertifikate, Konformitätsbewertungen

- <https://globaltrust.eu/certificate-policy/>

3. Geeignete Signaturerstellungsprodukte (inkl. für qualifizierte Zertifikate geeignete Produkte)

- <https://globaltrust.eu/geeignete-signaturerstellungseinheiten/>

4. Limits/Vorgaben bei Einsatz / Ausstellung von Zertifikaten

- <https://globaltrust.eu/limitation>

5. Verzeichnisdienst

- <http://www.globaltrust.eu/directory.html>

6. Sperre und Widerruf

- <https://www.globaltrust.eu/revocation.html>