[CQINFO] Information zum Einsatz qualifizierter Zertifikate GLOBALTRUST® qualified Version: v1.0

Inhalt

cn=Mag. Dr. Hans G. Zeger, Geschäftsführung, c=AT, l=Wien, st=Wien, o=e-commerce monitoring GmbH, email=hans.zeger@e-monitoring.at

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.pdf abgerufen werden und ist mit einer fortgeschrittenen elektronischen Signatur (iS § 2 Abs 3 SigG) versehen.

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

Die Information entspricht den Bestimmungen gemäß § 20 SigG (StF BGBl. I Nr. 137/2000 idgF).

2. VERWENDETE BEGRIFFE

Im Zusammenhang mit der vorliegenden Information werden die Begriffe gemäß SigG § 2 verwendet:

1. elektronische Signatur: elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung dienen;

2. Signator: eine Person oder eine sonstige rechtsfähige Einrichtung, der Signaturerstellungsdaten und Signaturprüfdaten zugeordnet sind und die im eigenen oder fremden Namen eine elektronische Signatur erstellt;

3. fortgeschrittene elektronische Signatur: eine elektronische Signatur, die

a) ausschließlich dem Signator zugeordnet ist,

b) die Identifizierung des Signators ermöglicht,

c) mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann, sowie

d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass jede nachträgliche Veränderung der Daten festgestellt werden kann;

3a. qualifizierte elektronische Signatur: eine fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit erstellt wird;

4. Signaturerstellungsdaten: einmalige Daten wie Codes oder private Signaturschlüssel, die vom Signator zur Erstellung einer elektronischen Signatur verwendet werden;

5. sichere Signaturerstellungseinheit: eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturerstellungsdaten verwendet wird und die den Sicherheitsanforderungen dieses Bundesgesetzes sowie der auf seiner Grundlage erlassenen Verordnungen entspricht;

6. Signaturprüfdaten: Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden;

7. Signaturprüfeinheit: eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturprüfdaten verwendet wird;

8. Zertifikat: eine elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird;

9. qualifiziertes Zertifikat: ein Zertifikat einer natürlichen Person, das die Angaben des § 5 enthält und von einem den Anforderungen des § 7 entsprechenden ZDA ausgestellt wird;

10. ZDA: eine natürliche oder juristische Person oder eine sonstige rechtsfähige Einrichtung, die Zertifikate ausstellt oder andere Signatur- und Zertifizierungsdienste erbringt;

11. Signatur- und Zertifizierungsdienste: die Bereitstellung von Signaturprodukten und -verfahren, die Ausstellung, Erneuerung und Verwaltung von Zertifikaten, Verzeichnis-, Widerrufs-, Registrierungs-

und Zeitstempeldienste sowie Rechner- und Beratungsdienste im Zusammenhang mit elektronischen Signaturen;
12. qualifizierter Zeitstempel: eine elektronische Bescheinigung, dass bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen sind, die den Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage erlassenen Verordnungen entspricht;
13. Signaturprodukt: Hard- oder Software bzw. deren spezifische Komponenten, die für die Erstellung und Überprüfung elektronischer Signaturen oder von einem ZDA für die Bereitstellung von Signatur- oder Zertifizierungsdiensten verwendet werden;
14. Kompromittierung: die Beeinträchtigung von Sicherheitsmaßnahmen oder Sicherheitstechnik, sodaß das vom ZDA zugrundegelegte Sicherheitsniveau nicht eingehalten ist;
15. Signaturrichtlinie: Richtlinie des Europäischen Parlamentes und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L Nr. 13 vom 19. Jänner 2000, S 12.

3. BETRIEBSVORAUSSETZUNGEN DES ZDA

Die Zertifizierungstätigkeit des ZDA unterliegt der Aufsicht der Telekom-Control-Kommission (TKK) bzw. Rundfunk und 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 ZDA wurde mit 29. Juni 2015 gemäß Bescheid A 4/2014-36 akkreditiert.

Angaben zum ZDA und seiner Zertifizierungsdienste sind bei der Aufsichtsstelle unter https://www.signatur.rtr.at/de/elsi/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 ZDA entnommen werden (http://www.e-monitoring.at/static/agb.pdf).

4. SICHERHEITSKONZEPT

Das Sicherheitskonzept des ZDA 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 ZDA 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 ZDA-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 ZDA 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 ZDAs 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 ZDA 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 ZDA.

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 ZDA 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 ZDA 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 ZDA relevante Vereinbarungen geschlossen hat, informiert. Alle beim ZDA 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.

5. RECHTSWIRKUNG DER VERWENDETEN SIGNATURVERFAHREN

Der ZDA bietet elektronische Signaturen in allen gemäß SigG § 2 Z 1,2,3 und 3a definierten Varianten an. In allen Fällen werden technische Verfahren verwendet, die den Vorgaben der Verordnung des Bundeskanzlers über elektronische Signaturen (SigV 2008, BGBl. II Nr. 3/2008 StF idgF) entsprechen.

Auszug aus SigG § 3 und 4

Allgemeine Rechtswirkungen

§ 3. (1) Im Rechts- und Geschäftsverkehr können Signaturverfahren mit unterschiedlichen Sicherheitsstufen und unterschiedlichen Zertifikatsklassen verwendet werden.

(2) Die rechtliche Wirksamkeit einer elektronischen Signatur und deren Verwendung als Beweismittel können nicht allein deshalb ausgeschlossen werden, weil die elektronische Signatur nur in elektronischer Form vorliegt, weil sie nicht auf einem qualifizierten Zertifikat oder nicht auf einem von einem akkreditierten ZDA ausgestellten qualifizierten Zertifikat beruht oder weil sie nicht unter Verwendung von technischen Komponenten und Verfahren im Sinne des § 18 erstellt wurde.

Besondere Rechtswirkungen

§ 4. (1) Eine qualifizierte elektronische Signatur erfüllt das rechtliche Erfordernis einer eigenhändigen Unterschrift, insbesondere der Schriftlichkeit im Sinne des § 886 ABGB, sofern durch Gesetz oder Parteienvereinbarung nicht anderes bestimmt ist.

(2) Eine qualifizierte elektronische Signatur entfaltet in folgenden Fällen nicht die Rechtswirkungen der Schriftlichkeit im Sinne des § 886 ABGB:

1. Bei Rechtsgeschäften des Familien- und Erbrechts, die an die Schrifttform oder ein strengeres Formerfordernis gebunden sind, es sei denn, die über das Rechtsgeschäft errichtete Urkunde enthält die Erklärung eines Rechtsanwalts oder eines Notars, dass er den Signator über die Rechtsfolgen seiner Signatur aufgeklärt hat; letztwillige Anordnungen können in elektronischer Form jedoch nicht wirksam errichtet werden.

2. Bei anderen Willenserklärungen oder Rechtsgeschäften, die zu ihrer Wirksamkeit an die Form einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts gebunden sind, soweit die öffentliche Beglaubigung, die gerichtliche oder notarielle Beurkundung oder der Notariatsakt in elektronischer Form nicht wirksam zustande kommt.

3. Bei Willenserklärungen, Rechtsgeschäften oder Eingaben, die zu ihrer Eintragung in das Grundbuch, das Firmenbuch oder ein anderes öffentliches Register einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts bedürfen, soweit die öffentliche Beglaubigung, die gerichtliche oder notarielle Beurkundung oder der Notariatsakt in elektronischer Form nicht wirksam zustande kommt.

4. Bei einer Bürgschaftserklärung (§ 1346 Abs. 2 ABGB), die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit abgegeben wird, es sei denn, diese enthält die Erklärung eines Rechtsanwalts oder eines Notars, dass er den Bürgen über die Rechtsfolgen seiner Verpflichtungserklärung aufgeklärt hat.

(3) Die Bestimmung des § 294 ZPO über die Vermutung der Echtheit des Inhalts einer unterschriebenen Privaturkunde ist auf elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, anzuwenden.

(4) Die Rechtswirkungen der Abs. 1 und 3 treten nicht ein, wenn nachgewiesen wird, daß die Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen

Verordnungen nicht eingehalten oder die zur Einhaltung dieser Sicherheitsanforderungen getroffenen Vorkehrungen kompromittiert wurden.

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.

6. PFLICHTEN DES SIGNATORS

Auszug aus der [GCP] GLOBALTRUST® Certificate Policy Abschnitt "4.5.1 Nutzung des privaten Schlüssels und des Zertifikates durch den Signator":

Dem Antragsteller werden alle Vertragsbedingungen auf der Website des ZDA zugänglich gemacht. Gleichzeitig mit dem Absenden des Bestellformulars bestätigt er deren Kenntnisnahme und Akzeptanz.
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.*
* *Die Prüfung der Korrektheit aller Angaben im Zertifikat auf deren Korrektheit unmittelbar nach erfolgter Zustellung.*
* *Die Aufbewahrung des privaten Schlüssels in einer Hardware-Einheit, zu der der Signator den alleinigen Zugriff hat (verschlüsseltes Abspeichern des privaten Schlüssels mittels Passwort, Signatur-PIN bzw. Passphrase, spezielle Signaturerstellungseinheiten, die das Auslesen des privaten Schlüssels verhindern oder wesentlich erschweren).*
* *Ungeeignete Schlüsselverfahren werden auf der Website des Betreibers bekannt gemacht und dürfen nicht verwendet werden.*
* *Die Anwendung entsprechender Vorsicht, um den unbefugten Gebrauch des privaten Schlüssels zu verhindern.*
* *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.*
* *Die unverzügliche vollständig Außerbetriebnahme des Schlüssels, sobald er Kenntnis über dessen Kompromitierung erhält.*
* *Die unverzügliche vollständig Außerbetriebnahme des Zertifikate, wenn ihm vom Betreiber eine Kompromitierung des CA-Schlüssels zur Kenntnis gebracht wird.*
* *Die sichere Verwahrung des Schlüssels liegt in der ausschließlichen Verantwortung des Signators.*
* *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.*
* *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 zur [GCP] GLOBALTRUST® Certificate Policy, den anzuwendenden Standards, den gültigen rechtlichen, insbesondere gesetzlichen Bestimmungen oder dem [GCPS] GLOBALTRUST® Certificate Practice Statement stehen.

* *Im Falle der Ausgabe qualifizierter Zertifikate gelten folgende Einschränkungen:*
  Das Schlüsselpaar darf ausschließlich für die Erstellung elektronischer Signaturen eingesetzt werden. Alle weiteren dem Signator bekanntgegebenen Einschränkrungen der Schlüsselverwaltung sind ebenfalls zu beachten.
  Das Zertifikat darf nur für elektronische Signaturen verwendet werden, die mit der dem Zertifikat zugehörigen SSCD erstellt wurden.
* *Im Falle der Kompromitierung eines CA- oder des Signator-Schlüssels hat der Signator die Anweisungen des ZDA 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.*
* *Der Signator akzeptiert, dass der ZDA 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.*

7. HAFTUNG DES ZDA

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

Der ZDA hat eine Haftpflichtversicherung bei einem Versicherungsunternehmen mit ausreichender Bonität, die den gesetzlichen Anforderungen entspricht. Der ZDA stellt keine Versicherung für Endnutzer zur Verfügung, die Gewährleistung erstreckt sich auf den in der [GCP] GLOBALTRUST® Certificate Policy zugesicherten Eigenschaften. Davon nicht berührt oder beschränkt sind Gewährleistung aufgrund gesetzlicher Bestimmungen.

Der ZDA 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 ZDA garantiert die Erfüllung der Auskunftspflichten gegenüber dem ⇨ Betroffenen und im Rahmen der gesetzlichen Verpflichtungen gegenüber Behörden und Dritten, sofern diese ein berechtigtes rechtliches Interesse nachweisen.

Der ZDA haftet

- *in seinem Verantwortungsbereich für die Einhaltung der [GCP] GLOBALTRUST® Certificate 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 ZDA 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 der [GCP] GLOBALTRUST® Certificate Policy dokumentiert.*
- *dafür, dass Hinweisen einer fehlerhaften Identitätsprüfung durch eine Registrierungsstelle oder anderen von der ZDA 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 qualifziertes Zertifikat zu den Signaturerstellungsdaten der Signaturerstellungseinheit passt, sofern diese vom ZDA erstellt wurde. Andernfalls dafür, dass der Signator zum Zeitpunkt der Ausstellung eines qualifizierten Zertifikates im Besitz des SSCD war.*

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

8. 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 ZDA herausgegeben wurden, sind nur im Rahmen dieser Policy gültig, daher müssen Nutzer von Zertifikaten und elektronisch signierten Informationen 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 ein qualifiziertes Zertifikat, 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 ZDA 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 ZDA.*
- *Sämtliche Vorkehrungen die in Vereinbarungen oder anderswo verordnet wurden, müssen eingehalten werden.*

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

9. NÜTZLICHE LINKS

1. Impressum / allgemeine rechtliche Informationen zum ZDA (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

10. GÜLTIGKEIT DES DOKUMENTS

Stand: 29. Juni 2015 [Datum der Akkreditierung: 29. Juni 2015]
Dokumentenkurztitel: [CQINFO]
Dokumententitel: Information zum Einsatz qualifizierter Zertifikate GLOBALTRUST® qualified
Version: v1.0
OID-Nummer: 1.2.40.0.36.1.2.5.1
Herausgeber: e-commerce monitoring GmbH, 1160 Wien, Redtenbacherg. 20
UID: ATU54992708
Firmenbuchgericht: Handelsgericht Wien FN 224536 a
Kontakt bei allgemeinen Fragen zu elektronischen Zertifikaten und elektronischer Signatur:
upport@globaltrust.eu ☎ +43/01/5320944, Fax +43/01/5320974
Geschäfts- und Besuchsadresse: A-1010 Wien, Vorlaufstraße 5/6
Informationen zu GLOBALTRUST®-Zertifikatsprodukten: http://www.globaltrust.eu