öffentlich

GLOBALTRUST® Certificate Policy

[GCP - ZDA Policy]

Autor: Hans G. Zeger

Version 1.8b / 1. Februar 2015

OID-Nummer: 1.2.40.0.36.1.1.8.1
Gültigkeitshistorie OID-Nummer: 1.2.40.0.36.1.1.8.99

Policy Online: http://www.globaltrust.eu/certificate-policy.html

Kontakt-Daten: http://www.globaltrust.eu/impressum.html

Sperre oder Widerruf: http://www.globaltrust.eu/revocation.html

Redaktioneller Hinweis: Das vorliegende Dokument ist mit einer fortgeschrittenen 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.

Mag. Dr. Hans G. Zeger,
Abwicklung A-CERT-Service
2015.04.12 15:37:30 +02'00'

INHALT

ANHANG

1. EINLEITUNG / INTRODUCTION

Management-Statement

Zertifizierungsdienste, insbesondere digitale elektronische Signaturen und digitale Zertifikate werden als Schlüsseltechnologien zur Herstellung vertrauenswürdiger globaler Geschäftsprozesse angesehen. Der sicheren Verwaltung vertraulicher Zertifizierungsdaten, die langfristige Nachvollziehbarkeit der Zertifizierungsvorgänge und die Überprüfbarkeit der Zertifizierungsdienste hat damit zentrale Bedeutung in der Geschäftstätigkeit des Zertifizierungsdienstanbieters (ZDA).

Als Informationssicherheit wird neben der Sicherheit der IT-Infrastruktur auch die sichere Verwendung aller zu den Zertifizierungsdiensten relevanten Informationen außerhalb der IT verstanden.

Grundlagen der Informationssicherheit sind die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit.

In diesem Sinn kommt der Bereitstellung geeigneter Techniken und Hilfsmittel zentrale Bedeutung zu. Die Erbringung von Zertifizierungsdiensten wird als zentrale Aufgabe des Betreibers angesehen. Alle Vorgaben oder Änderungen der Zertifizierungsdienste inklusive Änderungen in den die Zertifizierungsdienste betreffenden Policies erfolgen auf Grund von Anweisungen der Geschäftsführung unter besonderer Bedachtnahme strenger Informationssicherheitsmaßstäbe.

Grundlage dieser strengen Informationssicherheitsmaßstäbe ist, dass Zertifizierungsdienste ausschließlich auf Basis definierter Geschäftsmodelle erbracht werden.

Bei der Implementierung neuer Geschäftsprozesse bzw. der Anpassung bestehender Geschäftsprozesse werden deren Auswirkungen auf das bestehende Informationssicherheitskonzept vorab geprüft und die Implementierung so konzipiert, dass das bestehende Sicherheitskonzept (GLOBALTRUST® Certificate Security Policy (OID-Nummer: 1.2.40.0.36.1.2.2.1)[1]) eingehalten wird. Dieses Dokument ist nicht öffentlich verfügbar. Das Sicherheitskonzept beschreibt das Informations-Sicherheits-Management-System (ISMS) für alle Zertifizierungsdienste für die der Betreiber verantwortlich zeichnet (entweder als ZDA oder als Dienstleister für ZDAs).

Der Betrieb und die Anpassung bestehender und die Implementierung neuer Geschäftsprozesse erfolgt nach dem PDCA[2]-Modell, wobei die PDCA-Zyklen sich nach sachlich sinnvollen Zeitperioden orientieren. Unabhängig vom vordefinierten Standard-PDCA-Zyklus können unvorhergesehene Ereignisse (insbesondere bei Änderung wesentlicher technischer, personeller, wirtschaftlicher oder rechtlicher Rahmenbedingungen) zusätzliche oder verkürzte PDCA-Zyklen erfordern. Teilprozesse werden, soweit sachlich anwendbar, ebenfalls als Teil-PDCA-Zyklen organisiert.

---

1 Die GLOBALTRUST® Certificate Security Policy ist nicht öffentlich verfügbar.

2 PDCA = Plan (Planungsphase), Do (Entwicklungs-, Umsetzungs- oder Implementierungsphase), Act (Betriebsphase), Check (Überprüfungsphase mit dem Ziel Verbesserungspotentiale zu identifizieren)

Informationssicherheit wird weiters durch ein klares personelles Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) organisatorisch gesichert, wobei dem Zertifizierungs-Ausschuss eine zentrale Rolle in der Planung der Zertifizierungsdienste zukommt. Im Zertifzierungs-Ausschuss sind alle für die Zertifizierung relevanten Funktionen repräsentiert.

Im Zertifizierungs-Ausschuss erfolgt unter Berücksichtigung der rechtlichen Vorgaben und der wirtschaftlichen Ressourcen die ausreichende finanzielle Dotierung von Informationssicherheitsmaßnahmen.

Im Sinne der Motivation aller Mitarbeiter und um eine optimale Vorbildfunktion zu erreichen, verpflichten sich Geschäftsführung und die Mitglieder des Zertifizierungs-Ausschuss selbst zur regelmäßigen Teilnahme an Schulungsveranstaltungen und der genauen Beachtung aller Sicherheitsregeln. Alle Mitarbeiter werden zur Einhaltung des Datengeheimnisses verpflichtet.

Zur Aufrechterhaltung der Informationssicherheit führen alle zuständigen Funktionsträger regelmäßig Prüfungen der Informationssicherheitsprozesse durch, wobei internen und externen Audits eine wichtige Rolle zukommt. Erkannte Schwachstellen führen ausnahmslos zu Konsequenzen, Schwachstellen und Konsequenzen werden dokumentiert. Die Geschäftsführung verpflichtet sich zur regelmäßigen Evaluation der Eignung, Aktualität und Angemessenheit der Sicherheitsziele und -leitlinien.

Im Rahmen des Rollenkonzepts (⇨ GLOBALTRUST® Certificate Security Policy) wird sowohl der Informationsfluss, die erforderlichen Berichte an die Leitungsebene und die erforderlichen Dokumentationen festgelegt. Die interne Dokumentation der Zertifizierungsdienste erfolgt mittels eines internen Content Management Systems, die Dokumente sind allen zuständigen Personen zugänglich. Für Notfälle werden jene Dokumentationsteile in gedruckter Form bereit gehalten, die für die Wiederherstellung der IT-Infrastruktur unerlässlich sind. Durch ein komplexes und laufend erweitertes Berechtigungs- und Schlagwortkonzept können Dokumente flexibel bestimmten Themen und Aufgaben bzw. bestimmten Nutzungsgruppen zugeordnet werden (z.B. technische Dokumente, Anwendungsunterlagen, Vertrags- und Zertifizierungsunterlagen, Weisungen, Berichte usw.).

Der ZDA führt die erforderlichen Audits durch, um die Konformität seiner Zertifizierungsdienste mit den unter ⇨ 8. Prüfung der Konformität und andere Beurteilungen / COMPLIANCE AUDIT AND OTHER ASSESSMENTS (p95) gelisteten Dokumenten sicher zu stellen. Soweit erforderlich werden die Auditreports veröffentlicht bzw. zur Verfügung gestellt.

1.1 Übersicht / Overview

Der Betreiber bietet sämtliche Zertifizierungsdienste im Sinne dieses Dokuments an.

Die GLOBALTRUST® Certificate Policy (GCP) regelt alle Anforderungen der Zertifizierungsdienste des Betreibers. Soweit für einzelne Produkte Regelungen im jeweils anzuwendenden Practice Statement (insbesoondere dem GLOBALTRUST® Certificate Practice Statement) vorgenommen werden, sind diese als Ergänzungen im Rahmen dieser Policy zu verstehen.

Die in diesem Dokument beschriebene GLOBALTRUST® Certificate Policy wird im Folgenden kurz als "Policy" bezeichnet. Diese Policy ist als Grundlage zu verstehen, innerhalb derer die Zertifizierungsdienste erbracht werden. Zusätzliche Beschränkungen in der Anwendbarkeit der Policy auf bestimmte Zertifizierungsfälle und Signaturvorgänge ist durch Vereinbarungen möglich. Dies betrifft jedoch in keinem Fall eine Änderung gesetzlicher (insbesondere [SigRL], [SigG], [SigV], ...) oder technischer (insbesondere [CWA-14167-1], [ETSI TS 101 456] inkl. Nachfolger: [ETSI EN 319 411-2], [ETSI TS 102 042] inkl. Nachfolger [ETSI EN 319 411-3], ...) Grundlagen. Die AGB's des ZDAs oder zusätzliche Vereinbarungen der Partnerunternehmen können jedoch nicht die vorliegende Policy ganz oder teilweise außer Kraft setzen.

Alle für die Erbringung der Zertifizierungsdienste notwendigen Prozesse sind vom Betreiber intern dokumentiert.

Die GLOBALTRUST® Certificate Policy, das GLOBALTRUST® Certificate Practice Statement und die GLOBALTRUST® Certificate Security Policy sind gemeinsam Grundlage des der Aufsichtsbehörde zur Genehmigung vorgelegten Betriebskonzepts. Die Umsetzung der technischen Abläufe des Betriebskonzepts ist durch das interne Dokumentationssystem sichergestellt.

Änderungen oder Neuentwicklungen von Geschäftsprozessen erfolgen gemäß schriftlicher Dokumentation und enthält jedenfalls folgende Angaben: Beschreibung der geplanten Änderungen oder Neuentwicklungen, Initialisierungsdatum, beteiligte Mitarbeiter, voraussichtliche Dauer, Zwischenergebnisse und Angaben zum Fertigstellungstermin, eine laufende Anpassung des Fertigstellungsstatus inkl. Angaben der offenen Arbeiten und der verantwortlichen Person für die Abnahme, Dokumentation des fertig gestellten Geschäftsprozesses.

Änderungen oder Neuentwicklungen sind von verantwortlicher Stelle gemäß ⇨ GLOBALTRUST® Certificate Security Policy zu veranlassen. Im Zweifel ist die Genehmigung direkt durch die Geschäftsführung erforderlich.

1.2 Dokumenttitel und -identifikation / Document name and identification

Dokumententitel: "GLOBALTRUST® Certificate Policy" (GCP)

Diese für GLOBALTRUST® gültige Policy hat die OID-Nummer: 1.2.40.0.36.1.1.8.1).

Das vorliegende Dokument tritt mit dem Tag der Veröffentlichung auf der Website des Betreibers in Kraft. Sofern nicht anders vermerkt endet die Gültigkeit der früheren Version des Dokuments mit Beginn der Gültigkeit der neuen Version.

Das vorliegende Dokument wurde konform [RFC3647] erstellt.

Fremd-Dokumente werden in eckigen Klammern [] zitiert und finden sich im ⇨ Anhang A: 1 Bibliographie (p109) mit den bibliographischen Angaben gelistet. Sie werden mit Stand 1. Februar 2015 zitiert, aber in der jeweils gültigen Fassung bzw. zutreffenden Folgestandards angewandt.

Die Gültigkeit von Weblinks bezieht sich, sofern nicht ausdrücklich anders vermerkt auf den Redaktionsschluss dieses Dokuments.

Die vorliegende Certificate Policy enthält alle Regeln für die Ausstellung und Verwendung von Zertifikaten für einfache, fortgeschrittene und qualifizierte Signaturen.

Änderungen auf Grund gesetzlicher Änderungen werden zum Zeitpunkt des Inkrafttretens der gesetzlichen Bestimmungen wirksam, sonstige Änderungen nach Verlautbarung auf der Website von GLOBALTRUST®.

Sofern gesetzliche Änderungen oder Änderungen jener Dokumente und Standards, für die die Zertifizierungsdienste Konformität beanspruchen, eine Änderung der GLOBALTRUST® Certificate Policy, des GLOBALTRUST® Certificate Practice Statements oder der GLOBALTRUST® Certificate Security Policy erfordern, erfolgt die Anpassung so zeitgerecht, dass die geänderten Anforderungen erfüllt werden können.

Änderungshistorie

Die Vorversionen 1.0 bis 1.4 waren interne Fassungen und traten nie in Kraft.

Version 1.5 Stammfassung 10. August 2006

Version 1.6 Änderungen I 12. April 2007
- Erläuterungen zur Marke GLOBALTRUST®
- OID-Nummer für englische Übersetzung der Policy vergeben
- Konformität mit [ETSI TS 102 042] hergestellt
- Neu hinzugefügt Schlüsselverwaltung Signator
- Diverse redaktionelle Korrektur von Schreib- und Formulierungsfehlern

Version 1.7 Änderungen II 1. April 2014
- Neustrukturierung des Dokuments gemäß [RFC3647]
- Darstellung der detaillierten Zertifizierungsabläufe in ⇨ GLOBALTRUST® Certificate Practice Statement
- Erweiterung für die Ausstellung qualifizierter Zertifikate für fortgeschrittene und qualifizierte Signaturen
- Betrieb des Zeitstempeldienstes definiert
- Betrieb mobiler Zertifizierungsdienste definiert
- Änderung des Zertifizierungsdienstanbieters
- Ergänzungen und Korrekturen in der Literaturliste
- Regelung zur Kennzeichnung von einfachen Zertifikaten ab 1.7.2014 (⇨ GLOBALTRUST® Certificate Practice Statement).
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern

Version 1.8 Änderungen III 1. Juni 2014
- Antragsversion RTR
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern

Version 1.8a Änderungen IV 1. Oktober 2014
- Anpassungen auf Grund der Einschau vom 10. September 2014 durch RTR
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern

Version 1.8b Änderungen V 1. Februar 2015
- Anpassungen auf Grund der Besprechung am 15. Jänner 2015 bei RTR
- Präzisierung der verwendeten Schlüssel- und Hashalgorithmen
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern

1.3 Beteiligte / PKI participants

1.3.1 Zertifizierungsdienstanbieter / Certification authorities

Herausgeber und Zertifizierungsdienstanbieter (ZDA)
Herausgeber dieser GLOBALTRUST® Certificate Practice Statement und Zertifizierungsdienstanbieter (ZDA) ist die e-commerce monitoring GmbH, ein nach österreichischem Recht im Firmenbuch eingetragenes Unternehmen mit Sitz in Wien (Handelsgericht Wien FN 224536 a), und ist Erbringer aller zu GLOBALTRUST® zugeordneten Zertifizierungsdienste (verantwortlicher Zertifizierungsdienstanbieter). Der ZDA betreibt die Website http://www.globaltrust.eu. Der ZDA erfüllt alle Voraussetzungen einer zuverlässigen Organisation, insbesondere verfügt er über eine ausreichende finanzielle und personelle Ausstattung um alle im Rahmen der Zertifizierungsdienste eingegangenen Verpflichtungen zu erfüllen.

1.3.2 Registrierungsstelle / Registration authorities

Registrierungsstelle
Die Geschäftsstellen des ZDA und weitere vom ZDA autorisierte Zertifizierungspartner. Die Registrierungsstelle agiert im Rahmen der Vorgaben des ZDA. Sofern unabhängige Registrierungsstellen eingerichtet werden, müssen sie über alle erforderlichen Audits gemäß des GLOBALTRUST® Certificate Practice Statements, der GLOBALTRUST® Certificate Security Policy und dieser GLOBALTRUST® Certificate Policy verfügen, die für ihren Tätigkeitsbereich relevant sind.

Zertifizierungspartner
Personen, die zur Entgegennahme und Prüfung der Zertifizierungsanträge (inklusive Identitätsprüfung) im Auftrag des ZDA berechtigt sind.

Autorisierte Person
Natürliche Person, die zur Prüfung von Zertifizierungsanträgen und zur Durchführung von Zertifizierungsdiensten oder Teilen davon berechtigt ist. Dies können Mitarbeiter des ZDA (autorisierte Mitarbeiter), einer Registrierungsstelle, eines Dienstleisters, eines vertraglich berechtigten Zertifizierungspartners oder Mitarbeiter von Anbietern kommerzieller Identifizierungsdienste sein. Der Tätigkeitsumfang wird im Rahmen von Dienstanweisungen, Tätigkeitsbeschreibungen, vertraglichen Vereinbarungen und anderen geeigneten Dokumentationen nachweisbar festgehalten, dokumentiert und kann bei Vorliegen berechtigter Interessen Dritten zur Verfügung gestellt werden. Autorisierte Mitarbeiter des ZDA werden spezifisch geschult und sind besonders vertrauenswürdig.

1.3.3 Signator / Subscribers

Antragsteller
Person, die auf Basis einer gültigen Certificate Policy und allfälliger zusätzlicher Vereinbarungen einen Antrag auf Ausstellung eines Zertifikats für sich persönlich oder für eine private, eine öffentliche oder internationale Organisation stellt.

Signator, Unterzeichner
Eine Person, die eine Signaturerstellungseinheit besitzt und die entweder im eigenen Namen oder im Namen der von ihr vertretenen Stelle oder juristischen oder natürlichen Person handelt. Die Begriffe Signator und Unterzeichner werden synonym verwendet.

1.3.4 Nutzer / Relying parties

Nutzer
Eine natürliche Person, die Dienste, Produkte des Betreibers oder mit Diensten oder Produkten des Betreibers hergestellte Dienste oder Produkte benutzt. Die Nutzung kann mit oder ohne Vertrag mit dem Betreiber erfolgen. Insbesondere ist jeder Nutzer der einen mit Zertifikat des Betreibers bestätigten öffentlichen Schlüssel benutzt oder Empfängers von elektronisch signierten Informationen ist.

Beteiligte
Alle Personen und Einrichtungen, die dieser GLOBALTRUST® Certificate Policy und dem anzuwendenden GLOBALTRUST® Certificate Practice Statement unterworfen sind. Insbesondere sind dies der ZDA, Registrierungs- und Bestätigungsstellen, Dienstleister und Zertifizierungspartner in Hinblick auf Antragsprüfung, Ausgabe, Archivierung und Widerruf von Zertifikaten im Sinne dieser GLOBALTRUST® Certificate Policy. Weiters der Signator im Rahmen der Anwendung des Zertifikats (insbesondere bei elektronischen Signaturen) und die Nutzer.

1.3.5 Weitere Beteiligte / Other participants

Betreiber
Betreiber beschreibt die Rolle des ZDA als Dienstleister. Soweit der ZDA als Dienstleister für andere Zertifizierungsdienstanbieter tätig ist, verpflichtet er sich die technischen und organisatorischen Abläufe ident zu der beschriebenen GLOBALTRUST® Certificate Policy zu behandeln. In den Fällen, in denen sowohl auf die eigenständige Erbringung von Zertifizierungsdiensten (ZDA), als auch auf die Erbringung als Dienstleister verwiesen werden soll, wird in diesem Dokument umfassend von "Betreiber" gesprochen.

Dienstleister
Weitere Einrichtungen, die vom ZDA mit der technischen oder wirtschaftlichen Umsetzung von Zertifizierungsdiensten teilweise oder ganz betraut werden. Dienstleister ist der Herausgeber, wenn er Zertifizierungsdienste im Auftrag eines anderen Zertifizierungsdienstanbieters erbringt ("Dienstleister eines ZDA").

Vertriebspartner
Einrichtungen, die mit dem ZDA spezifische Vereinbarungen zum Vertrieb von Zertifizierungsdiensten haben. Eine Liste von Vertriebspartnern ist über die Website des ZDA abrufbar.

Aufsichtsbehörde
Eine für die Zertifizierungsdienste des ZDA auf Grund gesetzlicher Vorgaben zuständige Aufsichtsbehörde.

Bestätigungsstelle
Nach dem österreichischen Signaturgesetz [SigG] eingerichtete Bestätigungsstelle oder eine nach einer auf Basis der EU-Signatur-Richtlinie [SigRL] erlassenen gesetzlichen Bestimmung

in einem anderen Staat eingerichtete Bestätigungsstelle für sichere Signaturerstellungseinheiten.

kompetente unabhängige Auditstelle
Auditstelle, die befähigt ist Zertifizierungsstellen nach zumindest einem der folgenden oder einem strengerem Kriterium zu prüfen:
- [ETSI TS 101 456][3]
- [SIGRL]
- [SigG] + [SigV]
- [CABROWSER-BASE]
- [CABROWSER-EV]
- [MOZILLA-CAPOL]
- [WEBTRUST-CA]
- [WEBTRUST-EV]

Die Auditstelle beschäftigt Mitarbeiter die die Fähigkeit in der Prüfung von PK-Infrastruktur, IT-Sicherheits Techniken, IT-Sicherheits durch Audits und Akreditierung von Dritten haben. Die Auditstelle ist akredidiert nach ETSI TS 119 403 zur Prüfung von ETSI-Standards, nach ISO 27006 zur Durchführung von ISO 27001 Audits (oder vergleichbar). Die Auditstelle handelt auf Grund einer gesetzlichen Befugnis, nach öffentlichen Richtlinien oder folgt den Richtlinien eines Berufsverbandes. Die Auditstelle - soweit sie nicht im Rahmen einer gesetzlichen Befugnis tätig ist - verfügt über eine Haftpflichtvericherung mit einer Deckungssumme von mindestens USD 1.000.000.
Im Falle einer Prüfung gibt die Auditstelle bekannt, nach welchen Kriterien sie die Prüfung durchführte und nach welchen Kriterien sie tätig und akredidiert ist.

Betroffener
Alle Personen zu denen der Betreiber personenbezogene Daten verwaltet.

1.4 Verwendungszweck der Zertifikate / Certificate usage

1.4.1 Verwendungszweck / Appropriate certificate uses

Die zulässigen Verwendungszwecke ergeben sich aus den Einträgen im Zertifikat, dieser GLOBALTRUST® Certificate Policy und dem anzuwendenden GLOBALTRUST® Certificate Practice Statement.

Die zulässigen Formate der zu signierenden Daten können im Dokument ⇨ Anhang A: 3 Unterstützte Signaturerstellungsprodukte (p125), in der jeweils anzuwendenden Certificate Policy oder auf der Website des ZDA gelistet werden. Sofern bei Formaten Einsatzbeschränkungen bestehen, werden diese im Dokument angeführt. Zulässig ist dabei auch ein Verweis auf Publikationen der Aufsichtsstellen bezüglich zulässiger und/oder empfohlener Datei-Formate.

Bezüglich der Signaturerstellungseinheiten fortgeschrittener Signaturen werden keine zwingenden technischen Vorgaben gemacht. Der Signator ist im Einsatz der Signaturerstellungseinheiten frei, er muss jedoch rechtlich verbindlich die persönliche und alleinige Kontrolle über die ihm zugeordnete Signatur zusichern.

---

[3] inklusive der vereinfachten Version [ETSI TS 102 042]

Verbindliche Rechtsgeschäfte mit einem Wert von mehr als 100.000,- Euro erfordern ein qualifiziertes Zertifikat.

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 ist ausdrücklich ausgeschlossen.

Es ist zulässig über die Website oder sonstwie veröffentliche Bedingungen Einschränkungen in der Nutzung bzw. Gültigkeit des Zertifikats (insbesondere Beachtung von Betragsobergrenzen bis zu denen die Signatur gültig ausgestellt wird festzulegen). Gemäß dieser eingetragenen Einschränkungen und Obergrenzen beschränkt sich auch die Haftung des ZDA.

Zusätzliche Einschränkungen können sich aus dem Typus des ausgestellten Zertifikates und des Verwendungszweckes ergeben.

1.4.2 Untersagte Nutzung der Zertifikate / Prohibited certificate uses

Dort wo dies technisch machbar und sinnvoll ist werden Verwendungsbeschränkungen direkt in den Zertifikaten in der dem Standard entsprechenden Form eingetragen. Bei Sub-Zertifikaten die zur Ausstellung von Serverzertifikaten vorgesehen sind, erfolgt eine Beschränkung der zulässigen Domainnamen und IP-Adressen. Ist es nicht möglich eine vorgesehene Einschränkung technisch umzusetzen, dann erfolgt eine vertragliche Vereinbarung bezüglich der zulässigen Domainnamen und IP-Adressen.

1.5 Policy Verwaltung / Policy administration

1.5.1 Zuständigkeit für das Dokument / Organization administering the document

Das vorliegende Dokument unterliegt der alleinigen Verantwortung des Betreibers.

1.5.2 Kontaktperson / Contact person

Anfragen zum Dokument sind an den Betreiber zu richten. Die aktuellen Kontaktdaten sind auf der Website des Betreibers gelistet (⇨ Kontakt-Daten: http://www.globaltrust.eu/impressum.html).

1.5.3 Person die die Eignung der CPS bestätigt / Person determining CPS suitability for the policy

GLOBALTRUST® Certificate Practice Statements werden gemäß Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy durch den Zertifizierungs-Ausschuss in Auftrag gegeben und durch den Zertifizierungs-Ausschuss abgenommen.

1.5.4 Verfahren zur Freigabe der CPS / CPS approval procedures

GLOBALTRUST® Certificate Practice Statements werden durch die regulären Mitglieder des Zertifizierungs-Ausschusses geprüft und freigegeben. Die Eignung wird durch einen

Vertreter der Geschäftsführung und zumindest ein weiteres Mitglied des Zertifizierungs-Ausschusses bestätigt und intern dokumentiert.

1.6 Definitionen und Kurzbezeichnungen / Definitions and acronyms

Geschäftsprozess
Logische Einheit aller Maßnahmen und Abläufe zur Erreichung eines inhaltlich definierten Zieles. Die ⇨ Zertifizierungsdienste sind eine Untergruppe aller Geschäftsprozesse des Betreibers.

Zertifizierungsdienste
Gesamtheit aller Dienstleistungen, die der Betreiber erbringt, insbesondere sind dies folgende zentrale Dienste:
- Verwaltung von Antragstellern für Zertifikate (inkl. Identifikation der Antragsteller)
- Erstellen von Zertifikaten (inkl. Sperre und Widerruf von Zertifikaten)
- Ausliefern von Zertifikaten
- Verwaltung von Sperr- und Widerrufsanträgen
- Verbreitung von Sperr- und Widerrufsinformationen

Weitere Zertifizierungsdienste sind insbesondere
- Erstellen und Ausliefern von Signaturerstellungseinheiten
- Zeitstempeldienste
- sonstige Signaturdienste, wie Signaturdienste mittels mobile Devices ("Handysignatur"), sonstige serverbasierte Signaturdienste, insbesondere Dokumentenarchivierungsdienste die vom Betreiber selbst betrieben werden.

Die Erbringung erfolgt insbesondere gemäß [SigRL], [SigG] und [CWA-14167-1] und umfasst sowohl Dienstleistungen zur einfachen, fortgeschrittenen oder qualifizierten elektronischen Signatur, zu qualifizierten oder einfachen Zertifikaten, zu qualifizierten oder einfachen Zeitstempeldiensten.
Die einzelnen Dienste sind als ⇨ Geschäftsprozesse organisiert.

serverbasierte Signaturdienste
Dienstleistungen des Betreibers zur Verwaltung, Archivierung, Erstellung, Verifizierung oder Zustellung signierter Dokumente. Die Dokumente können individuell durch den Nutzer, den Betreiber, autorisierte Dritte oder einer Kombination aus den genannten Personengruppen signiert werden. Es können zum Nachweis der Authentizität qualifizierte oder nicht qualifizierte Zertifikate verwendet werden. Der serverbasierte Signaturdienst kann auch nur Teil eines Dienstangebots des Betreibers sein, etwa im Rahmen von Pseudonymisierungs- und Anonymisierungsdiensten.

elektronische Signatur
Daten in elektronischer Form im Sinne [SigRL], die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.

Zertifikatsdaten
Gesamtheit aller Daten, insbesondere Identifikationsdaten, die für Ausstellung, Prüfung oder Widerruf von Zertifikaten erforderlich sind.

einfache elektronische Signatur
Elektronische Signatur, die weder den Anforderungen der fortgeschrittenen elektronischen Signatur, noch denen der qualifizierten elektronischen Signatur entspricht.

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.

Amtssignatur
Fortgeschrittene elektronische Signatur gemäß E-Governmentgesetz [E-GOVG], insbesondere unter Berücksichtigung von [ASZ] und vergleichbarer Dokumentationen mit amtlichen Charakter.

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 erstellt wird.

Zertifikat
Eine elektronische Bescheinigung, mit der Signaturprüfdaten einer Person zugeordnet werden und die Identität dieser Person bestätigt wird.

einfaches Zertifikat
Zertifikat, das nicht den Kriterien eines qualifizierten Zertifikates entspricht.

qualifiziertes Zertifikat
Ein Zertifikat, das dem Stand der Technik ausgestellt wurde und insbesondere die Anforderungen der [SigRL] Anhang I erfüllt und von einem Zertifizierungsdiensteanbieter (ZDA) bereitgestellt wird, der die Anforderungen der [SigRL] Anhang II erfüllt.
Zertifikat im Sinne [SigRL]. Der Inhalt folgt [ETSI TS 101 862]. Die Laufzeit des qualifizierten Zertifikats ist auf Grund der rechtlichen Vorgaben auf maximal 5 Jahre limitiert und kann vom ZDA auf Grund geänderter rechtlicher Rahmenbedingungen oder anderer wichtiger Gründe jederzeit verkürzt werden.

qualifiziertes X.509v3-Zertifikat
Sie enthalten im Zertifikat entweder das Attribut id-etsi-qcs-QcCompliance ([ETSI TS 101 862] 5.2.1, OID: 0.4.0.1862.1.1) oder 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). Jedes Feld kann nur für jene Einträge verwendet werden, für das es gemäß der anzuwendenden Standards und Normen definiert ist.

Weitere Angaben im Zertifikat:
- X509 v3 Extensions: X509v3 Basic Constraints: critical CA:FALSE
- X509v3 Key Usage: critical Digital Signature
- X509v3 Extended Key Usage: critical (optional) z.B. id-kp-eInvoicing
- OCSP - URI:http://ocsp-**NN-****[4].globaltrust.eu
- 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
- 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
- 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),
  - id-etsi-qcs-QcLimitValue: QcEuLimitValue (OID 0.4.0.1862.2), (optional)
  - id-etsi-qcs-QcRetentionPeriod: QcEuRetentionPeriod (OID 0.4.0.1862.3), (optional)
  - id-etsi-qcs-QcSSCD (OID 0.4.0.1862.4)
- 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 elektr. Vollmachten (OID 1.2.40.0.10.1.7.2): NULL (optional)
- weitere OID-Einträge sofern im Einklang mit den Bestimmungen zur qualifizierten Signatur (optional)

Verwendeter Signature Algorithm: SHA2 (sha256WithRSAEncryption oder höher)

Root-Zertifikat

Zertifikat das vom ZDA ausschließlich zur Erbringung von Zertifizierungsdiensten verwendet wird und dass als oberste Instanz nur von sich selbst unterschrieben wird (auch Self-Signed-Zertifikat bzw. Wurzel-Zertifikat).
Die Root-Zertifikate sind in den Angaben von Herausgeber und Anwender (Antragsteller) ident und können auf Grund der Angaben im Zertifikat, insbesondere des Policy-Verweises verifiziert werden.
Der private Schlüssel von Root-Zertifikaten wird zumindest mittels RSA und einer Mindestlänge von 4096 bit ausgestellt, der verwendete Hash-Algorithmus ist für Root-Zertifikate SHA1, für Root-Zertifikate, die nach dem 1. Oktober 2014 erstellt werden zumindest SHA256.
Root-Zertifikate werden ausschließlich zum Signieren von CA-Zertifikaten, Widerrufslisten und Widerrufsdiensten verwendet. Andere Verwendungen werden auf Grund der Betriebsorganisation des ZDA ausgeschlossen.

---

[4] **NN** == Bezeichnung der Produktlinie des ZDA, z.B. qualified, ** == laufende Nummer, beginnend mit 1 zur (zukünftigen) Unterscheidung unterschiedlicher CA-Zertifikate derselben Produktlinie, z.B. GLOBALTRUST QUALIFIED 1 verwendet die Dateien http://service.globaltrust.eu/static/globaltrust-**qualified-1**-der.cer als Zertifikats-URL und http://service.globaltrust.eu/static/globaltrust-**qualified-1**.crl als Widerrufsliste. Die detaillierte Darstellung zu welchem Produkt welche Policy, welche CRL, welcher LDAP-Dienst und welches OCSP-Service zugeordnet ist findet sich unter ⇨ Policy Online: http://www.globaltrust.eu/certificate-policy.html

CA-Zertifikat
Zertifikate des ZDA, die zur Erbringung von Zertifizierungsdiensten erforderlich sind. CA-Zertifikate können Self-Signed-Zertifikate des ZDA sein (Root-Zertifikat) oder unter einem Self-Signed-Zertifikat ausgestellte Sub-Zertifikate, die zur Erbringung von Zertifizierungsdiensten vorgesehen sind. Die Fingerprints der CA-Zertifikate sind auf der Website des ZDA und bei den zuständigen Aufsichtsstellen hinterlegt.
Der private Schlüssel von CA-Zertifikaten die zur Ausstellung von qualifizierten Zertifikaten dienen wird mittels RSA und einer Mindestlänge von 4096 bit ausgestellt, der verwendete Hash-Algorithmus ist zumindest SHA256.
Die CA-Zertifikate enthalten jedenfalls folgende Herausgeberdaten: zweistelliger Länderbezeichnung gemäß ISO 3166-1 jenes Landes, in dem der ZDA seinen Sitz hat und Organisationsbezeichnung des ZDA laut Firmenbucheintrag[5].
CA-Zertifikate werden ausschließlich zum Signieren von Zertifikaten, Widerrufslisten und Widerrufsdiensten verwendet. Andere Verwendungen werden auf Grund der Betriebsorganisation des ZDA ausgeschlossen.

Endkundenzertifikat
Zertifikat, dass von einem CA-Zertifikat unterschrieben ist und für Signatur- und/oder Verschlüsselungszwecke verwendet werden kann. Es erlaubt keine Ausstellung weiterer (untergeordneter) Zertifikate.

Sub-Zertifikat
Zertifikat, dass von einem CA-Zertifikat unterschrieben ist und vom Signator auch für die Ausstellung weiterer Zertifikate verwendet werden kann.

Zeitstempel, Timestamp
Signierte Datenstruktur bestehend jedenfalls aus dem Hashcode eines Dokuments und dem Zeitpunkt der Unterzeichnung. Format und Methode der Erzeugung des Zeitstempels entspricht dem Standard [RFC3161]. Angaben zu den aktuellen Betriebsdaten des Zeitstempeldienstes (inkl. Zeitgenauigkeit, Zeitstempelverfahren) finden sich auf Website http://www.globaltrust.eu/produkte.html. Die Begriffe Zeitstempel und Timestamp werden synonym verwendet.

qualifizierter Zeitstempeldienst
Dienst der Zeitstempel durch ein qualifiziertes Zertifikat oder ein vergleichbares Verfahren erzeugt, das die Richtigkeit und Unverfälschtheit der Zeitangabe sicherstellt.

Betrieb
Gesamtheit aller Tätigkeiten des ZDA zur Erbringung der Zertifizierungsdienste.

Betriebskonzept
Gesamtheit aller Dokumente zum Betrieb der Zertifizierungsdienste die durch die ⇨ **Aufsichtsstelle** geprüft und genehmigt wurden.

Zertifizierungssystem

---

[5] Im Falle von X509v3-Zertifikaten verwendet der ZDA folgende Herausgeberangaben (Issuer-Daten): C=AT und O=e-commerce monitoring GmbH (Firmenbezeichnung lt. Firmenbuch)

Technisches System, dass die Abwicklung von Zertifizierungsdiensten, insbesondere Ausstellung oder Widerruf von Zertifikaten, ermöglicht.

Administratives System
Verwaltungssystem zur Prüfung und Erzeugung der für die Ausstellung oder den Widerruf von Zertifikaten erforderlichen Daten.

Informationssicherheitsmanagementsystem, ISMS
Gesamtheit aller technischen und organisatorischen Maßnahmen zur Planung, Herstellung, Aufrechterhaltung, Änderung der Informationssicherheit des Betreibers.

Private, öffentliche und internationale Organisationen
Private Organisationen sind Einrichtungen die in ihren Ländern nach den jeweils geltenden Regeln des Privat- bzw. Zivilrechts eingerichtet sind.
Öffentliche Organisationen sind Einrichtungen, die in ihren Ländern kraft Gesetz eingerichtet sind, etwa Behörden, staatliche Verwaltungen, Gemeinde-, Landes- oder Bundesdienststellen.
Internationale Organisationen sind Einrichtung, die auf Grund völkerrechtlicher Vereinbarungen eingerichtet sind.

Signaturerstellungsdaten
Eindeutige Daten wie Codes oder private kryptographische Schlüssel, die vom Unterzeichner (Signator) zur Erstellung einer elektronischen Signatur verwendet werden.

Aktivierungsdaten
Informationen des Signators, die er zur Durchführung einer Signatur benötigt, zumindest Teile davon sind vertraulich und nur dem Signator bekannt bzw. nur im Besitz des Signators (z.B. Signatur-PIN bzw. Passwort).

Signaturerstellungseinheit
Eine konfigurierte Software, Hardware oder Kombination aus beiden, die zur Implementierung der Signaturerstellungsdaten verwendet wird.

HSM
Hardware-Sicherheitsmodul oder englisch Hardware Security Module (HSM), Hardwareprodukt im Sinne ⇨ Signaturerstellungseinheit.

Sichere Signaturerstellungseinheit, sicherer Schlüssel
Eine Signaturerstellungseinheit, die dem Stand der Technik entspricht und jedenfalls die Anforderungen [SigRL] Anhang III erfüllt (secure signature creation device, SSCD), Hinweise des BSI, der A-SIT, vergleichbarer Einrichtungen und der Aufsichtstellen werden beachtet).

Signaturprüfdaten
Daten wie Codes oder öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden.

Produkt für elektronische Signaturen
Hard- oder Software bzw. deren spezifische Komponenten, die von einem Zertifizierungsdiensteanbieter (ZDA) für die Bereitstellung von Diensten für elektronische

Signaturen verwendet werden oder die für die Erstellung und Überprüfung elektronischer Signaturen verwendet werden.

Signaturbestimmungen
Gesamtheit der in den für die beschriebenen Zertifizierungsdienste zutreffenden Dokumente, insbesondere [SigG], [SigV], [SigRL] formulierten Bestimmungen inklusive den in den Bestimmungen zitierten Dokumenten.

24/7/365, Permanenzdienst, Bürozeiten
Dienste werden ganzjährig, sieben Tage die Woche und 24 Stunden täglich bereitgestellt. Ausfälle bzw. Fehler in der Bereitstellung werden dokumentiert. Im Einzelfall können zusätzlich Beschränkungen der Verfügbarkeit definiert werden, etwa tolerierte Ausfallszeiten von 1% pro Monat oder Jahr.
Soweit nicht im jeweiligen GLOBALTRUST® Certificate Practice Statement eines Dienstes abweichend beschrieben, nicht auf der Website des Betreibers oder auf einer in der jeweiligen Certificate Policy angegebenen Website abweichend veröffentlicht, gelten folgende Mindest-Bürozeiten für jede Form von Anfragen, Anträgen und Bestellungen, inkl. Anträgen zu Sperren und Widerrufen: werktags Mo-Fr 9:00 - 17:00
Außerhalb dieser Zeiten besteht ein Bereitschaftsdienst zur Behebung zertifizierungskritischer technischer Störungen, Gebrechen und sonstiger Notfälle.

Cross-Zertifizierung
Bestätigung eines Zertifikats eines anderen Zertifierungsdiensteanbieters, einer Aufsichtstelle durch den ZDA oder umgekehrt.

Endkundenschlüssel, Endkunden-Signaturerstellungseinheit
Schlüssel der vom ZDA für Endkunden (Signator, Unterzeichner) für die elektronische Signatur erstellt und ausgeliefert wird. Bei asymetrischen Verschlüsselungen beschreibt "Endkundenschlüssel" das Schlüsselpaar des privaten und öffentlichen Schlüssels.

gesicherte Umgebung
Gesamtheit aller technischen und organisatorischen Maßnahmen, die den kontrollierten Zertifizierungsbetrieb ermöglichen.

Produktzusatz
Ergänzende Angabe, die zur Beschreibung der Zertifizierungsdienste und Zertifikatsarten dient und Teil des vom ZDA ausgegebenen Zertifikates ist. Im Zusammenhang mit Zertifikaten nach dem X.509v3-Standard ist die Bezeichnung ergänzender Teil des CN eines CA-Zertifikates zur Bezeichnung GLOBALTRUST, z.B. GLOBALTRUST ADVANCED. Produktzusätze können im Rahmen der Geschäftstätigkeit des Betreibers definiert und vergeben werden, wobei sie nicht irreführend sein oder im Konflikt zu den in dieser Policy verwendeten Produktzusätzen sein dürfen.

EV Zertifikate
Bezeichnet Zertifikate, die auf Basis der vom CA/Browser Forum publizierten Richtlinien „CA/Browser Forum Guidelines for Extended Validation Certificates“ ([CABROWSER-EV] ausgegeben worden sind. Das CA-Zertifikat GLOBALTRUST® EV SSL SERVER entspricht der aktuellen Version der „CA/Browser Forum Guidelines for Extended Validation Certificates“ [EVG], die auf http://www.cabforum.org publiziert sind.

Ansonsten werden die Begriffe sinngemäß nach [SigG], [SigV], [SigRL], [X.509v3], [CWA-14167-1], [ETSI TS 101 456], [ETSI TS 102 042], [RFC3161], [RFC3739] und [RFC3647] oder anderer in ⇨ Anhang A: 1 Bibliographie (p109) genannten Dokumente verwendet.

2. VERÖFFENTLICHUNG UND AUFBEWAHRUNG / PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Aufbewahrung / Repositories

Die aktuelle Version dieses Dokuments ist über die Website des Betreibers abrufbar.

Historische Versionen des Dokuments sind bei der Aufsichtsstelle abzurufen oder unter der OID-Nummer 1.2.40.0.36.1.1.8.99 auf der Website des Betreibers abgelegt. Eine englische Übersetzung dieser Policy wird unter der OID-Nummer 1.2.40.0.36.1.1.8.12 veröffentlicht[6].

Über die Website bzw. sofern von den Zertifikatsinhabern verfügbar per E-Mail wird zeitgerecht über Änderungen informiert, die in der GLOBALTRUST® Certificate Policy vorgenommen werden.

2.2 Veröffentlichung von Zertifizierungsinformationen / Publication of certification information

Über die Website des Betreibers werden alle für die Erbringung der Zertifizierungsdienste erforderlichen Dokumente veröffentlicht, ebenso die verwendeten CA-Zertifikate und geeignete Prüfsummen.

Weiters werden Informationen zu den angebotenen Diensten und die verwendeten Verfahren zugänglich gemacht.

Der ZDA macht den Signatoren und den Benutzern, die auf die Zuverlässigkeit der GLOBALTRUST® Dienste vertrauen, die Bedingungen, die die Benutzung des jeweiligen Zertifikats betreffen, durch Veröffentlichung folgender Dokumente auf der Website des Betreibers zugänglich:

1. die gegenständliche Certificate Policy, sofern für einen Dienst erforderlich weitere in diesem Dokumenten bezeichnete Certificate Policies
2. Allgemeine Betriebs- und Nutzungsbedingungen
3. ergänzende Beschreibungen zu den einzelnen Zertifizierungsdiensten
4. - sofern anwendbar - ein Verweis auf die Anzeige des Zertifizierungsdienstes bei der Aufsichtsbehörde
5. sonstige Mitteilungen
6. alle Crosszertifikate die den ZDA als Inhaber identifizieren und aufgrund einer Vereinbarung des ZDA erstellt wurden oder von diesem akzeptiert wurden

Änderungen werden dem Signator mittels Bekanntmachung auf der Website des ZDA und ggf. zusätzlich per E-Mail oder brieflich mitgeteilt.

---

[6] Die Veröffentlichung erfolgt nach Abschluss der Genehmigung der GLOBALTRUST® Certificate Policy durch die Aufsichtsbehörde und hat informativen Charakter.

2.3 Häufigkeit der Veröffentlichung / Time or frequency of publication

Verbindliche Vereinbarungen werden fristgerecht vor Inkrafttreten veröffentlicht und gelten bis Widerruf. Im Falle von Befristungen, insbesondere der Gültigkeit von Zertifikaten, wird darauf in geeigneter Weise hingewiesen. Sonstige Informationen werden unverzüglich während der Bürozeiten veröffentlicht.

Änderungen werden unverzüglich veröffentlicht.

2.4 Zugangsbeschränkungen / Access controls on repositories

Es werden keine Maßnahmen zur Beschränkung des Zugriffs auf die öffentlichen Informationen ergriffen.

Interne Informationen werden gemäß GLOBALTRUST® Certificate Security Policy gesichert.

3. IDENTIFIZIERUNG UND AUTHENTIFIKATION / IDENTIFICATION AND AUTHENTICATION

Alle Zertifikatsdaten, insbesondere Angaben über verwendete Signaturerstellungeinheiten, Angaben zur Erzeugung von privaten Schlüsseln, Zertifikatsanforderungen (wie ein Certificate Signing Request), anzuwendende Policies werden nach Plausibilität, sachlicher und technischer Richtigkeit und nach Übereinstimmung mit gesetzlichen und sonstigen rechtlichen Vorgaben geprüft.

Dazu kann sich der ZDA auch externer Dienste und Sachverständiger bedienen. Soweit ein Nachweis über die rechtmäßige Verfügungsgewalt über einzelne Komponenten und vertrauliche Informationen erforderlich ist (insbesondere Signaturerstellungseinheiten, private Schlüssel usw.) sind jedenfalls Erklärungen vom Signator vorzulegen. Der ZDA kann bei berechtigten Zweifel an den abgegebenen Erklärungen zusätzliche Bestätigungen und Bescheinigungen anfordern. Eine Zustellung von Zertifikaten vor erfolgreichen Abschluss der Prüfung erfolgt nicht.

3.1 Benennung / Naming

Bezeichnungen werden so gewählt, dass sie den beschreibenden Sachverhalt ausdrücken oder dem Namen einer Person oder Einrichtung entsprechen. Sie können in beliebiger Sprache erfolgen. Irreführende, fehlerhafte oder rechtswidrige Bezeichnungen und Benennungen werden vom Betreiber nicht akzeptiert.

3.1.1 Arten der Benennung / Types of names

In den Zertifikaten werden ausschließlich Bezeichnungen zugelassen,
- über die der Antragsteller rechtmäßig verfügt oder
- im Falle nicht geschützter Begriffe und Bezeichnungen, soweit sie nicht irreführend sind oder gegen gesetzliche Bestimmungen verstoßen.

3.1.2 Notwendigkeit für aussagekräftige Namen / Need for names to be meaningful

Soweit für die Erfüllung eines Zweckes erforderlich werden aussagekräftige Bezeichnungen und Namen verlangt.

3.1.3 Behandlung von Anonymität oder Pseudonymen von Antragstellern / Anonymity or pseudonymity of subscribers

Zertifizierungsdienste können - sofern rechtlich und den technischen Standards entsprechend zulässig - auch in einer Form erbracht werden, bei denen die antragstellenden Personen, Organisationen oder Organe der antragstellenden Organisationen nicht öffentlich aufscheinen. In diesem Fall erfolgt eine interne Dokumentation in der die in Anspruch genommenen Zertifizierungsdienste eindeutig einer antragstellenden Person oder Organisation zugeordnet werden kann.

Pseudonyme werden jedenfalls bei qualifizierten Zertifikaten als solche eingetragen bzw. gemäß den technischen Standards gekennzeichnet.

Im Falle eines bescheinigten oder nachgewiesenen rechtlichen Interesses oder einer rechtlichen Verpflichtung werden die Identitätsdaten einer antragstellenden Person oder Organisation, inklusive den Organen oder Vertretungen bekannt gegeben.

3.1.4 Interpretationsregeln für verschiedene Benennungsformen / Rules for interpreting various name forms

Sind mehrere Benennungsformen gleichermaßen zulässig, dann wird grundsätzlich dem Antragsteller die Wahl gelassen, welche Benennungsform er wählt.

Von dieser Vorgangsweise wird abgegangen, wenn eine Benennungsform wesentlich einfacher und eindeutiger ist.

Im Fall von Benennungskonflikten schlägt der Betreiber die geeignetste Benennung vor.

3.1.5 Einmaligkeit von Benennungen / Uniqueness of names

Es werden keine Zertifizierungsdienste für unterschiedliche Signatoren erbracht, die dieselbe Bezeichnung haben. Jedenfalls wird sichergestellt, dass sich Zertifizierungsdienste durch eine Seriennummer oder eine vergleichbare Kennzeichnung unterscheiden.

3.1.6 Berücksichtigung und Authentifikation von Markennamen / Recognition, authentication, and role of trademarks

Es ist zulässig, eine öffentlich registrierte Markenbezeichnug als Organisationsname einzutragen, sofern der Antragsteller nachweisen kann, diese verwenden zu dürfen und der offizielle Firmenname der Markenbezeichnung in Klammern nachgestellt wird. Um die Länge des organizationName Feldes zu begrenzen sind Abkürzungen erlaubt, sofern sie nicht irreführend sind.

3.2 erstmalige Identitätsfeststellung / Initial identity validation

Alle Angaben zum Zertifikatsinhaber - insbesondere die Identitätsangaben - werden in jeder Zertifikatsvariante auf ihre Richtigkeit hin geprüft.

Im Falle der Erstantragsstellung erfolgt eine persönliche Identitätsfeststellung durch den ZDA oder eine vom ZDA authorisierte Person.

3.2.1 Nachweis über den Besitzes des privaten Schlüssels / Method to prove possession of private key

Sofern der private Schlüssel nicht durch den Betreiber erzeugt wird, verlangt der Betreiber einen Nachweis vom Signator, dass er tatsächlich im Besitz des privaten Schlüssels ist.

3.2.2 Authentifikation der Organisation / Authentication of organization identity

Soweit ein Antrag Angaben zu einer Organisation enthält, werden diese Daten geprüft.

Die Maßnahmen und Abläufe zur Identifikation und Registrierung des Antragstellers orientieren sich am jeweiligen Zertifizierungsdienst und seinen rechtlichen, insbesondere

gesetzlichen Vorgaben und können sowohl sachliche, als auch regionale Unterschiede aufweisen.

Als Auskunftsstelle für die Gültigkeit einer Organisation sind grundsätzlich alle staatlich anerkannten Behörden und Organisationen geeignet, die öffentliche Verzeichnisse führen und vor Aufnahme in diese Verzeichnisse eine Identitätsprüfung durchführen.

3.2.3 Identitätsprüfung von Personen / Authentication of individual identity

Vom Antragsteller sind die Angabe der Art des amtlichen Personaldokuments, die Nummer ,die Identitätsangaben der ausstellenden Behörde und das Ausstellungsdatum erforderlich.

a) Fall Überprüfung vor Ort

Findet die Überprüfung der Identität des Antragstellers durch eine autorisierte Person statt (z.B. Antragsteller ist in den Räumlichkeiten des ZDA oder einer Registrierungsstelle persönlich anwesend) dann ist das amtliche Personaldokument im Original oder als beglaubigte Kopie vorzulegen. Beglaubigte Kopien sind auszuhändigen, von einem Originaldokument sind - neben den Identitätsangaben des Antragstellers - jedenfalls Art des amtlichen Personaldokuments, die Nummer ,die Identitätsangaben der ausstellenden Behörde und das Ausstellungsdatum zu erfassen. Ein vorgelegtes Dokument kann abgelehnt werden, wenn auf Grund dieses Dokument die Person nicht zweifelsfrei identifiziert werden kann, das Dokument nicht(mehr) gültig ist oder der amtliche Charakter des Dokuments zweifelhaft ist. Kann der Antragsteller keine geeigneten Dokumente vorlegen, dann wird der Antrag auf Grund fehlgeschlagener Identitätsprüfung abgelehnt.

b) Fall Überprüfung nicht vor Ort

Kann die Identität des Antragstellers nicht auf Grund seiner persönlichen Anwesenheit geprüft werden, werden die Identitätsangaben und Angaben zum amtlichen Personaldokument, wie Art des amtlichen Personaldokuments, die Nummer ,die Identitätsangaben der ausstellenden Behörde und das Ausstellungsdatum auf Grund der Angaben des Antragstellers erfasst. Weiters erfolgt eine Plausibilitätsprüfung der Angaben auf Basis vorgelegter Kopien der Dokumente (eine Begleubigung ist nicht erforderlich). Ist die Plausibilitätsprüfung nicht erfolgreich oder bestehen Bedenken bei den vorgelegten Dokumente können zusätzliche Unterlagen, zusätzliche Kontakte oder Anfragen in vertrauenswürdigen öffentlichen Quellen erfolgen. Kann der Antragsteller trotz Aufforderung offene Fragen nicht ausreichend aufklären, dann wird der Antrag auf Grund fehlgeschlagenerPlausibilitätsprüfung abgelehnt.

Bei qualifizierten Zertifikaten sind zusätzlich zu den oben beschriebenen Mindestangaben folgende Informationen zur Person des Signators obligatorisch:

- Geburtstag und -ort
- Eine national anerkannte Identifikationsnummer oder ein vergleichbares Attribut, mit der die Person von anderen Personen gleichen Namens unterschieden werden kann.

Die Identitätsprüfung ist abgeschlossen, sofern der Antrag persönlich in einer der Registrierungsstellen erfolgte und vom Antragsteller ein amtliches Personaldokument im Original vorgelegt wurde oder durch ein geprüftes Rechtsgutachten der Identitätsnachweis erbracht wurde, insbesondere ein durch Gericht oder Notar beglaubigter Identitätsnachweis im Original ausgehändigt wurde (⇨ **a) Fall Überprüfung vor Ort**).

In allen anderen Fällen (**b) Fall Überprüfung nicht vor Ort**) erfolgt der Abschluss der Identitätsprüfung im Zuge der Antragsbearbeitung (⇨ 6.1.2 Zustellung privater Schlüssel an den Signator / Private key delivery to subscriber, p75).

Im Zertifikat können zusätzliche Angaben zur Person des Signators enthalten sein: Telefonnummer, Faxnummer und E-Mailadresse, Berufs- und Qualifikationsangaben, allenfalls weitere Daten. Abhängig vom Zertifizierungsdienst können einzelne Angaben optional oder obligatorisch sein.

3.2.4 Nicht-verifizierte Antragstellerdaten / Non-verified subscriber information

Die Zertifikate enthalten
a) entweder keine nicht-verifizierten Angaben (jedenfalls bei qualifizierten Zertifikaten oder EV-Zertifikaten) oder
b) sofern nicht-verifizierte Angaben zulässig sind (z.B. bei Zertifikaten die als Testzertifikate gekennzeichnet sind), werden sie als "Nicht-verifiziert" gekennzeichnet. Diese Kennzeichnung kann durch geeignete OID-Nummern oder andere geeignete Bezeichnungen erfolgen. Die Art und Weise der Kennzeichnung nicht-verifizierter Angaben ist im GLOBALTRUST® Certificate Practice Statement geregelt.

Ausgeschlossen sind jedoch in allen Fällen Angaben, die irreführend oder aus sonstigen rechtlichen Gründen offensichtlich unzulässig sind. Wird die Führung von Markennamen beansprucht, erfolgt jedenfalls eine Verifizierung.

3.2.5 Nachweis der Vertretungsbefugnis / Validation of authority

Die Registrierungsstelle übernimmt die Prüfung der Vertretungsbefugnis und der Angaben/Unterlagen der im Antrag genannten Personen.

Werden Zertifizierungsdienste in Vertretung von Personen oder Organisationen beantragt oder soll in Zertifizierungsdiensten die Vertretungsmacht für Dritte bescheinigt werden, dann ist das nur möglich, wenn die beanspruchten Vertretungen nachgewiesen werden. Vollmachtsumfang und Nachweis der Vollmacht für derartige Vertretungen müssen den gesetzlichen Bestimmungen jenes Staates entsprechen, in dem die Person oder Organisation für die die Zertifizierungsdienste erbracht werden sollen, seinen Sitz hat.

Der ZDA bzw. zur Zertifizierung autorisierte Personen haben bei Zweifel an einer rechtlich zulässigen Vertretungsmacht einen entsprechenden Antrag abzulehnen. Werden dem ZDA bzw. zur Zertifizierung autorisierte Personen im nachhinein Gründe bekannt, die eine gültige Vertretungsmacht ausschließen, sind die Zertifizierungsdienste unverzüglich einzustellen und Zertifikate zu widerrufen.

3.2.6 Kriterien für Interoperabilität / Criteria for interoperation

Nicht zutreffend

3.3 Identifikation und Authentifikation für Schlüsselerneuerung / Identification and authentication for re-key requests

Alle Angaben zum Zertifikatsinhaber - insbesondere die Identitätsangaben - werden bei Schlüsselerneuerung auf ihre Richtigkeit hin geprüft.

Sofern keine Änderungen des Antragstellers begehrt werden, werden nur jene Angaben auf ihre Richtigkeit hin überprüft, die seit der Erstantragstellung einer Änderung unterliegen können, insbesondere die Verfügung über Domainnamen, Muster- und Markenrechte, Angaben zum Firmensitz und dem Bestehen der Firma.

Änderungen die der Antragsteller begehrt werden so behandelt, wie im Fall der Erstantragstellung (⇨ 3.2 erstmalige Identitätsfeststellung / Initial identity validation, p30).

3.3.1 Identifikation und Authentifikation für routinemäßige Schlüsselerneuerung / Identification and authentication for routine re-key

Vorgehen wie ⇨ 3.3 Identifikation und Authentifikation für Schlüsselerneuerung / Identification and authentication for re-key requests (p32).

3.3.2 Identifikation und Authentifikation für Schlüsselerneuerung nach Widerrufen / Identification and authentication for re-key after revocation

Vorgehen wie ⇨ 3.3 Identifikation und Authentifikation für Schlüsselerneuerung / Identification and authentication for re-key requests (p32).

3.4 Identifikation und Authentifikation für Widerrufsanträge / Identification and authentication for revocation request

⇨ 4.9.2 Berechtigte für Antrag auf Widerruf / Who can request revocation (p48)

4. ANFORDERUNGEN ZERTIFIKATSLEBENSZYKLUS / CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Die Erbringung der Zertifizierungsdienste erfolgt ausschließlich auf Basis definierter Geschäftsprozesse, der Status eines Zertifikates, eines Zertifizierunsdienstes bzw. der Status der Zertifikatsausstellung wird durch definierte Statuswerte dokumentiert und ist zu jedem Zeitpunkt des Lebenszyklus des Zertifikates eindeutig definiert.

Die Personalisierung und Zustellung eines Zertifikats, einer Signaturerstellungseinheit oder vergleichbarer Produkte erfolgt erst nach Abschluss der für diese Dienstleistung erforderlichen administrativen Tätigkeiten, insbesondere nach erfolgreichem Abschluss der erforderlichen Identitätsfeststellungen.

4.1 Antragstellung / Certificate Application

Die vorliegende Policy beschreibt den grundlegenden Ablauf der Antragsbearbeitung, der im Einzelfall auf Grund sachlicher oder rechtlicher Gegebenheiten verfeinert werden kann. Jeder Zertifikatsausstellung geht ein Antrag voraus.

4.1.1 Berechtigung zur Antragstellung / Who can submit a certificate application

Natürliche Personen und Organisationen (insbesondere Unternehmen, Vereine, Behörden, Betriebe) können Anträge und Bestellungen zur Erbringung von Zertifizierungsdiensten in beliebiger Form vorbringen. Es bestehen keine regionalen oder sachlichen Einschränkungen.

Solange die Identität eines Antragstellers nicht festgestellt ist, werden die Anträge grundsätzlich als anonym gestellt betrachtet. Vor Ausgabe eines Zertifikats erfolgt jedenfalls eine Identitätsfeststellung. Der Umfang der Identitätsfeststellung erfolgt gemäß der jeweils anzuwendenden Certificate Policy.

Zu den Antragsdaten wird Zeitpunkt des Antrags und Art der Verbreitung der Zertifikatsdaten (öffentlich zugänglich oder nicht) aufgezeichnet.

4.1.2 Anmeldungsverfahren und Verantwortlichkeiten / Enrollment process and responsibilities

Anträge von Organisationen müssen von einem befugten Organ gestellt werden, wobei bei Personen die einen Antrag unter derselben Anschrift wie die betroffene Organisation stellen, grundsätzlich die Vermutung der Befugnis gegeben ist. Bei abweichenden Anschriftangaben des antragstellenden Organs und der betroffenen Organisation muss eine nach außen vertretungsbefugte Person die Berechtigung des antragstellenden Organs bestätigen.

Bevor der Vertrag zwischen dem Signator und dem ZDA abgeschlossen wird, werden dem Signator die Policy, und allfällige sonstige Bestimmungen (allgemeine

Geschäftsbedingungen, individuelle Vereinbarungen) zur Nutzung des Zertifikats elektronisch oder durch schriftliche Unterlagen zugänglich gemacht.

Es werden jedenfalls die folgenden Informationen festgehalten:
- Alle Unterlagen und Ereignisse, die die Antragsbearbeitung betreffen, inklusive Anträge auf Zertifikatsausstellung und -verlängerung.
- Alle Ereignisse die die Freigabe von Anträgen betreffen.

4.2 Bearbeitung von Zertifkatsanträgen / Certificate application processing

Die Daten des Antragsteller werden auf Basis folgender Dokumente und Informationsquellen[7] geprüft:
(1) Bestätigung vom Antragsteller
(2) Rechtsgutachten
(3) Bestätigung eines Wirtschaftsprüfers
(4) Qualifizierte unabhängige Informationsquelle (QIIS - Qualified independent information service)
(5) Qualifizierte behördliche Informationsquelle (QGIS - Qualified government information service)
(6) Qualifizierte behördliche Steuerinformationsquelle (QTIS - Qualified tax information service)

Die Registrierungsstelle nimmt folgende Überprüfungen des Antrags vor:
- Prüfung der Organisation bzw. von ihr verwendeter Markennamen (gemäß vom Antragsteller vorgelegter unbedenklicher Bescheinigungen, lt. Auskunft (inkl. Datenbankabfrage) einer qualifizierten behördlichen Informationsquelle oder anhand von qualifizierte unabhängige Informationsquelle, insbesondere Datenbanken vertrauenswürdiger Dritter).
- Sofern sich ein Zertifikat für die Signatur von E-Mails eignet, wird bei allen im Zertifikat einzutragenden E-Mail Adressen geprüft, ob der Antragsteller die Kontrolle über diese Adressen besitzt, oder von deren Inhaber autorisiert ist. Dies kann insbesondere durch direkte Kommunikation mit diesen Adressen erfolgen (Bestätigungsmail).
- Sofern sich ein Zertifikat für die SSL-Verschlüsselung auf Servern eignet, wird bei allen im Zertifikat einzutragenden Domain Namen geprüft, ob der Antragsteller dessen Inhaber des Domainnamens ist, oder von diesem autorisiert wurde und die Kontrolle über diese besitzt. Bei allen einzutragenden IP-Adressen wird geprüft, ob der Antragsteller die Kontrolle über diese besitzt. Dies kann insbesondere durch eine direkte Kommunikation mit dem Inhaber der Domain bzw. der Adresse laut öffentlich zugänglicher Datenbanken erfolgen.
- Sofern sich ein Zertifikat für die SSL Verschlüsselung auf Servern eignet, wird dessen Inhalt mindestens alle 39 Monate auf dessen Aktualität und Korrektheit hin geprüft.

[7] Im Falle der Prüfung eines Antragstellers für ein EV-Zertifikat entsprechen die Dokumente und Informationsquellen jedenfalls den Anforderungen gemäß [WEBTRUST-EV] und [CABROWSER-EV]. Die Anforderungen sind intern dokumentiert und können auf Wunsch Aufsichtsbehörden vorgelegt werden.

4.2.1 Durchführung Identifikation und Authentifikation / Performing identification and authentication functions

Im Falle von fortgeschrittenen Signaturen, Amtssignaturen oder qualifizierten Zertifikaten erfolgt eine persönliche Identitätsfeststellung des Antragstellers durch den Betreiber oder eine vom Betreiber authorisierte Person oder eine Prüfstelle, die zur Identitätsfeststellung befugt ist, insbesondere Gerichte, Notare, Zustelldienste, die auch eine Identitätsprüfung bei der Übergabe von Dokumenten anbietet (in Österreich ist das insbesondere die POST AG) oder vergleichbare Einrichtungen.

In allen Fällen erfolgt die Identitätsfeststellung des Antragstellers
- durch Vorlage eines amtlichen Ausweises oder
- durch persönliche Bekanntheit mit dem Prüforgan (vom Betreiber authorisierte Person oder Mitarbeiter einer Prüfstelle), wobei sich das Prüforgan für die zweifelsfreie Identitätsfeststellung verbürgt, die Prüfung schriftlich dokumentiert und mit Unterschrift bestätigt.

Wenn die Prüfung von einer Prüfstelle vorgenommen wird, dann gilt sie als abgeschlossen, wenn die erforderliche Bestätigung unterfertigt und mit Prüfvermerk der Prüfstelle versehen an den Betreiber retourniert wurde.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen / Approval or rejection of certificate applications

Ein Zertifikat wird erst dann ausgestellt, wenn alle für den jeweiligen Zertifikatstyp notwendigen Prüfschritte erfolgreich abgeschlossen wurden.

Die Genehmigung von Anträgen auf EV-Zertifikaten erfolgt nach dem Vier-Augen-Prinzip.

Nach Prüfung der Antragsdaten werden sie
(a) entweder zur Zertifikatserstellung freigegeben oder
(b) der Antragsteller erhält den Auftrag weitere Unterlagen beizubringen oder
(c) der Antragsteller wird von der Ablehnung seines Antrags verständigt.

Kommt ein Antragsteller der Aufforderung zur Ergänzung der Unterlagen auch nach Mahnung nicht nach, dann wird der Antrag abgelehnt.

4.2.3 Fristen für die Bearbeitung von Zertifkatsanträgen / Time to process certificate applications

Zertifikatsanträge werden gemäß gesetzlicher Vorgaben, vertraglicher Vereinbarungen und den auf der Website zugesicherten Fristen bearbeitet.

4.3 Zertifikatsausstellung / Certificate issuance

Der ZDA stellt Zertifikate auf Basis eines geprüften und freigegebenen Antrags und des öffentlichen Schlüssels des Antragstellers aus.

Der Betreiber erstellt Zertifikate gemäß der jeweiligen Anzeige bei der Aufsichtsbehörde oder auf Grund der auf seiner Website veröffentlichten Produktbeschreibung. Insbesondere sind dies Zertifikate im X.509v3 Format.

Die Zertifikatserstellung erfolgt ausschließlich in einer gesicherten Umgebung durch vorgegebene Prozesse (Sicherheitsprofile und Konfigurationen), die vor der Zertifikatserstellung die Authentizität der Zertifikatsanforderung und die Integrität der freigegebenen Antragsdaten prüfen und gemäß der zutreffenden Certificate Policy ablaufen.

Aufbau und Inhalt der Zertifikate hat der jeweils anzuwendenden Certificate Policy zu entsprechen. Qualifizierte Zertifikate enthalten jedenfalls alle zur elektronischen Signatur erforderlichen und den Signator identifizierenden Angaben.

Die in diesem Abschnitt beschriebenen Abläufe für die Zertifikatsausstellung gelten sinngemäß auch für
- ⇨ 4.6 Neuaustellung Zertifikat / Certificate renewal (p42)
- ⇨ 4.7 Neuausstellung des Zertifikats mit Erzeugung eines neuen Schlüsselpaares / Certificate re-key (p43)
- ⇨ 4.8 Zertifikatsänderung / Certificate modification (p44)

4.3.1 Vorgehen des ZDA bei der Ausstellung von Zertifikaten / CA actions during certificate issuance

Die zur Zertifikatserstellung erforderlichen Prozesse (Sicherheitsprofile und Konfigurationen) werden von der gemäß ⇨ GLOBALTRUST® Certificate Security Policy zuständigen Stelle freigegeben.

Das Zertifikat wird mit Signaturprüfdaten des Betreibers versehen und ist von ihm elektronisch signiert. Die dafür verwendeten Signaturerstellungsdaten wurden gemäß den Anforderungen der [SigRL] und anderer rechtlicher und technischer Vorgaben erzeugt.

Die Formate der Zertifkate, insbesondere der qualifizierten Zertifikate sind in der jeweils anzuwendenden Certificate Policy definiert. Sofern keine eigene Definition erfolgt, gilt [RFC5280]. Qualifizierte Zertifikate enthalten jedenfalls die erforderlichen Angaben gemäß [SigRL] Anhang I und [ETSI TS 101 862].

Bei Ausstellung eines Zertifikates wird ein Protokoll erstellt. Das Protokoll kann Aufsichtstellen, Akkreditierungseinrichtungen oder sonstigen Prüfstellen bei Bedarf vorgelegt werden. Weiters werden alle ausstellungsrelevanten Schritte der Signator-Zertifikate, der zur Signatur vom Betreiber verwendeten Zertifikate und Schlüssel, der Cross-Zertifikate und der Zertifikate der Identifikations- und Infrastrukturschlüssel protokolliert .
Die Ausstellung eines EV-Zertifikates oder eines qualifizierten Zertifkates erfolgt stets durch das manuelle Ausführen eines Befehls durch eine autorisierte Person.

Die Übergabe der zur Zertifizierung erforderlichen Daten an das Zertifizierungssystem erfolgt über gesicherte Pfade. Dabei wird die Vertraulichkeit und die Integrität der Informationen sicher gestellt. Als gesicherte Pfade gelten insbesondere die Verwendung ausschließlich für den Zweck der Übergabe vorgesehene externe Datenträger, dedizierte

VPN-Tunnel zwischen administrativem System und Zertifizierungssystem oder durch vergleichbare, dem Stand der Technik entsprechende Maßnahmen. Die Anforderung von Zertifikaten wird elektronisch signiert.

Alle Zertifikate werden mit einem privaten Schlüssel des ZDA signiert. Mit einem Root-Zertifikat werden ausschließlich CA-Zertifikate, Cross-Zertifikate, Zertifikate für Infrastrukturaufgaben oder interne Zertifikate ausgestellt.

4.3.2 Benachrichtigung des Signators über die Ausstellung des Zertifikats / Notification to subscriber by the CA of issuance of certificate

Der Signator wird nach Ausstellung des Zertifikates unverzüglich in geeigneter Form informiert.

In geeigneter Form erfolgt die Information insbesondere
- durch Verständigung per E-Mail (sofern eine Adresse im Antrag angegeben wurde oder auf Grund einer früheren Geschäftsbeziehung bekannt ist) oder
- durch Zustellung eines Briefes oder Faxes oder
- durch telefonische oder persönliche Mitteilung.

Es ist zulässig mehrere Verständigungsformen parallel zu wählen.

In keinem Fall enthält die Verständigung geheime Informationen, die für sich allein genommen die Nutzung eines Zertifikates erlauben.

4.4 Zertifikatsannahme / Certificate acceptance

Der Signator hat die Annahme des Zertifikates und der dazugehörigen Nutzungsbestimmungen, insbesondere diese GLOBALTRUST® Certificate Policy und das zugehörige GLOBALTRUST® Certificate Practice Statement zu bestätigen.

4.4.1 Verfahren zur Zertifikatsannahme / Conduct constituting certificate acceptance

Die Bestätigung der Zertifikatsannahme erfolgt schriftlich oder elektronisch, jedenfalls in Übereinstimmung mit gesetzlichen Vorgaben.

4.4.2 Veröffentlichung der Zertifikate / Publication of the certificate by the CA

Die erforderlichen Prüfdaten, wie insbesondere öffentliche Signaturschlüssel, Hash-Werte, weitere Angaben zum Betreiber werden auf der Website des Betreibers oder im anzuwendenden GLOBALTRUST® Certificate Practice Statement genannten Link veröffentlicht. Jedes ausgestellte Zertifikat enthält einen Verweis auf eine öffentlich zugängliche Stelle über die diese Prüfdaten abgerufen oder angefordert werden können.

4.4.3 Benachrichtigung von Dritten über die Zertifikatsaustellung / Notification of certificate issuance by the CA to other entities

Sonstige Einrichtungen werden vom Betreiber unverzüglich benachrichtigt,
- sofern ein ausgestelltes Zertifikat Auswirkungen auf ihre Tätigkeit hat oder
- es vertraglich vereinbart ist oder

- sonstige rechtliche Bestimmungen die Benachrichtigung erfordern.

4.5 Schlüsselpaar und Zertifikatsnutzung / Key pair and certificate usage

4.5.1 Nutzung des privaten Schlüssels und des Zertifikates durch den Signator / Subscriber private key and certificate usage

Der ZDA bindet den Signator vertraglich an die Einhaltung der nachfolgend angeführten Verpflichtungen.

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:

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 ZDA 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 Zertifikate, 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 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.
14. 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.
15. 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.

Sub-Zertifikate, bei denen der private Schlüssel unter Kontrolle des Signators ist, haben zu den unter ⇨ 7.1.2 Zertifikatserweiterungen / Certificate extensions (p91) genannten Einschränkungen nachstehende zusätzliche Bedingungen zu erfüllen.

Solche Zertifikate enthalten als Policy-Eintrag eine OID-Nummer mit der angezeigt wird, dass der Nutzer die Bestimmungen und Policies Dritter einhält, mit denen der ZDA Vereinbarungen zur Vorabanerkennung der CA-Zertifikate abgeschlossen hat, jedenfalls sind dies die Bestimmungen [CABROWSER-BASE] und [MS-CA]. In diesem Dokument legt der Signator außerdem seine EV-Policy dar (entweder die Erklärung keine derartigen Zertifikate auszustellen oder die Erklärung die Bestimmungen von [CABROWSER-EV] einzuhalten) . Darüber hinaus ist im Zertifikat keinenfalls ein Eintrag im Sinne "beliebige Policy" vorhanden, insbesondere ist bei x.509v3-Zertifikaten kein anyPolicy Eintrag vorgesehen.

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.

Ergänzende Bestimmungen bei Einsatz auslesbarer Datenträger für private Schlüssel:
Soweit der private Schlüssel in auslesbaren Datenträgern gespeichert ist (Diskette, USB-Stick, Festplatte usw.), verpflichtet sich der Signator zur getrennten Verwahrung erforderlicher Passwörter und zur besonders sorgfältigen Verwahrung des Datenträgers. Bei transportablen Datenträgern (Diskette, USB-Stick, CD, ...) erfolgt die Aufbewahrung in verschlossenen, nur für den Signator zugänglichen Behältern, bei fix eingebauten Datenträgern (Festplatten) ist die Verwendung auf den Signator beschränkt. Systemadministratoren sind vertraglich zur Sicherung der Vertraulichkeit des privaten Schlüssels zu verpflichten. Es ist sicherzustellen, dass nur vom Signator veranlasste Kopien erstellt werden (gilt auch für Backupkopien).

Weiters stellt der Signator nach dem Stand der Technik sicher, dass der verwendete Datenträger frei von Schadprogrammen ist, die den privaten Schlüssel auslesen, kopieren oder sonstwie verändern können. Insbesondere unternimmt der Signator ausreichende Schutzmaßnahmen gegen Malware jeglicher Art, insbesondere Viren, Würmer, Programme mit Trapdoorfunktionen und Spyware-Programme, die den privaten Schlüssel, das Zertifikat oder einen sonstigen Teil eines Signaturvorganges beeinträchtigen können.

4.5.2 Nutzung des öffentlichen Schlüssels und des Zertifikates durch Nutzer / Relying party public key and certificate usage

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 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.

4.6 Neuaustellung Zertifikat / Certificate renewal

Der ZDA stellt Zertifikate im Zuge der Neuausstellung eines Zertifikat auf Basis eines geprüften und freigegebenen Antrags und des öffentlichen Schlüssels des Antragstellers aus.

Ein bestehendes Zertifikat wird nicht verlängert, es ist jedoch zulässig zu einem bestehenden Schlüssel bzw. zu einem bestehenden CSR (Certificate Signing Request) ein neues Zertifikat mit neuer Laufzeit und neuen Zertifikatsangaben zu machen, sofern die verwendeten Algorithmen noch dem aktuellen technischen Standard entsprechen.

4.6.1 Umstände für Neuaustellung eines Zertifikats / Circumstance for certificate renewal

Eine Neuausstellung eines Zertifikates ist zulässig, wenn
- die Art des Zertifikates es rechtlich zulässt und
- keine individuellen Gründe gegen eine Neuausstellung sprechen.

4.6.2 Berechtigte für Antrag auf Neuaustellung Zertifikat / Who may request renewal

Für einen Antrag auf Neuausstellung ist der ursprüngliche Antragsteller berechtigt.

4.6.3 Bearbeitung eines Antrags auf Neuausstellung Zertifikat / Processing certificate renewal requests

Durch folgende Maßnahmen wird sicher gestellt, dass Anträge von Antragstellern, die anlässlich einer vorhergehenden Zertifikatsausstellung bereits registriert wurden, vollständig, korrekt und ordnungsgemäß autorisiert sind:
- Die Registrierungsstelle prüft die im Zertifikat enthaltenen Daten hinsichtlich ihrer aktuellen Gültigkeit.
- Allfällige Änderungen in der vorliegenden Policy, in den Geschäftsbedingungen und in den sonstigen Vereinbarungen werden zur Kenntnis gebracht.

Informationen für Serverzertifikate dürfen ohne neuerliche Prüfung wiederverwendet werden, sofern sie nicht älter als 39 Monate sind.

Der ZDA führt Zertifikatsneuausstellung mit Beibehaltung des Schlüsselpaares auf Basis eines geprüften und freigegebenen Antrags und des öffentlichen Schlüssels des Antragstellers aus.

4.6.4 Benachrichtigung des Signators über die Neuausstellung Zertifikat / Notification of new certificate issuance to subscriber

Die Benachrichtigung der Neuausstellung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.3.2 Benachrichtigung des Signators über die Ausstellung des Zertifikats / Notification to subscriber by the CA of issuance of certificate (p38).

4.6.5 Verfahren zur Annahme nach Neuausstellung Zertifikat / Conduct constituting acceptance of a renewal certificate

Das Verfahren zur Zertifikatsannahme nach Neuausstellung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.4.1 Verfahren zur Zertifikatsannahme / Conduct constituting certificate acceptance (p38).

4.6.6 Veröffentlichung der Neuausstellung Zertifikat durch ZDA / Publication of the renewal certificate by the CA

Die Veröffentlichung der Neuausstellung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.4.2 Veröffentlichung der Zertifikate / Publication of the certificate by the CA (p38).

4.6.7 Benachrichtigung von Dritten über die Ausstellung eines Zertifikates / Notification of certificate issuance by the CA to other entities

Die Benachrichtigung der Neuausstellung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.4.3 Benachrichtigung von Dritten über die Zertifikatsaustellung / Notification of certificate issuance by the CA to other entities (p38).

4.7 Neuausstellung des Zertifikats mit Erzeugung eines neuen Schlüsselpaares / Certificate re-key

Zertifikatsneuausstellung mit Erzeugung eines neuen Schlüsselpaares unterliegen denselben Verfahren und Beschränkungen wie ⇨ 4.6 Neuaustellung Zertifikat / Certificate renewal (p42).

4.7.1 Umstände für Neuausstellung Zertifikat mit Erzeugung eines neuen Schlüsselpaares / Circumstance for certificate re-key

Eine Neuausstellung eines Zertifikates mit Erzeugung eines neuen Schlüsselpaares ist zulässig, wenn

- die Art des Zertifikates es rechtlich zulässt und
- keine individuellen Gründe gegen eine Neuausstellung sprechen.

4.7.2 Berechtigte für Antrag auf Neuaustellung Zertifikat mit Erzeugung eines neuen Schlüsselpaares / Who may request certification of a new public key

Für einen Antrag auf Neuausstellung ist der Signator berechtigt.

4.7.3 Bearbeitung eines Antrags auf Neuausstellung Zertifikat mit Erzeugung eines neuen Schlüsselpaares / Processing certificate re-keying requests

Die Bearbeitung eines Antrag auf Neuausstellung mit Erzeugung eines neuen Schlüsselpaares unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6.3

Bearbeitung eines Antrags auf Neuausstellung Zertifikat / Processing certificate renewal requests (p42).

4.7.4 Benachrichtigung über die Neuausstellung Zertifikat mit Erzeugung eines neuen Schlüsselpaares / Notification of new certificate issuance to subscriber

Die Benachrichtigung der Neuausstellung eines Zertifikates mit Erzeugung eines neuen Schlüsselpaares unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6.4 Benachrichtigung des Signators über die Neuausstellung Zertifikat / Notification of new certificate issuance to subscriber (p42).

4.7.5 Verfahren zur Zertifikatsannahme nach Neuausstellung Zertifikat mit Erzeugung eines neuen Schlüsselpaares / Conduct constituting acceptance of a re-keyed certificate

Das Verfahren zur Zertifikatsannahme nach Neuausstellung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6.5Verfahren zur Annahme nach Neuausstellung Zertifikat / Conduct constituting acceptance of a renewal certificate (p43).

4.7.6 Veröffentlichung der Neuausstellung Zertifikat mit Erzeugung eines neuen Schlüsselpaares durch ZDA / Publication of the re-keyed certificate by the CA

Die Veröffentlichung der Neuausstellung mit Erzeugung eines neuen Schlüsselpaares unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6.6 Veröffentlichung der Neuausstellung Zertifikat durch ZDA / Publication of the renewal certificate by the CA (p43).

4.7.7 Benachrichtigung von Dritten über Neuausstellung Zertifikat mit Erzeugung eines neuen Schlüsselpaares / Notification of certificate issuance by the CA to other entities

Die Benachrichtigung der Neuausstellung mit Erzeugung eines neuen Schlüsselpaares unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6.7 Benachrichtigung von Dritten über die Ausstellung eines Zertifikates / Notification of certificate issuance by the CA to other entities (p43).

4.8 Zertifikatsänderung / Certificate modification

Zertifikatsänderungen unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6 Neuaustellung Zertifikat / Certificate renewal (p42)

4.8.1 Umstände für Zertifikatsänderung / Circumstance for certificate modification

Eine Zertifikatsänderung ist zulässig, wenn
- die Art des Zertifikates es rechtlich zulässt und
- keine individuellen Gründe gegen eine Neuausstellung sprechen.

4.8.2 Berechtigte für Antrag auf Zertifikatsänderung / Who may request certificate modification

Für einen Antrag auf Änderung ist der Signator und vertretungsbefugte Personen jenes Unternehmens berechtigt, das im Zertifikat eingetragen ist.

4.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung / Processing certificate modification requests

Zertifikatsänderungen unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6.3 Bearbeitung eines Antrags auf Neuausstellung Zertifikat / Processing certificate renewal requests (p42)

Ergänzend gilt: Geänderte Daten werden genauso geprüft, wie bei neuen Zertifikatsanträgen.

4.8.4 Benachrichtigung über die Zertifikatsänderung / Notification of new certificate issuance to subscriber

Die Benachrichtigung der Zertifikatsänderung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.3.2 Benachrichtigung des Signators über die Ausstellung des Zertifikats / Notification to subscriber by the CA of issuance of certificate (p38).

4.8.5 Verfahren zur Zertifikatsannahme nach Zertifikatsänderung / Conduct constituting acceptance of modified certificate

Das Verfahren zur Zertifikatsannahme nach Zertifikatsänderung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.4.1 Verfahren zur Zertifikatsannahme / Conduct constituting certificate acceptance (p38).

4.8.6 Veröffentlichung der Zertifikatsänderung / Publication of the modified certificate by the CA

Die Veröffentlichung der Zertifikatsänderung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.4.2 Veröffentlichung der Zertifikate / Publication of the certificate by the CA (p38).

4.8.7 Benachrichtigung über die Zertifikatsänderung / Notification of certificate issuance by the CA to other entities

Die Benachrichtigung der Zertifikatsänderung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.4.3 Benachrichtigung von Dritten über die Zertifikatsaustellung / Notification of certificate issuance by the CA to other entities (p38).

4.9 Zertifikatswiderruf und -sperre / Certificate revocation and suspension

Um eine möglichst praxisnahe Nutzung der Zertifikate zu gewährleisten, wird ein zweistufiges Widerrufskonzept angewandt:

- Aussetzung der Gültigkeit eines Zertifikates (Sperre)
- ungültig Erklären eines Zertifikates (Widerruf)

Sperr- und Widerrufsantrag haben auf den bekannt gegebenen Kanälen zu erfolgen und der Signator hat sich zu vergewissern, dass der Antrag auch tatsächlich eingelangt ist.

Der ZDA stellt folgende Möglichkeiten zur Verfügung:

(a) Sperre
Die Gültigkeit eines Zertifikates wird vorläufig aussetzt, kann manuell oder automatisiert ausgelöst werden und ist maximal für die rechtlich und technisch zulässige Dauer gültig ist

(b) Widerruf
Erfordert jedenfalls eine Autorisierung auf Grundlage der vorgegebenen Rollenverteilung (⇨ GLOBALTRUST® Certificate Security Policy) erfordert, führt zum vorzeitigen ungültig Erklären eines Zertifikates.

Ein Widerruf führt zur vorzeitigen Beendigung der Gültigkeit eines Zertifikats, eine Re-Aktivierung ist ausgeschlossen. Der Widerruf erfolgt unter Kontrolle von zumindest zwei Personen gemäß dem in ⇨ GLOBALTRUST® Certificate Security Policy definierten Rollenkonzept.

Zertifikatssperren können in einer eigenen Sperrliste eingetragen werden. Die Sperre informiert über eine mögliche Kompromittierung eines Zertifikates. Eine Sperre kann aufgehoben werden. Der Signator wird über das Einlangen der Zertifikatssperre verständigt und um Bestätigung oder Aufhebung der Sperre ersucht.

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

Die Tatsache der Sperre oder des Widerrufs eines Zertifkates ist öffentlich verfügbar.

Bei Server-Zertifikaten ist eine Sperre nicht möglich.

Es existiert außerdem die Möglichkeit für Dritte, vermutete Probleme oder den Missbrauch von Zertifikaten zu melden. Der ZDA wird diesen Hinweisen nachgehen und bei Bedarf die entsprechenden Zertifkate widerrufen oder sperren.

Wenn ein Ereignis, das einen Widerruf erforderlich machen kann, noch nicht abschliessend geprüft ist, hat ein Antrag auf Sperre des Zertifikates zu erfolgen.

Bei Widerruf eines Zertifikates wird ein Widerrufsprotokoll erstellt (⇨ Anhang A: 2 Inhalt Ausstellungs-, Sperr-, Entsperr- und Widerrufs-Protokoll für Zertifikate (p124). Das Widerrufsprotokoll kann Aufsichtstellen, Akkreditierungseinrichtungen oder sonstigen befugten Prüfstellen bei Bedarf vorgelegt werden. Weiters werden alle widerrufsrelevanten Schritte der Signator-Zertifikate, der zur Signatur vom ZDA verwendeten Zertifikate und Schlüssel, der Cross-Zertifikate und der Zertifikate der Identifikations- und Infrastrukturschlüssel protokolliert.

Signatoren werden über Sperre oder Widerruf ihres Zertifikates in geeigneter Form verständigt. Geeignet ist insbesondere die Information an eine geprüfte E-Mail-Adresse, die der Signator selbst bekannt gegeben hat und die nicht als ungültig dokumentiert ist, eine telefonische Information an eine vom Signator bekannt gegebene Telefonnummer oder eine Verständigung per Fax, sofern die Faxnummer vom Signator bekannt gegeben wurde. In allen anderen Fällen erfolgt eine Verständigung auf dem Postweg.

4.9.1 Umstände für Zertifikatswiderruf / Circumstances for revocation

Ein Zertifikat ist zu widerrufen, wenn die weitere Verwendung des Schlüssels im Sinne dieser Policy ist nicht mehr gewährleistet ist.

Widerrufsgründe sind jedenfalls:
1. Der Signator oder der Antragsteller stellt einen schriftlichen Antrag.
2. Eine Verständigung vom Antragsteller, dass der ursprüngliche Zertifikatsantrag nicht hinreichend autorisiert war und er diese Autorisierung nicht nachträglich erteilt.
3. Der Betreiber erhält einen Beweis, dass der verwendete private Schlüssel kompromittiert wurde oder nicht mehr den aktuellen technischen Anforderungen entspricht.
4. Der Betreiber erhält einen Beweis, dass das Zertifikat missbräuclich verwendet wurde
5. Der Betreiber erhält Kenntnis davon, dass der Signator die Nutzungsbedingungen, die Certifcate Policy, das Certificate Practice Statement oder eine sonstige vertragliche Vereinbarung verletzt hat.
6. Der Betreiber erhält Kenntnis darüber, dass der Signator nicht länger rechtlich befugt ist, eine im Zertifikat eingetragene Bezeichnung, insbesondere ein Domainname oder eine IP-Adresse, zu verwenden.
7. Der Betreiber erhält Kenntnis davon, dass ein Wildcardzertifikat dazu verwendete wurde um eine Subdomain in betrügerisch täuschender Absicht zu authentifizieren.
8. Der Betreiber erhält Kenntnis von einer signifikanten Änderung bezüglich der im Zertifkat eingetragenen Informationen.
9. Der Betreiber stellt fest, dass eine im Zertifikat eingetragen Information ungenau oder täuschend ist.
10. Der ZDA stellt seinen Betrieb ein, und hat mit keinem anderen Betreiber eine Vereinbarung zu einer Fortführung geschlossen.
11. Der Betreiber verliert das Recht, den jeweiligen Zertifikatstyp auszustellen, außer er er hat eine Vereinbarung geschlossen, den Widerrufsstatusdienst fortzuführen.
12. Der Betreiber erhält einen Beweis, dass der verwendete private Schlüssel des CA-Zertifikates kompromittiert wurde.
13. Es werden Gründe bekannt, die den technischen Inhalt oder das Format des Zertifikates zu einem inakzeptablen Sicherheitsrisiko machen.
14. Der Betreiber hat qualifizierte Hinweise auf eine vertragswidrige Verwendung eines Zertifikats durch den Signator. Vertragswidrige Verwendung sind insbesondere Verstöße gegen diese Policy, gegen das GLOBALTRUST® Certificate Practice Statement, gegen die vereinbarten AGBs oder sonstigen individuellen Vereinbarungen (inkl. Leistungs- und Zahlungsverpflichtungen).

Der Signator akzeptiert, dass der Betreiber 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.

Zertifikate zu Schlüsseln, die mit Verfahren erstellt werden, die gemäß gesetzlicher Bestimmungen, insbesondere Signaturverordnung ([SIGV])oder der Entscheidung der Aufsichtsstelle oder anerkannter Standardisierungsgremien (insbesondere gemäß den speziellen Empfehlungen [ETSI TS 102 176]) oder auf Grund interner Erkenntnisse als nicht

mehr sicher anzusehen sind, werden vom Betreiber widerrufen und alle betroffenen Parteien darüber in Kenntnis gesetzt.

Der Betreiber hat das Recht ein Zertifikat jederzeit aus organisatorischen oder technischen Gründen zu widerrufen. Erfolgt ein derartiger Widerruf aus Gründen die der Signator nicht zu verantworten hat und vor Ablauf der vertraglich vereinbarten Gültigkeitsdauer des Zertifikats, dann hat der Signator für die Dauer der vertraglich vereinbarten Restlaufzeit Anspruch auf Ausstellung eines gleichwertigen, mit sicheren Verfahren hergestellten Zertifikats. Sonstige Entschädigungen oder Kostenersätze sind nicht vorgesehen.

Ein Sub-Zertifikat wird jedenfalls nach spätestens 7 Tagen widerrufen wenn eines der folgenden Kriterien erfüllt ist:
1. Schriftlicher Antrag des Antragstellers.
2. Eine Verständigung vom Antragsteller, dass der ursprüngliche Zertifikatsantrag nicht hinreichend autorisiert war und er diese Autorisierung nicht nachträglich erteilt.
3. Der Betreiber erhält einen glaubhaften Hinweis, dass der verwendete private Schlüssel kompromittiert wurde oder nicht mehr den aktuellen technischen Anforderungen entspricht.
4. Der Betreiber erhält einen Beweis, dass das Zertifikat missbräuchlich verwendet wurde.
5. Der Betreiber erhält Kenntnis davon, dass der Signator die Nutzungsbedingungen, die Certifcate Policy, das Certificate Practice Statement, die Vereinbarung zur Verwendung des Sub-Zertifikates, einen vorgeschriebenen technischen Standard (insbesondere [CABROWSER-BASE]) oder eine sonstige vertragliche Vereinbarung verletzt hat.
6. Der ZDA stellt fest, dass eine im Zertifikat eingetragen Information fehlerhaft, ungenau oder täuschend ist.
7. Der Betreiber des Sub-Zertifikates stellt seine operative Tätigkeit ein, und hat keine Vorkehrungen für eine Übernahme der Tätigkeit getroffen.
8. Die Vereinbarung mit dem Betreiber dass dieser das Sub-Zertifikat zur Ausstellung von Zertifikaten verwenden darf ist abgelaufen, außer es besteht eine Zusatzvereinbarung, dass der Widerrufsdienst weiterhin betrieben wird.
9. Ein sonstiger Punkt dieser Certificate Policy bzw. des GLOBALTRUST® Certificate Practice Statements verlangt den Widerruf.
10. Es werden Gründe bekannt, die den technischen Inhalt oder das Format des Zertifikates zu einem inakzeptablen Sicherheitsrisiko machen.

4.9.2 Berechtigte für Antrag auf Widerruf / Who can request revocation

Zum Widerruf und zur Zertifikatssperre berechtigt sind folgende Stellen:
- der Signator,
- der Antragsteller,
- für die Fälle, bei denen der Signator in Vertretung einer anderen Person oder einer Organisation handelt und das Zertifikat zu diesem Zweck ausgestellt ist, diese Person bzw. ein ausgewiesener Vertreter der Organisation,
- der Betreiber, gemäß den Bedingungen ⇨ 4.9.1 Umstände für Zertifikatswiderruf / Circumstances for revocation (p46),
- sonstige Aufsichts- und Kontrollstellen, sofern dies auf Grund zwingender Bestimmungen erforderlich ist.

Wird ein Widerruf von einer anderen Stelle als dem Betreiber beantragt, ist zwingend eine vollständige Identitätsprüfung und Prüfung der Widerrufsberechtigung erforderlich.

4.9.3 Stellung eines Widerrufantrages / Procedure for revocation request

Ein Widerrufsantrag kann formlos telefonisch, per Fax, per E-Mail, schriftlich (⇨ Kontakt-Daten: http://www.globaltrust.eu/impressum.html) oder über die Website (⇨ Sperre oder Widerruf: http://www.globaltrust.eu/revocation.html) unter Angabe geeigneter Zertifikatsangaben und Kennzeichen (Produktbezeichnung, Seriennummer, Fingerprint, ...), die das Zertifikat eindeutig identifizieren und eines ausreichenden Nachweises der Berechtigung eingebracht werden.

Der ZDA behält sich vor bei Zweifel der Berechtigung weitere Nachweise zu verlangen und stattdessen nur eine Sperre durchzuführen.

Sofern der berechtigte Antragsteller es wünscht, kann sofort der Widerruf durchgeführt werden.

4.9.4 Informationsfrist für Antragstellung auf Widerruf / Revocation request grace period

Liegen einer natürlichen oder juristischen Person laut ⇨ 4.9.2 Berechtigte für Antrag auf Widerruf / Who can request revocation (p48) Informationen vor, die einen Widerruf gemäß einem der in⇨ 4.9.1 Umstände für Zertifikatswiderruf / Circumstances for revocation (p47) angeführten Gründe zur Folge haben kann, so sind diese dem Betreiber bei qualifizierten Zertifikaten unverzüglich, bei allen anderen Zertifikatsformen so rasch als möglich (jedenfalls binnen 72 Stunden) zu belegen. Davon unabhängig ist die Sperre, die ohne Begründung jederzeit beantragt werden kann.

4.9.5 Reaktionszeit des ZDAs auf einen Widerrufsantrag / Time within which CA must process the revocation request

Anträge per Telefon, Fax, Post und E-Mail werden während der Bürozeiten entgegen genommen und bearbeitet und unverzüglich nach Abschluss aller erforderlichen Prüfungen durchgeführt.

Widerrufsanträge via Webinterface werden rund um die Uhr entgegen genommen.

Die maximal zulässige Zeitdauer zwischen Einlangen des Widerrufs bzw. der Sperre und der Durchführung richtet sich nach den aktuellen gesetzlichen Bestimmungen, ist aber jedenfalls kleiner als 24 Stunden.

Im Falle qualifizierter Zertifikate erfolgt die Aktualisierung der Widerrufsdienste an Werktagen, ausgenommen Samstag, von 9 bis 17 Uhr spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes. Außerhalb dieser Zeit erfolgt die Sperre jedenfallsinnerhalb von sechs Stunden.

Kann der Antragsteller in der Zeit zwischen Antragstellung und maximal zulässiger Reaktionszeit keine ausreichenden Angaben zu seiner zuverlässigen Identifizierung und Widerrufsberechtigung machen, dann wird der Widerruf abgelehnt und eine Sperre durchgeführt.

Der Antragsteller hat für die maximal zulässige Dauer der Sperre (⇨ **(a) Sperre**, p46) Gelegenheit ausreichende Angaben zu seiner zuverlässigen Identifizierung und

Widerrufsberechtigung vorzulegen. Ist das innerhalb dieser Zeit nicht möglich, erfolgt die Aufhebung der Sperre.

Bei der Abarbeitung von Widerrufs- und Sperranträgen können einzelne Fälle aufgrund des ihnen zugrunde liegenden Risikos prioritär behandelt werden. Im Falle eines Hinweises auf strafbare Handlungen, können die zuständigen Behörden verständigt werden.

Eine Bestätigung des Einlangens kann automatisiert unverzüglich oder manuell im Zuge der nächsten Bürozeiten erfolgen. Im Zweifel hat der Signator seinen Sperr- oder Widerrufsantrag zu wiederholen. Die Bestätigung des Einlangens ist jedoch keine Bestätigung der tatsächlichen Durchführung. Die Bestätigung der Durchführung eines Widerrufsantrags kann manuell beim ZDA während der dem Antrag folgenden Bürostunden eingeholt werden oder ist automatisiert als Eintrag in der entsprechenden Widerrufsliste ablesbar. Die Bestätigung der Ablehnung eines Widerrufsantrags bedarf immer eine Prüfung durch autorisiertes Personal und erfolgt während der dem Antrag folgenden Bürostunden.

4.9.6 Verpflichtung der Nutzer zur Widerrufsprüfung / Revocation checking requirement for relying parties

Widerrufene (bzw. gesperrte) Zertifikate können anhand der jeweils vorgesehenen Sperr- bzw. Widerrufsliste(n) validiert werden.

Sorgfältige Überprüfung der Gültigkeit des Zertifikates mittels des Sperr- und Widerrufsstatus unter Verwendung der vom ZDA bereitgestellten Abfragemöglichkeiten ist im Rahmen der durch den Nutzer durchgeführten Prüfung (⇨ 4.5.2 Nutzung des öffentlichen Schlüssels und des Zertifikates durch Nutzer / Relying party public key and certificate usage, p41) obligatorisch.

4.9.7 Frequenz der CRL-Erstellung / CRL issuance frequency (if applicable)

Die Aktualisierung der Sperr- bzw. Widerrufslisten (CRL, Certificate Revokation List) erfolgt gemäß technischer Standards, rechtlicher Vorgaben, des GLOBALTRUST® Certificate Practice Statement, der anzuwendenden Certificate Policy, jedenfalls bei einer Sperre bzw. Widerruf eines Zertifikates. Im Falle widersprüchlicher Bestimmungen erfolgt die Aktualisierung gemäß der kürzesten erforderlichen Zeit .
Die Sperrlisten oder die Delta-Widerrufslisten (sofern vorhanden) werden - sofern technisch oder rechtlich erforderlich - auf täglicher Basis oder öfter erstellt. Der Inhalt der Delta-Widerrufslisten ist im Regelfall leer und dient zur Dokumentation der Aktualität der CRL.

Sperr- und Widerrufslisten werden im Falle einer Sperre oder eines Widerrufs von qualifizierten Zertifikaten sofort nach Abschluss von Sperre oder Widerruf aktualisiert. Dies führt auch zur sofortigen Aktualisierung der OCSP[8]-Antworten.

Bei Server- und EV-Zertifikaten beträgt die maximale Gültigkeitsdauer der Widerrufs- bzw. Sperrliste 10 Tage (wobei eine Aktualisierung mindestens alle 7 Tage erfolgt), die von OCSP-Antworten 10 Tage (wobei die zu Grunde liegenden Daten mindestens alle 4 Tage aktualisiert werden).

---

[8] OCSP = Online Certificate Status Protocol

Bei CA-Zertifikaten die EV-Zertifikate ausstellen beträgt die maximale Gültigkeitsdauer der Widerrufs- bzw. Sperrliste 12 Monate, eine Aktualisierung erfolgt in diesem Zeitraum jedenfalls aber nicht mehr als 24 Stunden nach einem durchgeführtem Widerruf. Die OCSP-Antworten für solche Zertifikate zu Grunde liegenden Daten werden mindestens alle 12 Monate aktualisiert, jedenfalls aber nicht später als 24 Stunden nach einem durchgeführten Widerruf.

Informationen über widerrufene Zertifikate bleiben zumindest bis zum Zeitpunkt des regulären Endes des Zertifkates bestehen.

4.9.8 Maximale Verzögerung der Veröffentlichung der CRLs / Maximum latency for CRLs (if applicable)

Die über das Internet abrufbaren Sperr- und Widerrufslisten werden nach jeder Sperre bzw. Widerruf aktualisiert.

4.9.9 Möglichkeit der online Widerrufsprüfung / On-line revocation/status checking availability

Die Verzeichnisdienste für Sperr- und Widerrufslisten sind öffentlich und international zugänglich. Eine Veröffentlichungssperre von widerrufenen oder gesperrten Zertifikaten ist nicht möglich.

4.9.10 Voraussetzungen für die online Widerrufsprüfung / On-line revocation checking requirements

Es wird sichergestellt, dass die gesamte Widerrufslisten Kette für EV-Zertifikate bei Normalbedingungen über eine analoge Telefonleitung in höchstens 3 Sekunden heruntergeladen werden kann. Die Antwortzeiten für CRL- und OCSP-Anfragen bleiben im Normalfall unter 10 Sekunden.

4.9.11 Andere verfügbare Widerrufsdienste / Other forms of revocation advertisements available

Der Betreiber behält sich vor - soweit technisch möglich und rechtlich zulässig - weitere Widerrufsdienste bereit zu stellen. Diese werden über die Website des Betreibers angekündigt.

Im Falle qualifizierter Zertifikate kann der aktuelle Status eines Zertifikates jedenfalls mittels OCSP abgefragt werden.

Unabhängig von der technischen Verfügbarkeit von Widerrufsdiensten kann der Nutzer den aktuellen Status eines ausgestellten Zertifikates beim Betreiber erfragen.

4.9.12 Spezielle Anforderung bei Kompromittierung des privaten Schlüssels / Special requirements re key compromise

Besteht der Verdacht der Komprimitierung des privaten Schlüssels ist dies unverzüglich dem ZDA zu melden. Widerrufe auf Grund der Komprimitierung des privaten Schlüssels werden bevorzugt behandelt.

4.9.13 Umstände für Zertifikatssperre / Circumstances for suspension

Gründe für eine Sperre sind jedenfalls:
1. Der Signator oder der Antragsteller stellt einen schriftlichen Antrag.
2. Eine Verständigung vom Antragsteller, dass der ursprüngliche Zertifikatsantrag nicht hinreichend autorisiert war und er diese Autorisierung nicht nachträglich erteilt.
3. Der Betreiber erhält einen Hinweis, dass der verwendete private Schlüssel kompromittiert wurde oder nicht mehr den aktuellen technischen Anforderungen entspricht.
4. Der Betreiber erhält einen Hinweis, dass das Zertifikat missbräuclich verwendet wurde.
5. Der Betreiber erhält einen Hinweis, dass der Signator die Nutzungsbedingungen, die Certifcate Policy, das Certificate Practice Statement oder eine sonstige vertragliche Vereinbarung verletzt hat.
6. Der Betreiber erhält einen Hinweis, dass der Signator nicht länger rechtlich befugt ist, eine im Zertifikat eingetragene Bezeichnung, insbesondere ein Domainname oder eine IP-Adresse, zu verwenden.
7. Der Betreiber erhält einen Hinweis, dass ein Wildcardzertifikat dazu verwendete wurde um eine Subdomain in betrügerisch täuschender Absicht zu autentifizieren.
8. Der Betreiber erhält einen Hinweis von einer signifikanten Änderung bezüglich der im Zertifkat eingetragenen Informationen.
9. Der Betreiber hat die Vermutung, dass eine im Zertifikat eingetragen Information ungenau oder täuschend ist.
10. Der Betreiber erhält einen Hinweis, dass der verwendete private Schlüssel des CA-Zertifikates kompromittiert wurde.
11. Der Betreiber hat Hinweise auf eine vertragswidrige Verwendung eines Zertifikats durch den Signator hat. Vertragswidrige Verwendung sind insbesondere Verstöße gegen diese Policy, gegen das GLOBALTRUST® Certificate Practice Statement, gegen die vereinbarten AGBs oder sonstigen individuellen Vereinbarungen (inkl. Leistungs- und Zahlungsverpflichtungen).

4.9.14 Berechtigte für Antrag auf Sperre / Who can request suspension

Zur Zertifikatssperre berechtigt sind folgende Stellen:
- der Signator oder der Antragsteller
- für die Fälle, bei denen der Signator in Vertretung einer anderen Person oder einer Organisation handelt und das Zertifikat zu diesem Zweck ausgestellt ist, diese Person bzw. ein ausgewiesener Vertreter der Organisation,
- der Betreiber, gemäß den Bedingungen ⇨ 4.9.1 Umstände für Zertifikatswiderruf / Circumstances for revocation (p47),
- sonstige Aufsichts- und Kontrollstellen, sofern dies auf Grund zwingender Bestimmungen rechtlich erforderlich ist.

4.9.15 Stellung eines Antrages auf Sperre / Procedure for suspension request

Ein Sperrantrag kann formlos unter Angabe geeigneter Zertifikatsangaben und Kennzeichen (Produktbezeichnung, Seriennummer, Fingerprint, ...) und einer glaubhaft Machung der Berechtigung eingebracht werden.

Sperranträge die via Webinterface einlangen werden - sofern ausreichend spezifiziert und eine eindeutige Zuordnung des Antragstellers und des betroffenen Zertifikates möglich ist - sofort automatisiert bearbeitet (ansonsten werden sie wie E-Mails behandelt).

Eine Zertifikatssperre wird nach Einlangen des Sperrantrags automatisiert wirksam. Eine Identitätsprüfung kann in diesem Fall auch automatisiert, etwa unter Verwendung von Zugangsdaten, die vom ZDA vergeben wurden oder von Daten, die üblicherweise nur dem Signator bekannt und/oder zugänglich sind, erfolgen. Erfolgt die Sperre nicht, verspätet oder sonstwie fehlerhaft, dann steht dem Antragsteller eine Kontaktmöglichkeit zum ZDA zur Verfügung, der die Ursache der fehlerhaften Sperre überprüft.

Im übrigen ist der Ablauf ident zu ⇨ 4.9.3 Stellung eines Widerrufantrages / Procedure for revocation request (p49).

4.9.16 Dauer einer Zertifikatssperre / Limits on suspension period

Eine Zertifikatssperre wird zu einem Widerruf des Zertifikates, wenn innerhalb der rechtlich maximal zulässigen Dauer einer Zertifikatssperre eine Bestätigung der Sperre erfolgt, keine Reaktion erfolgt oder keine Aufhebung der Zertifikatssperre verlangt wird.

Wenn eine Sperre aufgehoben wird, wird ein Protokoll mit den selben Informationen wie bei einer Sperre erstellt.

4.10 Zertifikatsstatusdienste / Certificate status services

Der Betreiber stellt ausreichende Dienste zur Feststellung des Status der Zertifikate bereit.

Unabhängig von der standardisierten Bereitstellung des Verzeichnis- und Widerrufsdienstes kann im Einzelfall der Status eines ausgestellten Zertifikates individuell beauskunftet werden. Zulässige Auskunftsmöglichkeiten sind mündlich, per Telefon, per Post, per eMail oder auf einem sonstigen elektronischen Übertragungsweg. Weitere Standards können auf Grund gesetzlicher, kundenspezifischer oder sonstiger Anforderungen bereitgestellt werden. Im Zusammenhang mit der Beauskunftung des Status eines ausgestellten Zertifikates erfolgt auch eine Angabe zur Zuverlässigkeit bzw. Integrität der Auskunft. Durch den ZDA elektronisch signierte Auskünfte gelten bis zu deren Ablaufdatum bzw. Widerruf als verbindlich.

Der ZDA kann bei von ihm ausgestellten qualifizierten Zertifikaten für die gesetzlich vorgesehene Dauer, zumindest jedoch bis 35 Jahre nach dem Zeitpunkt der Ausstellung den Signator für den das Zertifikat ausgestellt wurde und die Gültigkeit des Zertifikates bestätigen.

Es werden alle von GLOBALTRUST® ausgestellte Zertifikate den Signatoren und Nutzern folgendermaßen verfügbar gemacht:

1. Grundsätzlich werden alle Zertifikate in den Verzeichnisdienst(en) des ZDA veröffentlicht. Die Nutzungsdetails werden auf der Website (⇨ http://www.globaltrust.eu/directory.html) des ZDA veröffentlicht.
2. Die Bedingungen für die Benutzung eines Zertifikats werden vom ZDA allen Beteiligten in Form der GLOBALTRUST® Certificate Policy in Vermindung mit dem zutreffenden GLOBALTRUST® Certificate Practice Statement zur Kenntnis gebracht.
3. Der Verzeichnisdienst ist als ⇨ Permanenzdienst verfügbar. Unterbrechungen von mehr als 24h werden als Störfälle dokumentiert. Im Falle qualifizierter Zertifikate werden Störfälle ab einer Unterbrechung von 30 Minuten dokumentiert. Diese Dokumentation

ist für Aufsichts- und Auditstellen zugänglich, bei Vorhandensein berechtigter Interessen werden für einen relevanten Zeitraum die Unterlagen auch Dritten bereit gestellt.
4. Die Verzeichnisdienste sind öffentlich und international zugänglich.

Eine Aufnahme in den Verzeichnisdienst unterbleibt, wenn
- der Signator es wünscht oder andere gewichtige Gründe vorliegen und
- die Art des Zertifizierungsdienstes es erlaubt (wesentlich sind der Inhalt der Anzeige bei der Aufsichtsbehörde, Vorgaben durch Standards und Gesetze oder sonstige verbindliche rechtliche Vorgaben).

Auch zu den Zertifikaten die nicht im Verzeichnisdienst automatisiert veröffentlicht werden, wird Auskunft über den Inhaber erteilt, sofern der Auskunftssuchende ein berechtigtes Interesse glaubhaft macht.

Die Aufnahme in die Liste der gesperrten oder widerrufenen Zertifikate kann nicht unterbunden werden.

4.10.1 Betriebliche Voraussetzungen / Operational characteristics

Der Zugriff auf öffentlich zugängliche Daten, wie den Verzeichnisdienst, Widerrufslisten, Sperrlisten, Zertifizierungsstatusdienste, Informationen zur jeweils anzuwendenden Certificate Policy, Auskunftsdiensten usw. ist kontrolliert und erfolgt über eine nach dem Stand der Technik konfigurierte Firewall.

4.10.2 Verfügbarkeit / Service availability

Die Zertifikatsstatusdienste, insbesondere Sperr und Widerrufsdienste werden auf Basis von 24/7/365 betrieben.

4.10.3 Zusätzliche Funktionen / Optional features

Der Betreiber behält sich vor weitere Funktionen im GLOBALTRUST® Certificate Practice Statement zu spezifizieren.

4.11 Vertragsende / End of subscription

Zertifikate werden befristet ausgestellt, die maximal mögliche Laufzeit ist die Dauer jenes Zertifikates, dass das ausgestellte Zertifikat elektronisch signiert. Bei qualifizierten Zertifikaten ist die maximale Laufzeit auf gesetzliche Vorgaben begrenzt.

Abweichungen sind dann zulässig, wenn sie im jeweils anzuwendenden GLOBALTRUST® Certificate Practice Statement festgelegt werden und gesetzlichen und technischen Vorgaben nicht widersprechen. Ist die Laufzeit eines Zertifikats länger als die Laufzeit des unterschreibenden Zertifikates, dann behält es trotzdem seine Gültigkeit, sofern es innerhalb der Laufzeit des unterschreibenden Zertifikates ausgestellt und nicht widerrufen wurde.

Abgelaufene Zertifikate werden nicht widerrufen, elektronische Signaturen, die innerhalb der Gültigkeitsdauer eines Zertifikates erstellt wurden, behalten auch nach Ablauf des Zertifikates ihre Gültigkeit.

Die Verpflichtungen die sich aus dieser GLOBALTRUST® Certificate Policy und dem GLOBALTRUST® Certificate Practice Statement für ZDA, Betreiber und Signator ergeben, bleiben nach Ende der Laufzeit des Zertifikates für die für das jeweilige Zertifikat anwendbare Dauer bestehen.

4.12 Schlüsselhinterlegung und -wiederherstellung / Key escrow and recovery

Es werden keine Funktionen zur Wiederherstellung oder Archivierung von Schlüsseln bereitgestellt. Schlüssel, die für die qualifizierte elektronische Signatur geeignet sind werden ausschließlich in der dafür geeigneten Sicherheitshardware gespeichert und dem Signator bereit gestellt, alle anderen Schlüssel werden als verschlüsselte Datei nur solange bereit gehalten, bis die Zustellung zum Signator abgeschlossen ist.

4.12.1 Policy und Anwendung von Schlüsselhinterlegung und -wiederherstellung / Key escrow and recovery policy and practices

Es werden keine Schlüssel-Treuhandfunktionen ("key-escrow") zur Verfügung gestellt.

4.12.2 Policy und Anwendung für den Einschluß und die Wiederherstellung von Session keys / Session key encapsulation and recovery policy and practices

Es werden keine Funktionen zu Einschluß und Wiederherstellung von Session keys bereit gestellt.

5. ANFORDERUNGEN STANDORT, MANAGEMENT UND BETRIEB / FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Der ZDA ist für die Gestaltung und Dokumentation aller Prozesse im Rahmen der Zertifizierungsdienste (inklusive Zeitstempeldienste) verantwortlich; dies gilt auch für die an Vertragspartner ausgelagerten Dienste. Die eingesetzten Dokumentationsformate sind Teil der GLOBALTRUST® Certificate Security Policy, die verwendeten Dokumentationsmittel sind intern dokumentiert.

Die Aufgaben und zugeordneten Verantwortlichkeiten der Vertragspartner sind klar geregelt, weiters sind Kontrollen zur Überprüfung der ordnungsgemäßen Tätigkeit eingerichtet.

Der Zertifizierungsdienst ist inklusive der technischen (automatisierten) Verfügbarkeit der Widerrufslisten als Permanenzdienst organisiert. Dies gilt auch für die automatisierte Entgegennahme von Widerrufsanträgen.

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. Wird die angestrebte Verfügbarkeit in einem Monat nicht erreicht, werden zusätzliche organisatorische und technische Maßnahmen gesetzt, die eine Verbesserung der Verfügbarkeit erwarten lassen.

Entspricht die Verfügbarkeit nicht den Vorgaben der Aufsichtstellen oder der Gesetzeslage, erfolgt eine Mitteilung im Rahmen der rechtlichen Vorgaben und Vereinbarungen. Jedenfalls werden Störungen intern dokumentiert und - sofern erforderlich und technisch möglich - Maßnahmen zur künftigen Vermeidung entwickelt.

Die für die Sicherheit grundlegenden Vorgehensweisen sind in dieser Policy dokumentiert. Zusätzlich setzt der ZDA spezifische Sicherheitsmaßnahmen wie sie in der nicht öffentlichen GLOBALTRUST® Certificate Security Policy festgelegt sind. Diese Sicherheitsmaßnahmen werden entsprechend der Sicherheitsziele und -leitlinien gemäß GLOBALTRUST® Certificate Practice Statement gesetzt.

Alle betrieblichen Abläufe sind dokumentiert und unterliegen dieser GLOBALTRUST® Certificate Policy, der GLOBALTRUST® Certificate Security Policy und dem jeweils anzuwendenden GLOBALTRUST® Certificate Practice Statement.

5.1 Bauliche Sicherheitsmaßnahmen / Physical controls

Die Zertifizierungsdienste werden ausschließlich in geeigneten Räumlichkeiten erbracht. Die Details sind in der GLOBALTRUST® Certificate Security Policy geregelt.

5.1.1 Standortlage und Bauweise / Site location and construction

Die Geschäftsführung des ZDA entscheidet, an welchem Ort die Zertifizierungsdienste stattzufinden haben, dabei werden die Vorgaben der GLOBALTRUST® Certificate Security Policy beachtet.

5.1.2 Zutritt / Physical access

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.

5.1.3 Stromnetz und Klimaanlage / Power and air conditioning

Stromversorgung und Klimanalage sind in ausreichender Kapazität verfügbar. Die Details sind in der GLOBALTRUST® Certificate Security Policy geregelt.

5.1.4 Gefährdungspotential durch Wasser / Water exposures

Die Auswahl des Standortes der zertifizierungskritischen Komponenten erfolgt unter Bedachtnahme der Unwahrscheinlichkeit einer Gefährdung durch Wasser. Die Details sind in der GLOBALTRUST® Certificate Security Policy geregelt.

5.1.5 Brandschutz / Fire prevention and protection

Es sind ausreichende Vorkehrungen zum Brandschutz getroffen. Die Details sind in der GLOBALTRUST® Certificate Security Policy geregelt.

5.1.6 Aufbewahrung von Speichermedien / Media storage

Speichermedien werden entfernt vom Betriebsstandort der zertifizierungskritischen Komponenten aufbewahrt und gesichert. Die erforderlichen Maßnahmen sind in der GLOBALTRUST® Certificate Security Policy geregelt.

5.1.7 Abfallentsorgung / Waste disposal

Die Abfallentsorgung erfolgt gemäß den örtlichen gesetzlichen Bestimmungen.

5.1.8 Offsite Backup / Off-site backup

Backups werden entfernt vom Betriebsstandort der zertifizierungskritischen Komponenten aufbewahrt und gesichert. Die erforderlichen Maßnahmen sind in der GLOBALTRUST® Certificate Security Policy geregelt.

5.2 Prozessanforderungen / Procedural controls

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. Besonders im Störfall oder bei unvorhergesehenen Ereignissen ("Stress"-Situation) sollen geeignete Strategien und allgemeine Maßnahmen auch jene Fälle abdecken, die nicht vorausschauend vollständig als Geschäftsprozesse definiert werden konnten.

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

Alle für die Zertifizierung relevanten administrativen Geschäftsprozesse werden in einem internen Content-Management- und Monitoring-System dokumentiert. Beschreibung, Verwaltung und Nutzung dieser Prozesse erfolgt in der internen Betriebsdokumentation.

5.2.1 Rollenkonzept / Trusted roles

Das Rollenkonzept, die Rollenbeschreibung und die Berichtspflichten sind in der ⇨ GLOBALTRUST® Certificate Security Policy definiert. Änderungen in der Rollenverteilung sind so vorzunehmen, dass alle in diesem Practice-Statement und in den Certificate-Policies erforderlichen Tätigkeiten erfüllt werden können und ausreichende Vertretungen vorgesehen sind.

5.2.2 Mehraugenprinzip / Number of persons required per task

Kritische Prozesse unterliegen dem 4-Augenprinzip. Die beteiligten Personen werden dokumentiert.

5.2.3 Identifikation und Authentifikation der Rollen / Identification and authentication for each role

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. Authentifikationskennzeichen ausgeschiedener Mitarbeiter werden deaktiviert, jedoch weiterhin dokumentiert.

Zur Zertifizierung berechtigte Mitarbeiter weisen sich durch einen eigenen Hardware-Token (mit Identifikationsschlüssel) gegenüber dem Zertifizierungssystem aus. Dieser erfüllt die Anforderungen wie unter ⇨ 6. Technische Sicherheitsmaßnahmen / TECHNICAL SECURITY CONTROLS (p69) für Identifikationsschlüssel (⇨ Kategorie 3, p69) beschrieben.

5.2.4 Rollenausschlüsse / Roles requiring separation of duties

Alle Mitarbeiter sind ausschließlich im Rahmen der für sie definierten Rollen tätig und werden in die erforderlichen betrieblichen Abläufe eingewiesen und geschult. Sie erhalten nur die für ihre Tätigkeit erforderlichen Zugangsberechtigungen und Token.

5.3 Mitarbeiteranforderungen / Personnel controls

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 Geschäftsführung des ZDA kann für die Erbringung der Dienste gemäß dieser Policy im Rahmen des Rollenkonzeptes (⇨ GLOBALTRUST® Certificate Security Policy) geeignete bevollmächtigte Personen oder geeignete Dienstleister beauftragen. Diesen obliegen die Festlegung und Umsetzung aller operativen Maßnahmen inkl. der Festlegung der erforderlichen Dokumentationen, Zertifizierungsrichtlinien und Betriebsstandorte.

Die Systemadministratoren und sonstige mit Zertifizierungsaufgaben betraute Personen werden zur Einhaltung der Datensicherheitsbestimmungen gemäß der bestehenden Gesetze und Standards vertraglich verpflichtet.

Die Mitarbeiter des ZDAs sind als qualifiziertes Personal besonders geeignet, die in dieser Policy verankerten Bestimmungen umzusetzen und zu gewährleisten.

Zur Steuerung der Zertifizierungsdienste ist ein Zertifizierungs-Ausschuss eingerichtet, der nach Anforderung zusammentritt. Die näheren Kriterien bezüglich Zusammensetzung und Einberufung sind in Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) definiert.

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit / Qualifications, experience, and clearance requirements

Die Anforderungen werden im Rahmen des Rollenkonzepts (⇨ GLOBALTRUST® Certificate Security Policy) beschrieben.

- Sicherheitsrelevante Funktionen und Verantwortlichkeiten werden in den internen Stellenbeschreibungen und im internen Rollenplan dokumentiert. Jene Funktionen, von denen die Sicherheit der Zertifizierungsdienste abhängt, sind eindeutig identifiziert.

- 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.
- Alle in den Betrieb des Zertifizierungsdienstes involvierte Menschen durchlaufen vor ihrem Engagement eine Identitätsprüfung sowie eine Prüfung ihrer Vertraulichkeit.
- Angestellte und andere vom Betreiber beauftragte und in die Ausstellung von EV-Zertifikaten involvierte Personen durchlaufen eine Identitätsprüfung.
- Angestellte und andere vom Betreiber beauftragte und in die Ausstellung von EV-Zertifikaten involvierte Personen durchlaufen eine Hintergrundcheck, in dem vorige Arbeitgeber, Referenzen und die höchste oder relevanteste Ausbildung geprüft werden.
- Im Rollenplan als notwendig oder als Schlüsselrolle ausgezeichnete Rollen sind stets besetzt.
- Bei sicherheitsrelevante Funktionen und Verantwortlichkeiten wir darauf geachtet, dass keine Interessenskonflikte bzw. Unvereinbarkeiten entstehen.

5.3.2 Durchführung von Backgroundchecks / Background check procedures

Die Mitarbeiter werden, abhängig von den Anforderungen und Aufgaben ausreichenden und effektiven Sicherheitsüberprüfungen unterzogen.

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.

5.3.3 Schulungen/ Training requirements

Die Mitarbeiter werden mit Zertifizierungsaufgaben ausschließlich nach ausreichender Einschulung betraut.

5.3.4 Häufigkeit von Schulungen und Anforderungen / Retraining frequency and requirements

Das Betriebspersonal wird laufend in der Verwendung der Monitoring-Instrumente und sonstiger für die Erbringung der Zertifizierungsdienste erforderlichen Instrumente geschult.

Zusätzlich erfolgen anlassbezogene Schulungen, insbesondere bei Vorliegen sicherheitsrelevanter Vorfälle, bei geänderten rechtlichen oder technischen Voraussetzungen und bei EInführung neuer Verfahrensweisen.

5.3.5 Häufigkeit und Abfolge Arbeitsplatzrotation / Job rotation frequency and sequence

Es ist keine Arbeitsplatzrotation vorgesehen, neue Mitarbeiter durchlaufen jedoch alle notwendigen Stationen, die zur Erfüllung ihrer Aufgaben erforderlich sind.

5.3.6 Strafmaßnahmen für unerlaubte Handlungen / Sanctions for unauthorized actions

Unerlaubte Handlungen von Mitarbeitern werden gemäß den Bestimmungen des Angestelltengesetzes geahndet. Bei sonstigen vertraglich gebundenen Personen werden Straf- und Schadenersatzleistungen angemessen zum von der Tätigkeit der Person ausgehenden Risiko vereinbart.

5.3.7 Anforderungen an Dienstleister / Independent contractor requirements

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.

Sofern ein Dienstleister in die Erstellung von Serverzertifikaten involviert ist, wird vom Betreiber jährlich durch eine interne Prüfung ermittelt, ob dieser die Bestimmungen von [CABROWSER-BASE] einhält.

Ein Dienstleister darf niemals die Identitätsprüfung für einen Zertifikatsantrag einer Organisation durchführen auf die er bestimmenden Einfluss hat.

5.3.8 Zu Verfügung gestellte Unterlagen / Documentation supplied to personnel

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

Die Geschäftsführung des ZDA genehmigt die notwendigen Dokumentationen und Zertifizierungsrichtlinien und ernennt jene Personen und externe Vertragspartner, die für die Umsetzung der Zertifizierungsdienste gemäß internen Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) verantwortlich sind. Verabschiedung von Richtlinien und Ernennung von autorisierten Personen werden schriftlich dokumentiert.

5.4 Betriebsüberwachung / Audit logging procedures

5.4.1 Zu erfassende Ereignisse / Types of events recorded

Die Erstellung eines privaten Schlüssels für ein Root-Zertifikat, welcher nach dem 9.7.2013 erstellt wurde und für die Ausstellung von EV-Zertifikaten verwendet wird, wird von einer kompetenten und unabhängigen Auditstelle überwacht.

Auditreports kompetenter und unabhängiger Auditstellen enthalten folgende Angaben :

a) Der Vorgang der Root-Zertifikat Schlüsselerstellung und die zugehörigen Schutzmaßnahmen werden gemäß der GLOBALTRUST® Certificate Policy und - sofern

erforderlich - dem jeweils anzuwendendem Certificate Practice Statement (CPS) dokumentiert.

b) Das Ablaufprotokoll enthält ausreichende Details zur Schlüsselgenerierung (inkl. der verwendeten technischen Skripts).

c) Die Vorgaben a) wurden eingehalten, vollständig und korrekt durchgeführt.

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.

5.4.2 Überwachungsfrequenz / Frequency of processing log

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.

5.4.3 Aufbewahrungsfrist für Überwachungsaufzeichnungen / Retention period for audit log

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.

5.4.4 Schutz der Überwachungsaufzeichnungen / Protection of audit log

Die Dokumentation der Sicherheitsvorkehrungen, von Störfällen und besonderen Betriebssituationen erfolgt in statischen Dateiformaten bzw. in Dateiformaten ohne dynamische Elemente, insbesondere in Text-Formaten, in grafischen Formaten, wie beispielsweise JPG, TIFF, GIF oder PNG oder im PDF-Format ohne dynamische Elemente (insbesondere PDF/A-Format). Dokumentationsdaten mit besonderen Archivierungserfordernissen, insbesondere wenn gesetzlich, durch die GLOBALTRUST® Certificate Security Policy oder durch die anzuwendende Certificate Policy vorgegeben, werden mit einem Zeitstempel oder einer anderen geeigneten Form der elektronischen Signatur versehen.

Die konkrete Ausgestaltung des Überwachungssystems ist intern dokumentiert. Im Rahmen dieser Überwachungsdokumentation sind auch jene Prüfmaßnahmen dokumentiert, die bei Ausfall des automatisierten Überwachungssystems manuell gesetzt werden können.

Während des regulären Bürobetriebes wird das Überwachungssystem laufend gemäß Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) kontrolliert. Bei Ausfall kritischer Dienste erfolgt eine automatisierte Verständigung des Bereitschaftsdienstes per SMS. Der Bereitschaftsdienst reagiert im Rahmen einer festgelegten Eskalationsstrategie gemäß GLOBALTRUST® Certificate Security Policy, insbesondere Abschnitt "Ausfallsszenarien" wobei für kritische Dienste im Rahmen qualifzierter Angebote (Signatur-, Widerrufs-, Zertifikats-, Zeitstempeldienst, ...) während der Bürozeiten eine Mindestreaktionszeit von drei Stunden, außerhalb von sechs Stunden festgelegt ist, jedenfalls werden gesetzliche vorgesehene Reaktionszeiten, insbesondere wenn sie kürzer sind, eingehalten.

Zugriffe auf Zertifizierungseinrichtungen werden protokolliert und regelmäßig geprüft. Zusätzlich sind Überwachungs- und Monitoringdienste aktiviert, die unplausible bzw. kritische Zugriffsversuche elektronisch melden.

5.4.5 Sicherung des Archives der Überwachungsaufzeichnungen / Audit log backup procedures

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

5.4.6 Betriebsüberwachungssystem / Audit collection system (internal vs. external)

Der Betreiber setzt ein System zur Sammlung der betriebsrelevanten Audit-Daten ein, welches beim Systemstart aktiviert wird Die erforderlichen Maßnahmen sind in der GLOBALTRUST® Certificate Security Policy geregelt.

5.4.7 Benachrichtigung des Auslösers / Notification to event-causing subject

Nicht zutreffend

5.4.8 Gefährdungsanalyse / Vulnerability assessments

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

5.5 Aufzeichnungsarchivierung / Records archival

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. Im Zuge der Auslagerung in Backupsysteme (z.B. Bandarchiv) werden die ausgelagerten Dateien einem Verifikationsverfahren unterzogen.

Elektronisch verwaltete Unterlagen und Informationen werden im Rahmen eines Backupplans durch eine verantwortliche Person gemäß Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) verwaltet. Die so gesicherten Daten sind ausreichend, um den aktuellen Systemstand wiederherzustellen.

Die den Betrieb des Zertifizierungsdienstes betreffenden Ereignis- und Zertifizierungsdienstprotokolle (⇨ Anhang A: 2 Inhalt Ausstellungs-, Sperr-, Entsperr- und Widerrufs-Protokoll für Zertifikate, p124) werden 35 Jahre aufbewahrt.

5.5.1 Zu archivierende Aufzeichungen / Types of records archived

Zertifizierungsrelevante Vorgänge oder Abläufe werden protokolliert und unterliegen - soweit sinnvoll - einer Änderungshistorie. Dies betrifft insbesondere Entwicklungen zu den Zertifizierungsdiensten und deren technische Dokumentationen.

Unterlagen und Daten, die zur Prüfung bestehender, abgelaufener oder widerrufener Zerifikate erforderlich sind, Daten die zur Prüfung vergebener Zeitstempel erforderlich sind, einschließlich Zertifikate, Widerrufsstatusinformationen und der Dokumentation von Störfällen und besonderen Betriebssituationen, werden gemäß den Vorgaben der jeweiligen Certification Policy, insbesondere was Dauer und Ablageform betrifft, in dafür vorgesehenen Datenbanken, auf zentralen Servern, auf externen Datenträgern oder als manuelle Ablage archiviert.

Archivierte Unterlagen werden strukturiert abgelegt und sind durchsuchbar.

5.5.2 Aufbewahrungsfristen für archivierte Daten / Retention period for archive

Die Aufbewahrungszeit ist, sofern nicht im jeweils anzuwendenden 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.

Betriebsbedingt anfallende Audit- und Logdateien werden drei Monate, jedenfalls jedoch so lange aufbewahrt, wie sie zur Üebrwachung des Betriebs erforderlich sind.

5.5.3 Schutz der Archive / Protection of archive

Die Aufbewahrung richtet sich nach dem aktuellen Stand der Technik. Soweit Ausdrucke aufbewahrt werden (Papierausdrucke, Hardcopies) werden sie in versperrbaren Räumlichkeiten aufbewahrt. Elektronisch archivierte Dokumente werden in gängigen Datenformaten aufbewahrt (unter anderem in Plain-Text, XML, PDF (inkl. PDF/A), TIFF, JPG, GIF, PNG usw), von denen auch in Zukunft eine einfache Darstellbarkeit und Lesbarkeit erwartet werden kann. Sofern absehbar ist, dass bestimmte Formate in Zukunft nicht mehr lesbar sind, erfolgt zeitgerecht eine Konvertierung in zukunftssichere Formate.

Geheime Informationen, insbesondere Passwörter und private Schlüssel der Zertifizierungsdienste unterliegen keiner Archivierung, vertrauliche Informationen, insbesondere betrieblich erforderliche Informationen unterliegen einer Archivierung, deren Zugriff gemäß der ⇨ **Stufe "vertraulich"** (p100) beschränkt ist.

5.5.4 Sicherung des Archives / Archive backup procedures

Die Grundprinzipen der Archivierung sind:

- **Funktionalität:** Backups werden ausschließlich in Hinblick auf bestimmte, definierte Anwendungen erstellt.
- **Integrität:** Backups werden vergleichbar den Archiven durch geeignete Maßnahmen, insbesondere durch elektronische Signatur von archivierten Dateien, durch Zugriffsrestriktionen (Authentisierungsverfahren), durch Referenzdokumentationen/Hashverfahren oder durch eine Kombination der genannten Methoden gesichert.
- **Vertraulichkeit:** Grundsätzlich wird vermieden, dass Backups geheime Informationen (wie Passwörter, private Schlüssel usw.) enthalten. Sofern dies unumgänglich ist, erfolgt deren Speicherung in verschlüsselter Form. Die verwendeten Algorithmen entsprechen dem Stand der Technik, insbesondere den Vorgaben von [ETSI TS 102 176] und gesetzlichen Bestimmungen.
- **Zuverlässigkeit:** Backups werden durch geeignete Soft- und Hardwarekomponenten erstellt, die eine zuverlässige Aufbewahrung über die erforderlichen Zeiträume erwarten lassen.
- **Auslagerung:** Backups werden entsprechend ihrer Funktionalität so ausgelagert, dass eine der Funktionalität entsprechende ausreichende sichere Aufbewahrung und Verfügbarkeit gegeben ist. Es wird dabei das Prinzip der ausreichenden Entfernung vom Originaldatenbestand verfolgt. Die Aufbewahrung der Langzeit-Backups erfolgt in anderen Räumlichkeiten, als den Räumen, in denen die Server betrieben werden, Online-Sicherheits- und Betriebsbackups auf anderen Systemen, als die Systeme, die die Originaldaten enthalten. In allen Fällen ist der Zugang beschränkt und zur Erlangung des Zugangs zu den Backupdaten ist die Überwindung physischer und/oder technischer Hindernisse erforderlich.
- **Rekonstruierbarkeit:** Backups werden stichprobenweise auf ihre Rekonstruierbarkeit und Verfügbarkeit getestet, diese kann auch durch die Geschäftsführung beauftragt werden. Die Vorgangsweise zur Beauftragung ist intern dokumentiert.

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen / Requirements for time-stamping of records

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.

Die elektronischen Dokumente werden in geeigneten Systemen verwaltet, die durch Integritätsprüfungen Datenfehler erkennen und Datenverlust vermeiden können. Zu elektronisch archivierten Dokumenten wird zeitnah zum Ereignis ein Zeitstempel generiert, der den Zeitpunkt der Archivierung und die Unversehrtheit des Dokuments dokumentiert. Im übrigen erfolgt die Datensicherung gemäß GLOBALTRUST® Certificate Security Policy.

5.5.6 Archivierung (intern/extern) / Archive collection system (internal or external)

Die Datenintegrität wird durch Verwendung nicht überschreibbarer Datenträger, durch elektronische Signatur von archivierten Dateien, durch Zugriffsrestriktionen (Authentisierungsverfahren), durch Referenzdokumentationen/Hashverfahrten oder durch eine Kombination der genannten Methoden gesichert.

5.5.7 Verfahren zur Beschaffung und Verifikation von Aufzeichnungen / Procedures to obtain and verify archive information

Die Restoremechanismen sind so ausgelegt, dass das Zertifizierungssystem von Sicherungsbeständen wieder hergestellt werden kann.

Restoremaßnahmen werden durch eine verantwortliche Persongemäß Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) veranlasst.

Ist das Restore (die Wiederherstellung) von Daten aus einem Backup erforderlich, dann werden die dazu notwendigen Daten in einem eigenen Bereich wieder hergestellt und nach Kontrolle der Richtigkeit und Erforderlichkeit der Daten nur jene Daten in das Produktionssystem übernommen, die tatsächlich notwendig sind.

5.6 Schlüsselwechsel des Betreibers / Key changeover

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.

5.7 Kompromittierung und Geschäftsweiterführung / Compromise and disaster recovery

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.

5.7.1 Handlungsablauf bei Zwischenfällen und Kompromittierungen / Incident and compromise handling procedures

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. Die Details sind in der GLOBALTRUST® Certificate Security Policy beschrieben.

Der Übergang von Normalbetrieb ("primary") auf Ausfallsbetrieb ("disaster recovery") erfolgt weitestgehend automatisiert und mit Verzögerungen unter fünf Minuten. Die maximal zulässigen Ausfälle, die noch einen automatisierten Übergang vom Normalbetrieb in den Ausfallsbetrieb erlauben sind in der internen GLOBALTRUST® Certificate Security Policy als "Worst Case Szenario" beschrieben. Darüber hinausgehende Ausfälle erfordern manuelle Eingriffe autorisierten Personals. Die Reaktionszeit dieser manuellen Eingriffe beträgt maximal 24 Stunden, erfolgen jedoch zumindest innerhalb der zeitlichen Vorgaben der Aufsichtstelle.

Soweit alternative Dienste oder Systeme verwendet werden, entsprechen diese denselben Sicherheitsanforderungen wie die Hauptsysteme.

Die Übergänge vom Normalbetrieb zu Ausfallsbetrieb und das sonstige Ausfallsverhalten wird in regelmäßigen Abständen in einem Umfang, der sinnvoll und wirtschaftlich vertretbar ist, getestet.

5.7.2 Wiederherstellung nach Kompromittierung von Ressourcen / Computing resources, software, and/or data are corrupted

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

5.7.3 Handlungsablauf Kompromittierung des privaten Schlüssels des ZDA / Entity private key compromise procedures

Es besteht eine interne Dokumentation der zu setzenden Schritte und Maßnahmen bei Kompromittierung des privaten Schlüssels des ZDA.

5.7.4 Möglichkeiten zur Geschäftsweiterführung im Katastrophenfall / Business continuity capabilities after a disaster

Die Maßnahmen zur Geschäftsweiterführung im Katastrophenfall sind in der GLOBALTRUST® Certificate Security Policy dokumentiert.

5.8 Einstellung der Tätigkeit / CA or RA termination

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.

6. TECHNISCHE SICHERHEITSMAßNAHMEN / TECHNICAL SECURITY CONTROLS

Die Betriebsinfrastruktur des Betreibers wird regelmäßig überprüft und an geänderte Anforderungen angepasst. Änderungen, die einen Einfluss auf das Ausmaß der erreichten Sicherheit haben, sind vom Zertifizierungsauschuss gemäß Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) zu genehmigen. Im Falle einer Änderung der 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.

Diese Schlüssel werden in folgenden Kategorien verwaltet und bereit gestellt:

Kategorie 1: Signaturschlüssel zur Erbringung von Zertifizierungsdiensten. Umfasst sind Zertifizierungsdienste, die qualifizierte, also auch nicht-qualifizierte Zertifikate betreffen.

Kategorie 2: Infrastrukturschlüssel, zur Absicherung einzelner Prozesse, Geräte oder Objekte der Zertifizierungsdienste. Insbesondere sind dies Schlüssel zur gesicherten Datenübertragung zwischen Zertifizierungsrechenzentrum und Büro des ZDAs oder mobiler Zugangsgeräte, oder zur Signatur (inkl. Zeitstempel) von Log-Dateien, Programmen oder anderer für die Zertifizierung relevanter Dateien.

Kategorie 3: Identifikationsschlüssel, zur Absicherung der Kommunikation zwischen technischen Systemen und Mitarbeitern und der Authentifizierung der Mitarbeiter.

Kategorie 4: Session Keys, ausschließlich temporär generierte Schlüssel zur Absicherung der Kommunikation zwischen technischen Systemen.

Die Schlüssel der Kategorien 1 bis 3 werden nach dem Stand der Technik erstellt, wobei nationale und internationale Anforderungen, etwa von [ETSI TS 102 176] beachtet werden. Schlüssel der Kategorie 1 entsprechen jedenfalls den gesetzlichen Anforderungen zur Erbringung der Signaturdienste.

Der Zugriff auf Signaturerstellungsdaten wird gemäß GLOBALTRUST® Certificate Security Policy beschränkt. Der Zugriff auf Signaturerstellungseinheiten, die für Zertifizierungsdienste vorgesehen sind oder für Infrastruktur- oder Identifikationsschlüssel dienen unterliegt einer Zugangskontrolle.

6.1 Erzeugung und Installation von Schlüsslpaaren / Key pair generation and installation

Der Betreiber stellt Signaturerstellungseinheiten gemäß den rechtlichen Vorgaben und aktuellen technischen Standards sowohl für qualifizierte elektronische Signaturen und qualifizierte Zertifikate, als auch für fortgeschrittene und sonstige Signaturen zur Verfügung.

Für die Ausstellung von Signaturerstellungseinheiten, die für qualifizierte elektronische Signaturen geeignet sind, muss einer der folgenden Abläufe gewährleistet sein:
(a) Standardvorgabe
(b) Herstellervorgabe
(c) Policyvorgabe

Für Signaturerstellungseinheiten, die für sonstige (nicht-qualifizierte) elektronische Signaturen geeignet sind und für sonstige Zertifikate, erfolgt die Aus- und Zustellung gemäß der jeweils gültigen Certificate Policy.

(a) Standardvorgabe

Zur Ausstellung sicherer, damit für qualifizierte elektronische Signaturen geeigneter, Signaturerstellungseinheiten ist für die technische Komponente zumindest eine geeignete Sicherheitszertifizierung des Betriebssystems erforderlich. Eine Sicherheitszertifizierung ist insbesondere geeignet, wenn sie den Vorgaben gemäß [EG-REF] oder [CWA-14169] entspricht oder von den zuständigen Aufsichtstellen als geeignet bestätigt wird.

Die Ausstellung der Signaturerstellungseinheit erfolgt in einer vom ZDA gesicherten Umgebung und durchläuft folgende zwingende Schritte:

(i) Lieferung der Signaturerstellungseinheiten

Erfolgt durch
(a) persönliche Übergabe in den Geschäftsräumen des Herstellers, eines von ihm autorisierten Händlers oder in den Geschäftsräumen des Betreibers durch autorisierte Personen des Herstellers,
(b) durch Boten oder Postdienste, wobei die Signaturerstellungseinheiten in Verpackungen und/oder Behälter transportiert werden, bei denen die Unversehrtheit bei der Übergabe geprüft werden kann,
(c) durch sonstige Zustellung, sofern für jede einzelne Signaturerstellungeinheit die Herkunft vom Hersteller zweifelsfrei festgestellt werden kann (zum Beispiel mittels eines Herkunfts- oder Produktionszertifikates, das dem Hersteller eindeutig zugeordnet ist).

(ii) Pre-Personalisierung

Eine pre-personalisierte Signaturerstellungseinheit lässt keine Rückschlüsse auf eine bestimmte Person zu.

Unter Pre-Personalisierung wird die Festlegung der Datenstruktur auf der Signaturerstellungseinheit verstanden. Diese Datenstruktur kann auf Grund individueller Anforderungen unterschiedliche Struktur haben, enthält aber bei sicheren Signaturerstellungseinheiten die für qualifizierte Signaturen geeignet sind jedenfalls einen sicheren Schlüssel im Sinne dieses Dokuments (⇨ 6.1.2 Zustellung privater Schlüssel an den Signator / Private key delivery to subscriber, p75). Soweit die Signaturerstellungseinheit weitere Daten enthält, sind sie vom sicheren Schlüssel und qualifizierten Zertifikat so getrennt zu speichern, dass sicherer Schlüssel und qualifiziertes Zertifikat unabhängig von diesen Daten verwendet werden können und eine Beeinflussung ausgeschlossen ist.

Die Pre-Personalisierung erfolgt
(a) entweder beim Hersteller auf Grund der Vorgaben des ZDA oder
(b) beim Hersteller auf Grund einer Sicherheitszertifizierung bzw. Genehmigung durch eine Aufsichtstelle oder
(c) beim Betreiber gemäß dokumentierter Anforderungen, wobei die Anforderungen genereller Natur sein können (etwa auf Grund produktspezifischer Definitionen) oder auf Grund individueller Wünsche von Kunden.

(iii) Schlüsselerzeugung

In den Signaturerstellungseinheiten werden für qualifizierte elektronische Signaturen geeignete Endkundenschlüssel nach Stand der Technik erzeugt, wobei rechtliche und technische Vorgaben beachtet werden. Die Erzeugung kann sowohl beim Betreiber, beim Hersteller der Signaturerstellungseinheit, beim Signator oder bei einem vom Betreiber beauftragten Dienstleister erfolgen.

In allen Fällen sind die Vorgaben der jeweils anzuwendenden Certificate Policy zu beachten.

Sofern der Endkundenschlüssel nicht in der Signaturerstellungseinheit selbst erzeugt wird, erfolgt die Erzeugung in einer gesicherten Umgebung, die jedenfalls folgende Eigenschaften aufweist:
- die gesicherte Umgebung stellt für die gesamte Dauer die Kontrolle über den Endkundenschlüssel dessen Vertraulichkeit und Integrität sicher,
- die gesicherte Umgebung gewährleistet den vertraulichen Transfer des Endkundenschlüssels in die sichere Signaturerstellungseinheit,
- die gesicherte Umgebung sichert die Integrität des öffentlichen Endkundenschlüssels, wenn er in ein anderes System oder eine andere Applikation exportiert wird,
- die gesicherte Umgebung wird nur von identifizierten und autorisierten Benutzern verwendet,
- der Zugang und Zugriff zu den Diensten ist limitiert,
- die Funktionalität der gesicherten Umgebung kann geprüft und getestet werden und geht in einen definierten Ausgangszustand bei Auftreten von Fehlern,
- die gesicherte Umgebung ist gegen physische Angriffe (Beschädigungen) gesichert und geht in einen gesicherten Ausgangszustand, wenn derartige Angriffe erkannt werden.

Die Evaluation dieser Anforderungen entspricht den Vorgaben [CWA-14167-3] oder einem anderen vergleichbaren rechtlich und technisch zulässigen Verfahren. Die Übertragung des Endkundenschlüssels erfolgt auf gesicherte Weise, nach erfolgter Übertragung wird der Endkundenschlüssel in der gesicherten Umgebung auf nicht rekonstruierbare Weise gelöscht.

(iv) Lagerung

Soweit Signaturerstellungseinheiten beim ZDA gelagert werden (auf Vorrat gehalten werden), werden sie nur in einer Pre-personalisierten oder davor liegenden Form, nicht jedoch personalisiert gelagert.

Keine Lagerung ist die bloß kurzzeitige Aufbewahrung von personalisierten Signaturerstellungseinheiten zum Zwecke der Zustellung an den oder zur Abholung durch den Signator.

In allen Fällen werden Signaturerstellungseinheiten die für qualifizierte Zertifikate vorgesehen sind in versperrten Einrichtungen verwahrt, der Zugriff auf diese Einrichtungen ist auf autorisiertes Personal, dass mit der Ausstellung der Signaturerstellungseinheiten betraut ist, beschränkt.

(v) Qualifiziertes Zertifikat ausstellen

Zur Erstellung des qualifizierten Zertifikates wird bei asymetrischer Verschlüsselung der öffentliche Endkundenschlüssel aus der Signaturerstellungseinheit extrahiert und in der gesicherten Umgebung des Betreibers mit einem Schlüssel des Betreibers unterfertigt. Im Übrigen erfolgt die Ausstellung gemäß den Vorgaben ⇨ 4.3 Zertifikatsausstellung / Certificate issuance (p36) und ⇨ 7.1 Zertifikatsprofile / Certificate profile (p89) und dem jeweils anzuwendenden GLOBALTRUST® Certificate Practice Statement.

Insbesondere Laufzeit und Inhalt eines Zertifikates, Ablauf der Identitätsprüfung, die vertraglichen Verpflichtungen des Signators, des ZDA und des Betreibers werden in der jeweils anzuwendenden Certificate Policy festgelegt.

(vi) Zusätzliche Signaturerstellungsdaten ablegen

Aus produktspezifischen Gründen, aus gesetzlichen Gründen oder auf Grund von Kundenwünschen können auf der Signaturerstellungseinheit zusätzliche Daten abgelegt werden.

Zulässig und keine Beeinflussung der Signaturerstellungseinheit für Zwecke der qualifizierten Signatur sind folgende Datenstrukturen:

- Die Speicherung von Verweisen auf den in der Signaturerstellungseinheit abgelegten sicheren Schlüssel (öffentliche und private Komponente) insbesondere im Format eines PKCS#15 Containers [PKCS15].
- Zusätzliche Zertifikate und Endkundenschlüssel, die für sonstige Signaturen oder zur Verschlüsselung von Daten verwendet werden können.
- Zusätzliche (Cross-)Zertifikate, die auf den sicheren Schlüssel der Signaturerstellungseinheit verweisen und nicht im Widerspruch zu den Anforderungen des GLOBALTRUST® Certificate Practice Statements, der GLOBALTRUST® Certificate Security Policy, dieser GLOBALTRUST® Certificate Policy oder zwingenden rechtlichen oder technischen Bestimmungen stehen.
- Die für die Nutzung der Signaturerstellungseinheit als Bürgerkarte im Sinne des österreichischen eGovernemt-Gesetzes [BÜRGERKARTE] erforderlichen Daten.
- Jede weitere Datenstruktur, die von einer Aufsichtstelle als geeignet angesehen wird. Dabei sind auch allfällige Beschränkungen bei den zulässigen Signaturerstellungseinheiten und Nutzungen zu beachten.
- Jede weitere Datenstruktur, bei der im Einzelfall eine Beeinflussung der Signaturerstellungseinheit für Zwecke der qualifizierten Signatur ausgeschlossen ist.

(vii) Missbrauchsschutz

Alle auf der Signaturerstellungseinheit aufgebrachten Informationen, insbesondere Endkundenschlüssel zur qualifizierten elektronischen Signatur und qualifiziertes Zertifikat sind so aufgebracht, dass eine Verfälschung der Daten ausgeschlossen ist.

Der Missbrauchsschutz schließt nicht aus, dass der Signator zusätzliche Informationen auf der Signaturerstellungseinheit aufbringen kann, einzelne Informationen löschen kann oder die gesamte Signaturerstellungseinheit neu initialisieren kann.

Diese Änderungen können aber nur im Umfang erfolgen, wie sie gemäß anzuwendendem GLOBALTRUST® Certificate Practice Statement zulässig sind und können in keinem Fall zu irreführenden Angaben über Zertifikate oder über den Signator führen.

(viii) Transportsicherung

Die Signaturerstellungseinheit wird mit einem vertraulichen Initialisierungs-PIN versehen. Zusätzlich wird die Signaturerstellungseinheit mit einer Transportsicherung versehen. Die Signaturerstellungseinheit kann erstmalig nur durch Verwendung des Initialisierungs-PINs und Bruch/Beseitigung der Transportsicherung verwendet werden.

Geeignete Transportsicherungen sind
(a) technische Behältnisse, zu denen ausschließlich der Signator einen Schlüssel hat,
(b) Verpackungen oder Behälter, bei denen eine Beschädigung durch Dritte zuverlässig erkannt werden kann,
(c) Sicherung des Signaturschlüssels durch ein Passwort oder
(d) direkt auf der Signaturerstellungseinheit aufgebrachte Daten, die vor der ersten Verwendung der Signaturerstellungseinheit vom Signator entfernt werden müssen.

Eine geeignete Maßnahme im Sinne von (c) ist das Anbringen eines einmalig verwendbaren Transport-PINs der vor der erstmaligen Verwendung der Signaturerstellungseinheit zwingend eingegeben werden muss. Im Falle qualifizierter Zertifikate ist Fall (c) eine geeignete Transportsicherung.

Die Transportsicherung kann entfallen, die Kriterien dafür sind unter ⇨ 6.1.2 Zustellung privater Schlüssel an den Signator / Private key delivery to subscriber (p75) aufgelistet.

Werden im Rahmen der Transportsicherung vertrauliche Informationen (insbesondere Transport-PIN) verwendet, werden diese in einer Form zugestellt, die dem Empfänger erlaubt zu erkennen, ob Unberechtigte Kenntnisnahme der vertraulichen Informationen erlangen konnten. Geeignete Zustellformen sind insbesondere die Verwendung von verschlossenen Kuverts und die Absicherung der vertraulichen Informationen durch "High-Security-Labels".

Sofern bei Übergabe nicht die Unversehrtheit der Signaturerstellungseinheit beziehungsweise der Transporteinrichtung festgestellt werden kann, ist der Signator verpflichtet den ZDA davon in Kennntis zu setzen. Dieser hat das ausgestellte Zertifikat zu widerrufen. Die Verantwortung des Signators zur Prüfung der Unversehrtheit und der Meldung von möglichen Verletzungen der Unversehrtheit wird dem Signator vor Vertragsabschluss im Rahmen der jeweils anzuwendenden Certificate Policy zur Kenntnis gebracht.

(ix) Rahmenbedingungen

Sofern Fertigungsschritte beim Hersteller oder bei sonstigen Dienstleistern auf Wunsch des ZDA durchgeführt werden, die keine Zertifizierung einer Bestätigungsstelle aufweisen, wird im Einzelfall eine ausreichende Beaufsichtigung im Sinne dieser GLOBALTRUST® Certificate Policy in Verbindung mit der jeweils anzuwendenden GLOBALTRUST® Certificate Practice Statement vereinbart.

Eine ausreichende Beaufsichtigung ist vereinbart, wenn
(a) der Hersteller verantwortliche Aufsichtspersonen nennt, diese eine ausreichende Qualifikation aufweisen,
(b) der Betreiber die ordnungsgemäße Durchführung der Fertigungsschritte durch eigenes qualifiziertes Personal überwacht oder
(c) der Betreiber qualifizierte Dritte nennt, der die ordnungsgemäße Durchführung der Fertigungsschritte überwacht.

In allen Fällen ist die ordnungsgemäße Durchführung der Fertigungsschritte durch das überwachende Personal zu bestätigen.

Die Ausstellung des Zertifikats kann durch den Betreiber, einem beauftragten Dienstleister oder durch den Hersteller der Signaturerstellungseinheit im Auftrag des Betreibers erfolgen.

Der gesamte Ablauf der Initialisierung der Signaturerstellungseinheiten wird protokolliert.

(b) Herstellervorgabe

Die Ausstellung von Signaturerstellungseinheiten kann vollständig oder teilweise auch durch einen vom Hersteller der Signaturerstellungseinheit vorgegebenen Prozess erfolgen, wenn dieser Prozess von einer Aufsichtstelle für die Ausstellung qualifizierter Zertifikate bzw. Erstellung qualifizierter elektronischer Signaturen genehmigt bzw. anerkannt ist.

(c) Policyvorgabe

Die Ausstellung von Signaturerstellungseinheiten kann auch in der jeweils anzuwenden GLOBALTRUST® Certificate Practice Statement vorgegeben werden. In diesem Fall ist klarzustellen, ob die Ausstellung ausschließlich nach diesen Vorgaben erfolgt oder ob die Vorgaben des GLOBALTRUST® Certificate Practice Statement alternativ (optional) zur Ausstellung gemäß diesem GLOBALTRUST® Certificate Policy anzuwenden sind.

6.1.1 Erzeugung von Schlüsselpaaren/ Key pair generation

Erzeugung der privaten Schlüssel und des Zertifikates zu den CA-Zertifikaten

Die notwendigen Schlüssel zur Erbringung der Zertifizierungsdienste gemäß dieser Policy werden in einem dedizierten System nach dem Vier-Augen-Prinzip generiert und inklusive der verwendeten Methoden und Formate dokumentiert. Soweit diese Schlüssel zur Ausstellung von qualifizierten Zertifikaten verwendet werden, zur Ausstellung von qualifizierten Zeitstempeln oder für sonstige Diensterbringung erforderlich sind, werden sie in Systemen erstellt, die den Anforderungen [ETSI TS 101 456] in der zum Zeitpunkt der Schlüsselerstellung gültigen Version insbesondere [SigV]entsprechen. Diese Erstellung erfolgt gemäß den zum Zeitpunkt der Erstellung gültigen Regeln, insbesondere kann sie von einer unabhängigen Person überwacht oder auf Video festgehalten werden.

Die Signaturschlüssel des Betreibers die für die Zertifizierungsdienste, insbesondere die zur Ausstellung von Endkundenzertifikaten dienen, werden auf sicherer HSM Hardware erstellt. Sie sind nicht öffentlich verfügbar, sind auch nicht bei Dritten hinterlegt.
Die sicherheitstechnischen Anforderungen, die die HSM Module und das Signaturserver-System erfüllen müssen, werden in der GLOBALTRUST® Certificate Security Policy spezifiziert.

Erzeugung der privaten Schlüssel des Signators

Die Schlüssel des Signators werden abhängig vom betriebenen Zertifizierungsdienst entweder vom Signator oder vom Betreiber erzeugt.

Werden Schlüssel zu qualifizierten Zertifikaten erstellt, ist die Verwendung geeigneter sicherer Signaturerstellungseinheiten zwingend erforderlich. Geeignete Signaturerstellungseinheiten werden auf Anfrage vom ZDA bekannt gegeben oder auf der Website des ZDAs veröffentlicht. Deren Anforderung und der Prozess der Ausstellung ist in ⇨ 6.1 Erzeugung und Installation von Schlüsslpaaren / Key pair generation and installation (p70) beschrieben

6.1.2 Zustellung privater Schlüssel an den Signator / Private key delivery to subscriber

Private oder geheime Schlüssel werden in keinem Fall im Klartext-Format verteilt. Sie werden zumindest als verschlüsselte Datei gespeichert und verteilt oder ihre Verteilung erfolgt über passwort-gesicherte verschlüsselte Verbindungen oder einer sonstigen dem Stand der Technik entsprechenden gesicherten Übertragung.

Die Zustellung von Signaturschlüssel zur qualifizierten elektronischen Signatur an den Antragsteller erfolgt nur in Verbindung mit einer geeigneten Signaturerstellungseinheit. Die Zustellung der Signaturerstellungseinheit erfolgt im Rahmen des anzuwendenden Prozesses. Dabei wird sicher gestellt, dass der berechtigte Signator die Signaturerstellungseinheit übernimmt.

Die Übergabe von sonstigen Schlüssels (die nicht zur für qualifizierte Zertifikate vorgesehen sind) erfolgt entweder mittels geeigneter Transportsicherungen, persönlich oder durch gesicherte (verschlüsselte) Datenübertragungswege. Zu keinem Übergabezeitpunkt kann auf den privaten Schlüssel ohne Kenntnis eines Passwortes zugegriffen werden.

Dem Signator wird nach Erstellung des Zertifikats eine Zertifizierungsbestätigung zugestellt. Sie enthält zumindest den Namen des Antragstellers, des Vertragsunterzeichners und enthält einen Hinweis auf die Bestimmungen der Policy.

Diese Zertifizierungsbestätigung bindet den Signator vertraglich an die anzuwendende Policy und ist von einer autorisierten Person (⇨ 4.2 Bearbeitung von Zertifkatsanträgen / Certificate application processing, p35) unterfertigt zu retournieren.

Abhängig von der Antragstellung erfolgt die Zustellung nach folgenden Regeln:

- Bei Zertifikaten für fortgeschrittene Signaturen und Amtssignaturen als gewöhnliche Post (soweit möglich auch als elektronische Post inkl. E-Mail oder Fax), sofern die Identitätsprüfung im Rahmen der Antragstellung schon abgeschlossen wurde.
- Bei Zertifikaten für fortgeschrittene Signaturen und Amtssignaturen über einen Zustelldienst, der auch eine Identitätsprüfung bei der Übergabe von Dokumenten anbietet (in Österreich ist das insbesondere die POST AG), sofern die Identitätsprüfung noch nicht vollständig abgeschlossen wurde und nur eine Plausibilitätsprüfung der Identitätsangaben vorliegt. In Fall der POST AG werden Poststücke als "eingeschrieben, eigenhändig mit Rückschein" zugestellt, bei anderen Zustelldiensten werden gleichwertige Verfahren verwendet. Die Identitätsprüfung gilt in diesem Fall als abgeschlossen, wenn die zugestellte Zertifizierungsbestätigung unterschrieben retourniert wird und die darin enthaltene Unterschrift mit der Unterschrift auf vorab vorgelegten amtlichen Dokumenten vergleichbar ist. Bei erheblichen Abweichungen wird über einen getrennten Weg ein Unterschriftsprobenblatt mit der aktuellen Unterschrift des Antragstellers angefordert.
- Bei Zertifikaten für fortgeschrittene Signaturen und Amtssignaturen durch persönliche Abholung beim ZDA oder bei einer Registrierungsstelle, sofern die Identitätsprüfung noch nicht vollständig abgeschlossen wurde. Die Identitätsprüfung gilt als abgeschlossen, wenn die ausgehändigte Zertifizierungsbestätigung vor einer autorisierten Person unterschrieben wird und sich der Antragsteller durch ein amtliches Dokument (Original) ausweisen kann. Der Vorgang ist durch die autorisierte Person zu bestätigen.
- Bei qualifizierten Zertifikaten sind die Zustellungsvarianten ident wie bei Zertifikaten für fortgeschrittene Signaturen und Amtssignaturen zulässig, jedoch mit der Einschränkung, dass beim Betreiber erstellte geeignete Signaturerstellungseinheiten mit Transportsicherung (⇨ (viii) Transportsicherung, p73) ausgeliefert werden. Vom Erfordernis der Transportsicherung kann abgesehen werden, wenn die Signatur-erstellungseinheit von einer autorisierten Personen persönlich an den Signator übergeben wird oder wenn die Signaturerstellungseinheit vom Betreiber unter Aufsicht des Signators erstellt wurde. In diesem Fall ist der Signator verpflichtet unverzüglich (im Beisein der autorisierten Person) die Unversehrtheit der Signaturerstellungseinheit zu prüfen und durch ein eigenen nur ihm bekannten Authorisierungscode zu sichern. Die Signaturfunktion kann nur durch Verwendung von diese Authorisierungscodes ausgelöst werden. Die Verwendung der Authorisierungscodes kann zusätzlichen Beschränkungen, etwa der [SigRL] oder spezifischen Vorgaben der Aufsichtsstelle unterliegen.
- Bei Zertifikate auf Signaturerstellungseinheiten, die für einfache Signaturen vorgesehen sind, auch als gewöhnliche Post, sofern keine vernünftigen Zweifel zu den Identitätsangaben des Antragstellers existieren. Der ZDA behält sich vor, auf Grund technischer oder rechtlicher Vorgaben auch für diese Zertifikate die Zustellanforderungen gemäß Zertifikate für fortgeschrittene Signaturen anzuwenden.
- Für sonstige Zertifikate, die für einfache Signaturen vorgesehen sind, erfolgt die Zustellung in einer Form, die die zuverlässige und sichere Kenntnisnahme durch den Signator erlaubt (sofern geeignet auch als elektronische Post inkl. E-Mail oder Fax). Der ZDA behält sich vor, auf Grund technischer oder rechtlicher Vorgaben auch für diese Zertifikate die Zustellanforderungen gemäß Zertifikate für fortgeschrittene Signaturen anzuwenden.

Nach Erhalt und erfolgreicher Unterschriftsprüfung der vom Empfänger unterfertigten Zertifizierungsbestätigung wird der Zugang zu einfachen Zertifikaten und/oder privatem Schlüssel freigegeben. Sofern die Zustellung des privaten Schlüssels nicht in Form einer hardwarebasierten Signaturerstellungseinheit erfolgt, muss der Schlüssel über eine gesicherte Verbindung heruntergeladen werden, die folgende Mindestkriterien erfüllt:
- Ende-zu-Ende Verschlüsselung des Übertragungsweges,
- Authentifizierung des Antragstellers (zumindest mit dem vom Antragsteller selbst vergebenen Aktivierungspassworts und der in der Zertifizierungsbestätigung genannten Referenznummer⇨ GLOBALTRUST® Certificate Practice Statement Abschnitt 4.1 7.,
- Verschlüsselung des Schlüssel durch ein vom Antragsteller vergebenes Passwort.

6.1.3 Zustellung öffentlicher Schlüssel an den ZDA / Public key delivery to certificate issuer

Die in einer Registrierungsstelle erzeugten Zertifikatsdaten werden signiert und verschlüsselt an die Zertifizierungsstelle des Betreibers übertragen. Vertraulichkeit und Integrität sämtlicher Daten sind sicher gestellt. Das Erfordernis der Verschlüsselung und Signatur besteht nicht, wenn die übermittelten Daten nur Antragsgrundlage sind und beim ZDA erst nach inhaltlicher und formaler Prüfung in die Zertifikate übernommen werden.

Nicht zertifizierte öffentliche Schlüssel werden nicht verteilt und werden ausschließlich innerhalb der gesicherten Zertifizierungsumgebung verwaltet.

Die Integrität und Authentizität der öffentlichen Schlüssel anlässlich der Verteilung bleibt insbesondere durch folgende Maßnahmen gewahrt:
- durch Übergabe des öffentlichen Root-CA- und Sub-CA-Schlüssels zur Veröffentlichung an die Aufsichtsstelle durch Übermittlung eines signierten PKCS#10 Certificate Requests,
- durch Ausstellung und Veröffentlichung der Root-CA- und Sub-CA-Zertifikate auf der Website oder eines Verzeichnisdienstes des ZDA,
- durch freiwillige Zertifizierungen durch anerkannte (private oder staatliche) Audit- und Prüfeinrichtungen,
- durch Publikation und Integration in Software vertrauenswürdiger Drittfirmen. Der aktuelle Stand der Integration des Root-Zertifikates bei Drittfirmen kann über die Website des ZDAs abgerufen werden.

Im Zusammenhang mit Zertifikaten für fortgeschrittene und einfache Signaturen muss zumindest eine der Veröffentlichungsformen erfüllt sein. Im Zusammenhang mit qualifizierten Zertifikaten ist jedenfalls eine Veröffentlichung durch die vorgesehene Aufsichtsstelle erforderlich.

Bei der Übergabe der oben beschriebenen Daten an Dritte wird die Integrität gesichert, insbesondere durch den Einsatz von Signaturen oder Prüfsummen.

6.1.4 Verteilung öffentliche CA-Schlüssel / CA public key delivery to relying parties

Die Bereitstellung, der Zugriff und die Verbreitung von zertifikatsrelevanten Informationen (Informationsobjekten jeglicher Art) erfolgt ausschließlich gemäß den Vorgaben dieser GLOBALTRUST® Certificate Policy, dem anzuwendenden

GLOBALTRUST® Certificate Practice Statement und der
GLOBALTRUST® Certificate Security Policy. Dabei ist sicher gestellt, dass nur berechtigte Benutzer lesenden Zugriff auf die bereitgestellten Informationen haben und dass ein schreibender Zugriff nur in Übereinstimmung mit den definierten Zertifizierungsprozessen und der vorgegebenen Rollenverteilung gemäß Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) erfolgt..
Die Verbreitung von Zertifikaten an Dritte erfolgt gemäß den Vorgaben des Antragstellers und den zwingenden rechtlichen Vorgaben. Der ZDA bedient sich dabei geeigneter technischer Verfahren.

6.1.5 Schlüssellängen / Key sizes

Die verwendeten Standards, Algorithmen und Schlüssellängen für Zertifikate und Schlüssel entsprechen den zum Zeitpunkt der Erstellung gültigen technischen Empfehlungen der jeweils zutreffenden Aufsichtsbehörde, nationalen oder internationalen Bestimmungen, den ETSI-Standards, den Vorgaben jener Dokumente, zu denen der Zertifizierungsdienst konform ist (⇨ 8. Prüfung der Konformität und andere Beurteilungen / COMPLIANCE AUDIT AND OTHER ASSESSMENTS, p95) oder den Vorgaben anderer (privater oder staatlicher) Einrichtungen, die zur Prüfung der Zertifizierungsdienste des ZDAs herangezogen werden. Soweit die verschiedenen Empfehlungen unterschiedliche Anforderungen und Sicherheitsniveaus beschreiben wird jene Variante gewählt die zumindest den Mindestanforderungen aller relevanten Empfehlungen entspricht.

Soweit bei der Erstellung von Zertifikaten oder Schlüsseln für verschiedene Zeitpunkte unterschiedliche Anforderungen zur Anwendung kommen, beispielsweise auf Grund neuer Sicherheitsanforderungen, werden die geänderten Anforderungen auf der Website des ZDA veröffentlicht oder auf Wunsch Aufsichtsbehörden, Auditstellen oder sonstigen Partnern des ZDA zugänglich gemacht.

6.1.6 Festlegung der Schlüsselparameter und Qualitätskontrolle / Public key parameters generation and quality checking

Die Festlegung der Schlüsselparameter folgt denselben Abläufen und Maßnahmen wie unter ⇨ 6.1.5 Schlüssellängen / Key sizes (p78) festgelegt.

Die Qualität der erzeugten Schlüssel wird laufend gemäß Stand der Technik geprüft.

6.1.7 Schlüsselverwendung / Key usage purposes (as per X.509 v3 key usage field)

Die vorgesehene ausschließliche Verwendung des Schlüssels zur elektronischen Signatur ist - soweit technisch möglich und sinnvoll - im Zertifikat erkennbar zu machen, in den anderen Fällen durch einen entsprechenden Hinweis im anzuwendenden GLOBALTRUST® Certificate Practice Statement.

Der private Schlüssel der Zertifizierungsstelle wird nur für die Erstellung von den dafür ausdrücklich vorgesehenen Zertifikaten und für die Signatur der zugehörigen Widerrufslisten innerhalb der für die Zertifizierung bestimmten Räumlichkeiten verwendet.

6.2 Schutz des privaten Schlüssels und Anforderungen an Signaturerstellungseinheiten / Private Key Protection and Cryptographic Module Engineering Controls

Alle Maßnahmen, die die Signaturschlüssel betreffen, insbesondere die Erzeugung der Schlüssel, allfällige Export- und Importvorgänge, Backup oder Wiederherstellung, erfolgen - soweit diese Maßnahmen rechtlich zulässig sind - nach dem Vier-Augen-Prinzip ausschließlich durch autorisierte Personen und werden protokolliert, wobei das Protokoll Angaben zum Vorgang, zur verwendeten Hardware und zu den verantwortlichen Personen enthält. Die Generierung erfolgt jedenfalls nach dem Vier-Augen-Prinzip. Zur Generierung wird ein Protokoll gemäß interner Dokumentation erstellt.

Der Betreiber kann für verschiedene Zertifizierungsdienste unterschiedliche Signaturerstellungsdaten verwenden. Die gültigen und abgelaufenen Signaturerstellungsdaten (inkl. Zertifikate und sonstige Signaturprüfdaten, insbesondere Hash-Werte) werden auf der Webseite des Betreibers veröffentlicht, nicht jedoch die geheimen Signaturschlüssel. Alle ausgestellten Zertifikate enthalten einen Verweis (Link) wo die entsprechenden Signaturerstellungsdaten und die anzuwendende Certificate Policy des Betreibers abrufbar sind.

Für die Ausstellung von qualifizierten Zertifikaten sind jedenfalls eigene Signaturerstellungsdaten zu erzeugen. Diese Signaturerstellungsdaten werden nur zur Ausgabe und dem Widerruf qualifizierter Zertifikate verwendet.

Abhängig von der Kategorie des Schlüssels erfolgen unterschiedliche Risikobewertungen und Sicherheitsmaßnahmen der Schlüssel. Jedenfalls werden für alle Schlüssel folgende Punkte geregelt:
- Schlüsselgenerierung und -verteilung
- Schlüsselverwendung
- Schlüsseländerungen
- Schlüsselzerstörung bei Kompromittierung und/oder Ende seines Lebenszyklus
- Schlüsselspeicherung, -backup und -wiederherstellung
- Schlüsselarchivierung

Die Signaturschlüssel der ⇨ **Kategorie 1** (p69) haben die längste Laufzeit und für sie besteht das höchste Risiko. Sie werden im Rahmen der GLOBALTRUST® Certificate Security Policy einer gesonderten Bewertung unterzogen und unterliegen besonderen Sicherheitsmaßnahmen.

Allfällig notwendige zusätzliche Sicherheitsanforderungen der Schlüssel der ⇨ **Kategorie 2** (p69, "Infrastrukturschlüssel") werden in der GLOBALTRUST® Certificate Security Policy im Rahmen der Sicherheitsmaßnahmen jener Einrichtungen behandelt, in den sie eingesetzt sind. Soweit technisch möglich und organisatorisch sinnvoll werden für unterschiedliche Dienste/Zwecke unterschiedliche Infrastrukturschlüssel verwendet. Diese Schlüssel sind nicht ident mit Signaturschlüssel der ⇨ **Kategorie 1** (p69).

Die Schlüssel der ⇨ **Kategorie 3** (p69, "Identifikationsschlüssel") werden auschließlich an autorisiertes Personal vergeben und dienen zur Unterstützung und Vereinfachung von Identifikations- und Authentisierungsprozessen.

Alle privaten und geheimen Schlüssel werden sicher aufbewahrt, die Schlüssel der ⇨ **Kategorie 2** und 3 (p69) werden jedenfalls in für Kryptographie geeigneter Hardware erzeugt und verwaltet. Sofern die Schlüssel vom ZDA ausgestellt werden, gelten für die Ausstellung der Zertifikate sinngemäß dieselben Anforderungen wie unter ⇨ 4.3 Zertifikatsausstellung / Certificate issuance (p36) beschrieben. Soweit Schlüssel durch Drittanbieter verwendet werden, werden jene herangezogen, die vergleichbar mit ausgestellten Schlüsseln des ZDA sind. Die Verteilung erfolgt gemäß denselben Kritieren wie die Ausgabe von Zertifikaten, die für fortgeschrittene elektronische Signaturen von Antragstellern vorgesehen sind. Bei Verwendung der Zertifikate basierend auf den Schlüsseln der ⇨ **Kategorie 2** und 3 (p69) wird sichergestellt, dass diese noch gültig sind. Dies kann durch Prüfung der zugehörigen Widerrufsstatusinformationen oder anderer geeigneter technischer oder organisatorischer Maßnahmen erfolgen, insbesondere durch Maßnahmen im Rahmen der Betriebsüberwachung. Die Schlüssel der ⇨ **Kategorie 2** und 3 (p69) werden zeitgerecht vor Ablauf, wenn es objektive Hinweise darauf gibt, dass die verwendeten Algorithmen nicht mehr ausreichend sicher sind oder aus sonstigen Gründen erneuert werden, in sicherer Weise gewechselt.

Keiner gesonderten Dokumentation oder Überwachung unterliegen die Schlüssel der ⇨ **Kategorie 4** (p69), die nur kurzzeitig in Verwendung sind.

6.2.1 Standards und Sicherheitsmaßnahmen für Signaturerstellungseinheiten / Cryptographic module standards and controls

Zur qualifizierten elektronischen Signatur werden sichere Signaturerstellungseinheiten zur Verfügung gestellt.

Der ZDA stellt eine Liste der geeigneten Signaturerstellungsprodukte auf Anfrage und/oder über seine Website zur Verfügung.

Teil dieser Dokumentation ist die Angabe gemäß welcher Algorithmen und Parameter den Anforderungen für eine sichere Signaturerstellungseinheit entsprochen wird. Diese Angaben erfolgen gemäß den zu den Signaturerstellungseinheiten vorliegenden Bescheinigung(en). Alternativ ist auch der Verweis auf eine öffentlich zugängliche Bescheinigung (Zertifizierung) zulässig, die die erforderlichen Angaben enthält.

Private Schlüssel zur Signatur von Zertifikaten werden verwendet, solange die verwendeten Algorithmen als sicher im Sinne der Definition ⇨ Sichere Signaturerstellungseinheit, sicherer Schlüssel (p24) anzusehen sind.

Für die Erbringung der Zertifizierungsdienste verwendet der Betreiber ein HSM-System das redundant ausgeführt ist, der Datenabgleich zwischen den einzelnen Hardwaremodulen erfolgt in einem gesicherten Format, das Teil der Sicherheitszertifizierung der eingesetzten Hardware ist.

Die Liste der vom Betreiber verwendeten HSM-Produkte ist intern dokumentiert. Die Inbetriebnahme erfolgt mittels eines schriftlichen Protokolls. Form und Inhalt des Protokolls sind intern dokumentiert.

Zu den Signaturerstellungseinheiten und -verfahren wird dokumentiert auf Basis welcher Bescheinigung und welcher Bestätigungsstelle die Voraussetzungen für qualifizierte elektronische Signatur erfüllt sind. Bescheinigungen der Aufsichtstellen sind gleichwertig.

Soweit sich Bescheinigungen nur auf einzelne technische Komponenten beziehen dürfen diese für qualifizierte Signaturen nur in Kombinationen eingesetzt werden, die in ihrer Gesamtheit die Sicherheitsanforderungen für die qualifizierte Signatur erfüllen. Geeignete Kombinationen von technischen Komponenten können im ⇨ Anhang A: 3 Unterstützte Signaturerstellungsprodukte (p125) gelistet werden.

Bescheinigungen der Aufsichtstellen werden als Kopie oder als Verweis auf die Fundstellen der Aufsichtstellen vom Betreiber in Evidenz gehalten.

Erfüllen nur einzelne technische Komponenten diese Anforderungen, dann können sie nur in einer gesicherten Umgebung eingesetzt werden. Die Anforderungen dieser gesicherten Umgebung werden in der GLOBALTRUST® Certificate Security Policy festgelegt.

6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m) / Private key (n out of m) multi-person control

Die privaten Schlüssel der CA-Zertifikate des Betreibers werden gemäß 4-Augen-Prinzip genutzt.

6.2.3 Hinterlegung privater Schlüssel (key escrow) / Private key escrow

Nicht zutreffend

6.2.4 Backup privater Schlüssel / Private key backup

Die privaten Schlüssel der CA-Zertifikate des Betreibers bleiben im für die Durchführung der Zertifizierung vorgesehenen System redundant gespeichert.

Private Schlüssel der CA-Zertifikate des Betreibers, die den Sicherheitsanforderungen nicht mehr entsprechen oder aus anderen Gründen nicht mehr weiter betrieben werden, werden gelöscht. Es erfolgt keine Archivierung nicht mehr aktiver Schlüssel.

Entsprechen private Schlüssel der Signatoren nicht den Sicherheitsanforderungen gemäß den Zwecken, zu denen sie ausgegeben wurden, wird der Signator unverzüglich darüber informiert und aufgefordert den Schlüssel nicht weiter zu benutzen und zu löschen.

6.2.5 Archivierung privater Schlüssel / Private key archival

Die privaten Schlüssel der CA-Zertifikate des Betreibers bleiben im für die Durchführung der Zertifizierung vorgesehenen System gespeichert, es erfolgt keine Archivierung außerhalb des Zertifizierungssystems.

Allfällig vorhandene Archiv-Kopien von privaten Schlüsseln der Signatoren werden beim Betreiber so gesichert aufbewahrt, dass eine unbeabsichtigte Übernahme in produktive Systeme nicht möglich ist.

Kopien der privaten Schlüssels der Signatoren werden - sofern beim Betreiber vorhanden - nach Ende des Übergabeverfahrens beim Betreiber gelöscht.

In keinem Fall werden private Schlüssel in einem unverschlüsseltem Format, etwa als Text / "plain-text" gespeichert.

6.2.6 Transfer privater Schlüssel in oder aus Signaturerstellungseinheiten / Private key transfer into or from a cryptographic module

Ein Transfer von privaten Schlüsseln der CA-Zertifikate des Betreibers oder von privaten Schlüsseln die für qualifizierte Zertifikate dienen aus Signaturerstellungseinheiten wird ausgeschlossen.

6.2.7 Speicherung privater Schlüssel auf Signaturerstellungseinheiten / Private key storage on cryptographic module

Alle privaten Schlüsseln werden auf geeigneten Signaturerstellungseinheiten ge speichert.

Soweit Schlüssel der ⇨ Kategorien 1 bis 3 außerhalb der vorgesehen sicheren Systeme gespeichert werden müssen ("Schlüsselexport") erfolgt dies nach einer dem Stand der Technik entsprechende Sicherung der Vertraulichkeit, etwa durch kryptographische Maßnahmen die die Anforderungen von [ETSI TS 102 176] erfüllen und im Einklang mit den Sicherheitsmaßnahmen des sicheren Moduls sind.

Zur Sicherung der Authentizität der öffentlich verfügbaren Prüfdaten können Schlüssel der ⇨ **Kategorie 1** (p69) durch andere Zertifkate des ZDAs in derselben Vertrauensstufe, durch Zertifikate von Aufsichtstelle, Behörden, sonstigen vertrauenswürdigen Dritten, Cross-Zertifiziert werden. Dies gilt insbesondere zur Sicherung der Kontinuität der Vertrauenswürdigkeit abgelaufener oder neuer Signaturzertifikate des ZDA. Eine Cross-Zertifizierung erfolgt nur, wenn die Anforderung ausreichend authentisiert ist, die Integrität gewahrt ist und sichergestellt ist, dass keine Verfälschung der Anforderungen, insbesondere durch Replay-Angriffe möglich ist. Im übrigen erfolgt die Prüfung der Anforderungen gemäß ⇨ 4.1 Antragstellung / Certificate Application (p34).

Sofern geheime oder private Schlüssel im Klartext vorliegen, besteht die Möglichkeit die entsprechenden Speicherbereiche mit Nullen zu überschreiben

6.2.8 Aktivierung privater Schlüssel / Method of activating private key

Die Verwendung der Schüssel der CA-Zertifikate, die für die Erbringung der Zertifizierungsdienste erforderlich sind, ist im Falle der Ausgabe qualifizierter Zertifikate durch je zwei autorisierte Personen erlaubt, in den anderen Fällen können Zertifikate auch nur durch eine autorisierte Person erstellt werden.

6.2.9 Deaktivierung privater Schlüssel / Method of deactivating private key

Die Signaturerstellungseinheiten die die privaten Schlüssel der CA-Zertifikate des Betreibers beinhalten, werden bei der Beendigung des Zertifizierungssystems automatisch deaktiviert.

6.2.10 Zerstörung privater Schlüssel / Method of destroying private key

Private Schlüssel, von CA-Zertifikaten die den Anforderungen des Betreibers nicht entsprechen werden unverzüglich so gelöscht, dass eine Rekonstruktion nach Stand der Technik nicht möglich ist.. Dazu werden eine Reihe von Maßnahmen gesetzt:

- Signaturerstellungseinheiten die den privaten Schlüssel enthalten, werden außer Betrieb genommen.
- Zertifikate, die auf Grundlage des privaten Schlüssels ausgestellt wurden, werden widerrufen.
- Es werden technische und organisatorische Maßnahmen gesetzt, die eine Neuausstellung von Zertifikaten zu einem deaktivierten privaten Schlüssel verhindern.

Können auf Signaturerstellungseinheiten private Schlüssel nicht mit ausreichender Sicherheit gelöscht werden, wird die gesamte Signaturerstellungseinheit zerstört.

6.2.11 Beurteilung Signaturerstellungseinheiten / Cryptographic Module Rating

Die Signaturerstellungseinheiten werden gemäß ⇨ Sichere Signaturerstellungseinheit, sicherer Schlüssel (p24) bewertet.

6.3 Andere Aspekte des Managements von Schlüsselpaaren / Other aspects of key pair management

6.3.1 Archvierung eines öffentlichen Schlüssels / Public key archival

Öffentliche Schlüssel des ZDA und der Signatoren werden so archiviert, dass die Rekonstruierbarkeit und Prüfbarkeit für die zugesagte Dauer der Zertifikate gesichert ist.

6.3.2 Gültigkeitsdauer von Zertifikaten und Schlüsselpaaren / Certificate operational periods and key pair usage periods

Die zulässige Verwendung eines Signaturschlüssels zur elektronischen Signatur beginnt mit Aufhebung der Transportsicherung bzw. mit Übergabe der Signaturerstellungsdaten an den Signator, jedoch nicht vor Beginn des im Zertifikat eingetragenen Gültigkeitsdatums und endet spätestens mit dem im Zertifikat eingetragenen Endedatum der Gültigkeit, geht jedoch keinesfalls über das Widerrufsdatum des Zertifikats hinaus.

Der maximal zulässige Gültigkeitszeitraum richtet sich bei qualifizierten Zertifkaten nach den gesetzlichen Anforderungen und Vorgaben der Aufsichtsbehörden, in den anderen Fällen nach der jeweiligen Produktbeschreibung und den individuellen Anforderungen des Signators. Für einfache Zertifikate ist eine von der Policy abweichende Gültigkeitsdauer möglich, diese muss mit dem Signator vereinbart werden und kann nicht länger sein, als die maximal zulässige Gültigkeitsdauer des ausstellenden CA-Zertifikates.

Bei Serverzertifikaten mit einem Gültigkeitsbeginn nach dem 1.7.2012, beträgt die maximale Gültigkeitsdauer 60 Monate. Bei Serverzertifikaten mit einem Gültigkeitsbeginn nach dem 1.4.2015, beträgt die maximale Gültigkeitsdauer 39 Monate. Die maximale Gültigkeitsdauer von EV Zertifikaten beträgt 27 Monate.

Eine innerhalb des Gültigkeitszeitraums ausgestellte elektronische Signatur behält auch nach Ablauf der Gültigkeit, bei Sperre oder Widerruf des Zertifikates ihre Gültigkeit.

6.4 Aktivierungsdaten / Activation data

6.4.1 Generierung und Installation von Aktivierungsdaten / Activation data generation and installation

Fortgeschrittene Signaturen oder Signaturen, die mit einem qualifizierten Zertifikat versehen werden können nur mit Hilfe von Aktivierungsdaten ausgelöst werden.

6.4.2 Schutz von Aktivierungsdaten / Activation data protection

Aktivierungsdaten sind vertraulich zu halten und so aufzubewahren, dass eine unrechtmäßige Verwendung nach dem Stand der Technik nicht möglich ist.

6.4.3 Andere Aspekte von Aktivierungsdaten / Other aspects of activation data

Der Betreiber verpflichtet den Signator zur vertraulichen Behandlung seiner Aktivierungsdaten und unterstützt ihn- sofern rechtlich zulässig und ausdrücklich gewünscht- bei deren Auswahl.

6.5 Sicherheitsmaßnahmen IT-System / Computer security controls

Die zum Betrieb der Zertifizierungsdienste erforderlichen technischen Komponenten sind von sonstigen (Büro-)Einrichtungen des Betreibers hard- oder softwaretechnisch getrennt. Die im Rahmen der Zertifizierungsdienste erforderlichen organisatorischen und administrativen Maßnahmen sind dokumentiert, die getätigten Schritte können bei Bedarf nachvollzogen werden.

Soweit zur Ausstellung von Signaturerstellungsdaten eine Kommunikation mit den in einem Rechenzentrum installierten Zertifizierungskomponenten erforderlich ist, erfolgt sie gemäß den Vorgaben der GLOBALTRUST® Certificate Security Policy in einer Form, die die Kompromittierung der Zertifizierungsdienste wirksam verhindert, jedenfalls in Form eines gesicherten virtuellen privaten Netzes (VPN). Neben der technischen Absicherung werden dabei auch organisatorische Maßnahmen, wie Beschränkung der Zugriffsberechtigten, Beschränkung der zum Zugriff technisch geeigneten Geräten gesetzt.

Die Integrität der Computersysteme und Informationen ist gegen Viren und böswillige oder unautorisierte Software geschützt.

Kapazitätserfordernisse werden beobachtet und künftige Entwicklungen prognostiziert, sodass stets angemessene Bandbreiten, Prozessorleistungen und sonstige IT-Ressourcen zur Verfügung stehen.

Die sicherheitskritischen Funktionen im Rahmen der Zertifizierungs- und Widerrufsdienste werden von den gewöhnlichen administrativen Funktionen getrennt. Als sicherheitskritische Funktionen werden alle IT-Maßnahmen angesehen, die zur Erhaltung der Betriebsfähigkeit des Zertifizierungsdienstes dienen. Insbesondere sind dies

- Planung und Abnahme von Sicherheitssystemen,
- Schutz vor böswilliger Software und Angriffen,
- Aktive Überprüfung von Log-Files und Prüfberichten, Analyse von Zwischenfällen,
- Allgemeine System-Wartungstätigkeiten,
- Netzwerkadministration,
- Datenmanagement, Datenträgerverwaltung und –sicherheit,
- Softwareupdates.

6.5.1 Spezifische technische Sicherheitsanforderungen an die IT-Systeme / Specific computer security technical requirements

Die erforderlichen Sicherheitsanforderungen werden komponentenspezifisch definiert und umgesetzt und sind in der GLOBALTRUST® Certificate Security Policy dokumentiert.

6.5.2 Beurteilung der Computersicherheit / Computer security rating

Die Sicherheit des gesamten Zertifizierungssystems wurde einer Risikoanalyse unterzogen. Die Vorgangsweise der Analyse, die Ergebnisse und Maßnahmen sind intern, insbesondere in der GLOBALTRUST® Certificate Security Policy dokumentiert und werden jedenfalls im Zuge der vorgesehenen Audits regelmäßig evaluiert.

6.6 Technische Maßnahmen während des Lebenszyklus / Life cycle technical controls

Alle zertifizerungsrelevanten technischen Komponenten unterliegen während ihres gesamten Lebenszyklus einem laufenden Monitoring und sind über den gesamten Lebenszyklus dokumentiert.

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung / System development controls

Die Systementwicklung erfolgt in vom Echtbetrieb getrennten Entwicklungssystemen.

Die für die Zertifizierungsdienste notwendigen Prozesse werden laufend weiterentwickelt und optimiert. Neben einer Optimierung der Sicherheit bestimmt auch die Verbesserung der Kundenfreundlichkeit die Systementwicklung.

Die in Betrieb befindlichen Softwaremodule werden elektronisch signiert. Die Signaturen werden laufend geprüft, unerwünschte Änderungen können erkannt werden.

Zur Installation neuer Softwaremodule existieren Übergabeverfahren.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement / Security management controls

Die erforderlichen Sicherheitsmaßnahmen sind in der GLOBALTRUST® Certificate Security Policy dokumentiert.

6.6.3 Sicherheitsmaßnahmen während des Lebenszyklus / Life cycle security controls

Die erforderlichen Sicherheitsmaßnahmen sind in der GLOBALTRUST® Certificate Security Policy dokumentiert.

6.7 Sicherheitsmaßnahmen Netzwerke / Network security controls

Die erforderlichen Sicherheitsmaßnahmen sind in der GLOBALTRUST® Certificate Security Policy dokumentiert.

6.8 Zeitstempel / Time-stamping

Qualifizierte und nicht-qualifizierte Zeitstempel werden gemäß GLOBALTRUST® Certificate Practice Statement ⇨ 6.8 Zeitstempel / Time-stamping erbracht.

Qualifizierte Zeitstempel werden durch ein Zertifikat mit der Zusatzbezeichnung "TIMESTAMP QUALIFIED" und einer Ziffer zur Unterscheidung unterschiedlicher Versionen des Dienstes ausgestellt.

Die Erbringung von Zeitstempeldiensten erfolgt auf Basis der [SigRL]. Die Genauigkeit der Zeitangaben (maximale Abweichung von der tatsächlichen Zeit) erfüllt die rechtlichen Anforderungen für qualifizierte Zeitstempeldienste und wird im GLOBALTRUST® Certificate Practice Statement spezifiziert.

Zeitstempeldienste werden als Serverdienste angeboten, wobei die technischen Einrichtungen denselben Sicherheits- und Betriebsanforderungen wie für die Ausstellung von Zertifikaten unterliegt. Die Server werden in gesicherter Umgebung betrieben und sind baulich, technisch und organisatorisch gegen unbefugte Veränderungen gesichert. Diese Anforderungen sind in der GLOBALTRUST® Certificate Security Policy beschrieben.

Mit dem Zeitstempel bestätigt der Betreiber das Bestehen eines bestimmten Hashwertes zum im Zeitstempel ausgewiesenen Zeitpunkt. Akzeptiert werden Hashwerte, die mit Algorithmen erstellt werden, die dem Stand der Technik entsprechen, wobei nationale und internationale Anforderungen, etwa von [ETSI TS 102 176] beachtet werden. Die akzeptierten Hash-Verfahren werden auf der Website http://www.globaltrust.eu/produkte.html veröffentlicht, wobei sich der ZDA ausdrücklich vorbehält, bestimmte Verfahren (auch ohne Angabe von Gründen) jederzeit auszuschließen bzw. neue, geeignete Verfahren zu akzeptieren.

Die Bestätigung des Zeitstempels erfolgt mittels elektronischer Signatur die durch Mechanismen erzeugt wird, die den gesetzlichen Anforderungen und aktuellen technischen Standards (insbesondere [ETSI TS 102 176]) entspricht. Insbesondere erfolgt die Generierung des Zeitstempels durch eigene nur für den Zeitstempeldienst vorgesehene Schlüssel, die in Hardware erzeugt und verwaltet werden, die zur Kryptographie geeignet ist. Zur Verwaltung des Schlüssels werden Produkte verwendet, die zur Ausstellung qualifizierter Zertifikate geeignet sind. Sie werden in einer Form betrieben, die die Ausstellung von Massensignaturen erlauben. Diese Produkte sind gegen unbefugtes Auslesen und Veränderung der Schlüssel gesichert.

Die für den Zeitstempeldienst erforderlichen Schlüssel und Zertifikate werden in derselben Weise erzeugt, wie allgemein in der Ausstellung des Endkundenschlüssel für den Signator

beschrieben (⇨4.1 Antragstellung / Certificate Application, p34). Alle relevanten Vorgänge des Zeitstempeldienstes, insbesondere im Zusammenhang mit der Schlüsselerzeugung, dem Schlüssel-Lebenszyklusmanagements und Fehlfunktionen des Zeitstempeldienstes inkl. Abweichungen von der zugesicherten Zeit werden dokumentiert.

Die Verfügbarkeit des Zeitstempeldienstes ist grundsätzlich in den Geschäftszeiten des ZDA, jedenfalls jedoch zu den gesetzlich vorgegebene Mindestzeiten gegeben. Davon abweichende, insbesondere darüber hinausgehende Verfügungszeiten, werden auf der Website http://www.globaltrust.eu/auditreport.html des Betreibers bekannt gegeben oder mit Nutzern des Zeitstempeldienstes individuell vereinbart.

Der Betreiber strebt eine 99%ige Verfügbarkeit des Zeitstempeldienstes an (weniger als 88 Stunden Ausfall im Jahr) und wird jährlich einen Bericht über die Ausfallszeiten für registrierte Benutzer des Zeitstempeldienstes und Aufsichtstellen bereit stellen. Aus der Unterschreitung der Verfügbarkeitszeit allein kann jedoch keine Gewährleistung abgeleitet werden.

Jeder Zeitstempel wird mit einer eindeutigen Seriennummer, dem ausstellenden Zertifikat, einer Genauigkeitsangabe (bzw. mit einem Verweis auf die zugehörige Policy, in der die Genauigkeit definiert ist) und den Bedingungen der Zeitstempelvergabe (bzw. mit einem Verweis auf die zugehörige Policy, in der die Bedingungen beschrieben sind) versehen.

Weiters enthält jeder Zeitstempel die Angabe, auf welche Anforderung (Hash-Wert) er sich bezieht. Jeder vergebene gültige Zeitstempel wird archiviert. Die Zeitangaben zu denen ein vorgelegter Hashwert signiert und der Hashwert selbst sind integraler Teil der durch den Zeitstempeldienst signierten Datenstruktur (⇨ Zeitstempel, Timestamp).

Die zur Feststellung eines gültigen Zeitstempels erforderlichen aktuellen Signaturprüfdaten können durch das Zertifikat, das den Zeitstempel ausstellt, festgestellt werden. Zeitstempelzertifikate enthalten Verweise auf ein oder mehrere CA-Zertifikate, das oberste Zertifikat ist in allen Fällen das GLOBALTRUST®-Root-Zertifikat, ein früheres oder ein nachfolgendes Root-Zertifikat, für das der Betreiber verantwortlich ist. Die Zertifikatsprüfdaten für die Zeitstempel (inkl. dem aktuellen Zeitstempelverfahren) sind auf der Website des ZDA unter http://www.globaltrust.eu/certificate-policy.html oder in einem in der anzuwendenden Certificate Policy genannten Link veröffentlicht. Ein vom ZDA ausgestellter Zeitstempel kann durch jede standardkonforme Software (Standard rfc3161) geprüft werden, darüber hinaus stellt der ZDA eine Prüfsoftware zur Verfügung, die von der Website des ZDA kostenfrei http://www.globaltrust.eu/certificate-policy.html geladen werden kann. Kann die Korrektheit eines Zeitstempels vom Nutzer nicht zweifelsfrei festgestellt werden, bietet der ZDA eine individuelle Prüfung der Zeitstempeldaten durch den ZDA an.

Die Prüfung eines Zeitstempels erfolgt durch Vergleich der Hashwerte eines bestehenden Dokuments mit dem signierten Hashwert aus der Datenstruktur des Zeitstempels. Sind die Hashwerte ident, wird damit die Existenz des Dokuments zum Zeitpunkt gemäß Zeitangaben im Zeitstempel bestätigt.

Bei Zeitstempel, die mit Verfahren erstellt werden, die gemäß [SigV] oder gemäß der Entscheidung der Aufsichtsstelle oder anerkannter Standardisierungsgremien (insbesondere gemäß den Empfehlungen [ETSI TS 102 176]) als nicht mehr sicher zuverlässig anzusehen

sind, werden die Anforderer - sofern ihre Identität bekannt ist und gültige Kontaktdaten vorhanden sind - über die fehlende Zuverlässigkeit des Zeitstempels informiert.

Der Betreiber gewährleistet eine Genauigkeit des Zeitstempels mit einer maximalen Abweichung von 60 Sekunden zur tatsächlichen Zeit. Sofern europarechtliche Vorgaben oder internationale Standards eine höhere Genauigkeit verlangen, wird diese gewährleistet. Aktuelle Informationen zur Zeitgenauigkeit werden auf der Website des ZDA http://www.globaltrust.eu/produkte.html oder auf Anfrage bekannt gegeben. Als tatsächliche Zeit wird UTC definiert. Die Maßnahmen zur Einhaltung der tatsächlichen Zeit sind im GLOBALTRUST® Certificate Practice Statement beschrieben.

7. PROFILE DER ZERTIFIKATE, WIDERRUFSLISTEN UND OCSP / CERTIFICATE, CRL, AND OCSP PROFILES

Inhalt und technische Beschreibung des Zertifikats sind der jeweiligen Anzeige bzw. den Ankündigungen auf der Website des ZDA zu entnehmen. Bei der Verwendung von standardisierten Zertifikatsformaten (z.B. X509v3) genügt der Verweis auf die anzuwendenden Standards, wie z.B. [RFC5280].

Für Server- und EV-Zertifikate gilt darüberhinaus folgendes:
- Weitere Informationen zum Antragsteller sind nur dann zulässig, wenn diese im Rahmen der Antragsprüfung überprüft wurden. Sofern es aufgrund mangelnder Information notwendig ist, werden Felder im Subject String komplett leer gelassen.
- Der Issuer String enthält jedenfalls den Eintrag organizationName (Identifikation des Zertifizierungsdienstanbieters) und countryName (Geschäftsstandort des Zertifizierungsdienstanbieters). Darüberhinausgehend höchstens die Felder commonName (Beschreibung der CA) und domainComponent (alle geordneten Teile des registrierten Domainnamens der CA).

Zu den ausgestellten Zertifikaten werden grundsätzlich standardisierte Verzeichnis- und Widerrufsdienste gemäß folgender technischer Standards und technischer Normen bereitgestellt:
- Verzeichnisdienst als LDAP-Dienst gemäß [RFC4511] und den dazugehörigen Standards.
- Widerrufsdienst als OCSP-Dienst gemäß [RFC2560] und den dazugehörigen Standards.
- Widerrufsdienst als CRL-Service gemäß [RFC5280] und den dazugehörigen Standards verbreitet.

Umfang und Technik der bereitgestellten Verzeichnis- und Widerrufsdienste ergibt sich aus den individuellen Eintragungen im Zertifikat, der jeweils anzuwendenden Certificate Policy, den gesetzlichen Vorgaben und individuellen Vereinbarungen.

7.1 Zertifikatsprofile / Certificate profile

Unterstützt werden alle Zertifikatsformate die im jeweiligen GLOBALTRUST® Certificate Practice Statement beschrieben sind, jedenfalls jedoch Zertifikate gemäß X.509v3. Die zu X.509v3-Zertifikaten verwendeten Verfahren und Algorithmen sind in [ITU-X509v3] und [RFC5280] dokumentiert. Zusätzlich werden Einschränkungen und Vorgaben jener Standards und Dokumente beachtet, zu denen der Zertifizierungsdienst konform ist, insbesondere Vorgaben, die sich insbesondere aus Empfehlungen der Aufsichtsstelle, [CABROWSER-BASE] oder [CABROWSER-EV] ergeben.

Qualifizierte Zertifikate enthalten jedenfalls die Angaben gemäß [ETSI TS 101 862]. Zusätzliche Angaben in den Zertifikaten sind möglich, sofern sie nicht irreführend, sachlich richtig und nicht gegen zwingende rechtliche Bestimmungen verstoßen.

Qualifizierte Zertifikate werden so ausgegeben, dass sie jedenfalls den Anforderungen der [SigRL] Anhang I, [ETSI TS 101 862] entsprechen. In Ländern in denen die [SigRL] keine

Wirksamkeit hat, gemäß jenen nationalen Bestimmungen, in denen der Antragsteller seinen Sitz hat.

Dazu ergänzend kann ein zulässiges qualifiziertes Zertifikat auch jene Angaben (ergänzend oder alternativ) enthalten, die auf Grundlage anderer Bestimmungen zulässig sind.

EV Zertifikate erfüllen die Kriterien von [CABROWSER-EV] und [WEBTRUST-EV].

Jedes Zertifikat wird mit einer eindeutigen Seriennummer ausgestellt.

Die Seriennummer eines Serverzertifikates enthält zumindest 64 bit Entropie.

In allen Fällen der Zertifikatserstellung, inklusive von "Re-Certification" und "Re-Key" werden die Zertifikate mit neuer eindeutiger Nummer ausgestellt. Ein Austausch von Zertifikaten mit derselben Nummer ist nicht vorgesehen und wird durch technische und organisatorische Maßnahmen verhindert. Die Anforderungen für die Zertifikatserstellung entsprechen in beiden Varianten "Re-Certification" und "Re-Key" zumindest den Anforderungen der Originalausstellung.

Die Zertifikate enthalten zumindest folgende Angaben:
- Name oder Bezeichnung des Signators, wobei Bezeichnungen so zu wählen sind, dass sie nicht mit Namen Dritter verwechselt werden können,
- allfällige Pseudonyme sind so gesondert gekennzeichnet eingetragen, dass sie nicht mit Vor- bzw. Familiennamen, offiziellen Firmen- oder Organisationsbezeichnungen verwechselt werden können,
- den öffentlichen Schlüssel, der dem privaten Schlüssel des Signators zugeordnet ist,
- die fortgeschrittene Signatur des ZDA,
- eindeutige Bezeichnung und Seriennummer des Zertifizierungsdienstes,
- ein Beginndatum der Gültigkeit des Zertifikates,
- ein Endedatum der Gültigkeit des Zertifikates, das nicht vor dem Beginndatum liegt,
- der verwendete Signaturalgorithmus muss dem Stand der Technik entsprechen, jedenfalls jedoch nationalen und internationalen Vorgaben entsprechen, im Falle von RSA-Schlüsseln mit einer Mindestlänge von 2048 bit, bei eliptischen Kurven (EC)http://www.globaltrust.eu/produkte.html,
- einen Verweis auf die anzuwendende Certificate Policy.

Für EV Zertifikate gilt darüberhinaus folgendes:
- Das Zertifikat enthält jedenfalls einen geprüften Organisationsnamen.
- Wildcard Einträge sind weder im subjectAltName noch im commonName erlaubt.
- Der Subject String enthält das Feld businessCategory mit dem Inhalt "Private Organization", "Government Entity" oder "Non-Commercial Entity", je nach Kategorisierung der Organisation des Antragstellers (⇨ **Fehler! Verweisquelle konnte nicht gefunden werden.**, p**Fehler! Textmarke nicht definiert.**).
- Der Subject String enthält jedenfalls eine Auswahl der Felder jurisdictionOfIncorporationLocalityName, jurisdictionOfIncorporationStateOrProvinceName, jurisdictionOfIncorporationCountryName.
  Die Auswahl wird durch den rechtlichen Gültigkeitsbereich der Organisationsregistrierung bestimmt.

- Der Subject String enthält das Feld serialNumber welches die geprüfte Registrierungsnummer der Organisation enthält. Sofern eine solche nicht vorliegt, kann auch das Datum der Registrierung eingetragen werden.
- Die geprüfte Adresse der Organisation wird im Subject String jedenfalls in den Feldern countryName, stateOrProvincename (sofern für das Land zutreffend) und localityName abgebildet. Optional können auch die Felder postalCode und streetAddress eingetragen werden.

7.1.1 Versionsnummern / Version number(s)

Es wird jedenfalls die Versionsnummer 2 laut [RFC5280] (X509v3) unterstützt.

7.1.2 Zertifikatserweiterungen / Certificate extensions

Zertifikate im X.509 Format können beliebige technisch und rechtlich zulässige Erweiterungen enthalten die nicht dem Zertifikatszweck widersprechen und nicht irreführend sind. Die Aufnahme der Erweiterungen kann sowohl vom Antragsteller als auch vom ZDA initiiert werden. Dabei wird darauf geachtet, dass die Kennung und der Inhalt der Erweiterung ausreichend dokumentiert ist und die Bedingungen und Einschränkungen zur Verwendung erfüllt werden..

Soweit Serverzertifikate im Format X.509v3 ausgestellt werden enthalten sie in jedem Fall die Erweiterung subjectAltName [RFC5280]. Diese enthält ausschließlich Einträge des Typs dNSName oder iPAddress. Sofern der Subject das Feld commonName enthält, ist dessen Inhalt jedenfalls ein Eintrag (Domainname oder IP-Adresse) aus dem subjectAltName. Für Zertifikate mit privaten Domainnamen oder IP-Adressen gelten die Einschränkungen jener Dokumente, zu denen diese Policy konform ist.

Zur Verbreitung der Widerrufsstatusinformationen enthalten alle EV-Zertifikate folgende Erweiterungen:
1. Eine crlDistributionPoint Erweiterung, die als nicht kritisch markiert ist und eine HTTP URL zur entsprechenden Widerrufsliste enthält
2. Eine authorityInformationAccess Erweiterung, die als nicht kritisch markiert ist und eine HTTP URL zum entsprechenden OCSP Responder enthält.

Punkt 2 ist nicht erforderlich , wenn "OCSP Stapling" (laut [RFC4366]) eingesetzt wird und dies vom Betreiber entweder technisch geprüft oder vertraglich festgelegt wird.

Alle anderen CA-, Sub- und Endkunden-Zertifikate enthalten ebenfalls diese Erweiterungen, sofern nicht technische oder rechtliche Gründe dem entgegenstehen.

Der ZDA kann Sub-Zertifikate speziell für einen Signator erstellen. Dabei kann der private Schlüssel unter der alleinigen Kontrolle des ZDA verbleiben oder vom Nutzer verwaltet werden.

Ein Sub-Zertifikat wird nach Möglichkeit technisch eingeschränkt. Das bedeutet jedenfalls:
- Ein Sub-Zertifikat im Format X.509v3 enthält eine ExtendedKeyUsage Erweiterung, die die möglichen EKU Einstellungen von Endzertifkaten enthält. Diese Erweiterung enthält niemals den Wert anyExtendedKeyUsage.

- Wenn einem Sub-Zertifikat im Format X.509v3 die EKU id-kp-serverAuth erlaubt ist, so muss die Möglichkeit dNSName Einträge zu erstellen durch den Einsatz einer NameXConstraints Erweiterung auf bestätigte Domains (⇨ 7. Profile der Zertifikate, Widerrufslisten und OCSP / CERTIFICATE, CRL, AND OCSP PROFILES, p89) beschränkt werden oder Einträge vom Typ dNSName allgemein unterbunden werden.
- Wenn einem Sub-Zertifikat im Format X.509v3 die EKU id-kp-serverAuth erlaubt ist, so muss die Möglichkeit iPAddress Einträge zu erstellen durch den Einsatz einer NameConstraints Erweiterung auf bestätigte Addressbereiche (⇨ 7. Profile der Zertifikate, Widerrufslisten und OCSP / CERTIFICATE, CRL, AND OCSP PROFILES, p89) beschränkt werden, oder Einträge vom Typ iPAddress allgemein unterbunden werden (sowohl IPv4 als auch IPv6 Adressen).
- Wenn einem Sub-Zertifikat im Format X.509v3 die EKU id-kp-emailProtection erlaubt ist, so muss die Möglichkeit E-Mail Adressen Einträge zu erstellen auf bestätigte Addressbereiche (⇨ 7. Profile der Zertifikate, Widerrufslisten und OCSP / CERTIFICATE, CRL, AND OCSP PROFILES, p89) beschränkt werden.
- Wenn einem Sub-Zertifikat im Format X.509v3 die EKU id-kp-codeSigning erlaubt ist, so muss der mögliche directoryName mittels NameConstraints Erweiterung auf geprüfte organizationName und countryName sowie optional localityName und stateOrProvinceName Einträge beschränkt werden.

Sofern das Sub-Zertifikat nicht anhand der obigen Kriterien eingeschränkt ist, werden jedenfalls folgende organisatorische Bedingungen gemeinsam erfüllt:

- Das Zertifikat im Format X.509v3 wird im DER Format veröffentlicht bevor der Nutzer damit Zertifikate ausstellen kann.
- Die Certificate Policy und das Certificate Practice Statement des Sub-Zertifikates werden - sofern vorhanden - veröffentlicht. Es muss jedoch zumindest eines der Dokumente existieren.
- Die Certificate Policy/das Certificate Practice Statement des Sub-Zertifikates erfüllen jedenfalls die Kriterien von [MOZILLA-CAPOL].
- Es erfolgt zumindest einmal jährlich eine Auditierung der Certificate Policy des Sub-Zertifikates durch eine kompetente unabhängige Auditstelle. Die Auditierung muss zumindest den Kriterien [CABROWSER-BASE] entsprechen. Der Report dieser Auditierung wird veröffentlicht .

Alle oben angegebenen Veröffentlichungen erfolgen auf der Webseite des ZDA und sind ohne Einschränkungen verfügbar.

7.1.3 Algorithmen OIDs / Algorithm object identifiers

Zertifikate enthalten einen Hinweis auf den Algorithmus des öffentlichen Schlüssels und des Verfahrens mit dem es vom CA-Zertifikat unterschrieben wurde. Zulässig sind alle in [RFC5280] spezifizierten bzw. Referenzierten Verfahren sowie andere kompatible Algorithmen, die den technischen Ansprüchen des jeweiligen Zertifizierungsdienstes genügen.

7.1.4 Namensformate / Name forms

Zertifikate enthalten jedenfalls eine Identifikation des Signators (Subject) und der jeweiligen CA (Issuer).

Wurde bei einem Serverzertifikat die Identität des Antragstellers geprüft, so enthält das Zertifikat den Organisationsnamen laut offiziellen Registrierungsunterlagen. Soweit Serverzertifikate im Format X.509v3 ausgestellt werden beinhaltet das Subject einen organizationName Eintrag und zusätzlich einen countryName sowie einen localityName und/oder einen stateOrProvinceName Eintrag. In diesem Fall kann auch ein organizationalUnit Entrag vorhanden sein, sofern dieser keine irreführenden oder ungeprüften Informationen enthält. Das Land in countryName bezieht sich dabei entweder auf die IP-Adresse des Antragstellers, die IP-Adresse seiner Webseite, den Ländercode der eingetragenen Domain oder auf eine im Zuge der Identitätprüfung erhaltene Bestätigung.

Wurde bei einem Serverzertifikat lediglich eine technische Prüfung der einzutragenden Adressen und keine Identifikationsprüfung vorgenommen, so enthält der Subject des Zertifikates keines der folgenden Felder: organizationName, localityName, stateOrProvinceName, postalCode. Sofern das Subject einen domainComponent Eintrag besitzt, enthält dieses alle geordneten Teile eines im Zertifikat eingetragenen Domainnamen in umgekehrter Reihenfolge.

7.1.5 Namensbeschränkungen / Name constraints

Für alle Zertifikate gilt, dass derselbe Name (z.B. distinguishedName) innerhalb der jeweiligen CA niemals für zwei unterschiedliche Antragsteller verwendet wird.

7.1.6 Certificate Policy Object Identifier / Certificate policy object identifier

Zertifikate enthalten jedenfalls einen Verweis auf die anzuwendende GLOBALTRUST® Certificate Security Policy, nach der sie ausgestellt wurden. Darüberhinaus können an dieser Stelle ein Verweis auf Spezifikationen von Dritten enthalten sein, die bei der Erstellung des Signatorzertifikates beachtet wurden, insbesondere die in [CABROWSER-BASE] und [CABROWSER-EV] angegebenen.

Zertifikate die ab 1.7.2014 ausgestellt werden und deren Schlüssel nicht in einer Signaturerstellungseinheit erzeugt wurden, die nicht zumindest FIPS-140 2 L2 oder CC Protection Profile CWA 14169 entspricht erhalten den zusätzlichen Policy-OID-Eintrag 1.2.40.0.36.4.1.10.

7.1.7 Nutzung der Erweiterung „PolicyConstraints" / Usage of Policy Constraints extension

Diese Erweiterung kann bei Bedarf gemäß den Spezifikation von [RFC5280] eingesetzt werden.

7.1.8 Syntax und Semantik von „PolicyQualifiers" / Policy qualifiers syntax and semantics

Diese Erweiterung kann bei Bedarf gemäß den Spezifikation von [RFC5280] eingesetzt werden.

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung CertificatePolicies / Processing semantics for the critical Certificate Policies extension

Kritische und nicht-kritische Erweiterung werden gemäß den Spezifikation von [RFC5280] eingesetzt.

7.2 Sperrlistenprofile / CRL profile

Bei der Verwendung von standardisierten Zertifikatsformaten (z.B. X509v3) genügt der Verweis auf die anzuwendenden Standards. Der Inhalt der Widerrufsliste entspricht bei Zertifikaten die zur qualifizierten Signatur, zur Amtssignatur oder zur fortgeschrittenen Signatur geeignet sind [RFC5280].

Welche Widerrufs- und Sperrdienste verwendet werden, sind im ausgegebenen Zertifikat festgelegt. Dabei können individuelle technische Anforderungen der Signatoren berücksichtigt werden, soweit sie nicht im Widerspruch zu den verwendeten Standards, rechtlichen Vorgaben und dem anzuwendenden GLOBALTRUST® Certificate Practice Statement stehen.

Der Umfang der Widerrufs- bzw. Sperrliste ist - sofern anzeigepflichtig - der Anzeige des jeweiligen Zertifizierungsdienstes bei der Aufsichtsbehörde bzw. den Dokumentationen auf der Website des ZDA zu entnehmen.

7.2.1 Versionsnummern / Version number(s)

Jede CRL ist mit einer Versionsnummer versehen.

7.2.2 Erweiterungen von Widerrufslisten und Widerrufslisteneinträgen / CRL and CRL entry extensions

Widerrufslisten können in [RFC5280] spezifizierte oder mit [RFC5280] kompatible Erweiterungen enthalten

7.3 Profile des Statusabfragedienstes (OCSP) / OCSP profile

Der OCSP Dienst des Betreibers erfolgt gemäß [RFC6960].

OCSP Antworten für CAs die Serverzertifikate im Format X.509v3 ausstellen werden entweder vom CA Zertifikat selbst oder von einem dedizierten OCSP Responder-Zertifikat signiert, dass die Erweiterung id-pkix-ocsp-nocheck (laut [RFC2560]) enthält .

Ein OCSP-Responder liefert niemals den Status "good" für ein unbekanntes Zertifikat zurück.

7.3.1 Versionsnummern / Version number(s)

Die OCSP Antworten enthalten eine Versionsnummer gemäß [RFC6960].

7.3.2 OCSP-Erweiterungen / OCSP extensions

Die OCSP Antworten können Erweiterung gemäß [RFC6960] enthalten.

8. PRÜFUNG DER KONFORMITÄT UND ANDERE BEURTEILUNGEN / COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Der Betreiber erklärt, dass dieses Dokument gemeinsam mit dem GLOBALTRUST® Certificate Practice Statement (OID-Nummer: 1.2.40.0.36.1.2.3.1) und der GLOBALTRUST® Certificate Security Policy (OID-Nummer: 1.2.40.0.36.1.2.2.1) die Anforderungen gemäß folgender Bestimmungen erfüllen:

- Richtlinie 1999/93/EG für elektronische Signaturen [SigRL]
- Signaturgesetz [SigG] in Verbindung mit der Signaturverordnung [SigV]
- ETSI Policy requirements for certification authorities issuing qualified certificates [ETSI TS 101 456]
- Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements [CWA-14167-1]
- Microsoft Root Certificate Program [MS-CA]
- CA/Browser Forum: Baseline Requirements [CABROWSER-BASE] veröffentlicht insbesondere unter http://www.cabforum.org
- Mozilla CA Certificate Inclusion Policy [MOZILLA-CAPOL]
- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC3647]
- Trust Service Principles and Criteria for Certification Authorities [WEBTRUST-CA]
- Webtrust for Certification Authorities - Extended Validation Audit Criteria [WEBTRUST-EV]
- Konformität mit [ADOBE-TRUST]
- Konformität mit [CABROWSER-EV]
- Konformität mit [MOZILLA-CAMAINT]
- Konformität mit [APPLE-CA]
- Konformität mit [ENISA-ALG]

Die Einhaltung der Anforderungen wird durch regelmäßige Audits sicher gestellt, die den Konformitätsanforderungen der angebenen Dokumente entsprechen.

Im Fall von Inkonsistenzen zwischen den Dokumenten des Zertifizierungsdienstes und den Dokumenten, zu denen die Zertifizierungsdienste konform sind, gelten folgende Regeln:

a) gesetzliche Anforderungen sind unmittelbar vor den Anforderungen der Dokumente des Zertifizierungsdienstes wirksam,
b) Inkonsistenzen ohne direkten Einfluß auf die Policy des Zertifizierungsdienste werden auf der Website des ZDA interpretativ klargestellt,
c) Inkonsistenzen mit direkten Einfluß auf die Policy des Zertifizierungsdienste - sofern davon qualifizierte Zertifikate betroffen sind, führen zu Anpassungen der betroffenen Dokumente des Zertifizierungsdienstes, um die Konsistenzen herzustellen,
d) in allen anderen Fällen haben die Anforderungen der Konformitätsdokumente Vorrang.

8.1 Häufigkeit und Umstände für Beurteilungen / Frequency or circumstances of assessment

Audits erfolgen grundsätzlich einmal jährlich, jedenfalls so häufig, wie gesetzlich oder auf Grund der in ⇨ 8. Prüfung der Konformität und andere Beurteilungen / COMPLIANCE AUDIT AND OTHER ASSESSMENTS genannten Dokumenten zu denen diese GLOBALTRUST® Certificate Policy konform ist, vorgesehen ist.

8.2 Identifikation/Qualifikation des Gutachters / Identity/qualifications of assessor

Externe Gutachter werden nur herangezogen, wenn Sie eine ausreichende Qualifikation im Sinne der Definition von ⇨ kompetente unabhängige Auditstelle (p18) aufweisen. Bei internen Gutachtern, insbesondere im Rahmen von Self-Assessments, stellt der Betreiber die ausreichende Qualifikation sicher und haftet für die Tätigkeit.

In jedem Fall wird dokumentiert, welche Personen tatsächlich als Gutachter tätig wurden.

8.3 Beziehung des Gutachters zur zu überprüfenden Einrichtung / Assessor's relationship to assessed entity

Im Falle interner Gutachter wird ein Mitarbeiter des Betreibers gemäß Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) nominiert. Er ist für die Audittätigkeit unabhängig und an keine Weisungen gebunden.

8.4 Behandelte Themen der Begutachtung / Topics covered by assessment

Die im Rahmen einer Begutachtung behandelten Themen, insbesondere nach welchen Standards bzw. Vorgaben im Sinne ⇨ 8. Prüfung der Konformität und andere Beurteilungen / COMPLIANCE AUDIT AND OTHER ASSESSMENTS (p95) gelisteten Dokumenten eine Prüfung erfolgte, wird im Gutachten dokumentiert.

8.5 Handlungsablauf bei negativem Ergebnis / Actions taken as a result of deficiency

Kann auf Grund eines Gutachten eine bestimmte Eigenschaft oder Qualität der Zertifizierungsdienste im Sinne dieser GLOBALTRUST® Certificate Policy nicht bestätigt werden, dann erfolgt eine unverzügliche Anpassung der technischen und organisatorischen Abläufe um die erforderliche Eigenschaft oder Qualität zu erreichen.

Kann eine bestimmte Eigenschaft oder Qualität der Zertifizierungsdienste auch nach Änderung der technischen und organisatorischen Abläufe nicht erreicht werden, wird geprüft ob eine gleichwertige Eigenschaft oder Qualität der Zertifizierungsdienste möglich ist. Sofern erforderlich erfolgt in diesem Fall eine Anpassung der betroffenen Dokumente, insbesondere der GLOBALTRUST® Certificate Policy bzw. des GLOBALTRUST® Certificate Practice Statement.

Stehen keine Alternativen zur Verfügung wird die betroffene Eigenschaft oder Qualität der Zertifizierungsdienste aus den entsprechenden Dokumenten entfernt.

8.6 Mitteilung des Ergebnisses / Communication of results

Sofern auf Grund des negativen Ergebnisses erforderlich, erfolgt in geeigneter Form eine Verständigung aller ⇨ Beteiligten über die sie betreffenden Ergebnisse und getroffenen Maßnahmen.

9. REGELUNGEN FÜR SONSTIGE FINANZIELLE UND GESCHÄFTLICHE ANGELEGENHEITEN / OTHER BUSINESS AND LEGAL MATTERS

9.1 Kosten / Fees

Die Ausstellung von Zertifikaten und Erbringung von Zertifikatsdiensten erfolgt grundsätzlich kostenpflichtig.

Der Betreiber behält sich jedoch vor einzelne Dienste, insbesondere zu Testzwecken, kostenfrei anzubieten.

Zeitstempeldienste werden sowohl kostenpflichtig, als auch kostenfrei angeboten. Abfragen von Zeitstempel können sowohl authentisiert, als auch anonym erfolgen. In allen Fällen erfüllt der Zeitstempel dieselben technischen Sicherheitsanforderungen. Im Falle authentisierter Abfragen erfolgt die Aufzeichnung der abfragenden Stelle.

9.1.1 Kosten für Zertifikatsaustellung und -erneuerung / Certificate issuance or renewal fees

Die jeweils gültigen Kosten und Konditionen werden auf der Website des ZDA publiziert oder auf Anfrage beauskunftet.

9.1.2 Kosten für den Zugriff auf Zertifikate / Certificate access fees

Der Zugriff auf öffentliche Zertifikate ist im Rahmen der Website des Betreibers kostenfrei und unterliegt keinen unsachlichen Beschränkungen.

Für individuelle Auskünfte und Bestätigungen, insbesondere über Zertifikate die nicht mehr in Verwendung sind und nicht mehr Online abrufbar sind, kann ein Kostenersatz eingehoben werden. Dieser Kostenersatz hat maximal die Höhe der tatsächlich anfallenden Kosten.

9.1.3 Kosten für Widerruf oder Statusinformationen / Revocation or status information access fees

Die jeweils gültigen Kosten und Konditionen werden auf der Website des ZDA publiziert oder auf Anfrage beauskunftet.

9.1.4 Kosten für andere Dienstleistungen / Fees for other services

Die jeweils gültigen Kosten und Konditionen werden auf der Website des ZDA publiziert oder auf Anfrage beauskunftet.

9.1.5 Kostenrückerstattung / Refund policy

Der ZDA refundiert Kosten, die auf Grund von Fehlern seiner Tätigkeit verursacht wurden, die er zu verantworten hat.

Weiters bietet der ZDA kostenlosen Ersatz bei Produkten an, die nicht mehr den aktuellen technischen Standards entsprechen, unabhängig davon, was die Ursache ist. Ein weitergehender Ersatz von Kosten und Aufwändungen, insbesondere Folgekosten, die sich aus Installation oder Betrieb von Zertifikaten ergeben ist in diesem Fall ausdrücklich ausgeschlossen.

9.2 Finanzielle Verantwortung / Financial responsibility

Der ZDA ist sich seiner Verantwortung über ausreichende finanzielle Mittel zu verfügen bewusst und stellt durch entsprechende betriebliche Tätigkeit und finanzielle Ausstattung sicher, dass die Finanzierung der Zertifizierungsdienste langfristig gesichert ist.

9.2.1 Versicherungsdeckung / Insurance coverage

Der ZDA hat eine Haftpflichtversicherung bei einem Versicherungsunternehmen mit ausreichender Bonität, die den gesetzlichen Anforderungen entspricht abgeschlossen. Die abgeschlossene Versicherung ist intern dokumentiert.

9.2.2 Andere Ressourcen für Betriebserhaltung und Schadensdeckung / Other assets

Der ZDA betreibt zur Minimierung und zum frühzeitigen Erkennen neuer (technischer) Bedrohungen einen intensiven Erfahrungsaustausch mit vergleichbaren Einrichtungen.

9.2.3 Versicherung oder Gewährleistung für Endnutzer / Insurance or warranty coverage for end-entities

Der ZDA 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.

9.3 Vertraulichkeit von Geschäftsdaten / Confidentiality of business information

9.3.1 Definition vertrauliche Geschäftsdaten / Scope of confidential information

Zur Steuerung des Betriebs wurden für alle Informationen vier Sicherheitsstufen eingeführt, die zu entsprechend unterschiedlichen betrieblichen Sicherheitsmaßnahmen führen.

- **Stufe "public"**: Umfasst alle Daten, die zur Veröffentlichung bestimmt oder geeignet sind. Der Zugriff auf diese Daten ist nicht beschränkt, es werden jedoch Maßnahmen zum Erhalt der Verfügbarkeit und der Datenintegrität ergriffen.

Alle weiteren Stufen enthalten Daten, die nicht zur Veröffentlichung geeignet sind. Der Zugriff ist jeweils auf die für die Verwendung der Daten vorgesehenen Personen beschränkt. Abstufungen ergeben sich weiters im Umfang der technischen Maßnahmen zum Erhalt der Verfügbarkeit und der Datenintegrität.

- **Stufe "intern" (administration, "eingeschränkte Zugänglichkeit")**: Umfasst alle Daten, die zur ordnungsgemäßen Betriebsführung im kaufmännischen Sinn dienen, inkl. interne Dokumentationen, Buchhaltung, Kunden- und Interessentenadministration, Angebots- und Rechnungslegung. Der Zugriff auf diese Daten wird durch Dienstanweisung bzw. Tätigkeitsbeschreibung geregelt und ist auf Mitarbeiter und Bevollmächtigte des Betreibers beschränkt.

- **Stufe "vertraulich" (systemadministration, "Vertrauliche Informationen")**: Umfasst alle Daten, die zur Aufrechterhaltung und Weiterführung des Zertifizierungsbetriebs dienen. Der Zugriff ist durch Dienstanweisung bzw. Tätigkeitsbeschreibung und durch technische Zugangsbeschränkungen (z.B. Passwörter) beschränkt.

- **Stufe "geheim" (secure, "Geheime Informationen")**: Umfasst alle Daten, die besonderen Zertifizierungsprozessen unterworfen sind, insbesondere sind dies die Daten die im unmittelbaren Zusammenhang mit Schlüsselerstellung und Zertifikatsgenerierung stehen. Der Zugriff ist durch Dienstanweisung bzw. Tätigkeitsbeschreibung, durch erhöhte technische Zugangsbeschränkungen (z.B. Passwörter+Token) und durch spezifische sichere Hardwarekomponenten beschränkt.

9.3.2 Geschäftsdaten, die nicht vertraulich behandelt werden / Information not within the scope of confidential information

Nicht vertrauliche Geschäftsdaten werden im Sinne der ⇨ **Stufe "public"** behandelt.

9.3.3 Zuständigkeiten für den Schutz vertraulicher Geschäftsdaten / Responsibility to protect confidential information

Der Schutz vertraulicher Geschäftsdaten wird als Teil des umfassenden Informationssicherheitskonzepts angesehen (⇨ Management-Statement p12) und ist in den Sicherheitszielen und -leitlinien gemäß GLOBALTRUST® Certificate Practice Statement konzeptionell und gemäß GLOBALTRUST® Certificate Security Policy technisch geregelt. Die Zuständigkeiten ergeben sich aus dem Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy).

9.4 Datenschutz von Personendaten / Privacy of personal information

Alle im Rahmen der Zertifizierungsdienste erhaltenen personenbezpogenen Informationen werden vertraulich behandelt und nur für Zwecke des Zertifizierungsdienstes und für Verständigungszwecke im Zusammenhang mit den Zertifizierungsdienstleistungen des ZDAs verwendet.

Gesetzliche Aufbewahrungs- und Übermittlungsverpflichtungen bleiben unberührt. Eine Datenweitergabe an kommerzielle Datenhändler (Adressenverlage, Listbroker, ...) wird ausdrücklich ausgeschlossen.

9.4.1 Datenschutzkonzept / Privacy plan

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.

9.4.2 Definition von Personendaten / Information treated as private

Der ZDA versteht unter Personaldaten personenbezogen Daten im Sinne der jeweils geltenden europäischen Datenschutzbestimmung. Soweit österreichische Bestimmungen eine erweiterten Umfang vorsehen, fallen auch diese Datenkategorien unter den Definitionsumfang von Personendaten.

9.4.3 Daten, die nicht vertraulich behandelt werden / Information not deemed private

Veröffentlicht werden Daten des Signators ausschließlich auf Grund der Erfordernisse des jeweiligen Zertifizierungsdienstes (Verzeichnisdienst, Widerrufsdienst), aus gesetzlichen oder sonstigen zulässigen rechtlichen Gründen oder auf ausdrücklichen Wunsch des Signators.

9.4.4 Zuständigkeiten für den Datenschutz / Responsibility to protect private information

Die Einhaltung der Datenschutzbestimmungen erfolgt auf Grundlage des Rollenkonzepts (⇨ GLOBALTRUST® Certificate Security Policy).

9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten / Notice and consent to use private information

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

9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften / Disclosure pursuant to judicial or administrative process

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.

9.4.7 Andere Bedingungen für Auskünfte / Other information disclosure circumstances

Der ZDA gibt keine personenbezogene Daten weiter, wenn er dazu nicht ausdrücklich verpflichtet ist oder vom ⇨ Betroffenen ausdrücklich ermächtigt ist.

9.5 Schutz-und Urheberrechte / Intellectual property rights

Der Betreiber beachtet alle erforderlichen urheberrechtlichen Bestimmungen und stellt insbesondere sicher, dass er nur Produkte oder Dienste verwendet bzw. anbietet, zu denen er die erforderlichen Urheberrechte bzw. Lizenzen besitzt.

9.6 Zusicherungen und Garantien / Representations and warranties

9.6.1 Leistungsumfang des ZDA / CA representations and warranties

Der Leistungsumfang des ZDA ist in dieser GLOBALTRUST® Certificate Policy, dem anzuwendenden GLOBALTRUST® Certificate Practice Statement und der Website des Betreibers vollständig beschrieben.

9.6.2 Leistungsumfang der Registrierungsstellen / RA representations and warranties

Der aktuelle Leistungsumfang der Registrierungsstellen ist auf der Website des Betreibers beschrieben und geht in keinem Fall über die GLOBALTRUST® Certificate Policy hinaus.

9.6.3 Zusicherungen und Garantien des Signators / Subscriber representations and warranties

Es gelten die Allgemeinen Geschäftsbedingungen des Betreibers, diese Policy sowie das GLOBALTRUST Certificate Practice Statement.

9.6.4 Zusicherungen und Garantien für Nutzer / Relying party representations and warranties

Es bestehen mangels eines Vertragsverhältnisses keine Zusicherungen und Garantien für Nutzer.

9.6.5 Zusicherungen und Garantien anderer Teilnehmer / Representations and warranties of other participants

Es bestehen mangels eines Vertragsverhältnisses keine Zusicherungen und Garantien für andere Teilnehmer.

9.7 Haftungsausschlüsse / Disclaimers of warranties

Der ZDA haftet nicht, falls er nachweisen kann, dass ihn an der Verletzung der oben angeführten Verpflichtungen keine Schuld trifft und er nicht fahrlässig gehandelt hat. Dies trifft insbesondere zu, wenn

- Antragsteller oder Signatoren ausgegebene Zertifikate entgegen der gültigen Policy verwenden oder
- Nutzer von Signaturen, Zertifikaten und öffentliche Schlüssel es unterlassen Gültigkeitszeitraum, bestehende Sperren, Widerrufe oder sonstige Beschränkungen einer durch ein Zertifikat des ZDAs bestätigten Unterschrift zu beachten oder
- der Antragsteller gefälschte oder sonstwie manipulierte Unterlagen vorliegt und deren Manipulation bzw. Fälschung nicht offensichtlich erkennbar ist.

9.8 Haftungsbeschränkungen / Limitations of liability

Der ZDA 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 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 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 ZDA-internen Prozessdokumentation geregelt.
- 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, 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.

Diese Haftung gilt in gleicherweise für alle Serverzertifikate, die mittels Sub-Zertifikate ausgestellt wurden.

Softwarehersteller die die Root-Zertifikate des ZDA vertreiben, haften nicht für den Inhalte der Zertifikate. Sie werden vom ZDA, soweit dies rechtlich zulässig ist und keine Vorgänge betrifft, die der Softwarehersteller zu verantworten hat, klag und schadlos gehalten. Jedenfalls zu verantworten hat der Softwarehersteller die korrekte Anzeige des Gültigkeitsstatus eines Zertifikates des ZDA .

9.9 Schadensersatz / Indemnities

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

9.10 Gültigkeitsdauer der CP und Beendigung der Gültigkeit / Term and termination

9.10.1 Gültigkeitsdauer der CP / Term

Die GLOBALTRUST® Certificate Policy ist bis auf Widerruf gülltig.

9.10.2 Beendigung der Gültigkeit / Termination

Die Gültigkeit der GLOBALTRUST® Certificate Policy endet durch
- Widerruf oder
- Anzeige der Einstellung der Tätigkeit des ZDA bei der Aufsichtsbehörde oder
- Ausgabe einer neuen GLOBALTRUST® Certificate Policy

In allen Fällen erfolgt eine Verständigung der ⇨ Beteiligten in geeigneter Form, jedenfalls eine Veröffentlichung auf der Website des Betreibers.

9.10.3 Auswirkung der Beendigung / Effect of termination and survival

Die Auswirkungen der Beendigung ergeben sich aus der Art der Beendigung und werden jedenfalls in der Verständigung der ⇨ Beteiligten und derVeröffentlichung auf der Website des Betreibers dargestellt.

9.11 Individuelle Mitteilungen und Absprachen mit Beteiligten / Individual notices and communications with participants

Es erfolgen keine individuellen Mitteilungen und Absprachen mit ⇨ Beteiligten, die der GLOBALTRUST® Certificate Policy, dem GLOBALTRUST® Certificate Practice Statement oder sonstigen für die Erbringung der Zertifizireungsdienste wesentlichen Bestimmungen widersprechen.

9.12 Änderungen / Amendments

9.12.1 Verfahren bei Änderungen / Procedure for amendment

Änderungen werden im Rahmen des Rollenkonzepts (⇨ GLOBALTRUST® Certificate Security Policy) beauftragt, geplant und durchgeführt.

9.12.2 Benachrichtigungsmechanismen und –fristen / Notification mechanism and period

Die Benachrichtigung über Änderungen erfolgt - soweit zulässig und technisch möglich - auf elektronischen Wege. Betreffen Änderungen eine größer Zahl an ⇨ Beteiligten werden Änderungen auf der Website des Betreibers veröffentlicht.

Ist eine Benachrichtigung auf elektronischen Wege nicht möglich oder nicht zulässig und die Information auf der Wesite des Betreibers nicht ausreichend, werden andere geeignete Wege der Verständigung benutzt, insbesondere die Zustellung der Informationen durch Postdienste oder Boten.

Änderungen werden den ⇨ Beteiligten so frühzeitig wie möglich mitgeteilt. Ebenso welche Reaktionsmöglichkeiten die ⇨ Beteiligten haben.

9.12.3 Bedingungen für OID-Änderungen / Circumstances under which OID must be changed

Änderungen von OID-Kennzeichen insbesondere Änderungen der Bedeutung sind nur im Falle zwingender gesetzlicher Vorgaben oder durch Vorgaben der zuständigen Standardisierungsgremien vorgesehen.

9.13 Bestimmungen zur Schlichtung von Streitfällen / Dispute resolution provisions

Der ZDA behält sich vor außergerichtliche Schlichtungsstellen vorzuschlagen. Diese Schlichtungsstellen werden auf der Website des Betreibers veröffentlicht.

9.14 Gerichtsstand / Governing law

Der Betreiber ist ein im österreichischen Firmenbuch protokolliertes Unternehmen.

Gerichtsstand ist Wien. Es gilt österreichisches Recht.

Der ZDA untersteht den zuständigen Aufsichtsbehörden gemäß folgender Bestimmungen:
- Richtlinie 1999/93/EG für elektronische Signaturen [SigRL] in der geltenden Fassung oder einer nachfolgenden (ersetzenden oder ergänzenden) Regelung der Europäischen Union
- Signaturgesetz [SigG] in Verbindung mit der Signaturverordnung [SigV] in der jeweils gültigen Fassung
- den technischen Standards und rechtlichen Vorgaben gemäß ⇨ 8.Prüfung der Konformität und andere Beurteilungen / COMPLIANCE AUDIT AND OTHER ASSESSMENTS (p95)

Die Kontaktdaten der zuständigen Aufsichtsbehörden und die erforderlichen Registerinformationen des ZDA werden auf der Website des ZDA veröffentlicht.

9.15 Einhaltung geltenden Rechts / Compliance with applicable law

Alle in diesem Dokument beschriebenen Zertifizierungsdienste werden gemäß österreichischem Signaturgesetz inkl. Signaturverordnung [SigG] + [SigV] oder der Signatur-Richtlinie [SigRL] oder nach einem nationalen Gesetz eines anderen Mitgliedstaaten der Europäischen Union oder von anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum erlassen wurde, dass zur Beurteilung der Sicherheitsanforderungen für sichere Signaturerstellungseinheiten nach der Signaturrichtlinie [SigRL] geeignet ist oder sonstiger gesetzlicher Bestimmungen, die der Signatur-Richtlinie gleichwertig sind, erbracht.

Die technische Umsetzung erfolgt gemäß ETSI-Standard [ETSI TS 101 456], die Erweiterungen für die Ausgabe qualifizierter Zertifikate gemäß [ETSI TS 101 862] oder vergleichbarer gleichwertiger Standards. Weiters werden die Anforderungen

[CWA-14167-1] für den Betrieb des Zertifizierungsdienstes und [EG-REF] zur Ausstellung sicherer Signaturerstellungseinheiten erfüllt.

Das Sicherheitskonzept erfüllt jedenfalls die Anforderungen der Signaturrichtlinie [SigRL], [SigG], [ETSI TS 101 456] und [CWA-14167-1] und ist im Dokument GLOBALTRUST® Certificate Security Policy dargestellt. Sie gilt für alle vom Betreiber betriebenen Zertifizierungsdienste, einschließlich Zeitstempeldienste, mobiler Signaturen und serverbasierte Signaturdienste.

Alle in dieser GLOBALTRUST® Certificate Policy beschriebenen Zertifizierungsdienste werden gemäß den Anforderungen der europäischen Signaturrichtlinie [SigRL], dem österreichischen Signaturgesetz [SigG], der österreichischen Signaturverordnung [SigV], den Policy-Anforderungen [ETSI TS 101 456] (QCP Public + SSCD) im Zusammenhang mit der Erbringung qualifizierter Zertifizierungsdienste und [ETSI TS 102 042] im Zusammenhang sonstiger Zertifizierungsdienste und den Sicherheitsanforderungen [CWA-14167-1] erbracht. Weiters [ETSI TS 101 862] für die Erstellung qualifizierter Zertifikate. Sofern einzelne Bestimmungen in Konflikt stehen, wird die jeweils aktuellere Bestimmung, die den technischen und rechtlichen Anforderungen sicherer Zertifzierungsdienste am nächsten kommt, herangezogen.

Diese Policy wurde in Übereinstimmung mit den Signaturbestimmungen verfasst und bildet gemeinsam mit allfälligen individuellen Vereinbarungen und der - soweit gemäß [SigRL], [SigG] oder anderer Bestimmungen erforderlichen - Anzeige bei der Aufsichtsbehörde die Grundlage für die Verwendung von GLOBALTRUST® Zertifikaten durch den Signator.

Der Betrieb des Zertifizierungsdienstes erfolgt für alle in dieser Policy geregelten Zertifikate und Dienste gemäß [CWA-14167-1]. Die betriebstechnischen Details sind in einem eigenen GLOBALTRUST® Certificate Practice Statement dokumentiert. Soweit spezifische sicherheitsrelevante Vorkehrungen zu treffen sind, sind diese in der GLOBALTRUST® Certificate Security Policy dokumentiert.

9.16 Sonstige Bestimmungen / Miscellaneous provisions

9.16.1 Vollständigkeitserklärung / Entire agreement

Der ZDA verpflichtet sich sicherzustellen, dass alle Anforderungen, die sich aus den Zertifizierungsdiensten ergeben dokumentiert sind und die in ⇨ 4.5.1 Nutzung des privaten Schlüssels und des Zertifikates durch den Signator / Subscriber private key and certificate usage (p39) dargelegt sind, dem Signator zur Kenntnis gebracht wird und die Erfüllung vertraglich vereinbart wird.

Der ZDA ist verantwortlich für die Einhaltung aller Geschäftsprozesse zu den Zertifizierungsdiensten.

9.16.2 Abgrenzungen / Assignment

Die GLOBALTRUST® Certificate Security Policy, das GLOBALTRUST® Certificate Practice Statement und die GLOBALTRUST® Certificate Security Policy gemeinsam sind Grundlage des der

Aufsichtsbehörde zur Genehmigung vorgelegten Betriebskonzepts, sonstige - nicht in diesen Dokumenten beschriebenen - Bestimmungen kommen nicht zur Anwendung.

9.16.3 Salvatorische Klausel / Severability

Sollten Bestandteile dieser Vereinbarung unwirksam sein und sich gesetzliche Bestimmungen ändern, die die sachlichen Bestandteile dieser Vereinbarung berühren, bleiben die anderen Teile der Vereinbarung in Kraft.

9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht) / Enforcement (attorneys' fees and waiver of rights)

Der Zertifizierungsbetrieb auf Basis dieser GLOBALTRUST® Certificate Policy wird erst nach Genehmigung durch die zuständigen Aufsichtsstellen vorgenommen.

9.16.5 Höhere Gewalt / Force Majeure

Keine Haftung des ZDA und des Betreibers im Falle höherer Gewalt.

9.17 Andere Bestimmungen / Other provisions

Es liegt keine Änderung dieser GLOBALTRUST® Certificate Security Policy vor, wenn
- ausschließlich redaktionelle Korrekturen (Korrektur von Schreibfehlern, Nummerierungsfehlern, Verweis- und Linkfehlern, Grammatik) vorgenommen werden oder
- einzelne Textteile in andere Abschnitte oder Kapitel verlegt werden, erläuternde Zwischenüberschriften oder Kommentare eingefügt werden.

Auf derartige Änderungen wird auf der Website des Betreibers hingewiesen.

VERZEICHNISSE

Autor(en) und Gültigkeitshistorie

Die historischen Versionen dieses Dokuments sind über die Website des Betreibers abrufbar.

Die Gültigkeit der jeweiligen Dokumente ergibt sich aus dem Beginndatum der Gültigkeit und dem Beginndatum der Gültigkeit des nächstfolgenden Dokuments. Sofern nicht anders vermerkt endet die Gültigkeit des alten Dokuments am Vortag der Gültigkeit des neuen Dokuments.

Name	Version	Stand	Datei	Kommentar
	Version 1.0 bis Version 1.4			interne Fassungen, die nicht in Kraft traten
Hans G. Zeger	Version 1.5	10.08.2006	globaltrust-certificate-policy.20060810.pdf	Stammfassung
Hans G. Zeger	Version 1.6	12.04.2007	globaltrust-certificate-policy.20070412.pdf	Ergänzungen lt. Änderungshistorie Version 1.6 Änderungen I 12. April 2007
Hans G. Zeger	Version 1.7	1. April 2014		interne Fassungen, die nicht in Kraft trat
Hans G. Zeger	Version 1.8	1. Juni 2014		interne Fassungen, die nicht in Kraft trat
Hans G. Zeger	Version 1.8a	1. Oktober 2014		
Hans G. Zeger	Version 1.8b	1. Februar 2015	globaltrust-certificate-policy.pdf	

ANHANG

ANHANG A: DOKUMENTATION

1 BIBLIOGRAPHIE

Die Listung der Dokumente erfolgt mit Stand 1. Februar 2015. Zur Anwendung kommt die jeweils gültige Fassung bzw. der entsprechende zutreffende Folgestandard. Die eingesetzten Dokumente und Standards sind intern dokumentiert und werden laufend aktualisiert.

1 [ACOS-QES] Dateisystem mit Applikation für qualifizierte Signatur für Austriacard ACOS v0.6 Stand: 2013/02/11 AUSTRIA CARD-Plastikkarten und Ausweissysteme GmbH, A-1232 Wien, Lamezanstraße 4-8

2 [ACOS04-CC-CR-MAINT3] CC-EAL4+ Certification Report Nachtrag 3: Nachtrag Nr. 3 zur Sicherheitsbestätigung T-Systems.02166.TE.07.2008 ACOS EMV-A04V1 (r029) Stand: 2012/07/11
Original-Site: http://www.t-systems-zert.de/pdf/ein_02_sig_pro/zf_02166_3_d.pdf AUSTRIA CARD-Plastikkarten und Ausweissysteme GmbH, A-1232 Wien, Lamezanstraße 4-8

3 [ACOS04-CC-CR] CC-EAL4+ Certification Report: ACOS EMV-A04V1 (T-Systems.02166.TE.07.2008) Stand: 2008/07/18
Original-Site: http://www.t-systems-zert.de/pdf/ein_01_zer_itsec_cc/zr_01167-01168_e.pdf AUSTRIA CARD-Plastikkarten und Ausweissysteme GmbH, A-1232 Wien, Lamezanstraße 4-8

4 [ACOS05-CC-CR] CC-EAL4+ Certification Report: ACOS EMV-A05V1 Configuration A and Configuration B (T-Systems-DBZ-CC-01167/168-2009) Stand: 2009/10/30
Original-Site: http://www.t-systems-zert.de/pdf/ein_01_zer_itsec_cc/zr_01167-01168_e.pdf AUSTRIA CARD-Plastikkarten und Ausweissysteme GmbH, A-1232 Wien, Lamezanstraße 4-8

5 [ACOS05-CC-STA] CC-EAL4+ Security Target: ACOS EMV-A05V1 Configuration A Stand: 2009/10/16
Original-Site: http://www.t-systems-zert.de/pdf/ein_01_zer_itsec_cc/st_01167_e.pdf AUSTRIA CARD-Plastikkarten und Ausweissysteme GmbH, A-1232 Wien, Lamezanstraße 4-8

6 [ACOS05-CC-STB] CC-EAL4+ Security Target: ACOS EMV-A05V1 Configuration B Stand: 2009/10/16
Original-Site: http://www.t-systems-zert.de/pdf/ein_01_zer_itsec_cc/st_01168_e.pdf AUSTRIA CARD-Plastikkarten und Ausweissysteme GmbH, A-1232 Wien, Lamezanstraße 4-8

7 [ACOS] Austriacard ACOS Datenblatt Stand: 2010/11/01
Original-Site: http://www.austriacard.at/download/ACOS_CardOS_2010.pdf AUSTRIA CARD-Plastikkarten und Ausweissysteme GmbH, A-1232 Wien, Lamezanstraße 4-8

8 [ADOBE-TRUST] Adobe Approved Trust List Technical Requirements Version 1.3 - Anforderungen um mit dem Root Zertifikat in Adobe Acrobat eingetragen zu werden Stand: 2013/08/28
Original-Site: http://helpx.adobe.com/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download_0/file.res/aatl_technical_requirements_v13.pdf Adobe Systems Inc. (Corporate headquarters), USA-95110-2704 San Jose, CA, 345 Park Avenue

9 [APPLE-CA] Apple Root Certificate Program Stand: 2013/01/01
Original-Site: https://www.apple.com/certificateauthority/ca_program.html Apple Computer, Inc, USA-95014 Cupertino, 1 Infinite Loop

10 [ASIG-EXT] Hollosi A., X.509 Zertifikatserweiterungen für die Verwaltung, X509ext - v1.0.3 Stand: 2005/02/21
Original-Site: http://www.cio.gv.at/it-infrastructure/pki/X509ext-1.0.3-20050221.pdf Stabsstelle IKT-Strategie des Bundes (CIO Chief Information Officer), A-1010 Wien, Ballhausplatz 2

11 [ASIG-LAY] Layout Amtssignatur v2.0.1 Stand: 2014/12/31
Original-Site: http://www.ref.gv.at/AG-RS-Amtssignatur-las-2-0-1.3100.0.html Stabsstelle IKT-Strategie des Bundes (CIO Chief Information Officer), A-1010 Wien, Ballhausplatz 2

12 [ASIG-LTF] Leitfaden Amtssignatur v1.0.0 Stand: 2009/01/13
Original-Site: http://www.ref.gv.at/AG-RS-Amtssignatur-las-1-4-0.2195.0.html Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

13 [ASIG-MOA] MOA-Amtssignaturen - MOA-AS Spezifikation Version 1.0.1 Stand: 2008/02/11
Original-Site: https://demo.egiz.gv.at/plain/content/download/454/2634/file/Spezifikation-MOA-AS.pdf EGIZ E-Government Innovationszentrum, A-8010 Graz, Inffeldgasse 16a

14 [ASZ] Karlinger G., Amtssignaturzertifikate (ASZ) - Allgemeine Richtlinien für Amtssignaturzertifikate in der Verwaltung, Version 1.0.0 Stand: 2005/04/06
Original-Site: http://reference.e-government.gv.at/uploads/media/Amtssignaturzertifikate.AllgemeineRichtlinien.1-0-0.pdf Stabsstelle IKT-Strategie des Bundes (CIO Chief Information Officer), A-1010 Wien, Ballhausplatz 2

15 [BSI-100-1] BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS) v1.5 Stand: 2008/05/01
Original-Site: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001_pdf.pdf?__blob=publicationFile Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

16 [BSI-100-2] BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise v2.0 Stand: 2008/05/01
Original-Site: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

17 [BSI-100-3] BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz v2.5 Stand: 2008/05/01
Original-Site: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1003_pdf.pdf?__blob=publicationFile Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

18 [BSI-100-4] BSI-Standard 100-4 Notfallmanagement v1.0 Stand: 2008/11/01
Original-Site: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf?__blob=publicationFile Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

19 [BSI-DSZ-CC-0437-2008-MA-01] Certification report for SLE66CX680PE / m1534-a14, u.a. all optional with RSA2048 V1.5 and all with specific IC dedicated software - Assurance Continuity Maintenance Report Stand: 2008/09/25
Original-Site: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte04/0437_ma1_pdf.html Infineon Technologies AG, D-81726 München, -

20 [BSI-DSZ-CC-0437-2008-MA-02] Certification report for SLE66CX680PE / m1534-a14, u.a. all optional with RSA2048 V1.5 and all with specific IC dedicated software - Maintenancereport Stand: 2009/01/29
Original-Site:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte04/0437_ma2_pdf.html Infineon Technologies AG, D-81726 München, -

21 [BSI-DSZ-CC-0437-2008] Certification report for SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, all optional with RSA2048 V1.5 and all with specific IC dedicated software Stand: 2008/05/27
Original-Site:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte04/0437a_pdf.html Infineon Technologies AG, D-81726 München, -

22 [BSI-GRUND] BSI - IT Grundschutz - Beschreibung Stand: 2010/04/07
Original-Site:
https://www.bsi.bund.de/cln_174/DE/Themen/ITGrundschutz/StartseiteITGrundschutz/startseiteitgrundschutz_node.html Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

23 [BÜRGERKARTE] Die österreichische Bürgerkarte - Dokumentation und Spezifikation Version 1.2.0 Stand: 2008/02/20
Original-Site: http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/ A-SIT Zentrum für sichere Informationstechnologie - Austria, A-1030 Wien, Seidlgasse 22/9

24 [CABROWSER-BASE] CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v.1.2.3 Stand: 2014/10/16
Original-Site: https://cabforum.org/baseline-requirements-documents/ CA/Browser Forum, UUU keine aktuelle Adresse verfügbar

25 [CABROWSER-EV] Guidelines For The Issuance And Management Of Extended Validation Certificates v1.5.2 Stand: 2014/10/16
Original-Site: https://cabforum.org/extended-validation/ CA/Browser Forum, UUU keine aktuelle Adresse verfügbar

26 [CARDOS44-BSI-QES] Bestätigung BSI.02130.TE.07.2011 CardOS V4.4 with Application for QES, Version 1.01 Stand: 2011/07/15
Original-Site:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Signaturbestaetigung/02130_pdf.html Atos IT Solutions and Services GmbH, D-81739 München, Otto-Hahn-Ring 6

27 [CARDOS44-CC-CR-MAINT] CC EAL4+ Assurance Continuity Maintenance Report: "CardOS V4.4 with Application for QES Version 1.01" (BSI-DSZ-CC-0668-2010-MA-01 Zertifikat-Anhang) Stand: 2011/10/26
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/0668_ma1a_pdf.pdf Atos IT Solutions and Services GmbH, D-81739 München, Otto-Hahn-Ring 6

28 [CARDOS44-CC-CR] CC EAL4+ Certification Report: "CardOS V4.4 with Application for QES" (BSI-DSZ-CC-0668-2010) Stand: 2010/12/08
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/0668a_pdf.pdf Siemens IT Solutions and Services GmbH, D-81739 München, Otto-Hahn-Ring 6

29 [CARDOS44-CC-ST-MAINT] CardOS V4.4 CC "Security Target CardOS V4.4 with Application for QES" v0.70 Stand: 2011/07/13
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/0668_ma1b_pdf.pdf Atos IT Solutions and Services GmbH, D-81739 München, Otto-Hahn-Ring 6

30 [CARDOS44] Datenblatt Siemens CardOS 4.4 Stand: 2010/02/11
Original-Site:
http://www.insinova.ch/downloads/siemensproduktdatenblattcardosv4.4releasegp.pdf
Siemens Aktiengesellschaft - Med GS SEC, D-81737 München, Charles-de-Gaulle-Straße 2

31 [CARDOS50-BSI-QES] Bestätigung BSI.02136.TE.07.2013 CardOS V5.0 with Application for QES, V1.0 Stand: 2013/07/31
Original-Site:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Signaturbestaetigung/02136_pdf.pdf Atos IT Solutions and Services GmbH, D-81739 München, Otto-Hahn-Ring 6

32 [CARDOS50-CC-CR] CC EAL4+ Certification Report: "CardOS V5.0 with Application for QES, V1.0" (BSI-DSZ-CC-0833-2013) Stand: 2013/07/26
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/0833a_pdf.pdf Atos IT Solutions and Services GmbH, D-81739 München, Otto-Hahn-Ring 6

33 [CARDOS50-CC-ST] CC EAL4+ Security Target: "Security Target 'CardOS V5.0 with Application for QES V1.0', Rev. 2.00, Edition 03/2013" Stand: 2013/03/27
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/0833b_pdf.pdf Atos IT Solutions and Services GmbH, D-81739 München, Otto-Hahn-Ring 6

34 [CARDOS53-ASIT-QES] Bestätigung A-SIT-1.108 Sichere Signaturerstellungseinheit CardOS V5.3 QES, V1.0 Stand: 2014/08/08
Original-Site: http://www.a-sit.at/pdfs/bescheinigungen_sig/1108_bescheinigung_cardos-v53-qes-v10_final_signed.pdf Atos IT Solutions and Services GmbH, D-81739 München, Otto-Hahn-Ring 6

35 [CARDOS53-CC-CR] Certification Report "CardOS V5.3 QES, V1.0" (BSI-DSZ-CC-0921-2014) Stand: 2014/08/06 Atos IT Solutions and Services GmbH, D-81739 München, Otto-Hahn-Ring 6

36 [CARDOS53-CC-ST] Security Target 'CardOS V5.3 QES, V1.0', Rev. 1.61, Edition 07/2014 Stand: 2014/07/23 Atos IT Solutions and Services GmbH, D-81739 München, Otto-Hahn-Ring 6

37 [CC-ITSE] Common Criteria for Information Technology Security Evaluation v3.1 - Revision 3 (ISO 15408) Stand: 2009/07/01
Original-Site: http://www.commoncriteriaportal.org/cc/ Common Criteria - Management c/o GCHQ - Government Communications Headquarters, GB-GL51 0EX Cheltenham, Gloucestershire, Room A2b, Hubble Road

38 [CEM-ITSE] Common Methodology for Information Technology Security Evaluation v3.1 - Revision 3 (ISO 15408) Stand: 2009/07/01
Original-Site: http://www.commoncriteriaportal.org/cc/ Common Criteria - Management c/o GCHQ - Government Communications Headquarters, GB-GL51 0EX Cheltenham, Gloucestershire, Room A2b, Hubble Road

39 [CWA 15579] CWA 15579 - E-invoices and digital signatures (Dezember 2007) Stand: 2007/12/01
Original-Site: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eInvoicing/CWA15579-00-2007-Oct.pdf CEN-CENELEC Management Centre, B-1000 Brussels, Avenue Marnix 17

40 [CWA-14167-1] CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements Stand: 2003/06/01
Original-Site: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-01-2003-Jun.pdf CEN-CENELEC Management Centre, B-1000 Brussels, Avenue Marnix 17

41 [CWA-14167-2] CWA 14167-2 - Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP Stand: 2004/05/01
Original-Site: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-02-2004-May.pdf CEN-CENELEC Management Centre, B-1000 Brussels, Avenue Marnix 17

42 [CWA-14167-3] CWA 14167-3 - Cryptographic module for CSP key generation services protection profile - CMCKG PP Stand: 2004/05/01
Original-Site: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-03-2004-May.pdf CEN-CENELEC Management Centre, B-1000 Brussels, Avenue Marnix 17

43 [CWA-14167-4] CWA 14167-4 - Cryptographic module for CSP signing operations - Protection profile - CMCSO PP Stand: 2004/05/01
Original-Site: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-04-2004-May.pdf CEN-CENELEC Management Centre, B-1000 Brussels, Avenue Marnix 17

44 [CWA-14169] CWA 14169 - Secure signature-creation devices "EAL 4+" Stand: 2004/03/01
Original-Site: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14169-00-2004-Mar.pdf CEN-CENELEC Management Centre, B-1000 Brussels, Avenue Marnix 17

45 [DatenschutzRL] Richtlinie 95/46/EG (StF) idgF - Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr Stand: 2013/06/12
Original-Site: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:DE:HTML

46 [DSG 2000] BGBl. I Nr. 165/1999 (StF) idgF - Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000) Stand: 2014/01/01
Original-Site: http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597 Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

47 [E-GOVG] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG) - StF: BGBl. I Nr. 10/2004 Stand: 2010/12/30
Original-Site: http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230 Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

48 [eBillVO] Verordnung der Bundesministerin für Finanzen, mit der die Anforderungen an eine elektronische Rechnung bestimmt werden (E-Rechnung-UStV) - RIS-Version Stand: 2012/12/28
Original-Site: http://ftp.freenet.at/privacy/gesetze/ebilling-verordnung-2013.pdf BM für Finanzen (BMF), A-1010 Wien, Johannesgasse 5

49 [EG-REF] 2003/511/EG: Entscheidung der Kommission vom 14. Juli 2003 über die Veröffentlichung von Referenznummern für allgemein anerkannte Normen für Produkte für elektronische Signaturen gemäß der Richtlinie 1999/93/EG Stand: 2003/07/14
Original-Site: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003D0511:DE:HTML RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

50 [EG-SSCD] 2009/767/EG Maßnahmen zur Erleichterung der Nutzung elektronischer Verfahren über „einheitliche Ansprechpartner" gemäß der Richtlinie 2006/123/EG Stand: 2009/12/28
Original-Site: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:01_DEC_2009_767_54:DE:HTML RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

51 [EGOV-DOK] Übersicht E-Government-Dokumente Stand: 2014/12/31 Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

52 [ENISA-ALG] Algorithms, Key Sizes and Parameters Report - 2013 recommendations version 1.0 Stand: 2013/10/29
Original-Site: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report/at_download/fullReport European Network and Information Security Agency (ENISA), GR-700 13 Heraklion, Vassilika Vouton (P.O. Box 1309)

53 [ETOKEN-CC-CR] CC EAL4+ Certification Report: SafeNet eToken - Athena IDProtect/OS755 Java Card on Atmel AT90SC25672RCT-USB Microcontroller embedding IDSign applet Stand: 2011/03/04
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/ANSSI-CC_2011-03fr.pdf SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

54 [ETOKEN-CC-ST] CC EAL4+ Security Target: SafeNet eToken - Athena IDProtect/OS755 Java Card on Atmel AT90SC25672RCT-USB Microcontroller embedding IDSign applet v1.2 Stand: 2011/02/16
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/ANSSI-CC-cible_2011-03en.pdf SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

55 [ETOKEN-FIPS-CERT] FIPS 140-2 L2 Zertifikat #1135 Aladdin eToken PRO (Java) Stand: 2011/10/26
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1135.pdf SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

56 [ETOKEN-FIPS-SP] FIPS 140-2 L2 Security Policy #1135 Aladdin eToken PRO (Java) Stand: 2011/10/26
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1135.pdf SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

57 [ETOKEN] Safenet (USB) eToken pro - Produktbeschreibung Stand: 2012/10/08
Original-Site: http://www.safenet-inc.com/About_SafeNet/Resource_Library/Resource_Items/Product_Briefs_EDP/eToken_PRO_Product_Brief.aspx SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

58 [ETSI EN 319 411-2] ETSI EN 319 411-2 V1.1.1 (2013-01) ESI - Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates Stand: 2013/01/15
Original-Site: http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=34221 European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

59 [ETSI EN 319 411-3] ETSI EN 319 411-3 V1.1.1 ESI - Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates Stand: 2013/01/01
Original-Site: http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=34222 European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

60 [ETSI TR 101 564] ETSI TR 101 564 V1.1.1 : Electronic Signatures and Infrastructures (ESI); Guidance on ETSI TS 102 042 for Issuing Extended Validation Certificates for Auditors and CSPs Stand: 2011/09/01
Original-Site: http://www.etsi.org/deliver/etsi_tr/101500_101599/101564/01.01.01_60/tr_101564v010101p.pdf European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

61 [ETSI TS 101 862] ETSI TS 101 862 v1.3.3 Qualified Certificate profile Stand: 2006/01/01
Original-Site: http://www.etsi.org/deliver/etsi_ts/101800_101899/101862/01.03.03_60/ts_101862v010303p.pdf European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

62 [ETSI TS 102 042] ETSI TS 102 042 V2.4.1 (2013-02) - Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates Stand: 2013/02/04
Original-Site: http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.04.01_60/ts_102042v020401p.pdf European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

63 [ETSI TS 102 176] ETSI TS 102 176-1 V2.1.1 (2011-07) - Technical Specification Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms Stand: 2011/07/30
Original-Site: http://pda.etsi.org/exchangefolder/ts_10217601v020101p.pdf European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

64 [FIPS-140-2] FIPS PUB 140-2 - SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES inkl. Annex A-D Stand: 2001/05/25
Original-Site: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf NIST - National Institute of Standards and Technology, USA-MD 20899-107 Gaithersburg, 100 Bureau Drive, Stop 1070

65 [FORTIGATE-50B] Fortigate-50B Produktbeschreibung Stand: 2010/04/07
Original-Site: http://www.fortinet.com/products/fortigate/50B.html Fortinet Inc, USA-CA 94086 Sunnyvale, 1090 Kifer Road

66 [FORTIOS-CC-CR] Certification Report: EAL 4+ evaluation of Fortinet FortiGate Unified Threat Management Solutions and FortiOS 4.0 CC compliant firmware v1.0 Stand: 2012/01/23
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/383-4-133%20CR%20v1.0e.pdf Fortinet Inc, USA-CA 94086 Sunnyvale, 1090 Kifer Road

67 [FORTIOS-CC-ST] Fortinet FortiGate Unified Threat Management Solutions and FortiOS 4.0 CC Compliant Firmware Stand: 2011/12/06
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/383-4-133%20ST%20v1.2.pdf Fortinet Inc, USA-CA 94086 Sunnyvale, 1090 Kifer Road

68 [FORTIOS-FIPS-CERT] Fips 140-2 (Level 1) Certificate #1754: FortiOS v4.0MR3 Stand: 2012/07/17
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/FIPS140ConsolidatedCertList0019.pdf Fortinet Inc, USA-CA 94086 Sunnyvale, 1090 Kifer Road

69 [FORTIOS-FIPS-SP] Fips 140-2 (Level 1) Security Policy #1754: FortiOS 4.0 MR3 Stand: 2012/04/13
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1754.pdf Fortinet Inc, USA-CA 94086 Sunnyvale, 1090 Kifer Road

70 [HB-SICHERHEIT] Österreichisches Informationssicherheitshandbuch - Version 4.0.0 (Hrsg. Bundeskanzleramt) Stand: 2014/09/23
Original-Site: https://www.sicherheitshandbuch.gv.at/2013/index.php Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

71 [HPCURVE] HP ProCurve 2510-24 Switch - Produktbeschreibung Stand: 2010/04/07
Original-Site: http://h10010.www1.hp.com/wwpc/de/de/sm/WF06b/12883-12883-3445275-427605-427605-3356807-3637991.html Hewlett-Packard Company, USA-CA 94304-118 Palo Alto, 3000 Hanover Street

72 [HPDLR05] HP DL120 R05 Pentium E2160 Dual Core (1U) - Server - Produktbeschreibung Stand: 2010/04/07
Original-Site: http://h10010.www1.hp.com/wwpc/us/en/sm/WF06a/15351-15351-3328412-241644-3328421-3683232.html Hewlett-Packard Company, USA-CA 94304-118 Palo Alto, 3000 Hanover Street

73 [HPDL] HP ProLiant DL360R06 Server - Produktbeschreibung Stand: 2010/04/07 Original-Site: http://h10010.www1.hp.com/wwpc/de/de/sm/WF06b/15351-15351-3328412-241475-241475-3884319-3983580.html Hewlett-Packard Company, USA-CA 94304-118 Palo Alto, 3000 Hanover Street

74 [HPML] HP ProLiant ML350 - Server - Produktbeschreibung Stand: 2010/04/07 Original-Site: http://h10010.www1.hp.com/wwpc/us/en/sm/WF06b/15351-15351-241434-241646-241477-1121586-3199754-3785989.html?jumpid=reg_R1002_USEN Hewlett-Packard Company, USA-CA 94304-118 Palo Alto, 3000 Hanover Street

75 [ISO-7816-10] ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards Stand: 1999/01/01 Original-Site: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=30558 International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

76 [ISO-7816-11] ISO/IEC 7816-11:2004: Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods Stand: 2004/01/01 Original-Site: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=31419 International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

77 [ISO-7816-1234] ISO 7816-1: Physical Charcteristics of Integrated Circuit Cards ISO 7816-2: Dimensions and Location of the Contacts ISO 7816-3: Electronic Signals and Transmission Protocols ISO 7816-4: Interindustry Commands for Interchange Stand: 2008/03/01 Original-Site: http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-1.aspx International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

78 [ISO-7816-12] ISO/IEC 7816-12:2005: Identification cards - Integrated circuit cards -- Part 12: Cards with contacts -- USB electrical interface and operating procedures Stand: 2004/01/01 Original-Site: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=40604 International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

79 [ISO-7816-13] ISO/IEC 7816-13:2007: Identification cards -- Integrated circuit cards -- Part 13: Commands for application management in a multi-application environment Stand: 2004/01/01 Original-Site: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=40605 International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

80 [ISO-7816-15] ISO/IEC 7816-15:2004: Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application Stand: 2004/01/01 Original-Site: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=35168 International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

81 [ISO-7816-5] ISO/IEC 7816-5:2004: Identification cards -- Integrated circuit cards -- Part 5: Registration of application providers Stand: 2004/01/01 Original-Site: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=34259 International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

82 [ISO-7816-6C] ISO/IEC 7816-6:2004/Cor 1:2006: Corrigendum 1 for Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange Stand: 2006/01/01
Original-Site:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=44369 International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

83 [ISO-7816-6] ISO/IEC 7816-6:2004: Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange Stand: 2004/01/01
Original-Site:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=38780 International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

84 [ISO-7816-7] ISO/IEC 7816-7:1999: Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL) Stand: 2006/01/01
Original-Site:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=28869 International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

85 [ISO-7816-8] ISO/IEC 7816-8:2004: Identification cards -- Integrated circuit cards -- Part 8: Commands for security operations Stand: 2004/06/01
Original-Site:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=37989 International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

86 [ISO-7816-9] ISO/IEC 7816-9:2004: Identification cards -- Integrated circuit cards -- Part 9: Commands for card management Stand: 2006/01/01
Original-Site:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=37990 International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

87 [ISO27-A1TEL] A1 Telekom Austria - ISO 27001 Zertifikat 15/0 ISO/IEC 27001:2005 - pdf-Version deutsch + englisch Stand: 2012/11/28 A1 Telekom Austria AG, A-1020 Wien, Lassallestraße 9

88 [ITSEM] Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik Stand: 2003/09/01
Original-Site:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsem-dt_pdf.html Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

89 [ITU-X509v3-ERR] ITU-T Recommendation X.509v3 Fehlerbehebung Stand: 2011/02/01
Original-Site: http://handle.itu.int/11.1002/1000/11735 International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

90 [ITU-X509v3] ITU-T Recommendation X.509v3 - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks Stand: 2008/11/01
Original-Site: http://handle.itu.int/11.1002/1000/11735 International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

91 [ITU-X680] ITU-T Recommendation X.680 (11/2008), ISO/IEC 8824-1: 1998, Information Technology – Abstract Syntax Notation One (ASN.1), Specification of Basic Notation Stand: 2008/11/13
Original-Site: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.680-200811-I!!PDF-E&type=items International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

92 [ITU-X681] ITU X.681 - Abstract Syntax Notation One (ASN.1): Information object specification Stand: 2012/01/03
Original-Site: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.681-200811-I!!PDF-E&type=items

93 [ITU-X682] ITU X.682 - Abstract Syntax Notation One (ASN.1): Constraint specification Stand: 2012/01/03
Original-Site: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.682-200811-I!!PDF-E&type=items

94 [ITU-X683] ITU X.683 - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications Stand: 2012/01/03
Original-Site: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.683-200811-I!!PDF-E&type=items

95 [ITU-X690] ITU-T Recommendation X.690 (11/2008), ISO/IEC 8825-1: 1998, Information Technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) Stand: 2008/11/13
Original-Site: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.690-200811-I!!PDF-E&type=items International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

96 [ITU-X691] ITU X.691 - Abstract Syntax Notation One (ASN.1): Specification of Packed Encoding Rules (PER) Stand: 2012/01/03
Original-Site: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.691-200811-I!!PDF-E&type=items

97 [ITU-X692] ITU X.692 - Abstract Syntax Notation One (ASN.1): Specification of Encoding Control Notation (ECN) Stand: 2012/01/03
Original-Site: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.692-200811-I!!PDF-E&type=items

98 [ITU-X693] ITU X.693 - Abstract Syntax Notation One (ASN.1): XML Encoding Rules (XER) Stand: 2012/01/03
Original-Site: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.693-200811-I!!PDF-E&type=items

99 [LKVM] Linux KVM Virtualisierung - Produktinformation http://www.linux-kvm.org/ Stand: 2010/06/23
Original-Site: http://www.linux-kvm.org/page/Main_Page Red Hat, Inc, USA-27606 Raleigh, North Carolina, 1801 Varsity Drive

100 [LUNA-PCI-ADM] Luna PCI-E Administration Guide v5.4.1 Stand: 2014/07/04
Original-Site: http://test.a-cert.at/static/007-011329-006_lunapci_5-4-1_docs_revC/Content/PDF_PCI/ SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

101 [LUNA-PCI-CON] Luna PCI-E Configuration Guide v5.4.1 Stand: 2014/07/04
Original-Site: http://test.a-cert.at/static/007-011329-006_lunapci_5-4-1_docs_revC/Content/PDF_PCI/ SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

102 [LUNA-PCI-CREF] Luna PCI-E LunaCM Command Reference Guide v5.4.1 Stand: 2014/07/04
Original-Site: http://test.a-cert.at/static/007-011329-006_lunapci_5-4-1_docs_revC/Content/PDF_PCI/ SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

103 [LUNA-PCI-INS] Luna PCI-E Installation Guide v5.4.1 Stand: 2014/07/04
Original-Site: http://test.a-cert.at/static/007-011329-006_lunapci_5-4-1_docs_revC/Content/PDF_PCI/ SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

104 [LUNA-PCI-SDK] Luna PCI-E SDK Reference Guide v5.4.1 Stand: 2014/07/04
Original-Site: http://test.a-cert.at/static/007-011329-006_lunapci_5-4-1_docs_revC/Content/PDF_PCI/ SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

105 [LUNA-PCI-UTIL] Luna PCI-E Utilities Reference Guide v5.4.1 Stand: 2014/07/04
Original-Site: http://test.a-cert.at/static/007-011329-006_lunapci_5-4-1_docs_revC/Content/PDF_PCI/ SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

106 [LUNAK3-FIPS-CERT] FIPS 140-2 (L3) Zertifikat #685 "Luna PCI Cryptographic Module V2" (Hardware Version: VBD-01-0104; Firmware Version: 4.5.3) Stand: 2006/07/14
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt685.pdf SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

107 [LUNAK3-FIPS-SP] FIPS 140-2 (L3) Security Policy #685 "Luna PCI Cryptographic Module V2" (Hardware Version: VBD-01-0104; Firmware Version: 4.5.3) Revision 8 Stand: 2006/06/09
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp685.pdf SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

108 [LUNAK5-FIPS-CERT] FIPS 140-2 (L3) Zertifikat #1350 "Luna PCI-e 3000, Luna PCI-e 3000 Short-Form Factor (SFF), Luna PCI-e 7000 and Luna PCI-e 7000 SFF Cryptographic Modules V3.0" Stand: 2010/07/12
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1350.pdf SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

109 [LUNAK5-FIPS-SP] FIPS 140-2 (L3) Security Policy #1350 "Luna PCI-e 3000, Luna PCI-e 3000 Short-Form Factor (SFF), Luna PCI-e 7000 and Luna PCI-e 7000 SFF Cryptographic Modules V3.0" Revision 7 Stand: 2011/04/18
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1350.pdf SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

110 [MOBILE] Grundsatzpapier Mobile Signatur - Schwerpunktthema Bürgerkarte und eID - Version 1.0, 22.04.2008 Stand: 2008/04/22
Original-Site: https://demo.egiz.gv.at/plain/content/download/583/3362/file/Grundsatzpapier-Mobile-Signatur.pdf EGIZ E-Government Innovationszentrum, A-8010 Graz, Inffeldgasse 16a

111 [MOZILLA-CAMAINT] Mozilla CA Certificate Maintenance Policy (Version 2.2) Stand: 2013/07/26
Original-Site: https://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html Mozilla Foundation, USA-CA 94041-112 Mountain View, 1350 Villa Street, Suite C

112 [MOZILLA-CAPOL] Mozilla CA Certificate Inclusion Policy (Version 2.2) Stand: 2013/07/26
Original-Site: http://www.mozilla.org/projects/security/certs/policy/InclusionPolicy.html Mozilla Foundation, USA-CA 94041-112 Mountain View, 1350 Villa Street, Suite C

113 [MS-CA-TECHREQ] Windows Root Certificate Program - Technical Requirements version 2.0 Stand: 2013/11/11
Original-Site: https://social.technet.microsoft.com/wiki/contents/articles/1760.windows-root-certificate-program-technical-requirements-version-2-0.aspx Microsoft Corporation, USA-WA 98052-639 Redmond, One Microsoft Way

114 [MS-CA] Microsoft Root Certificate Program Stand: 2009/01/15
Original-Site: http://technet.microsoft.com/en-us/library/cc751157.aspx Microsoft Corporation, USA-WA 98052-639 Redmond, One Microsoft Way

115 [MySQL] MySQL - Server - Produktinformation Stand: 2010/04/07
Original-Site: http://www.mysql.com/downloads/mysql/ ORACLE CORP, USA-CA 94065 REDWOOD CITY, 500 ORACLE PARKWAY

116 [NAGIOS] Nagios - Dokumentation http://www.nagios.org/ Stand: 2010/04/07
Original-Site: http://www.nagios.org/about/features Nagios Enterprises, LLC, USA-MN 55108 Saint Paul, P.O. Box 8154

117 [OID-T1] Object Identifier der öffentlichen Verwaltung (Teil 1 - Hauptdokument) V1.0.0 Stand: 2009/02/27
Original-Site: http://www.ref.gv.at/AG-II-BK-OID-T1_OID-T2-1-0-0.2230.0.html Stabsstelle IKT-Strategie des Bundes (CIO Chief Information Officer), A-1010 Wien, Ballhausplatz 2

118 [OID-T2] Object Identifier der öffentlichen Verwaltung (Teil 2 - Taxative Definition) - Version 1.0.1 Stand: 2014/06/02
Original-Site: http://www.ref.gv.at/AG-II-BK-OID-T1_OID-T2-1-0-0.2230.0.html Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

119 [OSSH] OpenSSH - Produktbeschreibung Stand: 2010/04/07
Original-Site: http://www.openssh.com/features.html OpenBSD, CDN-T2G 1N8 Calgary, Alberta, 812 23rd Ave SE

120 [OSSL-FIPS-CERT] FIPS 140-2 certificate #1747 for OpenSSL FIPS Object Module Stand: 2012/07/16
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/FIPS140ConsolidatedCertList0018.pdf OpenSSL Software Foundation, Inc., USA-MD 21710 Adamstown, 1829 Mount Ephraim Road

121 [OSSL-FIPS-DOC] User Guide for the OpenSSL FIPS Object Module v2.0 Stand: 2012/07/03
Original-Site: http://www.openssl.org/docs/fips/UserGuide-2.0.pdf OpenSSL Software Foundation, Inc., USA-MD 21710 Adamstown, 1829 Mount Ephraim Road

122 [OSSL-FIPS-SP] OpenSSL FIPS 140-2 Security Policy Version 2.0.1 Stand: 2012/07/09
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1747.pdf OpenSSL Software Foundation, Inc., USA-MD 21710 Adamstown, 1829 Mount Ephraim Road

123 [OSSL-FIPS] FIPS 140-2 verification of the OpenSSL FIPS Object Module source distribution file (Übersicht) Stand: 2012/10/08
Original-Site: http://openssl.com/fips/verify.html OpenSSL Software Foundation, Inc., USA-MD 21710 Adamstown, 1829 Mount Ephraim Road

124 [OSSL] OpenSSL - Funktionsübersicht zu openssl (http://www.openssl.org/) Stand: 2014/06/12
Original-Site: http://www.openssl.org/ The OpenSSL Project, GB- unbekannt, unbekannt

125 [PKCS10] PKCS #10: Certification Request Syntax Standard Stand: 2000/05/26
Original-Site: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.pdf RSA The Security Division of EMC, USA-MA 01730 Bedford, 174 Middlesex Turnpike

126 [PKCS11] PKCS #11 v2.20: Cryptographic Token Interface Standard - pdf-Version Stand: 2004/06/28
Original-Site: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf RSA The Security Division of EMC, USA-MA 01730 Bedford, 174 Middlesex Turnpike

127 [PKCS12] PKCS #12: Personal Information Exchange Syntax Standard Stand: 1999/06/24
Original-Site: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf RSA The Security Division of EMC, USA-MA 01730 Bedford, 174 Middlesex Turnpike

128 [PKCS15] PKCS #15: Cryptographic Token Information Format Standard (v1.1) Stand: 2000/06/06
Original-Site: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-15/pkcs-15v1_1.pdf RSA The Security Division of EMC, USA-MA 01730 Bedford, 174 Middlesex Turnpike

129 [PKCS1] PKCS #1: RSA Cryptography Standard v2.1 Stand: 2002/06/14
Original-Site: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf RSA The Security Division of EMC, USA-MA 01730 Bedford, 174 Middlesex Turnpike

130 [PKCS8] PKCS #8: Private-Key Information Syntax Standard Stand: 1993/11/01
Original-Site: http://www.rsa.com/rsalabs/node.asp?id=2130 RSA The Security Division of EMC, USA-MA 01730 Bedford, 174 Middlesex Turnpike

131 [RFC2818] rfc2818 - HTTP Over TLS Stand: 2000/05/01
Original-Site: http://tools.ietf.org/html/rfc2818.html IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

132 [RFC3161] RFC3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) Stand: 2001/08/01
Original-Site: http://tools.ietf.org/html/rfc3161.html IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

133 [RFC3279] rfc3279 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile Stand: 2002/04/01
Original-Site: http://tools.ietf.org/html/rfc3279.html IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

134 [RFC3647] rfc3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework Stand: 2003/11/01
Original-Site: http://tools.ietf.org/html/rfc3647.html IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

135 [RFC3739] rfc3739 - Internet X.509 Public Key Infrastructure: Qualified Certificates Profile Stand: 2004/03/01
Original-Site: http://tools.ietf.org/html/rfc3739.html IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

136 [RFC4366] Transport Layer Security (TLS) Extensions Stand: 2006/04/01
Original-Site: http://tools.ietf.org/html/rfc4366.html IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

137 [RFC4511] rfc4511 - Lightweight Directory Access Protocol (LDAP): The Protocol Stand: 2006/06/01
Original-Site: http://tools.ietf.org/html/rfc4511.html IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

138 [RFC5280] rfc5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile Stand: 2008/05/01
Original-Site: http://tools.ietf.org/html/rfc5280.html IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

139 [RFC5652] Cryptographic Message Syntax (CMS) Stand: 2009/09/01
Original-Site: http://tools.ietf.org/html/rfc5652.html IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

140 [RFC5905] RFC5905 Network Time Protocol Version 4: Protocol and Algorithms Specification Stand: 2010/06/01
Original-Site: https://www.ietf.org/rfc/rfc5905.txt

141 [RFC6960] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP Stand: 2013/06/01
Original-Site: http://tools.ietf.org/html/rfc6960.html IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

142 [RTR-ALG] Empfohlene Algorithmen und Parameter für elektronische Signaturen - Fassung vom 1.6.2007 Stand: 2007/06/01 Rundfunk und Telekom Regulierungs-GmbH, A-1060 Wien, Mariahilfer Straße 77-79

143 [SigG] BGBl. I Nr. 190/1999 (StF) idgF - Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG) Stand: 2010/10/26
Original-Site:
http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10003685 Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

144 [SigVO-DE] VERORDNUNG (EU) Nr. 910/2014 elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt Stand: 2014/08/28
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910 RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

145 [SigVO-EN] REGULATION (EU) Nr. 910/2014 electronic identification and trust services for electronic transactions in the internal market Stand: 2014/08/28 RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

146 [SigV] BGBl. II Nr. 3/2008 (StF) idgF - Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 - SigV 2008) Stand: 2012/11/02
Original-Site:
http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20005618 Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

147 [SLES11] Suse Linux Enterprise Server 11 - Dokumentation http://www.suse.com/ Stand: 2010/04/07
Original-Site: https://www.suse.com/de-de/products/server/technical-information/ SUSE LINUX Products GmbH, D-90409 Nürnberg, Maxfeldstraße 5

148 [SLESHA] High Availability Extension - SUSE Linux Enterprise - Produktbeschreibung Stand: 2012/10/08
Original-Site: https://www.suse.com/de-de/products/highavailability/ SUSE LINUX Products GmbH, D-90409 Nürnberg, Maxfeldstraße 5

149 [SWALL-CC-CR] CC EAL4+ Certification Report: SonicOS v5.0.1 on NSA Series and TZ Series Appliances Stand: 2008/05/16
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/sonicwall-cert-e.pdf SonicWALL L.L.C., USA-CA 95124 SAN JOSE, 2001 LOGIC DRIVE

150 [SWALL-CC-ST] CC EAL4+ Security Target: SonicOS v5.0.1 on NSA Series and TZ Series Appliances Stand: 2008/05/16
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/sonicwall-sec-e.pdf SonicWALL L.L.C., USA-CA 95124 SAN JOSE, 2001 LOGIC DRIVE

151 [SWALL-FIPS-CERT] FIPS 140-2 L2 Zertifikat #1311: Sonicwall NSA-3500 (Firmware Version: SonicOS v5.5.1) Stand: 2010/05/19
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1311.pdf SonicWALL L.L.C., USA-CA 95124 SAN JOSE, 2001 LOGIC DRIVE

152 [SWALL-FIPS-SP] FIPS 140-2 L2 Security Policy #1311: Sonicwall NSA-3500 (Firmware Version: SonicOS v5.5.1) Stand: 2010/03/01
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1311.pdf SonicWALL L.L.C., USA-CA 95124 SAN JOSE, 2001 LOGIC DRIVE

153 [SWALL3500] Sonicwall NSA 3500 Produktbeschreibung - Übersicht Stand: 2010/04/07 Original-Site: http://www.sonicwall.com/us/products/NSA_3500.html SonicWALL L.L.C., USA-CA 95124 SAN JOSE, 2001 LOGIC DRIVE

154 [TKCERT] Nachweis der ISO 27001 - Zertifizierung der Telekom Austria AG Stand: 2010/04/14 Original-Site: http://www.iso27001certificates.com/Taxonomy/CertificatesResults.asp?Country=Austria A1 Telekom Austria AG, A-1020 Wien, Lassallestraße 9

155 [VKZ-EB] v1.2.12 Ebenen- und Bereichskennungen für das Verwaltungskennzeichen bzw. das Organisationskennzeichen Stand: 2014/01/10 Original-Site: http://reference.e-government.gv.at/uploads/media/VKZ-EB_1-2-12_2014-0110.pdf Stabsstelle IKT-Strategie des Bundes (CIO Chief Information Officer), A-1010 Wien, Ballhausplatz 2

156 [VKZ] Empfehlung Verwaltungskennzeichen (VKZ) 1.2.0 Kennzeichen für Organisationseinheiten von Gebietskörperschaften bzw. Körperschaften öffentlichen Rechts Stand: 2007/03/25 Original-Site: http://reference.e-government.gv.at/Veroeffentlichte-Informationen.203.0.html Stabsstelle IKT-Strategie des Bundes (CIO Chief Information Officer), A-1010 Wien, Ballhausplatz 2

157 [WEBTRUST-CA] Trust Service Principles and Criteria for Certification Authorities Version 2.0 Stand: 2011/07/01 Original-Site: http://www.webtrust.org/homepage-documents/item54279.pdf THE CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS, CDN-ON M5V 3H2 West Toronto, 277 Wellington Street

158 [WEBTRUST-EV] Webtrust for Certification Authorities - Extended Validation Audit Criteria v1.4 Stand: 2013/01/31 Original-Site: http://www.webtrust.org/homepage-documents/item72055.pdf THE CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS, CDN-ON M5V 3H2 West Toronto, 277 Wellington Street

159 [XMLSIG] XML Signature Syntax and Processing (Second Edition) - W3C Recommendation Stand: 2008/06/10 Original-Site: http://www.w3.org/TR/xmldsig-core/ W3C - World Wide Web Consortium, F-06902 Sophia Antipolis Cedex, 2004, route des Lucioles

2 INHALT AUSSTELLUNGS-, SPERR-, ENTSPERR- UND WIDERRUFS-PROTOKOLL FÜR ZERTIFIKATE

Protokoll zu Ausstellung Endkunden-Zertifikate

* Die Namen der Personen, die die Zertifizierung durchgeführt haben
* Zertifizierungszeitpunkt
* Eingesetztes Zertifzierungsprodukt (z.B. openssl)
* Bezeichnung des Zertifizierungsdienstes inkl. Name der verwendeten CA (z.B. A-CERT ADVANCED 3)
* Name und Organisation des Antragstellers
* Prüfung des Zertifiktes (Unterschrift des CA Zertifikates)
* Seriennummer des Zertifikates
* Fingerprint(s) des Zertifikates
* Textversion des Zertifikates
* PEM kodiertes Zertifikat
* Fingerprint(s) CA Zertifikat
* PEM kodiertes CA Zertifikat
* Verwendete ca-config Datei
* tatsächlich eingesetzte Hardware des privaten Schlüssels des CA-Zertifkates
* Tatsächlich eingesetzte Hardware des privaten Endkundenschlüssels (sofern Schlüssel von ZDA oder autorisierter Stelle erzeugt)
* Standort der Durchführung des Zertifizierungsdienstes
* Identifikationsdaten des Zertifizierungsrechners
* Versionsnummer des Zertifizierungstools

Protokoll zu Sperrung, Entsperrung und Widerruf Endkunden-Zertifikate

* Die Namen der Personen, die den Widerruf durchgeführt haben
* Durchführungsszeitpunkt
* Eingesetztes Zertifzierungsprodukt (z.B. openssl)
* Name der verwendeten CA (z.B. A-CERT ADVANCED 3)
* Seriennummer des widerrufenen Zertifikates
* Angaben zu den Sperr- und Widerrufsgründen
* Fingerprint(s) des widerrufenen-Zertifikates
* PEM kodiertes widerrufenen Zertifikates
* Textversion des widerrufenen Zertifikates
* Fingerprint(s) des CA-Zertifikates
* PEM kodiertes CA-Zertifikat
* Verwendete Konfiguration
* PEM kodierte CRL
* Signaturprüfung der CRL
* tatsächlich eingesetzte Hardware des privaten Schlüssels des CA-Zertifkates
* Standort der Durchführung des Zertifizierungsdienstes
* Identifikationsdaten des Zertifizierungsrechners
* Versionsnummer des Zertifizierungstools

3 UNTERSTÜTZTE SIGNATURERSTELLUNGSPRODUKTE

Die Aufzählung hat demonstrativen Charakter, weitere Produkte werden laufend auf der Website des ZDA veröffentlicht.

Produkte, die als sichere Signaturerstellungseinheiten geeignet sind:
- Smartcard mit Betriebssystem CardOS V4.4 [CARDOS44] mit Application for QES, zertifiziert gemäß CC EAL4+ (⇨ Certification Report [CARDOS44-CC-CR])
- Smartcard mit Betriebssystem ACOS ("Austria Card OS") [ACOS] mit Applikation lt. [ACOS-QES], Betriebssystem + Applikation Configuration A and Configuration B zertifiziert nach CC-EAL4+ (⇨ Certification Report [ACOS05-CC-CR])
- HSM inkl. Smartcards zu dem eine Bescheinigung gemäß [CWA-14169] vorgelegt werden kann

Weitere Produkte für Signaturerstellungseinheiten, die zur Ausstellung fortgeschrittener Signaturen geeignet sind:
- Safenet eToken PRO 72k zertifiziert gemäß FIPS 140-2 L2 Zertifikat #1135 [ETOKEN-FIPS-CERT] sofern gemäß Policy [ETOKEN-FIPS-SP] verwendet wird.
- alle Produkte, die zumindest eine Zertifizierung gemäß [CC-ITSE] EAL4+ oder gemäß [FIPS-140-2] L1 aufweisen

Produkte, die für mobile Signaturdienste geeignet sind:
- alle Produkte die gemäß Grundsatzpapier von E-GIZ zur mobilen Signatur ([MOBILE] in der aktuellen Version) als geeignet bezeichnet werden.
- alle Produkte, die zumindest eine Zertifizierung nach CC EAL4+ oder FIPS 140-2 L2 aufweisen

Produkte, die als serverseitige Signaturerstellungseinheit für qualifizierte Signaturen geeignet sind:
- HSM zu dem eine Bescheinigung gemäß [CWA-14169] vorgelegt werden kann

Produkte, die als mobile technische Einheiten für serverbasierte mobile Signaturdienste geeignet sind:
- alle Mobiltelefone, zu denen der Signator eine Erklärung abgibt, ausschließlich darüber zu verfügen