öffentlich

GLOBALTRUST® RKS-CARD Certificate Policy

[RKSCP - RKS-CARD Policy]

Autor: Hans G. Zeger

Version 1.0 / 1. Februar 2016

OID-Nummer: 1.2.40.0.36.1.1.61.1
Gültigkeitshistorie OID-Nummer: 1.2.40.0.36.1.1.61.99

Policy Online: http://service.globaltrust.eu/static/rks-card-policy.pdf

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

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

© e-commerce monitoring GmbH Februar 2016

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.

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

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 ZDA 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 bestehende Sicherheitskonzepte eingehalten werden

Informationssicherheit wird weiters durch ein klares personelles Rollenkonzept organisatorisch gesichert.

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.

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 (p61) gelisteten Dokumenten sicher zu stellen. Soweit erforderlich werden die Auditreports veröffentlicht bzw. zur Verfügung gestellt.

1.1 Übersicht / Overview

Die GLOBALTRUST® RKS-CARD Certificate Policy (GCP) regelt alle Anforderungen der Zertifizierungsdienste des ZDA gemäß [RKS-V] (Registrierkassensicherheitsverordnung) und den sachlich zugehörigen gesetzlichen Bestimmungen.

Die in diesem Dokument beschriebene GLOBALTRUST® RKS-CARD Certificate Policy wird im Folgenden kurz als "Policy" bezeichnet. 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 ZDA intern dokumentiert.

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.

1.2 Dokumenttitel und -identifikation / Document name and identification

Dokumententitel: "GLOBALTRUST® RKS-CARD Certificate Policy" (GCP)

Diese für GLOBALTRUST® gültige Policy hat die OID-Nummer: 1.2.40.0.36.1.1.61.1.

Das vorliegende Dokument tritt mit dem Tag der Veröffentlichung auf der Websitedes ZDA 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 (p72) mit den bibliographischen Angaben gelistet. Sie werden mit Stand 1. Februar 2016 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 Signaturen gemäß RKS-V.

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® RKS-CARD Certificate Policy erfordern, erfolgt die Anpassung so zeitgerecht, dass die geänderten Anforderungen erfüllt werden können.

Änderungshistorie

Version 1.0 Stammfassung 1. Februar 2016

1.3 Beteiligte / PKI participants

1.3.1 Zertifizierungsdienstanbieter / Certification authorities

Herausgeber und Zertifizierungsdienstanbieter (ZDA)

Herausgeber dieser GLOBALTRUST® RKS-CARD Certificate Policy und Zertifizierungsdiensteanbieter (ZDA) ist die e-commerce monitoring GmbH, ein nach österreichischem Recht im Firmenbuch eingetragenes Unternehmen mit Sitz in Wien (Handelsgericht Wien FN 224536 a). Der ZDA ist akkreditierter Zertifizierungsdiensteanbieter gemäß [SigG]. 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 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 ZDA oder mit Diensten oder Produkten des ZDA hergestellte Dienste oder Produkte benutzt. Die Nutzung kann mit oder ohne Vertrag mit dem ZDA erfolgen. Insbesondere ist jeder Nutzer der einen mit Zertifikat des ZDA bestätigten öffentlichen Schlüssel benutzt oder Empfängers von elektronisch signierten Informationen ist.

Beteiligte
Alle Personen und Einrichtungen, die dieser GLOBALTRUST® RKS-CARD Certificate Policy 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® RKS-CARD 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

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][1]
- [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 Akkreditierung von Dritten haben. Die Auditstelle ist akkreditiert 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 akkreditiert ist.

Betroffener
Alle Personen zu denen der ZDA 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 und dieser GLOBALTRUST® RKS-CARD Certificate Policy.

Bezüglich der Signaturerstellungseinheiten werden alle gemäß RKS-V zulässigen Produkte eingesetzt, insbesondere Smartcards oder HSMs, die zur sicheren Signatur geeignet sind.

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] inklusive der vereinfachten Version [ETSI TS 102 042]

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.

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 ZDA.

1.5.2 Kontaktperson / Contact person

Anfragen zum Dokument sind an den ZDA zu richten. Die aktuellen Kontaktdaten sind auf der Website des ZDA 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

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend, es werden keine CPS ausgegeben.

1.5.4 Verfahren zur Freigabe der CPS / CPS approval procedures

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend, es werden keine CPS ausgegeben.

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 ZDA.

Zertifizierungsdienste
Gesamtheit aller Dienstleistungen, die der ZDA zur RKS-V erbringt.
Die einzelnen Dienste sind als ⇨ Geschäftsprozesse organisiert.

serverbasierte Signaturdienste
Dienstleistungen des ZDA zur Verwaltung, Archivierung, Erstellung, Verifizierung oder Zustellung signierter Dokumente.

[RKS-V] Registrierkassensicherheits-Verordnung
Verordnung BGBl. II Nr. 410/2015 - Registrierkassensicherheitsverordnung, RKSV des BMF idF

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.

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).

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.

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].

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.

Zertifizierungssystem
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 ZDA.

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).

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.
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.

Produktbezeichnung

Ergänzende Angabe, die zur Beschreibung des Zertifizierungsdienstes dient. Unter anderem wird die Bezeichnung RKS-CARD verwendet.

2. VERÖFFENTLICHUNG UND AUFBEWAHRUNG / PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Aufbewahrung / Repositories

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

Historische Versionen des Dokuments werden versioniert und intern dokumentiert. Sie können auf Anfrage bei berechtigtem Interesse gegen Kostenersatz bereit gestellt werden.

2.2 Veröffentlichung von Zertifizierungsinformationen / Publication of certification information

Über die Website des ZDA 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 ZDA 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 Websitedes ZDA und ggf. zusätzlich per E-Mail oder brieflich mitgeteilt.

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.

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..

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 ZDA 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.

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.

Im Fall von Benennungskonflikten schlägt der ZDA 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 auf ihre Richtigkeit hin geprüft.

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

Sofern der private Schlüssel nicht durch den ZDA erzeugt wird, verlangt der ZDA 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.

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 Dokumentennummer, die Identitätsangaben der ausstellenden Behörde und das Ausstellungsdatum erforderlich.

Die Identitätsprüfung kann auch durch den bestand einer Geschäftsbeziehung mit dem ZDA oder einem Zertifizierungspartner des ZDA ersetzt werden.

Im Zertifikat können zusätzliche Angaben zur Person des Signators enthalten sein: Telefonnummer, Faxnummer und E-Mailadresse, Berufs- und Qualifikationsangaben, allenfalls weitere Daten. Die Korrektheit der zusätzlichen Daten wird geprüft.

3.2.4 Nicht-verifizierte Antragstellerdaten / Non-verified subscriber information

Die Zertifikate enthalten keine nicht-verifizierten Angaben.

Ausgeschlossen sind 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, soweit dies gemäß RKS-V erforderlich ist.

3.2.6 Kriterien für Interoperabilität / Criteria for interoperation

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

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

Die 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, p25).

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 (p26).

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 (p26).

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 (p38)

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.

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.

4.1.2 Anmeldungsverfahren und Verantwortlichkeiten / Enrollment process and responsibilities

Anträge von Organisationen müssen von einem befugten Organ gestellt werden. 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 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 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.

4.2.1 Durchführung Identifikation und Authentifikation / Performing identification and authentication functions

Die Identitätsfeststellung des Antragstellers erfolgt durch den ZDA, einen Zertifizierungspartner, eine vom ZDA 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 allen Fällen erfolgt die Identitätsfeststellung des Antragstellers
- durch Vorlage eines amtlichen Ausweises oder
- durch persönliche Bekanntheit mit dem Prüforgan oder
- durch Bestehen einer vertraglichen Geschäftsbeziehung zwischen Antragsteller und Prüfstelle.

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 ZDA 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.

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.

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 dieser Certificate Policy ablaufen.

Die in diesem Abschnitt beschriebenen Abläufe für die Zertifikatsausstellung gelten sinngemäß auch für
- ⇨ 4.6 Neuaustellung Zertifikat / Certificate renewal (p33)
- ⇨ 4.7 Neuausstellung des Zertifikats mit Erzeugung eines neuen Schlüsselpaares / Certificate re-key (p34)
- ⇨ 4.8 Zertifikatsänderung / Certificate modification (p35)

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

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

Bei Ausstellung eines Zertifikates wird ein Protokoll erstellt..
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.

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.

4.4 Zertifikatsannahme / Certificate acceptance

Der Signator hat die Annahme des Zertifikates und der dazugehörigen Nutzungsbestimmungen, insbesondere diese GLOBALTRUST® RKS-CARD Certificate Policy und das zugehörige **Fehler! Verweisquelle konnte nicht gefunden werden.** 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 ZDA werden auf der Website 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 ZDA 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 Zustellun
3. Die sichere Aufbewahrung der persönlichen Zertifikatszugangsdaten.

4. Die Anwendung entsprechender Vorsicht, um den unbefugten Gebrauch des privaten Schlüssels zu verhindern.
5. Die unverzügliche Benachrichtigung des ZDA, 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,
6. Die unverzügliche vollständig Außerbetriebnahme des Schlüssels, sobald er Kenntnis über dessen Kompromitierung erhält.
7. Die unverzügliche vollständig Außerbetriebnahme des Zertifikate, wenn ihm vom ZDA eine Kompromitierung des CA-Schlüssels zur Kenntnis gebracht wird.
8. Die sichere Verwahrung des Schlüssels liegt in der ausschließlichen Verantwortung des Signators.
9. Ungültige Schlüssel sind zu vernichten, dies gilt auch für auf Signaturerstellungeinheiten gespeicherte Schlüssel. Signaturerstellungseinheiten, die vom ZDA ersetzt werden sollen müssen an den ZDA retourniert werden..
10. 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 stehen.
11. 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.

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,
- sofern die Signatur im Rahmen einer Registrierkasse verwendet wird, werden die ergänzenden Bestimmungen der RKS-V beachtet,
- sämtliche Vorkehrungen die in der RKS-V oder anderen anzuwendenden Bestimmungen verordnet wurden, müssen eingehalten werden.

Bestehen Zweifel an der Gültigkeit des Zertifikats, insbesondere wenn die bereitgestellten Abfragemöglichkeiten zum 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.

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.

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 (p30).

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 (p31).

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 (p31).

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 (p31).

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 (p33).

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 (p33).

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 (p33).

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 ⇨ 4.6.5 Verfahren zur Annahme nach Neuausstellung Zertifikat / Conduct constituting acceptance of a renewal certificate (p33).

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 (p33).

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 (p34).

4.8 Zertifikatsänderung / Certificate modification

Zertifikatsänderungen unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6 Neuaustellung Zertifikat / Certificate renewal (p33)

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 (p33)

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 (p31).

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 (p31).

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 (p31).

4.9 Zertifikatswiderruf und -sperre / Certificate revocation and suspension

Widerruf: Ein Widerruf führt zur vorzeitigen Beendigung der Gültigkeit eines Zertifikats, eine Re-Aktivierung ist ausgeschlossen. Der Widerruf erfolgt unter Kontrolle von zumindest zwei Personen.

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

Die Tatsache des Widerrufs eines Zertifkates ist öffentlich verfügbar.

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.

Bei Widerruf eines Zertifikates wird ein Widerrufsprotokoll erstellt.

Signatoren werden über 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 ZDA erhält einen Beweis, dass der verwendete private Schlüssel kompromittiert wurde oder nicht mehr den aktuellen technischen Anforderungen entspricht.
4. Der ZDA erhält einen Beweis, dass das Zertifikat missbräuclich verwendet wurde
5. Der ZDA erhält Kenntnis davon, dass der Signator die Nutzungsbedingungen, die Certifcate Policy, das Certificate Practice Statement oder eine sonstige vertragliche Vereinbarung verletzt hat.
6. Der ZDA 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 ZDA erhält Kenntnis davon, dass ein Wildcardzertifikat dazu verwendete wurde um eine Subdomain in betrügerisch täuschender Absicht zu authentifizieren.
8. Der ZDA erhält Kenntnis von einer signifikanten Änderung bezüglich der im Zertifkat eingetragenen Informationen.
9. Der ZDA stellt fest, dass eine im Zertifikat eingetragen Information ungenau oder täuschend ist.
10. Der ZDA stellt seinen Betrieb ein, und hat mit keinem anderen ZDA eine Vereinbarung zu einer Fortführung geschlossen.
11. Der ZDA verliert das Recht, den jeweiligen Zertifikatstyp auszustellen, außer er er hat eine Vereinbarung geschlossen, den Widerrufsstatusdienst fortzuführen.
12. Der ZDA 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 ZDA hat qualifizierte Hinweise auf eine vertragswidrige Verwendung eines Zertifikats durch den Signator. Vertragswidrige Verwendung sind insbesondere Verstöße gegen diese Policy, gegen die vereinbarten AGBs oder sonstigen individuellen Vereinbarungen (inkl. Leistungs- und Zahlungsverpflichtungen).

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.

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 ZDA widerrufen und alle betroffenen Parteien darüber in Kenntnis gesetzt.

Der ZDA 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.

4.9.2 Berechtigte für Antrag auf Widerruf / Who can request revocation

Zum Widerruf 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 ZDA, 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 ZDA beantragt, ist zwingend eine 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.

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 (p38) Informationen vor, die einen Widerruf gemäß einem der in⇨ 4.9.1 Umstände für Zertifikatswiderruf / Circumstances for revocation (p36) angeführten Gründe zur Folge haben kann, so sind diese dem ZDA so rasch als möglich (jedenfalls binnen 72 Stunden) zu belegen.

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 Bürozeitenentgegen genommen und bearbeitet und unverzüglich nach Abschluss aller erforderlichen Prüfungen durchgeführt.

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.

Bei der Abarbeitung von Widerrufsanträgen 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 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 Zertifikate können anhand der vorgesehenen Widerrufsliste(n) validiert werden.

Sorgfältige Überprüfung der Gültigkeit des Zertifikates mittels des 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, p32) obligatorisch.

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

Die Aktualisierung der Widerrufslisten (CRL, Certificate Revokation List) erfolgt gemäß technischer Standards, jedenfalls bei jedem Widerruf eines Zertifikates.
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 Widerrufslisten werden nach jeder Sperre bzw. Widerruf aktualisiert.

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

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

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

Die Antwortzeiten für CRL- und OCSP[2]-Anfragen bleiben im Normalfall unter 10 Sekunden.

---

[2] OCSP = Online Certificate Status Protocol

4.9.11 Andere verfügbare Widerrufsdienste / Other forms of revocation advertisements available

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

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

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

4.9.14 Berechtigte für Antrag auf Sperre / Who can request suspension

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

4.9.15 Stellung eines Antrages auf Sperre / Procedure for suspension request

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

4.9.16 Dauer einer Zertifikatssperre / Limits on suspension period

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

4.10 Zertifikatsstatusdienste / Certificate status services

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

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® RKS-CARD Certificate Policy zur Kenntnis gebracht.
3. Der Verzeichnisdienst ist als ⇨ Permanenzdienst verfügbar. Unterbrechungen von mehr als 24h werden als Störfälle dokumentiert.
4. Die Verzeichnisdienste sind öffentlich und international zugänglich.

Eine Aufnahme in den Verzeichnisdienst unterbleibt, wenn der Signator es wünscht oder andere gewichtige Gründe vorliegen.

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 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 Widerrufsdienste werden auf Basis von 24/7/365 betrieben.

4.10.3 Zusätzliche Funktionen / Optional features

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

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.

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® RKS-CARD Certificate Policy für ZDA 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..

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 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.

Die Verfügbarkeit der zentralen Zertifizierungsdienste
- Verbreitung der ZDA-Zertifikate,
- Sperr- und Widerrufsmanagementund
- 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.

Die für die Sicherheit grundlegenden Vorgehensweisen sind in dieser Policy dokumentiert.

5.1 Bauliche Sicherheitsmaßnahmen / Physical controls

Die Zertifizierungsdienste werden ausschließlich in geeigneten Räumlichkeiten erbracht.

5.1.1 Standortlage und Bauweise / Site location and construction

Die Geschäftsführung des ZDA entscheidet, an welchem Ort die Zertifizierungsdienste stattzufinden haben.

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.

5.1.4 Gefährdungspotential durch Wasser / Water exposures

Die Auswahl des Standortes der zertifizierungskritischen Komponenten erfolgt unter Bedachtnahme der Unwahrscheinlichkeit einer Gefährdung durch Wasser.

5.1.5 Brandschutz / Fire prevention and protection

Es sind ausreichende Vorkehrungen zum Brandschutz getroffen.

5.1.6 Aufbewahrung von Speichermedien / Media storage

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

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.

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.

5.2.1 Rollenkonzept / Trusted roles

Die Zertifizierungsdienste werden gemäß dem intern festgelegten Rollenkonzepts erbracht.

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.

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 (⇨ Fehler! Verweisquelle konnte nicht gefunden werden.) 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.

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

- 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 Vertrauenswürdigkeit.
- 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 ZDA 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.

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.

5.4 Betriebsüberwachung / Audit logging procedures

5.4.1 Zu erfassende Ereignisse / Types of events recorded

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

Dokumentationsdaten mit besonderen Archivierungserfordernissen werden mit einem Zeitstempel oder einer anderen geeigneten Form der elektronischen Signatur versehen.

Während des regulären Bürobetriebes wird das Überwachungssystem laufend kontrolliert. Bei Ausfall kritischer Dienste erfolgt eine automatisierte Verständigung des Bereitschaftsdienstes per SMS. Der Bereitschaftsdienst reagiert im Rahmen einer festgelegten Eskalationsstrategie, 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.

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

Der ZDA setzt ein System zur Sammlung der betriebsrelevanten Audit-Daten ein, welches beim Systemstart aktiviert wird.

5.4.7 Benachrichtigung des Auslösers / Notification to event-causing subject

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

5.4.8 Gefährdungsanalyse / Vulnerability assessments

Die Zertifizierungsdienste wurden einer Risikoanalyse unterzogen.

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.

Die den Betrieb des Zertifizierungsdienstes betreffenden Ereignis- und Zertifizierungsdienstprotokolle werden bis Ende der Gültigkeit eines Zertifikates aufbewahrt.

5.5.1 Zu archivierende Aufzeichungen / Types of records archived

Zertifizierungsrelevante Vorgänge oder Abläufe werden protokolliert.

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.

5.5.2 Aufbewahrungsfristen für archivierte Daten / Retention period for archive

Die Aufbewahrungszeit ist die Dauer der Gültigkeit eines Zertifikates.

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

5.5.3 Schutz der Archive / Protection of archive

Die Aufbewahrung richtet sich nach dem Stand der Technik.

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" (p64) 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 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.

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

Die Integrität der Archive 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.

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 ZDA / Key changeover

Der Wechsel eines Schlüssels beim ZDA wird zeitgerecht geplant. 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 ZDA 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 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. 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 intern 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 ZDA wird regelmäßig überprüft und an geänderte Anforderungen angepasst.

Der technische Betrieb erfolgt beim ZDA 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 Zugriff auf Signaturerstellungsdaten wird beschränkt.

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

Der ZDA stellt Signaturerstellungseinheiten gemäß RKS-V zur Verfügung.

Die Ausstellung der Signaturerstellungseinheit erfolgt in einer vom ZDA gesicherten Umgebung

Lieferung der Signaturerstellungseinheiten erfolgt durch
(a) persönliche Übergabe in den Geschäftsräumen des Herstellers, eines von ihm autorisierten Händlers oder in den Geschäftsräumen des ZDA 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).

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.

Die Signaturschlüssel des ZDA 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.

Erzeugung der privaten Schlüssel des Signators

Die Schlüssel des Signators werden vom ZDA oder authorisierten Personen auf sicheren Signaturerstellungseinheiten oder RKS-V-konform bescheinigten Signaturerstellungseinheiten erzeugt.

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.
Die Zustellung von Signaturschlüssel an den Antragsteller erfolgt nur in Verbindung mit einer geeigneten Signaturerstellungseinheit..

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

Diese Zertifizierungsbestätigung bindet den Signator vertraglich an die anzuwendende Policy.
Abhängig von der Antragstellung erfolgt die Zustellung nach folgenden Regeln:

- 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 für diese Zertifikate die Zustellung von einer persönlichen Übernahmebestätigung abhängig zu machen.

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 ZDA 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.

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® RKS-CARD Certificate Policy.

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, insbesondere der RKS-V.

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 (p53) 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.

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.

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

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 (p20) anzusehen sind.

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

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

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

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

6.2.4 Backup privater Schlüssel / Private key backup

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

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

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 ZDA oder von privaten Schlüsseln 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.

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 ZDA 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 ZDA 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 (p20) 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 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 nach der Produktbeschreibung und den individuellen Anforderungen des Signators. Für Zertifikate der RKS-CARD ist die maximal zulässige Gültigkeitsdauer die Dauer des ausstellenden CA-Zertifikates.

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

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

6.4.2 Schutz von Aktivierungsdaten / Activation data protection

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

6.4.3 Andere Aspekte von Aktivierungsdaten / Other aspects of activation data

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

6.5 Sicherheitsmaßnahmen IT-System / Computer security controls

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

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

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 intern dokumentiert.

6.5.2 Beurteilung der Computersicherheit / Computer security rating

Die Sicherheit des gesamten Zertifizierungssystems wurde einer Risikoanalyse unterzogen..

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.

Zur Installation neuer Softwaremodule existieren Übergabeverfahren.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement / Security management controls

Die erforderlichen Sicherheitsmaßnahmen sind intern dokumentiert.

6.6.3 Sicherheitsmaßnahmen während des Lebenszyklus / Life cycle security controls

Die erforderlichen Sicherheitsmaßnahmen sind intern dokumentiert.

6.7 Sicherheitsmaßnahmen Netzwerke / Network security controls

Die erforderlichen Sicherheitsmaßnahmen sind intern dokumentiert.

6.8 Zeitstempel / Time-stamping

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

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

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.

7.1 Zertifikatsprofile / Certificate profile

Jedes Zertifikat wird mit einer eindeutigen Seriennummer ausgestellt.

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) ECDSA ab 256bit, jeweils mit einem Hash-Algorithmus der SHA2-Familie (z.B. SHA256),
- einen Verweis auf die anzuwendende Certificate Policy.

7.1.1 Versionsnummern / Version number(s)

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

7.1.2 Zertifikatserweiterungen / Certificate extensions

RKS-CARD-Zertifikate 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.

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).

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® RKS-CARD Certificate 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.

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

Welche Widerrufs- und Sperrdienste verwendet werden, sind im ausgegebenen Zertifikat festgelegt.

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 ZDA 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.

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 ZDA erklärt, dass dieses Dokument konform der RKS-V ist.

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

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

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

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

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

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

8.4 Behandelte Themen der Begutachtung / Topics covered by assessment

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

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

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

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.

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

Die jeweils gültigen Kosten und Konditionen werden auf der Website des ZDApubliziert 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 ZDA 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® RKS-CARD 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 ZDA 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

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

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).

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 gewährleistet die Geschäftsführung.

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 ZDA 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® RKS-CARD Certificate Policy, dem anzuwendenden **Fehler! Verweisquelle konnte nicht gefunden werden.** und der Website des ZDA vollständig beschrieben.

9.6.2 Leistungsumfang der Registrierungsstellen / RA representations and warranties

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

9.6.3 Zusicherungen und Garantien des Signators / Subscriber representations and warranties

Es gelten die Allgemeinen Geschäftsbedingungen des ZDA und diese Policy.

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.

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® RKS-CARD Certificate Policy ist bis auf Widerruf gülltig.

9.10.2 Beendigung der Gültigkeit / Termination

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

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

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 ZDA 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® RKS-CARD Certificate Policy oder sonstigen für die Erbringung der Zertifiziieungsdienste wesentlichen Bestimmungen widersprechen.

9.12 Änderungen / Amendments

9.12.1 Verfahren bei Änderungen / Procedure for amendment

Änderungen werden im Rahmen des internen Rollenkonzepts 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 ZDA veröffentlicht.

Ist eine Benachrichtigung auf elektronischen Wege nicht möglich oder nicht zulässig und die Information auf der Wesite des ZDA 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 ZDA veröffentlicht.

9.14 Gerichtsstand / Governing law

Der ZDA 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 (p61)

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

Die in diesem Dokument beschriebenen Zertifizierungsdienste zur RKS-V werden gemäß RKS-V erbracht.

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 ⇨ 4.5.1Nutzung des privaten Schlüssels und des Zertifikates durch den Signator / Subscriber private key and certificate usage (p31) 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

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

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)

Für diese GLOBALTRUST® RKS-CARD Certificate Policy nicht zutreffend.

9.16.5 Höhere Gewalt / Force Majeure

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

9.17 Andere Bestimmungen / Other provisions

Es liegt keine Änderung dieser **Fehler! Verweisquelle konnte nicht gefunden werden.** 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 ZDA hingewiesen.

VERZEICHNISSE

Autor(en) und Gültigkeitshistorie

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
Hans G. Zeger	Version 1.0	1. Februar 2016	Policy Online: http://service.globaltrust.eu/static/rks-card-policy.pdf	

ANHANG

ANHANG A: DOKUMENTATION

1 BIBLIOGRAPHIE

Die Listung der Dokumente erfolgt mit Stand 1. Februar 2016. 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 [A-SIT-VO] BGBl. II Nr. 31/2000 Verordnung A-SIT als Bestätigungsstelle gemäß SigG Stand: 2000/02/02
Original-Site:
http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20000371
Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

2 [ADOBE-TRUST-GENERAL] Adobe Approved Trust List - Übersicht über das CA Programm von Adobe Stand: 2013/08/28
Original-Site: http://helpx.adobe.com/acrobat/kb/approved-trust-list2.html
Adobe Systems Inc. (Corporate headquarters), USA-95110-2704 San Jose, CA, 345 Park Avenue

3 [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

4 [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

5 [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

6 [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

7 [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

8 [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

9 [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

10 [BMI-SZR] SZR 2.0 Anwendungsdokumentation extern Version 2.0 Stand: 2014/12/05
IT-Service - BM für Inneres (BMI), A-1090 WIEN, Berggasse 43

11 [BNA-ALG] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) Stand: 2014/01/13
Original-Site:
https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2014Algorithmenkatalog.pdf
Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, D-53113 Bonn, Tulpenfeld 4

12 [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

13 [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

14 [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

15 [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

16 [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, -

17 [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, -

18 [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, -

19 [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

20 [BÜRGERKARTE-STD] Standardisierte Key- und Infoboxen der österreichischen Bürgerkarte Stand: 2005/03/01
Original-Site: http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20140114/infoboxes/infoboxes.html
IT-Service - BM für Inneres (BMI), A-1090 WIEN, Berggasse 43

21 [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

22 [CABROWSER-BASE] CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.3.1 Stand: 2015/09/28
Original-Site: https://cabforum.org/baseline-requirements-documents/
CA/Browser Forum, UUU keine aktuelle Adresse verfügbar

23 [CABROWSER-EV] Guidelines For The Issuance And Management Of Extended Validation Certificates v1.5.7 Stand: 2015/09/28
Original-Site: https://cabforum.org/extended-validation/
CA/Browser Forum, UUU keine aktuelle Adresse verfügbar

24 [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

25 [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

26 [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

27 [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

28 [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

29 [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

30 [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

31 [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

32 [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

33 [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

34 [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

35 [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

36 [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

37 [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

38 [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

39 [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

40 [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

41 [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

42 [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

43 [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
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

44 [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

45 [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: 2013/05/23
Original-Site:
http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230
Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

46 [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

47 [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

48 [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

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

50 [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)

51 [EREGV-2009] Ergänzungsregisterverordnung 2009 - ERegV 2009 - RIS-Version Stand: 2015/08/26
Original-Site:
http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006490
Stammzahlenregisterbehörde, A-1010 Wien, Hohenstaufengasse 3

52 [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

53 [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

54 [ETOKEN-FIPS-L2-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

55 [ETOKEN-FIPS-L3-CERT] FIPS 140-2 L3 Zertifikat #1136 "Aladdin eToken PRO (java) HD" Stand: 2011/10/26
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1136.pdf
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

56 [ETOKEN-FIPS-L3-SP] FIPS 140-2 L3 Security Policy #1136 "Aladdin eToken PRO (java) HD" Stand: 2011/10/18
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1136.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 [ETSI TS 103 123] ETSI TR 103 123 V1.1.1 Electronic Signatures and Infrastructures (ESI); Guidance for Auditors and CSPs on ETSI TS 102 042 for Issuing Publicly-Trusted TLS/SSL Certificates Stand: 2012/11/16
Original-Site: http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?wki_id=38245
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

65 [ETSI TS 119 403] ETSI TS 119 403 V2.1.1 (2014-11) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers Stand: 2014/09/16
Original-Site: http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=44560
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

66 [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

67 [GOOGLE-DEP-SHA1] Issue 401365: Deprecate SHA-1 for certificates Stand: 2014/08/06
Original-Site: https://code.google.com/p/chromium/issues/detail?id=401365
Google Inc., USA-94043 Mountain View, CA, 1600 Amphitheatre Parkway

68 [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

69 [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

70 [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

71 [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

72 [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

73 [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

74 [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

75 [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

76 [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

77 [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

78 [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

79 [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

80 [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

81 [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

82 [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

83 [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

84 [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

85 [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

86 [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

87 [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

88 [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

89 [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

90 [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

91 [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

92 [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

93 [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

94 [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/index.html
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

95 [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/index.html
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

96 [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/index.html
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

97 [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/index.html
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

98 [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/index.html
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

99 [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/index.html
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

100 [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

101 [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

102 [LUNAK5-FIPS-CERT] FIPS 140-2 (L3) Zertifikat für Luna PCIe 3000 SFF (Hardware Version: VBD-04-0100; Firmware Version: 4.7.1) 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

103 [LUNAK5-FIPS-SP] FIPS 140-2 (L3) Security Policy für Luna PCIe 3000 SFF 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

104 [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

105 [MOZILLA-CAPOL] Mozilla CA Certificate Policy Version 2.2 Stand: 2013/07/25
Original-Site: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
Mozilla Foundation, USA-CA 94041-112 Mountain View, 1350 Villa Street, Suite C

106 [MOZILLA-CHECK] CA:SubordinateCA checklist Stand: 2014/09/16
Original-Site: https://wiki.mozilla.org/CA:SubordinateCA_checklist
Mozilla Foundation, USA-CA 94041-112 Mountain View, 1350 Villa Street, Suite C

107 [MOZILLA-PROB] Mozilla Wiki Problematic Practices Stand: 2014/05/27
Original-Site: https://wiki.mozilla.org/CA:Problematic_Practices
Mozilla Foundation, USA-CA 94041-112 Mountain View, 1350 Villa Street, Suite C

108 [MOZILLA-REC] Mozilla Wiki Recommended Practices Stand: 2014/05/27
Original-Site: https://wiki.mozilla.org/CA:Recommended_Practices
Mozilla Foundation, USA-CA 94041-112 Mountain View, 1350 Villa Street, Suite C

109 [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

110 [MS-CA] Microsoft Trusted Root Certificate: Program Requirements Stand: 2016/01/06
Original-Site: http://technet.microsoft.com/en-us/library/cc751157.aspx
Microsoft Corporation, USA-WA 98052-639 Redmond, One Microsoft Way

111 [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

112 [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

113 [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

114 [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

115 [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

116 [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

117 [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

118 [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

119 [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

120 [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

121 [PERSBIND-XML] XML-Spezifikation der Personenbindung v1.2.2 - pdf-Version Stand: 2005/02/14
Original-Site: http://www.buergerkarte.at/konzept/personenbindung/spezifikation/20050214/

122 [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

123 [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

124 [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

125 [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

126 [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

127 [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

128 [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

129 [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

130 [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

131 [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

132 [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

133 [RFC4366] 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

134 [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

135 [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

136 [RFC5652] 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

137 [RFC5816] rfc5816 - ESSCertIDv2 Update for RFC 3161 ("Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)") Stand: 2010/03/01
Original-Site: https://www.ietf.org/rfc/rfc5816.txt
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

138 [RFC5905] rfc5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification Stand: 2010/06/01
Original-Site: https://www.ietf.org/rfc/rfc5905.txt

139 [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

140 [RFC7159] The JavaScript Object Notation (JSON) Data Interchange Format Stand: 2014/03/01
Original-Site: https://tools.ietf.org/html/rfc7159
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

141 [RFC7515] The JavaScript Object Notation (JSON) Data Interchange Format Stand: 2015/05/01
Original-Site: https://tools.ietf.org/html/rfc7515
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

142 [RFC7518] JSON Web Algorithms (JWA) Stand: 2015/05/01
Original-Site: https://tools.ietf.org/html/rfc7518
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

143 [RKS-V] BGBl. II Nr. 410/2015 - Registrierkassensicherheitsverordnung, RKSV Stand: 2015/12/11
Original-Site: http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2015_II_410
BM für Finanzen (BMF), A-1010 Wien, Johannesgasse 5

144 [RTR-ALG] Empfohlene Algorithmen und Parameter für elektronische Signaturen - Fassung vom 1.6.2007 Stand: 2007/06/01
Rundfunk und Telekom Regulierungs-GmbH (RTR), A-1060 Wien, Mariahilfer Straße 77-79

145 [SigG] BGBl. I Nr. 190/1999 (StF) idgF - Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG) Stand: 2016/01/30
Original-Site:
http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10003685
Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

146 [SigRL-EN] Abl. L 13/12 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures Stand: 2000/01/19
Original-Site: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

147 [SigRL] Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen Stand: 2000/01/19
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:31999L0093
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

148 [SIGVO-DB-SPEZF-DE] Abl. L 235/37 Durchführungsbeschluss (EU) 2015/1506 Spezifikation Formate fortgeschrittene Signaturen/Siegel Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015D1506
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

149 [SIGVO-DB-SPEZF-EN] Abl. L 235/37 COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 specifications relating to formats of advanced electronic signatures Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015D1506
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

150 [SIGVO-DB-TRUST-DE] Abl. L 235/26 Durchführungsbeschluss (EU) 2015/1505 Vertrauenslisten Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015D1505
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

151 [SIGVO-DB-TRUST-EN] Abl. L 235/26 COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 trusted lists Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015D1505
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

152 [SIGVO-DB-TRUST-EN] Abl. L 235/26 Durchführungsbeschluss (EU) 2015/1505 Vertrauenslisten http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015D1505 Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1505&from=DE
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

153 [SIGVO-DB-ZUSAMMMEN-DE] Abl. L 53/14 Durchführungsbeschluss (EU) 2015/296 Verfahrensmodalitäten Zusammenarbeit Mitgliedstaaten auf Gebiet elektronische Identifizierung Stand: 2015/02/25
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015D0296
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

154 [SigVO-DE] Abl. L 257/73 VERORDNUNG (EU) 910/2014 elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt ("eIDAS-Verordnung") 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

155 [SIGVO-DV-INTER-DE] Abl. L 235/1 Durchführungsverordnung (EU) 2015/1501 Interoperabilitätsrahmen Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015R1501
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

156 [SIGVO-DV-INTER-EN] Abl. L 235/1 COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 interoperability framework Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015R1501
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

157 [SIGVO-DV-MINIMUM-DE] Abl. L 235/7 Durchführungsverordnung (EU) 2015/1502 Mindestanforderungen an technische Spezifikationen und Verfahren Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015R1502
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

158 [SIGVO-DV-MINIMUM-EN] Abl. L 235/7 COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 minimum technical specifications and procedures Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015R1502
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

159 [SIGVO-DV-TRUSTQ-DE] Abl. L 128/13 Durchführungsverordnung (EU) 2015/806 Spezifikationen EU-Vertrauenssiegels qualifizierte Vertrauensdienste Stand: 2015/05/23
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015R0806
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

160 [SIGVO-DV-TRUSTQ-EN] Abl. L 128/13 COMMISSION IMPLEMENTING REGULATION (EU) 2015/806 EU specifications trust mark for qualified trust services Stand: 2015/05/23
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015R0806
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

161 [SigVO-EN] Abl. L 257/73 REGULATION (EU) Nr. 910/2014 electronic identification and trust services for electronic transactions in the internal market ("eIDAS-Regulation") Stand: 2014/08/28
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

162 [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

163 [STZREGBEHV-2009] Stammzahlenregisterbehördenverordnung 2009 - StZRegBehV 2009 - RIS-Version Stand: 2015/08/26
Original-Site:
http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006487
Stammzahlenregisterbehörde, A-1010 Wien, Hohenstaufengasse 3

164 [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

165 [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

166 [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

167 [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

168 [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

169 [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