public / öffentlich

Final Version / Endfassung

GLOBALTRUST®
Certificate Practice Statement
[GCPS - VDA Betriebsleitlinien]

Autor: Hans G. Zeger

Version 2.0 / 22. Juni 2017

OID-Number/Nummer: 1.2.40.0.36.1.2.3.1
History/Historie OID-Number/Nummer: 1.2.40.0.36.1.2.3.99

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

Contact: http://www.globaltrust.eu/impressum.html

Limits: http://www.globaltrust.eu/limitation.html

Suspension(Sperre) / Revocation(Widerruf): http://www.globaltrust.eu/revocation.html

CONTENT/ INHALT

APPENDIX / ANHANG

1. INTRODUCTION / EINLEITUNG

This GLOBALTRUST® Certificate Practice Statement supplements the GLOBALTRUST® Certificate Practice Statement (OID 1.2.40.0.36.1.1.8.1) and sets out detailed procedures for the following product groups: GLOBALTRUST® and A-CERT.

The security requirements and measures of the CA are contained within the document, GLOBALTRUST® Certificate Security Policy (1.2.40.0.36.1.2.2.1). This document is not publicly available.

Product group GLOBALTRUST®

The certification services of the CA are carried out under the product description: GLOBALTRUST®. Products that conform to the requirements for qualified signatures and qualified certificates can contain the addition, "QUALIFIED". Products that conform to the requirements for advanced signatures as per the Signature Law [SVG] can contain the addition, "ADVANCED". The scope of validity comes from the applicable Certificate Policy.

Product group A-CERT

For A-CERT products, the issuer is not the CA but the operator. Operation takes place along the same standards as those for GLOBALTRUST® as per the policies of the applicable products. For A-CERT products, the CA is the "ARGE DATEN – Austrian Society for Data Protection" (ZVR 774004629), the association registered in Austria as per the association law, hereafter referred to as the "Society".

Dieses GLOBALTRUST® Certificate Practice Statement ergänzt die GLOBALTRUST® Certificate Policy (OID-Nummer: 1.2.40.0.36.1.1.8.1) und regelt die detaillierte Vorgangsweise für folgende Produktgruppen: GLOBALTRUST® und A-CERT.

Die sicherheitstechnischen Anforderungen und Maßnahmen des VDA sind im Dokument GLOBALTRUST® Certificate Security Policy (OID-Nummer: 1.2.40.0.36.1.2.2.1) enthalten. Dieses Dokument ist nicht öffentlich verfügbar.

Produktgruppe GLOBALTRUST®

Die Zertifizierungsangebote des VDA werden unter der Produktbezeichnung GLOBALTRUST® betrieben. Produkte die den Anforderungen der qualifizierten Signatur bzw. qualifizierten Zertifikaten entsprechen, können den Zusatz "QUALIFIED" erhalten, Produkte die den Anforderungen der fortgeschrittenen Signatur gemäß Signaturgesetz [SVG] entsprechen, können den Zusatz "ADVANCED" erhalten. Der Umfang der Gültigkeit ergibt sich aus der jeweils anzuwendenen Certificate Policy.

Produktgruppe A-CERT

Für die Produkte A-CERT ist der Herausgeber nicht Zertifizierungsdienstanbieter (VDA) sondern Betreiber. Der Betrieb erfolgt nach denselben Standards wie für GLOBALTRUST® gemäß den Policies zu den jeweiligen Produkten. Für die Produkte A-CERT ist der in Österreich nach dem Verreinsrecht eingetragene Verein "ARGE DATEN - Österreichische Gesellschaft für Datenschutz" (ZVR 774004629), in Folge kurz "Verein" VDA.

Product documentation

The list of certification products offered for GLOBALTRUST® and A-CERT, as per the GLOBALTRUST® Certificate Policy, the GLOBALTRUST® Certificate Practice Statement and GLOBALTRUST® Certificate Security Policy, a description and a reference to their valid applicable documents are published and continually updated on the website of the operator.

This product information assists the selection and application of the right certification products and does not replace the binding reference to the applicable Certificate Policy contained in every certificate issued.

Additional conditions for mobile signature services

Mobile signature services can contain the addition, "MOBILE", or are otherwise clearly labelled as mobile signature services. The label can be used on its own or in connection with "QUALIFIED".

Mobile signature services can be offered as qualified, advanced or simple electronic signature services.

Mobile signature services are initiated using mobile phones or other suitable mobile technical devices. Mobile signature services are offered as server services or as "direct electronic signature" (signature on end device) in a mobile technical device.

For server services, the technical facilities comply with the same security requirements that apply to server services for issuing certificates (⇨ GLOBALTRUST® Certificate Security Policy).

For server services, the mobile technical device performs the role of a security-strengthening factor to secure possession of the only signature-unlocking components (eg. mobile phones), alongside knowledge of privileged information (eg. knowledge of the signature PIN to unlock the signature function). This complies with two-factor authentication for server-side signature creation devices and is analogue with the procedure

Produktdokumentation

Die Liste der gemäß der GLOBALTRUST® Certificate Policy, des GLOBALTRUST® Certificate Practice Statement und GLOBALTRUST® Certificate Security Policy angebotenen Zertifizierungsprodukte zu GLOBALTRUST® und A-CERT, eine Beschreibung und der Verweis auf ihre jeweils gültigen Dokumente wird auf der Website des Betreibers veröffentlicht und laufend aktualisiert.

Diese Produktinformation dient zur Unterstützung in der Auswahl und Anwendung der richtigen Zertifizierungsprodukte und ersetzt nicht den verbindlichen Verweis auf die anzuwendende Certificate Policy, die in jedem ausgelieferten Zertifikat enthalten ist.

Ergänzende Bestimmungen für mobile Signaturdienste

Mobile Signaturdienste können den Zusatz "MOBILE" enthalten oder sind auf andere Weise eindeutig als mobiler Signaturdienst gekennzeichnet. Die Bezeichnung kann alleine oder in Verbindung mit "QUALIFIED" verwendet werden.

Mobile Signaturdienste können als qualifizierte, fortgeschrittene oder einfache elektronische Signaturdienste angeboten werden.

Mobile Signaturdienste werden mittels Mobiltelefonen oder anderer geeigneter mobiler technischer Einheiten ausgelöst. Mobile Signaturdienste werden als Serverdienste oder als "direkte elektronische Signatur" (Signatur am Endgerät) in der mobilen technischen Einheit angeboten.

Bei Serverdiensten entspricht die technische Einrichtung denselben Sicherheitsanforderungen wie sie der Ausstellung von Zertifikaten unterliegt (⇨ GLOBALTRUST® Certificate Security Policy).

Die mobile technische Einheit übernimmt bei Serverdiensten die Rolle des sicherheitsverstärkenden Faktors um neben dem Wissen um ein Geheimnis (z.B. Wissen der Signatur-PIN zum Auslösen der Signaturfunktion) auch den Besitz der alleinigen signaturauslösenden Komponente (z.B. Mobiltelefons) sicherzustellen. Dies entspricht der Zwei-Faktor-Authentifizierung gegenüber dem serverseitigen

for chipcard-based signature solutions (possession of a chipcard and knowledge of the PIN to initiate the signature function). Possession of the mobile technical device is verified using, in particular, a one-time password that is transmitted using suitable transmission paths (eg. verification SMS).

There are no special requirements for server-based signatures on a mobile phone. As mobile technical devices for server solutions, all systems that can be clearly identified without tampering and assigned to one person are taken into consideration. Suitable technical devices are listed on and continually added to the website of the CA.

Components that have a certification as per CC EAL4+ or FIPS 140-2 L2 are suitable as mobile technical devices for qualified electronic signature. In particular, this could be a SIM card with a cryptographic co-processor, microSD cards or USB tokens.

Specific obligations of the CA in performing mobile signature services

On the server-side, the CA is obligated to adhere to the GLOBALTRUST® Certificate Security Policy in the context of performing electronic signatures as a server service, as well as in performing other certification services, in particular, qualified timestamp services.

In the context of direct electronic signature, it is ensured that this can only be conducted on devices that conform to the technical requirements. For qualified electronic signatures, the signature component intended for this must have certification from a confirmation authority.

Server-based signature services are operated as per the same ⇨ as the other certification services of the CA.

The CA reserves the right to publish an additional Practice Statement to

Signaturerstellungsgerät und ist analog dem Vorgehen bei chipkarten-basierten Signaturlösungen (Besitz der Chipkarte und Wissen des PIN zum Auslösen der Signaturfunktion). Der Besitz der mobilen technischen Einheit wird insbesondere durch Abfrage eines Einmalpasswortes, dass über geeignete Übertragungswege übermittelt wurde (z.B. Verifikations-SMS) überprüft.

An ein Mobiltelefon werden bei einer serverbasierten Signatur keine besonderen Anforderungen gestellt. Als mobile technische Einheiten für Serverlösungen kommen alle Systeme in Betracht, die manipulationssicher eindeutig identifiziert und einer Person zugeordnet werden können. Geeignete technische Einheiten werden auf der Website des VDA gelistet und laufend ergänzt.

Als mobile technische Einheiten für die qualifizierte elektronische Signatur sind jene Komponenten geeignet, die eine Zertifizierung nach CC EAL4+ oder FIPS 140-2 L2 aufweisen, insbesondere können das SIM-Karten mit kryptographischen Coprozessor, microSD-Karten oder USB-Token sein.

Spezifische Verpflichtungen des VDA bei der Erbringung von Mobilen Signaturdiensten

Im Rahmen der Erbringung der elektronischen Signatur als Serverdienst verpflichtet sich der VDA serverseitig zur Einhaltung derselben GLOBALTRUST® Certificate Security Policy wie bei der Erbringung anderer Zertifizierungsdienste, insbesondere der qualifizierten Zeitstempeldienste.

Im Rahmen der direkten elektronischen Signatur wird sicher gestellt, dass diese nur auf Geräten erfolgen kann, die den technischen Anforderungen entsprechen. Im Falle der qualifizierten elektronischen Signatur muss die dafür vorgesehene Signaturkomponente die Zertifizierung einer Bestätigungsstelle aufweisen.

Serverbasierte Signaturdienste werden gemäß derselben ⇨ betrieben, wie die sonstigen Zertifizierungsdienste des VDA.

Der VDA behält sich vor, zu den serverbasierten Signaturdiensten auf

the server-based signature services on the basis of the GLOBALTRUST® Certificate Policy and the GLOBALTRUST® Certificate Security Policy.

Basis der GLOBALTRUST® Certificate Policy und der GLOBALTRUST® Certificate Security Policy ein ergänzendes Practice Statement zu veröffentlichen.

1.1 Overview / Übersicht

Documents are cited in square brackets [] and listed in ⇨ Appendix A:1 Bibliography / Bibliographie (p82) with bibliographic information. They are cited with the date, 22. Juni 2017, but are applied in the valid applicable version and applicable successor standards.

Where not otherwise stated, the validity of weblinks refers to editorial deadline of this document.

The current document, "GLOBALTRUST® Certificate Practice Statement" (GCPS), describes the essential operational processes for administering and issuing signature creation devices, signature creation data and certificates.

Adaptations to appendices, in particular taking current technical developments into consideration, do not mean changes to operational processes, and particularly do not mean changes to the security concept if they are carried out in accordance with the current document and the "GLOBALTRUST® Certificate Security Policy".

The GLOBALTRUST® Certificate Policy describes the general operational and technical requirements for issued certificates, where these are not already addressed in the current GLOBALTRUST® Certificate Practice Statement (GCPS) in detail. The GLOBALTRUST® Certificate Policy is recorded with its OID and the URL it can be retrieved from in every issued certificate.

Dokumente werden in eckigen Klammern [] zitiert und finden sich im ⇨ 1 Bibliography / Bibliographie (p82) mit den bibliographischen Angaben gelistet. Sie werden mit Stand 22. Juni 2017 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.

Das vorliegende Dokument "GLOBALTRUST® Certificate Practice Statement" (GCPS) beschreibt alle wesentlichen betrieblichen Abläufe zur Verwaltung und Ausstellung von Signaturerstellungseinheiten, Signaturerstellungsdaten und Zertifikate.

Anpassungen der Anhänge, insbesondere um aktuelle technische Entwicklungen zu berücksichtigen, bedeuten keine Änderung der betrieblichen Abläufe, insbesondere keine Änderung des Sicherheitskonzepts, wenn sie in Übereinstimmung mit dem vorliegenden Dokument und der "GLOBALTRUST® Certificate Security Policy" erfolgen.

Die GLOBALTRUST® Certificate Policy beschreibt die generellen betrieblichen und technischen Anforderungen zu den ausgegebenen Zertifikaten, soweit diese nicht im vorliegenden GLOBALTRUST® Certificate Practice Statement (GCPS) detailliert behandelt sind. Die GLOBALTRUST® Certificate Policy ist mit OID-Nummer und Abrufstandort in jedem ausgegebenen Zertifikat eingetragen.

1.2 Document name and identification / Dokumenttitel und -identifikation

Document title: "GLOBALTRUST® Certificate Practice Statement" (GCPS).

This Practice Statement has the
OID-Number/Nummer: 1.2.40.0.36.1.2.3.1).

The current document enters into force on the day of its publication on the website of the operator. Where not otherwise stated, the validity of earlier versions of the document ends when the new version becomes valid.

The current document was drafted in conformity with [RFC3647].

The current document describes all operational processes of the CA in conceptual form and is publicly available on the website of the operator.

History of changes

Version 1.0 Draft

Internal version and never entered into force

History of changes

Version 1.0a Draft

Internal version and never entered into force

Version 1.0b Original version

Editorial deadline: 22. Juni 2017

Dokumententitel: "GLOBALTRUST® Certificate Practice Statement" (GCPS)

Dieses Practice Statement hat die
OID-Number/Nummer: 1.2.40.0.36.1.2.3.1).

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

Das vorliegende Dokument wurde konform zu [RFC3647] erstellt.

Das vorliegende Dokument beschreibt alle betrieblichen Abläufe des VDA in konzeptioneller Form und ist über die Website des Betreibers öffentlich abrufbar.

Änderungshistorie

Version 1.0 Entwurf

Interne Fassung und trat nie in Kraft.

Änderungshistorie

Version 1.0a Entwurf

Interne Fassung und trat nie in Kraft.

Version 1.0b Stammfassung

Redaktionsschluss: 22. Juni 2017

1.3 PKI participants / Beteiligte

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

1.3.1 Certification authorities / Zertifizierungsdienstanbieter

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

1.3.2 Registration authorities / Registrierungsstelle

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

1.3.3 Subscribers / Signator

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

1.3.4 Relying parties / Nutzer

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

1.3.5 Other participants / Weitere Beteiligte

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

1.4 Certificate usage / Verwendungszweck der Zertifikate

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

1.4.1 Appropriate certificate uses / Verwendungszweck

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

1.4.2 Prohibited certificate uses / Untersagte Nutzung der Zertifikate

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

1.5 Policy administration /Policy Verwaltung

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

1.5.1 Organization administering the document /Zuständigkeit für das Dokument

The current document is the sole responsibility of the CA.	Das vorliegende Dokument unterliegt der alleinigen Verantwortung des VDA.

1.5.2 Contact person / Kontaktperson

Queries about the document can be directed to the operator. Current contact data is listed on the website of the operator.	Anfragen zum Dokument sind an den Betreiber zu richten. Die aktuellen Kontaktdaten sind auf der Website des Betreibers gelistet.

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

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

1.5.4 CPS approval procedures / Verfahren zur Freigabe der CPS

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

1.6 Definitions and acronyms / Definitionen und Kurzbezeichnungen

As per GLOBALTRUST® Certificate Policy

In addition, the following definitions apply:

Product addition ADVANCED

Label used for certificates suitable for issuing advanced electronic signatures.

Product addition GOVERNMENT

Label used for certificates suitable for issuing governmental signatures as per the Austrian E-Government Law. At the same time, these certificates are suitable for advanced electronic signatures.

Product addition COMPANY

Describes all products for which sub-certificates are issued for subscribers. The rules for awarding sub-certificates can be specified using additional COMPANY policies. These are recorded in the issued sub-certificates.

Product addition QUALIFIED

Label used for qualified certificates suitable for creating advanced and qualified signatures. These certificates are subject to additional limitations on use.

Product addition CLIENT, SERVERCERT, FREECERT, DEMO, SERVER SERVER OV, SERVER EV

Label used for certificates suitable for creating other signatures (simple signatures) and encyption. Other additions not mentioned always denote certificates that are only suitable for creating simple signatures and for encryption.

Gemäß GLOBALTRUST® Certificate Policy

Zusätzlich gelten folgende Definitionen:

Produktzusatz ADVANCED

Bezeichnet Zertifikate, die für die Erstellung fortgeschrittener elektronischer Signaturen geeignet sind.

Produktzusatz GOVERNMENT

Bezeichnet Zertifikate, die für die Erstellung von Amtssignaturen nach dem österreichischen E-Government-Gesetz geeignet sind. Diese Zertifikate sind gleichzeitig für fortgeschrittene elektronische Signaturen geeignet.

Produktzusatz COMPANY

Beschreibt alle Produkte, bei denen Sub-Zertifikate für Signatoren ausgestellt werden. Die Regeln zur Vergabe der Sub-Zertifikate können durch zusätzliche COMPANY-Policies spezifiziert werden. Diese sind im ausgegebenen Sub-Zertifikat eingetragen.

Produktzusatz QUALIFIED

Bezeichnet qualifizierte Zertifikate, die für die Erstellung fortgeschrittener und qualifizierter Signaturen geeignet sind. Diese Zertifikate unterliegen zusätzlichen Anwendungsbeschränkungen.

Produktzusatz CLIENT, SERVERCERT, FREECERT, DEMO, SERVER SERVER OV, SERVER EV

Bezeichnet Zertifikate, die für die Erstellung sonstiger Signaturen (einfache Signaturen) und zur Verschlüsselung geeignet sind. Sonstige nicht angeführte Zusätze bezeichnen immer Zertifikate, die ausschließlich zur Erstellung einfacher Signaturen und zur Verschlüsselung geeignet sind.

Test certificates

Label used for certificates issued on the basis of X.509v3 standards for the purposes of testing. Identity verification of the applicant (subscriber) does not take place. Test certificates are identifiable, if at least one of the conditions is fulfilled:

- for X509v3 certificates, the CN identifier of the CA (issuer) is GLOBALTRUST FREECERT, GLOBALTRUST ADVANCED TEST, GLOBALTRUST GOVERNMENT TEST, in general, GLOBALTRUST ***[1] TEST
- for X509v3 certificates, the O identifier (organisation identifier) of the applicant (subject) features the mark, "Test: " prominently. For private persons, this is entered as "Test certificate",
- for X509v3 certificates, the certificate contains the corresponding extension (see CPS 7.1.2)
- for other certificate types, information on the CA and/or the applicant is selected so that its test status is clear.

Qualified certificates cannot be issued as test certificates.

Testzertifikate

Bezeichnet Zertifikate, die auf Basis des X.509v3-Standards zu Testzwecken ausgestellt werden. Eine Identitätsprüfung der Antragsteller (Signatoren) findet nicht statt. Testzertifikate sind erkennbar, wenn zumindest eine der Bedingungen erfüllt ist:

- bei X509v3-Zertifikaten lautet die CN-Bezeichnung des VDAs (Issuer) GLOBALTRUST FREECERT, GLOBALTRUST ADVANCED TEST, GLOBALTRUST GOVERNMENT TEST, allgemein GLOBALTRUST ***[2] TEST
- bei X509v3-Zertifikaten hat die O-Bezeichnung (Organisationsbezeichnung) des Antragstellers (Subject) den führenden Vermerk "Test: ", bei Privatpersonen den Eintrag "Testzertifikat",
- bei X509v3-Zertifikaten enthält das Zertifikat eine entsprechende Erweiterung (siehe CPS 7.1.2)
- bei anderen Zertifikatstypen sind VDA- und/oder Antragstellerangaben so zu wählen, das ihre Testeigenschaft eindeutig zum Ausdruck kommt.

Qualifizierte Zertifikate können nicht in Form von Testzertifikaten ausgestellt werden.

1 *** = additional productname

2 *** = beliebiger zulässiger Produktzusatz

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES / VERÖFFENTLICHUNG UND AUFBEWAHRUNG

2.1 Repositories / Aufbewahrung

The current version of this document is available on the website of the operator.
Historical versions of this document are available at the office of the regulator or under the OID 1.2.40.0.36.1.2.3.99 on the website of the operator.

Certificate holders are informed in a timely fashion of changes to the GLOBALTRUST® Certificate Practice Statement on the website and per email, if provided.

Die aktuelle Version dieses Dokuments ist über die Website des Betreibers abrufbar.
Historische Versionen des Dokuments sind bei der Aufsichtsstelle abzurufen oder unter der OID-Nummer 1.2.40.0.36.1.2.3.99 auf der Website des Betreibers abgelegt. Eine englische Übersetzung dieses Practice Statements wird unter der OID-Nummer 1.2.40.0.36.1.2.3.12 veröffentlicht[3].

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

2.2 Publication of certification information / Veröffentlichung von Zertifizierungsinformationen

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

2.3 Time or frequency of publication / Häufigkeit der Veröffentlichung

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

[3] Die Veröffentlichung erfolgt nach Abschluss der Genehmigung des GLOBALTRUST® Certificate Practice Statement durch die Aufsichtsbehörde und hat informativen Charakter.

2.4 Access controls on repositories / Zugangsbeschränkungen

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

3. IDENTIFICATION AND AUTHENTICATION / IDENTIFIZIERUNG UND AUTHENTIFIKATION

3.1 Naming /Benennung

The clear assignment of the certificate to the subscriber is ensured by:

- creating the PKCS#10 request (for X.509v3 certificates) as a foundation for the certification,
- creating the certificate after a registration office or the certification office of the CA has checked all application data for correctness .

Die eindeutige Zuordnung des Zertifikats zum Signator ist sicher gestellt durch:

- Erstellung des PKCS#10-Requests (bei X.509v3 Zertifikaten) als Grundlage für die Zertifizierung,
- Erzeugung des Zertifikats nach Überprüfung aller Antragsdaten auf ihre Korrektheit durch eine Registrierungsstelle oder an der Zertifizierungsstelle des VDAs.

3.1.1 Types of names / Arten der Benennung

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

3.1.5 Uniqueness of names / Einmaligkeit von Benennungen

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

3.2 Initial identity validation / erstmalige Identitätsfeststellung

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

Verification can take place using, in particular, technical verification of signed data (certificate signing request) in accordance with suitable algorithms as per [ETSI TS 102 176].

Die Prüfung kann insbesondere durch die technische Prüfung von signierten Daten (Certificate Signing Request) unter Beachtung geeigneter Algorithmen nach [ETSI TS 102 176] passieren.

3.2.2 Authentication of organization identity / Authentifikation der Organisation

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

3.2.3 Authentication of individual identity / Identitätsprüfung von Personen

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

3.2.4 Non-verified subscriber information / Nicht-verifizierte Antragstellerdaten

In addition to the GLOBALTRUST® Certificate Policy, non-verified information is permitted under the following conditions:
- the certificate is labelled as a test certificate

Ergänzend zur GLOBALTRUST® Certificate Policy sind nicht-verifzierte Angaben unter folgenden Bedingungen zulässig:
- beim Zertifikat handelt es sich um ein als Testzertifikat gekennzeichnetes Zertifikat

- the additional label, "non-verified", is shown in close proximity to the non-verified applicant information, <Information> (non-verified)

- Nicht-verifizierte Antragstellerangaben erhalten in unmittelbarer Nähe die zusätzliche Bezeichnung "nicht-verifiziert", z.B. <Angaben> (nicht-verifiziert)

3.2.5 Validation of authority / Nachweis der Vertretungsbefugnis

In addition to the GLOBALTRUST® Certificate Policy, additional information on the represented organisation is necessary. If a person requests a certificate which can be used to conduct legal transactions for the organisation or another person, the following additional information is obligatory: name and address of the organisation/person and type of organisation (eg. registered society, registered business....). Furthermore, at least one agency should be named as a suitable source of information on the organisation (eg. a chamber the organisation belongs to, commercial register, an authority in charge of associations...). If the organisations are established according to the law, the legal provisions providing for their establishment should be named in place of an information source.

Furthermore, the functions (range of functions) the subscriber is authorised to represent are listed (where applicable, the scope is limited by value or procedure).

Ergänzend zur GLOBALTRUST® Certificate Policy sind zusätzliche Angaben zur vertretenen Organisation erforderlich: Wird von einer Person ein Zertifikat beansprucht, mit dem Rechtsgeschäfte für eine Organisation oder eine andere Person erledigt werden können, dann sind folgende Zusatzinformationen obligatorisch: Name und Anschrift der Organisation/Person und Organisationsform (z.B. eingetragener Verein, protokolliertes Unternehmen, ...). Weiters ist zumindest eine Stelle anzugeben, die als Auskunftsstelle für diese Organisation geeignet ist (z.B. zugehörige Kammer, Firmenbuch, Vereinsbehörde, Aufsichtsbehörde, ...). Sind Organisationen per Gesetz eingerichtet, ist statt der Auskunftsstelle die Gesetzesstelle anzuführen, auf Grund der die Einrichtung erfolgte.

Weiters kann angegeben werden, für welche Aufgaben (Aufgabenbereiche) der Signator vertretungsbefugt ist (gegebenenfalls ist der Umfang wertmäßig oder vorgangsmäßig zu begrenzen).

3.2.6 Criteria for interoperation / Kriterien für Interoperabilität

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS / ANFORDERUNGEN ZERTIFIKATSLEBENSZYKLUS

4.1 Certificate Application / Antragstellung

1. Applications for certification can be received online as well as offline. In particular, applications can be made using an online form, in written form, by email, fax, other means of electronic communication, by telephone, in person and in particular, verbally. Information on means of making an application can be found on the website of the CA, the GLOBALTRUST® Certificate Practice Statement or other publicly available publications of the CA.

2. The application form and all necessary information are available on the website of the CA or the reseller.
3. The certificate application contains the following minimum information: the name and address of the subscriber.
4. Information on the purpose of the certificate: information on the purpose can be optional or obligatory depending on the certification service provided.
5. Applications for server certificates contain at least a domain name or an IP address.
6. Notification of and consent to the general terms and conditions (GTCs) of the CA, this Policy and, where applicable further agreements dependent on certification.

7. A secure means of access is agreed with the applicant (for example, an activation password), with which he can access the provided documents (personal certificate, private key...) after successful

1. Anträge zur Zertifizierung werden sowohl online als auch offline entgegen genommen. Insbesondere können Anträge mittels Online-Formular, schriftlich, per eMail, per Fax, sonstige elektronische Kommunikationsmittel, telefonisch, persönlich, insbesondere auch mündlich gestellt werden. Über die Möglichkeiten der Antragstellung informiert die Website des VDA, das GLOBALTRUST® Certificate Practice Statement oder sonstige öffentlich zugängliche Publikationen des VDA.
2. Das Antragsformular und alle erforderlichen Informationen sind über die Website des VDAs oder der Vertriebspartner zugänglich.
3. Der Zertifikatsantrag enthält folgende Mindestangaben: den Namen und die Anschrift des Signators.
4. Angaben zum Zweck der Verwendung des Zertifikats: Die Angaben zum Zweck können je nach bereitgestelltem Zertifizierungsdienst optional oder obligatorisch sein.
5. Anträge für Serverzertifkate enthalten zumindest einen Domainnamen oder eine IP-Adresse.
6. Kenntnisnahme und Zustimmung zu den Allgemeinen Betriebs- und Nutzungsbedingungen (AGB's) des VDAs, zur vorliegenden Policy und gegebenenfalls zu weiteren zertifizierungsabhängigen Vereinbarungen.
7. Mit dem Antragsteller wird eine sichere Zugangsweise (etwa ein Aktivierungspasswort) vereinbart, mit dessen Hilfe er nach erfolgter Zertifizierung Zugang zu den bereitgestellten Unterlagen

certification.

(persönliches Zertifikat, privater Schlüssel, ...) hat.

4.1.1 Who can submit a certificate application / Berechtigung zur Antragstellung

Proof of identity is considered concluded if the signature creation data and documents can be delivered to the same address (in the same form) specified during a previous identity check and not revoked in the meantime.

Der Identitätsnachweis gilt als erbracht, wenn Signaturerstellungsdaten und -unterlagen an dieselbe Adresse (in derselben Form) zugestellt werden können, die bei einer vormaligen Identitätsprüfung festgelegt wurden und zwischenzeitlich kein Widerruf erfolgte.

4.1.2 Enrollment process and responsibilities / Anmeldungsverfahren und Verantwortlichkeiten

In addition to the GLOBALTRUST® Certificate Policy, the following applies:
Information provided by the subscriber on the hardware on which the private key is generated is checked by the CA as to whether the stated product is indeed suitable for the safekeeping of the private key. The foundation of this check is information from the manufacturer ("self declaration") or reports from registration authorities.

A X509v3 certificate contains the following extension if the associated key is stored on such hardware: 1.2.40.0.36.4.1.2: <used hardware>
Under "<used hardware>", the customary label or the label used by the registration authority is used to clearly label the hardware.

In addition, for all qualified certificates the necessary confirmations must be obtained from the regulatory authority, where applicable.

Ergänzend zur GLOBALTRUST® Certificate Policy gilt:
Angaben des Signators zur Hardware auf der der private Schlüssel generiert wird, werden vom VDA dahingehend geprüft, ob das angegebene Produkt tatsächlich zur gesicherten Verwahrung eines privaten Schlüssels geeignet ist. Grundlage dieser Überprüfung sind Herstellerangaben ("Selbst-Deklaration") oder Berichte von Bestätigungsstellen.

Ein X.509v3-Zertifikat erhält dann folgende Erweiterung:
1.2.40.0.36.4.1.2: <verwendete Hardware>
Unter "<verwendete Hardware>" wird die handelsübliche oder durch eine Bestätigungsstelle verwendete Bezeichnung zur eindeutigen Kennzeichnung der Hardware angegeben.

Bei qualifizierten Zertifikaten sind zusätzlich allfällig erforderliche Bestätigungen der Aufsichtsstellen einzuholen.

4.2 Certificate application processing / Bearbeitung von Zertifkatsanträgen

In addition to the GLOBALTRUST® Certificate Policy, the following applies:
It is checked as to whether the technical qualities of the subscriber's key comply with the requirements as per certificate type.

Ergänzend zur GLOBALTRUST® Certificate Policy gilt:
Es wird geprüft, ob die technischen Eigenschaften des Schlüssels des Signators den vom Zertifikatstypen abhängigen Anforderungen

Qualified, authoritative sources of information can be called upon to verify information on the organisation, in particular, the official telephone book or official directory. Organisations whose data is not available from a suitable qualified, authoritative source of information or who have not been established by law are treated on equal terms to a private person. Organisation information is seen as optional additional information, comparable to the job or qualifications of a private person.

If a domain name must be checked before it is entered in a certificate, this takes place using one of the following methods:

1. Verifying at the registry that the domain owner and the applicant are identical.
2. Direct communication with the domain owner using an address, email address or telephone number either provided by the registry or obtained from a WHOIS entry.
3. A written confirmation from the domain owner, the registry or one of the persons listed in the WHOIS data.
4. Direct communication with the domain owner about a generic email address, for example, admin@domainname or webmaster@domainname. Parts of the domain name may be omitted.
5. The applicant can practically demonstrate control over the domain, in particular using a pre-agreed change to the website.
6. Another appropriate and well-documented method that ensures the same security as the methods above.

For EV certificates, only methods 1 to 5 are permitted.

If an IP address must be checked before it is entered in a certificate, this

entspricht.

Zur Prüfung der Angaben einer Organisation können qualifizierte behördliche Informationsquellen, insbesondere zusätzlich das amtliche Telefonbuch oder der Amtskalender herangezogen werden. Organisationen, deren Daten weder über eine geeignete qualifizierte behördliche Informationsquelle abrufbar noch per Gesetz eingerichtet sind, werden Privatpersonen gleichgestellt behandelt. Die Organisationsangaben werden als optionale Zusatzangaben, vergleichbar dem Beruf oder der Qualifikation einer Privatperson angesehen.

Muss vor der Eintragung in ein Zertifkat ein Domainname geprüft werden, so passiert dies mit einer der folgenden Methoden:

1. Beim Registrar verifizieren, dass Domaininhaber und Antragsteller ident sind.
2. Direkte Kommunikation mit dem Domaininhaber über eine Adresse, E-Mail Adresse oder Telephonnummer die entweder vom Registrar zur Verfügung gestellt wurde oder einem WHOIS Eintrag entnommen wurde.
3. Eine schriftliche Bestätigung des Domaininhabers, des Registrars oder einer in den WHOIS Daten angeführten Person.
4. Direkte Kommunikation mit dem Domaininhaber über eine generische E-Mail Adresse, beispielsweise admin@domainname oder webmaster@domainname. Dabei können Teile des Domainnamens weggelassen werden.
5. Der Antragsteller kann die Kontrolle über die Domain praktisch demonstrieren, insbesondere durch eine abgesproche Änderung einer Webseite
6. Eine andere passende und wohldokumentierte Methode, die selbe Sicherheit wie die obigen gewährleistet.

Bei EV Zertifikaten sind nur die Methoden 1-5 zulässig.

Muss vor der Eintragung in ein Zertifkat eine IP-Adresse geprüft werden,

takes place using one of the following methods:

1. The applicant can practically demonstrate control over the ip address, in particular using a pre-agreed change to the website.

2. Verification of information by international or regional registration services for IP addresses (such as IANA or RIPE).

3. The domain name whose IP address is investigated using reverse lookup has been verified in compliance with the conditions of this policy.
4. Another appropriate and well-documented method that ensures the same security as the methods above.

The CA explicitly reserves the right to conduct additional checks, which can be particularly necessary if

- information from the information source is insufficient,
- doubts arise as to the right to use particular number or name elements (such as the right to use a particular domain name)

- the authority to represent the organisation has not been sufficiently outlined or documented,
- in the event of other discrepancies or ambiguities in the certification application,
- a certification application is viewed as a high-risk enterprise (in particular if the domain for which a server certificate is to be issued is the known target of phishing attacks)
- previous applications have been rejected or revoked due to evidence of deceit and are connected to the current application.

The approach in such cases is documented internally.

If a domain name is entered with a wildcard, this must checked in its entirety using the domain name covered by the wildcard as described

so passiert dies mit einer der folgenden Methoden:

1. Der Antragsteller kann die Kontrolle über die IP-Adresse praktisch demonstrieren, insbesondere durch eine abgesproche Änderung einer Webseite.
2. Durch Prüfung von Informationen von internationalen oder regionalen Registrierungs-Agenturen für IP-Adressen (etwa IANA oder RIPE).
3. Der Domainname, der von der IP-Adresse mittels reverse lookup ermittelt wurde, wurde entsprechend den Bestimmungen dieser Policy geprüft.
4. Eine andere passende und wohldokumentierte Methode, die selbe Sicherheit wie die obigen gewährleistet.

Zusätzliche Prüfungen werden ausdrücklich vorbehalten und können insbesondere erforderlich sein, wenn

- die Auskünfte der zuständigen Auskunftsstellen ungenügend sind,
- Zweifel an der Verfügungsberechtigung über bestimmte Nummern- oder Namenselemente bestehen (etwa Verfügungsberechtigung über einen bestimmten Domainnamen),
- die Vertretungsbefugnis nicht ausreichend umschrieben bzw. dokumentiert ist,
- bei sonstigen Widersprüchen oder Unklarheiten im Zertifizierungsantrag,
- ein Zertifikatsantrag als Hochrisikofall betrachtet wird (insbesondere wenn die Domain für die ein Serverzertifikat ausgestellt werden soll ein bekanntes Ziel von Phishingangriffen darstellt)
- es in der Vergangenheit Antragsablehnungen oder Widerrufe gab, die auf Hinweise auf betrügerische Handlungen zurückzuführen waren und die mit dem bestehenden Antrag in Zusammenhang stehen.

Die Vorgangsweisen in diesen Fällen sind intern dokumentiert.

Soll ein Domainname mit einer Wildcard eingetragen werden, so muss jedenfalls der gesamte durch diese Wildcard abgedeckte Domainbereich

above. The use of wild cards for EV certificates is not permitted.

Additional verification steps for EV certificate applications

In addition to the general verification steps for applications, additional verification steps for EV certificate applications are summarised in this section.

EV certificates are only issued for domain names that are composed out of characters from the latin alphabet and delineating punctuation (hyphen).

Applications for EV certificates must be made, checked, authorised and a legally binding contract must be confirmed by one or more sufficiently authorised person(s) designated by the applicant organisation. The signatures on the certificate application and the subscriber agreement are checked for sufficient plausibility and that they come from the correct persons. The name, title, relationship to the organisation making the application and the relevant authorisation to represent the organisation of the persons involved is verified.

In addition, the following applies:

- EV certificates are only issued to private, public or international organisations (⇨ 3.2.5 Validation of authority / Nachweis der Vertretungsbefugnis, p25)
- EV certificates are not issued to organisations which the CA is prohibited by local law from having a business relationship with, whether this is directly or indirectly due to the organisation's country of origin.
- For a private organisation, the information source stated is consulted (⇨ 3.2.5 Validation of authority / Nachweis der Vertretungsbefugnis, p25) to establish that the registration of the applicant organisation has not expired and is neither invalid nor out-of-date.

wie oben beschrieben geprüft werden. Der Einsatz von Wildcards bei EV-Zertifikaten ist nicht zulässig.

Ergänzende Prüfschritte bei Antrag eines EV-Zertifikates

Ergänzend zu den allgemeinen Prüfschritten bei Antragstellung werden in diesem Abschnitt die ergänzenden Prüfschritte bei der Antragstellung eines EV-Zertifikates zusammen gefasst.

EV Zertifikate werden nur für Domainnamen die sich ausschließlich aus Zeichen des lateinischen Alphabets und gebräuchlichen Trennzeichen (Bindestrich) zusammensetzen ausgestellt.

Anträge für EV Zertifikate müssen von einer oder mehreren hinreichend autorisierten Person(en) die von der antragstellenden Organisation namhaft gemacht werden, geprüft, genehmigt und der Vertrag rechtlich bindend bestätigt werden. Die Unterschriften des Zertifikatsantrages und des Subscriber Agreements werden so geprüft, dass es hinreichend plausibel ist, dass sie von den richtigen Personen stammen. Von den beteiligten Personen wird jedenfalls Name, Titel, Verhältnis zur antragstellenden Organisation und die entsprechende Vertretungsvollmacht geprüft.

Außerdem gilt:

- EV Zertifikate werden nur an private, öffentliche oder internationale Organisationen (⇨ 3.2.5 Validation of authority / Nachweis der Vertretungsbefugnis, p25) ausgestellt
- Es werden keine EV Zertifikate an Organisationen ausgestellt, mit denen dem VDA aufgrund von lokalen gesetzlichen Bestimmungen Handelsbeziehungen untersagt sind, sei es unmittelbar oder mittelbar aufgund des Herkunftslandes der Organisation
- Bei einer privaten Organisation wird bei der angegebenen Auskunftsstelle (⇨ 3.2.5 Validation of authority / Nachweis der Vertretungsbefugnis, p25) überprüft, ob die Registrierung der antragstellenden Organisation nicht als abgelaufen, ungültig oder

- For private organisations, it is checked as to whether actual, physical representation exists.
- For international organisations established by a treaty, accord or convention between several sovereign states, their existence is verified using either their constitutional documents or confirmation from a signatory state or by checking the list published on the CA/Browser Forum, particularly at http://www.cabforum.org.

- For private organisations, the formal existence and identity, any pseudonyms, official name and registration, the name of a person authorised to represent the organisation and where necessary, relationships with mother, daughter and sister companies.
- For legally established and international organisations, the formal existence, the name and registration number (if available). It is verified as to whether the address given is the actual business address of the applicant organisation or a mother/daughter company (and not just a postbox). The telephone number of the business address is verified. Sources for the telephone number are information from the telephone operator or an appropriate information source ('qualified independent information source, QIIS or a 'qualified governmental information source', QGIS), or a verified 'legal opinion' or the 'confirmation of an auditor'.

Verification is considered successful if:

1. the information source used to verify the existence of the organisation is a 'qualified governmental information source' (QGIS) and the

veraltet gekennzeichnet ist

- Bei privaten Organisationen wird geprüft, ob eine tatsächliche physische Representanz besteht
- Bei internationalen Organisationen, die aufgrund eines Vertrages, Abkommen oder einer Konvention zwischen mehreren souveränen Staaten eingerichtet wurden, wird die Existenz entweder über das konstituierende Dokument oder durch die Bestätigung einer Behörde eines Signatarstaates oder durch Kontrolle der vom CA/Browser Forum insbesondere auf -http://www.cabforum.org veröffentlichten Liste geprüft.
- Bei privaten Organisationen die formelle Existenz und Identität, etwaige Pseudonyme, offizieller Name und Registrierung, Name einer vertretungsbevollmächtigten Person und falls notwendig, Relationen zu Mutter-, Tochter- oder Schwesterunternehmen.
  Bei gesetzlich eingerichteten und internationalen Organisationen die formelle Existenz, der Name und die Registrierungsnummer (falls vorhanden).
  Es wird geprüft, ob es sich bei der angegebenen Adresse um einen tatsächlichen Geschäftsstandort (und nicht nur einen Briefkasten) der antragstellenden Organisation oder eines Mutter-/Tochterunternehmens handelt.
  Die Telefonnummer des Geschäftsstandortes wird geprüft. Dazu wird jedenfalls die Nummer durch einen Anruf verifiziert. Als Quelle der Telefonnummer wird entweder auf die Auskunft des Telefonbetreibers oder einer passenden Auskunftstelle ('qualifizierte unabhängige Informationsquelle', QIIS oder eine 'qualifizierte behördliche Infromationsquelle', QGIS) oder ein geprüftes 'Rechtgutachten' oder die 'Bestätigung eines Wirtschaftsprüfers' vertraut.

Die Prüfung gilt als erfolgreich wenn:

1. die Auskunftsstelle, die zur Prüfung der Existenz der Organisation herangezogen wurde, eine 'qualifizierte behördliche

address given in the application corresponds or

2. a verified 'legal opinion' or a 'confirmation of an auditor' is received or

3. it is performed on-site by an authorised person.

If the business address is not in the same state as the place of registration, only point 2 listed above is permitted.

If the verified registration of the organisation is younger than three years old, the operative existence of the organisation is verified. This draws upon either information from the banking institution of the organisation that an active bank account exists, a verified 'legal opinion' or the confirmation of an auditor.

Before an EV certificate is issued, all necessary information is verified by an authorised person who has not collected the information. Any discrepancies, as well as erroneous or missing information, are documented and remedied before the document is issued. If this is not possible within an acceptable timeframe, the certification application is rejected. If documents do not exist in the working language of the operator, verification is carried out by a person with the necessary language qualifications or using the services of a translator.

Informationsquelle' (QGIS) ist und die dort angegebene Adresse der des Antrages entspricht oder

2. ein geprüftes 'Rechtsgutachten' oder eine geprüfte 'Bestätigung eines Wirtschaftsprüfers' vorliegt oder
3. durch Vorort-Prüfung einer autorisierten Person.

Sofern sich der Geschäftsstandort nicht im selben Staat wie der Ort der Registrierung befindet ist nur der oben angebene Punkt 2. zulässig.

Sofern die geprüfte Registrierung der Organisation jünger als drei Jahre ist, wird die operative Existenz der Organisation geprüft. Dazu wird entweder auf eine Auskunft des Bankinstitutes der Organisation über das Vorhandensein eines aktiven Kontos zurückgegriffen, auf ein geprüftes 'Rechtsgutachten' oder Bestätigung eines Wirtschaftsprüfers.

Sämtliche für die Ausstellung eines EV-Zertifikates notwendigen Informationen werden vor dessen Ausstellung von einer autorisierten Person geprüft, die nicht deren Sammlung durchgeführt hat. Etwaige Diskrepanzen sowie fehlerhafte oder fehlende Informationen werden vor der Ausstellung des Zertifikates dokumentiert und behoben, sofern dies nicht in einem akzeptablen Zeitrahmen möglich ist, wird der Zertifizierungsantrag abgelehnt. Sofern Unterlagen nicht in der Arbeitssprache des Betreibers vorliegen, erfolgt die Prüfung durch eine Person mit den notwendigen sprachlichen Qualifikationen oder es wird auf die Dienste eines Übersetzers zurückgegriffen.

4.2.1 Performing identification and authentication functions / Durchführung Identifikation und Authentifikation

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.3 Certificate issuance / Zertifikatsausstellung

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.4 Certificate acceptance / Zertifikatsannahme

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.4.1 Conduct constituting certificate acceptance / Verfahren zur Zertifikatsannahme

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.5 Key pair and certificate usage / Schlüsselpaar und Zertifikatsnutzung

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.6 Certificate renewal / Neuaustellung Zertifikat

Renewal is not permitted for qualified certificates. | Im Fall von qualifizierten Zertifikaten ist die Neuausstellung nicht

zulässig.

4.6.1 Circumstance for certificate renewal / Umstände für Neuaustellung eines Zertifikats

As per GLOBALTRUST® Certificate Policy

Renewal without creating a new key pair is not permitted for qualified certificates.

Gemäß GLOBALTRUST® Certificate Policy

Im Fall von qualifizierten Zertifikaten ist die Neuausstellung ohne Erzeugung eines neuen Schlüsselpaares nicht zulässig.

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

In addition to the CPS 4.2 criteria for the renewal of EV certificates, the following applies:

For the renewal of an EV certificate, verified data can only be carried over without further verification if it is not older than 13 months old. Each EV certificate issued must be associated with its own application and signature to the subscriber conditions (as per [CABROWSER-EV] 11.13.1 (4), conforms to confirmation of receipt for certificates for advanced signature).

If the applicant already possesses a current, valid EV certificate, the following information can be used again without further verification:

- address of the applicant
- telephone number of the applicant (if it has been called again to verify that it is still current)
- the operative existence of the applicant
- name, title and authenticity of the acting persons, if there is no separate agreement between the applicant and the operator that

Bei der Neuausstellung von EV Zertifikaten gilt zusätzlich zu den in CPS 4.2 Kriterien das folgende:

Für die Neuausstellung eines EV Zertifikates können die geprüften Daten nur dann ohne neuerliche Prüfung übernommen werden, falls sie nicht älter als 13 Monate sind. Es muss auf jeden Fall jedes ausgestellte EV Zertifikat mit einem eigenen Antrag und einer eigenen Unterschrift der Signaturbedingungen versehen sein (gemäß [CABROWSER-EV] 11.13.1 (4), entspricht Übernahmebestätigung bei Zertifikaten zur fortgeschrittenen Signatur).

Sofern der Antragsteller bereits ein aktuelles und gültiges EV Zertifikat besitzt, dürfen folgende Informationen in jedem Fall ohne neuerliche Prüfung wieder verwendet werden:

- Adresse des Antragstellers
- Telefonnummer des Antragstellers (sofern deren Aktualität durch einen neuerlichen Anruf verifiziert wurde)
- die operative Existenz des Antragstellers
- Name, Titel und Autentizität der handelnden Personen, sofern kein gesonderter Vertrag zwischen dem Antragsteller und dem Betreiber

provides for a different provision.
- email address used by the operator for confirmations from the applicant.
- the right to use a domain name, if this has been previously established using a verified legal opinion or the confirmation of an auditor and the owner of the domain has not changed (according to its WHOIS entry) or the applicant can demonstrate control over the domain name anew.

besteht, der eine andere Regelung vorsieht.
- E-Mail Adresse die vom Betreiber für Bestätigungen vom Antragsteller verwendet wird.
- Das Recht einen Domainnamen zu benützen, sofern dieses in der Vergangenheit durch ein geprüftes Rechtsgutachten oder die Bestätigung eines Wirtschaftsprüfers festgestellt wurde und sich seit damals der Inhaber der Domain (laut WHOIS Eintrag) nicht geändert hat oder der Antragsteller die Verfügungsgewalt neuerlich demonstrieren kann.

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.8 Certificate modification / Zertifikatsänderung

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.8.1 Circumstances for certificate modification / Umstände für Zertifikatsänderung

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.8.3 Processing certificate modification requests / Bearbeitung eines Antrags auf Zertifikatsänderung

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.9 Certificate revocation and suspension / Zertifikatswiderruf und -sperre

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.9.1 Circumstances for revocation / Umstände für Zertifikatswiderruf

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.9.2 Who can request revocation / Berechtigte für Antrag auf Widerruf

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.9.3 Procedure for revocation request / Stellung eines Widerrufantrages

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.9.4 Revocation request grace period / Informationsfrist für Antragstellung auf Widerruf

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

The revocation services are performed according to the following standards in particular: as a signed CRL list as per [RFC5280], created using software that fulfils the requirements of [RFC3279] or as an OCSP service as per [RFC2560].

For server and EV certificates, revocation status information is distributed using a OCSP responder.

Suspension and revocation lists contain the date of revocation or suspension, the latest time that the next list will be published, as well as the signature by the relevant CA certificate or by a certificate referenced by the CA certificate.

Suspension and revocation information that contains an entry with the OID 1.2.40.0.36.4.5.1.0 or 1.2.40.0.24.4.5.1.0 has been created for testing purposes and is not authentic. Typical reasons for testing are, in

Die Widerrufsdienste werden insbesondere nach folgenden Standards erbracht: als signierte CRL-Liste gemäß [RFC5280], wobei zur Erstellung Software verwendet wird, die die Vorgaben von [RFC3279] erfüllt oder als OCSP-Dienst nach [RFC2560].

Für Server- und EV-Zertifikate werden die Widerrufsstatusinformationen jedenfall mittels eines OCSP Responders verbreitet.

Jedenfalls in Sperr- bzw. Widerufsliste enthalten sind Datum von Widerruf bzw. Sperre, ein Zeitpunkt für die späteste Veröffentlichung einer Nachfolgeliste sowie eine Signatur vom jeweiligen CA-Zertifikat oder eines davon bestimmten Zertifikates.

Sperr- und Widerrufsinformationen die einen Eintrag mit der OID-Nummer 1.2.40.0.36.4.5.1.0 oder 1.2.40.0.24.4.5.1.0 enthalten, wurden zu Testzwecken erstellt und sind nicht authentisch. Typische

particular, testing of new developments (software tests) and tests of functionality of suspension and revocation lists. The use of suspension and revocation for testing purposes is limited to certificates that have been issued for testing purposes and certificates that concern test CAs.

Testzwecke sind insbesondere Tests von Neuentwicklungen (Softwaretests), Tests zur Funktionsfähigkeit der Sperr- und Widerrufsdienste. Die Verwendung von Sperren und Widerrufen zu Testzwecken ist auf Zertifikate beschränkt, die zu Testzwecken ausgestellt wurden bzw. Zertifikate die Test-CAs betreffen.

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

4.9.11 Other forms of revocation advertisements available / Andere verfügbare Widerrufsdienste

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

4.9.13 Circumstances for suspension / Umstände für Zertifikatssperre

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

4.9.14 Who can request suspension / Berechtigte für Antrag auf Sperre

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

4.9.15 Procedure for suspension request / Stellung eines Antrages auf Sperre

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

4.9.16 Limits on suspension period / Dauer einer Zertifikatssperre

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

4.10 Certificate status services / Zertifikatsstatusdienste

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.10.1 Operational characteristics / Betriebliche Voraussetzungen

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.10.2 Service availability / Verfügbarkeit

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.10.3 Optional features / Zusätzliche Funktionen

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.11 End of subscription / Vertragsende

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

4.12 Key escrow and recovery / Schlüsselhinterlegung und -wiederherstellung

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

All security measures and security-relevant functions for the provision of certification services are documented internally and implemented and maintained in compliance with the documentation.

For the management of operations, security levels have been introduced for all levels. These levels lead to different operational security measures and are detailed in the section 9.3 Confidentiality of business information / Vertraulichkeit von Geschäftsdaten in the GLOBALTRUST® Certificate Policy.

Detailed processes, in particular, requirements for installing the certification system, administering certification services and using certification systems and services, are documented internally and continually adjusted to operational requirements.

Requirements that cannot be technically installed as a business process are supported by a system of checklists.

A reboot of the certification system (in particular the HSM module) is only possible at the site of installation of the HSM module. This requires possession (token) as well as knowledge (initialisation password). The necessary steps for a reboot of the certification system are documented internally.

1. Damages caused by security-critical incidents and malfunctions are recognised early, prevented or at least minimised using sufficient recording and recovery procedures.

2. Data carriers are protected from damage, theft and unauthorised access.

Alle Sicherheitsmaßnahmen und sicherheitsrelevanten Funktionen zur Bereitstellung der Zertifizierungsdienste werden dokumentiert und entsprechend der Dokumentation implementiert und gewartet.

Zur Steuerung des Betriebs wurden für alle Informationen Sicherheitsstufen eingeführt, die zu entsprechend unterschiedlichen betrieblichen Sicherheitsmaßnahmen führen und im GLOBALTRUST® Certificate Policy Abschnitt 9.3 Confidentiality of business information / Vertraulichkeit von Geschäftsdaten detailliert dargestellt sind.

Detailprozesse, insbesondere die Anforderungen zur Installation des Zertifizierungssystems, der Verwaltung der Zertifizierungsdienste und der Verwendung der Zertifizierungssysteme und -dienste werden intern dokumentiert und laufend an betriebliche Anforderungen angepasst.

Anforderungen, die nicht als Geschäftsprozesse technisch installiert werden können, werden durch ein System von Checklisten unterstützt.

Ein Neustart des Zertifizierungssystems (insbesondere der HSM-Module) ist nur am Ort der Installation des HSM-Moduls möglich. Er erfordert sowohl Besitz (Token), als auch Wissen (Initialisierungspasswort). Die erforderlichen Schritte für einen Neustart des Zertifizierungssystems sind intern dokumentiert.

1. Schäden durch sicherheitskritische Zwischenfälle und Fehlfunktionen werden durch ausreichende Aufzeichnungen und Fehlerbehebungsprozeduren frühzeitig erkannt, verhindert oder zumindest minimiert.
2. Datenträger werden vor Beschädigung, Diebstahl und unautorisiertem Zugriff geschützt.

3. Detailed processes are used for the implementation of security-critical and administrative functions that affect the performance of certification services.
4. Data carriers are treated according to their security level and are stored securely. Data carriers that are no longer needed and that contain confidential data are destroyed using secure methods.

The monitoring of security-critical functions is the responsibility of authorised persons as per the internally documented role concept of the CA or persons designated responsible by a contractor.

3. Für die Ausführung von sicherheitskritischen und administrativen Aufgaben, die sich auf die Erbringung der Zertifizierungsdienste auswirken, sind detaillierte Prozesse in Verwendung.
4. Datenträger werden je nach ihrer Sicherheitsstufe behandelt und gesichert aufbewahrt. Nicht mehr benötigte Datenträger, die vertrauliche Daten beinhalten, werden in sicherer Weise vernichtet.

Die Überwachung der sicherheitskritischen Funktionen obliegt autorisierten Personen gemäß intern dokumentiertem Rollenkonzept des VDAs oder vom verantwortlichen Dienstleister nominierten Sicherheitsbeauftragten.

Security objectives and guidelines / Sicherheitsziele und -leitlinien

1 Setting and implementation of objectives / Zielsetzung und Umsetzung

The security guidelines detailed in this section serve to fulfil the legal and technical requirements for the operator's performance of certification services.

Die in diesem Abschnitt beschriebene Sicherheitsleitlinie dient zur Erfüllung der rechtlichen und technischen Auflagen bei der Erbringung von Zertifizierungsdiensten durch den Betreiber.

The documents and processes necessary for the operation of certification services are made demonstrably available to the employees responsible. Responsibilities ensue as per the internal role concept and role assignment. The certification committee is composed of all employees responsible for certification operations.

Die zum Betrieb der Zertifizierungsdienste erforderlichen Dokumente und Prozesse werden nachweislich den zuständigen Mitarbeitern zur Kenntnis gebracht. Die Zuständigkeit ergibt sich gemäß internen Rollenkonzept und Rollenzuteilung. Die Gesamtheit der für den Zertifizierungsbetrieb verantwortlichen Mitglieder bilden den Zertifizierungs-Ausschuss.

2 Identification of risks / Identifikation von Risken

All activities and incidents are designated as risks that lead to interruptions in operation, interruption in the availability of critical services or the impairment of confidentiality or integrity of data and applications.

Als Risken werden alle Vorgänge und Vorfälle bezeichnet, die zu Unterbrechungen des Betriebs, zur Unterbrechung der Verfügbarkeit kritischer Dienste, oder zu Schädigungen der Vertraulichkeit oder der Integrität von Daten und Anwendungen führen.

This particularly includes all incidents for which the operator is liable according to legal provisions.

Insbesondere davon erfasst sind alle Vorfälle für die der Betreiber gemäß rechtlicher Bestimmungen haftet.

Employees are required to document and immediately report deviations and disruptions in operation or potential security problems to the persons responsible, independent of their own formal responsibilities. In the event

Mitarbeiter sind angehalten Abweichungen und Störungen des Betriebs oder potentielle Sicherheitsprobleme, unabhängig von ihrer formalen Zuständigkeit zu dokumentieren und unverzüglich den zuständigen

that responsibilities are unclear, the certification committee and management must be informed.

Stellen (Personen) zu melden. Im Falle unklarer Zuständigkeiten ist der Zertifizierungs-Ausschuss oder die Geschäftsführung zu informieren.

3 Principle of minimality / Prinzip der Minimalität

On principle, all business processes are designed with a view to minimising risks. As few components (hardware and software) and people as possible should be involved.

Grundsätzlich werden alle Geschäftsprozesse in Hinblick auf Minimierung von Risken entworfen. Es sollen so wenig Komponenten (Hardware und Software) und Personen als möglich involviert sein.

Furthermore, all business processes are continually optimised so that the effects of impairments and damage remain as localised as possible.

Weiters werden die Geschäftsprozesse laufend dahingehend optimiert, dass bei Beeinträchtigungen und Schäden die Auswirkungen möglichst lokal begrenzt bleiben.

4 Principle of authentication and identification / Prinzip der Authentifikation und Identifikation

On principle, all business processes are organised so that it is clear which person is involved in the business process.

Grundsätzlich werden alle Geschäftsprozesse so gestaltet, dass feststellbar ist, welche Personen am Geschäftsprozess beteiligt sind.

In the course of business processes, authorised persons must authenticate themselves. If individual processes concern the certification system directly, repeated failed authentication attempts lead to suspension and if this involves the authentication of the system administrator, this leads to the supervisor responsible being informed.

Im Zuge der Abwicklung der Geschäftsprozesse müssen sich berechtigte Personen authentifizieren. Soweit einzelne Maßnahmen direkt das Zertifizierungssystem betreffen, führen mehrfach fehlerhafte Authentifikationen zu einer Sperre bzw. falls es sich um eine Authentifikation als Systemadministrator handelt zu einer Information zuständiger Aufsichtspersonen.

The number of failed attempts permitted and the rules for informing and notifying are separately stated for each businesss process and take the quality of the identification mechanisms used into account (passwords, keys, tokens, smartcards). On principle, identification mechanisms and the number of failed attempts permitted are chosen so that the probability of erroneous identification is neglibly low (less than 1:1000).

Die Zahl der zulässigen Fehlversuche und die Informations- und Benachrichtigungsregeln werden für die Geschäftsprozesse gesondert festgelegt und berücksichtigen die Qualität der verwendeten Identifikationsmechanismen (Passwörter, Schlüssel, Tokens, Smartcard). Grundsätzlich sind Identifikationsmechanismen und zulässige Zahl der Fehlversuche so zu wählen, dass die Wahrscheinlichkeit von fehlerhaften Identifikationen vernachlässigbar gering ist (weniger als 1:1000).

In individual cases, identification and authentication can be carried out using a specific system component or generally on the basis of the system that this is based on.

Die Identifizierung und Authentifizierung kann im Einzelfall durch eine spezifische Systemkomponente erfolgen oder generell auf Basis des darunter liegenden Systems.

The certification system supports the identification and authentication of two persons ("dual person control") for certification services that require the four-eyes principle as per the applicable Certificate Policy.

Das Zertifizierungssystem unterstützt die Identifizierung und Authentifizierung von zwei Personen ("dual person-control") für Zertifizierungsdienstleistungen die gemäß anzuwendender Certificate

Policy das Vier-Augen-Prinzip erfordern.

5 Principle of confidentiality / Prinzip der Vertraulichkeit

All critical information, processes and systems are subject to limitations on access. These are ensured using physical barriers to entering the system, general access restrictions and individual access profiles.

Alle kritischen Informationen, Prozesse und Systeme unterliegen einer Zugangsbeschränkung. Diese wird durch physikalische Zutrittsbeschränkungen zu den Systemen, durch generelle Zugriffsbeschränkungen bzw. individuelle Zugriffsprofile sichergestellt.

For central certification services, access is restricted using a combination of the measures named.

Im Falle der zentralen Zertifizierungsdienste erfolgt die Beschränkung durch eine Kombination der genannten Maßnahmen.

The personal information of an applicant or a third party is treated confidentially unless the purpose of the certification service explicitly provides otherwise. Certificates (as well as their contents) are not subject to confidentiality if they are released for publication. Information on the revocation time and identification data of revoked certificates is not subject to confidentiality.

Persönliche Informationen der Antragsteller oder Dritter werden vertraulich behandelt, es sei denn der Zweck eines Zertifizierungsdienstes sieht ausdrücklich etwas anderes vor. Keine vertraulichen Informationen sind zur Veröffentlichung freigegebene Zertifikate und deren Inhalte. Keiner Vertraulichkeit unterliegen Angaben über den Zeitpunkt und Identifikationsdaten widerrufener Zertifikate.

6 Principle of up-to-dateness / Prinzip der Aktualität

Critical parts of the business processes are continually verified for their up-to-dateness and appropriateness, taking the state of the art into account.

Kritische Teile der Geschäftsprozesse werden laufend auf ihre Aktualität und Angemessenheit in Hinblick auf den Stand der Technik geprüft.

Messages from the regulatory authority, messages from the producer, national and international CERT information, feedback from customers and industry publications are also taken into account. Each business process is regularly and systematically investigated and optimised with regard to previously unrecognised risks and weaknesses. The frequency of checks is based on operational necessities and the potential risks of each business process and lies in a timeframe of between 12 and 18 months.

Dazu werden Mitteilungen der Aufsichtstelle, Mitteilungen der Hersteller, nationale und internationale CERT-Informationen, Rückmeldungen von Kunden und Fachpublikationen herangezogen. Regelmäßig wird jeder Geschäftsprozess systematisch in Hinblick auf bisher nicht erkannte Risken und Schwachstellen untersucht und optimiert. Die Prüffrequenz richtet sich nach den betrieblichen Erfordernissen und den potentiellen Risken jedes Geschäftsprozesses und liegt in einem Zeitraum von 12 bis 18 Monaten.

7 Principle of redundancy and fail-safe (emergency guidelines) / Prinzip von Redundanz und Fail-Safe (Notfallleitlinie)

Critical business processes, systems and activities are conducted with redundancy. In addition, the design of processes is arranged so that in the event of disruptions that are not reparable in the context of documented processes, escalation strategies can be used that can eventually lead to shutdown of services provided.

Kritische Geschäftsprozesse, Systeme und Tätigkeiten sind redundant ausgeführt. Das Design der Prozesse ist zusätzlich so ausgelegt, dass bei Störungen, die nicht im Rahmen dokumentierter Verfahren behebbar sind, Eskalationsstrategien verwendet werden, die am Ende auch zur Abschaltung angebotener Dienste führen können.

In the event of the failure of individual components with redundancy, this can lead to reduced availability. In some circumstances, queries and requests must be made repeatedly to be successful, depending on the client software used (eg. browser, reader, signature verification programs).

Bei Ausfall einzelner, redundant ausgeführter Komponenten kann es zur verminderten Verfügbarkeit kommen. Anfragen bzw. Anforderungen an diese Dienste müssen, abhängig von der eingesetzen Clientsoftware (z.B. Browser, Reader, Signaturprüfprogramme), um erfolgreich zu sein, unter Umständen mehrfach erfolgen.

All employees of the certification committee are involved in implementing escalation strategies.

Bei der Umsetzung der Eskalationsstrategien sind alle Mitglieder des Zertifizierungs-Ausschusses eingebunden.

8 Maintenance agreement / Wartungsvereinbarung

Maintenance agreements exist for critical components, which allow replacement of faulty components within a timeframe shorter than the customary average outage time probability of the component. Critical components are those components that cannot be quickly acquired from general retail due to their construction and/or complexity.

Zu kritischen Komponenten existieren Wartungsvereinbarungen, die einen Ersatz schadhafter Komponenten innerhalb eines Zeitraums erlauben, der kürzer ist als die übliche durchschnittliche Ausfallszeitwahrscheinlichkeit einer Komponente. Kritische Komponenten sind jene Komponenten, die auf Grund ihrer Bauart und/oder Komplexität nicht kurzfristig im allgemeinen Handel beschaft werden können.

With regard to assessable risks, the combination of redundancy and maintenance agreements ensures that at least one component is available for regular operations.

In der Kombination von Redundanz und Wartungsvereinbarung ist für abschätzbare Risken gesichert, dass zumindest eine Komponente für den regulären Betrieb zur Verfügung steht.

For non-critical components, organisational precautions are made for the continuance of operations in the event of outages.

Für nicht-kritische Komponenten wurden für Ausfälle organisatorische Vorkehrungen zur Aufrechterhaltung des Betriebs getroffen.

9 Principle of outsourcing / Prinzip der Auslagerung

Unavoidable residual risks that can neither be technically nor organisationally solved are prevented or at least reduced by being "outsourced".

Nicht vermeidbare Restrisken, die weder technisch noch organisatorisch gelöst werden können, werden durch "Auslagerung" verhindert oder zumindest reduziert.

The conclusion of indemnity insurance is considered first and foremost in this matter.

Furthermore, special on-call service times, special expertise or operational requirements are covered by relationships with suitable specialists. On principle, providers with relevant qualifications are preferred for these relationships. The list of suitable specialists and the agreements concluded with them is documented internally. Specialists who have actually been used are recorded internally.

Dazu zählt in erster Linie der Abschluss einer Haftpflichtversicherung.

Weiters werden besondere Bereitschaftszeiten, spezielle Fachkenntnisse oder Betriebserfordernisse durch Beiziehung geeigneter Spezialisten abgedeckt. Bei Beiziehung sind Anbieter mit einschlägigen Zertifizierungen, bei ansonsten gleichen Voraussetzungen, grundsätzlich zu bevorzugen. Die Liste geeigneter Spezialisten und mit ihnen abgeschlossene Vereinbarungen ist intern dokumentiert, die tatsächlich herangezogenen Spezialisten werden intern protokolliert.

10 Principle of risk acceptance / Prinzip der Risikoakzeptanz

The principles described in this guideline are detailed and assessed in the GLOBALTRUST® Certificate Security Policy for all services of the CA. The risk analysis uses the protection requirement categorisation, "normal", "high" und "very high" as per [BSI-GRUND]. All remaining residual risks in the "normal" protection requirement category after the measures detailed in GLOBALTRUST® Certificate Security Policy have been implemented are explicitly acknowledged and accepted by the management of the CA.

Die in dieser Leitline beschriebenen Prinzipien werden in der GLOBALTRUST® Certificate Security Policy für alle Dienste des VDA beschrieben und bewertet. Die Risikoanalyse verwendet in diesem Zusammenhang die Schutzbedarfskategorisierung "normal", "hoch" und "sehr hoch" gemäß [BSI-GRUND]. Alle nach Umsetzung der in der GLOBALTRUST® Certificate Security Policy beschriebenen Maßnahmen verbleibenden Restrisiken der Schutzbedarfskategorie "normal" werden ausdrücklich von der Geschäftsführung des VDA zur Kenntnis genommen und akzeptiert.

Risks that go beyond this and are, for example, categorised as "high" or "very high", are minimised using additional measures to the extent that the risk becomes acceptable. Measures for minimising risks are detailed in the GLOBALTRUST® Certificate Security Policy. Remaining residual risks are explicitly acknowledged and accepted by the management of the CA.

Risken die darüber hinaus gehen und etwa als "hoch" oder "sehr hoch" eingestuft werden, werden durch Zusatzmaßnahmen soweit minimiert, dass das Risiko akzeptabel ist. Die Maßnahmen zur Minimierung der Risken sind in der GLOBALTRUST® Certificate Security Policy beschrieben. Verbleibende Restrisken werden ausdrücklich von der Geschäftsführung des VDA zur Kenntnis genommen und akzeptiert.

5.1 Physical controls / Bauliche Sicherheitsmaßnahmen

In particular, the following security measures apply:

1. The systems for generating certificates and for revocation services are operated using technical and organisational measures in a secure

Insbesondere gelten folgende Sicherheitsmaßnahmen:

1. Die Systeme für die Zertifikatsgenerierung und die Widerrufsdienste werden durch technische und organisatorische Maßnahmen in einer

environment so that compromisation from unauthorised access is prevented.
2. Systems for generating certificates, for creating signature creation devices and for revocation services are separated using clearly defined security zones as well as physical barriers.

3. Security measures include building protection, the computer systems themselves and any other facilities essential for their operation. Protection of facilities for creating and making revocation services available includes physical entry controls, averting dangers from forces of nature, fire, burst pipes and building collapse, protection from failure of supply units as well as from theft, break-in and system failure.

4. The unauthorised retrieval of information, data carriers, software and fixtures that belong to the certification services is prevented using control measures.

Technical, physical and organisational security measures, such as system redundancy, an emergency generator and fire protection, are used against physical disruptions.

gesicherten Umgebung betrieben, sodass eine Kompromittierung durch unautorisierte Zugriffe verhindert wird.
2. Die Abgrenzung der Systeme für Zertifikatsgenerierung, Erstellung von Signaturerstellungseinheiten und Widerrufsdienste erfolgt durch klar definierte Sicherheitszonen sowie physischen ZutrittsschutzGLOBALTRUST® Certificate Security Policy.
3. Die Sicherheitsmaßnahmen beinhalten den Gebäudeschutz, die Computersysteme selbst und alle sonstigen Einrichtungen, die für deren Betrieb unerlässlich sind. Der Schutz der Einrichtungen für die Zertifikatserstellung und Bereitstellung der Widerrufsdienste umfasst physische Zutrittskontrolle, Abwendung von Gefahren durch Naturgewalten, Feuer, Rohrbrüche und Gebäudeeinstürze, Schutz vor Ausfall von Versorgungseinheiten sowie vor Diebstahl, Einbruch und Systemausfällen.
4. Die unautorisierte Entnahme von Informationen, Datenträgern, Software und Einrichtungsgegenständen, welche zu den Zertifizierungsdiensten gehören, wird durch Kontrollmaßnahmen verhindert.

Gegen physikalische Störungen bestehen technische, bauliche und organisatorische Sicherungsmaßnahmen wie redundante Systemführungen, Notstromaggregate, Brandschutz.

5.1.1 Site location and construction / Standortlage und Bauweise

All critical IT components for performing certification services, including for creating qualified certificates and qualified timestamps, are stored externally in a data centre with an ISO 27001 certification, an equivalent certification or an equivalent individual security concept compliant with the state of the art.

The current place of business and IT components deployed are documented internally. Individual security measures, in particular the

Alle kritischen IT-Komponenten für die Erbringung von Zertifizierungsdiensten, inklusive der Ausstellung qualifizierter Zertifikate und qualifizierter Zeitstempel, sind in einem Rechenzentrum ausgelagert, dass eine ISO 27001-Zertifizierung, eine gleichwertige Zertifizierung oder ein gleichwertiges individuelles Sicherheitskonzept, das dem Stand der Technik entspricht, vorweist.

Der aktuelle Standort und die eingesetzten IT-Komponenten sind intern dokumentiert, die einzelnen Sicherheitsmaßnahmen insbesondere der

protection of technical components from unauthorised changes are documented in the GLOBALTRUST® Certificate Security Policy.

Schutz der technischen Komponenten vor unbefugten Veränderungen im Dokument GLOBALTRUST® Certificate Security Policy.

5.1.2 Physical access / Zutritt

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

5.1.3 Power and air conditioning / Stromnetz und Klimaanlage

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

5.1.4 Water exposures / Gefährdungspotential durch Wasser

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

5.1.5 Fire prevention and protection / Brandschutz

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

5.1.6 Media storage / Aufbewahrung von Speichermedien

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

5.1.7 Waste disposal / Abfallentsorgung

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

5.1.8 Off-site backup / Offsite Backup

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

5.2 Procedural controls / Prozessanforderungen

5.2.1 Trusted roles / Rollenkonzept

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

5.2.2 Number of persons required per task / Mehraugenprinzip

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

5.2.4 Roles requiring separation of duties / Rollenausschlüsse

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

5.3 Personnel controls / Mitarbeiteranforderungen

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

5.3.2 Background check procedures / Durchführung von Backgroundchecks

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

5.3.3 Training requirements / Schulungen

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

5.3.4 Retraining frequency and requirements / Häufigkeit von Schulungen und Anforderungen

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

5.3.5 Job rotation frequency and sequence / Häufigkeit und Abfolge Arbeitsplatzrotation

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

5.3.6 Sanctions for unauthorized actions / Strafmaßnahmen für unerlaubte Handlungen

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

5.3.7 Independent contractor requirements / Anforderungen an Dienstleister

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

5.3.8 Documentation supplied to personnel / Zur Verfügung gestellte Unterlagen

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

5.4 Audit logging procedures / Betriebsüberwachung

Self-audits are carried out regularly to ensure quality. For EV and server certificates, at least 3% (at least one) of all certificates issued since the last self-audit are checked, as well as 6% of all EV certificates and 3% of all server certificates, for which identity verification and the final inspection were carried out by a contractor. Self-audits for server certificates are carried out at least once per quarter.

Zur Qualitätssicherung werden regelmäßig Selbst-Audits durchgeführt. Bei EV- und Server-Zertifikaten werden zumindest 3% (mindestens eines) aller seit dem letzten Selbst-Audit ausgestellten Zertifikate überprüft sowie 6% aller EV-Zertifkate und 3% aller Serverzertifikate, bei welchen die Identitäts- oder Endprüfung von einem Dienstleister durchgeführt wurde. Die Selbst-Audits für Server-Zertifikate erfolgen zumnidest einmal pro Quartal.

The CA is obliged to carry out one inspection per quarter of at least 3% (at least one) of all technically limited sub-certificates issued in the quarter whose private key is not under the sole control of the CA for compliance with all applicable conditions, in particular [CABROWSER-BASE].

Der VDA verpflichtet sich einmal im Quartal eine Prüfung von mindestens 3% (mindestens eines) aller der in diesem Quartal ausgestellter, technisch eingeschränkter Sub-Zertifikate, deren privater Schlüssel sich nicht unter der alleinigen Kontrolle des VDA befindet ausgestellten Zertifikaten auf Einhaltung aller anwendbarer Bestimmungen, insbesondere von [CABROWSER-BASE], durchzuführen.

Operation monitoring, on-call service and recording of exceptional operational situations

The regular operation of the certification system is subject to continual, automated monitoring of operations with several interfaces. Among other things, operational status can always be checked by authorised persons using web interfaces. For particular incidents, the persons responsible are notified with an automated message. Notification can take place by email, SMS or another appropriate signal or messaging service.

Betriebsüberwachung, Bereitschaftsdienst und Protokollierung besonderer Betriebssituationen

Der reguläre Betrieb des Zertifizierungssystems unterliegt einer laufenden, automationsunterstützten Betriebsüberwachung, die mehrere Interfaces aufweist. Unter anderem kann der Betriebszustand jederzeit über Web-Interfaces von befugten Personen kontrolliert werden. Bei bestimmten Ereignissen erfolgt eine automatisierte Benachrichtigung der verantwortlichen Stellen. Diese Benachrichtigung kann per eMail, SMS oder anderer geeigneter Signal- oder Nachrichtendienste erfolgen.

The monitoring system itself is operated so that the monitoring takes place at the relevant location, as far as is technically reasonable. The functionality of the corresponding local monitoring system is itself monitored using another, external monitoring system.

Das Überwachungsystem selbst ist so ausgeführt, dass die Überwachung - soweit technisch sinnvoll - direkt an den entsprechenden Standorten erfolgt, die Funktionsfähigkeit des jeweiligen lokalen Überwachungssystems selbst wird durch ein anderes, externes Überwachungssystem überwacht.

If the monitoring system is permanently not available, manual monitoring

Sofern ein Überwachungssystem dauerhaft nicht verfügbar ist, sind für

measures are envisaged for all critical processes. The type of measures is documented internally.	die kritischen Prozesse manuelle Überwachungsmaßnahmen vorgesehen. Die Art der Maßnahmen ist intern dokumentiert.

5.4.1 Types of events recorded / Zu erfassende Ereignisse

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

5.4.2 Frequency of processing log / Überwachungsfrequenz

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

5.4.3 Retention period for audit log / Aufbewahrungsfrist für Überwachungsaufzeichungen

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

5.4.4 Protection of audit log / Schutz der Überwachungsaufzeichnungen

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

5.4.5 Audit log backup procedures / Sicherung des Archives der Überwachungsaufzeichnungen

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

5.4.7 Notification to event-causing subject / Benachrichtigung des Auslösers

N/A	Nicht zutreffend

5.4.8 Vulnerability assessments / Gefährdungsanalyse

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

5.5 Records archival / Aufzeichnungsarchivierung

The certification application and all data and documents sent by the applicant in connection with the application (copies of personal identification, where applicable confirmations about the company and authorisation to represent), as well as all agreements and contracts concluded for the certificate, are archived in electronic or paper form for a duration of at least 35 years after expiration of validity, so that the original application, certificate issuance and certificate delivery can be reproduced.

Der Zertifizierungsantrag und alle damit im Zusammenhang stehenden vom Antragsteller zugesandten und vorliegenden Daten und Dokumente (Ausweiskopien, gegebenenfalls Bestätigungen über das Unternehmen und die Vertretungsbefugnis) sowie alle zum Zertifikat geschlossenen Vereinbarungen und Verträge werden auf die Dauer von mind. 35 Jahren nach Ablauf der Gültigkeit elektronisch oder in Papierform in dem Umfang archiviert, dass die ursprüngliche Antragstellung, Zertifikatsausstellung und Zertifikatszustellung nachvollzogen werden können.

5.5.1 Types of records archived / Zu archivierende Aufzeichungen

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

5.5.2 Retention period for archive / Aufbewahrungsfristen für archivierte Daten

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

5.5.3 Protection of archive / Schutz der Archive

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

5.5.4 Archive backup procedures / Sicherung des Archives

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

5.6 Key changeover / Schlüsselwechsel des Betreibers

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

5.7 Compromise and disaster recovery / Kompromittierung und Geschäftsweiterführung

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

5.8 CA or RA termination / Einstellung der Tätigkeit

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

6. TECHNICAL SECURITY CONTROLS / TECHNISCHE SICHERHEITSMAßNAHMEN

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

6.1.1 Key pair generation / Erzeugung von Schlüsselpaaren

Creation of private key and certificate for CA certificates

The creation of a private key for a certificate that has been issued after 9.7.2013 and is used to issue EV certificates is monitored by a competent independent auditor.

Creation of subscriber private key

If special hardware components used for the signature creation device prevent the private key from being read, this can be evaluated (certified) by a confirmation authority. Alternatively, suitability can be established by a self-declaration from the producer. The operator documents which criteria and standards a signature creation device fulfils. This is available on the website of the operator or upon request.

The use of this kind of signature creation device can be recorded in a certificate as an X.509v3 extension.

This can be entered in the following forms:

- provision of the key by the operator
- key generation at the offices of the subscriber

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

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

Erzeugung der privaten Schlüssel des Signators

Werden für die Signaturerstellungseinheit spezielle Hardwarekomponenten verwendet die das Auslesen des privaten Schlüssels verhindern, können diese von Bestätigungsstellen evaluiert (zertifiziert) sein. Alternativ kann die Eignung durch Selbstdeklaration des Herstellers gegeben sein. Welchen Kriterien und Standards eine Signaturerstellungseinheit genügt wird vom Betreiber dokumentiert und kann über dessen Website oder auf Anfrage abgerufen werden.

Die Verwendung derartiger Signaturerstellungseinheiten kann als X.509v3-Erweiterung im Zertifikat eingetragen werden.

Der Eintrag kann in folgender Form erfolgen:

- Bereitstellung des Schlüssels durch den Betreiber
- Schlüsselgenerierung beim Signator

- key generation by an authorised third party

a Provision of the key by the CA / Bereitstellung des Schlüssels durch den VDA

Option 1: Creation of the key in a secure signature creation device

The private key of the subscriber is generated by the CA in a special suitable signature creation device and is delivered only in this signature creation device. There is no copy of the private key outside of the signature creation device at the offices of the CA.

A X.509v3 certificate can contain the following extension:
1.2.40.0.36.4.1.1: <used hardware>

Under "<used Hardware>", the customary labelling or the labelling used by a confirmation authority is used to clearly label the hardware, for example, "Safenet eToken Pro64k" for a USB token with the evaluated component "CardOS V4.2 CNS with Application for Digital Signature" of the company, ATOS.

The current status of supported hardware components and which confirmation authorities used which legal conditions for evaluation can be found on the website of the CA.

If the certificate is published in the registry of the CA, the used hardware is recorded under the label, "globaltrustIssuerInfo", in the associated certificate record.

This option is possible for qualified and simple certificates.

Option II: Creation of the key for the subscriber in a secure certification environment

The subscriber's private key is created by the CA in a signature creation environment specially operation for this purpose and is encrypted with a password from the subscriber upon transfer.

This option is only possible for simple certificates.

- Schlüsselgenerierung durch befugte Dritte

Variante I: Erzeugen des Schlüssels in einer sicheren Signaturerstellungseinheit

Der private Schlüssel des Signators wird vom VDA in einer dafür speziell geeigneten Signaturerstellungseinheit generiert und nur in dieser Signaturerstellungeinheit ausgeliefert. Beim VDA existiert keine Kopie des privaten Schlüssels außerhalb der Signaturerstellungseinheit.

Ein X.509v3-Zertifikat kann folgenden Erweiterung enthalten:
1.2.40.0.36.4.1.1: <verwendete Hardware>

Unter "<verwendete Hardware>" wird die handelsübliche oder durch eine Bestätigungsstelle verwendete Bezeichnung zur eindeutigen Kennzeichnung der Hardware verwendet, z.B. "Safenet eToken Pro64k" für einen USB-Token mit der evaluierten Komponente "CardOS V4.2 CNS with Application for Digital Signature" der Firma ATOS.

Der aktuelle Stand der unterstützten Hardwarekomponenten und welche Bestätigungsstellen nach welchen gesetzlichen Bestimmungen die Evaluation durchführten, findet sich auf der Website des VDA.

Wird das Zertifikat im Verzeichnisdienst des VDA veröffentlicht wird in den Stammdaten zusätzlich die verwendete Hardware unter der Bezeichnung "globaltrustIssuerInfo" eingetragen.

Diese Variante ist für qualifizierte und einfache Zertifikate möglich.

Variante II: Erzeugen des Schlüssels für den Signator in einer gesicherten Zertifizierungsumgebung

Der private Schlüssel des Signators wird vom VDA in einer dafür speziell betrieben Signaturerstellungsumgebung erstellt und wird zur Übergabe mit einem vom Signator vergebenen Passwort verschlüsselt.

Diese Variante ist nur für einfache Zertifikate möglich.

b Key generation by the subscriber / Schlüsselgenerierung beim Signator

The subscriber states which hardware has been used to create the private key. If the certificate is published in the registry of the CA, the used hardware is recorded under the label, "globaltrustSignerInfo" in the associated certificate record. This option is only possible for simple certificates.	Der Signator gibt an, mit welcher Hardware er den privaten Schlüssel generiert hat. Wird das Zertifikat im Verzeichnisdienst des VDAs veröffentlicht wird in den Stammdaten zusätzlich die verwendete Hardware unter der Bezeichnung "globaltrustSignerInfo" eingetragen. Diese Variante ist nur für einfache Zertifikate möglich.

c Key generation by an authorised third party / Schlüsselgenerierung durch befugte Dritte

Conditions such as ⇨ aProvision of the key by the CA / Bereitstellung des Schlüssels durch den VDA (p61). Keys are generated by a sufficiently authorised third party, eg. civil engineers who confirm the correct generation of a private key. This option is possible for qualified and simple certificates.	Bedingungen wie ⇨ a Provision of the key by the CA / Bereitstellung des Schlüssels durch den VDA (p61), die Schlüsselgenerierung erfolgt jedoch durch ausreichend befugte Dritte, z.B. Ziviltechniker, die die ordnungsgemäße Generierung des privaten Schlüssels bestätigen. Diese Variante ist für qualifizierte und einfache Zertifikate möglich.

d Completion / Abschluss

If both X509v3 extensions are missing and the certificate does not contain an entry as a qualified certificate, the storage conditions for private keys as per the section, "Additional conditions in deployment of readable data carriers for private keys" in the ⇨ GLOBALTRUST® Certificate Policy apply.	Fehlen beide X509v3-Erweiterungen und enthält das Zertifikat keinen Eintrag als qualifiziertes Zertifikat, dann gelten jedenfalls die Aufbewahrungsbestimmungen für den privaten Schlüssel gemäß ⇨ GLOBALTRUST® Certificate Policy Abschnitt "Ergänzende Bestimmungen bei Einsatz auslesbarer Datenträger für private Schlüssel".

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

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

6.1.5 Key sizes / Schlüssellängen

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

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

Keys for qualified certificates are only issued on secure signature creation devices.

Schlüssel für qualifizierte Zertifikate werden nur auf sicheren Signaturerstellungseinheiten ausgestellt.

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

For keys intended for advanced signatures, this will be all products that have a certification as per [CC-ITSE] EAL4+ or [FIPS-140-2] L1.

Für Schlüssel, die für fortgeschrittene Signaturen vorgesehen sind werden alle Produkte, die zumindest eine Zertifizierung gemäß [CC-ITSE] EAL4+ oder gemäß [FIPS-140-2] L1 aufweisen.

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

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

6.2.4 Private key backup / Backup privater Schlüssel

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

6.2.5 Private key archival / Archivierung privater Schlüssel

If created by the operator and copies are available, the subscriber's private keys are deleted by the operator after the subscriber has retrieved them and confirmed correct receipt.	Die privaten Schlüssel des Signators werden, sofern sie vom Betreiber erstellt wurden und Kopien vorhanden sind, nach Abruf durch den Signator und der Bestätigung des korrekten Empfangs durch den Signator, beim Betreiber gelöscht.

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

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

6.2.8 Method of activating private key / Aktivierung privater Schlüssel

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

6.2.9 Method of deactivating private key / Deaktivierung privater Schlüssel

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

6.2.10 Method of destroying private key / Zerstörung privater Schlüssel

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

6.2.11 Cryptographic Module Rating / Beurteilung Signaturerstellungseinheiten

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

6.3.1 Public key archival / Archvierung eines öffentlichen Schlüssels

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

6.4 Activation data / Aktivierungsdaten

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

6.4.2 Activation data protection / Schutz von Aktivierungsdaten

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

6.4.3 Other aspects of activation data / Andere Aspekte von Aktivierungsdaten

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

6.5 Computer security controls / Sicherheitsmaßnahmen IT-System

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

6.5.2 Computer security rating / Beurteilung der Computersicherheit

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

6.6 Life cycle technical controls / Technische Maßnahmen während des Lebenszyklus

6.6.1 System development controls / Sicherheitsmaßnahmen bei der Entwicklung

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

6.6.2 Security management controls / Sicherheitsmaßnahmen beim Computermanagement

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

6.6.3 Life cycle security controls / Sicherheitsmaßnahmen während des Lebenszyklus

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

6.7 Network security controls / Sicherheitsmaßnahmen Netzwerke

The necessary security measures are documented in the GLOBALTRUST® Certificate Security Policy.

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

6.8 Time-stamping / Zeitstempel

The systems relevant to certification services are synchronised with one another and and continually calibrated to "Universal Time Coordinated (UTC)".

To this purpose, the NTP [RFC1305] protocol or an equivalent protocol recognised as a reliable time calibration mechanism is used. Time is calibrated using publicly available NTP servers operated by recognised facilities, for example, the National Metrology Institute of Germany, or other technical systems that can directly receive standardised time values. This is, in particular, DCF77 time format, GPS time format, or equivalent related satellite-supported positioning systems with equivalent exact time data (synchronous time). At least two independent time sources are used to calculate the correct time, this allows the synchronisation of time for certification services with "Universal Time Coordinated (UTC)" within one second. This accuracy is particularly valid for the time source of timestamp services.

The failure of one or more time sources is detected and documented by operations monitoring. Failures that give cause to anticipate a greater

Die für die Zertifizierungsdienste relevanten Systeme sind zeitlich untereinander synchronisiert und werden laufend mit der "Universal Time Coordinated (UTC)" abgeglichen.

Zu diesem Zweck wird das Protokoll NTP [RFC1305] oder ein gleichwertiges Protokoll herangezogen, das als verlässlicher Mechanismus zum Zeitabgleich anerkannt ist. Der Zeitabgleich erfolgt über öffentlich verfügbare NTP-Server anerkannter Einrichtungen, wie z.B. die deutsche Physikalisch-Technische Bundesanstalt oder sonstiger technischer Systeme, die standardisierte Zeitwerte direkt empfangen können. Insbesondere sind dies DCF77-Zeitformat, das GPS-Zeitformat oder vergleichbare, verwandte satellitengestützte Positionierungssysteme mit vergleichbar genauen Zeitangaben (Synchronzeit). Es werden zumindest zwei unabhängige Zeitquellen herangezogen, die korrekte Zeit wird durch Abgleich der unterschiedlichen Quellen ermittelt und erlaubt die Synchronisation der Zeiten für die Zertifizierungsdienste mit der "Universal Time Coordinated (UTC)" innerhalb einer Sekunde. Diese Genauigkeit gilt insbesondere für die Zeitquelle des Zeitstempeldienstes.

Der Ausfall einer oder mehrerer Zeitquellen wird durch die Betriebsüberwachung erkannt und dokumentiert. Ausfälle, die eine

deviation from the time as is considered acceptable by the regulatory authority lead to the stop of all certification services that require exact time information, in particular timestamp services, signature of OCSP response and signature of revocation and suspension lists.

To ensure accuracy, synchronous time is synchronised regularly with the system time of the system that creates timestamps. The system time is compared to synchronous time at least once a day and any deviations as according to [RFC1305] or equivalent are eliminated.

The operator reserves the right to use additional procedures to ensure the correct time.

Statistics are continually made of observed deviations and the availability of synchronous time to document time accuracy.

Circumstances, that result in leaps in time equal or higher than the accuracy of the time stamp service (for instance leap seconds) will be documented and constraints of the validity of the time stamp will be published on the website of the VDA under "limits".

Timestamps that contain an entry with the OID 1.2.40.0.36.4.5.2.0 or 1.2.40.0.24.4.5.2.0 have been created for testing purposes and are not authentic. In particular, their time information can deviate from the requirements of this policy or the GLOBALTRUST® Certificate Practice Statement. Typical testing is in particular testing of new developments (software tests) and tests of functionality of timestamp services.

größere Zeitabweichung als die durch die Aufsichtstellen vorgegebene akzeptable Abweichung erwarten lassen, führen zum Stopp aller Zertifizierungsdienste die eine exakte Zeitangabe erfordern, insbesondere der Zeitstempeldienste, der Signatur des OCSP-Response und der Signatur der Widerrufs- und Sperrlisten.

Zur Sicherung der Genauigkeit wird die Synchronzeit regelmäßig mit der Systemzeit des Systems, das die Zeitstempel erstellt, synchronisiert. Dazu wird zumindest einmal täglich die Systemzeit mit der Synchronzeit verglichen und allfällige Abweichungen gemäß [RFC1305] oder gleichwertig eliminiert .

Der Betreiber behält sich vor, zusätzliche Verfahren zur Sicherung der korrekten Zeit heranzuziehen.

Zur Dokumentation der Zeitgenauigkeit werden laufend Statistiken über die beobachteten Abweichungen und die Verfügbarkeit der Synchronzeiten durchgeführt.

Ereignisse die zu Zeitsprüngen größer oder gleich der Genauigkeit des Zeitstempeldienstes führen (zB Schaltsekunden), werden dokumentiert und Beschränkungen in der Aussagekraft des Zeitstempels auf der Webseite des VDA unter "Limits" veröffentlicht.

Zeitstempel die einen Eintrag mit der OID-Nummer 1.2.40.0.36.4.5.2.0 oder 1.2.40.0.24.4.5.2.0 enthalten, wurden zu Testzwecken erstellt und sind nicht authentisch, insbesondere können die Zeitangaben von den Vorgaben dieser Policy oder dem GLOBALTRUST® Certificate Practice Statement abweichen. Typische Testzwecke sind insbesondere Tests von Neuentwicklungen (Softwaretests) und Tests zur Funktionsfähigkeit der Zeitstempeldienste.

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

7.1 Certificate profile / Zertifikatsprofile

7.1.1 Version number(s) / Versionsnummern

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

7.1.2 Certificate extensions / Zertifikatserweiterungen

Test certificates in X509v3 format can be distinugished with the extension 1.2.40.0.36.4.1.0=DER:01:01:FF (test property = TRUE). **This extension is not allowed for qualified certificates.**	Testzertifikate im X509v3-Format können mit der Erweiterung 1.2.40.0.36.4.1.0=DER:01:01:FF (Testeigenschaft = TRUE) ausgezeichnet werden**. Diese Erweiterung ist nicht für qualifizierte Zertifikate erlaubt.**

7.1.3 Algorithm object identifiers / Algorithmen OIDs

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

7.1.4 Name formats / Namensformate

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

7.1.5 Name constraints / Namensbeschränkungen

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

7.1.6 Certificate policy object identifier / Certificate Policy Object Identifier

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

7.2 CRL profile / Sperrlistenprofile

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

7.2.1 Version number(s) / Versionsnummern

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

7.3 OCSP profile / Profile des Statusabfragedienstes (OCSP)

7.3.1 Version number(s) / Versionsnummern

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

7.3.2 OCSP extensions / OCSP-Erweiterungen

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

8.4 Topics covered by assessment / Behandelte Themen der Begutachtung

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

8.6 Communication of results / Mitteilung des Ergebnisses

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

9.1 Fees / Kosten

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.1.2 Certificate access fees / Kosten für den Zugriff auf Zertifikate

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.1.4 Fees for other services / Kosten für andere Dienstleistungen

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.1.5 Refund policy / Kostenrückerstattung

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.2 Financial responsibility / Finanzielle Verantwortung

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.2.1 Insurance coverage / Versicherungsdeckung

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.2.2 Other assets / Andere Ressourcen für Betriebserhaltung und Schadensdeckung

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.3 Confidentiality of business information / Vertraulichkeit von Geschäftsdaten

9.3.1 Scope of confidential information / Definition vertrauliche Geschäftsdaten

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.4 Privacy of personal information / Datenschutz von Personendaten

9.4.1 Privacy plan / Datenschutzkonzept

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.4.2 Information treated as private / Definition von Personendaten

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.4.4 Responsibility to protect private information / Zuständigkeiten für den Datenschutz

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.4.7 Other information disclosure circumstances / Andere Bedingungen für Auskünfte

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

9.5 Intellectual property rights / Schutz-und Urheberrechte

The operator offers certification services under the trademark GLOBALTRUST®.
GLOBALTRUST® is an EU-wide registered Community Trade Mark (http://oami.europa.eu) under the number 002286649 of the Austrian-registered society, "ARGE DATEN – Austrian Society for Data Protection" (ZVR 774004629), hereafter known as the "Society". The right to use the trade mark GLOBALTRUST® for certification services and in particular to use the ensuing root certificates for the certification (especially signature) of certificates and signature creation devices of the CA, of the Society or of a third party is granted by the Society to the CA without any restriction and for an unlimited period of time.

Der Betreiber bietet Zertifizierungsdienste unter der Markenbezeichnung GLOBALTRUST® an.
GLOBALTRUST® ist eine EU-weit unter der Nummer 002286649 eingetragene Gemeinschaftsmarke (http://oami.europa.eu) des in Österreich eingetragenen Vereins "ARGE DATEN - Österreichische Gesellschaft für Datenschutz" (ZVR 774004629), in Folge kurz "Verein". Die Nutzungsrechte der Marke GLOBALTRUST® für Zertifizierungsdienste und insbesondere die Nutzung folgender Root-Zertifikate zur Zertifizierung (insbesondere Signatur) von Zertifikaten und Signaturerstellungsdaten des VDA, des Vereins oder Dritter und wird dem VDA vom Verein uneingeschränkt und auf unbestimmte Zeit eingeräumt.

9.6 Representations and warranties / Zusicherungen und Garantien

9.6.1 CA representations and warranties / Leistungsumfang des VDA

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

9.6.2 RA representations and warranties / Leistungsumfang der Registrierungsstellen

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

9.6.3 Subscriber representations and warranties / Zusicherungen und Garantien des Signators

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.6.5 Relying party representations and warranties of other participants / Zusicherungen und Garantien anderer Teilnehmer

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.7 Disclaimer of warranties / Haftungsausschlüsse

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.8 Limitations on liability / Haftungsbeschränkungen

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.9 Indemnities / Schadensersatz / Indemnities

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

9.10.1 Term / Gültigkeitsdauer der CP / Term

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.10.2 Termination / Beendigung der Gültigkeit / Termination

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.10.3 Effect of termination and survival / Auswirkung der Beendigung

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.12 Amendments / Änderungen

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.12.1 Procedure for amendment / Verfahren bei Änderungen

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.12.2 Notification mechanism and period / Benachrichtigungsmechanismen und –fristen

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

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

As per GLOBALTRUST® Certificate Policy | Gemäß GLOBALTRUST® Certificate Policy

9.13 Dispute resolution provisions / Bestimmungen zur Schlichtung von Streitfällen

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

9.14 Governing law / Gerichtsstand

As per GLOBALTRUST® Certificate Policy

Gemäß GLOBALTRUST® Certificate Policy

9.15 Compliance with applicable law / Einhaltung geltenden Rechts

The GLOBALTRUST® Certificate Practice Statement applies for all certificates issued for simple, advanced and qualified signatures. In particular, it applies for the performance of all certification services defined under ⇨1.6 Definitions and acronyms / Definitionen und Kurzbezeichnungen (p19).

Timestamp services, server-side or mobile signature services can be offered as qualified, advanced or simple electronic signature services. Mobile signature services are initiated using mobile phones or other mobile technical devices. Mobile signature services are offered as server services or as "direct electronic signature" (signature on end device) in a mobile technical device.

Issued simple certificates can be used by the subscriber for secrecy (encryption) as well as to sign one or more electronic documents.

Issued qualified certificates serve to sign (electronic signature or qualifed electronic signature) one or more electronic documents (data).

Das GLOBALTRUST® Certificate Practice Statement gilt für alle Zertifikate, die für einfache, fortgeschrittene und qualifizierte Signaturen ausgestellt wurden. Insbesondere gilt sie für die Erbringung aller unter ⇨1.6 Definitions and acronyms / Definitionen und Kurzbezeichnungen (p19) definierten Zertifizierungsdienste.

Zeitstempeldienste, serverseitige oder mobile Signaturdienste können als qualifizierte, fortgeschrittene oder einfache elektronische Signaturdienste angeboten werden. Mobile Signaturdienste werden mittels Mobiltelefone oder anderer mobiler technischer Einheiten ausgelöst. Mobile Signaturdienste werden als Serverdienste oder als "direkte elektronische Signatur" (Signatur am Endgerät) in der mobilen technischen Einheit angeboten.

Die ausgestellten einfachen Zertifikate können vom Signator sowohl zur Durchführung von Geheimhaltungsoperationen (Verschlüsselung), als auch zum Signieren einzelner oder mehrerer elektronischer Dokumente verwendet werden.

Die ausgestellten qualifizierten Zertifikate dienen zum Signieren (elektronische Signatur oder qualifizierte elektronische Signatur) einzelner oder mehrerer elektronischer Dokumente (Dateien).

9.16 Miscellaneous provisions / Sonstige Bestimmungen

9.16.1 Entire agreement/ Vollständigkeitserklärung

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

9.16.2 Assignment / Abgrenzungen

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

9.16.3 Severability / Salvatorische Klausel

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

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

Certification operations on the basis of this GLOBALTRUST® Certificate Practice Statement are only carried out after approval from the responsible regulatory authority.	Der Zertifizierungsbetrieb auf Basis dieser GLOBALTRUST® Certificate Practice Statement wird erst nach Genehmigung durch die zuständigen Aufsichtsstellen vorgenommen.

9.16.5 Force Majeure / Höhere Gewalt

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

9.17 Other provisions / Other provisions

As per GLOBALTRUST® Certificate Policy	Gemäß GLOBALTRUST® Certificate Policy

SCHEDULE / VERZEICHNISSE

Author(s) and validity / Autor(en) und Gültigkeitshistorie

Previous versions of this document are available on the website of the operator.

Each document is valid between the date it becomes valid and the date the successor document becomes valid. If not otherwise marked, the validity of the old document ends the day before the new document becomes valid.

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

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

Name	Version	Date / Stand	File / Datei	Comment / Kommentar
Hans G. Zeger	Version 1.0	1. Juni 2014	/static/globaltrust-practice-statement.20140601.pdf	Stammfassung
Hans G. Zeger	Version 1.0a	1. Februar 2015		Interne Version
Hans G. Zeger	Version 1.0b	1. Februar 2015	/static/globaltrust-practice-statement.20150201.pdf	Redaktionelle Überarbeitung
Hans G. Zeger	Version 2.0	22. Juni 2017	/static/globaltrust-practice-statement.pdf	Ergänzungen auf Grund [eIDAS-VO]

APPENDIX / ANHANG

APPENDIX / ANHANG A: DOCUMENTATION / DOKUMENTATION

1 BIBLIOGRAPHY / BIBLIOGRAPHIE

As per GLOBALTRUST® Certificate Policy / Gemäß GLOBALTRUST® Certificate Policy