ARGE DATEN

A-CERT TIMESTAMP Certificate Policy

[gültig für A-CERT TIMESTAMP Zeitstempeldienst]

Version 1.2/Juni 07 - a-cert-timestamp-policy.20070626.doc
OID-Nummer: 1.2.40.0.24.1.1.6.1

cn=Mag. Dr. Hans G. Zeger,
Abwicklung A-CERT-Service,
c=AT, l=Wien, o=e-commerce
monitoring GmbH, email=hans.
zeger@e-monitoring.at
2010.07.29 11:00:37 +02'00'

ARGE DATEN - Österreichische Gesellschaft für Datenschutz
A-1160 Wien, Redtenbachergasse 20
PSK 7214.741 (BLZ 60.000), DVR: 0530794
http://www.argedaten.at
☎ +43/1/4803209, Fax +43/1/4803209
e-mail: info@argedaten.at

INHALT:

ANHANG:

I. ÄNDERUNGSDOKUMENTATION

1. RTR-STAMMFASSUNG 26. JUNI 2007

- Diverse redaktionelle Korrekturen von Schreib- und Formulierungsfehlern.

2. STAMMFASSUNG 12. DEZEMBER 2006

II. GRUNDLAGEN

A. DEFINITIONEN UND KURZBEZEICHNUNGEN

Herausgeber
Herausgeber dieser Certificate Policy ist die ARGE DATEN - Österreichische Gesellschaft für Datenschutz

A-CERT
Ist der Sammelbegriff für alle Zertifizierungsdienste des Herausgebers. Unterschiedliche Zertifizierungsdienste werden mit Zusätzen zu A-CERT gekennzeichnet.

Policy
Die in diesem Dokument beschriebene A-CERT Certification Policy wird im Folgenden kurz als "Policy" bezeichnet. Diese Policy ist als Rahmen zu verstehen, innerhalb dessen die Zertifizierungsdienste erbracht werden. Dieser Rahmen kann nicht erweitert werden. Eine Einschränkung der Anwendbarkeit der Policy auf bestimmte Zertifizierungsfälle und Signaturvorgänge ist jedoch durch Vereinbarungen möglich. Die AGB's des Herausgebers oder zusätzliche Vereinbarungen der Partnerunternehmen können jedoch nicht die vorliegende Policy ganz oder teilweise außer Kraft setzen. Die zu A-CERT TIMESTAMP gültige Policy wird im vorliegenden Dokument beschrieben und hat die OID-Nummer 1.2.40.0.24.1.1.6.1. Historische Versionen des Dokuments sind bei der Aufsichtsstelle abzurufen oder unter der OID-Nummer 1.2.40.0.24.1.1.6.99 abgelegt.

Zeitstempel
Signierte Datenstruktur bestehend aus dem Hashcode eines Dokuments und dem Zeitpunkt der Unterzeichnung. Format und Methode der Erzeugung des Zeitstempels entspricht dem RFC 3161. Der Begriff Timestamp wird in dieser Policy synonym verwendet.

Anforderer
Stelle, die einen Zeitstempel anfordert.

Diensterbringer
Stelle, die den Zeitstempeldienst durchführt.

Abfrager
Stelle, die zu einem angegebenen Hash-Code die zugehörigen Zeitstempelinformationen abruft.

Signaturbestimmungen
Gesamtheit der in den Dokumenten [SigG], [SigV], [SigRL] (=EU-Signaturrichtlinie) verabschiedeten Bestimmungen.

Aufsichtsbehörde
Die für die A-CERT Zertifizierungsdienste zuständige Aufsichtsbehörde.

Ansonsten werden die Begriffe gemäß SigG, SigV, SigRL, gem. X.509, den RFCs 1305, 3161, 3280 und 3647 verwendet.

B. ÜBERBLICK

Die vorliegende Certificate Policy enthält alle Regeln für die Ausstellung von Zeitstempeln. Die Signatur für den Zeitstempel entspricht der fortgeschrittenen Signatur. Die verwendeten Zertifikate entsprechen der Definition §2 Abs. 8 [SigG].

Diese Policy wurde in Übereinstimmung mit den Signaturbestimmungen verfasst und bildet gemeinsam mit den "A-CERT Allgemeine Betriebs- und Nutzungsbedingungen" (AGB's) und der Anzeige bei der Aufsichtsbehörde die Grundlage für die Verwendung von A-CERT Zertifikaten durch den Signator.

Änderungen auf Grund gesetzlicher Änderungen werden zum Zeitpunkt des Inkrafttretens der gesetzlichen Bestimmungen wirksam, sonstige Änderungen vier Wochen nach Verlautbarung auf der Internet-Seite von A-CERT.

C. ANWENDUNGSBEREICH

Die A-CERT TIMESTAMP Certificate Policy gilt für alle Zeitstempel, die im Rahmen des A-CERT TIMESTAMP - Dienstes ausgestellt werden.

Beschränkungen in den Dokumentenformaten und -inhalten, für die ein Zeitstempel ausgestellt wird, bestehen nicht.

Die mittels dieser Policy ausgestellten Zeitstempel sind mit digitalen Signaturen im Sinne des SigG §2 Z3 lit. a bis d [SigG] erstellt und als fortgeschrittene Signaturen im Sinne des RTR GmbH - Positionspapiers [POS] anerkannt.

III. VERPFLICHTUNGEN UND HAFTUNGSBESTIMMUNGEN

A. VERPFLICHTUNGEN DES DIENSTERBRINGERS

Der Diensterbringer verpflichtet sich sicherzustellen, dass alle Anforderungen, die im Abschnitt III dargelegt sind, erfüllt werden.

Der Diensterbringer ist verantwortlich für die Einhaltung aller Richtlinien, die in der gegenständlichen Policy beschrieben sind; dies gilt auch für jene Funktionen, deren Ausführung an Vertragspartner ausgegliedert wurde (z. B. technischer Betrieb des Zeitstempeldienstes, Vertrieb).

Bei Zeitstempel, die mit Verfahren erstellt werden, die gemäß Signaturverordnung oder gemäß der Entscheidung der Aufsichtsstelle oder anerkannter Standardisierungsgremien (insbesondere gemäß den speziellen Empfehlungen ETSI SR 002 176 bzw. des Folgestandards ETSI TS 102 176) als nicht mehr sicher zuverlässig anzusehen sind, werden die Anforderer - sofern ihre Identität bekannt ist und gültige Kontaktdaten vorhanden sind - über die fehlende Zuverlässigkeit des Zeitstempels informiert.

Der Diensterbringer behält sich das Recht vor, den Zeitstempeldienst temporär oder permanent einzustellen, wenn die Zuverlässigkeit der verwendeten Zeit oder der sonstigen eingesetzten Methoden nicht mehr garantiert werden kann. Anforderer erhalten in diesem Fall einen Warnhinweis, dass kein Zeitstempel ausgestellt werden kann.

Der Diensterbringer speichert Hash-Wert und Zeitstempel des angeforderten Dokuments. Der Diensterbringer ist berechtigt jedem Abfrager bei Vorlage eines Hash-Werts den (die) verfügbaren Zeitstempel bekannt zu geben.

Der Diensterbringer gewährleistet eine Genauigkeit des Zeitstempels mit einer maximalen Abweichung von einer Sekunde zur tatsächlichen Zeit. Als tatsächliche Zeit wird die von der Physikalisch-Technischen Bundesanstalt (PTB) in Mainflingen im DCF77-Format bekannt gegebene Zeit (offizielle deutsche Zeit) definiert (Synchronzeit I).

Die Zeit wird im Format "JJJJMMTThhmmss.sssZ" ausgegeben, mit JJJJ = Jahr, MM = Monat, TT = Tag hh = Stunde, mm = Minute, ss = Sekunde, .sss = Microsekunde (werden nicht berücksichtigt) und Z steht für "UTC, Coordinated Universal Time".

Zur Sicherung der Genauigkeit wird die Synchronzeit I regelmäßig mit der Systemzeit des Systems, das die Zeitstempel erstellt, synchronisiert. Dazu wird jede Minute die Systemzeit mit der

Synchronzeit I verglichen und allfällige Abweichungen gemäß [RFC1305] eliminiert.

Bei Ausfall der DCF77-Zeit wird die exakte Zeit von einem Pool von verschiedenen öffentlich verfügbaren Internet-Time-Servern (nach ntp-Standard RFC 1305, Synchronzeit II) bezogen. Die Genauigkeit wird sichergestellt, indem die Zeitangaben mehrerer Zeitserver (mindestens 5) zur Synchronisation herangezogen werden. Zeitserver mit unplausiblen Zeitabweichungen werden automatisch ausgeschieden.

Die Synchronzeit II dient nur zur Überbrückung eines allfälligen Ausfalls der Synchronzeit I.

Bestehen Hinweise, dass die angegebene Zeitgenauigkeit nicht mehr garantiert werden kann, dann wird der Zeitstempeldienst solange abgeschalten, als eine ausreichend genaue Zeitsynchronisation gegeben ist. Die Abschaltung und der Neustart des Zeitstempeldienst erfolgt automatisch, der Diensterbringer wird von den Vorfällen per Mail verständigt. Die Abschaltung erfolgt jedenfalls, wenn die Synchronzeit I länger als 600 Minuten nicht verfügbar ist. Sind sowohl Synchronzeit I als auch Synchronzeit II länger als 30 Minuten nicht verfügbar, dann erfolgt ebenfalls eine Abschaltung des Zeitstempeldienstes.

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

Der Diensterbringer strebt eine 99,9%ige Verfügbarkeit des Zeitstempeldienstes an (weniger als 9 Stunden Ausfall im Jahr) und wird quartalsweise einen Bericht über die Ausfallszeiten veröffentlichen.

B. VERPFLICHTUNGEN DES ANFORDERERS

Der Anforderer kann nur Zeitstempel gemäß der technischen Spezifikationen von A-CERT TIMESTAMP anfordern.

Der Diensterbringer kann, muss jedoch nicht, detaillierte Spezifikationen und Programme zum Abruf von Zeitstempeln zur Verfügung stellen.

C. HAFTUNG

Der Diensterbringer haftet
- für die Einhaltung dieser Policy
- für die Genauigkeit des Zeitstempels

Der Diensterbringer haftet nicht, falls er nachweisen kann, dass ihn an der Verletzung der oben angeführten Verpflichtungen kein Verschulden trifft.

IV. SPEZIFIKATIONEN ZUR ERBRINGUNG DES ZEITSTEMPELDIENSTES

A. OPERATIVE MAßNAHMEN

Zur Gewährleistung eines ordnungsgemäßen Betriebs des Zeitstempeldienstes wurden folgende Maßnahmen ergriffen:

1. Die für die Erstellung der Zeitstempel notwendigen Prozesse und Programme sind vom Diensterbringer vollständig dokumentiert.
2. Über die Website des Diensterbringers werden sowohl diese Policy, die allgemeinen Betriebs- und Nutzungsbedingungen (AGB's), als auch laufende Informationen zu den angebotenen Diensten und verwendeten Verfahren zugänglich gemacht.
3. Der Vorstand des Diensterbringers genehmigt die notwendigen Dokumentationen und Richtlinien und ernennt jene Personen und externe Vertragspartner, die für die operative Umsetzung verantwortlich sind. Verabschiedung und Ernennung werden schriftlich dokumentiert.
4. Der Vorstand des Diensterbringers entscheidet auch, an welchem Ort der Zeitstempeldienst erbracht wird.
5. Über die Website wird zeitgerecht über Änderungen informiert, die im Certification Policy Statement vorgenommen werden. Die aktuelle Version ist jeweils online abrufbar.

B. SCHLÜSSELVERWALTUNG

1. *ERZEUGUNG DER TIMESTAMP SCHLÜSSEL*

Die notwendigen Schlüssel und Zertifikate zur Erbringung des Zeitstempeldienstes werden als fortgeschrittene digitale Signaturen A-CERT ADVANCED gemäß der jeweils gültigen Policy (OID-Nummer: 1.2.40.0.24.1.1.1.3) erzeugt.

2. *SPEICHERUNG DER CA SCHLÜSSEL*

Die notwendigen Schlüssel werden passwortgeschützt im vorgesehenen System gespeichert. Eine Sicherungskopie wird extern in einem Tresor verwahrt. Das für die Verwendung des Schlüssels benötigte Passwort wird beim Start des Timestamp-Servers eingegeben und kann nicht ausgelesen werden.

3. *VERTEILUNG DER ÖFFENTLICHEN CA SCHLÜSSEL*

Der Diensterbringer stellt durch folgende Maßnahmen sicher, dass die Integrität und Authentizität der für diesen Dienst

erfoderlichen öffentlichen Schlüssel anlässlich der Verteilung gewahrt bleibt:
- durch Übergabe der Schlüssels zur Veröffentlichung an die Aufsichtsstelle durch Übermittlung der signierten PKCS#10 Certificate Requests,
- durch Veröffentlichung des Zertifikats.

4. SCHLÜSSELOFFENLEGUNG

Der geheime Schlüssel ist nicht öffentlich verfügbar.

5. ENDE DER GÜLTIGKEITSPERIODE DER TIMESTAMP-SCHLÜSSEL

Die geheimen Schlüssel zur Erstellung von Zeitstempel werden verwendet, solange die verwendeten Algorithmen als sicher im Sinne II.A dieser Policy anzusehen sind.

Schlüssel, die den Sicherheitsanfoderungen nicht mehr entsprechen oder aus anderen Gründen nicht mehr weiter verwendet werden, werden gelöscht. Es erfolgt keine Archivierung nicht aktiver Schlüssel.

C. ERZEUGEN DER ZEITSTEMPEL

1. ANFORDERUNG

Anforderungen für Zeitstempel werden ausschließlich online gemäß [RFC3161] entgegen genommen.

Anforderer haben die Möglichkeit Zeitstempel über http-Requests oder TCP/IP-Requests anzufordern. Dazu ist die Präsentation eines sicheren Hash-Codes jenes Dokuments erforderlich, zu dem ein Zeitstempel erzeugt werden soll. Die Übermittlung des Dokuments an den Diensterbringer ist nicht vorgesehen.

Die http-Anforderungen können unter
https://timestamp.a-cert.at:10080 bzw.
https://timestamp.a-cert.at:11080 gestellt werden, die TCP/IP-Anforderungen unter timestamp.a-cert.at:10318 Es handelt sich um verschiedene technisch bedingte Abläufe, um eine möglichst breite Palette von Produkten, die Timestamps anfordern können, zu unterstützen.

In allen Fällen hat der Timestamp denselben Aufbau.

Als sichere Hash-Codes werden derzeit Hashcodes, die nach den Verfahren SHA-1 und RIPE-MD160 erzeugt wurden, akzeptiert. Der Diensterbringer behält sich ausdrücklich vor, in Zukunft Hash-Verfahren, die nicht mehr als sicher anzusehen sind, nicht mehr zu unterstützen bzw. weitere sichere Hash-Verfahren freizugeben.

Der Diensterbringer kann, muss jedoch keine Identifikation des Anforderers vornehmen.

Grundlage der Diensterbringung ist die vorliegende Policy und - sofern der Dienst kostenpflichtig genutzt wird - für die Verrechnung die vertragliche Vereinbarung des Anforderers mit dem Diensterbringer.

2. ANFORDERUNGSPRÜFUNG

Der Diensterbringer nimmt ausschließlich eine formale Prüfung des übermittelten Hash-Codes vor. Er prüft die Länge und die Übereinstimmung mit der erwarteten Länge des angegebenen Hash-Verfahrens. Es erfolgt keine Prüfung, ob zu dem Hash-Code auch tatsächlich ein Dokument existiert.

3. ANFORDERUNGSBEARBEITUNG

Die Erstellung des Zeitstempels erfolgt automatisiert unmittelbar bei Einlangen der Anforderung. Das Ergebnis (der Zeitstempel) wird über denselben Port retourniert wie die Anforderung.

Ist der Dienst nicht verfügbar, wird die Anforderung abgelehnt. Der Anforderer kann den Zeitstempel zu einem späteren Zeitpunkt neuerlich anfordern. Eine Zwischenspeicherung der nicht erfolgreichen Anforderungen findet nicht statt.

4. ANFORDERUNGSARCHIVIERUNG

Hash-Code, Timestamp und Verwaltungsdaten zur Identifikation des Vorgangs werden in einer Datenbank des Diensterbringers gespeichert und können in Zukunft zur Auskunftserteilung genutzt werden.

5. ZERTIFIKATSINHALT

Inhalt und technische Beschreibung des Timestamps ist der jeweiligen Anzeige zu entnehmen.

D. BEKANNTMACHUNG DER VERTRAGSBEDINGUNGEN

Der Diensterbringer macht den Anforderern von Zeitstempel und anderen Benutzern, die auf die Zuverlässigkeit der A-CERT Dienste vertrauen, die Bedingungen, die die Benutzung des jeweiligen Zertifikats betreffen, durch Veröffentlichung folgender Dokumente auf der A-CERT Homepage zugänglich:

1. die gegenständliche Certificate Policy,
2. die Allgemeinen Betriebs- und Nutzungsbedingungen,
3. ergänzende Beschreibungen zu den einzelnen Zertifizierungsdiensten,
4. ein Verweis auf die Anzeige des Zertifizierungsdienstes bei der Aufsichtsbehörde,

5. sonstige Mitteilungen.
Änderungen werden dem Signator mittels Bekanntmachung auf der A-CERT Homepage und ggf. zusätzlich per e-mail oder brieflich mitgeteilt. Sie sind von jedermann über die A-CERT Homepage abrufbar.

E. VERÖFFENTLICHUNG DER ZERTIFIKATE

Grundsätzlich werden alle von A-CERT zum Zeitstempeldienst verwendeten Zertifikate den Anforderen und den Überprüfern folgendermaßen verfügbar gemacht.

Alle verwendeten Zertifikate werden in den Verzeichnisdienst(en) von A-CERT veröffentlicht. Details dazu sind der dem Zertifikat zugeordneten Certificate Policy zu entnehmen.

F. WIDERRUF

Müssen die für den Zeitstempdienst maßgeblichen Zertifikate widerrufen werden, wird der Zeitstempeldienst umgehend mit neuen, geeigneten Zertifikaten ausgestattet. Bis zur Ausstattung mit neuen Zertifikaten ist der Betrieb des Zeitstempeldienstes unterbrochen.

V. A-CERT BETRIEBSORGANISATION

A. SICHERHEITSMANAGEMENT

Der Diensterbringer ist für alle Prozesse im Rahmen des Zeitstempeldienstes verantwortlich; dies gilt auch für die an Vertragspartner ausgelagerten Dienste. Die Verantwortlichkeiten der Vertragspartner sind klar geregelt, weiters sind Kontrollen zur Überprüfung der ordnungsgemäßen Tätigkeit eingerichtet. Die für die Sicherheit relevanten Vorgehensweisen sind in dieser Policy veröffentlicht.

Die Betriebsinfrastruktur von A-CERT wird ständig überprüft und an geänderte Anforderungen angepasst. Jegliche Änderungen, die einen Einfluss auf das Ausmaß der erreichten Sicherheit haben, sind vom Vorstand des Diensterbringers zu genehmigen.

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

Der technische Betrieb erfolgt in den Räumen des Diensterbringers oder bei entsprechend qualifizierten Vertragspartnern. Die jeweils aktuellen Vertragspartner werden der Aufsichtsbehörde bekannt gegeben und auf der Website von A-CERT veröffentlicht. Alle Vertragspartner sind an die Wahrung der Datensicherheit im Sinne dieser Policy, des DSG 2000 und der Signaturbestimmungen vertraglich gebunden.

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

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

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

- Stufe administration: Umfasst alle Daten, die zur ordnungsgemäßen Betriebsführung im kaufmännischen Sinn dienen, inkl. interne Dokumentationen, Buchhaltung, Kunden- und Interessentenadministration, Angebot- und Rechnungslegung.

- Stufe systemadministration: Umfasst alle Daten, die zur Aufrechterhaltung und Weiterführung des IT-Betriebs dienen.

- Stufe security: Umfasst alle Daten, die besonderen Prozessen unterworfen sind, insbesondere sind dies die Daten die im unmittelbaren Zusammenhang mit Schlüsselerstellung und Zertifizierung der für den Zeitstempeldienst erforderlichen Schlüssel stehen.

B. ZUGRIFFSVERWALTUNG

Eine Benutzerverwaltung, die den verschiedenen Funktionen unterschiedliche Zugriffsrechte einräumt, ist eingerichtet; insbesondere werden sicherheitsrelevante von nicht sicherheitskritische Funktionen sorgfältig getrennt. Alle mit der Zertifizierung im unmittelbaren Zusammenhang stehenden technischen Prozesse sind zugriffsgesichert und erfordern
- den Zutritt zu bestimmten, gesichert aufbewahrten Hardwarekomponenten und/oder
- die Eingabe von 1 bis 2 Passwörtern.

Die individuellen Erfordernisse jedes einzelnen Prozessschrittes sind dokumentiert.

Mittels Firewalls wird das interne Netzwerk vor Zugriffen durch Dritte geschützt.

Vertrauliche Daten werden bei Übertragung über unsichere Netzwerke durch Verschlüsselung geschützt.

Änderungen in den Zugriffsrechten werden im System sofort nachgezogen. Die Kontrolle der Benutzerverwaltung ist Teil des internen Audits.

Zugriff auf Informationen und Anwendungen ist auf Grund der vergebenen Zugriffsrechte eingeschränkt. Administrative und den Betrieb betreffende Prozesse sind getrennt.

Das Personal muss sich vor jedem kritischen Zugriff auf Applikationen, die in Zusammenhang mit dem Zertifikatsmanagement stehen, authentifizieren.

Die Zugriffe auf den Zeitstempeldienst werden in Log-Dateien aufgezeichnet. Die log-Dateien werden in regelmäßigen Abständen ausgelagert und durch einen Zeitstempel gegen nachträgliche Änderungen geschützt.

Änderungen (Löschungen, Hinzufügungen) bei den Verzeichnis- und Widerrufsdiensten werden durch eine Signatur der Zertifizierungsstelle gesichert.

Versuche des unauthorisierten Zugriffs auf Verzeichnis- und Widerrufsdienste werden aufgezeichnet.

Die Systemadministratoren und sonstiges Personal sind zur Einhaltung der Datensicherheitsbestimmungen gem. DSG 2000 §14 verpflichtet.

C. PERSONELLE SICHERHEITSMAßNAHMEN

Die Mitarbeiter von A-CERT sind als qualifiziertes Personal besonders geeignet, die in dieser Policy verankerten Bestimmungen umzusetzen und zu gewährleisten.

- Sicherheitsrelevante Funktionen und Verantwortlichkeiten werden in den jeweiligen Stellenbeschreibungen dokumentiert. Jene Funktionen, von denen die Sicherheit der Zertifizierungsdienste abhängt, sind eindeutig identifiziert.
- Für die Mitarbeiter bei A-CERT sind klare Stellenbeschreibungen ausgearbeitet, in denen die Pflichten, Zugriffsrechte und Kompetenzen dargelegt sind.
- Alle Leitungsfunktionen sind mit Personen besetzt, die über Erfahrung mit der Technologie digitaler Signaturen und Verschlüsselungen und mit der Führung von Personal, das Verantwortung für sicherheitskritische Tätigkeiten trägt, verfügen.
- Entsprechend § 10 Abs 4 [SigV] beschäftigt der Herausgeber keine Personen, die strafbare Handlungen begangen haben, welche sie für eine vertrauenswürdige Position ungeeignet erscheinen lassen.

D. PHYSIKALISCHE UND ORGANISATORISCHE SICHERHEITSMAßNAHMEN

Es ist sicher gestellt, dass der Zutritt zu Räumlichkeiten, in denen sicherheitskritische Funktionen ausgeübt werden, beschränkt ist und die Risken einer physischen Beschädigung von Anlagen minimiert sind.

Insbesondere gilt:

1. Der Zugriff zu den Geräten, mit denen die Zeitstempeldienste erbracht werden, ist auf autorisiertes Personal beschränkt.
2. Es werden Maßnahmen ergriffen, um den Verlust, die Beschädigung oder die Kompromittierung von Anlagen und die Unterbrechung des Betriebes zu verhindern.
3. Weitere Maßnahmen gewährleisten, dass eine Kompromittierung oder ein Diebstahl von Daten und Daten verarbeitenden Anlagen nicht möglich ist.
4. Die Systeme mit denen die Zeitstempeldienste erbracht werden, werden durch technische und organisatorische Maßnahmen in einer gesicherten Umgebung betrieben, sodass eine Kompromittierung durch unautorisierte Zugriffe nicht möglich ist.
5. Die Abgrenzung der Systeme für Zertifikatsgenerierung und Widerrufsdienste erfolgt durch klar definierte Sicherheitszonen, d. h. durch räumliche Trennung von anderen organisatorischen Einheiten sowie physischen Zutrittsschutz.

6. 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.
7. Die unautorisierte Entnahme von Informationen, Datenträgern, Software und Einrichtungsgegenständen, welche zu den Zertifizierungsdiensten gehören, wird durch Kontrollmaßnahmen verhindert.

E. LAUFENDE BETRIEBLICHE MAßNAHMEN

1. Schäden durch sicherheitskritische Zwischenfälle und Fehlfunktionen werden durch entsprechende Aufzeichnungen und Fehlerbehebungsprozeduren frühzeitig erkannt, verhindert oder zumindest minimiert.
2. Datenträger werden vor Beschädigung, Diebstahl und unautorisiertem Zugriff geschützt.
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 aufbewahrt. Nicht mehr benötigte Datenträger, die vertrauliche Daten beinhalten, werden in sicherer Weise vernichtet.
5. Die Integrität der Computersysteme und Informationen ist gegen Viren und böswillige oder unautorisierte Software geschützt.
6. Kapazitätserfordernisse werden beobachtet und künftige Entwicklungen prognostiziert, sodass stets angemessene Bandbreiten, Prozessorleistungen und sonstige IT-Ressourcen zur Verfügung stehen.
7. Die sicherheitskritischen Funktionen im Rahmen der Zertifizierungs- und Widerrufsdienste werden von den gewöhnlichen administrativen Funktionen strikt getrennt. Als sicherheitskritische Funktionen werden alle IT-Maßnahmen angesehen, die zur Erhaltung der Betriebsfähigkeit des Zertifizierungsdienstes dienen. Insbesondere sind dies
   - Planung und Abnahme von Sicherheitssystemen,
   - Schutz vor böswilliger Software und Angriffen,
   - Aktive Überprüfung von Log-Files und Prüfberichten, Analyse von Zwischenfällen,
   - Allgemeine System-Wartungstätigkeiten,
   - Netzwerkadministration,
   - Datenmanagement, Datenträgerverwaltung und –sicherheit,
   - Softwareupdates.

Die Überwachung der sicherheitskritischen Funktionen obliegt unmittelbar einem vom Vorstand des Diensterbringers nominierten Sicherheitsbeauftragten.

F. SYSTEMENTWICKLUNG

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

Zur Installation neuer Softwaremodule existieren Übergabeverfahren.

G. ERHALTUNG DES UNGESTÖRTEN BETRIEBES UND BEHANDLUNG VON ZWISCHENFÄLLEN

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

VI. SONSTIGES

A. EINSTELLUNG DER TÄTIGKEIT

Gem. § 12 SigG wird der Diensterbringer die Einstellung der Tätigkeit unverzüglich der Aufsichtsstelle anzeigen und sicher stellen, dass eine eventuelle Beeinträchtigung ihrer Dienstleistungen sowohl gegenüber Anforderern als auch gegenüber allen auf die Zuverlässigkeit der Dienste vertrauenden Parteien möglichst gering gehalten wird.

B. INFORMATION GEM. DSG 2000

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

Veröffentlicht werden Daten des Signators ausschließlich auf Grund der Erfordernisse des jeweiligen Zertifizierungsdienstes (Verzeichnisdienst, Widerrufsdienst) oder auf ausdrücklichen Wunsch des Signators.

Gesetzliche Aufbewahrungs- und Übermittlungsverpflichtungen bleiben unberührt. Eine Datenweitergabe gem. §151 GewO an Adressenverlage wird ausdrücklich ausgeschlossen.

ANHANG

ANHANG A: LITERATURLISTE

[DSG 2000] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000). BGBl. I Nr. 165/1999

[ETSI] ETSI SR 002 176 V1.1.1 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures

[POS] RTR GmbH, Positionspapier zu § 2 Z 3 lit. a bis d SigG („fortgeschrittene elektronische Signatur"), Version 1.0, 13.4.2004

[RFC1305] RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis (NTP), März 1992

[RFC3161] RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), August 2001

[RFC3280] RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002

[RFC3647] RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003

[SigG] Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG). BGBl. I Nr. 190/1999

[SigRL] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 13.12.1999

[SigV] Verordnung zum Signaturgesetz, BGBl II 2000/30, 02. 02. 2000

[X.509] ITU-T Recommendation X.509, März 2000

ANHANG B: DOKUMENTENINFORMATION

AUTOR(EN):

Name	Version	Bearbeitung	Datei	Kommentar
	0	0	dokumentation-argedaten.dot	Quelle
Hans G. Zeger	1.1	16.12.06 15:47	a-cert-timestamp-policy.20051214.doc	Stammfassung
Daniel Weller	1.2	26.06.07 09:16	a-cert-timestamp-policy.20070626.doc	RTR-Stammfassung