A1 Telekom Austria AG

Sicherheits- und Zertifizierungskonzept (Policy) gültig für Zertifikate der **A1 Telekom Austria AG Issuing CA 01**

Version: 1.2
12.11.2015

INHALT

1 Einführung

Das vorliegende Sicherheits- und Zertifizierungskonzept enthält alle Regeln für die Ausstellung und Verwendung von Zertifikaten für einfache elektronische Signaturen, welche an Endbenutzer ausgestellt werden und gemäß der EU-Richtlinie (SigRL) und dem österreichischen Bundesgesetz über elektronische Signaturen (SigG) für die Erstellung einfacher elektronischer Signaturen sowie zur Datenverschlüsselung geeignet sind.

1.1 Überblick

Das Ziel des vorliegenden Dokuments besteht darin, die Richtlinien bezüglich Zertifikaten der Klasse *A1 Telekom Austria AG Issuing CA 01* derart festzulegen, dass die Voraussetzungen für eine sichere und zuverlässige Abwicklung des angebotenen Signatur- und Zertifizierungsdienstes gewährleistet sind.

1.2 Identifikation des Sicherheits- und Zertifizierungskonzepts (Policy)

Name der Policy: *A1 Telekom Austria AG Issuing CA 01*
Version: 1.0, 25.08.2015
Object Identifier: 1.3.6.1.4.1.25602.1.2.900.1.*

1.3 Anwendungsbereich

Dieses Sicherheits- und Zertifizierungskonzept gilt für *A1 Telekom Austria AG Issuing CA 01* Zertifikate, welche an Endbenutzer ausgestellt werden und gemäß der EU-Richtlinie (SigRL) und dem österreichischen Bundesgesetz über elektronische Signaturen (SigG) für die Erstellung einfacher Signaturen und zur Datenverschlüsselung geeignet sind.

Die geheimen Schlüssel der Signaturen befinden sich auf deren Rechner. Die öffentlichen Schlüssel werden in keinem öffentlichen Verzeichnisdienst publiziert.

2 Verpflichtungen und Haftungsbestimmungen

2.1 Verpflichtungen von A1 Telekom Austria AG

A1 Telekom Austria AG verpflichtet sich sicherzustellen, dass alle Anforderungen, die im Abschnitt 3 dargelegt sind, erfüllt werden.

A1 Telekom Austria AG ist verantwortlich für die Einhaltung aller Richtlinien, die im gegenständlichen Sicherheits- und Zertifizierungskonzept beschrieben sind; dies gilt auch für jene Funktionen, deren Ausführung eventuell an Vertragspartner ausgegliedert werden (z. B. Identitätsprüfung).

Es sind keine zusätzlichen Verpflichtungen direkt oder durch Referenzieren in den Zertifikaten ausgewiesen, dementsprechend bestehen auch keine zusätzlichen Verpflichtungen aus diesem Titel.

Zertifikate zu Schlüsseln, die mit Verfahren erstellt werden, die gemäß Signaturverordnung oder gemäß der Entscheidung der Aufsichtsstelle oder anerkannter Standardisierungsgremien als nicht mehr sicher anzusehen sind, werden von A1 Telekom Austria AG widerrufen.

A1 Telekom Austria AG behält sich das Recht vor, auch dann Zertifikate zu widerrufen, wenn die verwendeten Verfahren nach eigenen Erkenntnissen nicht mehr sicher sind oder die enthaltenen Eigenschaften irreführend oder unvollständig sind.

A1 Telekom Austria AG wird alle Veröffentlichungen (insbesondere Sicherheits- und Zertifizierungskonzept, Zertifikatsverzeichnis und Widerrufslisten) in geeigneter, für die Allgemeinheit jederzeit über öffentliche Telekommunikationsverbindungen zugänglicher Weise durchführen.

2.2 Verpflichtungen des Signators

A1 Telekom Austria AG bindet den Signator an die Einhaltung der nachfolgend angeführten Verpflichtungen.

Dem Signator werden die Verpflichtungen (diese Policy) zugänglich gemacht. Mit der Installation des Zertifikats bestätigt er deren Kenntnisnahme und Akzeptanz.

Die dem Signator auferlegten Verpflichtungen umfassen insbesondere:

1. die Angabe vollständiger und korrekter Informationen in Übereinstimmung mit den Anforderungen dieses Sicherheits- und Zertifizierungskonzepts insbesondere anlässlich des Vorgangs der Registrierung,

2. die ausschließliche Verwendung des privaten Schlüssels für die im Zertifikat eingetragenen Zwecke unter Beachtung der dem Anwender mitgeteilten Beschränkungen,

3. seine Signaturerstellungsdaten (private Schlüssel) ordnungsgemäß zu verwahren und vor Zugriffen unbefugter Dritter zu schützen sowie nicht an andere Personen weiterzugeben,

4. die sichere Vernichtung der Signaturerstellungsdaten nach Ablauf der Gültigkeitsperiode,

5. die unverzügliche Benachrichtigung von A1 Telekom Austria AG, wenn vor Ablauf der Gültigkeitsdauer eines Zertifikats, einer oder mehrere der nachfolgenden Fälle eintreten:
   - der private Schlüssel des Signators wird möglicherweise durch Dritte missbräuchlich genutzt,
   - die Kontrolle über den privaten Schlüssel ging verloren,
   - die im Zertifikat beinhalteten Informationen sind inkorrekt oder haben sich geändert.

6. die nationalen Ausfuhrbestimmungen sowie mögliche nationale Nutzungsbeschränkungen bei einer Verwendung im Ausland zu beachten.

2.3 Verpflichtungen des Überprüfers von Zertifikaten

Ein Überprüfer, der ein *A1 Telekom Austria AG Issuing CA 01* Zertifikat zur Verifizierung einer Signatur oder zur Verschlüsselung verwendet, kann diesem nur dann vertrauen, wenn er

- eine Überprüfung der Gültigkeitsperiode und des Widerrufsstatus des Zertifikats unter Verwendung der von A1 Telekom Austria AG bereitgestellten Abfragemöglichkeiten vornimmt,
- eventuelle im Zertifikat oder den veröffentlichten Geschäftsbedingungen dargelegte Einschränkungen der Nutzung des Zertifikats beachtet

2.4 Haftung

A1 Telekom Austria AG haftet als Aussteller von *A1 Telekom Austria AG Issuing CA 01* Zertifikaten

- für die Einhaltung dieses Sicherheits- und Zertifizierungskonzepts, insbesondere für die darin festgelegten Maßnahmen zur Veröffentlichung von Widerrufslisten und die Einhaltung der in der Zertifizierungsrichtlinie genannten Standards (ITU X.509),

- dafür, dass die im Zertifikat enthaltenen Daten zum Zeitpunkt der Ausstellung anlässlich der Registrierung überprüft wurden und keine Abweichungen der Daten gegenüber den Prüfverzeichnissen festgestellt wurden.

A1 Telekom Austria AG haftet nicht, falls sie nachweisen kann, dass sie an der Verletzung der oben angeführten Verpflichtungen keine Schuld trifft.

3 Anforderung an die Erbringung von Zertifizierungsdiensten

Im Rahmen dieses Sicherheits- und Zertifizierungskonzepts werden die Maßnahmen zu Registrierung, Zertifikatsgenerierung, Zertifikatsausgabe, Widerrufsdiensten und Abfragediensten über den Zertifikatsstatus dargestellt.

3.1 Maßnahmen für die Erbringung des Zertifizierungsdienstes

A1 Telekom Austria AG hat folgende Maßnahmen ergriffen, um die für die Erbringung von Zertifizierungsdiensten nötige Sicherheit und Verlässlichkeit zu gewährleisten:

1. Alle Vorgangsweisen und Prozeduren, die nötig sind, um die Anforderungen aus diesem Sicherheits- und Zertifizierungskonzept zu erfüllen, sind von A1 Telekom Austria AG vollständig dokumentiert.
2. Das Sicherheits- und Zertifizierungskonzept für *A1 Telekom Austria AG Issuing CA 01* benennt die Verpflichtungen von A1 Telekom Austria AG und aller externen Vertragspartner, die Dienstleistungen für A1 Telekom Austria AG, unter Beachtung des jeweils anwendbaren Sicherheits- und Zertifizierungsdienstes, erbringen.
3. A1 Telekom Austria AG macht allen Signatoren und anderen Personen, die auf die Zuverlässigkeit der A1 Telekom Austria AG Zertifizierungsdienste vertrauen, alle Informationen zu den angebotenen Diensten und verwendeten Verfahren zugänglich.
4. Dieses Sicherheits- und Zertifizierungskonzept wird von einer A1 Telekom Austria AG Expertengruppe entwickelt, die sich aus den Bereichen Marketing, Technik und Recht zusammensetzt.
5. Änderungsvorschläge zur aktuellen Version des Sicherheits- und Zertifizierungskonzepts müssen zunächst der Expertengruppe in schriftlicher Form übermittelt werden.
6. Die eingebrachten Änderungsvorschläge werden in der Sicherheits- und Zertifizierungskonzept-Expertengruppe behandelt und verabschiedet.
7. Die Expertengruppe trägt auch die Verantwortung für die ordnungsgemäße Implementierung des Sicherheits- und Zertifizierungskonzepts.
8. A1 Telekom Austria AG wird zeitgerecht über Änderungen informieren, die im Sicherheits- und Zertifizierungskonzept vorgenommen werden und eine überarbeitete Version des Sicherheits- und Zertifizierungskonzepts unverzüglich über die Webseite zugänglich zu machen.

3.2 Schlüsselverwaltung

3.2.1 Erzeugung der Zertifizierungsschlüssel des Zertifizierungsdienstes – CA (Certificate Authority) Schlüssel

Die Erzeugung der zur Erbringung der Zertifizierungsdienste gemäß dieses Sicherheits- und Zertifizierungskonzepts notwendigen Schlüssel wird von dazu autorisiertem Personal im Vier-Augen-Prinzip in einer abgesicherten Umgebung durchgeführt.

3.2.2 Speicherung der CA Schlüssel

A1 Telekom Austria AG stellt sicher, dass der private Schlüssel im für die Durchführung der Zertifizierung vorgesehenen System gespeichert bleibt.

3.2.3 Verteilung der öffentlichen CA Schlüssel

A1 Telekom Austria AG stellt durch die folgenden Maßnahmen sicher, dass die Integrität und Authentizität der öffentlichen Schlüssel anlässlich der Verteilung gewahrt bleibt:

- Durch Übergabe des Root-Schlüssels zur Veröffentlichung an die Aufsichtsstelle durch Übermittlung eines signierten PKCS#10 Certificate Request
- Durch Ausstellung und Veröffentlichung eines selbstsignierten Root-Zertifikats.

Das Zertifikat des CA Schlüssels wird den Signatoren durch Veröffentlichung im Rahmen des Verzeichnisdienstes zugänglich gemacht. A1 Telekom Austria AG gewährleistet die Authentizität dieses Zertifikats.

3.2.4 Schlüsseloffenlegung

Eine Offenlegung der geheimen CA Schlüssel ist nicht vorgesehen.

3.2.5 Verwendungszweck von CA Schlüsseln

Der private Schlüssel der A1 Telekom Austria AG wird nur für die Erstellung von *A1 Telekom Austria AG Issuing CA 01* Zertifikaten und für die Signatur der zugehörigen Widerrufslisten verwendet.

3.2.6 Ende der Gültigkeitsperiode von CA Schlüsseln

Geheime Schlüssel zur Signatur von *A1 Telekom Austria AG Issuing CA 01* Zertifikaten werden verwendet, solange die verwendeten Algorithmen den Sicherheitserwartungen entsprechen.

Die Zertifikate über die Schlüssel des Zertifizierungsdienstes werden spätestens alle 10 Jahre erneuert. Wenn die Algorithmen den Sicherheitserwartungen nicht mehr entsprechen, findet keine Erneuerung statt und die Schlüssel werden mit Erreichen des Endes der Gültigkeit gelöscht. Es erfolgt keine Archivierung der geheimen Schlüssel.

3.2.7 Erzeugung der Schlüssel für die Signatoren

Der Signator kann die Erzeugung des Schlüssels auch von A1 Telekom Austria AG durchführen lassen. A1 Telekom Austria AG erzeugt die Schlüssel in einer gesicherten Umgebung im Rechenzentrum. Die Übergabe des Zertifikats und des Schlüsselpaares an den Zertifikatsinhaber erfolgt in verschlüsselter und gegen Veränderung gesicherter Form. Für die Sicherheit des privaten Schlüssels ist der Zertifikatsinhaber verantwortlich. Die Speicherung obliegt dem Signator.

3.3 Zertifikate der Antragsteller

3.3.1 Registrierung der Signatoren

Die Maßnahmen zur Identifikation und Registrierung des Zertifikatsinhabers (Signators) stellen sicher, dass der Antrag auf Ausstellung eines *A1 Telekom Austria AG Issuing CA 01* Zertifikats korrekt, vollständig und autorisiert ist.

- Der Benutzer (Signator) oder eine übergeordnete Stelle meldet dem Zertifikatsadministrator, dass ein Zertifikat beantragt wird. Die Benutzer sind intern über entsprechende Verzeichnisse identifiziert.

- Der Zertifikatsadministrator stellt über das Intranet eine Verbindung zur Administrationsseite für *A1 Telekom Austria AG Issuing CA 01* her. Er wird automatisch anhand seines eigenen Zertifikats oder durch Angabe von Username/Passwort authentifiziert und leitet den Antrag für ein Benutzer-Zertifikat ein.

- Der Benutzer erhält automatisch ein Zertifikat.

3.3.2 Antragsprüfung, Zertifikatserstellung und Installation

3.3.2.1 Manuell erstellte Zertifikate

- Für speziell gesicherte Applikationen und Services sind individuelle Zertifikate erforderlich.
- Diese können nur manuell beim zuständigen Zertifikatadministrator angefordert werden.
- Es wird ein Auftragsticket erstellt und der CSR (Certificate Signing Request) beigefügt.
- Der Zertifikatsadministrator prüft den Request und stellt das Zertifikat aus.
- Im Anschluss setzt er sich mit dem Auftraggeber in Verbindung.

3.3.2.2 Automatisch erstellte Zertifikate

- Es werden automatisch alle Mitarbeiter von A1 Telekom Austria AG mit einem Zertifikat ausgestattet.

- Hierfür wird eine Liste der Zertifikatsempfänger erstellt und das generieren der Zertifikate angestoßen.

- Alle weiteren Installationsschritte sind wie bei den manuellen Zertifikaten.

3.3.3 Zertifikatsinhalt, Gültigkeitsdauer

A1 Telekom Austria AG Issuing CA 01 Zertifikate werden als X.509 v3 Zertifikate erstellt und beinhalten mindestens den Namen des Zertifikatsinhabers und eine E-Mail-Adresse.

Die ausgestellten Zertifikate haben eine maximale Gültigkeitsdauer von 5 Jahren.

3.3.4 Verlängerung der Gültigkeit eines Zertifikats und Ausstellung von weiteren Zertifikaten

Durch folgende Maßnahmen wird sichergestellt, dass Anträge von Antragstellern, die anlässlich einer vorhergehenden Zertifikatsausstellung bereits registriert wurden, vollständig, korrekt und ordnungsgemäß autorisiert sind. Die Maßnahmen gelten sowohl für die Verlängerung der Gültigkeitsdauer, für die Ausstellung weiterer gleichartiger Zertifikate, als auch für die Neuausstellung nach Ablauf oder Widerruf eines Zertifikats.

- A1 Telekom Austria AG prüft die im Zertifikat enthaltenen Daten hinsichtlich ihrer aktuellen Gültigkeit.
- Änderungen im vorliegenden Sicherheits- und Zertifizierungskonzept, in den Geschäftsbedingungen und in den sonstigen Vereinbarungen werden zur Kenntnis gebracht.

3.3.5 Wiederherstellung des PKCS#12-Downloads (Public/Private Key Recovery)

Der Signator kann analog zu einer Neuausstellung die Widerherstellung des Public-/Private Keys beim Systemadministrator beantragen.

Hierfür meldet er beim Servicedesk den entsprechenden Auftrag ein.

Der Zertifikatsadministrator veranlasst, dass das Zertifikat abgelegt wird und das dem Benutzer das Passwort hierfür übermittelt wird.

Alle weiteren Installationsschritte wie unter Manuell erstellte Zertifikate.

3.3.6 Veröffentlichung von Zertifikaten

A1 Telekom Austria AG Issuing CA 01 Zertifikate werden den Signatoren und den Überprüfern folgendermaßen verfügbar gemacht.

- Alle Zertifikate werden im GAL (Global Address List) publiziert.

3.3.7 Widerruf von Zertifikaten

Zum Widerruf berechtigt ist der Signator. Für die Fälle, bei denen der Signator in Vertretung einer Person oder einer Organisation handelt, sind auch diese Person bzw. ausgewiesene Vertreter der Organisation zum Widerruf berechtigt.

Ein Widerrufsantrag kann formlos am Servicedesk bekanntgegeben werden. Es wird dann ein Ticket für den Zertifikatsadministrator erstellt, der dann das Zertifikat widerruft.

Auf Verlangen eines Gerichts oder einer Behörde sowie bei missbräuchlicher Verwendung des Zertifikats (gesetzwidrige Zwecke) kann das Zertifikat durch A1 Telekom Austria AG widerrufen werden. Es erfolgt kein wie immer gearteter Ersatz der Kosten des Zertifikats oder Schadenersatz.

3.4 A1 Telekom Austria AG Betriebsorganisation

3.4.1 Sicherheitsmanagement

A1 Telekom Austria AG ist für alle Prozesse im Rahmen der Zertifizierungsdienste verantwortlich; dies gilt auch für die an eventuelle Vertragspartner ausgelagerten Dienste. Die Verantwortlichkeiten der Vertragspartner sind klar geregelt und Kontrollen zur Überprüfung der ordnungsgemäßen Tätigkeit eingerichtet. Die für die Sicherheit relevanten Vorgehensweisen sind in diesem Sicherheits- und Zertifizierungskonzept veröffentlicht.

Eine Expertengruppe von A1 Telekom Austria AG ist unmittelbar verantwortlich für die Definition der Sicherheitsrichtlinien und deren Kommunikation an die mit sicherheitsrelevanten Vorgängen befassten Mitarbeiter.

Die Betriebsinfrastruktur für den Zertifizierungsdienst wird von A1 Telekom Austria AG ständig überprüft und an sich ändernde Anforderungen angepasst. Jegliche Änderungen, die einen Einfluss auf das Ausmaß der erreichten Sicherheit haben, sind von der Expertengruppe der A1 Telekom Austria AG zu genehmigen.

Alle Sicherheitsmaßnahmen und sicherheitsrelevanten Funktionen zur Bereitstellung der Zertifizierungsdienste werden von A1 Telekom Austria AG dokumentiert und entsprechend der Dokumentation implementiert und gewartet.

Der technische Betrieb erfolgt in Räumlichkeiten der A1 Telekom Austria AG.

3.4.2 Personelle Sicherheitsmaßnahmen

A1 Telekom Austria AG beschäftigt ausschließlich Personal, welches über das benötigte Fachwissen, die Qualifikation und Erfahrung für die jeweilige Position verfügt.

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

Entsprechend § 10 Abs 4 [SigV] beschäftigt der Herausgeber keine Personen, die strafbare Handlungen begangen haben, welche sie für eine vertrauenswürdige Position ungeeignet erscheinen lassen. Eine Beschäftigung erfolgt erst nach einer diesbezüglichen Überprüfung.

3.4.3 Technische und Organisatorische Sicherheitsmaßnahmen

Es ist sichergestellt, dass der Zutritt zu Räumlichkeiten, in welchen sicherheitskritische Funktionen ausgeübt werden, beschränkt ist und die Risiken einer physischen Beschädigung von Anlagen minimiert sind.

Der Zugriff zu den Geräten, in denen Zertifizierungs- und Widerrufsdienste erbracht werden, ist auf autorisiertes Personal beschränkt. Die Systeme, welche Zertifikate ausstellen, sind vor Gefährdung durch Umweltkatastrophen baulich geschützt.

Es werden Maßnahmen ergriffen, um den Verlust, die Beschädigung oder das Kompromittieren von Anlagen und die Unterbrechung des Betriebes zu verhindern.

Weitere Maßnahmen gewährleisten, dass ein Kompromittieren oder ein Diebstahl von Daten und Daten verarbeitenden Anlagen nicht möglich ist.

Die Systeme für die Zertifikatsgenerierung und die Widerrufsdienste werden durch technische und organisatorische Maßnahmen in einer gesicherten Umgebung betrieben, sodass ein Kompromittieren durch unautorisierte Zugriffe nicht möglich ist.

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.

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

3.4.4 Laufende betriebliche Maßnahmen

Schäden durch sicherheitskritische Zwischenfälle und Fehlfunktionen werden durch entsprechende Aufzeichnungen und Fehlerbehebungsprozeduren frühzeitig erkannt, verhindert oder zumindest minimiert.

Datenträger werden vor Beschädigung, Diebstahl und unautorisiertem Zugriff geschützt.

Für die Ausführung von sicherheitskritischen und administrativen Aufgaben, die sich auf die Erbringung der Zertifizierungsdienste auswirken, sind detaillierte Prozesse in Verwendung.

Datenträger werden je nach ihrer Sicherheitsstufe behandelt und aufbewahrt. Nicht mehr benötigte Datenträger, die vertrauliche Daten beinhalten, werden in sicherer Weise vernichtet.

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

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

3.4.5 Zugriffsverwaltung

Eine Benutzerverwaltung, die den verschiedenen Funktionen unterschiedliche Zugriffsrechte einräumt, ist eingerichtet; insbesondere werden sicherheitsrelevante von nicht sicherheitskritischen 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 und andere technische Maßnahmen 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.

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 werden in Log-Dateien aufgezeichnet.

Versuche des unautorisierten Zugriffs auf Verzeichnis- und Widerrufsdienste werden aufgezeichnet. Die Entdeckung von unautorisierten und/oder außergewöhnlichen Zugriffsversuchen auf die eigentliche Zertifizierungsstelle und die Widerrufsdienste wird durch geeignete Maßnahmen gesichert, sodass ggf. sofort Gegenmaßnahmen ergriffen werden können.

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

3.4.6 Systementwicklung

A1 Telekom Austria AG verwendet vertrauenswürdige Systeme und Produkte, die gegen Veränderung geschützt sind.

Eine Analyse der Sicherheitsanforderungen muss im Stadium der Design- und Anforderungsspezifikation im Rahmen jedes Entwicklungsprojekts erfolgen, das von A1 Telekom Austria AG oder von Dritten im Auftrag von A1 Telekom Austria AG durchgeführt wird.

Änderungskontrollprozeduren existieren für die Erstellung von geplanten Programmversionen, sonstigen Änderungen und Fehlerbehebungen.

3.4.7 Erhaltung des ungestörten Betriebes und Behandlung von Zwischenfällen

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

A1 Telekom Austria AG wird sich bemühen, nach Katastrophenfällen, inklusive dem Kompromittieren eines Zertifizierungsschlüssels, den Betrieb so rasch wie möglich wiederaufzunehmen.

A1 Telekom Austria AG sieht das (tatsächliche oder vermutete) Kompromittieren des privaten Zertifizierungsschlüssels als Katastrophenfall an.

Sollte dieser Fall eintreten, so hat A1 Telekom Austria AG die Aufsichtsstelle (siehe § 6 Abs 5 [SigG]), die Signatoren, die auf die Verlässlichkeit der Zertifizierungsdienste vertrauenden Personen und gegebenenfalls andere Zertifizierungsdiensteanbieter, mit

denen Vereinbarungen bestehen, davon zu unterrichten und mitzuteilen, dass die Widerrufs- und Zertifikatsinformationen nicht mehr als zuverlässig anzusehen sind.

Zertifikate und Widerrufslisten werden als nicht mehr gültig gekennzeichnet. Den Signatoren werden mit Hilfe eines neu generierten sicheren Zertifizierungsschlüssels neue Zertifikate ausgestellt.

3.4.8 Einstellung der Tätigkeit

Gem. § 12 SigG wird der Herausgeber die Einstellung der Tätigkeit für externe Zertifikate unverzüglich der Aufsichtsstelle anzeigen und sicherstellen, dass eine eventuelle Beeinträchtigung seiner Dienstleistungen sowohl gegenüber Signatoren als auch gegenüber allen auf die Zuverlässigkeit der Dienste vertrauenden Parteien möglichst geringgehalten wird.

Vor Beendigung der Dienstleistung werden alle Signatoren, Zertifizierungsdiensteanbieter und sonstige Parteien, mit denen A1 Telekom Austria AG eine geschäftliche Verbindung unterhält, direkt und andere auf die Zuverlässigkeit der Dienste vertrauende Parteien durch Veröffentlichung von der Einstellung unterrichtet und Vorkehrungen zur Übernahme der Verzeichnis- und Widerrufsdienste sowie der Aufzeichnungen durch einen anderen Zertifizierungsdienstanbieter getroffen.

3.4.9 Übereinstimmung mit gesetzlichen Regelungen

A1 Telekom Austria AG handelt grundsätzlich in Übereinstimmung mit den gesetzlichen Regelungen und Auflagen gemäß Signaturgesetz.
Wichtige Aufzeichnungen werden vor Verlust, Zerstörung und Verfälschung bewahrt.
Die Anforderungen des Datenschutzgesetzes werden befolgt.
Nötige technische und organisatorische Maßnahmen sind ergriffen worden, um persönliche Daten vor unautorisierter und ungesetzlicher Verarbeitung sowie vor versehentlicher Zerstörung oder Beschädigung zu schützen.
Den Signatoren wird versichert, dass die an A1 Telekom Austria AG übermittelten Informationen nur mit ihrem Einverständnis, mit gerichtlichem Beschluss oder auf Basis gesetzlicher Regelungen offengelegt werden.