SICHERHEITS- UND ZERTIFIZIERUNGSKONZEPT

FÜR DEN ZERTIFIZIERUNGSDIENST

E-CONTROL CERTIFICATION SERVICES

DER ENERGIE-CONTROL AUSTRIA

RUDOLFSPLATZ 13A
1010 WIEN

Energie-Control Austria
für die Regulierung der Elektrizitäts- und
Erdgaswirtschaft

Rudolfsplatz 13a, A-1010 Wien
Tel: +43-1-24 7 24
Fax : +43-1-24 7 24-900

e-mail: office@e-control.at
www.e-control.at

VERSIONSVERWALTUNG

DATUM	VERSION	AUTOR	BEMERKUNG
16.11.2005	0.7	DKR	FERTIGE UNTERLAGE
17.11.2005	1.0	ELU	ORIGINALFASSUNG
28.01.2006	1.1	OVA	KAP. 3.4: AUSREICHENDE ZUFALLSQUALITÄT BEI DER SCHLÜSSELERZEUGUNG KAP. 1.1 WIDERRUF VON ZERTIFIKATEN KAP. 3.6 WIDERRUF VON ZERTIFIKATEN KAP. 2.1: ALLGEMEINE APASSUNGEN KAP. 4.7: ALLGEMEINE APASSUNGEN
07.04.2006	1.2	OVA	KAP. 3.1 REGISTRIERUNG (ÜBERPRÜFUNG DER IDENTITÄT DES SIGNATORS)
28.03.2011	1.2.1	KLE	FIRMENWORTLAUTÄNDERUNG IN E-CONTROL AUSTRIA UND ÄNDERUNG KAP. 1.1 ENERGIE-CONTROL AUSTRIA
09.12.2015	1.3	KLE	GENERELLE ÜBERARBEITUNG

INHALTSVERZEICHNIS

1 EINLEITUNG

1.1 Energie-Control Austria

Die Energie-Control Austria wurde vom Gesetzgeber auf Grundlage des Energieliberalisierungsgesetzes eingerichtet und hat am 1. März 2001 ihre Tätigkeit aufgenommen. Mit 3. März 2011 wurde die Energie-Control Austria in eine Anstalt öffentlichen Rechts umgewandelt (§ 2, § 43 Energie-Control Gesetz). Die Energie-Control Austria hat die Aufgabe, die Umsetzung der Liberalisierung des österreichischen Strom- und Gasmarktes zu überwachen, zu begleiten und gegebenenfalls regulierend einzugreifen. Für die gesicherte Kommunikation mit den von der Energie-Control Austria beaufsichtigten Unternehmen und anderen Kommunikationspartnern betreibt die Energie-Control Austria den in diesem Sicherheits- und Zertifizierungskonzept beschriebenen Zertifizierungsdienst E-Control Certification Services sowie einen Zeitstempeldienst (E-Control Timestamping Services). Diese Dienstleistungen werden von der Energie-Control Austria in nicht kommerzieller Weise erbracht.

Kontaktinformationen: Energie-Control Austria, Rudolfsplatz 13a, 1010 Wien, https://cert-services.e-control.at/, Tel. +43 1 24724-0, Fax +43 1 24724-900, cert.services@e-control.at

Anträge auf Widerruf eines Zertifikates sind an die E-Mail-Adresse cert.revocation@e-control.at zu richten.

Alle für den Zertifizierungsdienst E-Control Certification Services relevanten Informationen, insbesondere die jeweils aktuelle Fassung dieses Sicherheits- und Zertifizierungskonzepts, werden auf der Website der Energie-Control Austria, https://cert-services.e-control.at/, veröffentlicht.

Bei der Ausstellung von Zertifikaten werden jedenfalls die Policy-Vorgaben des Root-CA-Betreibers e-commerce monitoring GmbH beachtet. Die aktuelle Policy des Root-CA-Betreibers findet sich unter:

- GLOBALTRUST® Certificate Policy (OID=1.2.40.0.36.1.1.8.1)

http://www.globaltrust.eu/static/globaltrust-certificate-policy.pdf

- GLOBALTRUST® Practice Statement (OID=1.2.40.0.36.1.2.3.1)

http://www.globaltrust.eu/static/globaltrust-practice-statement.pdf

1.2 Haftung

Die Energie-Control Austria erbringt den Zertifizierungsdienst E-Control Certification Services nicht kommerziell und schließt daher jegliche Haftung aus.

1.3 Verpflichtungen der Signatoren

Die Bedingungen, zu denen Zertifikate ausgestellt werden, sind in Kapitel 3.3 dieses Sicherheits- und Zertifizierungskonzepts genannt.

1.4 Verpflichtungen von Personen, die auf Zertifikate vertrauen

Die ausgestellten Zertifikate entsprechen dem Standard X.509 v3. Information darüber, welche Zertifikate widerrufen wurden, wird in Form von Widerrufslisten im Format X.509 v2 veröffentlicht. Personen, die auf Zertifikate des Zertifizierungsdienstes E-Control Certification Services vertrauen, sollen Software verwenden, welche die Zertifikate interpretieren kann und welche die aktuelle Widerrufsliste abruft und interpretiert.

Es sei darauf hingewiesen, dass die beim Zertifizierungsdienst E-Control Certification Services ausgestellten Zertifikate den Namen des Signators (oder ein Pseudonym) enthalten und optional auch einen Hinweis auf eine Organisation enthalten können, für welche der Signator tätig ist. Bei der Ausstellung des Zertifikates wird die Identität des Signators anhand einer Kopie eines Lichtbildausweises und eines telefonischen Kontrollanrufs überprüft (siehe Kapitel 3.2). Zur optional eingetragenen Organisation wird nur (durch Kontrollanruf) überprüft, ob der Signator für diese Organisation tätig ist. Es wird nicht überprüft, welche Position der Signator innerhalb der Organisation einnimmt und inwieweit er bevollmächtigt ist, für die Organisation zu handeln.

Informationen zum Zertifizierungsdienst, insbesondere die jeweils aktuelle Version dieses Sicherheits- und Zertifizierungskonzepts, werden auf der Website der Energie-Control Austria, https://cert-services.e-control.at/, veröffentlicht.

2 SCHLÜSSELMANAGEMENT

2.1 Generierung der Schlüssel für den Zertifizierungsdienst

Alle Schlüsselpaare, die für einen Zertifizierungsdienst der Energie-Control Austria erzeugt werden, werden in gesicherter Umgebung im Serverraum der Energie-Control Austria (siehe Kapitel 4.4) unter Wahrung des Vier-Augen-Prinzips von zwei Personen erzeugt, die mit der Rolle eines Systemadministrators betraut wurden (siehe Kapitel 4.3).

Die Schlüsselgenerierung erfolgt auf einem Server des Zertifizierungsdienstes. Bei der Schlüsselgenerierung wird der private Schlüssel so in die Signaturerstellungseinheit eingebracht, dass er daraus nicht mehr exportiert werden kann. Weiters wird ein Backup des privaten Schlüssels erstellt (siehe Kapitel 2.2). Außerhalb der für die Speicherung des privaten Schlüssels vorgesehenen Signaturerstellungseinheit wird dieser auf dem Server des Zertifizierungsdienstes nicht gespeichert. Die Sicherheitsanforderungen an den Server und die Signaturerstellungseinheit sind in Kapitel 4.7 beschrieben.

Bei der Auswahl der Algorithmen und Parameter werden die Anfordungen der einschlägigen internationalen Standards und Empfehlungen beachtet. Für den Zertifizierungsdienst E-Control Certification Services wird derzeit der Algorithmus RSA mit einer Schlüssellänge von mind. 2048 Bit verwendet.

2.2 Speicherung, Backup und Wiederherstellung von Schlüsseln

Die privaten Schlüssel der Zertifizierungsdienste der Energie-Control Austria werden in einer eigenen Signaturerstellungseinheit gespeichert (vgl. Kapitel 4.7). Die Schlüssel können aus dieser Signaturerstellungseinheit nicht ausgelesen werden.

Bei der Generierung des privaten Schlüssels wird ein Backup des Schlüssels erstellt (siehe Kapitel 2.1). Das Backup wird in einem verschlossenen Kuvert in einem Bankschließfach hinterlegt. Im Fall eines Defekts der Signaturerstellungseinheit wird das Backup in eine neue Signaturerstellungseinheit eingebracht und der Datenträger wiederum im Bankschließfach hinterlegt.

Für sämtliche Vorgänge im Zusammenhang mit den privaten Schlüsseln der Zertifizierungsdienste, insbesondere für die Erzeugung (siehe Kapitel 2.1) und Speicherung dieser Schlüssel und die Aktivierung der Signaturerstellungseinheiten, die Erstellung des Backups des Schlüsselpaars, die Lagerung des Backups im Bankschließfach und die Wiederherstellung des Systems ist ein Vier-Augen-Prinzip vorgesehen.

Das Vier-Augen-Prinzip wird organisatorisch dadurch abgesichert, dass die Systemadministratoren durch Dienstanweisung dazu verpflichtet werden, Handlungen im Zusammenhang mit privaten Schlüsseln der Zertifizierungsdienste ausschließlich zu zweit vorzunehmen. Jene Personen, die Zugang zum Serverraum oder zum Bankschließfach haben, ohne mit der Rolle eines Systemadministrators betraut zu sein, werden ebenfalls durch Dienstanweisung dazu angehalten, die Server der Zertifizierungsdienste nicht zu verändern, die Signaturerstellungseinheit nicht vom Server zu entfernen und das im verschlossenen Kuvert im Bankschließfach aufbewahrte Backup des privaten Schlüssels nicht daraus zu entfernen. Zum Serverraum und zum Bankschließfach haben nur sehr wenige Personen Zutritt, gegen unbefugten Zutritt wird der Serverraum durch technische Maßnahmen, das Bankschließfach durch technische und organisatorische Maßnahmen der Bank geschützt.

2.3 Verteilung der öffentlichen Schlüssel

Das von der Root-CA signierte Wurzelzertifikat der Energie-Control Austria sowie die von der Root-CA für den Zertifizierungsdienst E-Control Certification Services und den Zeitstempeldienst E-Control Timestamping Services ausgestellten Zertifikate werden auf der Website der Energie-Control Austria, https://cert-services.e-control.at/, veröffentlicht.

2.4 Schlüsselhinterlegung

Die Energie-Control Austria speichert keine privaten Schlüssel von Signatoren.

2.5 Schlüsselverwendung

Die privaten Schlüssel der Energie-Control Austria, die in diesem Kapitel 2 beschrieben werden, werden ausschließlich für die Erbringung des jeweiligen Zertifizierungsdienstes verwendet. Insbesondere wird der private Schlüssel des Zertifizierungsdienstes E-Control Certification Services ausschließlich zur Signatur von Zertifikaten und von Widerrufslisten verwendet. Die Verwendung erfolgt ausschließlich in der in diesem Konzept beschriebenen Signaturerstellungseinheit (siehe Kapitel 4.7) und ausschließlich in gesicherter Umgebung (siehe Kapitel 4.4).

2.6 Ende des Lebenszyklus der privaten Schlüssel

Die Schlüssel der Zertifizierungsdienste der Energie-Control Austria werden jedenfalls dann außer Betrieb genommen, wenn die verwendeten asymmetrischen Algorithmen, die Schlüssellängen oder die in den für die Schlüssel ausgestellten Zertifikaten verwendeten Hash-Verfahren nicht mehr ausreichend sicher erscheinen. Die Energie-Control Austria orientiert sich dabei sowohl an den einschlägigen rechtlichen Vorschriften als auch an einschlägigen internationalen Empfehlungen.

Die Energie-Control Austria kann auch aus anderen Gründen jederzeit ein Schlüsselpaar außer Betrieb nehmen, z. B. wegen Änderungen der Hardware oder Software oder wegen der Einstellung des Betriebs.

Wird ein Schlüsselpaar außer Betrieb genommen, dann stellen die Systemadministrator sicher, dass der private Schlüssel aus der Signaturerstellungseinheit zuverlässig gelöscht oder die Signaturerstellungseinheit vernichtet wird, sowie dass alle erstellten Backups (siehe Kapitel 2.2) zuverlässig und nicht wiederherstellbar vernichtet werden. Weiters wird dem neuen Schlüsselpaar von der Root-CA ein neues Zertifikat ausgestellt. Das Zertifikat, welches die Root-CA dem alten Schlüsselpaar ausgestellt hat, wird auf der Widerrufsliste der Root-CA widerrufen.

2.7 Lebenszyklus der eingesetzten Hardware

Wird Hardware, die als Signaturerstellungseinheit verwendet wurde, außer Betrieb genommen, dann müssen alle darauf befindlichen privaten Schlüssel der Energie-Control Austria zuverlässig gelöscht werden. Wenn die Hardware keine zuverlässige Löschung der Schlüssel unterstützt, muss die Hardware vernichtet werden.

2.8 Schlüsselmanagementdienste für Signatoren

Die Energie-Control Austria erbringt keine Schlüsselmanagementdienste für Signatoren.

2.9 Signaturerstellungseinheiten der Signatoren

Die Energie-Control Austria stellt den Signatoren keine Signaturerstellungseinheiten (wie z.B. Chipkarten) zur Verfügung. Es bleibt den Signatoren überlassen, auf welchen Geräten sie ihre privaten Schlüssel speichern.

Im Zuge ihres Antrages auf Ausstellung eines Zertifikates (siehe Kapitel 3.2) müssen sich die Signatoren dazu verpflichten, ihren privaten Schlüssel unter ihrer alleinigen Kontrolle zu halten, indem sie diesen z. B. in verschlüsselter Form speichern und das für die Verwendung des privaten Schlüssels erforderliche Passwort vertraulich behandeln und niemandem weitergeben. Weiters werden die Signatoren dazu verpflichtet, umgehend einen Widerruf ihres Zertifikates (siehe Kapitel 3.5) zu veranlassen, wenn sie die alleinige Kontrolle über ihr Zertifikat verlieren sollten.

3 AUSSTELLUNG UND WIDERRUF VON ZERTIFIKATEN

3.1 Registrierung

Zertifikate des Zertifizierungsdienstes E-Control Certification Services werden ausschließlich an natürliche Personen (die „Signatoren“) ausgestellt. Es besteht die Möglichkeit, im Zertifikat außerdem einen Hinweis auf eine Organisation aufzunehmen, für welche der Signator tätig ist.

Die Ausstellung eines Zertifikates muss über ein Webformular auf der Website der Energie-Control Austria beantragt werden. In dieses Formular müssen die in das Subject-Feld des Zertifikates aufzunehmenden Daten eingetragen werden. Verpflichtend ist die Eintragung des Namens (Vorname, Nachname) und der E-Mail-Adresse. Weiters können die Bezeichnung der Organisation (Firma), der Abteilung, der Stadt, des Bundeslands und des Staats eingetragen werden. Im Feld „CommonName“ (CN) kann auch optional ein Pseudonym eingetragen werden. Wenn als Pseudonym nicht ein Wort eingetragen ist, bei dem eindeutig erkennbar ist, dass es sich um eine Funktionsbezeichnung in einem Unternehmen handelt (z. B. „Buchhaltung“, „Rechnungswesen“, „Regulatory Affairs“), dann muss das Pseudonym durch den Zusatz „(Pseudonym)“ unverwechselbar als solches gekennzeichnet werden.

Vor der Antragstellung wird der Signator über die Bedingungen für die Ausstellung und Nutzung der Zertifikate informiert (siehe Kapitel 3.3) und muss diesen Bedingungen mit seinem Antrag zustimmen. Die Bedingungen sind in deutscher Sprache abgefasst und werden auf der Website so dargestellt, dass der Signator sie abspeichern und ausdrucken kann.

Nach der Antragstellung über die Website überprüft die Energie-Control Austria die Identität des Signators und (falls diese im Zertifikat ausgewiesen werden soll) auch seine Zugehörigkeit zu einer Organisation (Firma). Dazu wird der Signator aufgefordert, eine Kopie eines gültigen amtlichen Lichtbildausweises an die Energie-Control Austria zu faxen.

In Fällen, wo die Identität der Antragsteller dem Geschäftsführer und dem Leiter der Stabstelle IT&TK bekannt ist (z. B. Mitarbeiter der Energie-Control Austria, BMWA-Mitarbeiter, langjährige Lieferanten oder Ansprechpartner in Behörden und bei Marktteilnehmern u. ä.) kann die Energie-Control Austria auf die Überprüfung der Identität verzichten.

Ein Systemadministrator überprüft den elektronisch eingelangten Antrag auf Ausstellung eines Zertifikates und den eingelangten amtlichen Lichtbildausweis. Da die Zertifikate im Regelfall für Mitarbeiter von Unternehmen ausgestellt werden, mit denen bereits eine regelmäßige Kommunikationsbeziehung besteht, kann zur Überprüfung teilweise auf das interne elektronische Adressbuch der Energie-Control Austria zurückgegriffen werden. Insgesamt werden die folgenden Überprüfungen vorgenommen:

- Überprüfung des Ausweises: Wenn die übermittelte Kopie schlecht lesbar ist oder nicht alle erforderlichen Daten (Vorname(n), Nachname, Geburtdatum, Geburtsort, Ausstellungsdatum, ausstellende Behörde, Seriennummer) aus der Kopie hervorgehen, wird der Signator telefonisch oder per E-Mail aufgefordert, nochmals eine Kopie zu übermitteln.

- Name: Geprüft wird die Übereinstimmung des im Zertifikatsantrag übermittelten Namens (Vorname(n) und Nachname) mit der Schreibweise im amtlichen Lichtbildausweis. Wenn die Namensschreibweise nicht übereinstimmt, wird der Signator per E-Mail oder Telefon aufgefordert, das Webformular neu auszufüllen.

- Pseudonym: Wenn im Namensfeld kein Name, sondern ein Pseudonym angegeben ist, wird überprüft, ob Verwechslungsgefahr besteht. Wenn eindeutig erkennbar ist, dass es sich um eine Funktionsbezeichnung in einem Unternehmen handelt (z. B. „Buchhaltung“, „Rechnungswesen“, „Regulatory Affairs“), dann ist keine ausdrückliche Kennzeichnung als Pseudonym erforderlich. Wenn es sich nicht um eine solche Funktionsbezeichnung handelt, dann muss das Pseudonym mit dem Zusatz „(Pseudonym)“ gekennzeichnet werden. Keinesfalls darf das Pseudonym anstößig sein, Verwechslungsgefahr mit anderen Personen bestehen oder in fremde Namens- oder Markenrechte eingegriffen werden. Wenn das Pseudonym diesen Kriterien nicht entspricht, wird der Signator per E-Mail oder Telefon aufgefordert, das Webformular neu auszufüllen.

- E-Mail-Adresse: Der Systemadministrator prüft die E-Mail-Adresse gegen das interne elektronische Adressbuch der Energie-Control Austria. Wenn dort keine E-Mail-Adresse eingetragen ist, sendet der Systemadministrator an die E-Mail-Adresse eine E-Mail mit der Aufforderung, den Empfang zu bestätigen.

- Organisation (Firma): Wenn im Zertifikatsantrag ein Eintrag für das Organisation-Attribut im Zertifikat enthalten ist, dann nimmt der Systemadministrator folgende Überprüfungen vor: Wenn die Organisation bereits im internen elektronischen Adressbuch der Energie-Control Austria eingetragen ist und die Schreibweise im Adressbuch und im Zertifikatsantrag übereinstimmt, dann ist keine weitere Überprüfung der Organisation erforderlich. Wenn die Schreibweisen voneinander abweichen, dann wird die korrekte Schreibweise anhand eines amtlichen Registerauszugs (z. B. Firmenbuchauszug) überprüft. Wenn kein Registerauszug vorhanden ist, wird der Signator aufgefordert, einen entsprechenden Nachweis beizubringen. Es ist zulässig, die Bezeichnung der Organisation im Zertifikat abzukürzen, wenn dadurch keine Verwechslungsgefahr entsteht. Es ist insbesondere erforderlich, eine Kurzform zu verwenden, wenn sonst die Maximallänge von 64 Zeichen für den Organisationseintrag im Zertifikat überschritten würde.

- Abteilung (OrganisationalUnit): Der Signator kann frei wählen, was im OrganisationalUnit-Attribut (OU) des Zertifikates eingetragen wird. Der Signator darf dieses Feld allerdings nur verwenden, wenn er auch ins Feld Organisation/Firma etwas eingetragen hat (das wie oben beschrieben überprüft wird). Der Eintrag darf weiters nicht missverständlich, irreführend oder anstößig sein. Insbesondere darf es sich nicht um den Namen einer Person oder eines Unternehmens handeln. Der Name einer natürlichen Person darf im Zertifikat nur in dem für den Namen des Signators vorgesehenen Attribut (CommonName) eingetragen werden, der Name einer juristischen Person nur im Organisation-Attribut.

- Stadt und Bundesland: Wenn im Zertifikatsantrag eine Stadt bzw. ein Bundesland eingetragen ist, dann wird diese gegen das interne elektronische Adressbuch der Energie-Control Austria geprüft. Es muss sich dabei entweder um den Wohnsitz des Signators oder eine Niederlassung der im Zertifikat eingetragenen Organisation handeln. Wenn sich die Stadt bzw. das Bundesland nicht durch das interne elektronische Adressbuch bestätigen lassen, kann der Signator entweder aufgefordert werden, einen geeigneten Nachweis zu übersenden, oder das Zertifikat kann ohne diese Zusätze ausgestellt werden.

- Staat: Als Staat wird im Zertifikat jener Staat eingetragen, der den vom Signator vorgelegten Lichtbildausweis ausgestellt hat. „AT“ für Österreich kann aber auch dann eingetragen werden, wenn im Zertifikat eine Organisation eingetragen wird, die ihren Sitz in Österreich hat.

- Algorithmen und Parameter: Der im Zertifikatsantrag übermittelte öffentliche Schlüssel muss dem Verfahren RSA entsprechen und eine Schlüssellänge von mindestens 2048 Bit aufweisen. Auf Anfrage und nach Maßgabe der technischen Möglichkeiten kann die Energie-Control Austria auch andere Algorithmen oder Parameter akzeptieren.

- Kontrollanruf: Um sicherzustellen, dass der Antrag vom Signator stammt und dass der Signator für die Organisation (Firma) tätig ist, die er im Webformular angegeben hat, ruft der Systemadministrator den Signator zurück. Die Rufnummer wird dabei dem internen elektronischen Adressbuch der Energie-Control Austria entnommen. Wenn dort zur betreffenden Organisation keine Telefonnummer eingetragen ist, schlägt der Systemadministrator die Telefonnummer im Telefonbuch nach. Beim Kontrollanruf teilt der Systemadministrator dem Signator auch allfällige Fehler mit, die bei den oben genannten Überprüfungen hervorgekommen sind. Wenn sich alle Überprüfungen als erfolgreich herausgestellt haben, teilt der Systemadministrator dem Signator mit, wann und wo er sein Zertifikat herunterladen kann.

Der Systemadministrator verweigert die Ausstellung des Zertifikates in den folgenden Fällen:

- wenn Zweifel an der Echtheit des übermittelten Ausweises bestehen, oder wenn die übermittelte Ausweiskopie schlecht lesbar ist oder nicht alle erforderlichen Daten abdeckt

- wenn der Signator nicht unter einer bereits im internen elektronischen Adressbuch erfassten oder aus dem Telefonbuch herausgesuchten Telefonnummer zurückgerufen werden kann, oder wenn sich im Telefonat herausstellt, dass der Antrag nicht vom Signator stammt oder

- wenn die im Zertifikat einzutragenden Daten nicht wie oben beschrieben verifiziert werden konnten, insbesondere wenn die Namensschreibweise im Zertifikat nicht mit der Ausweiskopie übereinstimmt, wenn ein gewähltes Pseudonym oder Domainname nicht den oben genannten Regeln entspricht oder wenn die einzutragende Organisation nicht wie oben beschrieben verifiziert werden konnte (z. B. wenn die Organisation nicht bereits bekannt ist und auch kein Registerauszug vorgelegt wird oder wenn Zweifel bestehen, dass der Signator für diese Organisation tätig ist),

- wenn der vom Signator im Zertifikatsantrag übermittelte öffentliche Schlüssel nicht einem der von der Energie-Control Austria akzeptierten Algorithmen (siehe oben) entspricht oder eine zu geringe Schlüssellänge aufweist.

- Die Energie-Control Austria kann auch darüber hinaus die Ausstellung von Zertifikaten ohne Angaben von Gründen verweigern. Da der Zertifizierungsdienst nicht kommerziell erbracht wird, kann die Energie-Control Austria die Ausstellung von Zertifikaten insbesondere dann verweigern, wenn der Antragsteller nicht zum beabsichtigten Adressatenkreis gehört.

Wenn die oben beschriebenen Überprüfungen erfolgreich waren, stellt der Systemadministrator das Zertifikat aus. Beim zuvor durchgeführten Kontrollanruf wird dem Signator mitgeteilt, wann und wie er das Zertifikat abholen kann.

3.2 Ausstellen von Zertifikaten

Die im Rahmen des Zertifizierungsdienstes E-Control Certification Services ausgestellten Zertifikate entsprechen dem Standard X.509 v3.

Die Zertifikate enthalten insbesondere folgende Felder und Attribute:

- Im Ausstellerfeld (Issuer) die Bezeichnung des Ausstellers (O=Energie-Control Austria), des Zertifizierungsdienstes (CN=E-Control Certification Services) und den Code für den Staat, in welchem die Energie-Control Austria ihren Sitz hat (C=AT)

- Im Antragsteller-Feld (Subject) wird jedenfalls im Attribut CommonName (CN) der Name des Signators oder ein Pseudonym eingetragen. Im Organisation-Attribut (O) kann eine Organisation eingetragen werden, für welche der Signator tätig ist. Im OrganisationalUnit-Attribut (OU) kann eine vom Signator frei gewählte Bezeichnung der Abteilung innerhalb der Organisation eingetragen werden. Weiters können die E-Mail-Adresse des Signators, Stadt, Bundesland und Staat eingetragen werden. Die Überprüfung der einzelnen Attribute ist oben in Kapitel 3.1 beschrieben.

- Als Beginn des Gültigkeitszeitraums des Zertifikates wird der Zeitpunkt der Ausstellung des Zertifikates eingetragen. Der Gültigkeitszeitraum der ausgestellten Zertifikate beträgt zwei Jahre, wobei SHA-1 basierte Zertifikate nur bis 31.12.2015 ausgestellt werden und maximal bis 31.12.2016 gültig sind.

- Die ausgestellten Zertifikate enthalten jeweils einen Verweis auf die URL, an der die Widerrufsliste abgerufen werden kann.

3.3 Bedingungen für die Ausstellung von Zertifikaten

Mit dem Antrag auf Ausstellung eines Zertifikates muss der Signator den folgenden Bedingungen zustimmen:

- Die im Rahmen des Zertifizierungsdienstes E-Control Certification Services ausgestellten Zertifikate werden natürlichen Personen für deren alleinige Nutzung ausgestellt. Der Signator ist verpflichtet, seinen privaten Schlüssel unter seiner alleinigen Kontrolle zu halten, z. B. indem der private Schlüssel in verschlüsselter Form gespeichert wird und das zur Verwendung des privaten Schlüssels erforderliche Passwort geheim gehalten wird. Ob die Speicherung auf der Festplatte des Signators erfolgt oder ob der Signator eigene Hardware einsetzt, bleibt dem Signator überlassen.

- Der Signator ist verpflichtet, umgehend einen Widerruf seines Zertifikates zu veranlassen, wenn er die alleinige Kontrolle über den privaten Schlüssel verliert oder wenn sich die im Zertifikat bescheinigten Daten ändern, insbesondere wenn sich der Name des Signators oder die Bezeichnung der im Zertifikat genannten Organisation ändern oder wenn der Signator nicht mehr für die im Zertifikat genannte Organisation tätig ist.

- Der Signator nimmt zur Kenntnis, dass die Energie-Control Austria sich zwar bemühen wird, einen Antrag auf Widerruf während der Geschäftszeiten rasch zu behandeln, dass das Sicherheits- und Zertifizierungskonzept für den Zertifizierungsdienst E-Control Certification Services aber keine rasche Durchführung garantiert. Insbesondere ist für den Fall eines Gesamtausfalls des Dienstes vorgesehen, dass das System binnen maximal vierzehn Tagen wiederhergestellt wird.

- Die ausgestellten Zertifikate sind primär zur Sicherung der Kommunikation zwischen dem Signator und der Energie-Control Austria gedacht. Der Signator kann das ihm ausgestellte Zertifikat darüber hinaus auch für beliebige andere Zwecke verwenden, die Energie-Control Austria schließt aber sowohl gegenüber dem Signator als auch gegenüber allfälligen Kommunikationspartnern des Signators, welche den Zertifikaten vertrauen, jegliche Haftung aus.

- Zur Überprüfung der Gültigkeit der ausgestellten Zertifikate können vom Signator und anderen Personen, die dem Zertifikat vertrauen, beliebige Produkte verwendet werden, welche den Standard X.509 unterstützen. Dabei ist darauf zu achten, dass die Produkte auch die jeweils aktuelle Widerrufsliste (CRL) überprüfen. Grundsätzlich soll die Zertifikatskette bis hinauf zum Wurzelzertifikat der Root-CA geprüft werden.

- Zur Generierung des privaten Schlüssels werden geeignete sichere Verfahren angewandt, die eine ausreichende Zufallsqualität bei der Schlüsselerzeugung gewährleisten. Insbesondere sind dies ausdrücklich dafür vorgesehene Hardware- oder Softwarekomponenten, die es erlauben durch Systemereignisse die Zufallsqualität zu erhöhen (Angabe von Dateien mit Zufallszahlen, Durchführen von Mausbewegungen oder Tastaturanschlägen während der Schlüsselgenerierung). Energie-Control Austria behält sich vor, vom Signator vollständige Auskunft über den Schlüsselgenerierungsvorgang zu verlangen und bei Bedenken bezüglich der Zufallsqualität des Schlüssels einen Zertifizierungsantrag abzulehnen.

- Weiters wird der Signator auf dieses Sicherheits- und Zertifizierungskonzept verwiesen.

Die oben genannten Bedingungen und dieses Sicherheits- und Zertifizierungskonzept werden auf der Website der Energie-Control Austria so bereitgestellt, dass sie vom Signator abgespeichert und ausgedruckt werden können.

3.4 Verzeichnisdienst

Die Energie-Control Austria betreibt keinen Verzeichnisdienst, in dem Zertifikate der Signatoren veröffentlicht werden. Veröffentlicht werden auf der Website https://cert-services.e-control.at/ lediglich die Zertifikate der Root-CA, die von der Root-CA ausgestellten Zertifikate für Zwischenzertifizierungsstellen und die Widerrufslisten der Root-CA und der Zwischenzertifizierungsstellen.

3.5 Widerruf von Zertifikaten

Die im Rahmen des Zertifizierungsdienstes E-Control Certification Services ausgestellten Zertifikate werden in den folgenden Fällen widerrufen:

- Ein Signator kann jederzeit einen Widerruf seines Zertifikates verlangen.

- Die Energie-Control Austria nimmt einen Widerruf vor, wenn sie erfährt, dass im Zertifikat bescheinigte Umstände nicht mehr zutreffen, dass das Zertifikat auf Grund unrichtiger Angaben erwirkt wurde, dass der Signator verstorben ist oder dass die Gefahr einer missbräuchlichen Verwendung des Zertifikates besteht (z. B. weil der Signator die alleinige Kontrolle über seinen privaten Schlüssel verloren hat).

- Da der Zertifizierungsdienst nicht kommerziell betrieben wird, behält sich die Energie-Control Austria darüber hinaus vor, Zertifikate jederzeit ohne Angabe von Gründen widerrufen zu können, insbesondere im Fall der Einstellung des Betriebs (siehe Kapitel 4.9).

Ein Widerruf kann vom Signator jederzeit durch eine an die in Kapitel 1.1 genannte E-Mail-Adresse gerichtete E-Mail verlangt werden. Sofern der Signator noch in der Lage ist, eine auf seinem Zertifikat basierende Mailsignatur zu erstellen, soll er dafür sein Zertifikat verwenden. Der Systemadministrator, der den Widerruf durchführen soll, prüft die Signatur der E-Mail. Wenn die Signatur gültig ist und unzweifelhaft der Widerruf des Zertifikates verlangt wird, wird der Widerruf unverzüglich durchgeführt, ohne dass eine weitere Überprüfung vorgenommen wird. Wenn die E-Mail unsigniert ist oder berechtigte Zweifel an Echtheit des Widerrufs bestehen oder ein Widerrufsantrag in anderer Form einlangt, dann wird der Systemadministrator vor der Durchführung des Widerrufs durch einen Kontrollanruf beim Signator überprüfen, dass der Widerrufsantrag tatsächlich vom Signator stammt. Wenn ein Widerrufsantrag ausschließlich telefonisch eingebracht wird, dann soll der Anrufer dazu aufgefordert werden, seinen Wunsch durch eine (nach Möglichkeit signierte) E-Mail auf die im Kapitel 1.1 genannte E-Mail-Adresse gerichtete E-Mail zu bestätigen.

Eine Organisation, die in einem Zertifikat genannt ist, kann ohne Angabe von Gründen (insbesondere aber, wenn der im Zertifikat genannte Signator nicht mehr für sie tätig ist) den Widerruf des Zertifikates verlangen. Der Systemadministrator, der den Widerruf durchführt, soll vorher durch einen Kontrollanruf überprüfen, dass der Widerrufsantrag tatsächlich von der entsprechenden Organisation stammt.

Darüber hinaus kann jede Person die Energie-Control Austria darauf hinweisen, dass in Zertifikat bescheinigte Umstände unrichtig sind, z. B. dass sich der Name des Signators oder die Bezeichnung (Firma) der Organisation geändert haben. Daraufhin wird von einem Systemadministrator geprüft, ob die Behauptung zutrifft (z. B. durch Kontrollanruf beim Signator, durch Kontrollanruf bei der Organisation oder durch Rückfrage in der Rechtsabteilung, ob der Energie-Control Austria aus ihrer aufsichtsbehördlichen Funktion bereits entsprechende Informationen vorliegen). Wenn die im Zertifikat eingetragenen Daten nicht mehr zutreffen, ist das Zertifikat zu widerrufen.

In jedem Fall wird der betroffene Signator von einem Widerruf mittels E-Mail verständigt. Wenn der Widerruf von einer im Zertifikat eingetragenen Organisation verlangt wurde, wird auch diese darüber verständigt, dass der Widerruf vorgenommen wurde.

Die Energie-Control Austria wird sich bemühen, einlangende Widerrufsanträge möglichst rasch zu bearbeiten. Die Systemadministratoren werden angewiesen, Widerrufsanträge prioritär zu behandeln. Nachdem ein Widerrufsantrag von einem Systemadministrator bearbeitet wurde, wird vom System umgehend eine neue Widerrufsliste erstellt und veröffentlich. Da die Energie-Control Austria den Zertifizierungsdienst E-Control Certification Services nicht kommerziell betreibt, kann aber nur im Falle eines unzweifelhaften Widerrufansuchens durch Signator ein unverzüglicher Widerruf gewährleistet werden. Ansonsten kann keine kurze Bearbeitungszeit garantiert werden. Insbesondere werden Widerrufe, die nicht vom Signator selbst eingebracht wurden oder falls der Widerruf nur nach Rückfragen erfolgen kann nur an Werktagen durchgeführt. Weiters kann es, da für den Server des Zertifizierungsdienstes kein Zweitgerät bereit gehalten wird, im Fall eines Totalausfalls des Systems einge Tage dauern, bis ein Ersatzsystem in Betrieb genommen werden kann (siehe Kapitel 4.8). Im Extremfall kann es daher bis zu 14 Tagen dauern, bis ein einlangender Widerruf bearbeitet und veröffentlicht wird. Dementsprechend wird in die einzelnen Widerrufslisten als Zeitpunkt der nächsten Aktualisierung ein 14 Tage in der Zukunft liegender Zeitpunkt eingetragn. Im Regelbetrieb wird allerdings mehrmals täglich eine neue Widerrufsliste ausgestellt.

Es ist nicht vorgesehen, dass Zertifikate vorläufig gesperrt werden und die Sperre wieder aufgehoben werden kann. Wenn ein Zertifikat einmal widerrufen wurde, kann dieser Status nicht mehr geändert werden. Dem Signator kann nach neuerlicher Registrierung ein neues Zertifikat ausgestellt werden (vgl. Kapitel 3.1).

4 MANAGEMENT UND BETRIEB

4.1 Sicherheitsmanagement

Die Energie-Control Austria hat eine Risikoanalyse vorgenommen, um die notwendigen Sicherheitsmaßnahmen zu ergreifen.

Die Energie-Control Austria trägt die Gesamtverantwortung für den Zertifizierungsdienst E-Control Certification Services. Der Zertifizierungsdienst wird in den Räumlichkeiten der Energie-Control Austria erbracht. Die Energie-Control Austria ist die einzige Registrierungsstelle, es gibt keine an andere Einrichtigungen ausgelagerten Registrierungsstellen. Soweit für den Zertifizierungsdienst Dienstleistungen anderer Unternehmen herangezogen werden (Internet-Anbindung, Hardware- und Softwaresupport), wird bei der Vertragsgestaltung auf die Einhaltung der Anforderungen aus diesem Sicherheits- und Zertifizierungskonzept geachtet, insbesondere wird Fremdpersonal beim Hardware- und Softwaresupport beaufsichtigt.

Die Weiterentwicklung dieses Sicherheits- und Zertifizierungskonzeptes sowie die Qualitätssicherung obliegt dem Leiter der Stabsstelle IT & TK. Dieser zieht dazu einen Mitarbeiter der Rechtsabteilung bei. Änderungen des Sicherheits- und Zertifizierungskonzepts werden vom Leiter der Stabsstelle IT & TK beschlossen. Bei Änderungen des Sicherheits- und Zertifizierungskonzepts wird jeweils eine neue Versionsnummer vergeben.

4.2 Vom Sicherheitskonzept umfasste Einrichtungen

Die folgenden Einrichtungen werden für die Erbringung der Zertifizierungsdienste benötigt und sind daher vom Sicherheitskonzept umfasst:

- Der Zertifizierungsdienst E-Control Certification Services und der Zeitstempeldienst E-Control Timestamping Services werden auf einem Server betrieben, an den eine Funkuhr sowie eine Signaturerstellungseinheit (siehe Kapitel 4.7) angeschlossen ist. Der Server befindet sich im Serverraum der Energie-Control Austria. In diesem Raum befinden sich auch die für die Internet-Anbindung erforderlichen Einrichtungen (Router) und die Firewall. Weiters befindet sich im Serverraum ein Archivsystem, das für alle Daten der Energie-Control Austria, unter anderem auch für die bei den Zertifizierungsdiensten archivierten Daten (siehe Kapitel 0), genutzt wird. Die gesamte Netzwerkverkabelung zwischen den erwähnten Geräten sowie die Switches befinden sich ebenfalls innerhalb des Serverraums.

- In einem Bankschließfach werden unter anderem auch Backups (Images) der Server hinterlegt.

4.3 Personelle Sicherheit

Sämtliche Aufgaben im Zusammenhang mit den Zertifizierungsdiensten der Energie-Control Austria dürfen nur von Personen durchgeführt werden, die mit der Rolle eines Systemadministrators oder eines Systemoperators betraut wurden. Voraussetzung dafür ist das erforderliche Fachwissen und die erforderliche Erfahrung und Zuverlässigkeit. Die Betrauung mit der Rolle eines Systemadministrators oder eines Systemoperators erfolgt durch den Leiter der Stabsstelle IT & TK; dieser kann die Rolle auch selbst wahrnehmen.

Zu den Aufgaben eines Systemadministrators gehören sämtliche in diesem Sicherheits- und Zertifizierungskonzept genannten Aufgaben. Im Regelfall kann ein Systemadministrator die Aufgaben, mit denen er betraut wurde, alleine wahrnehmen. Für die Erzeugung und Speicherung der privaten Schlüssel der Zertifizierungsdienste, das Backup dieser Schlüssel und die Wiederherstellung sowie die Aktivierung der Signaturerstellungseinheiten sieht Kapitel 2 dieses Sicherheits- und Zertifizierungskonzepts ein Vier-Augen-Prinzip vor. Systemadministratoren haben Zugang zum Serverraum und zum Bankschließfach.

Mit Aufgaben der laufenden Betriebssystemwartung (Einspielen von Updates oder Patches) kann anstelle eines Systemadministrators auch ein Systemoperator betraut werden. Ein Systemoperator darf keine darüber hinaus gehenden Aufgaben wahrnehmen, insbesondere nicht die privaten Schlüssel der Zertifizierungsdienste erzeugen oder Zertifikate ausstellen bzw. widerrufen. Systemoperatoren haben Zugang zum Serverraum, aber nicht zum Bankschließfach.

Personen, die nicht mit der Rolle eines Systemadministrators oder Systemoperators betraut wurden, aber dennoch Zugang zum Serverraum oder zum Bankschließfach haben, dürfen die Server der Zertifizierungsdienste nicht verändern und die im verschlossenen Kuvert im Bankschließfach hinterlegten Backups nicht öffnen und nicht aus dem Bankschließfach entfernen.

4.4 Physikalische Sicherheit

Der Serverraum der Energie-Control Austria ist durch ein elektronisches Zutrittskontrollsystem sowie durch ein mechanisches Schloss gegen unbefugten Zutritt geschützt. Die Zutrittsberechtigung wird nur einer kleinen Anzahl von Mitarbeitern der Energie-Control Austria erteilt. Der Serverraum befindet sich in den Geschäftsräumlichkeiten der Energie-Control Austria, die ihrerseits durch verschiedene Sicherheitsmaßnahmen gegen unbefugten Zutritt geschützt werden. Weiters ist der Serverraum mit Brandmeldern, Sensoren gegen Wassereinbruch, einer Alarmanlage und einer Klimaanlage ausgestattet.

Wenn externe Personen Zutritt zum Serverraum benötigen (z. B. für Hardware- oder Softwarewartung), werden sie durch zutrittsberechtigte Personen der Energie-Control Austria beaufsichtigt.

Das Bankschließfach wird durch die Bank gegen Einbruch und sonstigen unbefugten Zutritt geschützt.

4.5 Organisatorische Sicherheitsmaßnahmen

Die Server der Zertifizierungsdienste werden gegen Viren und andere schädliche Software geschützt.

Sicherheitsprobleme sind unverzüglich dem Leiter der Stabsstelle IT & TK zu melden.

Alle verwendeten Datenträger sind gegen ungewollte Beschädigung, Diebstahl und unberechtigten Zugriff zu schützen. Insbesondere ist darauf zu achten, dass Datenträger, die ein Backup von privaten Schlüsseln enthalten, gemäß Kapitel 2.2 und 2.6 behandelt werden (Vier-Augen-Prinzip, Hinterlegung im verschlossenen Kuvert im Bankschließfach, sichere Zerstörung des Datenträges).

4.6 Zugriffsschutz

Der Zugriff auf die Server der Zertifizierungsdienste ist den Systemadministratoren bzw. den Systemoperatoren (siehe Kapitel 4.3) vorbehalten. Die Passwörter dieser Server sind nur den Systemadministratoren und Systemoperatoren bekannt.

Der Server der Zertifizierungsdienste befindet sich in einem eigenen Firewallsegment. Durch die Firewall wird der Zugriff auf die Server auf die unbedingt erforderlichen Protokolle eingeschränkt. Ein Fernzugriff zur Administration der Server ist weder für externe Personen (Softwarewartung) noch für Mitarbeiter der Energie-Control Austria möglich.

Die für den Zertifizierungsdienst E-Control Certification Services verwendete Software stellt Folgendes sicher: Nur ein Systemadministrator, der sich ordnungsgemäß authentifiziert hat, kann ein neues Zertifikat erstellen. Nur solcherart erstellte Zertifikate werden im Verzeichnis veröffentlicht. Nur ein Systemadministrator, der sich ordnungsgemäß authentifiziert hat, kann ein Zertifikat widerrufen.

4.7 Vertrauenswürdige Systeme

Die Energie-Control Austria verwendet für die Speicherung der privaten Schlüssel der Zertifizierungsdienste eigene Signaturerstellungseinheiten. Als Signaturerstellungseinheit wird Hardware ausgewählt, welche für solche Zwecke entwickelt und nach einem international anerkannten Standard (z. B. FIPS 140, Common Criteria) evaluiert und zertifiziert wurde. Der private Schlüssel des Zertifizierungsdienstes E-Control Certification Services wird gemäß der Regelung des Kapitels 2.1 generiert. Die Signaturerstellungseinheit wird mit dem Server so verbunden (z. B. durch Versiegelung), dass sie nicht auf einfache Weise und jedenfalls nicht unbemerkt vom Server getrennt oder durch andere, ähnlich aussehende Hardware ersetzt werden kann.

Auf dem Server des Zertifizierungsdienstes wird nur Software installiert, die für den Betrieb der Zertifizierungsdienste oder verwandte sicherheitsrelevante Aufgaben benötigt wird. Nicht benötigte Dienste des Betriebssystems werden nach Möglichkeit deaktiviert. Die Systemadministratoren und Systemoperatoren achten darauf, dass sicherheitsrelevante Bugfixes und Patches so rasch wie möglich installiert werden. Vor der Installation neuer Softwareversionen und Upgrades wird die entsprechende Software von den Systemadministratoren bzw. Systemoperatoren getestet und daraufhin untersucht, ob die neue Software den Anforderungen dieses Sicherheits- und Zertifizierungskonzepts entspricht.

4.8 Elementarereignisse und Kompromittierung

Bei einem Totalausfall des Systems (z. B. Hardwaredefekt, Feuer) wird umgehend ein neuer Server angeschafft und das System mit Hilfe eines der im Bankschließfach hinterlegten Backups (Images) wiederhergestellt. Für den Fall eines Defekts der Signaturerstellungseinheit wird Ersatzhardware vorrätig gehalten.

Auch die Daten des Archivs der Energie-Control Austria werden regelmäßig im Bankschließfach ausgelagert und können daher im Fall eines Datenverlustes wiederhergestellt werden.

Bei allen schweren Zwischenfällen, unter anderem bei Einbrüchen, Diebstahl, erfolgreichen Hacker-Attacken oder wenn einer der verwendeten kryptographischen Algorithmen gebrochen wird, analysieren die Systemadministratoren, ob durch den Zwischenfall eine Kompromittierung der Sicherheit des Zertifizierungsdienstes, insbesondere des privaten Schlüssels, eingetreten ist. Soweit erforderlich, werden die folgenden Maßnahmen gesetzt:

- Das alte Schlüsselpaar wird widerrufen und ein neues Schlüsselpaar generiert.
- Vom Zwischenfall unmittelbar betroffene Zertifikate werden widerrufen und die betroffenen Signatoren werden darüber informiert.
- Alle Signatoren werden über den Zwischenfall informiert, insbesondere darüber, dass den mit dem alten Schlüsselpaar signierten Zertifikaten und Widerrufslisten nicht mehr uneingeschränkt vertraut werden kann.
- Für die auf die Zertifikate vertrauenden Personen wird auf der Website eine entsprechende Information veröffentlicht.

4.9 Einstellung des Betriebs

Die Energie-Control Austria betreibt den Zertifizierungsdienst E-Control Certification Services nicht kommerziell und behält sich die Möglichkeit vor, den Zertifizierungsdienst jederzeit ohne Angaben von Gründen einzustellen.

Im Fall der Einstellung des Betriebs wird jedenfalls die Ausgabe neuer Zertifikate eingestellt. Ob die bereits ausgestellten Zertifikate noch einige Zeit gültig bleiben oder sofort widerrufen werden, wird die Energie-Control Austria bei der Einstellung des Betriebes entscheiden.

In jedem Fall wird der Widerrufsdienst (siehe Kapitel 3.5) auch über die Einstellung des Betriebes hinaus aufrecht erhalten: Solange noch gültige Zertifikate in Umlauf sind, wird die Energie-Control Austria Widerrufsanträge wie in Kapitel 3.5 beschrieben entgegennehmen und bearbeiten sowie die jeweils aktuelle Widerrufsliste abrufbar halten. Auch dann, wenn alle Zertifikate widerrufen sind, wird die Widerrufsliste noch so lange abrufbar gehalten, bis die Gültigkeitszeiträume sämtlicher ausgestellter Zertifikate abgelaufen sind.

Alle von der Einstellung des Betriebs betroffenen Signatoren werden darüber verständigt. Weiters wird die Energie-Control Austria auf ihrer Website über die Einstellung des Betriebs informieren.

Die privaten Schlüssel der Energie-Control Austria werden zerstört, sobald sie nicht mehr benötigt werden (siehe Kapitel 2.6).

4.10 Übereinstimmung mit rechtlichen Anforderungen

Die Energie-Control Austria hat ihren Sitz in Wien und unterliegt österreichischem Recht. Bei der Erbringung der Zertifizierungsdienste werden insbesondere das Signaturgesetz und die Signaturverordnung sowie das Datenschutzgesetz in der jeweils geltenden Fassung beachtet.

4.11 Protokollierung und Archivierung

Die Energie-Control Austria verfügt über ein zentrales elektronisches Archivierungssystem. In diesem System werden auch die im Folgenden genannten Informationen über den Zertifizierungsdienst E-Control Certification Services archiviert. Die im Archivierungssystem gespeicherten Informationen über die Zertifizierungsdienste der Energie-Control Austria werden über einen Zeitraum von mindestens sieben Jahren nach Einstellung der Zertifizierungsdienste archiviert.

Über sicherheitsrelevante Ereignisse, inbesondere das Aufsetzen der Server, Änderungen der Konfiguration der Server, die Installation neuer Software, das Erzeugen privater Schlüssel, das Erstellen von Backups der Schlüssel, die Wiederherstellung nach Elementarereignissen sowie über sicherheitsrelevante Zwischenfälle, legen die damit befassten Systemadministratoren ein Protokoll an und archivieren dieses.

Zur Ausstellung jedes einzelnen Zertifikates werden die übermittelten Zertifikatsanträge und die ausgestellten Zertifikate archiviert, weiters die übermittelte Ausweiskopie, allfällige weitere übermittelte Dokumente (z. B. ein Registerauszug der Organisation) sowie ein Vermerk darüber, welcher Systemadministrator die Unterlagen geprüft, den Kontrollanruf durchgeführt und das Zertifikat ausgestellt hat.

Zum Widerruf jedes einzelnen Zertifikates wird ein Vermerk archiviert, aus dem hervorgeht, welcher Systemadministrator den Widerruf vorgenommen hat, welches Zertifikat widerrufen wurde und warum das Zertifikat widerrufen wurde (z. B.: Widerrufsantrag vom Signator, Signator hat die im Zertifikat vermerkte Organisation verlassen, Einstellung des Betriebs), allfällige E-Mail- oder sonstige Korrespondenz, Vermerke über Telefonate. Auch die ausgestellten Widerrufslisten werden archiviert.

In Logdateien auf dem Server des Zertifizierungsdienstes ist unter anderem vermerkt, wann sich ein Systemadministrator bzw. Systemoperator beim Betriebssystem angemeldet bzw. abgemeldet hat, wann Zertifikate ausgestellt wurden und wann Widerrufslisten erstellt wurden. Diese Logdateien werden nicht in das Archivsystem übernommen.

Auskünfte über die zu einem Zertifikat bzw. zu einem Widerruf archivierte Information werden in Übereinstimmung mit dem Datenschutzgesetz bzw. dem Signaturgesetz erteilt.