Aufsichtsstelle für elektronische Signaturen

Sicherheits- und Zertifizierungskonzept – Certificate Policy

Version 2.0

12.12.2011

Aufsichtsstelle für elektronische Signaturen
Telekom-Control-Kommission
Mariahilfer Straße 77–79, 1060 Wien, Tel. +43/1/58058-0, Fax: +43/1/58058-9191
http://www.signatur.rtr.at/, signatur@signatur.rtr.at

Inhaltsverzeichnis

1. Einführung

1.1 Überblick

Dieses Dokument enthält die Certificate Policy der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen. Anderen Stellen, welche die Bedingungen dieser Certificate Policy erfüllen und welche Zertifikate für die Schlüssel von Zertifizierungsdiensteanbietern (ZDA) ausstellen, steht es frei, diese Certificate Policy zu übernehmen. Änderungen am vorliegenden Dokument dürfen jedoch ausschließlich durch die Telekom-Control-Kommission oder in deren Auftrag vorgenommen werden.

Diese Policy wurde ursprünglich nach den Vorgaben des Standards ETSI TS 101 456 V1.2.1 (2002-04) „Policy requirements for certification authorities issuing qualified certificates“ erstellt. Die von der Aufsichtsstelle ausgestellten Zertifikate waren allerdings keine qualifizierten Zertifikate im üblichen Sinn, da sie nicht an natürliche Personen, sondern an ZDA für deren Zertifizierungsdienste ausgestellt wurden. Aufgrund einer Novellierung des Signaturgesetzes stellt die Aufsichtsstelle seit 2008 keine qualifizierten Zertifikate aus. Deshalb orientiert sich die Certificate Policy seit Version 1.1 für neu ausgestellte Zertifikate nicht mehr an ETSI TS 101 456 V1.2.1 (2002-04), sondern an ETSI TS 102 042 V1.2.4 (2007-03), „Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates“ bzw. seit Version 2.0 an ETSI TS 102 042 V2.1.2 (2010-04). In Kapitel 2 wird dargestellt, inwieweit die Anforderungen des Standards ETSI TS 102 042 erfüllt sind.

1.2 Identifikation

Bezeichnung des Dokuments: Sicherheits- und Zertifizierungskonzept – Certificate Policy, Version 2.0, 12.12.2011.

Die Certificate Policy wird von der Rundfunk und Telekom Regulierungs-GmbH im Auftrag der Aufsichtsstelle für elektronische Signaturen unter http://www.signatur.rtr.at/ in der Rubrik „Dokumente“ („Repository“) veröffentlicht.

Bei der Versionsnummer wird die Zahl vor dem Punkt als „größere“, jene hinter dem Punkt als „kleinere“ Versionsnummer bezeichnet. Innerhalb einer Zertifikatskette müssen alle Zertifikate nach untereinander verträglichen Versionen der Certificate Policy ausgestellt sein. Versionen mit identischer größerer Versionsnummer sind untereinander verträglich.

Der ASN.1 Object Identifier (OID) für dieses Dokument ist 1.2.040.0.21.0.1.0.2. Die letzte OID-Komponente bezeichnet die größere Versionsnummer der Certificate Policy. OIDs früherer Versionen enthielten auch die kleinere Versionsnummer. Darauf wird ab Version 2.0 aus Gründen der Interoperabilität verzichtet. Zur Identifizierung der für ein Zertifikat geltenden Certificate Policy ist dies auch nicht erforderlich, weil sich die Version aus dem Ausstellungsdatum des Zertifikats ergibt.

Die in ETSI TS 102 042, Punkt 5.2, spezifizierten Object Identifier 0.4.0.2042.1.1, 0.4.0.2042.1.2, 0.4.0.2042.1.3, 0.4.0.2042.1.4 und 0.4.0.2042.1.5 werden nicht verwendet.

1.3 Anwendungsbereiche

1.3.1 Zertifizierungsstellen

Zertifikate nach dieser Certificate Policy werden von einer Stelle zur Überwachung von ZDA im Sinne von Art. 3 Abs. 3 der Richtlinie 1999/93/EG ausgestellt. Eine solche Stelle wird im vorliegenden Dokument kurz als „Aufsichtsstelle“ bezeichnet.

Von einer Aufsichtsstelle können mehrere Zertifizierungsstellen in dem Sinne betrieben werden, dass unterschiedliche Schlüssel zum Signieren der Zertifikate verwendet werden.

Aufsichtsstellen können Zertifikate für ZDA, für die von ihnen erbrachten Zertifizierungsdienste, Zertifikate für eigene Zertifizierungsstellen oder Zertifikate zur Administration einer Public-Key-Infrastruktur ausstellen. Zertifizierungsstellen im Sinne des vorliegenden Dokuments stellen entweder ausschließlich Zertifikate für ZDA bzw. deren Dienste oder ausschließlich Zertifikate für eigene Zertifizierungsstellen oder ausschließlich Zertifikate zur Administration einer Public-Key-Infrastruktur aus.

1.3.2 Registrierungsstellen

Eine Aufsichtsstelle, die nach dieser Certificate Policy Zertifikate ausstellt, kann hierfür auch Registrierungsstellen heranziehen. Die Aufsichtsstelle hat jedoch zumindest zu überwachen, dass die Bestimmungen von ETSI TS 102 042 in der aktuellen Version, insbesondere von Abschnitt 7.3.1, erfüllt werden. Die Registrierungsstellen sind im Certification Practice Statement oder in einem Dokument, auf das im Certification Practice Statement verwiesen wird, anzugeben.

1.3.3 Zertifikatsempfänger

Zertifizierungsstellen im Sinne des vorliegenden Dokuments stellen entweder ausschließlich Zertifikate für ZDA bzw. deren Dienste oder ausschließlich Zertifikate für eigene

Zertifizierungsstellen oder ausschließlich Zertifikate zur Administration einer Public-Key-Infrastruktur aus.

1.3.4 Anwendungsbereich

Zertifikate für ZDA oder für Zertifizierungsstellen können im Zuge der Überprüfung elektronischer Signaturen verwendet werden. Durch das Zertifikat bestätigt die Aufsichtsstelle, dass die Identität des ZDA überprüft worden ist und dass der ZDA Inhaber des im Zertifikat angegebenen Schlüssels ist. Zertifikate für Schlüssel, die ausschließlich zum Signieren von Zertifikatswiderrufslisten verwendet werden, gelten ebenfalls als Zertifikate für Zertifizierungsstellen.

Zertifikate zur Administration einer Public-Key-Infrastruktur dienen zur Authentifizierung von Rechnern oder von Personen, nicht jedoch zum Signieren von Zertifikaten, von Zertifikatswiderrufslisten oder von Dokumenten, die nicht mit der Public-Key-Infrastruktur in Zusammenhang stehen.

1.4 Kontaktinformation

Herausgeber dieses Dokuments ist die bei der Rundfunk und Telekom Regulierungs-GmbH angesiedelte Telekom-Control-Kommission. Die Rundfunk und Telekom Regulierungs-GmbH ist Geschäftsstelle der Telekom-Control-Kommission.

Rundfunk und Telekom Regulierungs-GmbH
Mariahilfer Straße 77–79
A-1060 Wien
Tel.: +43 1 58058 0
Fax.: +43 1 58058 9191
E-Mail: signatur@signatur.rtr.at
Web: http://www.signatur.rtr.at/

2. Verhältnis zu ETSI TS 102 042

2.1 Grundsätzliche Erfüllung des Standards

Die Anwendung dieser Certificate Policy zwingt grundsätzlich zur Einhaltung der Vorgaben der im Standard ETSI TS 102 042 V2.1.2 (2010-04), „Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates“, spezifizierten Lightweight Certificate Policy (LCP). Einige dieser Vorgaben werden in Kapitel 2.2 konkretisiert. In Kapitel 2.3 werden Punkte aus dem Standard angeführt, die bei der Public-Key-Infrastruktur einer Aufsichtsstelle nicht anwendbar sind.

2.2 Abweichungen von ETSI TS 102 042

Da die Zertifikate nicht an Endbenutzer ausgestellt werden, sondern an ZDA, ergeben sich folgende Konkretisierungen der Anforderungen des Standards ETSI TS 102 042 in dessen Punkt 7.3.1:

Für die Identitätsüberprüfung ist bei natürlichen Personen das persönliche Erscheinen des Zertifikatswerbers, bei juristischen Personen das persönliche Erscheinen eines entsprechend Bevollmächtigten erforderlich. Die Identität wird in beiden Fällen anhand eines amtlichen Lichtbildausweises geprüft. Die Vollmacht des Vertreters einer juristischen Person wird auf Plausibilität geprüft, beispielsweise durch einen Firmenbuchauszug oder durch telefonische Rückfrage.

Eine Aufsichtsstelle steht (abgesehen von Fällen der Cross-Zertifizierung mit ausländischen Stellen) üblicherweise nicht in einem vertraglichen Verhältnis zum Zertifikatswerber, sondern in einem durch Rechtsnormen geregelten Aufsichtsverhältnis. Es gibt daher z. B. keine allgemeinen Geschäftsbedingungen oder Entgeltbestimmungen, weshalb diese dem Zertifikatswerber auch nicht im Sinne von Punkt 7.3.1 c) aus ETSI TS 102 042 auf einem dauerhaften Datenträger ausgefolgt werden müssen. Eine Aufsichtsstelle archiviert auch keinen Zertifikatswerbervertrag im Sinne von Punkt 7.3.1 m) aus ETSI TS 102 042, sondern die vom Zertifikatswerber in seinem Antrag zu nennenden Informationen.

Die in Punkt 7.3.1 aus ETSI TS 102 042 genannten Anforderungen werden daher nur sinngemäß angewendet.

2.3 Nicht anwendbare Punkte des Standards ETSI TS 102 042

Eine Reihe von Anforderungen des Standards ETSI TS 102 042 ist innerhalb der Public-Key-Infrastruktur einer Aufsichtsstelle nicht anwendbar:

- Anforderungen zum Backup der privaten Schlüssel (Punkt 7.2.2 des Standards ETSI TS 102 042): Nach der jeweiligen Rechtslage kann der Aufsichtsstelle untersagt sein, dass die für die Erstellung von Zertifikaten verwendeten privaten Schlüssel aus der Signaturerstellungseinheit, in der sie erzeugt wurden, auslesbar sind. Es gibt in solchen Fällen kein Backup der Schlüssel. Punkt 7.2.2 ist daher – soweit Backup und Wiederherstellung betroffen sind – nicht anwendbar.

- Schlüsselhinterlegung (Key escrow, Punkt 7.2.4 des Standards ETSI TS 102 042): Nach der jeweiligen Rechtslage kann der Aufsichtsstelle untersagt sein, dass die für die Erstellung von Zertifikaten verwendeten privaten Schlüssel aus der Signaturerstellungseinheit, in der sie erzeugt wurden, auslesbar sind. Private Schlüssel der Empfänger von Zertifikaten (der ZDA) werden gar nicht gespeichert. Punkt 7.2.4 ist daher nicht anwendbar.

- Schlüsselmanagementdienste (Punkt 7.2.8) und Vorbereitung sicherer Benutzergeräte (Punkt 7.2.9 des Standards ETSI TS 102 042): Eine Aufsichtsstelle erzeugt und verwaltet üblicherweise keine Schlüssel für Dritte. Eine Aufsichtsstelle stellt üblicherweise keine Signaturerstellungseinheiten für Dritte bereit. Die Punkte 7.2.8 und 7.2.9 sind daher nicht anwendbar.

- Veröffentlichung der Geschäftsbedingungen (Punkt 7.3.4 des Standards ETSI TS 102 042): Eine Aufsichtsstelle steht (abgesehen von Fällen der Cross-Zertifizierung mit ausländischen Stellen) üblicherweise nicht in einem vertraglichen Verhältnis zum Zertifikatswerber, sondern in einem durch Rechtsnormen geregelten Aufsichtsverhältnis. Es gibt daher keine allgemeinen Geschäftsbedingungen oder Entgeltbestimmungen. Die rechtlichen Grundlagen, die Certificate Policy und das Certification Practice Statement werden auf der Website der jeweiligen Aufsichtsstelle veröffentlicht. Punkt 7.3.4 wird daher nur sinngemäß erfüllt.

- Datenschutz (verschiedene Punkte des Standards ETSI TS 102 042): Da die Zertifikate nicht an Endbenutzer ausgestellt werden und da der Zweck der Public-Key-Infrastruktur einer Aufsichtsstelle darin liegt, ein Verzeichnis der ZDA zu führen, werden die Daten der Zertifikatswerber (insbesondere Name, Adressen und Zugangsmodalitäten zu deren Verzeichnissen) nicht vertraulich behandelt, sondern auf der Website der Aufsichtsstelle veröffentlicht.