
Aufsichtsstelle für elektronische Signaturen

Sicherheits- und Zertifizierungskonzept – Certificate Policy

Version 1.0

09.09.2002

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

Inhaltsverzeichnis.....	2
1. Einführung.....	2
1.1 Überblick.....	2
1.2 Identifikation	3
1.3 Anwendungsbereiche	3
1.3.1 Zertifizierungsstellen	3
1.3.2 Registrierungsstellen.....	3
1.3.3 Zertifikatempfänger.....	3
1.3.4 Anwendungsbereich.....	4
1.4 Kontaktinformation.....	4
2. Verhältnis zu ETSI TS 101 456	4
2.1 Grundsätzliche Erfüllung des Standards	4
2.2 Abweichungen von ETSI TS 101 456	5
2.2.1 Registrierung.....	5
2.2.2 Zertifikatsinhalt	5
2.3 Nicht anwendbare Punkte des ETSI TS 101 456	6

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 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 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 sind allerdings keine qualifizierten Zertifikate im üblichen Sinn, da sie nicht an natürliche Personen, sondern an Zertifizierungsdiensteanbieter für deren Zertifizierungsdienste ausgestellt werden. In Kapitel 2 wird dargestellt, inwieweit die Anforderungen des ETSI TS 101 456 erfüllt sind.

Inwieweit die Zertifikate – obwohl sie in der Regel nicht an natürliche Personen ausgestellt werden – qualifizierte Zertifikate im Sinne der jeweils anwendbaren nationalen Rechtsordnung sind, wird im Certification Practice Statement dargelegt.

1.2 Identifikation

Bezeichnung des Dokuments: Sicherheits- und Zertifizierungskonzept – Certificate Policy, Version 1.0, 09.09.2002.

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.

Der ASN.1 Object Identifier für dieses Dokument ist 1.2.040.0.21.0.1.0.1.0. Die letzten beiden OID-Komponenten bezeichnen die größere und die kleinere Versionsnummer der Certificate Policy.

Die in ETSI TS 101 456, Punkt 5.2 spezifizierten Object Identifier 0.4.0.1456.1.1 bzw. 0.4.0.1456.1.2 werden nicht verwendet.

1.3 Anwendungsbereiche

1.3.1 Zertifizierungsstellen

Zertifikate nach dieser Certificate Policy werden von einer Stelle zur Überwachung von Zertifizierungsdiensteanbietern 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 Zertifizierungsdiensteanbieter, 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 Zertifizierungsdiensteanbieter 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 101 456 in der aktuellen Version, insbesondere von Abschnitt 7.3.1, erfüllt werden. Die Registrierungsstellen sind im CPS oder in einem Dokument, auf das im CPS verwiesen wird, anzugeben.

1.3.3 Zertifikatsempfänger

Zertifizierungsstellen im Sinne des vorliegenden Dokuments stellen entweder ausschließlich Zertifikate für Zertifizierungsdiensteanbieter 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 Zertifizierungsdiensteanbieter oder für Zertifizierungsstellen können im Zuge der Überprüfung elektronischer Signaturen verwendet werden. Durch das Zertifikat bestätigt die Aufsichtsstelle, dass die Identität des Zertifizierungsdiensteanbieters überprüft worden ist und dass der Zertifizierungsdiensteanbieter 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.

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/(0)1/58058-0
Fax.: +43/(0)1/58058-9191
E-Mail: signatur@signatur.rtr.at
Web: <http://www.signatur.rtr.at/>

2. Verhältnis zu ETSI TS 101 456

2.1 Grundsätzliche Erfüllung des Standards

Die Anwendung dieser Certificate Policy zwingt grundsätzlich zur Einhaltung der Vorgaben des Standards ETSI TS 101 456 V1.2.1 (2002-04) „Policy requirements for certification authorities issuing qualified certificates“. Die nach dieser Certificate Policy ausgestellten Zertifikate sind allerdings keine qualifizierten Zertifikate im üblichen Sinn, da sie nicht an Endbenutzer, sondern an Zertifizierungsdiensteanbieter für deren Zertifizierungsdienste ausgestellt werden. In Kapitel 2.2 wird dies näher ausgeführt. In Kapitel 2.3 werden weitere Punkte aus dem Standard angeführt, die bei der Public-Key-Infrastruktur einer Aufsichtsstelle nicht anwendbar sind.

Die Punkte 5.2 und 5.3 des ETSI TS 101 456 unterscheiden zwischen zwei verschiedenen qualifizierten Certificate Policies: „QCP public + SSCD“ und „QCP public“. Die beiden Policies unterscheiden sich darin, dass bei ersterer qualifizierte Zertifikate ausschließlich für die Nutzung mit sicheren Signaturerstellungseinheiten (SSCD) im Sinne des Anhang III der Signaturrichtlinie 1999/93/EG bestimmt sind.

In der Regel werden die Zertifikate einer Aufsichtsstelle nicht für die Nutzung mit sicheren Signaturerstellungseinheiten im üblichen Sinne ausgestellt, da sie nicht an Endnutzer (die z. B. Chipkarten verwenden), sondern an Zertifizierungsdiensteanbieter für deren Zertifizierungsdienste ausgestellt werden. Die von den Zertifizierungsdiensteanbietern verwendeten Signaturerstellungseinheiten sind zwar in vielen Fällen evaluiert (dies gilt insbesondere für Anbieter, die akkreditiert sind, oder andere Anbieter, die qualifizierte Zertifikate ausstellen), allerdings ergibt sich die Sicherheit der Signaturerstellungseinheit

manchmal nicht aus der technischen Komponente selbst, sondern aus organisatorischen Maßnahmen. Weiters wird die Signatur häufig automationsunterstützt und nicht durch einen Willensakt im Einzelfall ausgelöst. Für Anbieter, die keine qualifizierten Zertifikate ausstellen, gibt es keine Anforderungen an die Sicherheit der verwendeten Signaturerstellungseinheiten.

Im Regelfall entsprechen die von einer Aufsichtsstelle an Zertifizierungsdiensteanbieter ausgestellten Zertifikate also nicht der Policy „QCP public + SSCD“, sondern der Policy „QCP public“ – abgesehen davon, dass sie nicht natürlichen Personen, sondern Zertifizierungsdiensteanbietern ausgestellt werden.

2.2 Abweichungen von ETSI TS 101 456

Da die Zertifikate nicht an Endbenutzer ausgestellt werden, sondern an Zertifizierungsdiensteanbieter, ergeben sich folgende Ausnahmen zu den Anforderungen des Standards ETSI TS 101 456 in dessen Punkten 7.3.1 und 7.3.3:

2.2.1 Registrierung

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 des Punkt 7.3.1 b) aus ETSI TS 101 456 auf einem dauerhaften Datenträger ausgefolgt werden müssen. Eine Aufsichtsstelle archiviert auch keinen Zertifikatswerbervertrag (Punkt 7.3.1 h) aus ETSI TS 101 456), sondern die vom Zertifikatswerber in seinem Antrag zu nennenden Informationen.

Die in Punkt 7.3.1 aus ETSI TS 101 456 genannten Anforderungen werden daher nur sinngemäß angewendet.

2.2.2 Zertifikatsinhalt

Die von einer Aufsichtsstelle ausgestellten Zertifikate werden grundsätzlich im Einklang mit Anhang I und Anhang II g) der Signaturrechtlinie 1999/93/EG ausgestellt. Da es sich aber nicht um qualifizierte Zertifikate im üblichen Sinne handelt, die an natürliche Personen ausgestellt würden, wird keines der in ETSI TS 101 862 definierten „Qualified Certificate Statements“ verwendet, um die Zertifikate als qualifizierte Zertifikate zu kennzeichnen. Die Zertifikate verweisen stattdessen in der Erweiterung CertificatePolicies auf dieses Dokument, in welchem dargelegt wird, dass eine Aufsichtsstelle die Anforderungen, die an qualifizierte Zertifikate gestellt werden – abgesehen davon, dass sie nicht an natürliche Personen, sondern an Zertifizierungsdiensteanbieter ausgestellt werden – erfüllt. Im übrigen verwendet eine Aufsichtsstelle das von ETSI TS 101 862 vorgegebenen Format. Im Issuer-Feld des Zertifikates wird der Name des Ausstellers einschließlich des Attributes countryName angegeben.

2.3 Nicht anwendbare Punkte des ETSI TS 101 456

Eine Reihe von Anforderungen des Standards ETSI TS 101 456 ist innerhalb der Public-Key-Infrastruktur einer Aufsichtsstelle nicht anwendbar:

- Anforderungen zum Backup der privaten Schlüssel (Punkt 7.2.2 des ETSI TS 101 456): 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 ETSI TS 101 456): 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 Zertifizierungsdiensteanbieter) werden gar nicht gespeichert. Punkt 7.2.4 ist daher nicht anwendbar.
- Schlüsselmanagementdienste (Punkt 7.2.8) und Vorbereitung sicherer Signaturerstellungseinheiten (Punkt 7.2.9 des ETSI TS 101 456): 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 ETSI TS 101 456): 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 ETSI TS 101 456): Da die Zertifikate nicht an Endbenutzer ausgestellt werden und da der Zweck der Public-Key-Infrastruktur einer Aufsichtsstelle darin liegt, ein Verzeichnis der Zertifizierungsdiensteanbieter zu führen, werden die Daten der Zertifikatswerber (insbes. Name, Adressen und Zugangsmodalitäten zu deren Verzeichnissen) nicht vertraulich behandelt, sondern auf der Website der Aufsichtsstelle veröffentlicht.