Zertifizierungs-richtlinien (Policy) der RBG-Server-CA

Version: 2.01 , Stand: 14. Juni 2004
Dieses Dokument ist gültig bis zum 31. Januar 2010 oder bis eine neue Version dieser Policy veröffentlicht wird.

Diese Policy ist angelehnt an die World Wide Web Policy der DFN-PCA Version 1.4[1], weicht jedoch in einigen wesentlichen Punkten davon ab.

Dieses Dokument löst Version 1.0 ab, und beinhaltet Änderungen in folgenden Punkten: Rechtliche Bedeutung, Minimale Schlüssellänge, Zertifizierungsregeln und Zertifikats-Erweiterungen, sowie bei der Namensgebung.

Identität der RBG-CA

Fakultät für Informatik der Technischen Universität München
Rechnerbetriebsgruppe
Boltzmannstraße 3
85748 Garching
Deutschland

Telefon: 089-289-18534
Fax: 089-289-18507
E-Mail: ca@in.tum.de
WWW: http://ca.in.tum.de/

Zuständigkeitsbereich der RBG-Server-CA

Die RBG-Server-CA ist Teil der RBG-CA[2]-Hierarchie.

Der Zuständigkeitsbereich der RBG-Server-CA umfasst die Angehörigen der Fakultät für Informatik der Technischen Universität München.

[1] http://www.dfn-pca.de/certification/policies/x509policy.html
[2] http://ca.in.tum.de

Art der Zertifikate

Die RBG-Server-CA erteilt nur X.509v3 SSL/TLS-ServerZertifikate.

Rechtliche Bedeutung

Eine Zertifizierung durch die RBG-CA oder untergeordnete CAs zieht keinerlei rechtliche Bedeutung nach sich. Ein gesetzlicher Anspruch auf die Erteilung eines Zertifikates besteht grundsätzlich nicht. Insbesondere ist die allgemeine rechtliche Relevanz einfacher digitaler Signaturen derzeit unklar. Der Sinn der durch die RBG-CA bereitgestellten Public Key Infrastructure (PKI) liegt in der Schaffung der technischen Voraussetzungen für eine gesicherte elektronische Kommunikation. Alle Aufgaben werden von den Mitarbeitern der RBG-CA nach bestem Wissen und Gewissen durchgeführt, die Abwicklung erfolgt jedoch ohne Gewährleistung.

Die dieser Policy zugrundeliegenden Anforderungen an technische Komponenten und Verfahren zur Zertifizierung genügen derzeit nur den Kriterien der „einfachen digitalen Signatur“ nach § 2 Nr. 1 SigG 2001. Sie sind also weder „fortgeschritten“ noch „qualifiziert“ oder gar „akkreditiert“ nach § 2 Nr. 2 u. 3 SigG 2001 bzw. § 15 Abs. 1 SigG 2001. Die gesetzliche Anscheinsvermutung für eine Beweiserleichterung nach ZPO greift hier also nicht. Vielmehr müssen Gerichte und Gutachter im Streitfall den rechtlichen Wert der eingesetzten Schlüssel, Zertifikate und Signaturen im Einzelfall prüfen.

Sicherheitsanforderungen

Sicherheitsanforderungen an die RBG-Server-CA

Folgende Sicherheitsanforderungen werden von der RBG-Server-CA erfüllt:

- Für die Dienste der CA wird ein Rechner eingesetzt, der in geeigneter Weise vor missbräuchlicher Benutzung geschützt ist. Der unbefugte Zugriff auf den CA-Rechner und eventuell gespeicherte Schlüsseldaten ist

durch den Einsatz geeigneter Hard- und Software unterbunden. Der Rechner ist nicht im allgemeinen Netzwerk erreichbar.

- Die geheimen Schlüssel der CA zum Erzeugen digitaler Signaturen sind ausreichend vor Missbrauch durch Unbefugte geschützt und werden auf keinen Fall weitergegeben. Der Zugriff auf die geheimen CA-Schlüssel ist durch komplexe Passwörter geschützt, welche nur den CA-Administratoren bekannt und niemals im Klartext abgelegt sind, und die nicht über ungeschützte Netzwerkverbindungen gesendet werden.
- Mit dem geheimen Signatur-Schlüssel der CA werden ausschließlich Endteilnehmer-Schlüssel bzw. Widerrufslisten (CRLs) unterschrieben – für Standard-Kommunikation werden die geheimen Signatur-Schlüssel nicht verwendet.
- Asymmetrische Schlüsselpaare der CA zur Erzeugung von Signaturen haben eine Mindestlänge von 2048 Bit RSA.
- Die CA hat ihre Schlüsselpaare selbst erzeugt.
- Für Endteilnehmer generierte Schlüsselpaare werden auf dem CA-Rechner erzeugt. Die Schlüsselpaare werden den Endteilnehmern in einem gebräuchlichen Austauschformat (PKCS12) übergeben. Nach der Schlüsselübergabe werden die geheimen Schlüssel gelöscht. Sie werden auf keinen Fall an Dritte weitergegeben. Bis zur Übergabe werden die geheimen Schlüssel, mit komplexen Passwörtern verschlüsselt, gespeichert. Die Passwörter werden sicher aufbewahrt und nur dem Endteilnehmer übergeben.

Sicherheitsanforderungen an Endteilnehmer

Der geheime Schlüssel des Endteilnehmers muss ausreichend vor Missbrauch durch Unbefugte geschützt und darf nicht weitergegeben werden; hierfür ist jeder Endteilnehmer selbst verantwortlich.

Das Verzeichnis bzw. die Dateien, in denen die kryptographischen Schlüssel von Anwendungen[3] gespeichert werden, sind vom Server-Verwalter nach Maßgabe der Möglichkeiten vor unbefugtem Missbrauch zu schützen. Dies kann z. B. durch das Setzen bestimmter Zugriffsrechte geschehen, sofern das eingesetzte Betriebssystem dies unterstützt. Die Speicherung der kryptographischen Schlüssel auf externen Datenträgern (z. B. Diskette) wird dringend empfohlen.

Wird keine externe Peripherie (z. B. Diskette) zum Speichern des geheimen Schlüssels eingesetzt, sollte der Zugriff auf den geheimen Schlüssel des Endteilnehmers durch das Setzen eines nicht-trivialen Passworts (Mindestlänge: 8 Zeichen) bzw. einer PIN geschützt werden. Weder die optionale Peripherie noch Passwort bzw. PIN dürfen an andere Personen weitergegeben werden. Passwort bzw. PIN dürfen niemals im Klartext abgelegt bzw. über ungeschützte Netzwerkverbindungen gesendet werden.

Das asymmetrische Schlüsselpaar des Endteilnehmers muss eine minimale Länge von 2048 Bit RSA (oder vergleichbares Niveau) aufweisen. Die Wahl größerer Schlüssellängen wird dringend empfohlen und richtet sich nach der technischen Verfügbarkeit. In besonderen Ausnahmefällen können Schlüssel bis zu einer minimalen Schlüssellänge von 1024 Bit RSA (oder vergleichbares Niveau) verwendet werden.

Zertifizierungsregeln

Die RBG-Server-CA generiert für registrierte SSL-Server ein asymmetrisches Schlüsselpaar und erstellt die entsprechenden Zertifikate.

Das Schlüsselpaar sowie das Zertifikat werden in einem geeigneten Austauschformat (PKCS12) verschlüsselt gespeichert.

Der Server-Verantwortliche muss persönlich im Servicebüro RBG erscheinen, um sein Passwort für die PKCS12-Datei entgegenzunehmen, wobei die Vorlage eines Personalaus-

[3] SSL-Server, Apache mod_SSL ...

weises/Reisepasses oder eines vergleichbaren Dokuments erforderlich ist. Zusätzlich sollte der Studentenausweis bzw. der Mitarbeiterausweis vorgelegt werden.

Falls der Endteilnehmer aus technischen Gründen sein persönliches asymmetrisches Schlüsselpaar selber erzeugen muss, so muss der entsprechende Zertifizierungsantrag diesen Richtlinien in allen Punkten genügen, vor allen was die Namensgebung und die Schlüssellänge betrifft, sonst wird er von der CA nicht angenommen.
Der Endteilnehmer schickt seinen Zertifizierungswunsch über den vorgegebenen Übertragungsweg zur CA.

Zertifikate für Endteilnehmer haben eine Gültigkeitsdauer von maximal einem Jahr. Stichtag ist jeweils der 31. Mai.

Jedes Zertifikat muß eine Seriennummer beinhalten, die von der zertifizierenden CA vergeben wird. Dabei hat jede CA bei der Zertifizierung zu gewährleisten, daß von ihr keine Seriennummer mehrfach vergeben wird.

Zertifikate werden in der Regel nicht automatisch durch die ausstellende CA erneuert; Anträge auf Rezertifizierung sind gegebenenfalls bei der entsprechenden CA zu stellen.

Zertifikats-Erweiterungen

X.509v3-Zertifikate zeichnen sich dadurch aus, dass jedes Zertifikat Erweiterungen („certificate extensions“) enthalten kann. Jede Erweiterung kann darüber hinaus durch das Setzen eines bestimmten Bits („critical flag“) als besonders signifikant gekennzeichnet werden.

Folgende Zertifikats-Erweiterungen werden von der RBG-Server-CA unterstützt:

- Basic Constraints, critical
- Subject Key Identifier
- Authority Key Identifier
- Key Usage, critical
- Extended Key Usage
- Subject Alternative Name
- Issuer Alternative Name
- CRL Distribution Points
- Certificate Policies
- Netscape Cert Type
- Netscape Comment
- Netscape Revocation URL
- Netscape CA Revocation URL
- Netscape CA Policy URL

Erklärung der Teilnehmer

Alle Teilnehmer der RBG-CA-Hierarchie haben handschriftlich eine Erklärung zu unterzeichnen, in der sie über ihre Rechte und Pflichten, sowie über die Risiken und Gefahren beim Einsatz von Public Key-Systemen aufgeklärt werden. Diese Erklärung, die im Einzelfall auch vom Teilnehmer an die zertifizierende CA gefaxt, bzw. per Mail mit einer durch die RBG-Server-CA zertifizierten Signatur geschickt werden kann, wird von der zertifizierenden Instanz verwahrt und beinhaltet in erster Linie die Zustimmung zu den Richtlinien dieser Policy, sowie gegebenenfalls eine Erklärung darüber, von welcher Instanz das zu zertifizierende asymmetrische Schlüsselpaar erzeugt wurde.

Management von Zertifikaten

Alle Teilnehmer erklären sich grundsätzlich mit der Veröffentlichung ihres Zertifikates einverstanden.
Der Teilnehmer kann die Veröffentlichung auf den Bereich der Fakultät beschränken, andernfalls gilt sie weltweit.

Für die Überprüfung der Zertifikate hat die RBG-CA ein Verzeichnis eingerichtet, dessen Aufgabe die Überprüfung und Verteilung von Zertifikaten und CRLs ist.

Widerruf von Zertifikaten

Die RBG-Server-CA kann erteilte Zertifikate jederzeit vor Ablauf der Gültigkeitsdauer ohne Angabe von Gründen widerrufen.

Jeder Zertifikatnehmer kann von der Instanz, die seinen Public Key zertifiziert hat, ohne Angabe von Gründen verlangen, dass diese ein für ihn ausgestelltes Zertifikat widerruft.

Alle widerrufenen Zertifikate werden auf einer Widerrufsliste veröffentlicht, welche allen Teilnehmern zur Verfügung gestellt wird.

Einmal widerrufene Zertifikate können nicht erneuert oder verlängert werden. Jedoch hat jeder Teilnehmer die Möglichkeit, ein neues Zertifikat zu beantragen.

Unmittelbar nach der Aufnahme des Betriebs hat jede CA eine Certification Revocation List (CRL) herauszugeben. Diese CRL wird mindestens im monatlichen Abstand erneuert.

Für die Bereitstellung von CRLs hat die RBG-Server-CA ein Verzeichnis eingerichtet.

Namensgebung

Allen Zertifikatsnehmern wird ein eindeutiger Name (Distinguished Name, DN) zugeordnet, welcher bei der Ausstellung eines Zertifikates für einen Teilnehmer als dessen X.509-Subjektname verwendet wird.

Ein DN enthält eine Folge von eindeutig kennzeichnenden Namensattributen, durch die alle Teilnehmer einer Hierarchie referenziert werden können.

Aus Gründen der Interoperabilität wird auf unübliche Sonderzeichen (z. B. Umlaute) innerhalb des DNs verzichtet.

Für Teilnehmer der RBG-Server-CA wird ein DN mit folgendem Aufbau erzeugt:

C	DE
L	Muenchen
O	TUM
OU	IN
CN	<*hostname bzw servicename*>
Email	<*Verwalter* >@in.tum.de

Zusätzliche Hostnamen:
<*name*>.informatik.tu-muenchen.de
<*name*>.in.tum.de
<*name*>.cs.tum.edu