Leibniz
Universität
Hannover

IT-Sicherheit

Digitale Zertifikate für sichere E-Mail- und Serverkommunikation

Stand: 15. Januar 2009

R|R|Z|N|

Regionales Rechenzentrum für Niedersachsen

Was ist ein digitales Zertifikat?

Ein wichtiges Verfahren für die vertrauliche und vertrauenswürdige Kommunikation ist die asymmetrische Verschlüsselung, bei der für das Ver- und Entschlüsseln ein Paar verschiedener Schlüssel eingesetzt wird: Der „Public Key" wird veröffentlicht und steht allen Kommunikationspartnern zur Verfügung, der zugehörige „Private Key" ist nur dem Schlüsselinhaber bekannt und muss vor Dritten verborgen gehalten werden.
Die Zusammengehörigkeit eines Public Keys mit den Angaben des Inhabers dieses Keys zu seiner Person wird durch eine Zertifizierungsinstanz (CA) beglaubigt und wird dadurch zu einem digitalen Zertifikat.
Für Teilnehmer innerhalb der Leibniz Universität Hannover wird diese Beglaubigung von der UH-CA (Certification Authority der Universität Hannover) durchgeführt.

Wie erhalte ich ein digitales Zertifikat?

Mitarbeiter und Studierende der Leibniz Universität Hannover beantragen ihr persönliches Zertifikat komfortabel über die Webseiten der UH-CA. Die damit einhergehende persönliche Identifizierung wird bei der Registrierungsstelle (RA) der UH-CA im RRZN vorgenommen.

Webseite:
http://www.rrzn.uni-hannover.de/zertifizierung.html

Persönliche Identifizierung und Ansprechpartner für Fragen:

Dr. Ingrid Gnutzmann
Dipl.-Biol. Birgit Gersbeck-Schierholz

Telefon: 05 11/7 62-79 90 42
E-Mail: uhca@ca.uni-hannover.de

Wozu digitale Zertifikate?

Sichere E-Mail-Kommunikation

Die Anwendung kryptografischer Verfahren für Ihre E-Mail garantiert Ihnen

- die eindeutige Identität des Absenders (Authentizität),
- den unveränderten Inhalt des Dokumentes (Integrität),
- die Nicht-Abstreitbarkeit der Daten (Verbindlichkeit).

. . . in jedem Fall verschlüsselt der Absender mit seinem geheimen Private Key.

- Die Nicht-Lesbarkeit durch Dritte (Vertraulichkeit)

. . . wird durch Verschlüsselung mit dem Public Key des Empfängers erreicht.

Signieren von Dokumenten und Programmcode

Setzen Sie ein digitales Zertifikat zum Signieren von Dokumenten (z. B. PDF) und Programmcode (z. B. Makros) ein, können Sie gewährleisten, dass Sie der Urheber sind und dass Ihr Dokument nicht von Dritten verändert wurde.

Serverzertifikate

Ein Serverzertifikat ermöglicht eine verschlüsselte Datenübertragung zwischen Anwender und z. B. einem Webserver (HTTPS) und stellt zudem die Authentizität des Servers gegenüber dem Nutzer sicher. Arbeiten auch die Klienten mit einem Zertifikat, erfolgt ein gesicherter Datenaustausch nach Authentifizierung beider Kommunikationspartner.

Sicherheit schafft Vertrauen!

Zertifizierungsstelle der Leibniz Universität Hannover (UH-CA)

Die UH-CA stellt digitale Zertifikate nach dem internationalen Standard X.509v3 aus. Als Teilnehmer am PKI Projekt des DFN (Deutsches Forschungsnetz) ist sie von der DFN-Verein PCA Global zertifiziert, welche wiederum mit einem Wurzelzertifikat der T-Systems (Deutsche Telekom Root CA 2) verkettet ist.

Zertifikatdaten

Vollständiger Name der UH-CA (Subject DN):
`C=DE,O=Leibniz Universitaet Hannover,OU=RRZN,`
`CN=CA der LUH (UH-CA) - G03`

SHA1 Fingerprint:
`91:BA:3B:3B:E9:C2:C3:B3:00:CC:52:5E:18:4A:`
`9D:C6:7F:4B:B4:92`

MD5 Fingerprint:
`A7:7A:5A:CA:D1:21:6C:30:B0:7C:46:DA:2A:22:`
`72:19`

Policy:
`https://info.pca.dfn.de/uh-ca/cpcps.pdf`

Zertifikat Sperrlisten (CRLs):
`https://pki.pca.dfn.de/uh-ca/pub/crl/g_cacrl.crl`

Impressum:

Regionales Rechenzentrum für Niedersachsen
Leibniz Universität Hannover
Schloßwender Straße 5
D-30159 Hannover

Telefon	05 11/7 62-28 83
Telefax	05 11/7 62-30 03
E-Mail	security@rrzn.uni-hannover.de
Internet	http://www.rrzn.uni-hannover.de

Verantwortlich: Dipl.-Biol. Birgit Gersbeck-Schierholz