R|R|Z|N

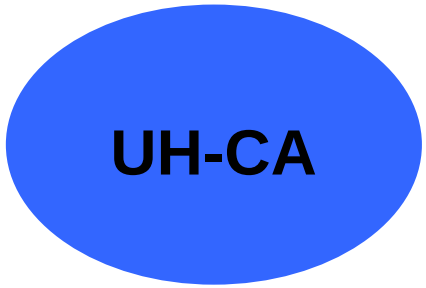
Die UH-CA in der 3. Generation

Sicherheitstage SS/07

Birgit Gersbeck-Schierholz, RRZN

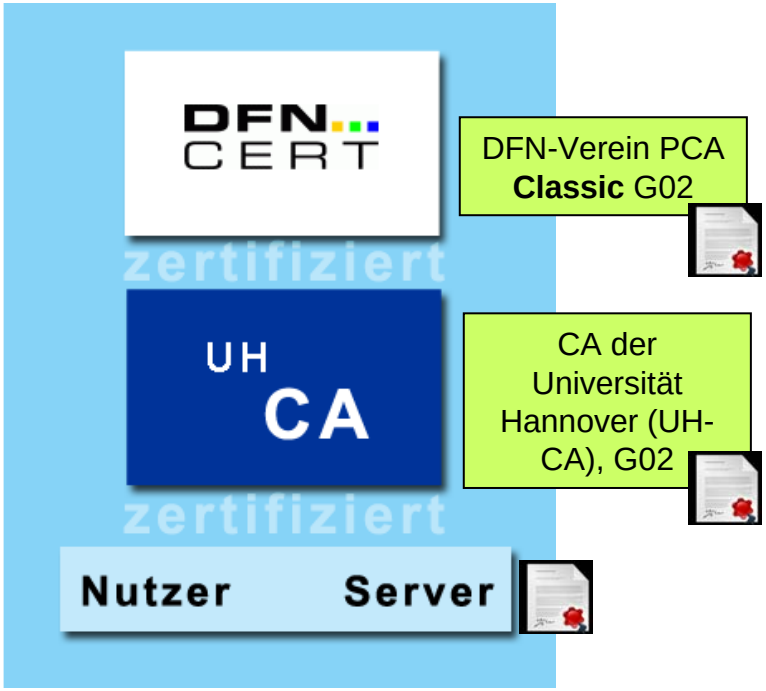
Die Zertifizierungsstelle der Universität Hannover

- **Zertifizierungsstelle der Universität Hannover seit Mai 2004**
- **Benutzerschnittstelle:** *www.rrzn.uni-hannover.de/zertifizierung.html*

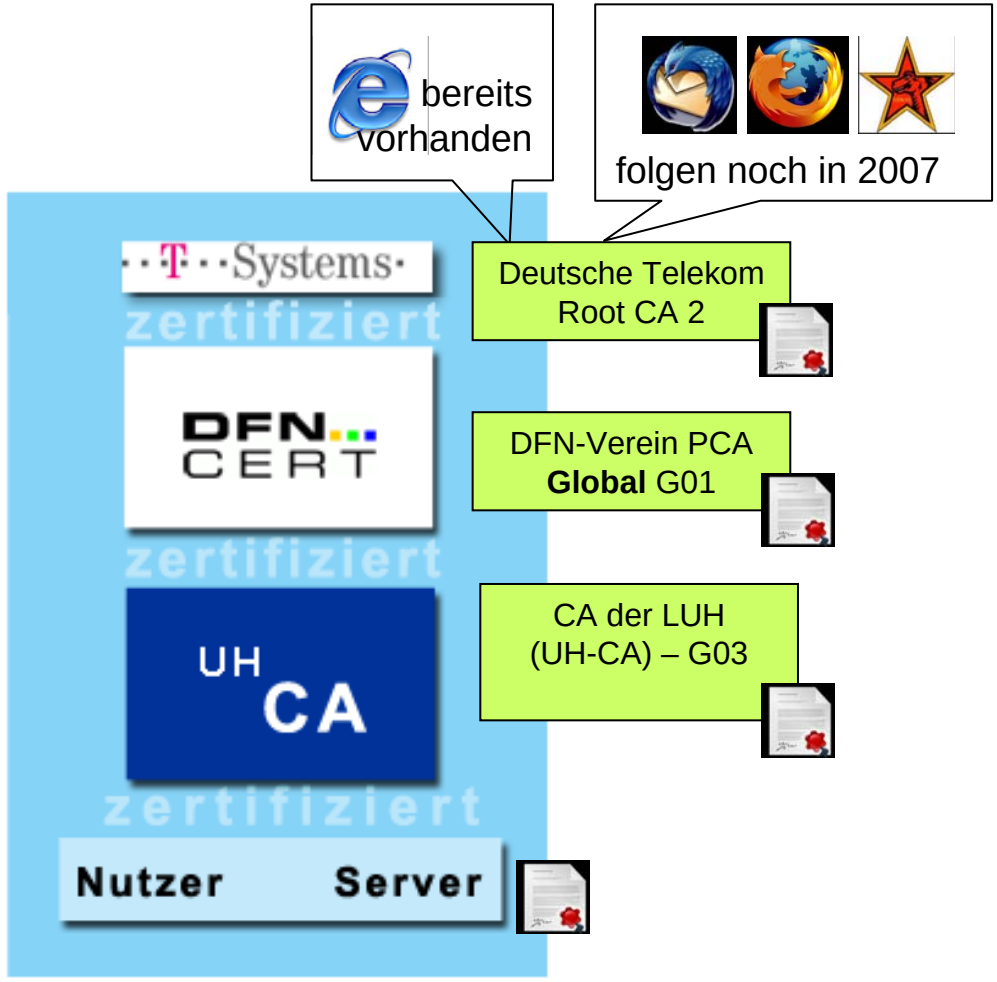


- **Erstellt digitale Zertifikate für z.B. sichere E-Mail- und Serverkommunikation**
- **Zertifikate für Mitglieder der Universität Hannover**
- **Integriert in die PKI (Public Key Infrastructure) des Deutschen Forschungsnetzes**

2. Generation - alte Hierarchie: **DFN - Classic**



3. Generation - neue Hierarchie: **DFN - Global**



Die Global Hierarchie der DFN-PKI

R|R|Z|N

- **Verkettung mit der Telekom erfordert hohes Vertrauen in die CAs der DFN-PKI seitens der Telekom**
  - Betrieb von CAs in Global ausschließlich bei der DFN-PCA
  - Neue Policy, abgestimmt auf Telesec
  - Höhere Sicherheitsbestimmungen

Die Global Hierarchie der DFN-PKI

R|R|Z|N

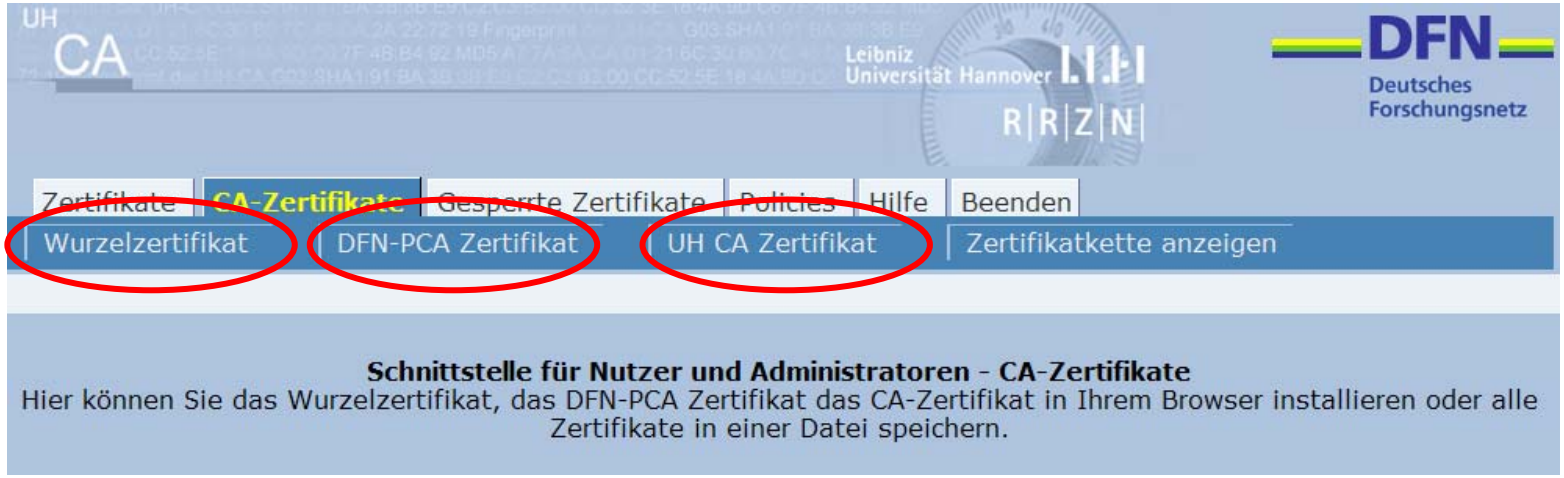
- **Vorteile**
  - Wurzel der Telekom vorinstalliert
    - Keine Warnmeldungen für Server-Zertifikate
    - E-Mail Signaturen werden weltweit verifiziert
  - Längere Laufzeiten
    - 3 Jahre Laufzeit für Nutzerzertifikate
    - 5 Jahre Laufzeit für Serverzertifikate
  - Längere Schlüssel
    - Zukunftssicher durch mind. 2048 Bit Schlüssel

Die Global Hierarchie der DFN-PKI

R|R|Z|N

- **Vorläufige Einschränkung:**
  - Das Zertifikat der Deutschen Telekom ist bisher nur im IE/Outlook installiert
    - Vertragliche Zusicherung für Mozilla noch im Sommer 2007
    - Gespräche auch mit anderen Anbietern mit eigenen Zertifikatspeichern (z.B. SUN -> Java Keystore)

CA-Zertifikate der Global Hierarchie der DFN-PKI



Die Global Hierarchie der DFN-PKI

R|R|Z|N

Mozilla Firefox: Zertifikat-Manager

Die Global Hierarchie der DFN-PKI

R|R|Z|N

Webschnittstelle der UH-CA für die Beantragung digitaler Zertifkate