

Die UH-CA in der 3. Generation



Sicherheitstage SS/07

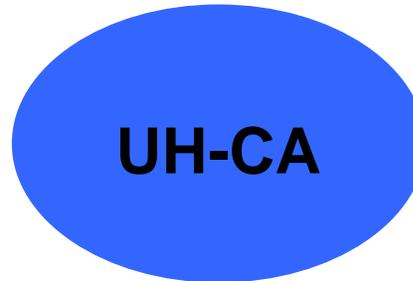
Birgit Gersbeck-Schierholz, RRZN

- **Zertifizierungsstelle der Universität Hannover seit Mai 2004**

- **Benutzerschnittstelle:**

www.rzrn.uni-hannover.de/zertifizierung.html

- **Erstellt digitale Zertifikate für z.B. sichere E-Mail- und Serverkommunikation**

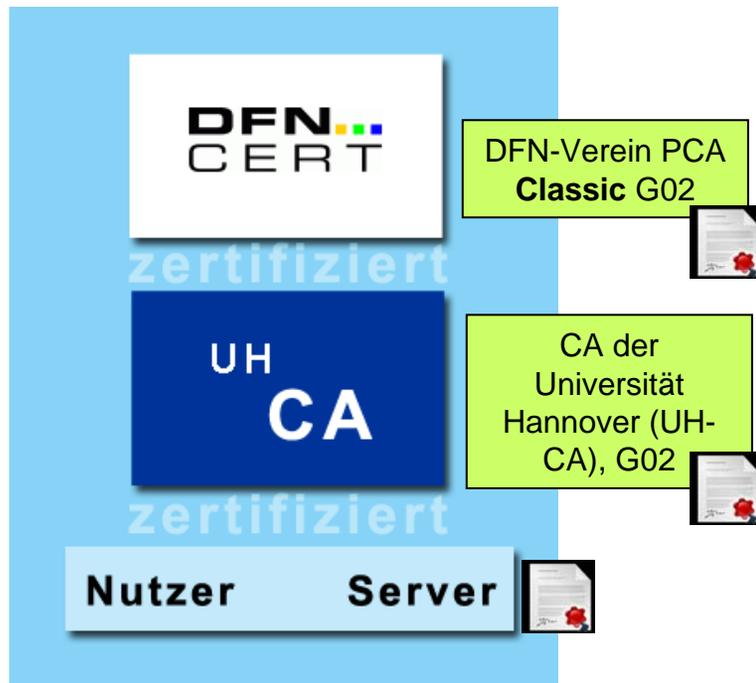


- **Zertifikate für Mitglieder der Universität Hannover**

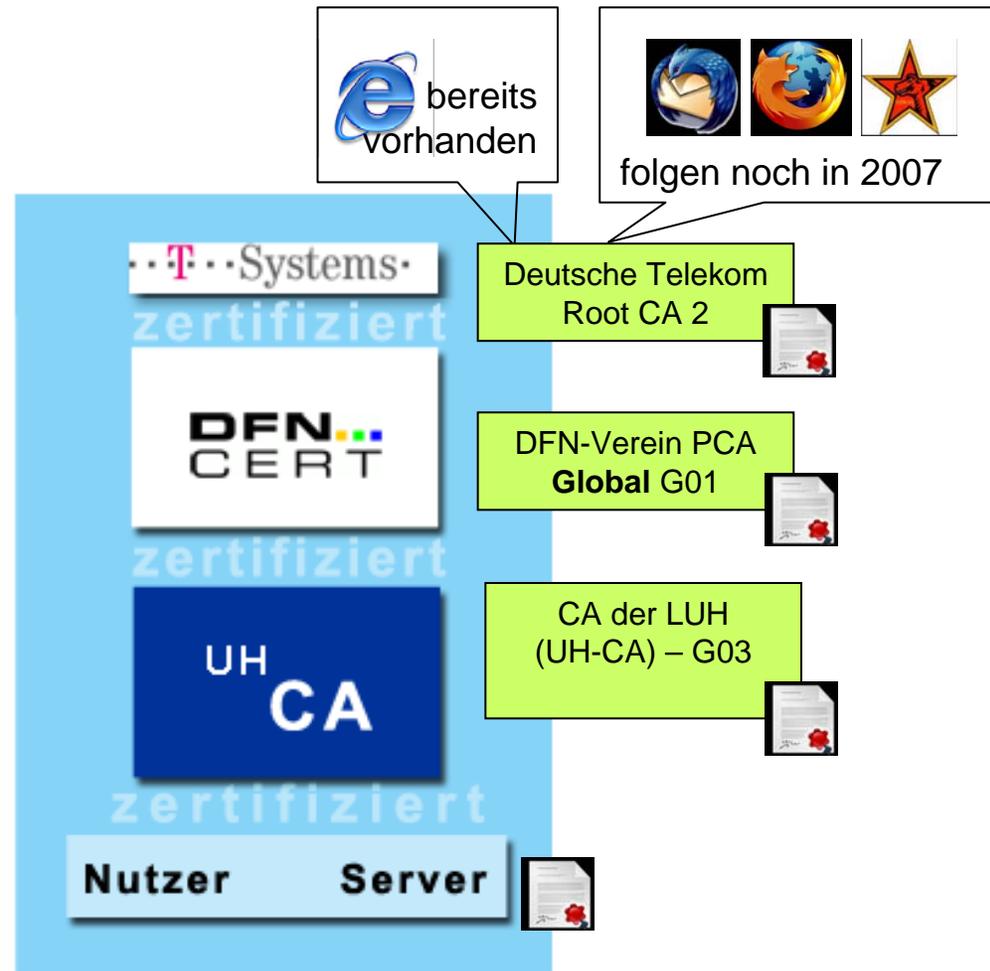
- **Integriert in die PKI (Public Key Infrastructure) des Deutschen Forschungsnetzes**

DFN
CERT

2. Generation - alte Hierarchie: DFN - Classic



3. Generation - neue Hierarchie: DFN - Global



- **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

■ 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

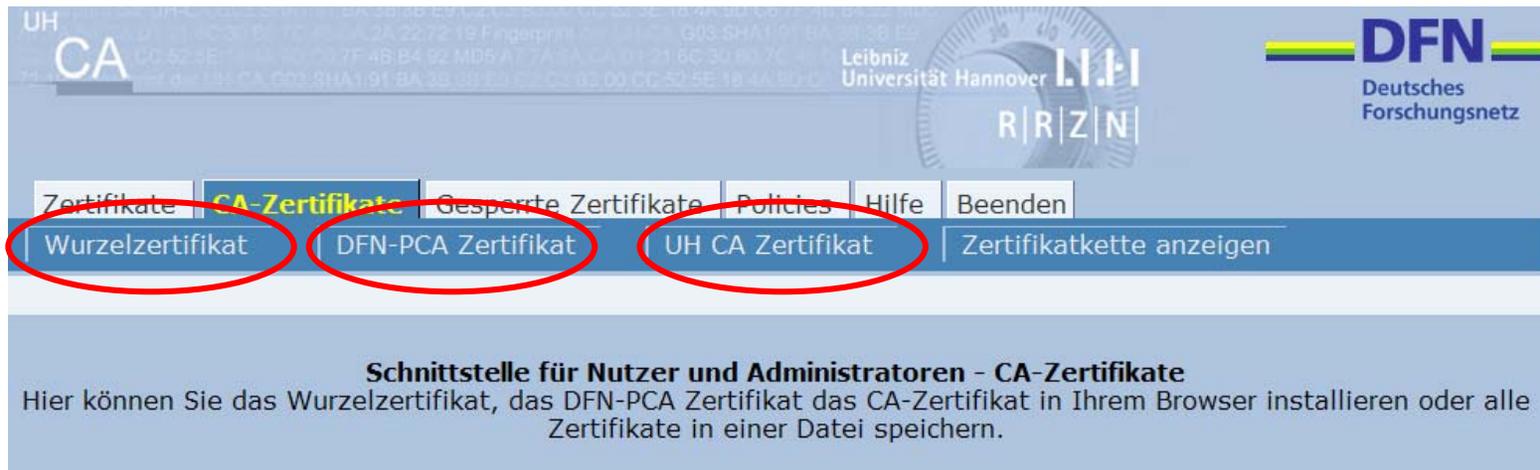
■ Längere Schlüssel

- Zukunftssicher durch mind. 2048 Bit Schlüssel

■ Vorläufige Einschränkung:

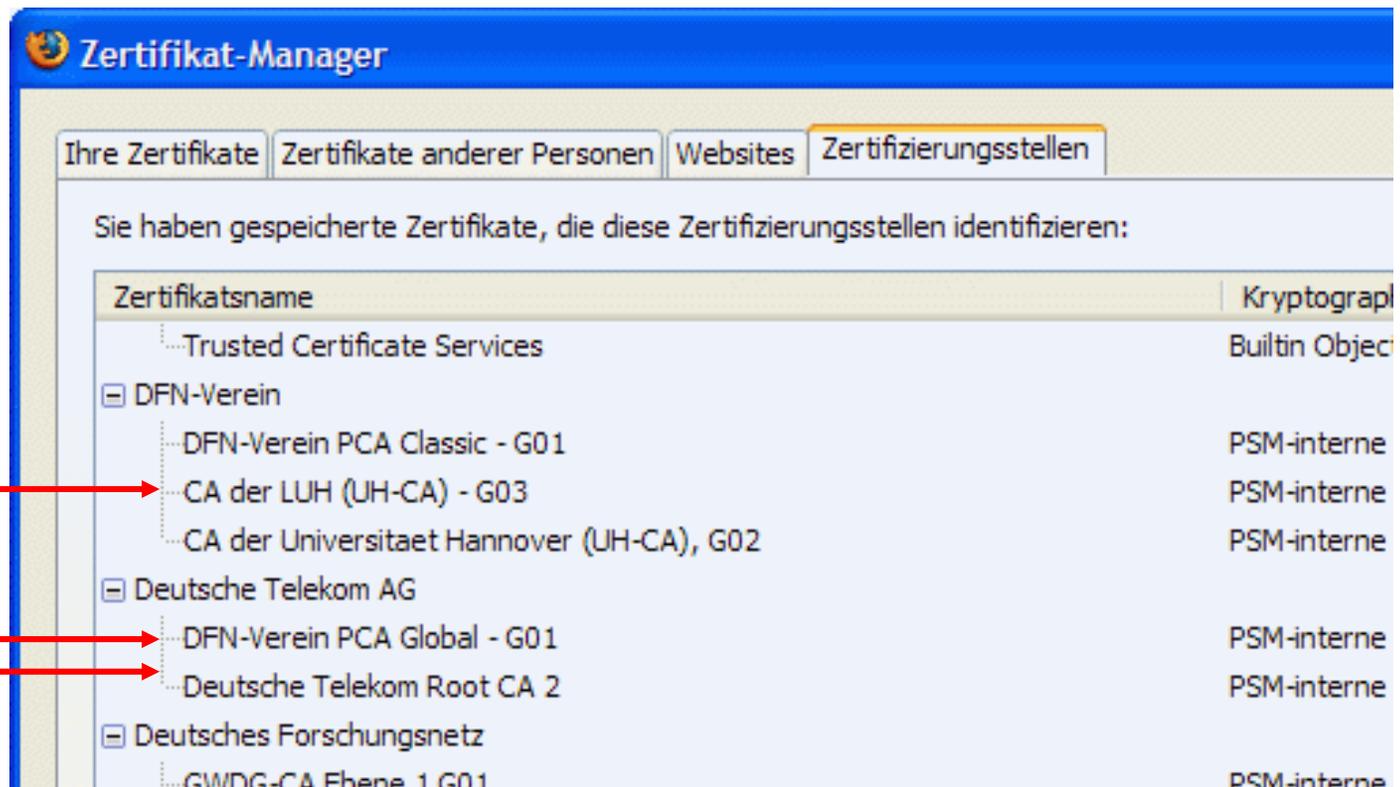
- Das Zertifikat der Deutschen Telekom ist bisher nur im IE/Outlook installiert
 - Vertragliche Zusicherung für Mozilla noch im Sommer 2007
 - Gespräche auch mit anderen Anbietern mit eigenen Zertifikatspeichern (z.B. SUN -> Java Keystore)

CA-Zertifikate der Global Hierarchie der DFN-PKI



Schnittstelle für Nutzer und Administratoren - CA-Zertifikate
Hier können Sie das Wurzelzertifikat, das DFN-PCA Zertifikat das CA-Zertifikat in Ihrem Browser installieren oder alle Zertifikate in einer Datei speichern.

Mozilla Firefox: Zertifikat-Manager



Webschnittstelle der UH-CA für die Beantragung digitaler Zertifikate



The screenshot shows the web interface of the UH-CA (University of Hannover Certificate Authority). At the top, there is a header with the text "UH CA" and "Leibniz Universität Hannover". To the right of the header is the DFN logo (Deutsches Forschungsnetz) and a circular graphic with the text "R | R | Z | N |". Below the header is a navigation menu with the following items: "Zertifikate" (highlighted), "CA-Zertifikate", "Gespernte Zertifikate", "Policies", "Hilfe", and "Beenden". Below the navigation menu is a sub-menu with the following items: "Nutzerzertifikat", "Serverzertifikat", "Zertifikat sperren", and "Zertifikat suchen". The main content area contains the following text:

Willkommen zur DFN-PKI
Schnittstelle für Nutzer und Administratoren - Zertifikate
Hier können Sie Zertifikate beantragen, sperren lassen und nach Zertifikaten suchen.

- Bitte importieren Sie alle CA-Zertifikate in Ihren Browser über die Registerkarte "CA-Zertifikate".
- Bitte wählen Sie aus den Registerkarten eine Funktion aus.

Kontaktinformationen für Rückfragen finden Sie unter "Hilfe"