HUMBOLDT-UNIVERSITÄT ZU BERLIN

Dienstleistungen der Public Key Infrastructure HU-PKI

Eine Kurzdarstellung

Übersicht

- Organisatorisch

  DFN-PKI (technischen Betrieb zentraler Komponenten)

  HU-PKI (org. Aufgaben, Registrierungsstelle)

  Vertraglich geregelt; Policy
- Vertrauensanker

  Deutsche Telekom Root CA 2 (Wurzelzertifikat)
  seit 08/2009 in allen relevanten Anwendungen und Betriebssystemen enthalten

Zertifikate für Personen (E-Mailadresse)

- Antrag über Webformular (E-Mailadresse, Account)
- persönliche Abholung (PIN-Brief), Identifizierung
- Format: HU-CA-Smartcard, Softzertifikate (pkcs#12)
- Zertifikat 3 Jahre gültig
- Zertifikat wird im HU-LDAP veröffentlicht (Adressbuch)
- Verwendung für:

Signieren von E-Mail, PDF

Ver-/Entschlüsseln von E-Mail, PDF, Dateisystem

Authentifizieren z.B. an Web-Portalen, Windowsdomäne

HU-CA-Smartcard oder Softzertifikat

HU-CA-Smartcard	Softzertifikat
-Installation von Hard- und Software an jedem PC erforderlich an dem die Smartcard genutzt werden soll (Kartenleser, CardOS-API) - sicherer, da der private/geheime Schlüssel die Karte nie verlässt - kann als Zutrittskarte verwendet werden - kann für Windows-Anmeldung verwendet werden -Zertifikat kann auf Karte erneuert werden	-keine zusätzliche Hard- und Software erforderlich - muss in jede Anwendung installiert werden in der das Zertifikat genutzt werden soll; der private/geheime Schlüssel liegt dann in jeder Anwendung und muss durch diese geschützt werden -Muss nach Ablauf komplett neu beantragt werden
Antragsverfahren ist für beide gleich. Für beide Varianten gibt es die Möglichkeit unter Verwendung des PIN-Briefes die Smartcard, oder das Softzertifikat wieder herzustellen.	

Zertifikate für Server (FQDN, IP-Adresse)

- Übergabe Request und schriftlichen Antrag
- Format: pem, pkcs#12
- Zertifikat 5 Jahre gültig
- Verwendung für:
  SSL-Verbindungen (https, ldaps)
  Verifizieren von Webseiten aus Benutzersicht
  gesicherte Benutzeranmeldung am Mailserver SSL/TLS
- Second-Level-Domain muss für die Einrichtung registriert sein

Zertifikate für CodeSigning

- Übergabe Request und schriftlichen Antrag
- Format: pem, pkcs#12
- Zertifikat 3 Jahre gültig
- Verwendung für:
  selbstentwickelte Softwareobjekte Java-Applets, VBA‘s, …
  die Integrität und die Quellcodes von Anwendungen sichern

Zertifikate für WLAN-Zugang (eduroam)

Außerhalb der DFN-PKI (andere Policy)

- Authentifizieren mit CMS-Account/Passwort an Webformular
- Format: pkcs#12
- Zertifikat 3 Jahre gültig, wird bei Neuausstellung oder Accountsperre ungültig (CRL)
- Verwendung:
  auf mobilen Geräten für den WLAN-Zugang

Das war‘s.

- Mehr Informationen:
  http://www.cms.hu-berlin.de/dl/zertifizierung

- Fragen?
  pki@hu-berlin.de
  209370043