HU-PKI - Ausbau der Dienstleistung

Informationen zur Dienstleistung und zu Anwendungen

Inhalt

Übersicht
- Struktur, was + wie

Dienstleistung
- bisher und weiterhin
- zusätzlich / neu HU-CA Smartcard

Ausblick

Übersicht

- Struktur – Wurzel bildet DFN-PCA
- Schalenmodel mit 2 sich überschneidenden HU-CA‘s
- Ausgabe von X509 Zertifikaten
  - Maschinenzertifikate (Web-, Mail-, VPN-Server, Domaincontroller)
  - Personenzertifikate (HU-CA Smartcard, Softzertifikat)
- Widerruf von Zertifikaten, CRL

wie bekommen Sie was

- Maschinenzertifikate
  Übermittlung PKCS#10 Requests / SCEP
  Serverseitige Key- und Requestgenerierung
- Personenzertifikate
  Softzertifikat (im lokalen Browser)

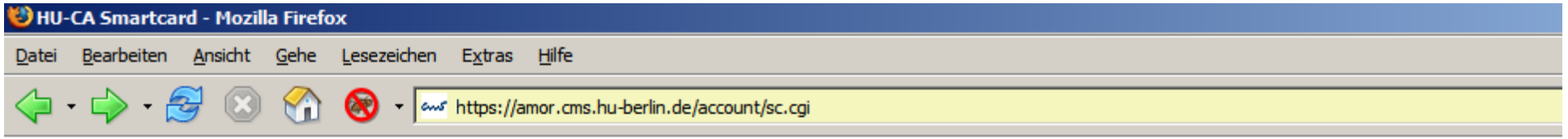
  alles bisher: über unsere Onlineschnittstelle
  (Zertifizierungsinstanz – aktuelle Endnutzer-DCA)

  Neu: HU-CA Smartcard für Personenzertifikate
  (bevorzugt, wird hier geschildert)

Webbasiertes Antragsformular

- Karte beantragen (Account, Passwort, Domain)
  - Anerkennung der HU-CA Policy
- Antrag zurückziehen
- Karte verloren und neu beantragen
- Karte sperren

https://amor.cms.hu-berlin.de/account/sc.cgi



HU-CA Smartcard

Bitte wählen Sie die gewünschte Aktion aus und authentifizier

- (•) Ich möchte eine Smartcard beantragen.
  - [x] Ich erkenne die Policy der HU-CA an.
- ( ) Karte defekt oder verloren **und** neue Karte beantragen
- ( ) Karte sperren oder Antrag zurückziehen

Account:	platzers
Passwort:	**********
Windowsdomäne:	CMS

Weiter | Abbruch | Löschen

Kontakt: PKI | Letzte Änderung: 2006-06-02 Mathias Roland

und dann …?

- Karte wird komplett fertig gestellt (HU-CA)
- E-Mailbenachrichtigung an den Antragsteller über Abholbereitschaft
- persönliches Abholen (Ausweis mitbringen) (Karte, PIN/PUK-Brief, Zertifikat auf Karte)
- Kartenreader anschließen
- Kartensoftware (Windows, Linux, Mac OS X) installieren
- Karte anwenden

Einsatz der HU-CA Smartcard vorerst …

- verschlüsseln und signieren von E-Mail
- gesicherte Remotezugriffe (z.B. VPN)
- signieren und schützen von Dokumenten
- Smartcard basierende Anmeldung (Windows-Domäne)
- Festplattenverschlüsselung mit Smartcard

Beschreibungen zum Einsatz in den Applikationen
CMS / DL / PKI-Services / HU-CA Smartcard

HU-CA Smartcard - Layout

- Vorname Name, Lfd. Nr., HU-Logo
- Angepasst an Layout Zutrittskarte (HUZT-HUCA)
- Rückseite noch nutzbar

Smartcard - personalisieren

- Vordefiniertes Profil
  Filestruktur angelegt private/public
  Security Manager verwaltet den Zugriff auf privaten Schlüssel über PIN
  Fehlbedienungszähler (Karte sperren - PUK)
- Schlüsselpaar wird auf der Karte erzeugt
- Zertifikat wird bei Übergabe der Karte aufgebracht

HU-CA Smartcard - Sicherheitshinweise

- Keine triviale PIN verwenden
- Verhindern Sie das Ausspähen Ihrer PIN
- Bewahren Sie Ihre Karte vor Verlust und Beschädigung
- Achten Sie auf ordnungsgemäßen Zustand des Kartenlesers

Ausblick: mögliche Erweiterungen geplante Optimierungen

- Kombination der HU-CA Smartcard mit Funktionen die der kontaktlose Mifarechip erfüllen kann (Zutritt, Bezahlfunktionen)
- Gestaltung der freien Rückseite als Sichtausweis, und/oder mit Barcode
- noch einfachere Zertifikatserneuerung

Das war‘s …

weiter Informationen

http://www.cms.hu-berlin.de/dl/zertifizierung/
CMS – Dienstleistung – PKI-Services

Kontakt:
pki@hu-berlin.de
2093 7043