

Neues aus der DFN-PKI

Jürgen Brauckmann
dfnpca@dfn-cert.de

- Browser-Integration DFN-PKI
- Aktuelle Betriebsinformationen
- T-Systems Audit 2009
- Neues DFN-PKI CP Version 2.2
- Neue Version der Java-GUI für RAs

Browser-Integration DFN-PKI

Reaktionen auf Browser-Integration DFN-PKI in Firefox 3.5 (30.06.2009):

*„Gepriesen sei der Herr der Herrlichkeit.
ENDLICH! Das macht hier vieles einfacher.“*

„Juhu!“

*„JA!!! wir haben gestern Nacht hier schon freudig
drauf angestoßen - Danke an alle, die da positiv
mitgewirkt haben!“*

*„Wir hatten Herrn Pietrus Kampf auf Bugzilla
mitverfolgt. ;-) „*

Status der Integration Telekom Root CA2

- **Windows:** alle aktuellen Desktop Versionen
- **Apple:** seit Juni 2008 (Mac OS X, iPod, iPhone)
- **Opera:** in aktueller Version
- **Mozilla:** Seamonkey $\geq 1.1.18$
Firefox $\geq 3.0.12$
Thunderbird $\geq 2.0.0.2$
- **Sun Java:** Integration ab V6u11 erfolgt (11.08)
- **Google Chrome:** OK, da abhängig vom OS

Alle Informationen zur Integration unter
www.pki.dfn.de/integration

Aktuelle Betriebsinformationen

- Mehr als 240 Einrichtungen nutzen DFN-PKI
- Zertifikate für Studenten:
 - 6 Einrichtungen geben Zertifikate an alle Studenten aus
 - Multifunktionale Chipkarten
 - Zweck: Authentifizierung für Self-Service-Funktionen
 - Meistens Kartenproduktion direkt bei Einschreibung

- OCSP System ist verfügbar
 - Bei Interesse: dfnpca@dfn-cert.de
- Zeitstempeldienst: Stetige Nutzung (>500 pro Monat)

Vortrag von Moxie Marlinspike auf der Blackhat-Konferenz im Juli:

- Sonderzeichen in Zertifikat-DN problematisch
- Speziell: NULL-Byte hebt Namensprüfung bei SSL durch Browser aus
 - CN=**www.boese.test\0www.harmlos.test** wird von alten Browsern als Zertifikat für **www.boese.test** akzeptiert
 - CAs prüfen Legitimität von **www.harmlos.test**
- Kein Problem bei DFN-PKI-Zertifikaten
- Aktuelle Browser nicht betroffen

T-Systems Audit 2009

- 2 Tage:
 - Besuch bei der RA der Universität Hamburg
 - Audit bei der PCA
 - Erfolgreich, keine Auflagen
 - Anregungen:
 - Mehr Dokumentation für RA-Ernennung
 - Technische Durchsetzung von Domainnamenprüfung
- Neue Formulare!

DFN-PKI CP 2.2

- Seit April 2009 in Kraft
- Motivation: Mozilla, T-Systems, kleinere Ergänzungen
- Änderungen:
 - Verpflichtung zur Kontrolle von Domainnamen durch PCA
 - OCSP ohne CPS-Ergänzung möglich
 - PostIdent für Teilnahme an der DFN-PKI möglich
 - „GRP - “ anstatt „GRP:“

Neue Version der Java-GUI für RAs

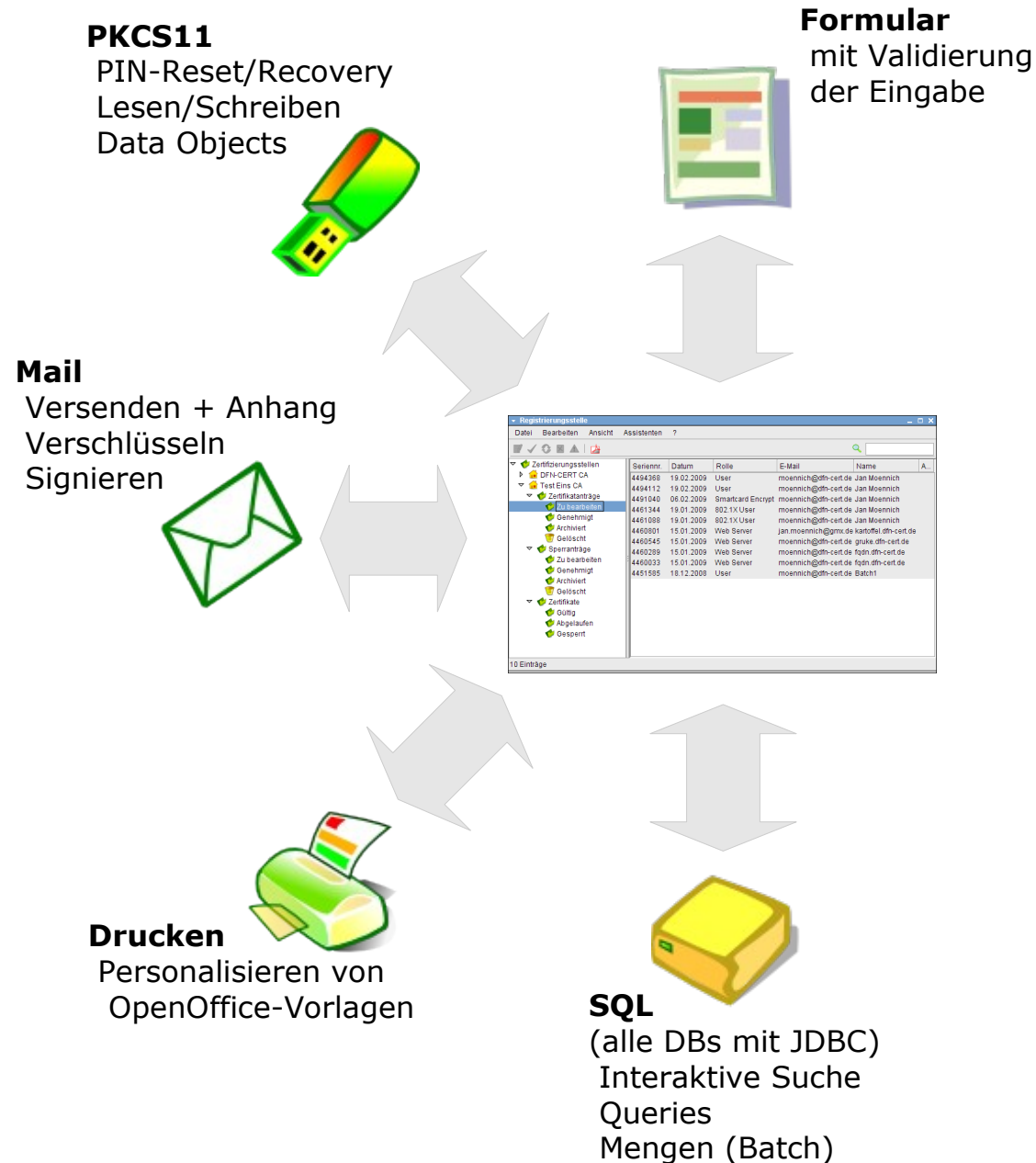
Neue Version im August 2009 veröffentlicht:



Mehr Möglichkeiten bei der Gestaltung von Assistenten, z.B.:

- Mail-Versand
- CSV-Import
- Truecrypt-Unterstützung

Bei Interesse:
pki@dfn.de



- Browser-Integration abgeschlossen
- Betrieb erfolgreich
- Audit durch T-Systems erfolgreich
- Neues DFN-PKI CP 2.2 in Kraft
- Neue Version der Java-GUI für Registrierungsstellen im Einsatz

pki@dfn.de
<https://www.pki.dfn.de>