

Multifunktionale Chipkarte thoska+

Jena

Schmalkalden

Weimar



Erfurt

Nordhausen

Ilmenau

Thüringer Hochschul- und Studentenwerkskarte

Jörg Deutschmann (Berichterstatter)

Gliederung

1. Einführung
 - ... oder „die T(h)ücke liegt im Detail“
2. thoska+ im Überblick
 - Funktionen
 - Layout
3. Prozesse rund um die multifunktionale Chipkarte
 - Aspekte der Personalisierung
 - Validierung
4. thoska+ und die Teilnahme an der DFN-PKI
 - Sicherheitszertifikate der DFN-PKI als Dienst
 - Sicherheitszertifikate der DFN-PKI auf der thoska+
5. Zusammenfassung und Ausblick

Einführung

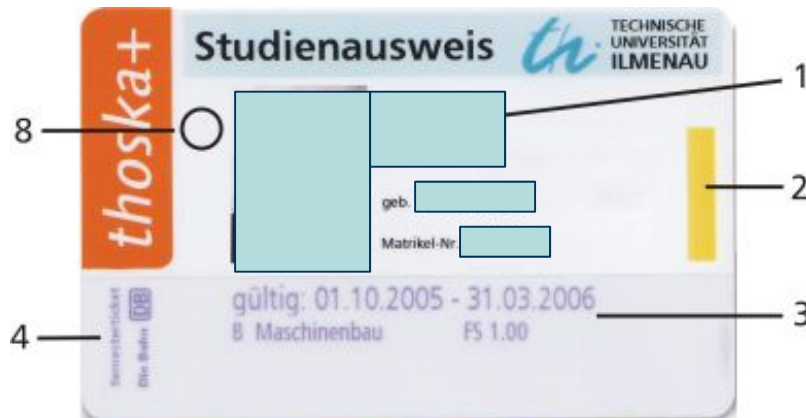
- „Ein t(h)ückisches Objekt“, Modell für eine Thüringer Chipkarte, Ilmenauer Uni-Nachrichten 41/7/98 S. 10
 - Projektstart 1997: THUringer(Hochschul-)ChipKartE "THÜCKE"
- **thoska** - ein Gemeinschaftsprojekt der Thüringer Hochschulen und des Thüringer Studentenwerks
- thoska+ - Erweiterung der multifunktionalen Chipkarte um einen Kryptoprozessor in Ilmenau
- thoska+ in Ilmenau für
 - Studierende ab Wintersemester 2005/06, Matrikel 2004 rückwirkend zum Wintersemester 2006/07
 - Bedienstete seit 2005
 - Angehörige der Universität (lt. § 20 ThürHG)

Funktionen der thoska+ im Überblick

- Ausweisfunktionen (1)
 - Studierendenausweis (1, 2, 3), Dienstausweis (1, 2, 3), Angehörigenausweis (1, 2, 3), Bibliotheksausweis (1, 2, 3, 6), Semesterticket (4), DB Großkunden-Abo (5)
- Mifare-Chip (8)
 - Rückmeldung / Aufdruck der Gültigkeit, Zutrittskontrolle für Kfz – Stellplätze, Zutrittskontrolle für Gebäude und Räume, Arbeitszeiterfassung, Elektron. Geldbörse, Kopieren & Drucken
- Kryptoprozessor (7) – nur in Ilmenau
 - SB-Funktionen, wie An- und Abmeldung zu Prüfungen, Notenspiegel, Bescheinigungsdruck, Adressänderung
 - Signieren von E- Mails, Rücksetzen beim Passwortmanagement, Upload-/Download-Server, Administration von Mailinglisten

Layout der thoska+ an der TU Ilmenau

Rückseite



nicht personalisiert



Aspekte der Personalisierung

- Zusammentragen von Daten aus unterschiedlichen Quellen

- HISSOS, HISSVA (Name, Vorname, akad. Grad, ...)



- Bibliotheksbenutzerbarcode (Access-DB)



- Schlüsselpaar und Zertifikat (.p12)

OpenCA
„CA der Herzen“



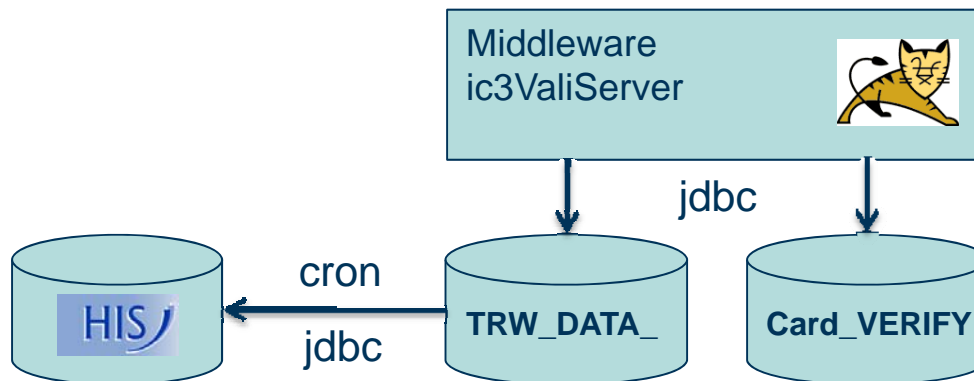
- Bilddatei (.jpg)



- Stammdatensatz in der Inter-card-Datenbank

Validierung

- flexiblen Validierung (FlexVali) der Firma Intercard
 - Validierungsinformationen nicht mehr direkt aus den Datenbanken von HISSOS und HISSVA
 - Relationale Datenbank mit TRW_DATA (Studierende) und TRW_DATA_PKZ1 (Mitarbeiter) als Zwischenschicht erforderlich
 - Befüllung der Zwischenstruktur durch die Einrichtung selbst
 - Vorteile: Zentrale Abspeicherung des Layouts, keine unnötigen Schreibprozesse auf den TRW-Streifen



„Sicherheitszertifikate“ als Dienst

- Ausgelagerte Zertifizierungsinstanz im Rahmen der DFN-PKI (seit Februar 2009)
- Trennung der technischen Aufgaben einer Zertifizierungsstelle (CA) von den organisatorischen Aufgaben einer Registrierungsstelle (RA)
- DFN bietet Schnittstellen zur Beantragung einzelner Zertifikate (Web) als auch einer großen Anzahl von Zertifikaten im "Self-Service" Verfahren (SOAP).
- Fortgeschrittene Zertifikate, zur Zeit für
 - Server
 - Grid Nutzer
 - Grid Server

Sicherheitszertifikate (DFN-PKI, Grid) www.tu-ilmenau.de/pki

The screenshot shows a web browser window displaying the 'Sicherheitszertifikate (DFN-PKI, Grid)' page of the University of Ilmenau. The browser is Windows Internet Explorer, and the address bar shows 'http://www.tu-ilmenau.de/unirz/Sicherheitszertifika.4603.0.html'. The website has a navigation bar with 'Deutsch' and 'English' language options, and a search bar. The main content area is titled 'Sicherheitszertifikate (DFN-PKI, Grid)' and 'Vertraulichkeit, Integrität und Authentizität von Daten'. It describes the university's digital certificate services, including the issuance of certificates for secure communication. A sidebar on the left lists various services offered by the UniRZ, with 'Sicherheitszertifikate (DFN-PKI, Grid)' highlighted. The bottom of the page shows the status bar with 'Internet | Geschützter Modus: Aktiv' and a 100% zoom level.

Universitätsrechenzentrum - Sicherheitszertifikate (DFN-PKI, Grid) - Windows Internet Explorer

http://www.tu-ilmenau.de/unirz/Sicherheitszertifika.4603.0.html

Deutsch | English

Kontakt | Übersicht | Suche | Erweiterte Suche | Impressum

Sie sind hier: Universitätsrechenzentrum » Dienste » Sicherheitszertifikate (DFN-PK...

Betriebseinheiten
Universitätsrechenzentrum

TECHNISCHE UNIVERSITÄT
ILMENAU

Sicherheitszertifikate (DFN-PKI, Grid)
Vertraulichkeit, Integrität und Authentizität von Daten

An der Technischen Universität Ilmenau werden digitale Zertifikate für eine sichere Kommunikation eingesetzt, wie zum Beispiel beim Zugriff auf die Dienste der Prüfungsämter und Studierendenverwaltung. Es handelt sich hierbei um Zertifikate auf Basis des X.509 Standards.

Für die Ausstellung, Verteilung und Prüfung digitaler Zertifikate entwickelte das UniRZ zunächst eine haus eigene Public Key Infrastructure (PKI) mit [eigener Zertifizierungsstelle](#) (CA – Certification Authority). Ein Zertifikat dieser PKI erhält jeder Benutzer auf dem Kryptoprozessor der multifunktionalen Chipkarte [thoska+](#).

Seit Anfang 2009 organisiert das UniRZ die Teilnahme an der DFN-PKI, der Public Key Infrastructure im Deutschen Forschungsnetz. Die Zertifizierungsstelle der Technischen Universität Ilmenau (TU Ilmenau CA) wurde an den DFN-Verein ausgelagert, um die technischen Aufgaben einer Zertifizierungsstelle von den organisatorischen Aufgaben einer Registrierungsstelle (RA – Registration Authority) zu trennen.

Das UniRZ übernimmt als Registrierungsstelle die Vermittlung digitaler Zertifikate von der DFN-PKI. Es unterstützt momentan die Ausstellung von Serverzertifikaten. Die Ausstellung von Nutzerzertifikaten im Rahmen der DFN-PKI wird derzeit organisatorisch-technisch geprüft.

Der DFN-Verein ist akkreditiertes Mitglied der European Grid Policy Management Authority (EUGridPMA) und stellt im Rahmen der DFN-PKI Grid Zertifikate für Server und Nutzer aus. Auch hier übernimmt das UniRZ als Registrierungsstelle die Vermittlung digitaler Grid Zertifikate.

→ [Beantragung von Serverzertifikaten](#)
Diese Zertifikatsart ist zum Beispiel für Webserver geeignet.

→ [Beantragung von Grid Nutzerzertifikaten](#)
Nur für Wissenschaftler, die an Grid-Projekten beteiligt sind.

→ [Beantragung von Grid Serverzertifikaten](#)
Nur für Server, die in Grid-Projekte eingebunden sind.

Startseite des UniRZ
Newsletter
Zentrale Auskunft
Kommunikationsnetze
Hörsaaltechnik
Zertifizierungsinstanz
Dienste
Accountübersicht
Mailsystem
TYPO3
Datenhaltung
Compute Service
MS WSUS-Server
McAfee Virenschutz
FTP-Server
Upload- & Download-Server
Sicherheitszertifikate (DFN-PKI, Grid)
Beantragung von Serverzertifikaten
Beantragung von Grid Nutzerzertifikaten
Beantragung von Grid Serverzertifikaten

Kontakt
Jörg Deutschmann
Telefon: 2649
joerg.deutschmann@tu-ilmenau.de

Internet | Geschützter Modus: Aktiv

Sicherheitszertifikate der DFN-PKI auf der multifunktionalen Chipkarte thoska+

- Realisierungsvorschlag: Trennung von Personalisierung und Registrierung
 - Zentrale Auskunft des UniRZ als Registrierungsstelle (RA)
- Treffen mit dem DFN-Verein am 02. September 2009
 - Organisatorische und technische Details
- Meta Directory intern am 23. Oktober 2009
 - Festlegung der Anforderungen (Auth., elektr. Sig., E-Mail-Schutz)
- Treffen mit Personalrat und Datenschutz am 20.01.2010
 - Anlage zur Dienstvereinbarung Chipkarte
 - Bestandteil des Verfahrensverzeichnis
 - Einverständniserklärung zur Datenübermittlung

DFN-PKI auf der thoska+

DFN-PKI

Zertifikatsantrag mit Identifizierung

Antragsnummer: 3360

Eindeutiger Name: emailAddress=joerg.deutschmann@tu-ilmenau.de, CN=Joerg Deutschmann, O=Technische Universität Ilmenau, C=DE

Public Key Fingerprint: D9:F0:4C:57:A6:ED:29:B3:B2:E3:9A:2D:33:93:F5:1E:13:3E:08:C7

Schlüssellänge: 2048

Veröffentlichen: Ja

Angaben zur Person

☐ Frau ☐ Herr

Vorname Nachname: Joerg Deutschmann

E-Mail: joerg.deutschmann@tu-ilmenau.de

Telefonnummer: _____

Ausweis (Art u. letzte 5 Zeichen der Nummer): _____

Abteilung / Institut: _____

Straße u. Hausnummer: _____

Postleitzahl u. Ort: _____

- Ich versichere, dass sämtliche Angaben im Antrag vollständig sind und der Wahrheit entsprechen.
- Ich kenne die gültigen Zertifizierungsrichtlinien und die Erklärung zum Zertifizierungsbetrieb und stimme ihnen zu.
- Ich stimme der Verarbeitung und Speicherung der bei der Zertifizierung anfallenden Daten zu. Die Daten werden gemäß den geltenden Datenschutzbestimmungen vertraulich behandelt.

(Ort, Datum) _____ (Unterschrift - wie im Ausweis) _____

Wird von der Registrierungsstelle ausgefüllt

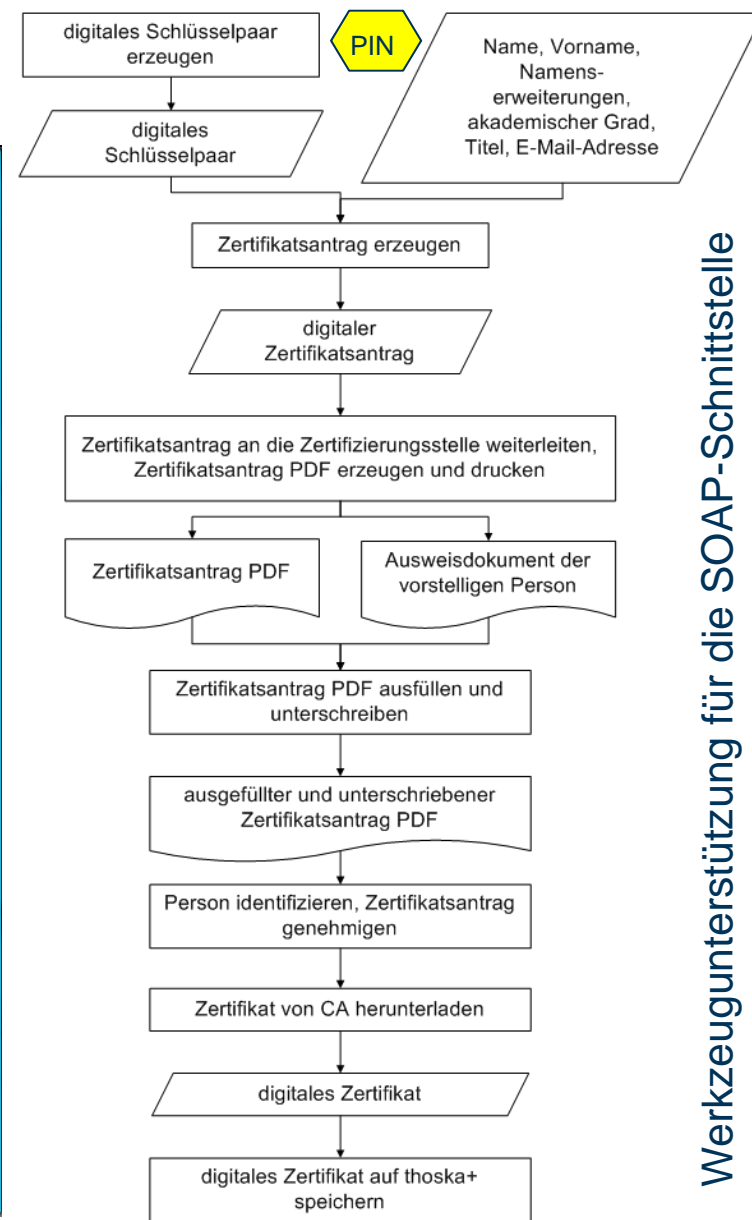
Prüfung der Ausweisdaten:

Name ☐ Unterschrift ☐ Bild ☐ Bereits geprüft ☐ Gültigkeit ☐ Nummer ☐

Name des Prüfers: _____

Zugehörige Registrierungsstelle: _____

(Datum, Unterschrift des Prüfers) _____



Werkzeugunterstützung für die SOAP-Schnittstelle
der DFN-PKI
mit Prototyp für Token Lifecycle Management

Zusammenfassung und Ausblick

- thoska-Projekt aus Sicht des UniRZ der TU Ilmenau
- thoska+ Mehrwert und mehr Aufwand durch fortgeschrittene Zertifikate an der TU Ilmenau
- Weitere Aufgaben
 - Ablösung des kontaktlosen Mifare-Chips durch Mifare DesFire
 - Verbesserung des thoska-Kartenmanagements u.a. mit IdM
 - Dokumente für Personalrat (DV) und Datenschutz (VV)
 - in Ilmenau Anpassung der Zertifizierungsrichtlinie (CP, CPS)
 - in Ilmenau Umsetzung der Prozesse für die Zentrale Auskunft des UniRZ als Registrierungsstelle (RA)