

## Anlage 2 Dienstausweis

Die Anlage Dienstausweis beschreibt die Chipkarte, die Chipkartenproduktion und den Transfer von personalisierten Daten aus einem Quellsystem, dem thoska-Kartenmanagementsystem (thosKMS), auf die Oberfläche (visuelle Daten) und den RFID-Chip der Chipkarte.

### 1. Bezeichnung

Dienstausweis

### 2. Kurzbeschreibung, Zweckbestimmung

Der Dienstausweis dient der visuellen Authentifizierung gegenüber Dritten.

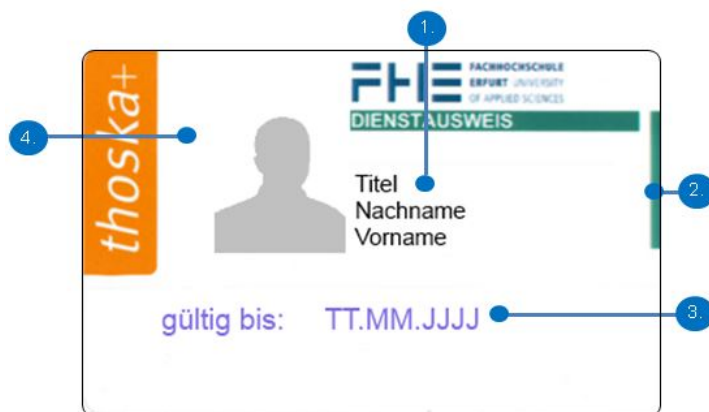


Abbildung 1: Vorderseite Chipkarte

1. Persönliche Daten
2. Farbbalken zur Unterscheidung der Ausweisarten:  
gelb: Studenten,  
grün: Mitarbeiter,  
blau: Bibliotheks- und  
Gästekarten
3. Gültigkeit
4. Lage des RFID-Chip (nicht sichtbar)



Abbildung 2: Rückseite Chipkarte

4. Lage des RFID-Chip (nicht sichtbar)
5. Bibliotheksbenutzernummer, auch als Barcode
6. Krypto-Chip

### 3. Benutzerkreis

Die Chipkarte ist Dienstausweis für alle Beschäftigten und Professoren.

### 4. Hardwareausstattung und Systembeschreibung

Das CIS besteht aus CIS-Anwendungsserver, CIS-Datenbankserver, CIS-Validierungsserver, Validierungsstation und einer Kartenpersonalisierungsstation. Die Kartenpersonalisierungsstation besteht aus einem Computer inkl. Kartendrucker (Druck/Codierung) und Validierungsgerät (siehe Abbildung 3).

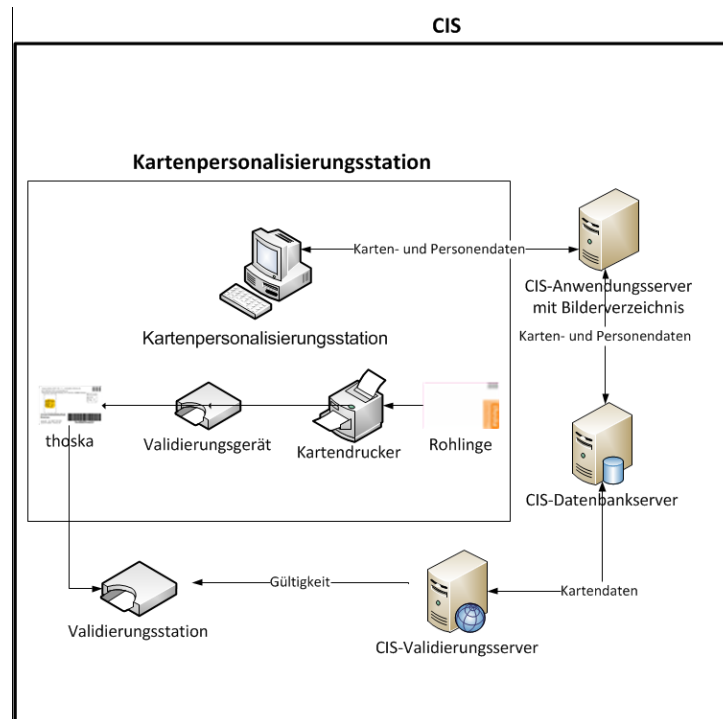


Abbildung 3: CIS

Die Personalisierung wird durch den thoska-Beauftragten durchgeführt. Personenbezogene Daten stammen aus dem thosKMS. Die Befüllung des thosKMS wird in der Anlage 10 der „Dienstvereinbarung zu Einführung und Betrieb des Meta Directory mit den daran angeschlossenen Quell- und Zielsystemen (Identity Management System)“ behandelt und ist somit nicht Gegenstand dieses Dokuments. Durch die smart.Life Software erfolgt in Zusammenarbeit des CIS-Anwendungsservers mit dem CIS-Datenbankserver die Personalisierung der Chipkarte auf der Kartenpersonalisierungsstation. Der Validierungsserver aktualisiert über das Validierungsgerät bzw. die Validierungsstation die Gültigkeit der Chipkarte.

## 5. Authentifizierung des Benutzers und Nutzungsvorgang

Bei der Verwendung als Dienstaussweis wird die Chipkarte vorgezeigt.

## 6. Nutzung des Datennetzes und Schnittstellen

Das thosKMS und das CIS befinden sich in unterschiedlichen Subnetzstrukturen des FHE-Netzes. Die Kommunikation zwischen den Systemen erfolgt ausschließlich über gesicherte Verbindungen. Die Netzsicherheit wird im Sicherheitskonzept der Fachhochschule Erfurt beschrieben. Insbesondere gilt, dass durch die Einordnung der Server in Subnetzstrukturen ein hohes Maß an Sicherheit gewährleistet ist. Für die Regelwerke der Firewalls gilt, dass alles verboten ist, was nicht dediziert erlaubt wurde. Somit wird gewährleistet, dass alle nichtadministrativen Zugriffe von außerhalb der geschützten Netzsegmente abgewiesen werden.

Der Datentransfer erfolgt für die Personalisierung und Validierung. Daten abgebende Stellen sind das thosKMS und das Bilderverzeichnis. Daten übernehmende Stellen sind die Personalisierungsstation, die Validierungsstationen und die CIS-Server (CIS-Anwendungsserver, CIS-Datenbankserver, CIS-Validierungsserver).

Alle oben genannten Systeme werden vom HRZ betreut.

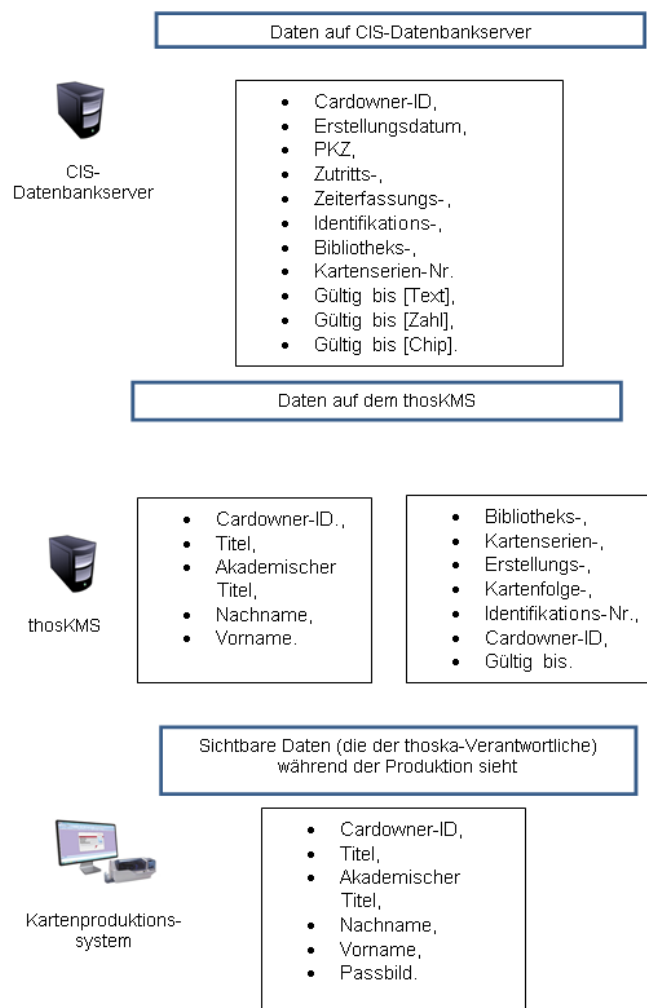
## 7. Daten und Datenverarbeitung

Folgende Daten befinden sich auf der Chipkarte:

Daten	Herkunft	Speicherort	Verarbeitung / Definition
<b>Systemdaten</b>			
Kartenserienn-Nr.	RFID-Chip	CIS-Datenbank, RFID-Chip	Zur eindeutigen Unterscheidung der Chipkarte
Schlüssel	RFID-Chip	RFID-Chip	Zur Kommunikation der Chipkarte mit berechtigten Lesegeräten.
Geldbörse	RFID-Chip	RFID-Chip	Dient der bargeldlosen Bezahlungsfunktion mit der Chipkarte.
<b>Berechtigungsdaten</b>			
PKZ	CIS-Anwendungs-server	CIS-Datenbank	Preisermäßigungsschlüssel für Bezahlungsfunktion.
Cardowner-ID	thosKMS	CIS-Datenbank, RFID-Chip	Zur eindeutigen Zuordnung der Karte zum Nutzer.
Identifikations Nr.	thosKMS	CIS-Datenbank	Zur Erstellung von Kartenfolgennummern
Titel	thosKMS	Chipkarte (Druck)	Zur optischen Authentifizierung des Karteninhabers
Akademischer Titel	thosKMS	Chipkarte (Druck)	
Nachname	thosKMS	Chipkarte (Druck)	
Vorname	thosKMS	Chipkarte (Druck)	
Passfoto		Bilderverzeichnis, Chipkarte (druck)	
Diese Daten werden vom Anwendungsserver in die Datenbank des CIS-Datenbankservers zurückgeschrieben und für den Validierungsserver bereitgehalten.			
Gültig bis [Text]	CIS-Validierungsserver	CIS-Datenbank, Chipkarte (Druck)	Text: „Gültig bis“
Gültig bis [Zahl]	CIS-Validierungsserver	CIS-Datenbank, Chipkarte (Druck)	Datum
Gültig bis [Chip]	CIS-Validierungsserver	CIS-Datenbank, RFID-Chip	Datum
Während der Produktion der Chipkarte entstehen folgende Daten:			
Zutritts-Nr.	CIS-Anwendungs-server	CIS-Datenbank, thosKMS, RFID-Chip	Zur Authentifizierung des Karteninhabers im Zutrittssystem.

Zeiterfassung-Nr.	CIS-Anwendungs-server	CIS-Datenbank, thosKMS, RFID-Chip	Zur Authentifizierung des Karteninhabers im Zeiterfassungssystem.
Bibliotheks-Nr. und -Barcode	CIS-Anwendungs-server	CIS-Datenbank, thosKMS, RFID-Chip	Zur Authentifizierung des Karteninhabers in der Bibliothek.
Erstellungsdatum	CIS-Anwendungs-server	CIS-Datenbank	Nötig um Folgekarten zu erstellen.
<b>Ereignisdaten</b>			
<p>Während der Produktion der Chipkarte und Nutzung des CIS-Datenbankservers wird eine Protokolldatei erstellt. In dieser befinden sich keine personenbezogenen Daten, sondern nur Auskünfte über die Funktionsweise des Systems.</p> <p>Auf dem CIS-Anwendungsserver wird eine Protokolldatei erstellt, in der Zugriffe auf die Datenbank protokolliert werden.</p> <p>Auf dem CIS Validierungsserver werden 9 Protokolle erstellt. Diese geben Auskunft über verschiedene Zugriffe und Funktionsweisen der einzelnen Systeme. Hier werden keine personenbezogenen Daten gespeichert.</p>			

Im Folgenden sind die Speicherorte der Daten grafisch dargestellt:



Im Prozess der Personalisierung wird von der Software „smart.Life“, die sich auf dem CIS-Anwendungsserver befindet, ein temporärer Datensatz angelegt. Dieser temporäre Datensatz führt die Personendaten aus dem thosKMS und die Chipkartendaten zum Zwecke der Kartenproduktion zusammen.

Bei der Kartenproduktion werden Name, Vorname, akademischer Titel und ein Passbild auf die Chipkarte gedruckt (visuelle Daten). Die zur Authentifizierung in verschiedenen Anwendungen benötigten Chipkartendaten werden erzeugt (Bibliotheks-, Zutritts- und Zeiterfassungsnummer) und zusammen mit der Cardowner-ID und der Kartenseriennummer auf dem RFID-Chip der Chipkarte und auf dem CIS-Datenbankserver gespeichert.

Im Validierungsprozess werden vom CIS-Validierungsserver die Daten für die Validierung zusammengestellt. Es wird aus dem thosKMS für die betreffende Person das späteste Enddatum des Beschäftigungsverhältnisses gelesen. Entsprechend dem Enddatum ergibt sich eine Gültigkeit der Chipkarte von maximal 5 Jahren. Das Enddatum wird auf den TRW-Streifen (ThermoReWrite: wiederbeschreibbarer Bereich der Chipkarte) sichtbar auf die Chipkarte gedruckt und in den CIS-Datenbankserver übernommen. Auf dem Validierungsserver werden das Datum der Validierung und die Nummer der Validierungsstation gespeichert.

Der Krypto-Chip bleibt bei diesem Verfahren unberührt.

Die Löschfristen für die Bilder sowie der Daten auf dem CIS-Datenbankserver werden analog zur „Dienstvereinbarung zu Einführung und Betrieb des Meta Directory mit den daran angeschlossenen Quell- und Zielsystemen (Identity Management System)“ angewandt.

## **8. Auswertung**

Es erfolgen keine Auswertungen.

## **9. Maßnahmen zur Datensicherheit**

Die CIS-Server stehen in einem gesicherten Bereich des HRZ, der baulich und technisch vor unbefugten Zugriffen geschützt ist. Die Personalisierungs- und Validierungsstationen stehen ebenfalls in einem gesicherten Bereich. Der Datenaustausch der CIS-Server erfolgt ausschließlich über eine verschlüsselte Verbindung.

Die CIS-Server sind durch eine Firewall geschützt, die Anlagen werden nur durch die Systemadministratoren, die Thoska-Beauftragten oder ihre Vertreter bedient und sind zusätzlich durch Passwort auf die personelle Benutzung beschränkt.

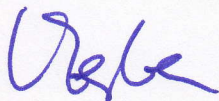


### 10. Übersicht Benutzermanagement

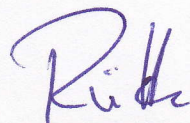
Rolle	Rechte	Beschreibung
Administrator	Vollzugriff: lesen, schreiben, ändern, ausführen, löschen	Administratoren sind Personen die Vollzugriff auf die CIS-Systeme, ihre Anwendungen und Daten haben.
Produzent	In Software smart.Life: lesen und ausführen	Der Produzent nutzt die Kartenproduktionsstation und darf Karten produzieren.

Administratoren der CIS-Systeme werden auf der Homepage der Fachhochschule Erfurt benannt, ebenso die Ansprechpartner für Anwender/Nutzer.

Erfurt, den 29.08.2014



Prof. Dr. V. Zerbe  
Leiter der Hochschule



Claudia Rütten  
amt. Kanzlerin



Karola Güth  
Personalrat