
# Campuskartenschnittstellen zu Anwendungen

Integration der Campuskarten als verlässliches Zugangskontrollsystem für WEB-basierte Anwendungen.

Berlin, den 29.05.2002

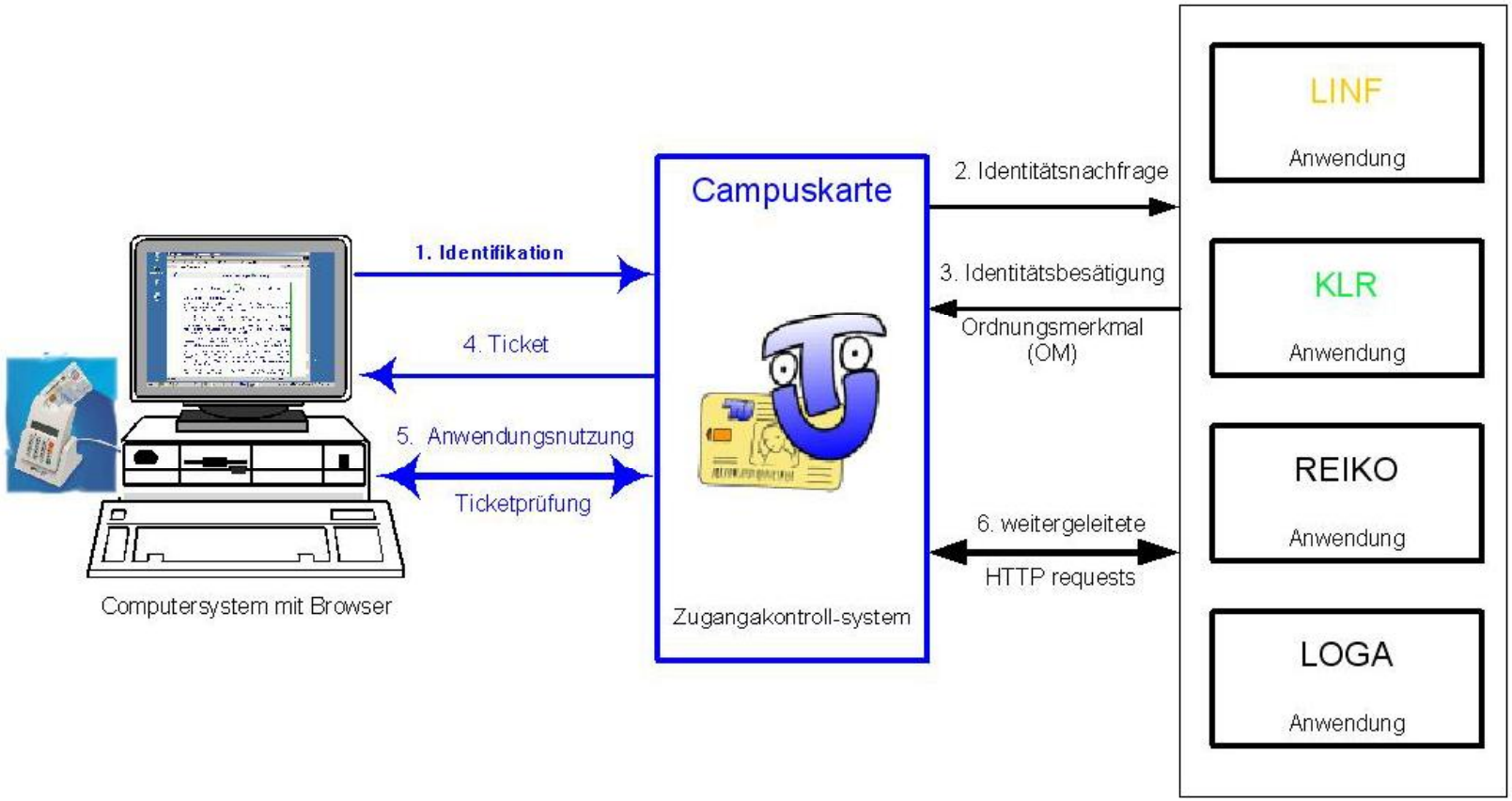


# Inhalt

- Funktionsstruktur der Zusammenarbeit von Zugangskontrolle und Anwendung.
- Welche Daten werden zwischen Zugangs-kontrolle und Anwendung ausgetauscht?
- Interaktion zwischen Zugangskontrolle und Anwendung.
- Daten zur Identifikationsauthentisierung.

# Funktionsstruktur der Zusammenarbeit von Zugangskontrolle und Anwendung

## Zusammenarbeit zwischen Campuskarteninfrastruktur und Anwendungen



# Funktionsstruktur der Zusammenarbeit von Zugangskontrolle und Anwendung

## *Authentisierungsverfahren*

- Name-Passwort-Authentisierung
- Smart-Card-Authentisierung

## *Anwendung der Authentisierungsverfahren*

- Name-Passwort-Authentisierung
- Smart-Card-Authentisierung
- Beide Verfahren gemeinsam

# Funktionsstruktur der Zusammenarbeit von Zugangskontrolle und Anwendung

## *Clientsystemvoraussetzungen*

- WEB-Browser der folgende Eigenschaften unterstützt:
  - SSL-Verbindungen,
  - Schlüsselaushandlung für SSL über X509v3 Zertifikate in PEM- oder DER-Codierung mit einer 1024 Bit Schlüssellänge,
  - Ausführung von Java Applets.
- Installierte Java Runtime Environment die:
  - der Funktion der SUN JRE Version 1.2.1 entspricht,
  - vom installierten Browser zur Ausführung der Applets, genutzt werden kann.

# Welche Daten werden zwischen Zugangskontrolle und Anwendung ausgetauscht?

## *Name-Passwort Authentisierung*

| Campuskartensystem | Anwendung |
|---|---|
| • Name, Passwort | • Name, Passwort Überprüfung |
| • Ordnungsmerkmal (OM) | • Ordnungsmerkmal (OM) |
| • geg. Rechtedescriptor | • geg. Rechtedescriptor |

## *Smart-Card Authentisierung*

| Campuskartensystem | Anwendung |
|---|---|
| • PIN | • Ordnungsmerkmal (OM) |
| • Ordnungsmerkmal (OM) | • geg. Rechtedescriptor |
| • geg. Rechtedescriptor | |

# Welche Daten werden zwischen Zugangskontrolle und Anwendung ausgetauscht?

## *Tickets*

**User Ticket**

- Ausstellungszeit
- Gültig bis
- IP-Nummer
- SSL-Key
- Data:
  - OM (Ordnungsmerkmal)
  - PS (Personenstatus)
  - von
  - bis
  - applikationsspezifische Daten

**Domain Ticket**

- Host1
- Host2
- Host3

Interaktion zwischen Zugangskontrolle und Anwendung.

## *Name-Passwort Authentisierung*

- Erfassung der Identitätskennung.
- Übergabe der Identitätskennung an die Anwendung zur Prüfung.
- Entgegennahme eines der Identität zugeordneten Ordnungs-merkmals (OM).
- Übermittlung des OMs an die Anwendung zur Überprüfung der Nutzungsrechte.
- Entgegennahme eines Rechtedescriptors von der Anwendung.

Interaktion zwischen Zugangskontrolle und Anwendung.

## *Smart-Card Authentisierung*

- Verifikation der Smart-Card.
- Evaluierung des Ordnungsmerkmals auf der Karte.
- Übergabe des OMs an die Anwendung zur Überprüfung der Nutzungsrechte.
- Entgegennahme eines Rechtedescriptors von der Anwendung.

# Daten zur Identifikationsauthentisierung.

## *Name-Passwort Authentisierung*

- Name
- Passwort

## *Alle Authentisierungsverfahren*

- Ordnungsmerkmal (OM)
- Rechtedescriptor