Fachhochschule Brandenburg

Vorstellung des Projektes

www.CIDAS.org

Configurable Internet Directory and Authentication Service

Projektgruppe CIDAS
<info@cidas.org>

Brandenburg, den 18. Mai 2005

Gliederung

1. Vertrauen und Sicherheit im Internet
2. Datenschutz und Datensicherheit
3. Identity-Management-Systeme
4. Existierende Lösungen
5. CIDAS – Aufbau und Funktionsweise
6. Authentifizierung mit passiven Speichermedien
7. CIDAS-Kommunikation
8. Anbindung von Applikationen
9. Kooperationsmöglichkeiten

1. Vertrauen und Sicherheit im Internet

- Vertrauen und Sicherheit im Internet?

  1. Identifizierung – Wer ist ein Benutzer?
  2. Authentifizierung – Ist er es wirklich?
  3. Autorisierung – Was darf er?

- Identifizierung und Authentifizierung werden üblicherweise über die Eingabe eines Benutzernamen und eines Passwortes realisiert
- Wieviele Passworte haben Sie? – Wie merken Sie sich die?
- Warum können Sie Chipkarten, Fingerprint-Sensoren, usw. nicht allgemein nutzen?

2. Datenschutz und Datensicherheit

- immer wieder Skandale um Datenweitergabe
- Haben kleinere Anbieter genügend Know-How, um gespeicherte Daten zu schützen?
- Wie werden personenbezogene Daten in Sites gespeichert, wie wird mit ihnen umgegangen?
- Anbieter haben keinen Einfluss/ wissen nicht, wie beim Hosting-Partner mit den Daten umgegangen wird
- Benutzer haben häufig keine Möglichkeiten zur Dateneinsicht bzw. zur Änderung gespeicherter Daten

3. Identity-Management-Systeme

Gebotene Funktionalität:

- Access-Management
- Passwort-Synchronisierung
- Single-Sign-On
- Passwort-Reset

- Sammelbegriff für Lösungen zur Vereinfachung von administrativen Aufgaben im Bereich der Benutzerverwaltung in Computernetzwerken
- vereinfachen Umsetzung von Richtlinien für Datenschutz und Sicherheit
- Vorteile sowohl für Administratoren als auch Benutzer

3. Identity-Management-Systeme

Gebotene Funktionalität:

- Access-Management
- Passwort-Synchronisierung
- Single-Sign-On
- Passwort-Reset

- Autorisierungsinformationen werden an einer zentralen Stelle gespeichert
- dementsprechend auch zentrale Verwaltung von Zugriffsrechten

3. Identity-Management-Systeme

Gebotene Funktionalität:

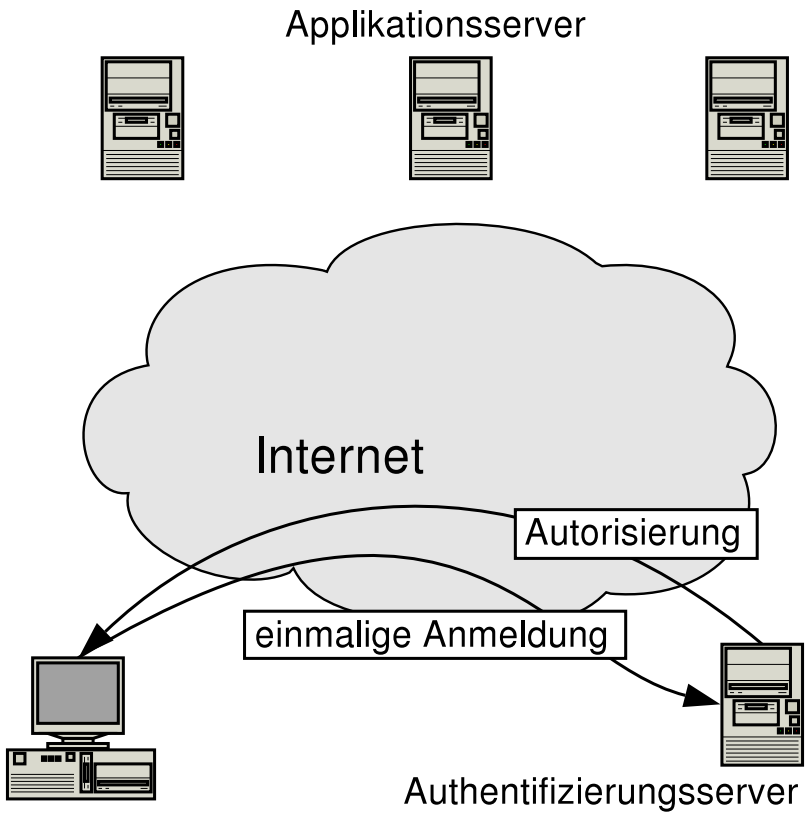
- Access-Management
- Passwort-Synchronisierung
- Single-Sign-On
- Passwort-Reset

- Identity-Management-System speichert Passwort eines Benutzers und verbreitet es auf alle benutzten Anwendungen
- Benutzer kann sich anschließend überall mit dem gleichen Passwort anmelden
- erhöhtes Sicherheitsrisiko durch Übertragung und Speicherung von Passworten

3. Identity-Management-Systeme

Gebotene Funktionalität:

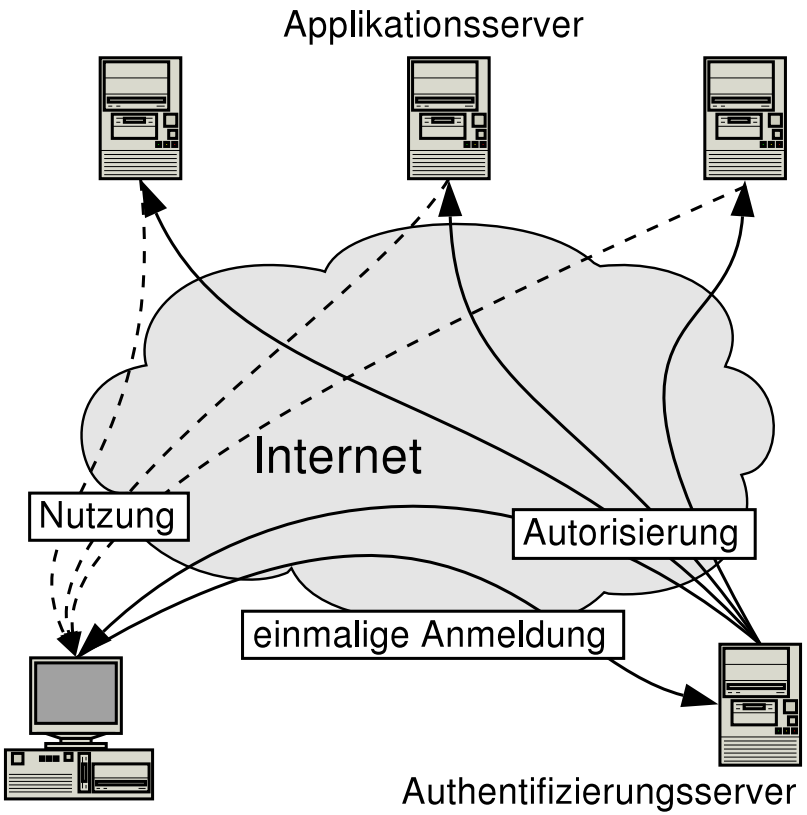
- Access-Management
- Passwort-Synchronisierung
- Single-Sign-On
- Passwort-Reset



3. Identity-Management-Systeme

Gebotene Funktionalität:

- Access-Management
- Passwort-Synchronisierung
- Single-Sign-On
- Passwort-Reset



3. Identity-Management-Systeme

Gebotene Funktionalität:

- Access-Management
- Passwort-Synchronisierung
- Single-Sign-On
- Passwort-Reset

- Identity-Management-Lösungen stellen dem Benutzer Möglichkeiten zur Verfügung, ihre Authentifizierungsdaten selbstständig zurückzusetzen
- neue Passworte werden automatisch, beispielsweise per E-Mail oder Post zugestellt
- Reduzierung von administrativen Tätigkeiten

4. Existierende Lösungen

- Evidian
- Microsoft Passport
- Liberty Alliance Project
- RSA Security Inc.
- CIDAS

- seit ca. 5 Jahren gibt es verschiedene Lösungsansätze
- Produktreife noch nicht bei allen erreicht
- Probleme bei Sicherheit und Datenschutz
- bislang nur geringe Akzeptanz im Internet, auch Firmenintern nur selten eingesetzt

4. Existierende Lösungen

- Evidian
- Microsoft Passport
- Liberty Alliance Project
- RSA Security Inc.
- CIDAS

- Web Edition - transp. Proxy
- Standard Edition - Windows-Plattformen und IE, Legacy-Anwendungen
- Automatische Passwort-Generierung und -Änderung
- Dezentrale Administration und globale Replikation
- Closed Source, ab 10.000 EUR + 20% Wartung jährlich

4. Existierende Lösungen

- Evidian
- Microsoft Passport
- Liberty Alliance Project
- RSA Security Inc.
- CIDAS

- Lösung mit derzeit größtem Kundenbestend von ca. 250 Mio.
- zentrale Datenhaltung auf Microsoft-Server
- Bedenklich vorrangig aus der Sicht des Datenschutzes
- von Anbietern von Internet-Diensten bislang kaum akzeptiert

4. Existierende Lösungen

- Evidian
- Microsoft Passport
- Liberty Alliance Project
- RSA Security Inc.
- CIDAS

- entstand in direkter Konkurrenz zu Passport, Entwicklung wird in Kooperation von ca. 150 Firmen betrieben
- erlaubt dezentrale Datenhaltung, es gibt so genannte Identity-Provider, die eine Authentifizierung gewährleisten
- Spezifikationen frei verfügbar, bislang keine Produkte

4. Existierende Lösungen

- Evidian
- Microsoft Passport
- Liberty Alliance Project
- RSA Security Inc.
- CIDAS

- verwenden HTTP als Kommunikationsprotokoll und eignen sich damit prinzipiell nur für WWW-Dienste
- es werden Cookies oder Weiterleitungen für den Datenaustausch verwendet, Angriffe sind bekannt
- unterstützen nur textuelle Authentifizierungsverfahren

4. Existierende Lösungen

- Evidian
- Microsoft Passport
- Liberty Alliance Project
- RSA Security Inc.
- CIDAS

- bietet Hardware-basierte Sicherheitslösungen an
- geeignet für WWW-Dienste
- Closed-Source-Lösung

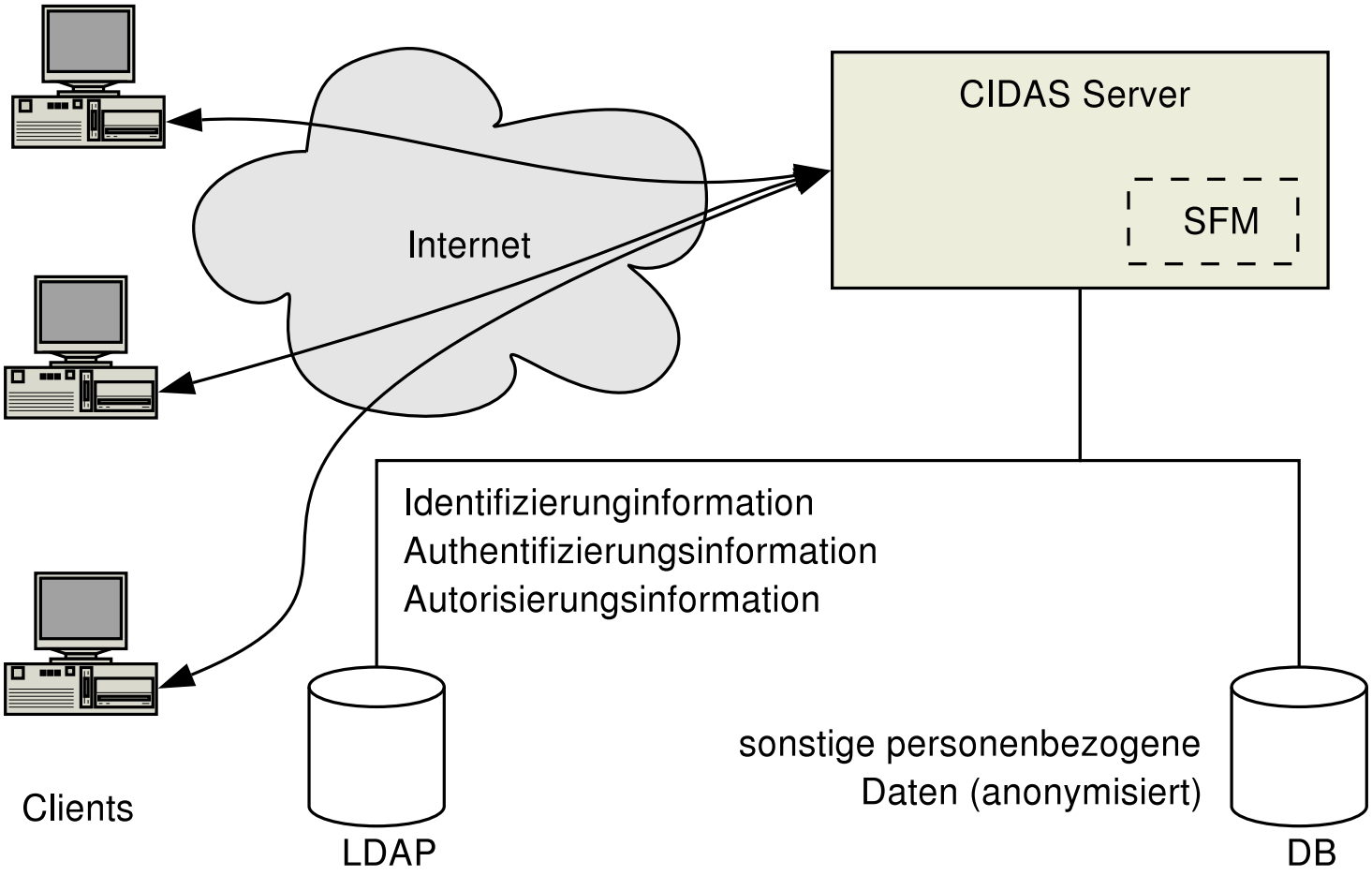
4. Existierende Lösungen

- Evidian
- Microsoft Passport
- Liberty Alliance Project
- RSA Security Inc.
- CIDAS

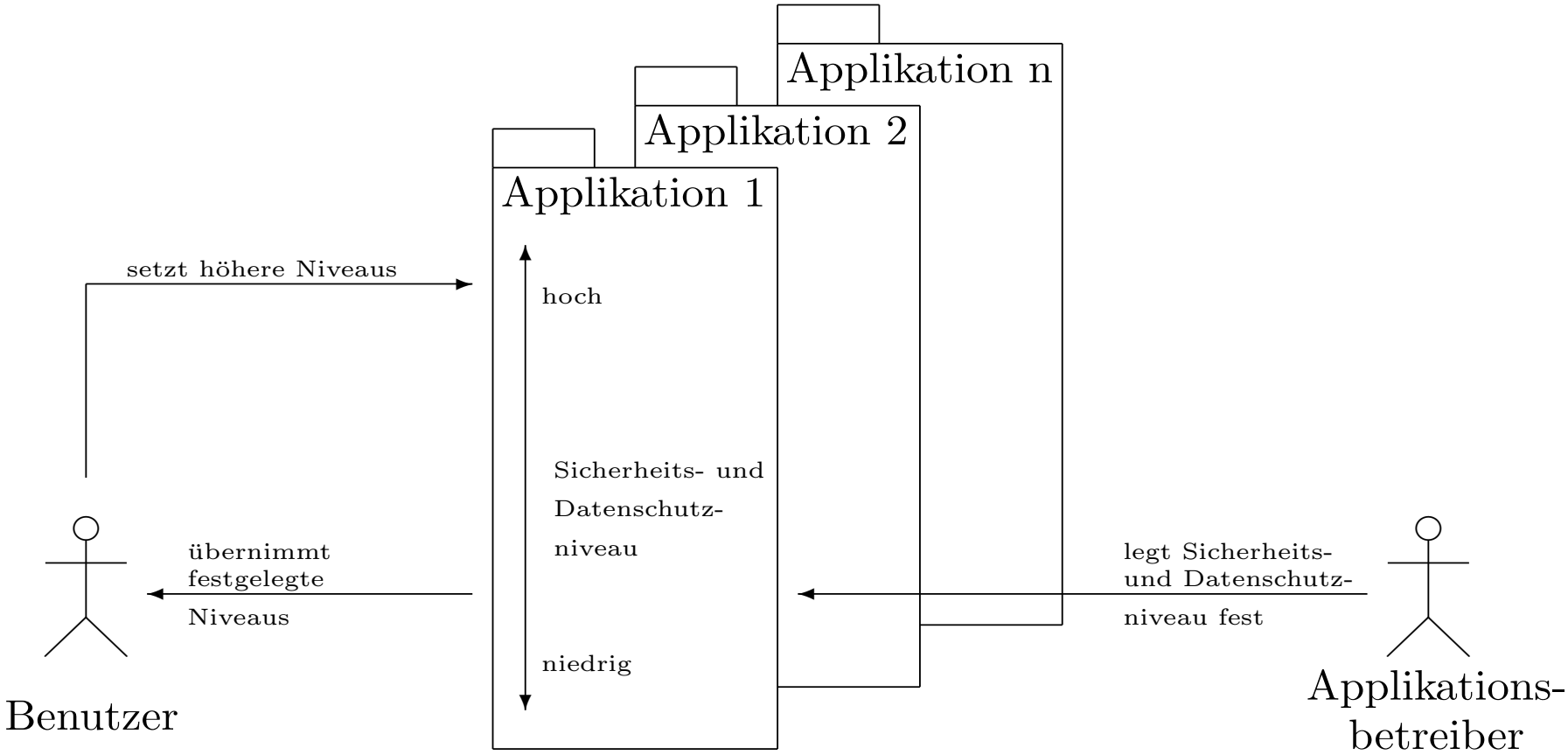
Configurable Internet Directory and Authentication Service

- ist ein freier, vielseitiger und skalierbarer Lösungsansatz
- Entwicklung vorrangig an der FH Brandenburg in Kooperation mit regionalen Partnern

5. CIDAS – Aufbau und Funktionsweise



5. CIDAS – Sicherheitsstufen



5. CIDAS – Authentifizierungsverfahren

Sich.-stufe	Identifizierung	Authentifizierung
...	beliebig	einfache textuelle Verfahren
3	beliebig	Biometrie, sichtbare Merkmale
4	1 eindeutiges Merkmal	Passwort
5	1 eindeutiges Merkmal	Biometrie, unsichtbare Merkmale
6	1 eindeutiges Merkmal	kryptographische Verfahren mit passiven Datenträgern
7	1 eindeutiges Merkmal	kryptographische Verfahren mit aktiven Datenträgern
...	1 eindeutiges Merkmal	kombinierte Verfahren

5. CIDAS – Zusammenfassung

- Client- und Server-basierter Lösungsansatz, eigenes Kommunikationsprotokoll
- dezentrale Datenhaltung möglich, Verzeichnisdienst
- einfache Erweiterbarkeit durch hohe Modularität
- erlaubt Integration beliebiger Authentifizierungssysteme und -verfahren
- weitreichende Unterstützung von Anwendungen
- offene Spezifikationen, offenen Quellen, freie Verfügbarkeit

6. Authentifizierung mit passiven Speichermedien

- Speicherung von Schlüsselmaterial auf passiven, identifizierbaren Medien
- Einsetzbarkeit in heterogenen Umgebungen; es sind die verschiedensten transportablen Speicher benutzbar
- Verwendung von asymmetrischer Kryptographie
- Verwendung standardisierter Datenformate
- Benutzer müssen keine nicht von ihnen beeinflußbaren Daten signieren
- Spezifikation des Verfahrens ist frei verfügbar

6. Authentifizierung mit passiven Speichermedien

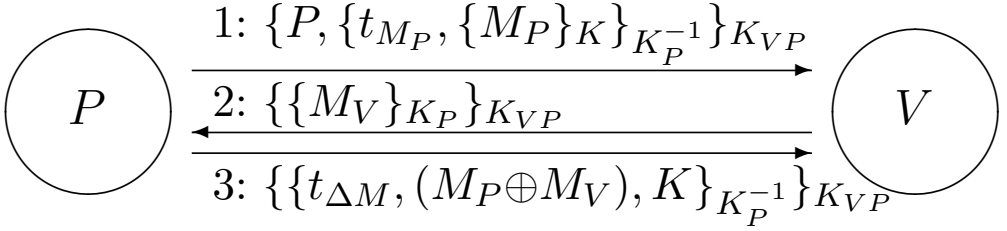
- eigenes Verfahren auf Basis von OpenPGP oder S/MIME
- Nachrichtenaustausch:

t : Zeitstempel

M : Nachrichten

K : Schlüssel

$\{M\}_K$: M verschlüsselt mit K



7. CIDAS-Kommunikation – Client und Server

- Clients und Server als auch Server untereinander kommunizieren über ein eigens hierfür konzipiertes Protokoll, Spezifikationen sind frei verfügbar
- Funktionsumfang:
  - Identifizierung, Authentifizierung
  - Behandlung und Austausch von Autorisierungsinformationen
  - Änderungen an den Datenbeständen
  - Nutzung zusätzlicher Funktionalität des Servers
- Sicherung von Vertraulichkeit und Integrität aller übertragener Daten wird auf der Ebene des Transprotprotokolls realisiert

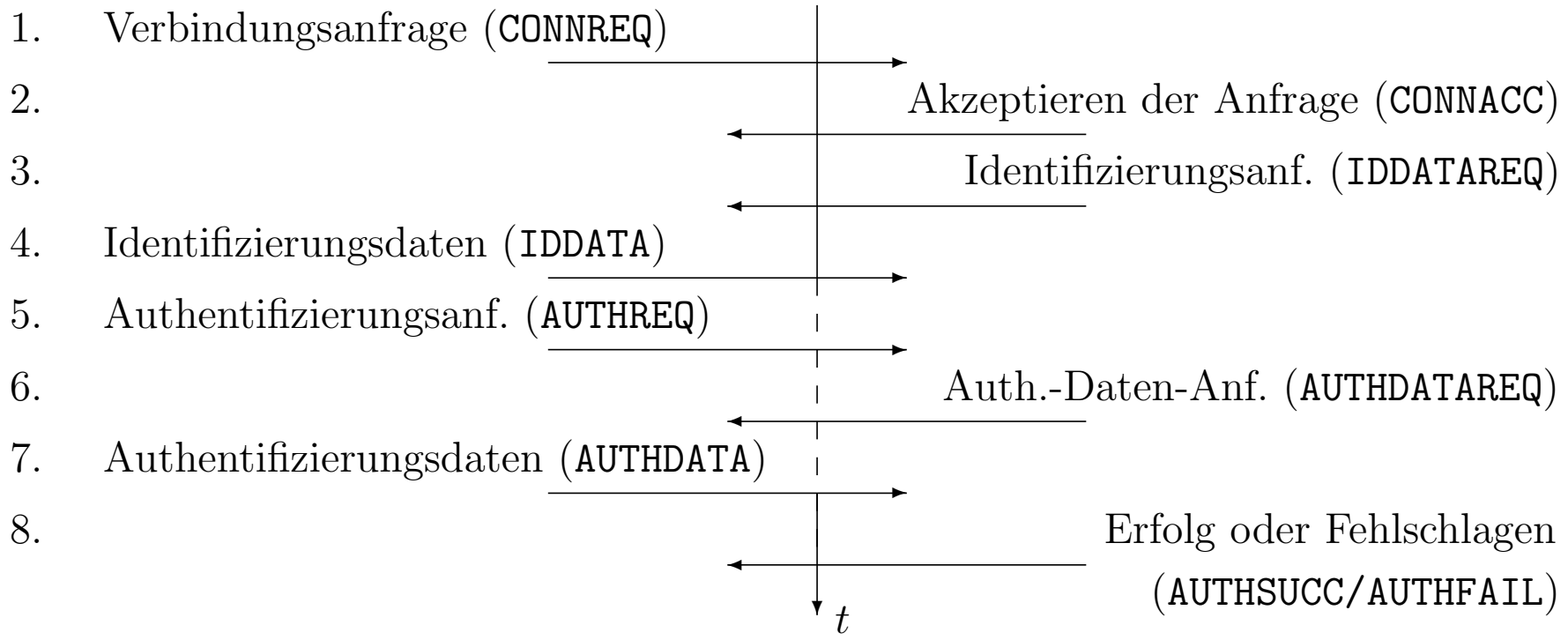
7. CIDAS-Kommunikation – Protokollaufbau

- Designentscheidungen:
  - Nachrichtenorrientiertheit
  - Zustandsabhängigkeit
  - Verwendung von XML
  - Nutzung von SSL/TLS

Oktett 0 0 1 2 3 4 5 6 7	Oktett 1 0 1 2 3 4 5 6 7	Oktett 2 0 1 2 3 4 5 6 7	Oktett 3 0 1 2 3 4 5 6 7
PVer	PSubVer	MType	Flags
SeqC0	SeqC1	PSize0	PSize1
SID0	SID1	SID2	SID3
SID4	SID5	SID6	SID7
Payload Payload Payload ...			

Aufbau einer CIDAS-Nachricht

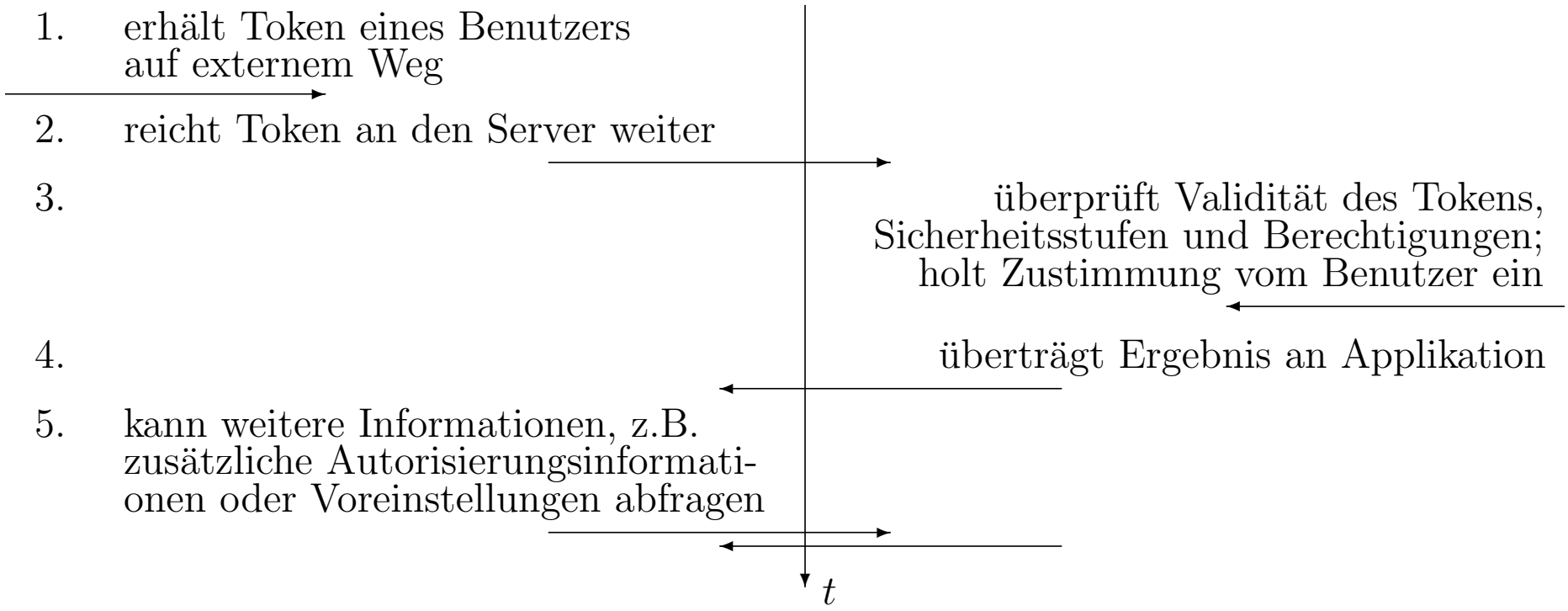
7. CIDAS-Kommunikation – Protokollablauf



7. CIDAS-Kommunikation – Token

- Autorisierungsinformationen werden vom CIDAS-Server direkt verbreitet
- es werden *Token* zur Identifizierung eines Benutzers durch eine Applikation und zur Zuteilung von Autorisierungsinformationen verwendet
- CIDAS-Server gibt generische Autorisierungsinformation („darf“ oder „darf nicht“) zurück
- beliebig hohe Granularität der Autorisierung kann duch nachträgliche Abfrage von Applikationsattributen erreicht werden

7. CIDAS-Kommunikation – Token-Austausch



8. Anbindung von Applikationen

- CIDAS unterstützt sowohl die Anmeldung auf Arbeitsplatz-Systemen als auch die Benutzerauthentifizierung für Web-basierte Anwendungen
- eingebunden werden kann jede Anwendung, die das CIDAS-Protokoll implementiert, über eine Schnittstelle zu einem CIDAS-Client verfügt oder bereits LDAP zur Authentifizierung verwendet
- Schnittstellen zu Legacy-Anwendungen vorgesehen, jedoch bislang nicht verfügbar
- sowohl Client als auch Server werden für viele gängige Betriebssysteme verfügbar sein

8. Anbindung von Applikationen

- kurzfristig werden folgende Applikationsgruppen unterstützt werden:
  - auf Apache und PHP basierende Web-Anwendungen
  - sicherheitskritische Applikationslogik in CIDAS-SFMs
  - UNIX-Worstation-Logins und Anbindung an PAM
- für Windows basierte Arbeitsplatzsysteme wird mittelfristig ein Client verfügbar sein, der die Verwendung weiterer Dienste gestattet
- die Fertigstellung eines CIDAS basierten Windows-Logins ist derzeit nicht abzusehen

9. Kooperationsmöglichkeiten

- Wir bieten an:
  - in absehbarer Zeit ein marktreifes, freies, universell einsetzbarse und einfach erweiterbares Identity-Management-System
  - Unterstützung bei Wartung, Integration und Erweiterung des Systems
  - Technologietransfer zwischen Hochschule und Industrie

9. Kooperationsmöglichkeiten

- Wir benötigen:
  - Know-How und Arbeitskräfte im Bereich der Realisierung des Windows-Clients
  - Unterstützung beim Ausbau der Server-Software und des UNIX-Clients
  - Realitätsnahe Testumgebungen
  - Anforderungsanalysen aus Unternehmen, Verwaltungs- und Forschungseinrichtungen mit Problemen in den Bereichen Benutzerverwaltung und Sicherheit

Kontakt

Internet:

http://www.cidas.org — info@cidas.org

Das Team:

Prof. Dr. Friedich-L. Holl
<holl@fh-brandenburg.de>

Jan Tobias Mühlberg
<muehlber@fh-brandenburg.de>

Dipl. Wi-Inform. (FH)
Ingo Schäfer
<schaefei@fh-brandenburg.de>

Markus Dahms
<dahms@fh-brandenburg.de>