Fachhochschule Brandenburg

Kolloquium zur Diplomarbeit

„Konzeption und prototypische Umsetzung von Authentifizierungsverfahren und Kommunikationsschnittstellen für das Identity-Management-System CIDAS unter besonderer Berücksichtigung mobiler identifizierbarer Datenträger“

Vorgelegt von:

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

Betreut von:

Prof. Dr. Friedrich-L. Holl und
Prof. Dr. Barbara Wiesner

Brandenburg, den 25. Mai 2004

Gliederung

1. Problemstellung
2. CIDAS
3. Aufgabe für die Diplomarbeit
4. Entwurf des Kommunikationsprotokolls
5. Entwurf des Authentifizierungsverfahrens
6. Demonstration des Prototypen
7. Zusammenfassung und Ausblick

1. Problemstellung – Vertrauen im Internet

- Sicherheit und Vertrauen im Internet?
  → Identifizierung, Authentifizierung
  → Autorisierung

- Wieviele Passworte haben Sie? – Wie merken Sie sich die?

- Nutzbarkeit anderer Authentifizierungsverfahren?

1. Problemstellung – Moderne Lösungsansätze

Identity-Management-Systeme:

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

1. Problemstellung – Moderne Lösungsansätze

Identity-Management-Systeme:

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

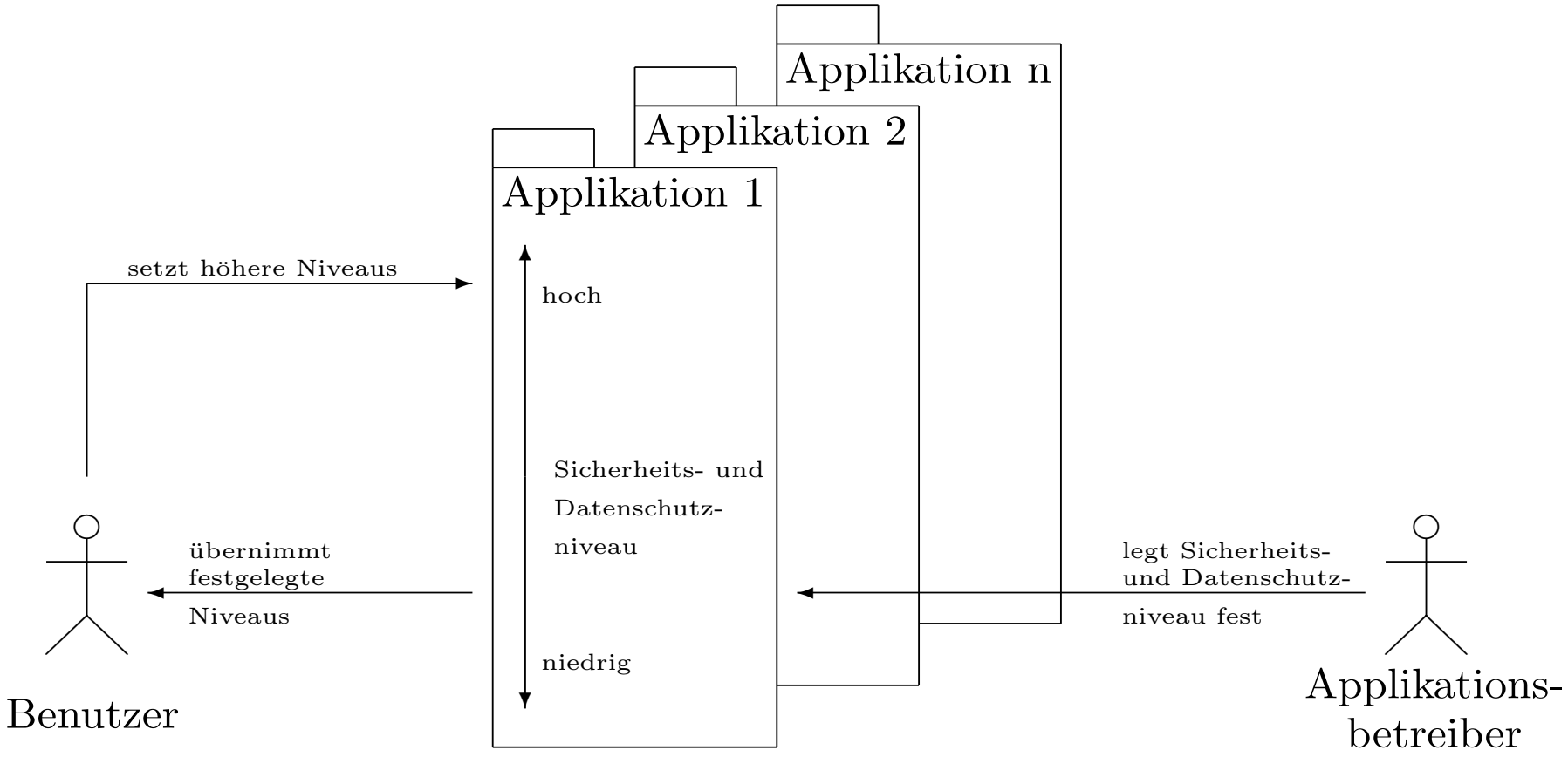
Existierende Lösungen:

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

2. CIDAS – Überblick

- „Configurable Internet Directory and Authentication Service“
- offene Spezifikationen, offenen Quellen, freie Verfügbarkeit
- Client- und Server-basierter Lösungsansatz
- dezentrale Datenhaltung möglich, Verzeichnisdienst
- einfache Erweiterbarkeit durch hohe Modularität
- erlaubt Integration beliebiger Authentifizierungssysteme und -verfahren
- weitreichende Unterstützung von Anwendungen

2. CIDAS – Sicherheitsstufen



3. Aufgabe für die Diplomarbeit

- Ausgangssituation: Es existierte ein Konzept für CIDAS und die Idee, passive Datenträger – primär USB-Sticks – als Authentifizierungsgeräte nutzbar zu machen.

- 3-teilige Aufgabenstellung:

  1. Entwicklung eines Kommunikationsprotokolls für den Datenaustausch zwischen CIDAS-Server und -Client
  2. Überprüfung der Einsetzbarkeit passiver Speichermedien für die Authentifizierung von Benutzern, Konzeptentwicklung
  3. Prototypische Umsetzung

4. Entwurf des Kommunikationsprotokolls

4. Entwurf des Kommunikationsprotokolls

- Abzubildende Funktionalität:
  - Identifizierung, Authentifizierung
  - Behandlung und Austausch von Autorisierungsinformationen
  - Änderungen an den Datenbeständen
  - Nutzung zusätzlicher Funktionalität des Servers
  - Sicherung von Vertraulichkeit und Integrität aller übertragener Daten
  - Offenheit und freie Verfügbarkeit der Protokollbeschreibung

4. Entwurf des Kommunikationsprotokolls

- Recherchen ergaben, daß diese Funktionalität mit keinem bereits verfügbaren Kommunikationsprotokoll abgedeckt werden kann.
  - Protokolle sind häufig zu spezifisch auf einen Anwendungsfall bezogen
  - es konnten vielfach erfolgreiche Angriffe durchgeführt werden
  - Protokolle sind oft nur sehr schwer erweiterbar
  - viele im Bereich des Identity-Management verwendete Protokolle sind nicht zugänglich
- Die Entwicklung eines neuen Protokolls birgt natürlich immer auch die Gefahr neuer Schwachstellen.

4. Entwurf des Kommunikationsprotokolls

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

5. Entwurf des Authentifizierungsverfahrens

5. Entwurf des Authentifizierungsverfahrens

- Anforderungen an das Verfahren:
  - Verwendung von asymmetrischer Kryptographie
  - Speicherung von Schlüsselmaterial auf passiven, identifizierbaren Medien
  - Benutzer soll keine nicht von ihm beeinflußbaren Daten signieren/verschlüsseln müssen
  - Einsetzbarkeit in herterogenen Umgebungen
  - Verwendung standardisierter Datenformate
  - frei verfügbare Spezifikation des Verfahrens

5. Entwurf des Authentifizierungsverfahrens

- Existierende Verfahren:
  - viele Verfahren beschrieben, nur wenige effektiv im Einsatz, z.B. Needham-Schroeder, X.509
  - Verfahren integrieren meist Schlüssel- oder anderweitigen Datenaustausch
  - Verfahren wurden unter anderen Gesichtspunken und Anforderungen spezifiziert
  - Analysen ergaben Schwachstellen

5. Entwurf des Authentifizierungsverfahrens

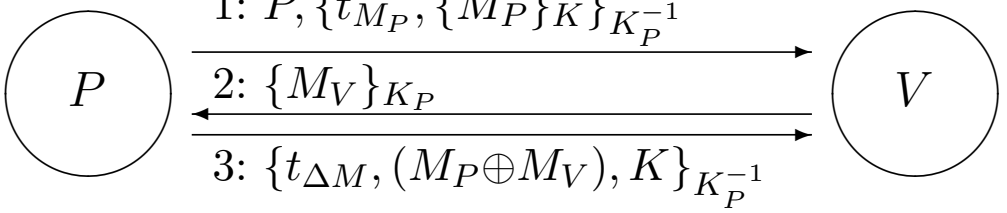
- eigenes Verfahren auf Basis von OpenPGP oder S/MIME
- Nachrichtenaustausch:

t : Zeitstempel

M : Nachrichten

K : Schlüssel

$\{M\}_K$: M verschlüsselt mit K



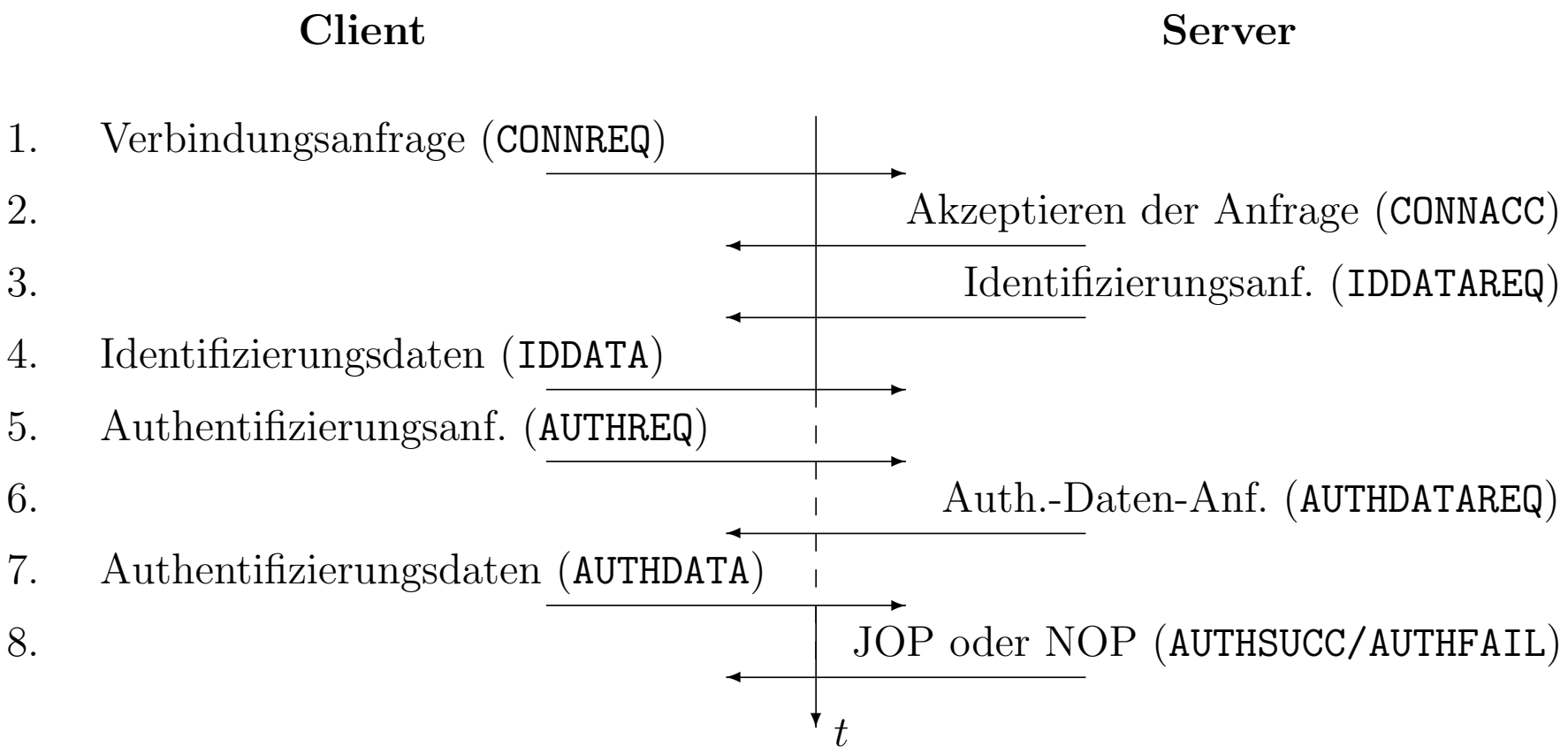
6. Demonstration des Prototypen

6. Demonstration des Prototypen

- Nachrichtenaufbau im CIDAS-Protokoll:

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 ...			

6. Demonstration des Prototypen



7. Zusammenfassung und Ausblick

- Es existieren:
  - Konzept für CIDAS
  - Kommunikationsprotokoll und ein nicht-textuelles Authentifizierungsverfahren
  - ein Prototyp
- Es fehlen:
  - formale Überprüfung des Kommunikationsprotokolls
  - Integration weiterer Authentifizierungsverfahren
  - Ausbau des Prototypen zu einem Produkt, Integration verschiedener bereits spezifizierter Komponenten
  - Einbindung von CIDAS in bestehende Infrastrukturen