

Vorstellung des Projektes

www. **CIDAS** .org

Configurable Internet Directory and Authentication Service

Projektgruppe CIDAS

<info@cidas.org>

Brandenburg, den 6. Juli 2005

Gliederung

1. Aufbau und Funktionsweise von CIDAS
2. Sicherheitsstufen und Authentifizierung
3. CIDAS-Kommunikation
4. Anbindung von Applikationen
5. Prototypische Umsetzungen von CIDAS
6. Kontaktmöglichkeiten

1. CIDAS – Überblick

- Client- und Server-basierter Lösungsansatz
- eigenes Kommunikationsprotokoll, eigene Formate für Datenpakete, Token, etc.
- offene Spezifikationen, offenen Quellen, freie Verfügbarkeit

1. CIDAS – Überblick

- erlaubt Authentifizierung von Benutzern und Verbreitung von Autorisierungsinformationen über ein Netz → Single-Sign-On
- unterstützt Integration beliebiger Authentifizierungssysteme und -verfahren
- Anmeldung bei Anwendungen/Diensten erfolgt pseudonym

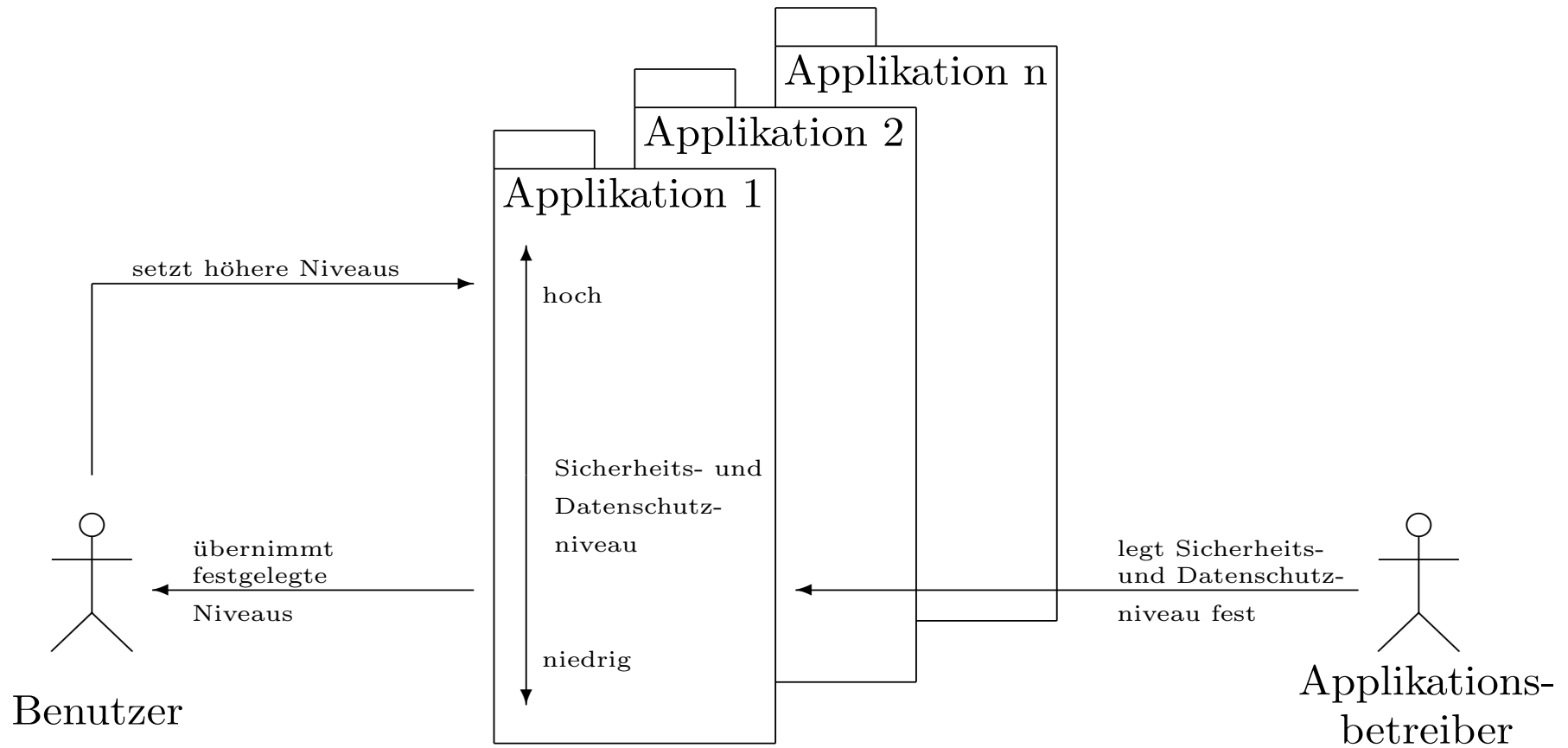
1. CIDAS – Überblick

- dezentrale Datenhaltung möglich, Verwendung von LDAP als Verzeichnisdienst
- einfache Erweiterbarkeit durch hohe Modularität
- weitreichende Unterstützung von Anwendungen ist geplant

2. Sicherheitsstufen. . .

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 (OpenPGP und X.509)
...	1 eindeutiges Merkmal	kombinierte Verfahren

2. Sicherheitsstufen...



2. Kryptographische Auth.

- Verwendung von asymmetrischer Kryptographie zur Benutzerauthentifizierung; eigenes Authentifizierungsprotokoll
- Schlüsselmaterial kann auf einem beliebigen Medium gespeichert sein – denkbar sind Festplatten auf vertrauenswürdigen Arbeitsplätzen, transportable Medien oder Chip-Karten

2. Kryptographische Auth.

- Verwendung standardisierter Datenformate (OpenPGP oder X.509)
- Einsetzbarkeit in heterogenen Umgebungen
- Missbrauchsschutz: Benutzer müssen keine nicht von ihnen beeinflussbaren Daten signieren

2. Kryptographische Auth.

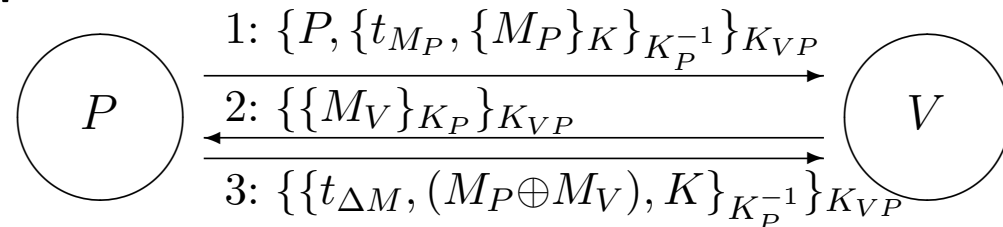
- eigenes Verfahren auf Basis von OpenPGP oder S/MIME
- Nachrichtenaustausch:

t : Zeitstempel

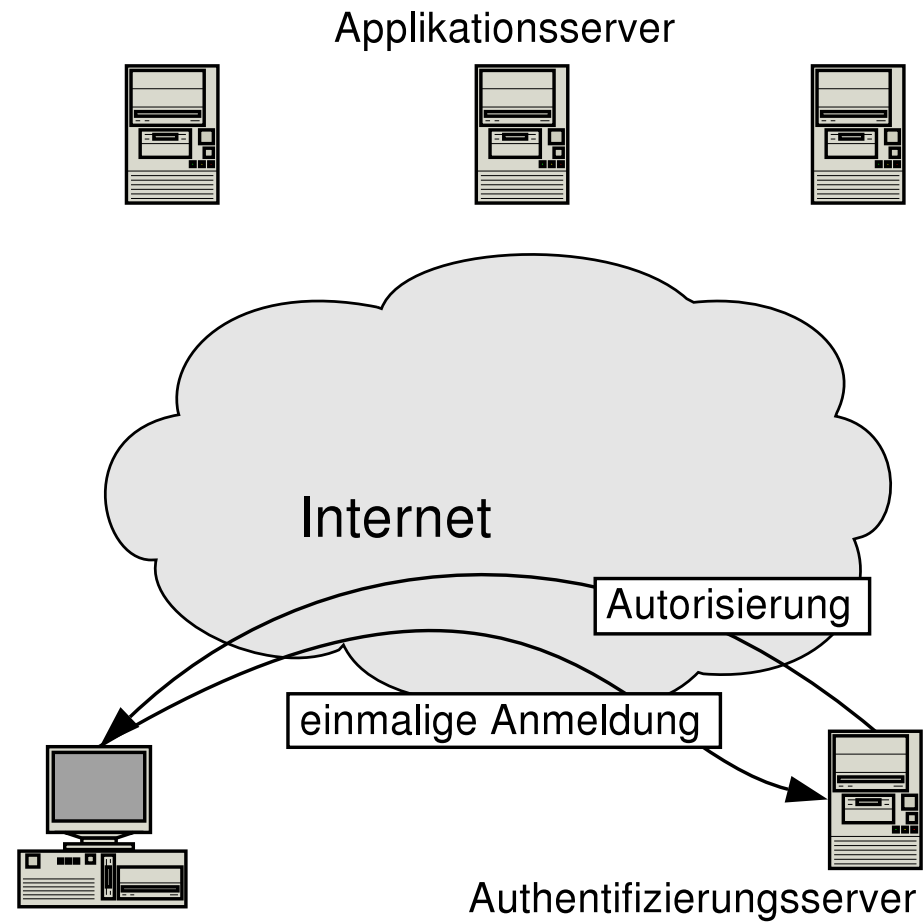
M : Nachrichten

K : Schlüssel

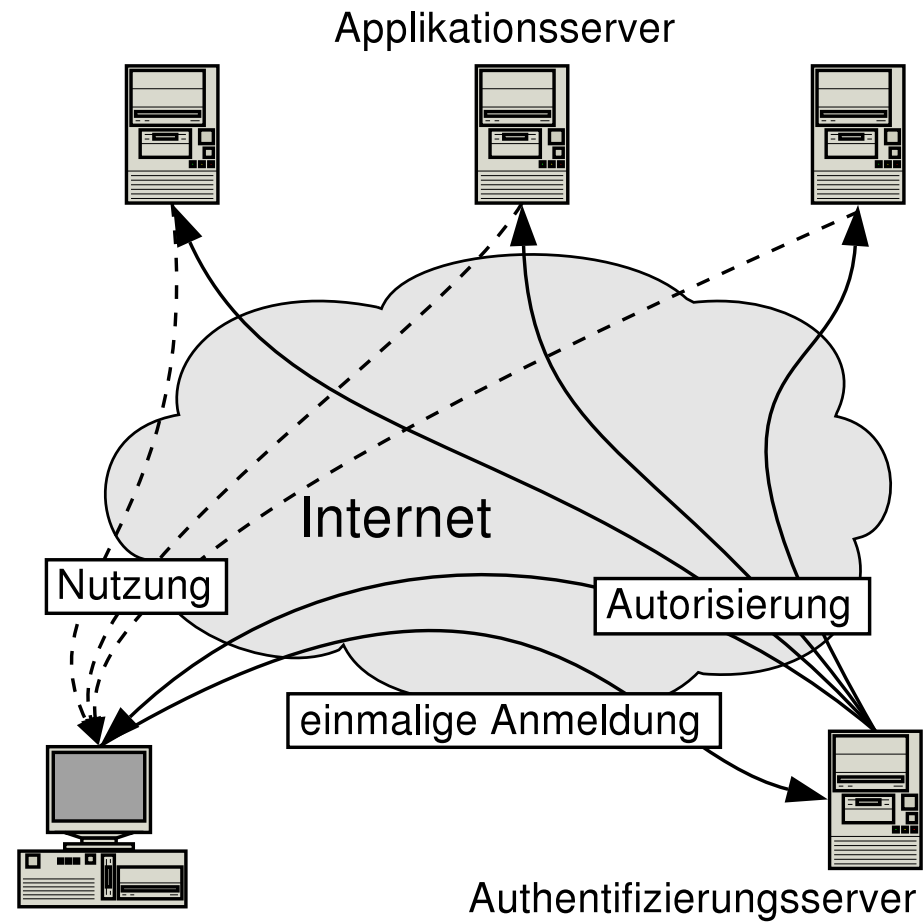
$\{M\}_K$: M verschlüsselt mit K



3. CIDAS-Kommunikation



3. CIDAS-Kommunikation



3. 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

3. Client und Server

- Sicherung von Vertraulichkeit und Integrität aller übertragener Daten wird auf der Ebene des Transprotokolls realisiert

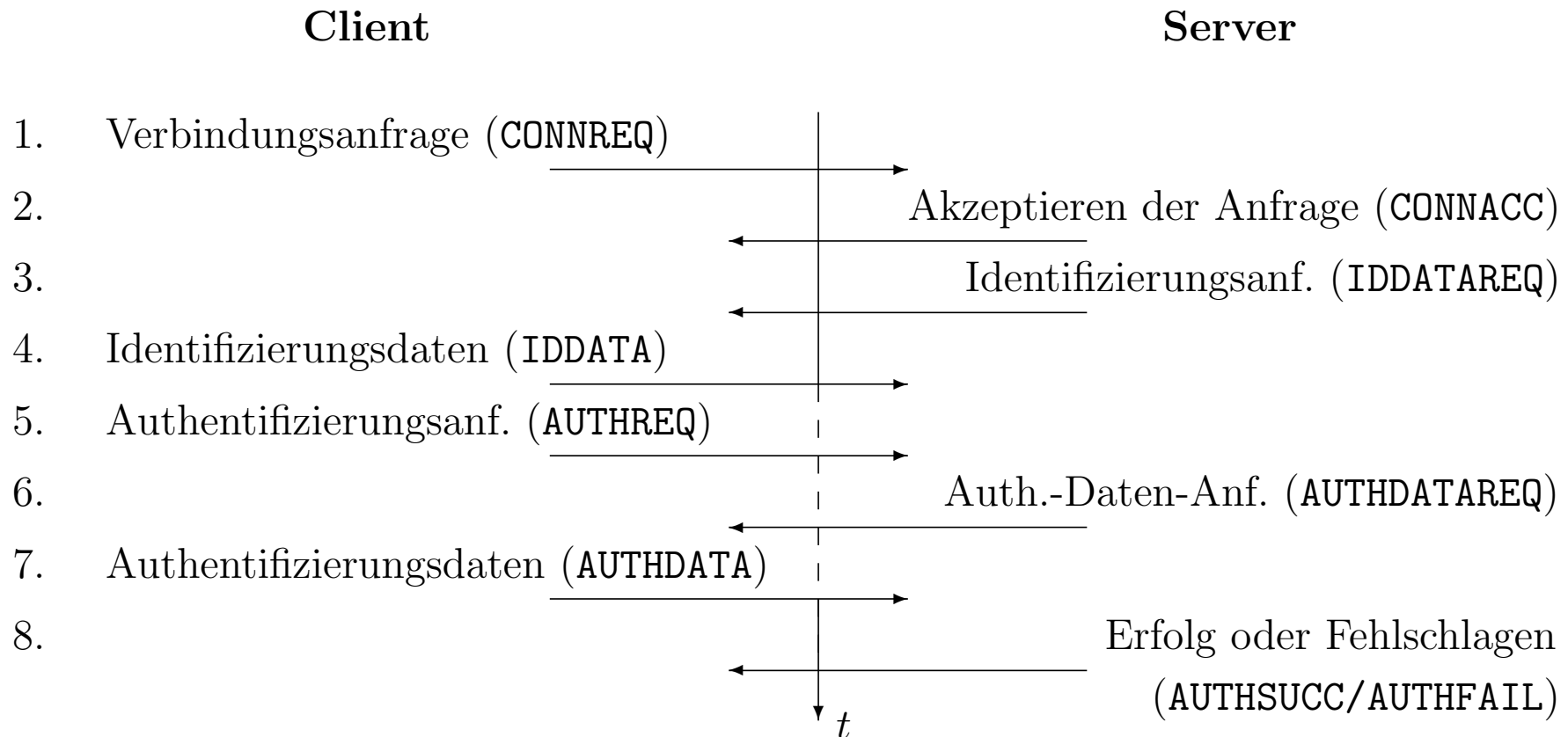
3. Protokollaufbau

- Designentscheidungen:
 - Nachrichtenorientiertheit
 - 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

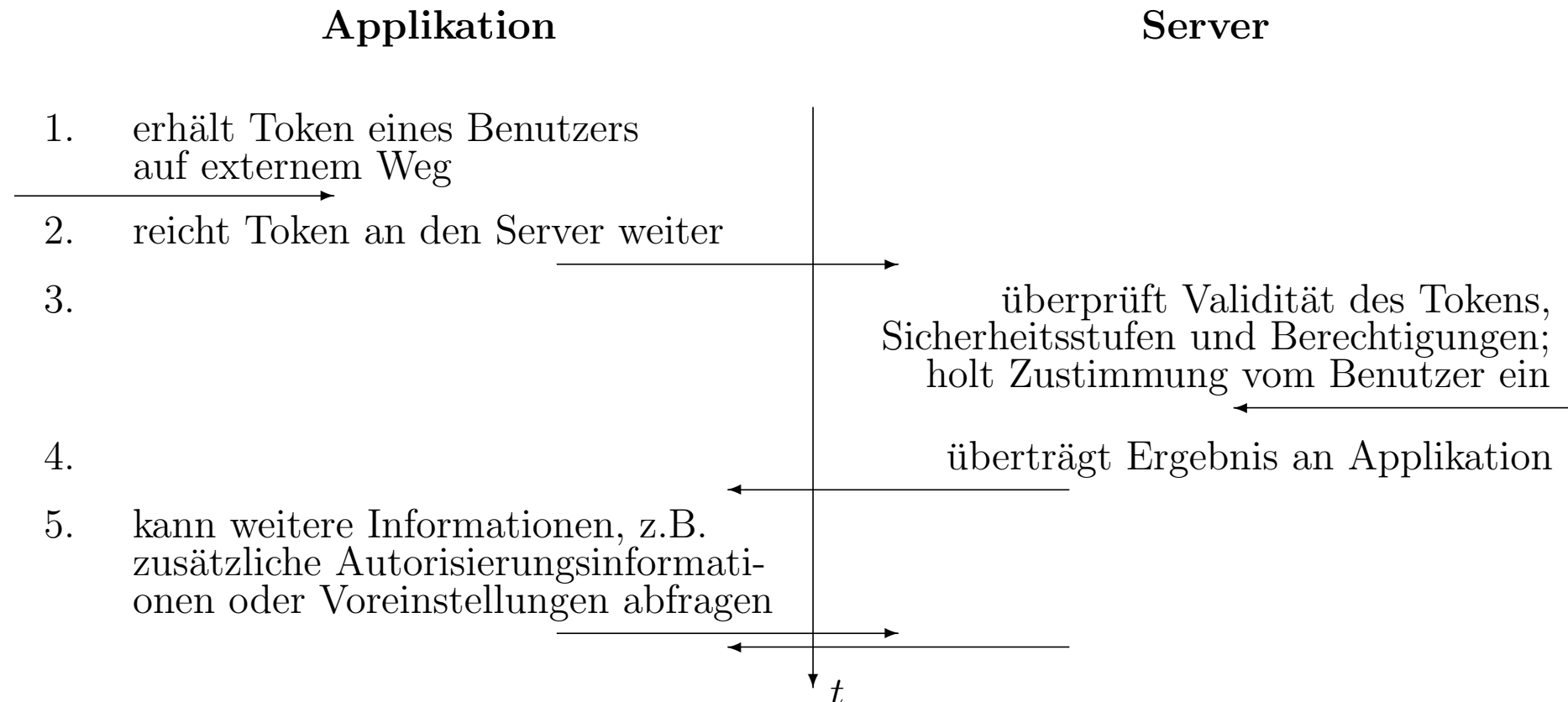
3. Protokollablauf



3. 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
- beliebig hohe Granularität der Autorisierung kann durch nachträgliche Abfrage von Applikationsattributen erreicht werden

3. CIDAS-Kommunikation – Token



4. 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 sind derzeit nicht vorgesehen

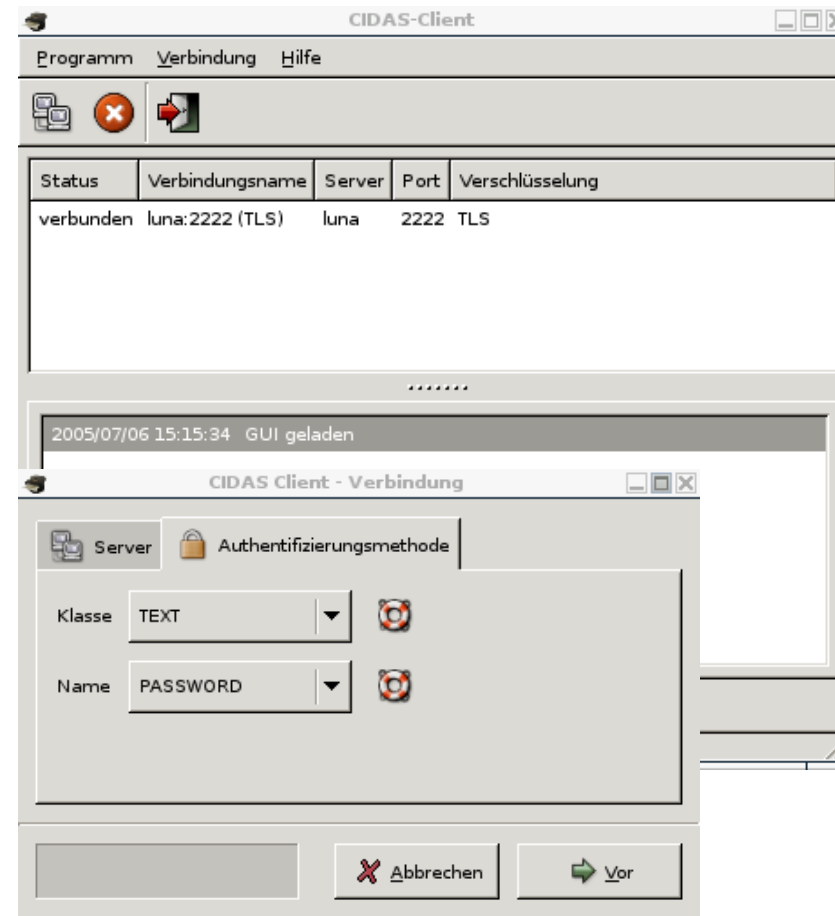
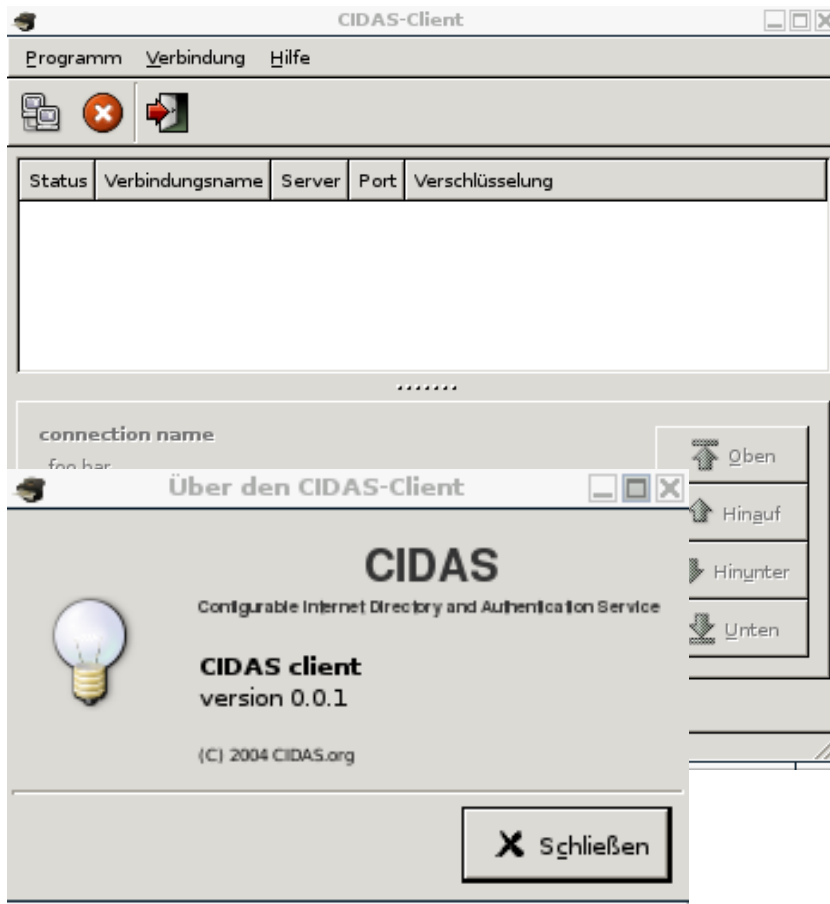
5. Prototypen. . .

- seit etwas über einem Jahr gibt es einen Prototypen zu CIDAS
- Server und Client implementieren derzeit einen Großteil der Protokollspezifikation und textuelle und kryptographische (nur OpenPGP) Authentifizierungsverfahren

5. Prototypen. . .

- geplant ist vorerst die Unterstützung folgender Applikationsgruppen:
 - auf Apache und PHP basierende Web-Anwendungen
 - sicherheitskritische Applikationslogik in CIDAS-SFMs
 - UNIX-Workstation-Logins und Anbindung an PAM
- für Windows-basierte Arbeitsplatzsysteme wird mittelfristig ein Client verfügbar sein, der die Verwendung weiterer Dienste gestattet

5. Prototypen...



5. Prototypen...

```
Terminal - [2]
secret key          : 1 - GnuPG keyring
                   : 2 - CD-ROM
                   : 3 - USB stick
                   : 4 - type in path by hand

Source to use      : 3
Connect your USB stick to this computer and press return.

Select a device:
  1 - /dev/sda: Fujitsu - Memorybird
Device to use     :
Invalid device. Try again.
Device to use     : 1
2005-07-06 15:29:19 W: * mount() failed: Das Argument ist ungültig.
2005-07-06 15:29:19 W: * mount() failed: Das Argument ist ungültig.
2005-07-06 15:29:19 W: * mount() failed: Das Argument ist ungültig.
2005-07-06 15:29:19 W: * mount() failed: Das Argument ist ungültig.
Please select one of the following secret keys:
  1 - A55F7D16F8AAA860 Klaus (A test key for CIDAS.) <klaus@cidas.org>
                                FPR: 17E3E1B0A9F09C65A6AD5DEAA55F7D16F8AAA860
Key to use        : 1
2005-07-06 15:29:37 I: Selected key A55F7D16F8AAA860.
Please enter the passphrase for key:
  A55F7D16F8AAA860 Klaus (A test key for CIDAS.) <klaus@cidas.org>
Passphrase: █
```

5. Prototypen...



6. Kontaktmöglichkeiten

Internet:

<http://www.cidas.org> — <info@cidas.org>

Das Team:

Prof. Dr. Friedrich-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>