University of Applied Sciences in Brandenburg

Presentation of the Project

www.CIDAS.org

Configurable Internet Directory and Authentication Service

Project Group CIDAS
<info@cidas.org>

Brandenburg, 18th May 2005

Disposition

1. Trust and Security within the WWW
2. Privacy and Security
3. Identity Management Systems
4. Existing Solutions
5. CIDAS – Structure and Design
6. Authentication with Passive Storage Media
7. CIDAS Communication
8. Integration of Existing Applications
9. Possibilities for Co-operation

1. Trust and Security within the WWW

- Is there something like trust and security within the WWW?

  1. Identification – Who are you?
  2. Authentication – Prove it!
  3. Authorisation – You are allowed to...

- Identification and authentication is usually done by entering username and password.

- How many passwords do you have? – How do you remember them?

- Why are smart cards, fingerprint sensors and other hardware based authentication methodes not commonly used?

2. Privacy and Security

- Frequent affairs about privacy and security...
- Do small application providers have enough know-how and capacities to implement privacy and security directives?
- How is personal data stored by common websites? How is it used? Who uses it?
- Do application provider know how data is protected by their business partners? Any means of influence?
- Why do users have no posibilities to view and change their personal data?

3. Identity Management Systems

Range of functions:

- Access Management
- Password Syncronisation
- Single Sign-On
- Password Reset

- collective term describing solutions to simplify and centralise administrative tasks dealing with user and access management
- simplify appliance of privacy and security directives
- advantages for administrators as well as for users

3. Identity Management Systems

Range of functions:

- Access Management
- Password Syncronisation
- Single Sign-On
- Password Reset

- centralised storage of authorisation information
- results in centralised user and access management

3. Identity Management Systems

Range of functions:

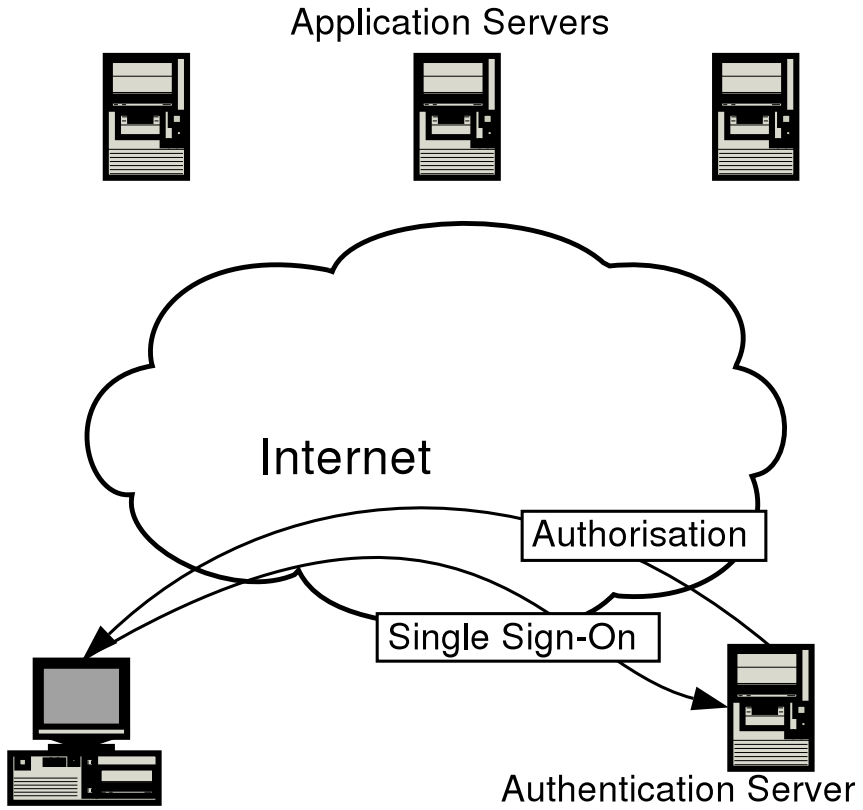
- Access Management
- Password Syncronisation
- Single Sign-On
- Password Reset

- passwords are stored by the IMS; they are distributed to used applications on demand
- users may login to all services using the same password
- high security risks because of storing and transfering passwords

3. Identity Management Systems

Range of functions:

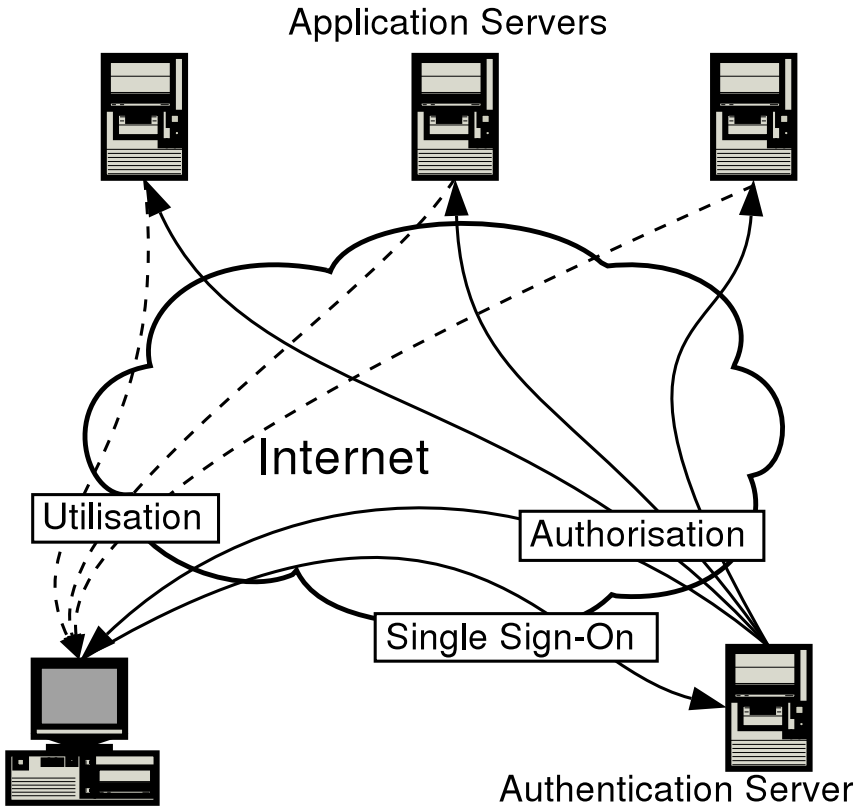
- Access Management
- Password Syncronisation
- Single Sign-On
- Password Reset



3. Identity Management Systems

Range of functions:

- Access Management
- Password Syncronisation
- Single Sign-On
- Password Reset



3. Identity Management Systems

Range of functions:

- Access Management
- Password Syncronisation
- Single Sign-On
- Password Reset

- IMS provides facilities to allow a user to reset his password in case of loss
- new passwords are automatically send by mail or email
- administrative efforts are reduced

4. Existing Solutions

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

- a few modern solutions since approx. five years
- only partial production readiness
- problems with security and privacy
- only minor consumer acceptance, rarely used in companies and education

4. Existing Solutions

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

- Web Edition - transp. proxy
- Standard Edition - only MS operating systems, legacy applications are supported
- automatic password generation and change
- decentral administration; data replication
- closed source, 10,000 EUR and 20% maintenance p.a.

4. Existing Solutions

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

- most accepted solution right now, 250 mill. registred users
- central data storage on MS server
- problems with security and privacy
- rarely used by service providers

4. Existing Solutions

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

- developed to compete with Passport, co-operation of approx. 150 companies
- main goal was to implement distributed storage of personal data; authentication is done by Identity Providers
- free specifications; only few attempts of implementation

4. Existing Solutions

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

- communication is based on HTTP, therefore mainly meant to authenticate users of WWW services
- cookies and redirects are used for distribution of authorisation information; attacks are known
- right now only textual authentication methods are supported

4. Existing Solutions

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

- provides hardware based authentication
- mainly usable for WWW services
- closed source solution

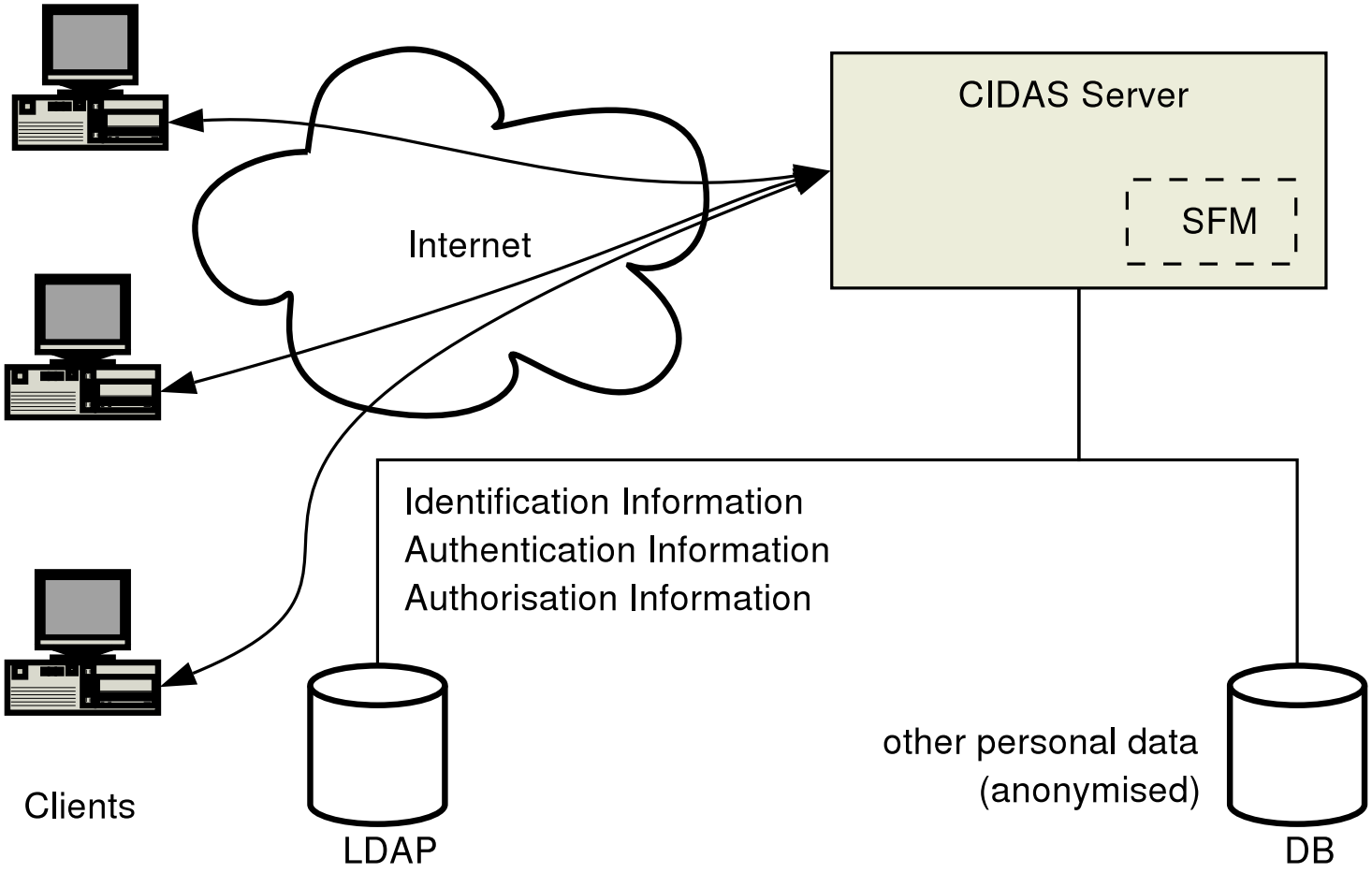
4. Existing Solutions

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

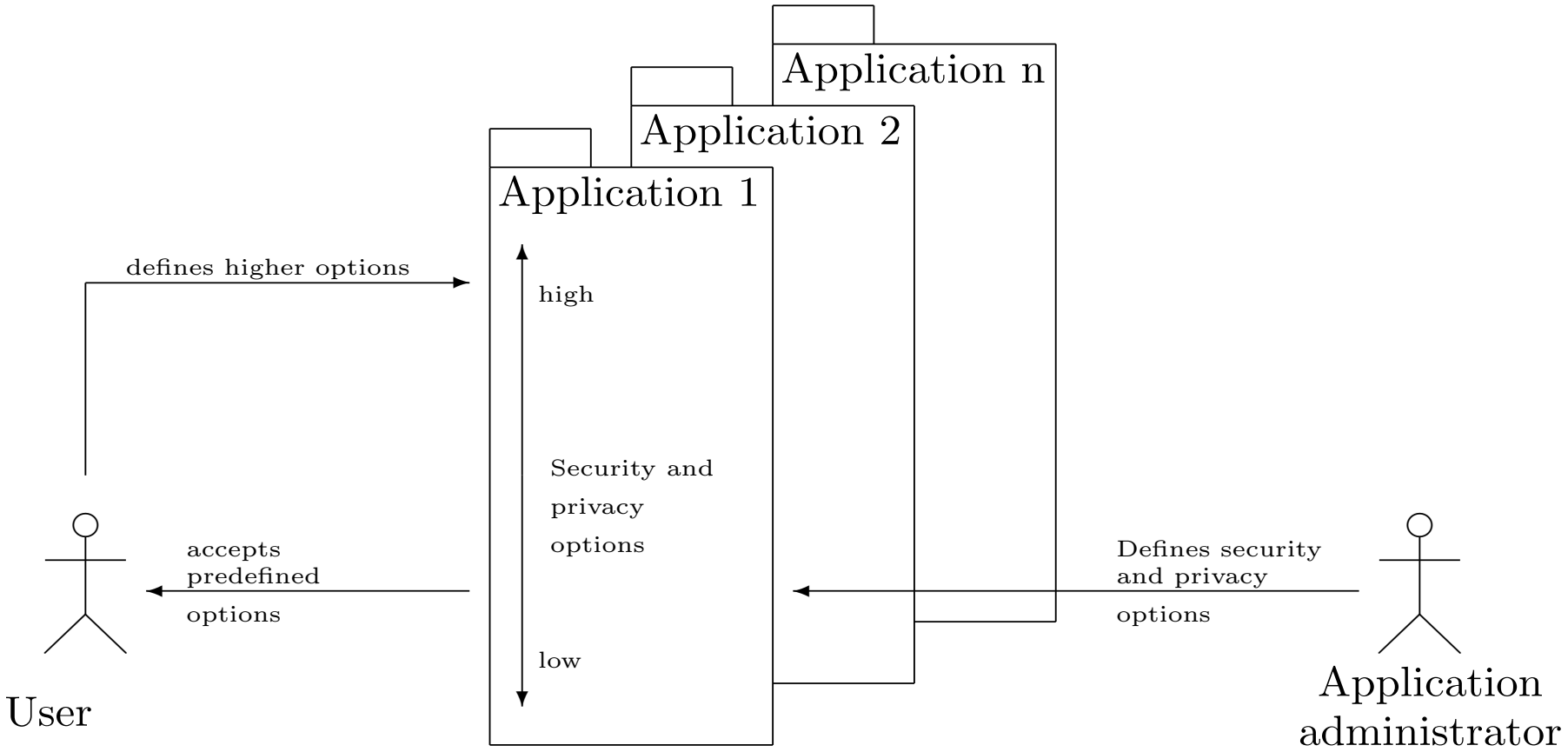
Configurable Internet Directory and Authentication Service

- free, versatile and scalable approach
- development is mainly done at Brandenburg University, local partners are involved

5. CIDAS – Structure and Design



5. CIDAS – Security Options



5. CIDAS – Authentication Methods

Sec. Level	Identification	Authentication
...	any	basic textual methods
3	any	biometry, visible attributes
4	1 definite attribute	passwords
5	1 definite attribute	biometry, invisible attributes
6	1 definite attribute	cryptographic methods using passive media
7	1 definite attribute	cryptographic methods using active media
...	1 definite attribute	combined methods

5. CIDAS – Résumé

- client/server system; own communication protocol
- distributed storage possible, uses directory service
- high extensibility, modular architecture
- arbitrary and possibly user-defined authentication systems can be used
- extensive support of applications
- open specifications, open source, freely available

6. Authentication with Passive Storage Media

- keying material is stored on passive and identifiable media
- usability in heterogenous network environments; almost every kind of medium might be used
- use asymmetric cryptography and standardised data formats
- users never need to sign any non-arbitrary data
- open specification and sources

6. Authentication with Passive Storage Media

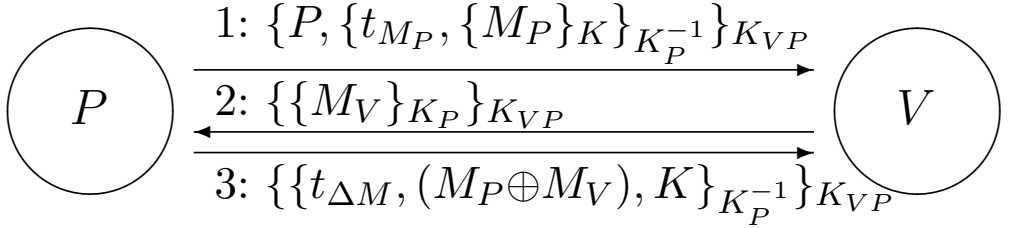
- own authentication scheme on basis of OpenPGP or S/MIME message formats
- Message flow:

t : timestamps

M : messages

K : keying material

$\{M\}_K$: M encrypted with K



7. CIDAS Communication – Client and Server

- communication between clients and a server, as well as between servers among each other, is done by an own protocol, specifications are freely available
- Functional range:
  - identification, authentication
  - handling and exchange of authorisation information
  - modifications to personal data
  - utilisation of additional functionality of the server
- confidentiality and integrity protection is done on the by the transport protocol being used

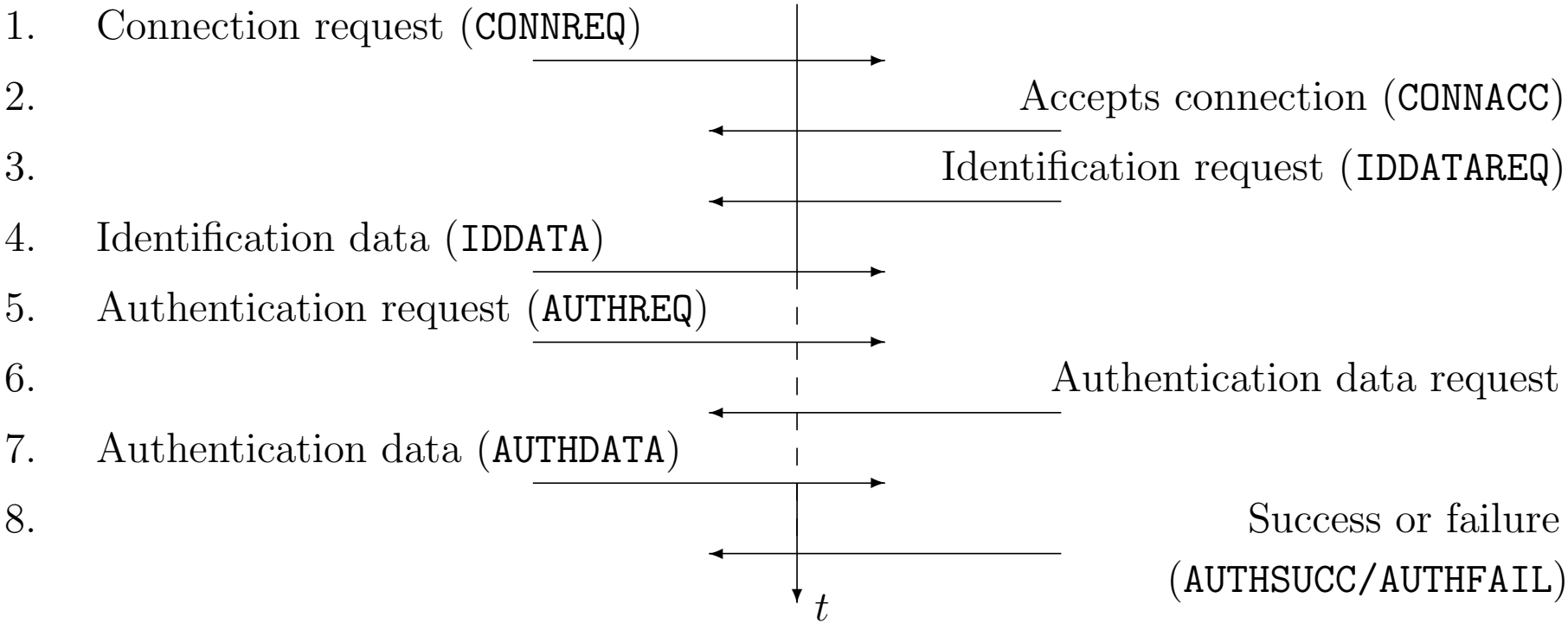
7. CIDAS Communication – Protocol Design

- basic ideas:
  - message based communication
  - condition-based message flow
  - utilisation of XML
  - SSL/TLS for confidentiality and integrity protection

Octet 0 0 1 2 3 4 5 6 7	Octet 1 0 1 2 3 4 5 6 7	Octet 2 0 1 2 3 4 5 6 7	Octet 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 ...			

Structure CIDAS message

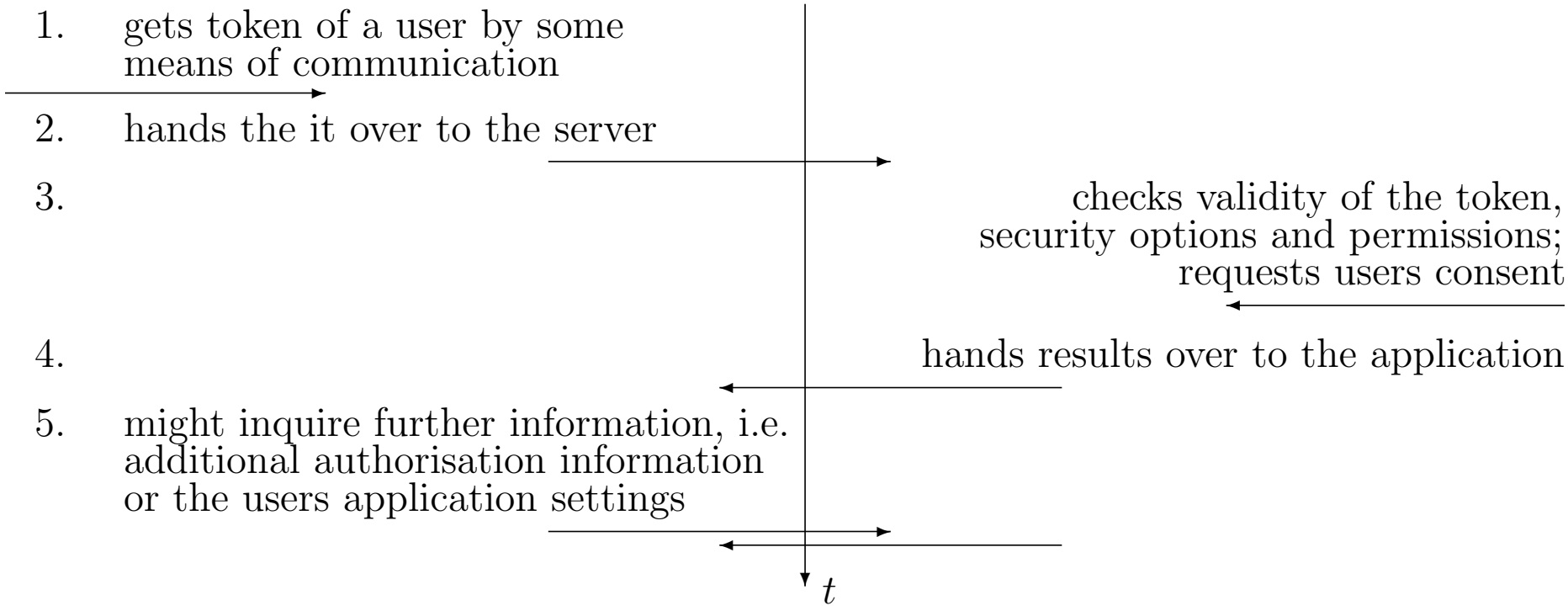
7. CIDAS Communication – Message Flow



7. CIDAS Communication – Authorisation Token

- authorisation information is distributed by the CIDAS server
- *Tokens* are used for identification of authenticated users by applications and for distribution of authorisation information
- a CIDAS server only returns generic authorisation information like "you are allowed to acces this application"
- clients or applications may inquire more detailed information later on

7. CIDAS Communication – Token Exchange



8. Integration of existing applications

- CIDAS supports workstation logons as well as user authentication for web based services
- every kind of application or service that natively supports the CIDAS protocol, is able to use the CIDAS client or that already uses LDAP for user authentication
- there are plans for the integration of legacy applications
- client and server will be available for almost all widely used operating systems

8. Integration of Existing Applications

- within the next months the following groups of applications will be supported:
  - web based services on basis of Apache und PHP
  - sensitive application logic in CIDAS SFMs
  - UNIX workstation logins and PAM support
- there will be a client for Windows based workstations allowing the use of CIDAS aware services
- a replacement for the Windows login will not be provided within the near future

9. Possibilities for Co-operation

- we proudly provide:
  - a free, versatile and extensible Identity Management System, product readiness within the next months
  - support for integration, operation, modification and maintenance of this system
  - technology transfer between university and business partners

9. Possibilities for Co-operation

- we need help:
  - know-how and manpower to implement the Windows client for CIDAS
  - support for extending the server and UNIX client
  - realistic testing environments
  - requirement analysis of companies and institutions with problems in the range of user and access management

Contact Information

Internet:

http://www.cidas.org — info@cidas.org

The Team:

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

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

Ingo Schäfer
<schaefei@fh-brandenburg.de>

Markus Dahms
<dahms@fh-brandenburg.de>