AAI for Croatian Academic and Research Community

Miroslav Milinović
University Computing Centre – SRCE,
Universty of Zagreb, Zagreb, Croatia
miro@srce.hr

Workshop WS-3
CUC 2004, Zagreb, September 2004

srce

CUC · 2004

Contents

- Part 1: AA(A) problem and solutions
  - Needs & challenges
  - AA(A) problem
  - AA(A) Infrastructure
  - AAI vs. PKI
  - SSO
- Part 2: AAI@EduHr
  - Current status in Croatia
  - AAI@EduHr project & deliverables

Part 1:
AA(A) problem and solutions

Needs

- Network & application access
  - simple
  - reliable
  - allow **resource owner** to:
    - define who and under what conditions can access
    - monitor users / audit activities
- Use combination of remote resources to fulfill a task:
  - computation
  - data handling
  - information retrieval
  - visualization
  - collaboration support
  - multimedia distribution
  - experimentation
  - ...

Challenges

- Different perspectives:
  - providers (service and/or content)
  - intermediaries
  - users (individual and/or organisations)

- Different problems:
  - technical (programming could be difficult)
  - non-technical (laws & policies, organisational and social aspects)

What is Middleware?

- broad definition: “glue” between the network infrastructure and user applications
- commonly used word (buzzword?) with unclear scope
- specialized networked services that are shared by applications and users
- a set of core software components that permit scaling of applications and networks
- tools that take the complexity out of application integration
- a second layer of the IT infrastructure, sitting above the network

- *the intersection of the stuff that network engineers don’t want to do with the stuff that applications developers don’t want to do*

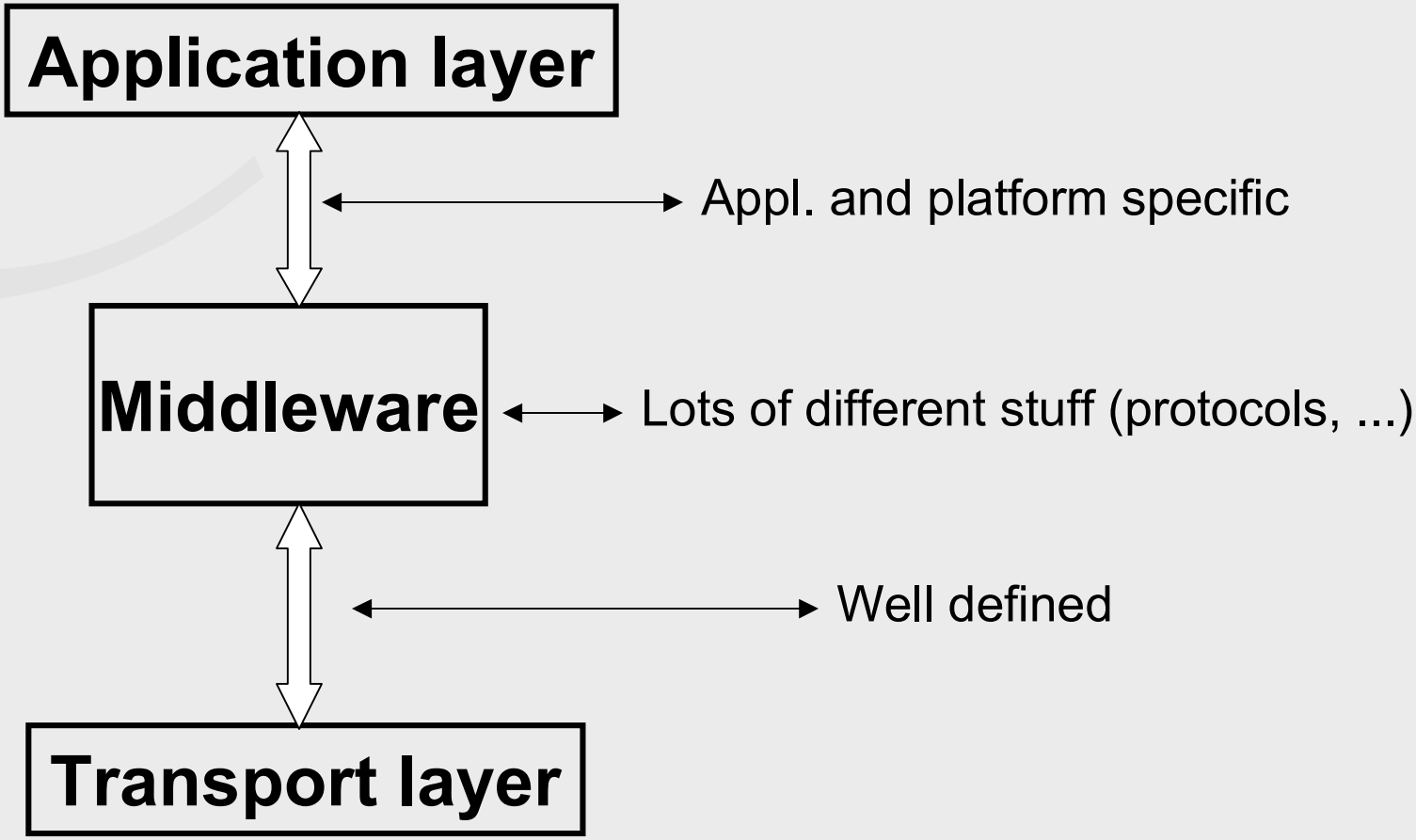
(*Ken Klingenstein)*

Middleware Scope

- Core middleware
  - Identifiers
  - **Directories**
  - **Authentication, Authorisation, Accounting (AAA)**
  - **Certificates and PKI**

- Upper middleware (Upperware)
  - “services that applications would like to have provided for them, rather than having to perform these functions themselves”
  - computing, data repositories, resource discovery, multimedia ...

Middleware Model



Directories

- specialised databases designed for storing and retrieving information about individuals, organisations, services, resources, ...
- designed for storing and retrieving information
  - fast reading, writing is slower
  - static view on the data
  - simple updates without transactions
- network protocol for access (X.500, **LDAP**, ...)
- history: used for White pages services

Directories & Middleware

- essential for almost all middleware services
- move from White pages to Directory Enabled Networks
- currently LDAP based directories are considered as the best practice
- activities in:
  - IETF
  - TERENA
  - Internet 2 Middleware

AAA

- Authentication (AuthN)
- Authorisation (AuthZ)
- Accounting (Auditing)

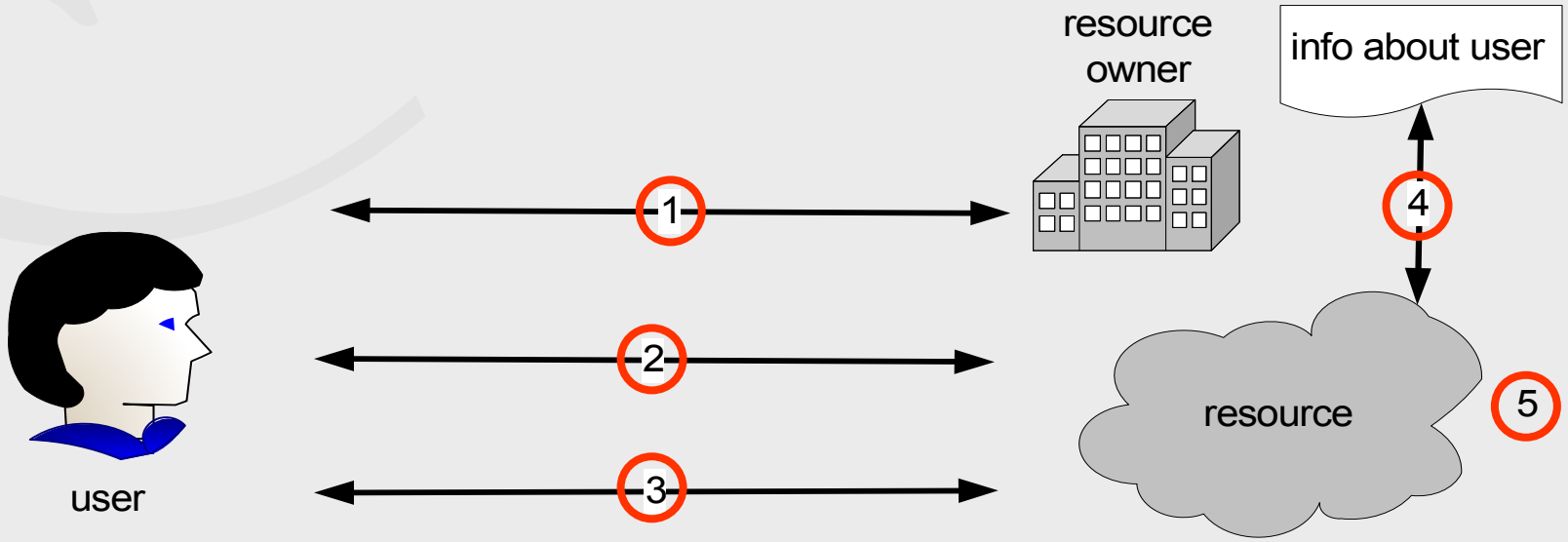
Authentication

- process of establishing whether or not a real-world subject is who or what its identifier says it is
- identity can be proven by:
  - something you know, like a password
  - something you have, like a smart cards or public-key certificates
  - something you are, as with positive photo identification, fingerprints, and biometrics
- should be secure, efficient and effective

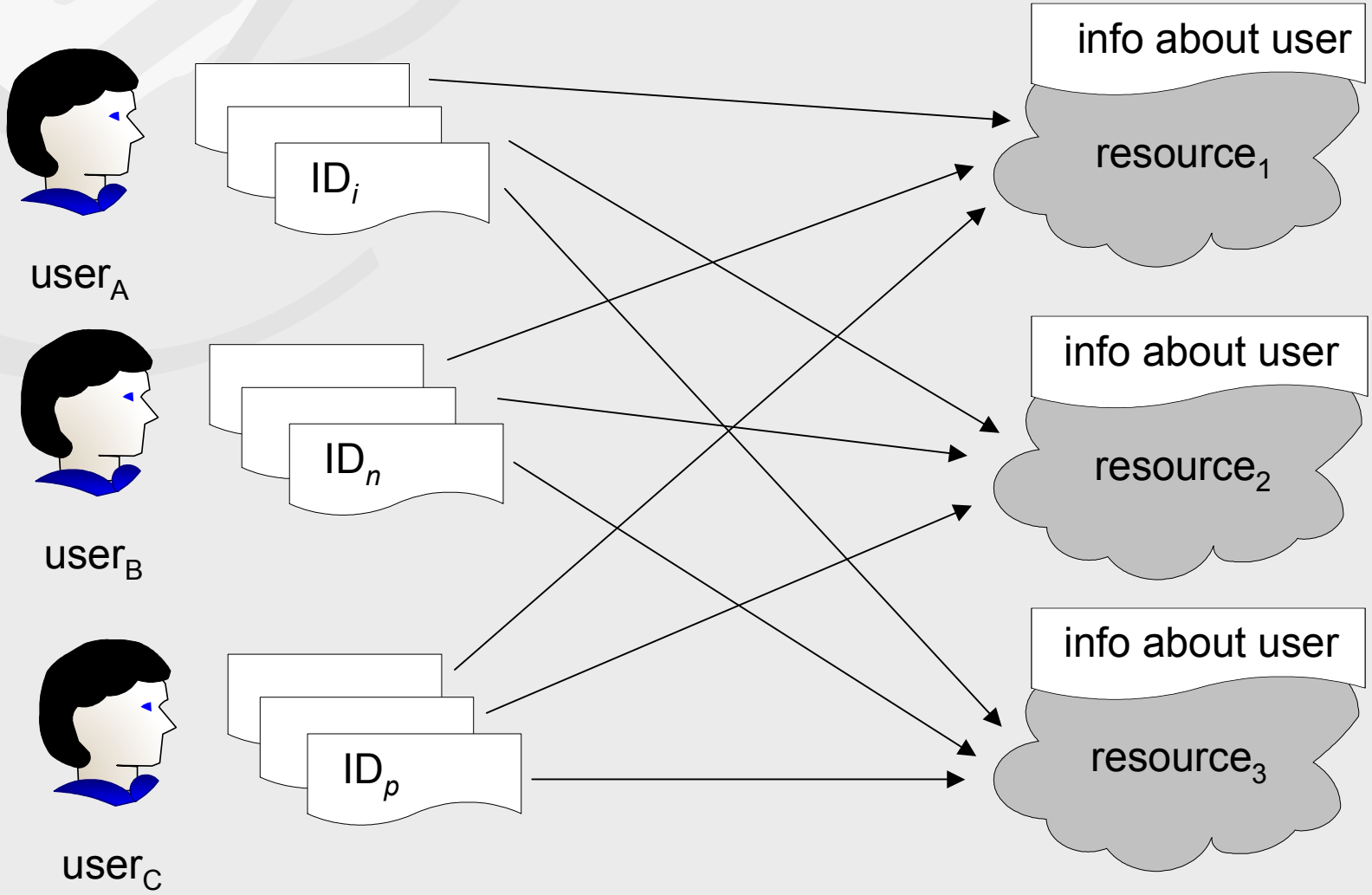
Authorisation

- assume the user is known (successfully authenticated)
- the user has attributes determining what he/she is allowed to do
- the resource has use conditions set by the resource owner
- **authorisation process = make the access decision**
- requires mapping user's attributes with resource's use conditions

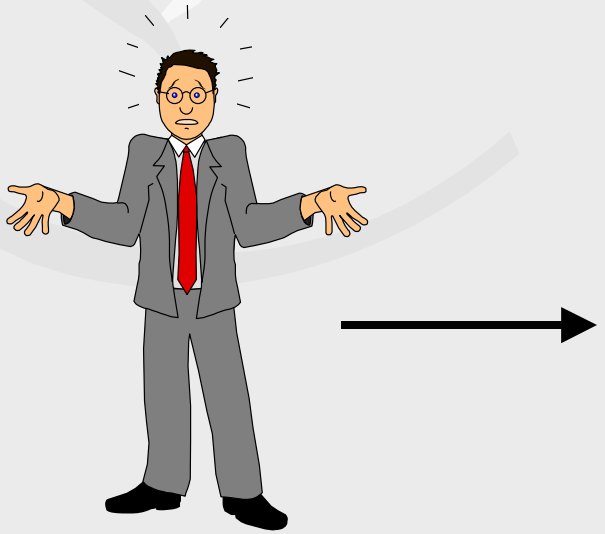
Steps in AA Process



AA Problem

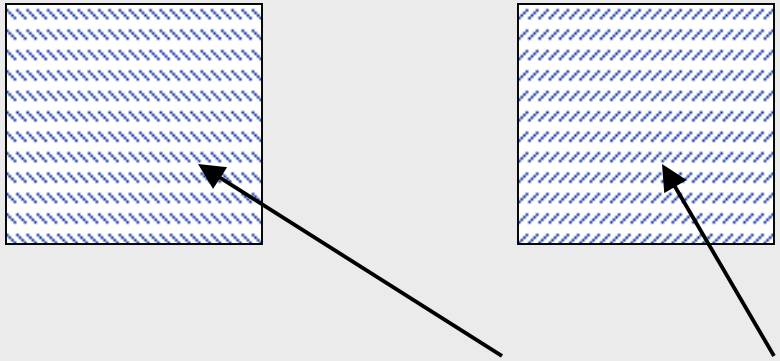

info about user
resource$_1$
ID$_i$
user$_A$
info about user
resource$_2$
ID$_n$
user$_B$
info about user
resource$_3$
ID$_p$
user$_C$

Traditional Applications



Userid / Password Lists

Access Control Lists

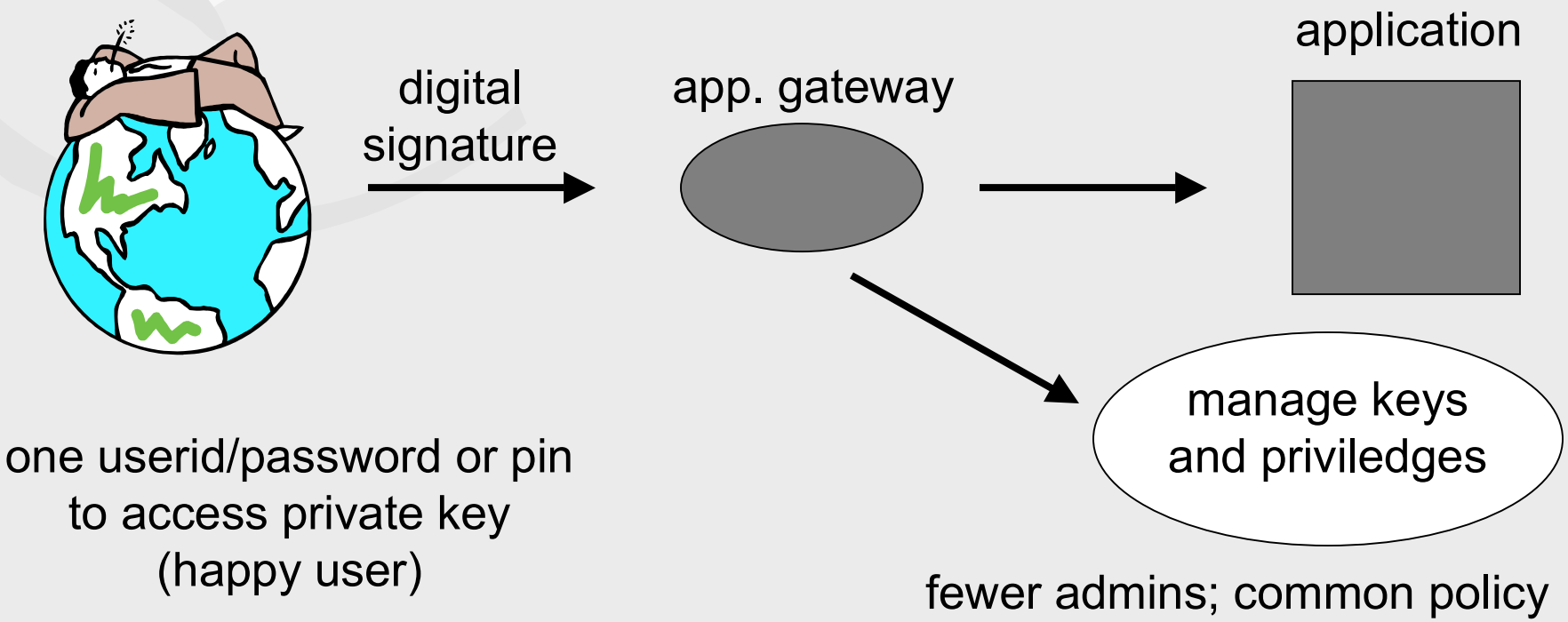


multiple userids/passwords (confused user)

mulitiple admins; no common policy

Authentication and authorisation are internal to the application

Ultimate Goal



Authentication and authorisation are external to the application

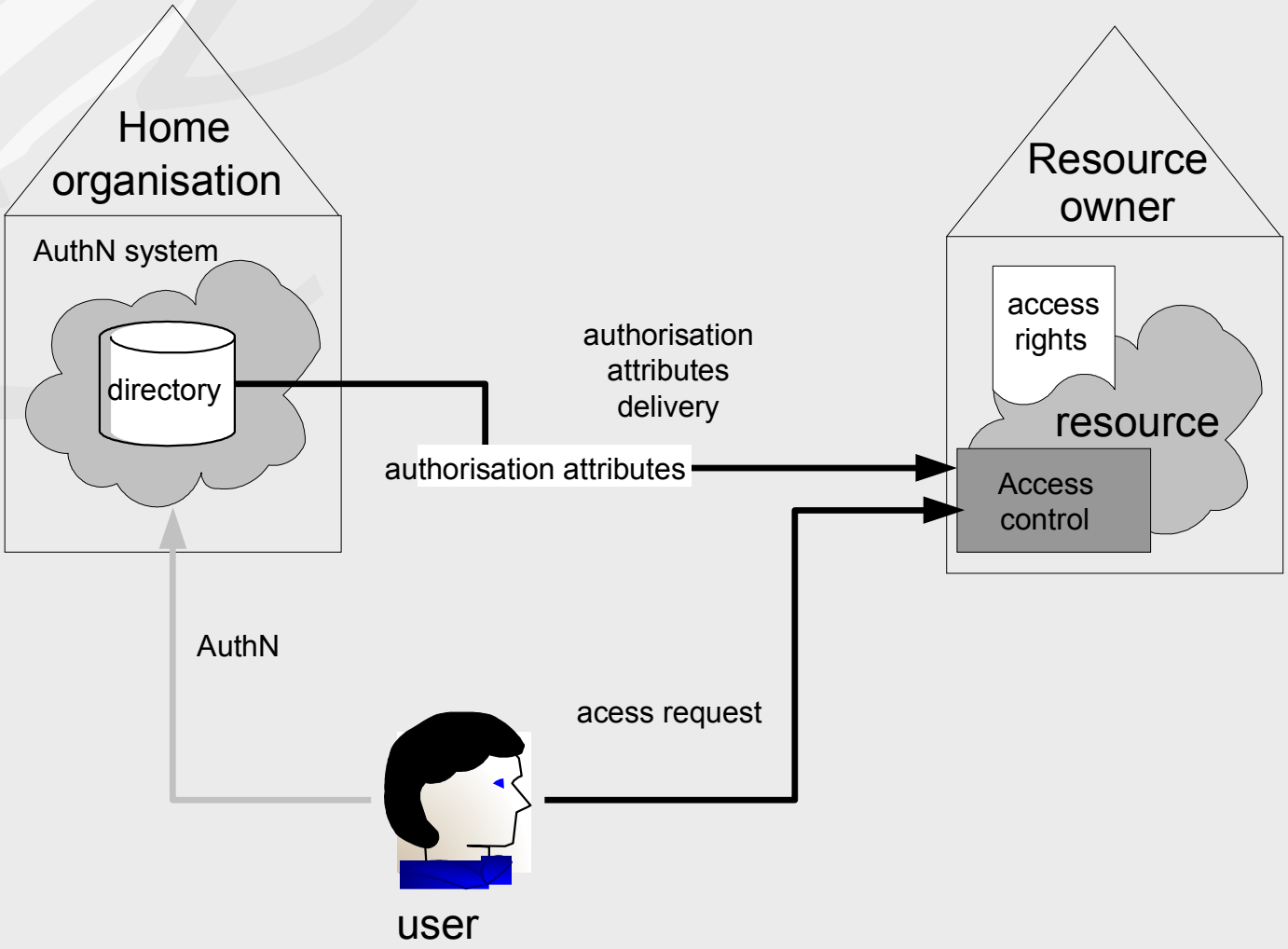
Inter-institutional AA

- disclosing credentials beyond your administrative domain:
  - mobility
  - virtual organisations
  - publishers, distance education, grids, ...
- increased flexibility:
  - better than IP address-based authentication
- increased security:
  - weak userid/passwd replaced by certificate

AA Infrastructure

- solution for (inter-institutional) AA problem
- 3 key elements:
  - user, home organisation, resource owner
- 3 basic actions:
  - user AuthN performed by (his) home organisation
  - delivery of user's authorisation attributes from home organisation to resource (owner); set of attributes has to be configurable to meet the needs of both parties (strong privacy)
  - resource owner decides about the access (AuthZ).

AAI: Model


Home organisation
AuthN system
directory
authorisation attributes delivery
authorisation attributes
Resource owner
access rights
resource
Access control
AuthN
acess request
user

AAI: Expectations

- The AAI should:
  - minimise the work of the system administrators,
  - be scalable to work with many users,
  - be standards based
  - be secure,
  - should reduce to the minimum the need to install new software on end user systems.

In a highly distributed and decentralised environment, it is important that the user administration is equally distributed

AAI: Challenges

- AAI phases:
  - AuthN, AuthZ, (Control of Session, proxy – frontend element)
    - description
    - architecture review
    - elements involved
- centralised vs. distributed infrastructure

Authentication Phase

- many solutions:
  - most common: user + password
  - other: one time password, digital certificates (key cards, tokens), biometrics,...
- various protocols used (LDAP, Radius, ...)
- distributed vs. centralised solutions
- (LDAP) directories used to store the data about the users

Authorisation Phase

- based on rules that implement access control policies
- uses: origin address of the request, client's identity, client's attributes, time ranges, ...
- possible use of external authorisation server or authorisation engine
- in distributed AAI (sometimes) it is necessary to have an identification manager to know: "who are you" , "where may I ask about you"

Control of Session

- allows to identify the client of the request
- improves performance of a AAI
- allows AAI not to repeat a heavy AuthZ process in each request
- problems
  - very dependent of applications and protocols
  - security problems
- Web browser (HTTP):
    - Cookies
    - Reference parameters
    - Coded in URLs

Access Control Proxy Element

- helps to integrate the new technology with old services
- for the home organization
  - controls the access of home users to external organizations resources
  - useful for content providers
- for the resource owner
  - firewall for services
  - centralises the access control policies for all the resources of the organisation
- helps in the integration between different solutions

Centralised Solutions

- common servers or services for all the organizations involved
- advantages
  - No inter-organizations trust problem
  - No client (or home site) identification problem
- disadvantages
  - scalability
  - difficult management
  - flexibility (?)

Distributed Solutions

- elements may stay in different organizations, even in third trust parties
- advantages
  - flexibility
  - scalability
- disadvantages
  - inter-organizations trust
  - client (or home site) identification
  - common attribute schemas (for directories)

PKI Concept

- enhanced security
- public keys / certificates replace weak user/password based AA
- Public Key Infrastructure (PKI) is a combination of
  - software,
  - protocols,
  - legal agreements

  that are necessary to effectively use certificates.
- X.509 standard for certificates is used

PKI Components

- **Certificate Authority (CA)**, that manages and signs certificates for an institution
- **Registration Authorities (RA)**, operating under the auspices of the CA, that validate users as having been issued certificates
- **PKI management tools**, including software to manage revocations, validations and renewals
- **Directories** to store certificates, public keys, and certificate management information
- **Databases and key-management software** to store escrowed and archived keys
- **Applications** that can make use of certificates and can seek validation of others' certificates
- **Trust models** that extend the realm of secure communications beyond the original CA
- **Policies** that identify how an institution manages certificates, including legal liabilities and limitations, standards on contents of certificates, and actual campus practices

PKI Components

Infrastructure System

- Registration
- Certification
- Directory
- Time Stamping

End User System

- Signature Component
- Verification Component
- Visualisation Component

What is Single-Sign On?

- **SSO**
- authenticate once, access multiple (network or application) services
- simple(r) task: separate SSO systems for network and application access
- ultimate goal: SSO across network and application domains

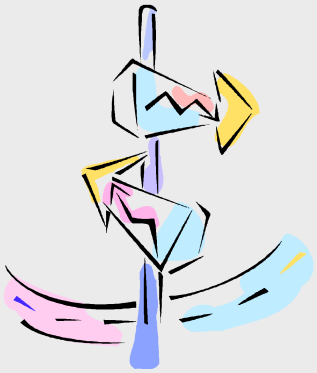
Network access & SSO

- access to the same type of network (e.g. WiFi) with a single account (horizontal roaming)
- access to different networks (e.g. WiFi and GPRS) with a single account (vertical roaming)

Application access & SSO

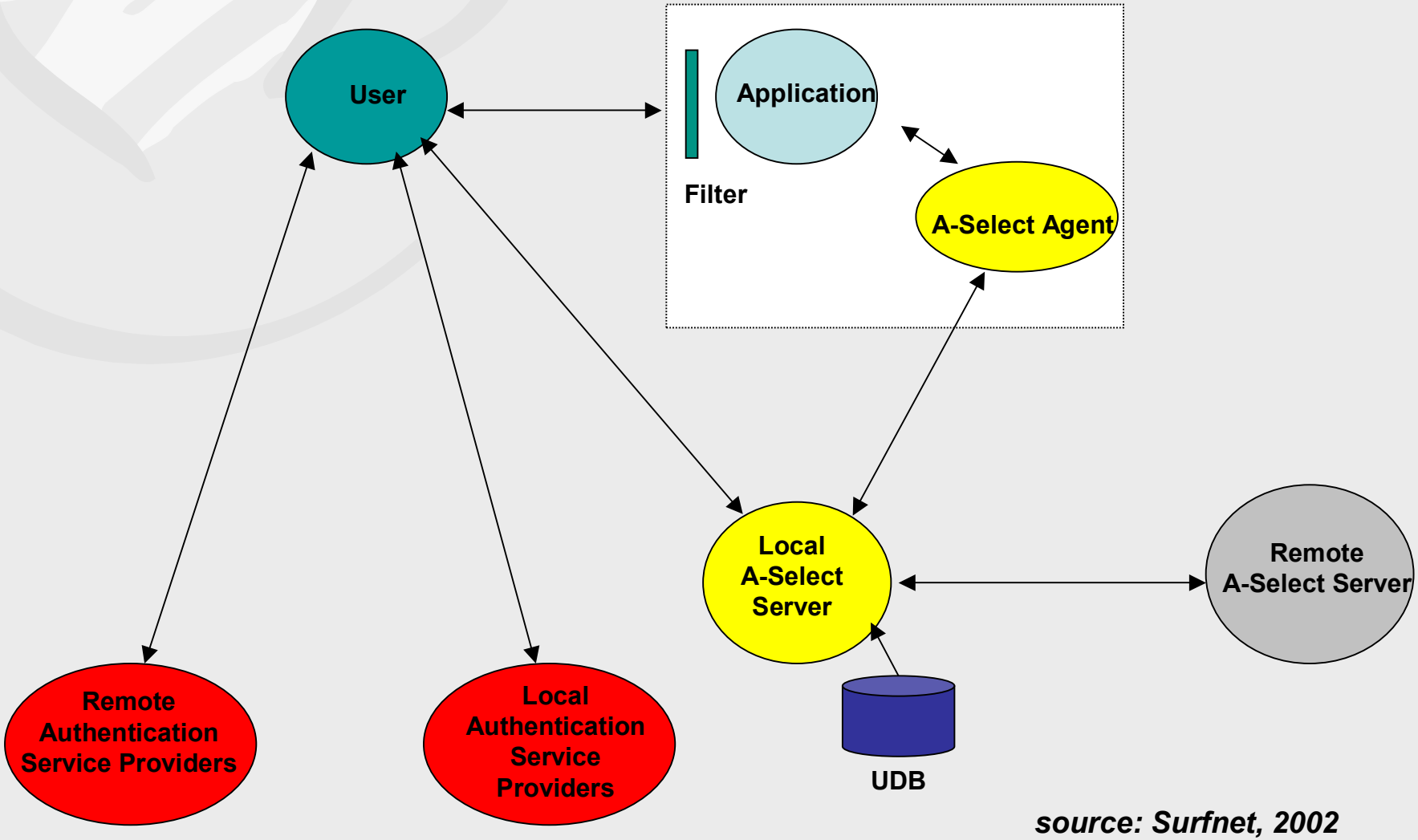
- thru a web login or webISO server
- embedded in an AAI environment:
  - authN services
  - authZ services (roles, attributes, etc.)
- simple within a single domain
- challenging part: SSO across multiple domains

AAI in real life



- A-select (http://a-select.surfnet.nl)
- FEIDE (http://www.feide.no/)
- FEIDHE (http://www.csc.fi/suomi/funet/middleware/english/index.phtml)
- GSI (http://www.globus.org/security/)
- PAPI (http://www.rediris.es/app/papi/index.en.html)
- Shibboleth (http://shibboleth.internet2.edu/)
- Switch AAI (http://www.switch.ch/aai/)
- Permis (http://www.permis.org/)
- Athens (http://www.athensams.net/)
- ...
- TERENA (http://www.terena.nl/tech/)
- Internet 2 (http://middleware.internet2.edu/)
- ...

A-Select overview

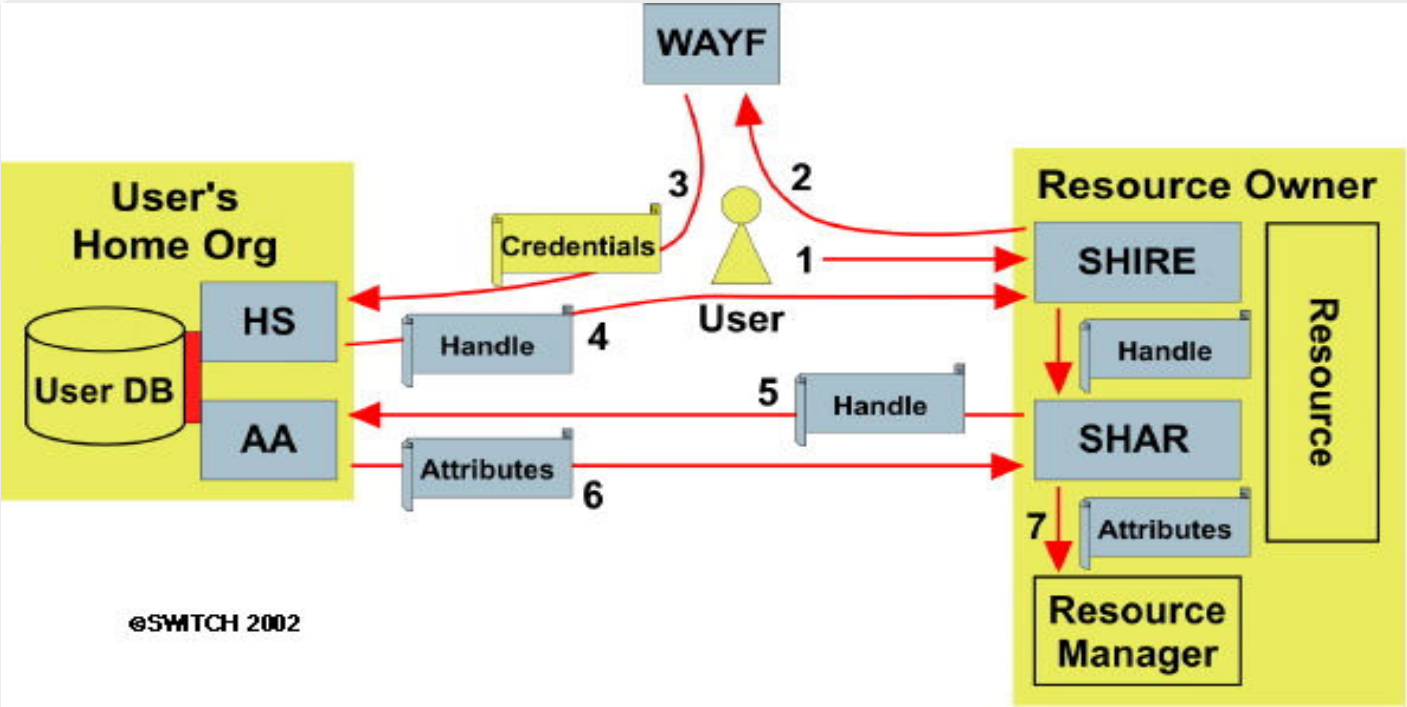


source: Surfnet, 2002

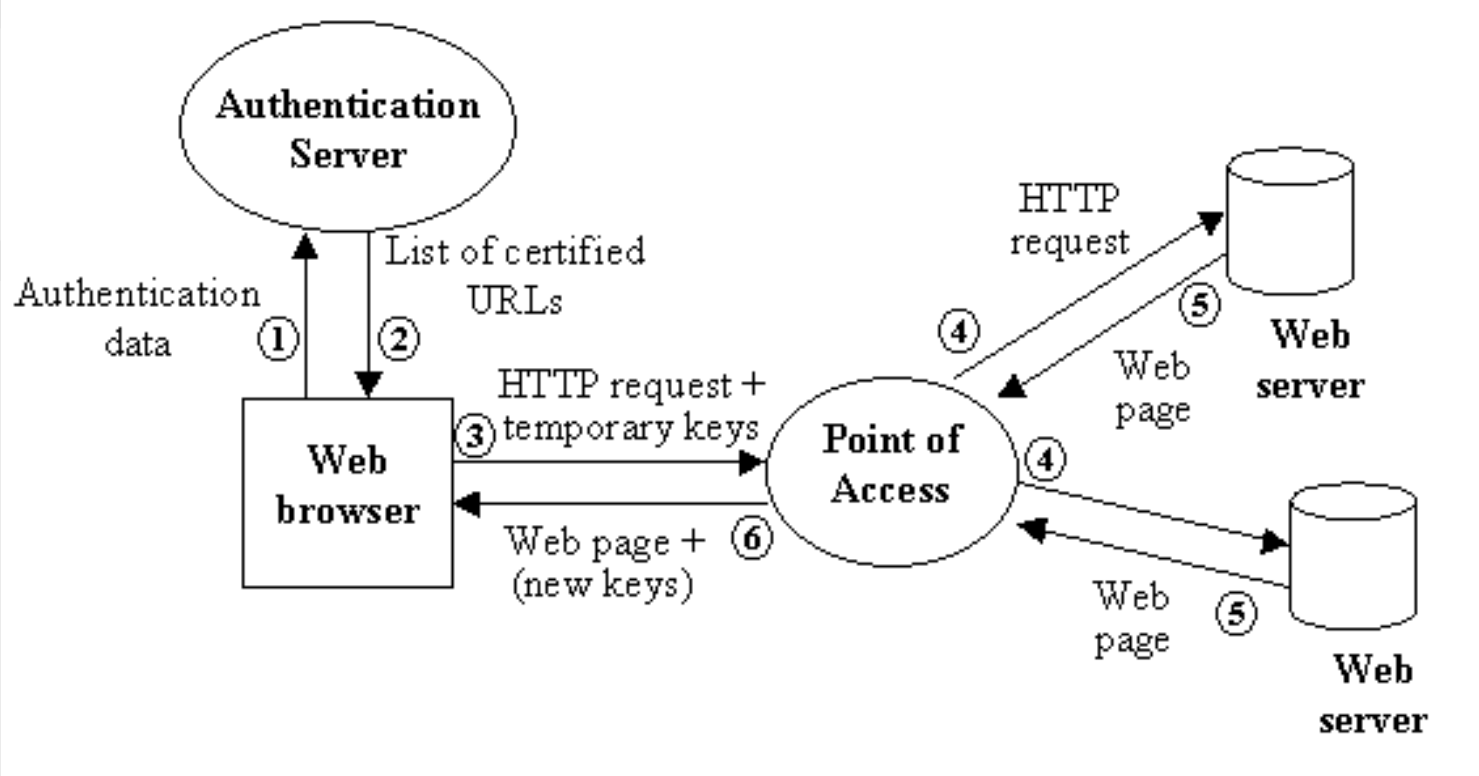
Shibboleth (Internet2)

- federated administration
- delegates authentication and attribute assertion to campuses
- resource owner requests attributes from campus and makes decisions based on the response
- model allows both campus and user control over attribute release (strong emphasis on privacy)

Shibboleth Architecture



Basic PAPI Architecture

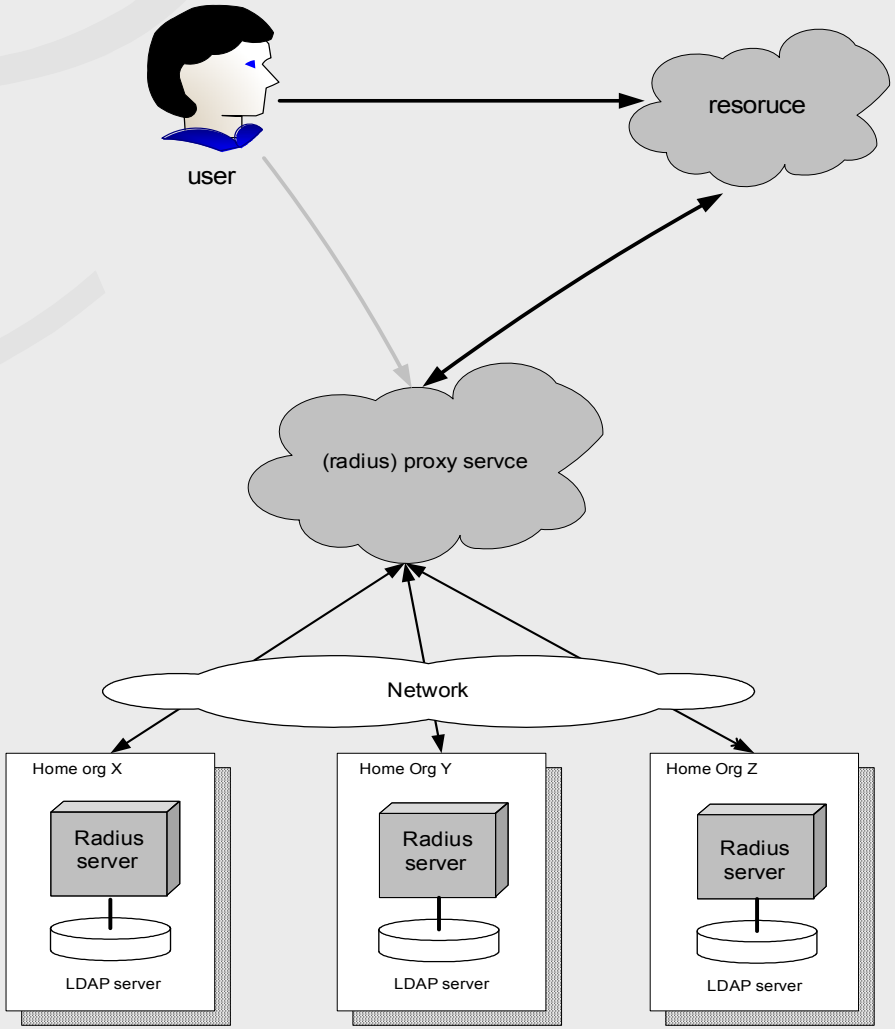


source: RedIris

AAI & Network Access

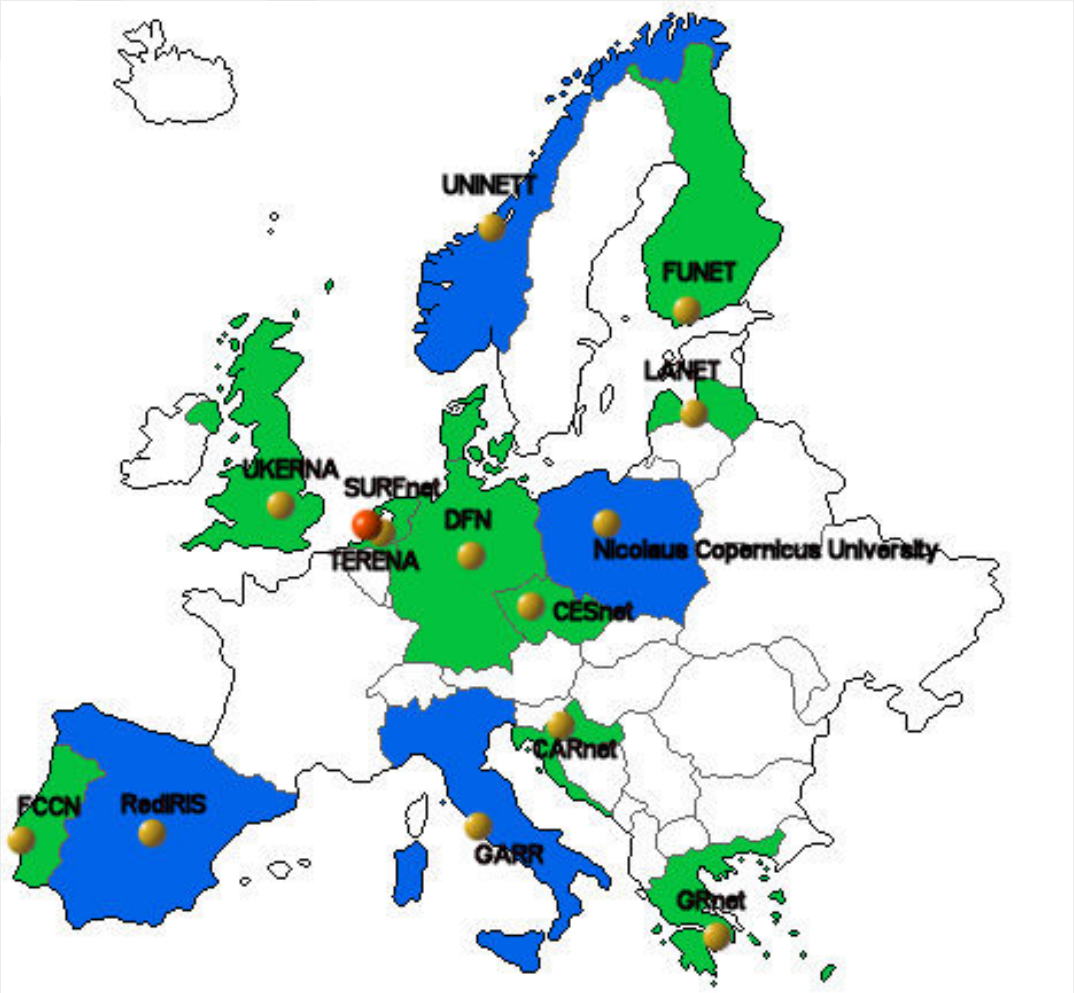
- For access control to the network there are in essence three approaches being used in the academic world:
  - based on web-based access in combination with a RADIUS-infrastructure;
  - based on VPNs;
  - based on 802.1X, the IEEE-standard for port-based authentication, in combination with a RADIUS-infrastructure.

AAI for Network Access



Srce & CARNet

Inter-NREN roaming



http://www.terena.nl/tech/task-forces/tf-mobility/eduroam.html

Requirements for inter-NREN roaming

- **Major requirements:**
  - **scalability** of the proposed solution must be maintained
  - **administrative overhead** must be minimised
  - required **security** must be maintained for all partners in the process
- **Minor requirements:**
  - **usability** must be good for all needed/used platforms.
  - **accountability and logging functionality** must be provided to track abuse
- **Regulation/Legislation issues**

(proposed by TERENA TF-Mobility)

Part 2: AAI@EduHr

AAI in use

- enable access to:
  - network
    (dial-up, wireless, wired, cable, DSL, ...)
  - networked computer resources
    (grid, networked disks, ...)
  - basic network services
    (ssh/telnet, e-mail, ftp, ...)
  - web resources (web-based applications)
  - specific applications
    (on-line databases, e-learning, video conferencing, ...)
  - ...

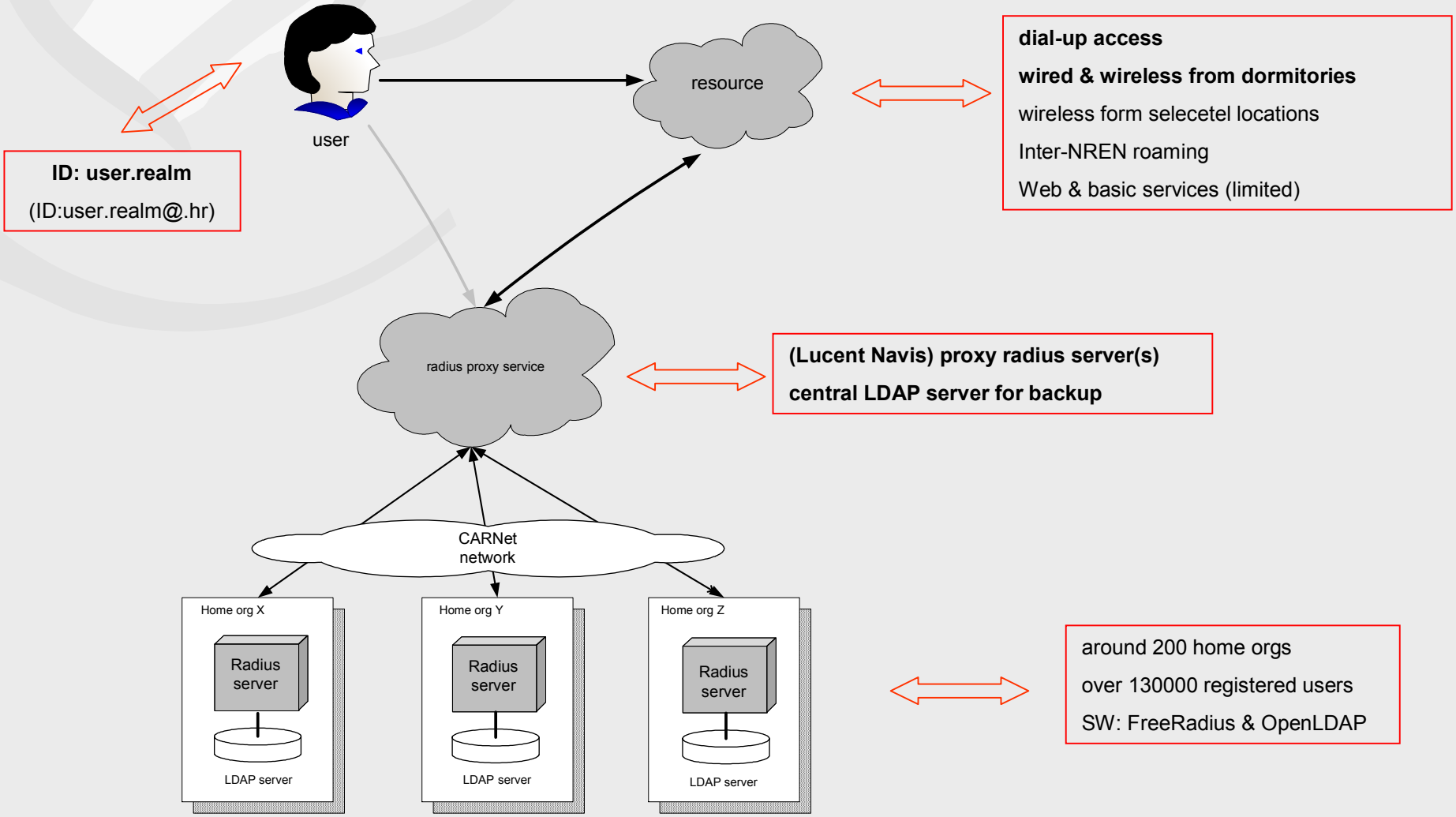
Current status

- growing needs:
  - ongoing development
  - projects and services
- experience:
  - established system of distributed LDAP directories
  - established national Radius/LDAP hierarchy
  - AAI for dial-up service: CMUng system
  - AAI for network access in student dormitories: StuDom project
  - access to web-based applications (using LDAP and/or Radius)
  - access to basic network services (unix/linux PAM)
  - access to networked computer resources (SAMBA)
  - bridging Open LDAP and MS Active Directory

(Expected) Application of AAI

- Access to:
  - network for end users
    (dial-up, any access based on Radius / 802.1x)
  - access to basic services: telnet/ssh, ftp, samba, POP/IMAP
    (via modified PAM module & LDAP/Radius infrastructure)
  - Web-based application
  - e-learning environments (e.g. WebCT)
  - VoD, streaming, video
  - grids
  - on-line databases
  - advanced applications like student's card ("X-ica") or higher education information system (ISVU)
  - LANs (classrooms, labs, Intranet, public areas, ...)
  - ...

Current status



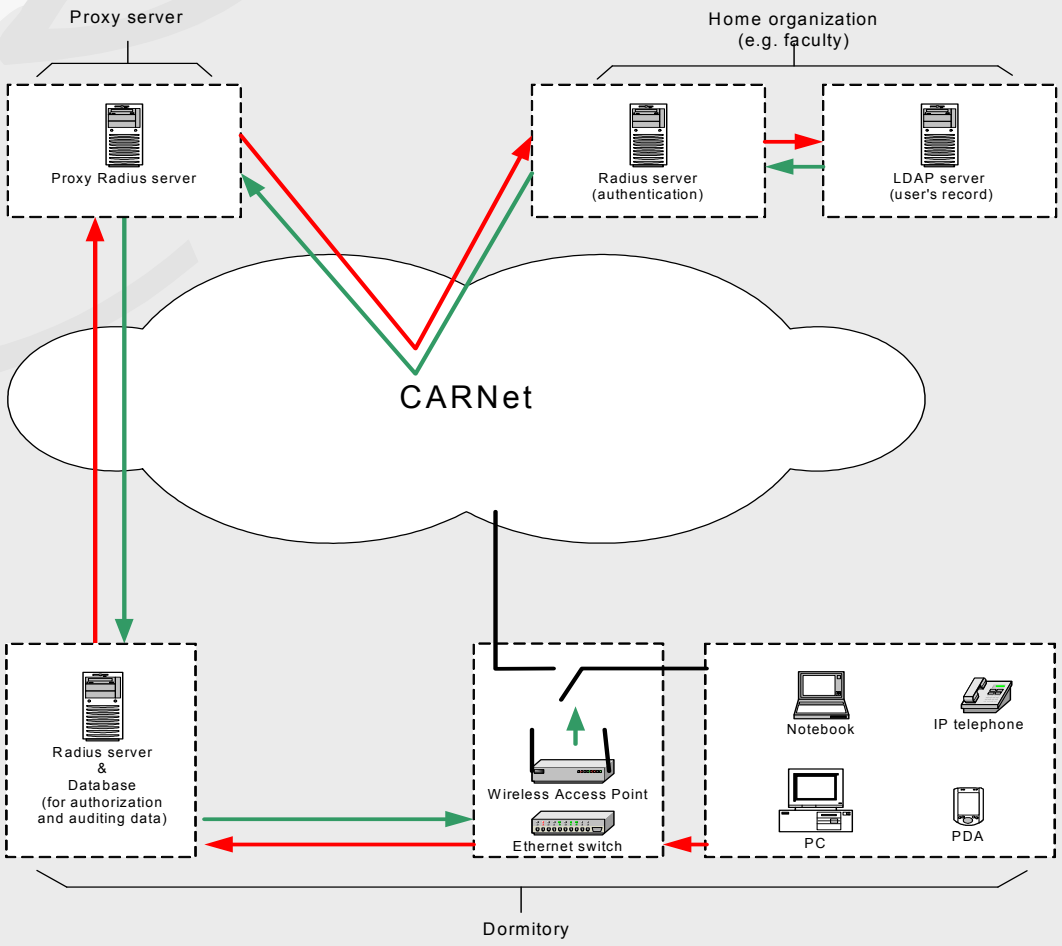
Virtual identity

- home orgs register users and provide them with the virtual identity (username / password)
- username consist of two parts:
  - unique user identifier (e.g. unix account login)
  - unique institution identifier (e.g. home orgs domain name)
  - an example: miro.srce
- for inter-NREN roaming @*.hr* extension has to be used:
  - miro.srce@.hr

Client for network access (802.1x)

- any device with EAP supplicant (client) for AuthN
- some of available clients:
  - MS Windows 2000 i MS Windows XP – secureW2
    http://www.alfa-ariss.com/
  - LINUX/UNIX - *http://www.open1x.org/*
  - Win95, Win98, Win98 SE, MAC
    http://www.mtghouse.com/
    http://www.funk.com/

StuDom AA(A)


Proxy server
Home organization
(e.g. faculty)
Proxy Radius server
Radius server
(authentication)
LDAP server
(user's record)
CARNet
Radius server
&
Database
(for authorization
and auditing data)
Wireless Access Point
Ethernet switch
Notebook
IP telephone
PC
PDA
Dormitory

StuDom AA(A) system - technology

- authenticated and Authorized wired and wireless access to CARNet network using IEEE 802.1X
- Username/Password based Authentication
- User Mobility: connection from any part of the StuDom Network
- no simultaneous network access allowed: connection to only one work place at the time using same username/password
- switch uses EAPOL and EAP-TTLS for the exchange of authentication messages with a client and Radius server

StuDom AA(A) - implementation

- each user has to be **authenticated** or recognised as a member of Croatian academic and research community
- each user has to be **authorised** for the use of the StuDOM service (network access)
- adding **auditing** element as a way of supervision of the StuDOM service usage

AAI@EDU.HR project

- joint project of Srce and CARNet endorsed and financed by Ministry of Science, Education and Sports

- main goal: to establish AAI for higer education community in Croatia
- 2 years:
  - Phase I (first year): define and establish basic AAI
  - Phase II (second year): introduce certificates/PKI and ensure wide use of established AAI

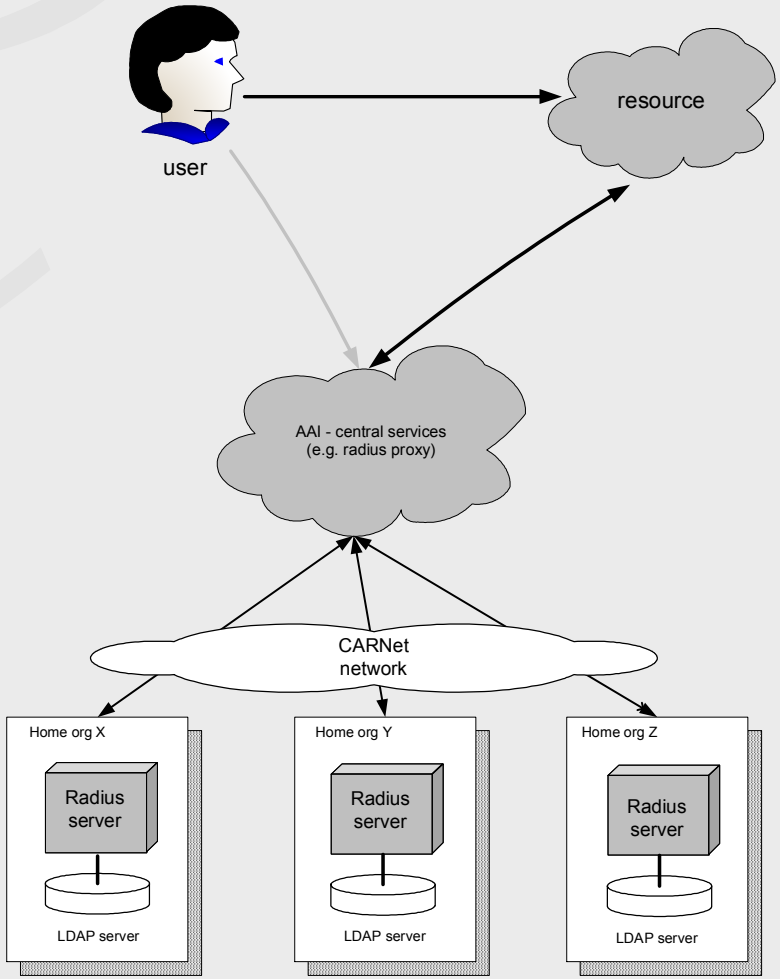
AAI@EDU.HR: Goals

- define concepts, architecture and standards of AAI for higer education community
- define rules an policies in order to ensure the reliability, quality and consitency, of the directories used for storing data about the users
- establish basic AAI for higer education community
- ensure that the established infrastructure is used as widely as possible
- examine the possibility and introduce use of certificates / PKI instead of weak user/password AuthN

AAI@EDU.HR: Deliverables

- AAI.1: establish the “AAI Board”;
- AAI.2: an overview of current status regarding the use of AA(A) systems;
- **AAI.3**: **technical and organisational standards of AAI** for higher education community;
- AAI.4: rules and policies for AAI maintainance (technical, informational, organisational);
- **AAI.5**: extensible **CroEduPerson directory schema** (with rules and policies for further development / maintenance);
- AAI.6: rules and policies for LDAP directories maintenance (technical, informational, organisational);
- **AAI.7**: **extensible and functional AAI** based on distrubuted LDAP directories;
- **AAI.8**: **AAI deployed** (in use for selected / major resources);
- **AAI.9**: **center for support and training**;
- AAI.10: application of certificates /PKI;
- AAI.11: test and implement SSO;
- **AAI.12**: **interconnect with other national/international AAIs**

AAI@EDU.HR: Model



CroEduPerson schema

- follow European and Internet2 experience but meet local needs
- current CMU schema – starting point
- based on available and widely accepted schemas:
  - person, orgPerson, inetOrgPerson, eduPerson
- make sure to:
  - meet the needs of Croatian higher education community
  - be interoperable
  - support standards like: H.350, X.509 certificates
- ver. 1.0 will be available for comments in October 2004

Contents

- Part 1: AA(A) problem and solutions
  - Needs & challenges
  - AA(A) problem
  - AA(A) Infrastructure
  - AAI vs. PKI
  - SSO
- Part 2: AAI@EduHr
  - Current status in Croatia
  - AAI@EduHr project & deliverables

Your task ...

... help us to solve the AAI puzzle!

aai@srce.hr

http://www.srce.hr/aai