SWITCH

The Swiss Education & Research Network

# Authentication and Authorisation Infrastructure - AAI

**Christoph Graf <graf@switch.ch>**

**Project Leader AAI**

**SWITCH**

SWITCH aai

# e-Academia / AAI Concept

SWITCH
The Swiss Education & Research Network

## Vision of e-Academia

"We want a virtual community across our institutions in which all persons associated with the Swiss Higher Education System are able to gain access to its electronic resources, independent of the accrediting organization and independent of the place where they happen to be working."

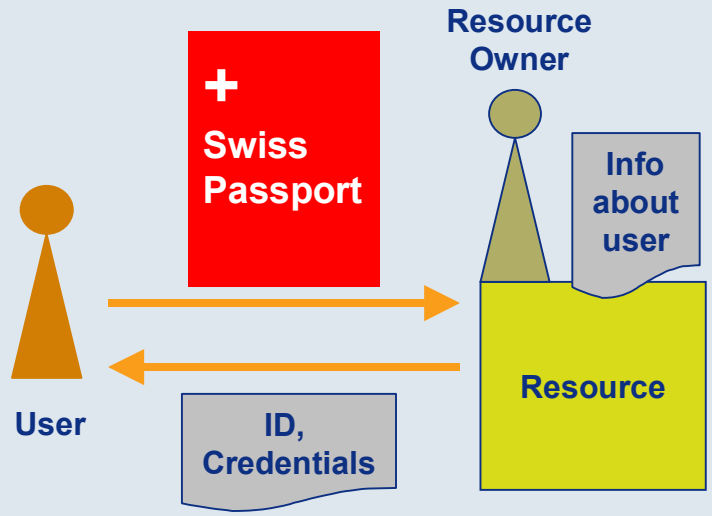
## AAI as the foundation of e-Academia

"… let's develop e-Academia, let us build the foundations in the form of a uniform authentication and authorization infrastructure (AAI) for the higher education system in Switzerland…"

## Roadmap

# The AA Problem (1)

SWITCH
The Swiss Education & Research Network



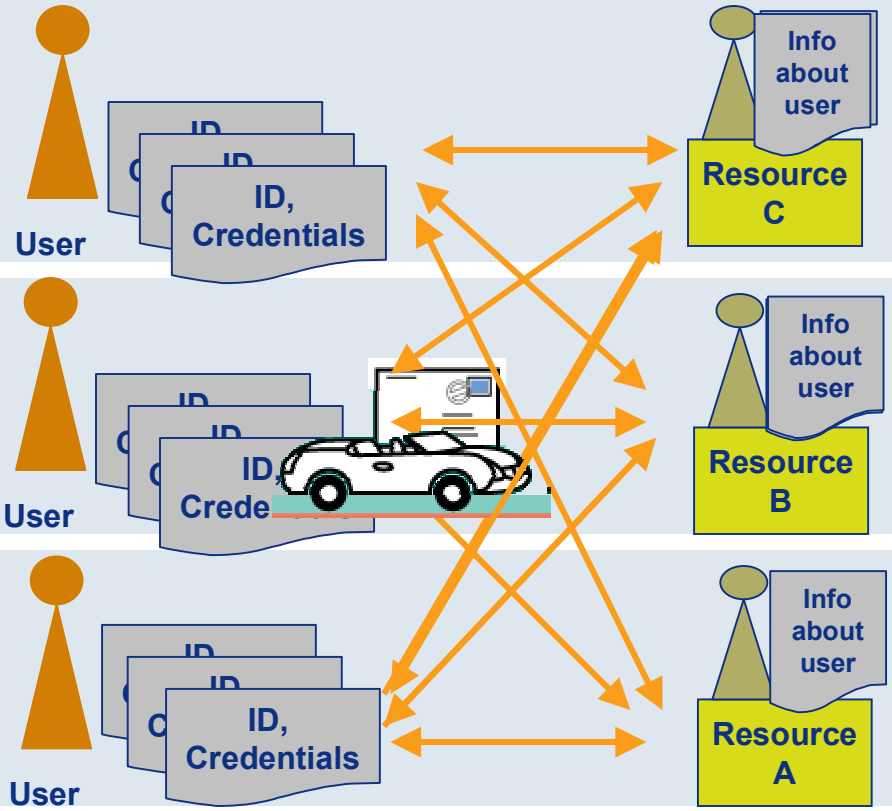

University of Zurich

**1 user - 1 resource - 1 organization:**

**NO PROBLEM**

# The AA Problem (2)

SWITCH
The Swiss Education & Research Network

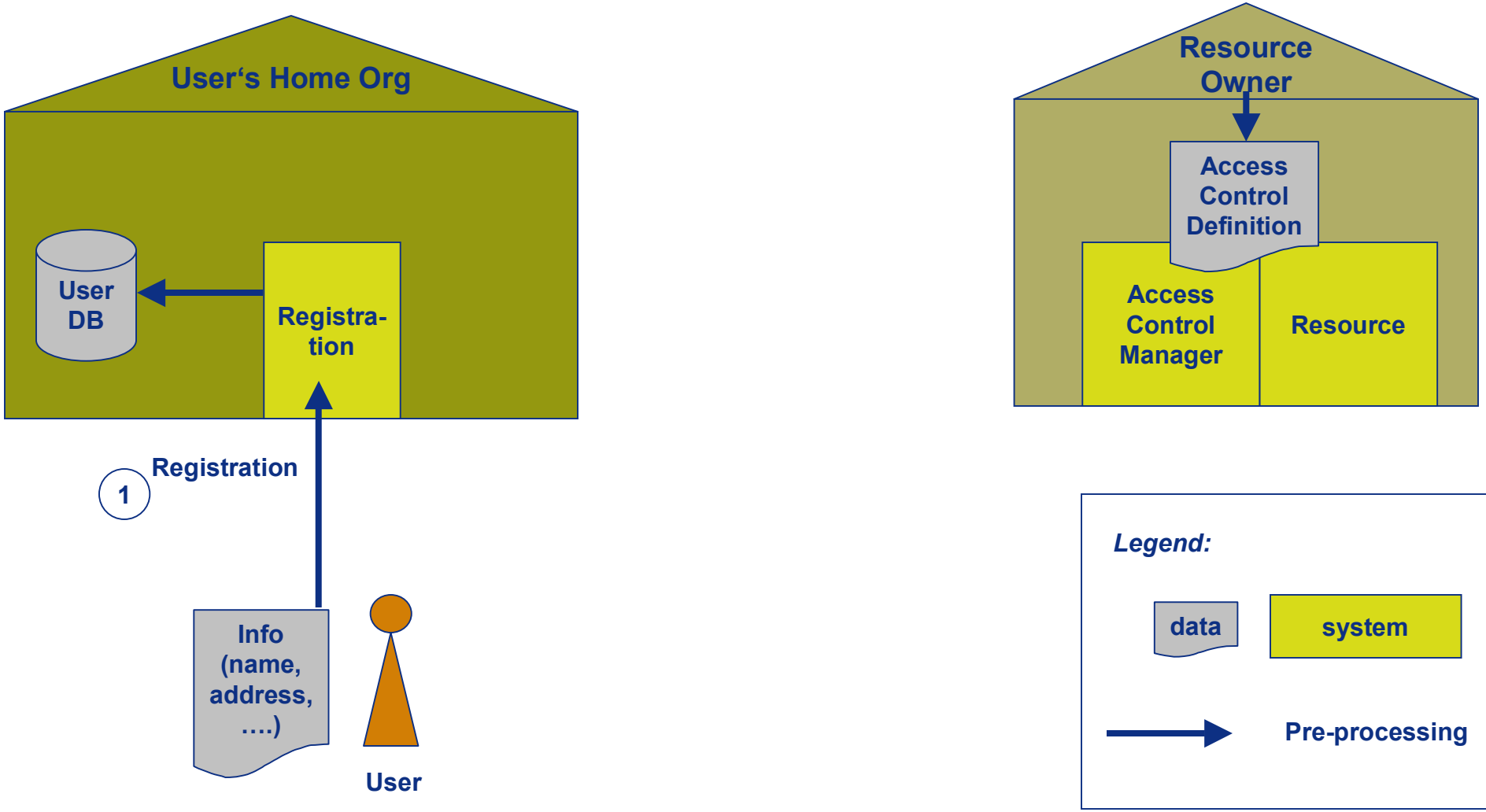



**Many users - many resources - many organizations:**

**A PROBLEM**

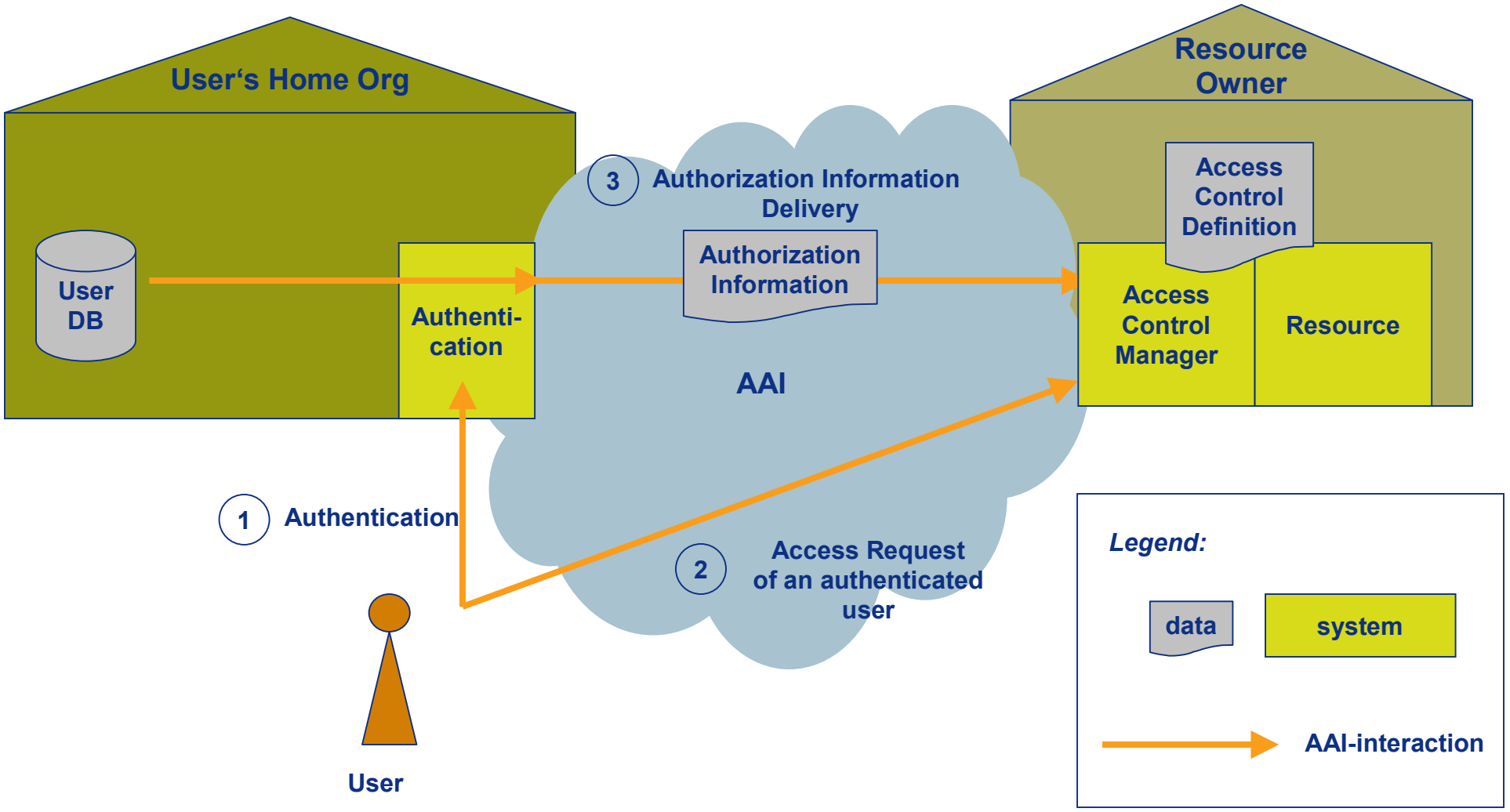
# The AA Model (1)

SWITCH
The Swiss Education & Research Network



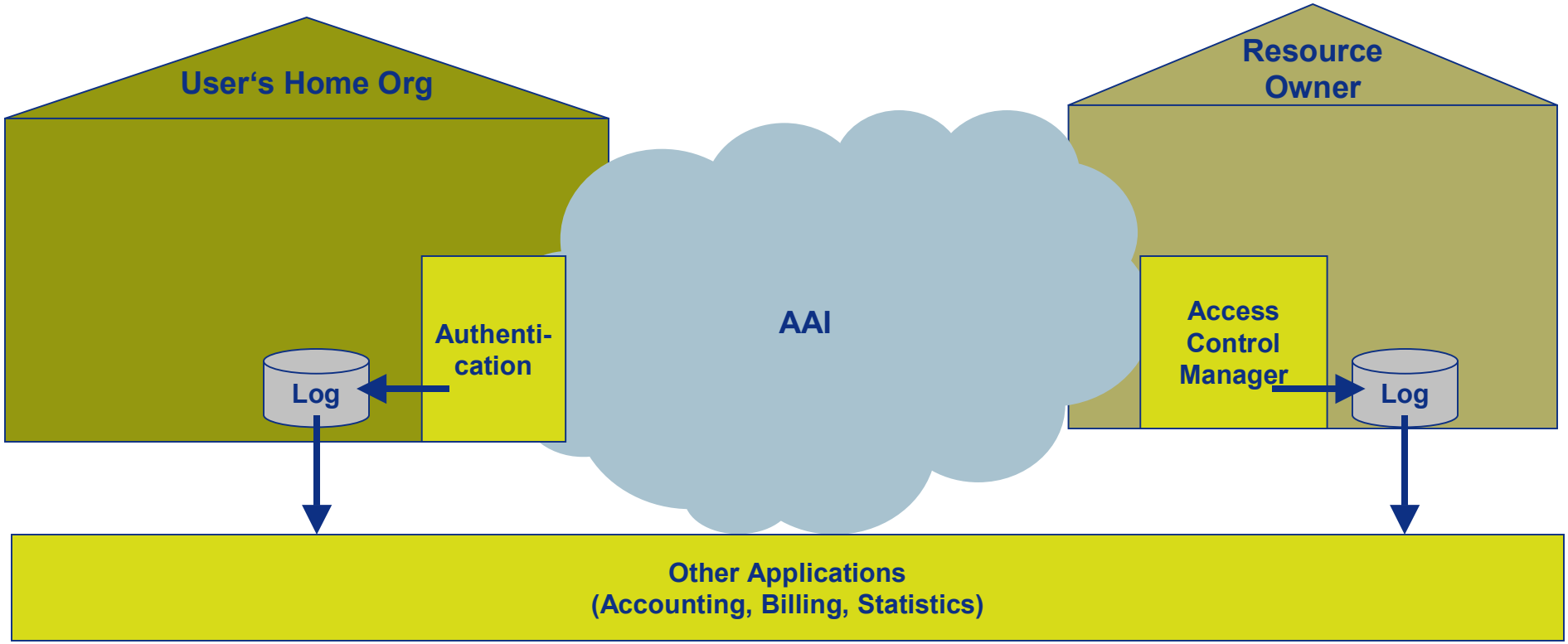
# The AA Model (2)

SWITCH
The Swiss Education & Research Network



# The AA Model (3)

SWITCH
The Swiss Education & Research Network




**Input to Accounting or Billing systems:**

- **AAI provides Identity of User and/or Name of Home Organization**
- **Resource measures the interactions between a user and the resource**

# Advantages of an AAI

SWITCH
The Swiss Education & Research Network

| | |
|---|---|
| **Virtual Mobility** | AAI is a requirement if students of different universities wish to use common resources, and it is the basis for initiatives such as the Swiss Virtual Campus. |
| **Information protection** | AAI simplifies the protection of information by applying standardized mechanisms. Resource owners can concentrate on the protection of their resources without having to implement an entire system including registration and authentication. |
| **Remote access** | AAI makes it possible to authorize users based on personal attributes of a user instead of IP addresses. User authorization thus becomes location-independent. |
| **User friendliness** | After a single registration a user can access a number of resources. Only one authentication technology is applied. |
| **IT efficiency** | Standardized AA systems and cooperation among IT organizations improve the efficiency in the implementation and operation of security solutions. |
| **Administration overhead** | Without AAI, a user has to register with various organizations. It is feared that the administrative overhead of individual organizations will increase dramatically. AAI counteracts this tendency. |
| **Image** | Complicated and inconsistent AA mechanisms, or isolation of resources and user groups, respectively, is no longer state of the art. Not having an AAI will damage the image in the long run. |

# Authorisation Attributes

SWITCH
The Swiss Education & Research Network

**Personal attributes**

- Unique Identifier (anonymous)
- Surname
- Given name
- Date of birth
- Gender
- E-mail
- Address(es)
- Phone number(s)
- Preferred language

**Group membership**

- Name of Home Organization
- Type of Home Organization
- Affiliation (student, staff, faculty, …)
- Study branch
- Study level
- Staff category
- Organization Path
- Organization Unit Path
- Group membership

**User attributes for AAI**

- are based on standards (LDAP: eduPerson, SHIS/SIUS)
- have to be available in real-time
- have to be handled as required by federal and cantonal data protection laws:
  - attributes have to be accurate
  - attributes have to be stored securely
  - attributes should only be transferred to resources with a valid case to use it.
- will be revised in the future in a standardised change process, depending on the requirements of Resource Owners and Home Organizations

# Simple Identity Management Classification

SWITCH
The Swiss Education & Research Network

simple

complex

## MS Passport

- Trust model: One external trust broker, trust monopoly
- One central user database
- One single Home Organisation for all users

## Shibboleth

- Trust model: “Club” of organisations trusting each other (but not necessarily their users!)
- Decentralised user database at “Club” member sites
- “Club” members acting as Home Organisation
- Users are registered with exactly one Home Organisation, maintaining their electronic identity (otherwise, they end up owning multiple electronic identities)

## Liberty Alliance

- Same as Shibboleth except:
- Users may register with multiple “Club” members
- Each Club member is maintaining a part of their user’s electronic identity