

# Attributes in Shibboleth



# SWITCH

Serving Swiss Universities

Christoph Witzig

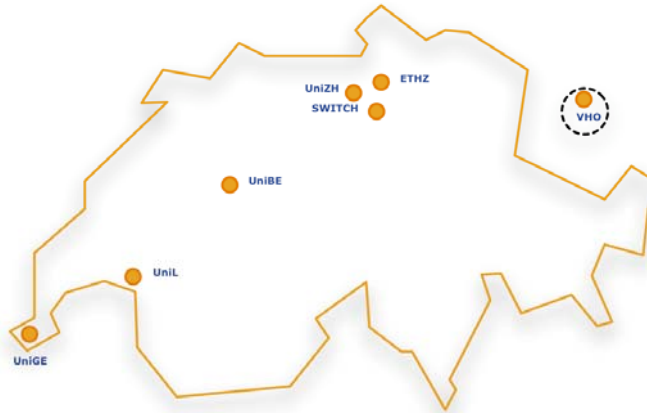
[christoph.witzig@switch.ch](mailto:christoph.witzig@switch.ch)

# Content

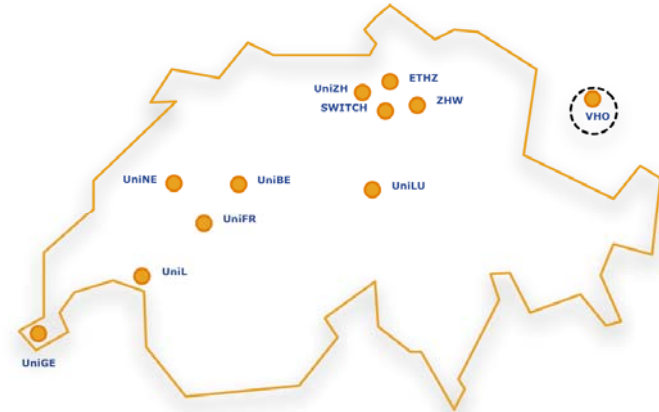
- Introduction
- Attribute Handling in Shibboleth - the software part
- Defining Attributes - the “real world” part
- Outlook

# Introduction: SWITCHHai Federation

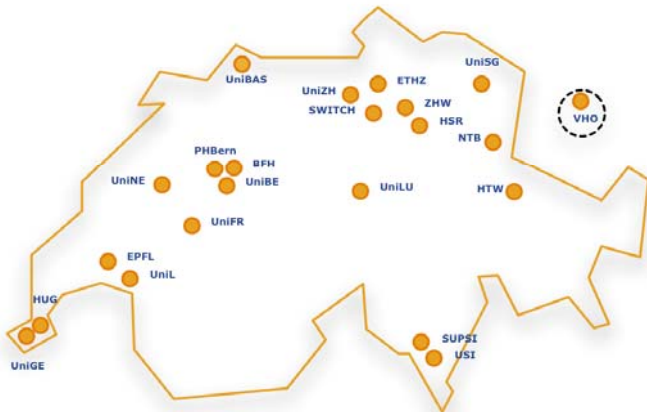
Operating Home Organizations  
Ende 2004



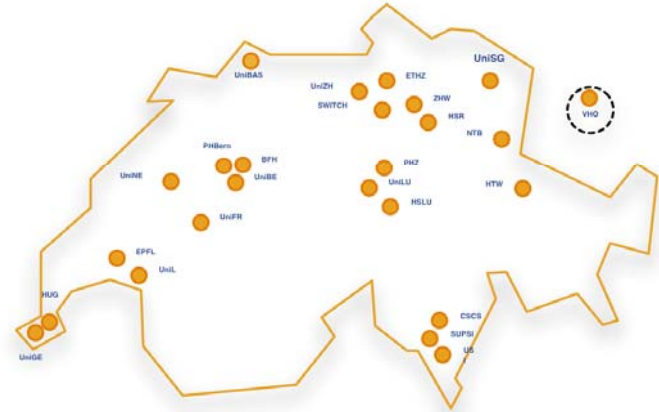
Operating Home Organizations  
Ende 2005



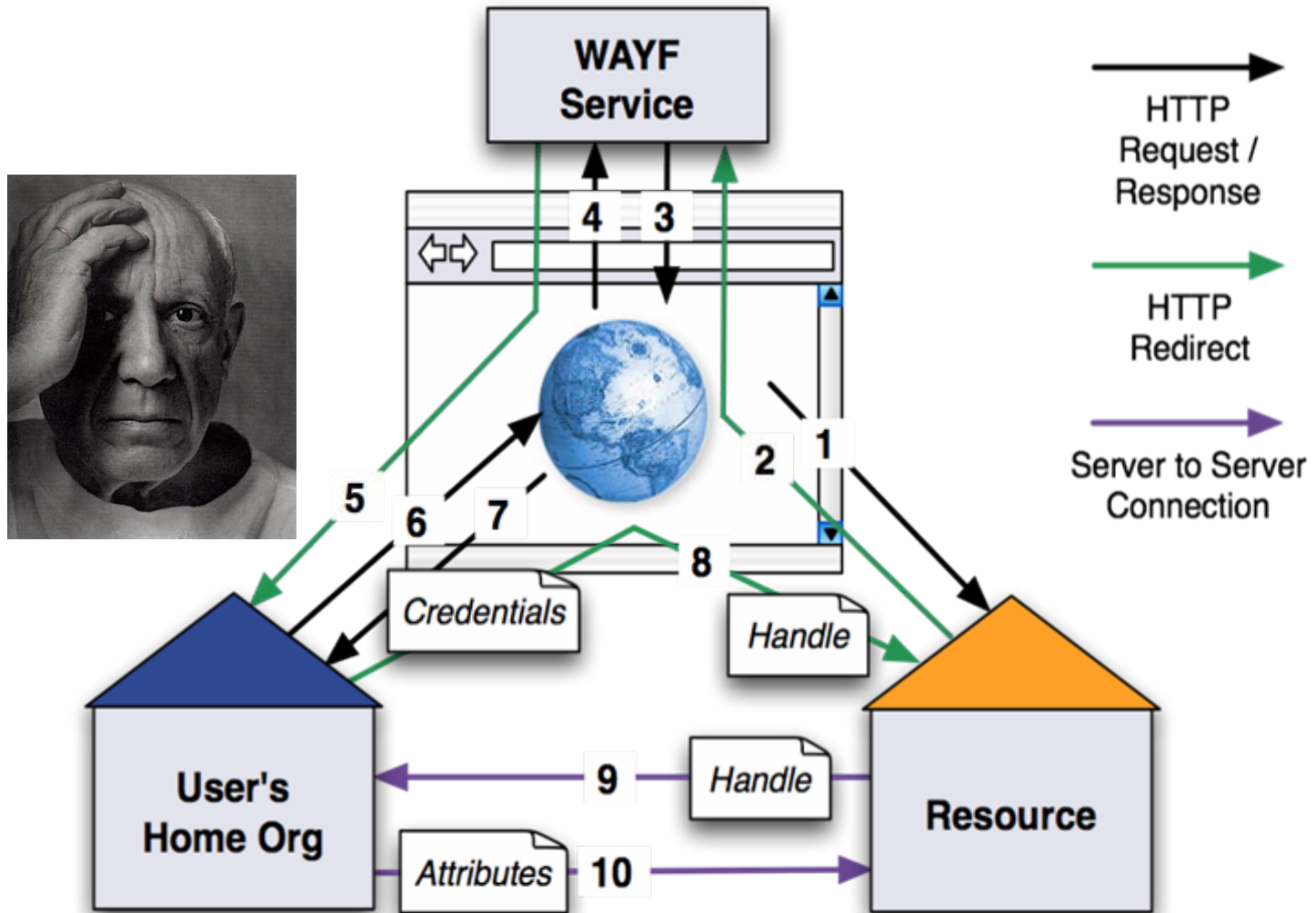
Operating Home Organizations  
Ende 2006



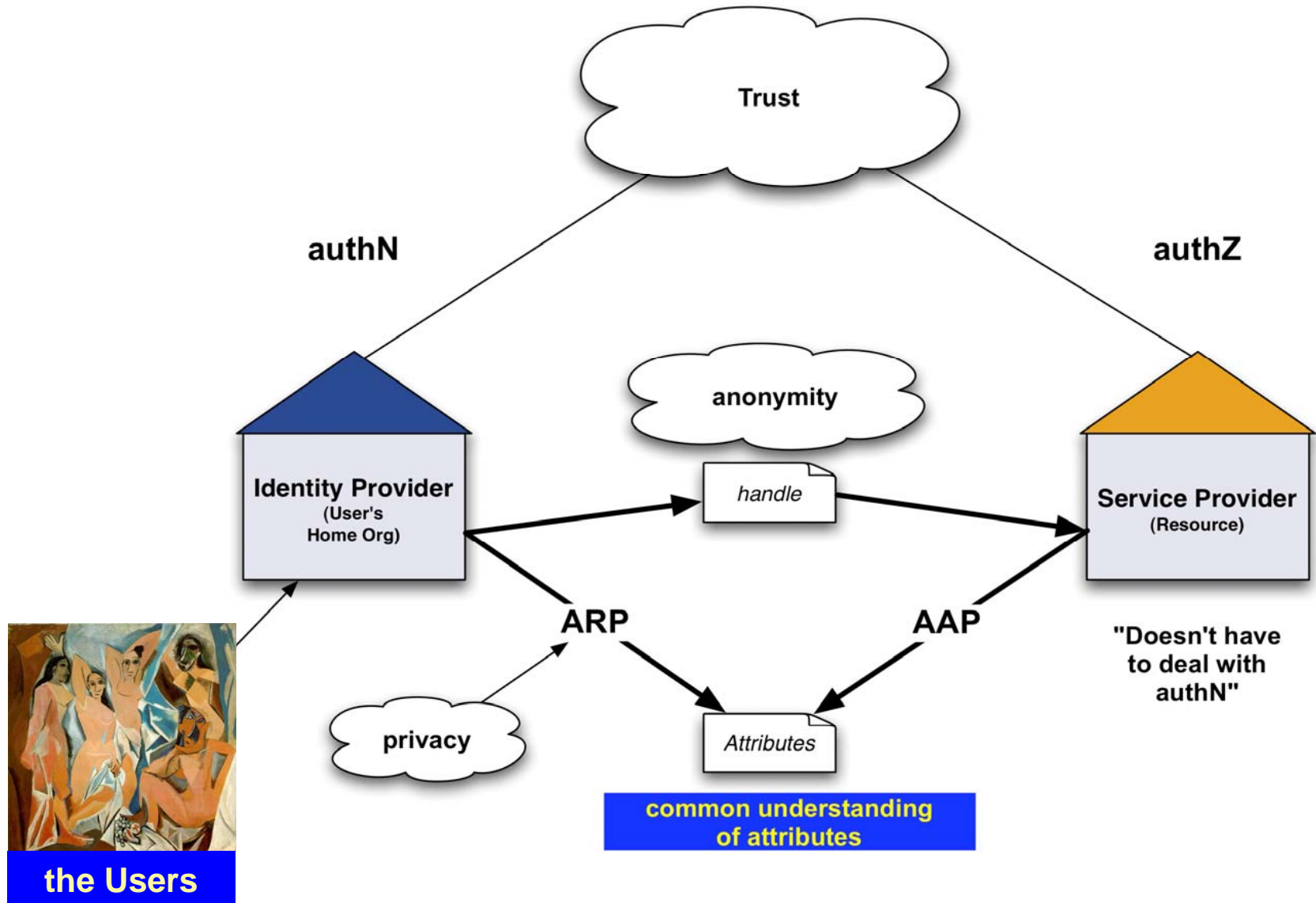
Operating Home Organizations  
September 2007



# Shibboleth User Experience



# Shibboleth Concepts



# Attribute Handling

- There must be a common understanding of the meaning of the attributes within the federation
  - I.e. across all IdP's and SP's
  - Naming (URN/OID) and values must be consistent
- Attribute Release Policy (ARP) and Attribute Acceptance Policy (AAP) must be coordinated
- Consistent metadata handling within the Federation
  - Resource Registry developed by SWITCH

# Attribute Definition SWITCHaai

- Naively you would expect this to be easy, but ....
- SwissEduPerson based on EduPerson
- SwissEduPerson contains additional information about StudyLevel and StudyBranch
  - Defined and coordinated at the federal level
  - Consistent across all Cantonal Universities, ETH Bereich and Universities of Applied Science
- Group specific attributes and attributes specific for an individual user
- Distinguish between mandatory, recommended and optional attributes
- Allow for attributes specific for a given institution

# Attribute Specification Taskforce

- Was formed in 2002 (!) with members from all institutions involved
- An ongoing effort
  - Otherwise the attribute handling would inevitably break over time
- Task force only defines attributes that are
  - Can be implemented by the IdP's
  - Are useful to transfer with Shibboleth
- <http://www.switch.ch/aai/attributes>

# Shibboleth Attributes vs VOMS Attributes

Shibboleth	VOMS
Atomic attributes	Composed attributes (groups and roles) (FQAN) e.g. /atlas/analysis/role=production
Key - value pairs	Fixed strings (not key-value pair)
Multi-value attributes	Fixed strings
Attribute release policy and attribute acceptance policy	Groups are always present Roles are chosen by user
User can control ARP (several implementations exist)	User can control order of groups and presence of roles
SP authorizes user based on attribute value(s) [ &&,    ]	Evaluates FQAN depending on MW (w, w/o wildchars)

**Note:** newer versions of VOMS support generic attributes (key-value pairs)

# Summary

- Consistent attributes are essential for a production AAI
  - Software as well as policy
  - An ongoing process
- Inter-federation handling
  - The same applies for inter-federation access
  - ... just when you thought you were done with your own federation, then...