

**AAI:
Authentication and Authorization Infrastructure
for the
Swiss Higher Education System**

**Christoph Graf
SWITCH
Zürich, Switzerland
graf@switch.ch**

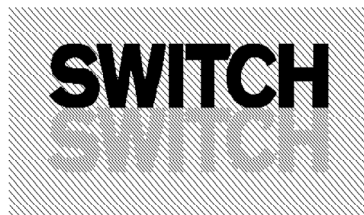
About SWITCH



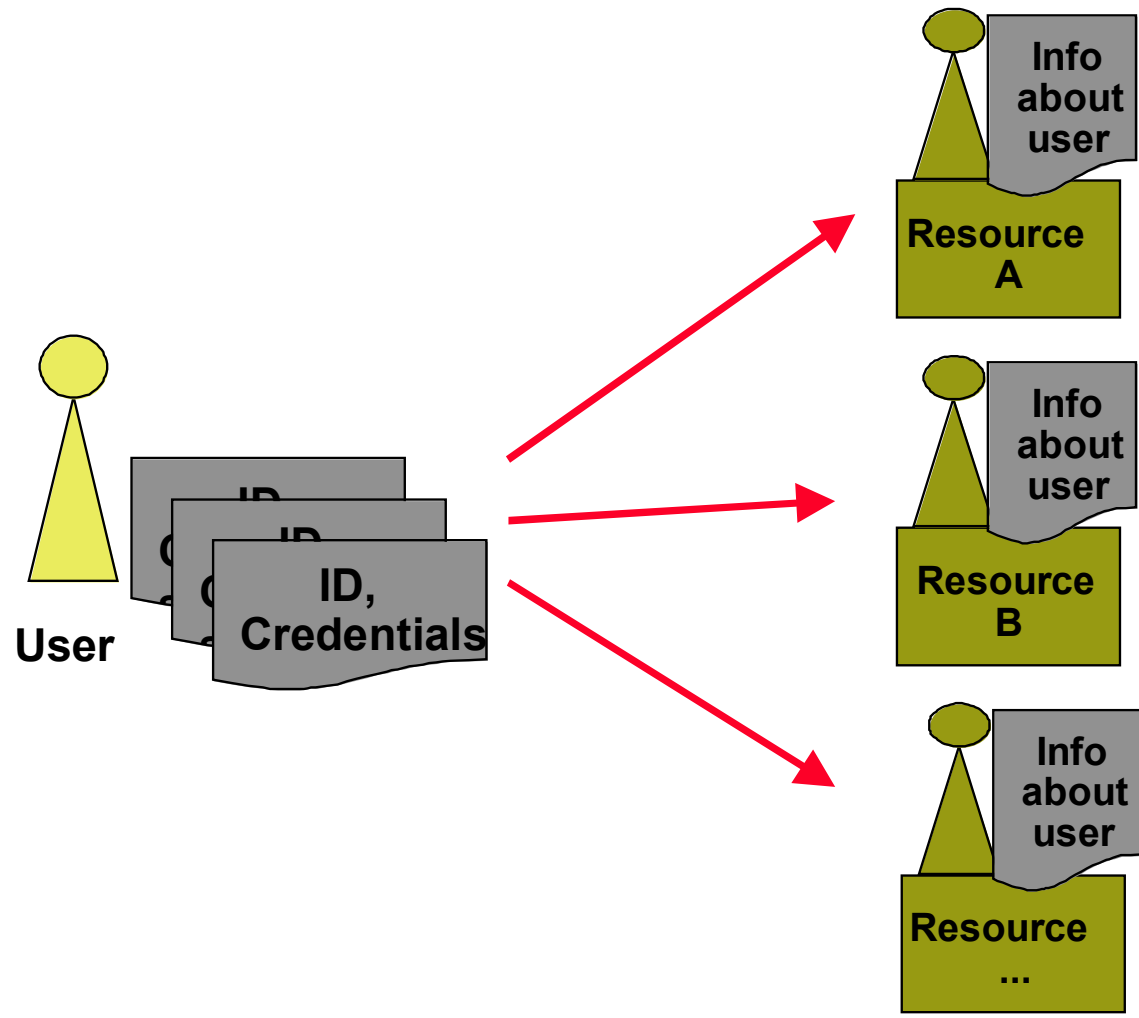
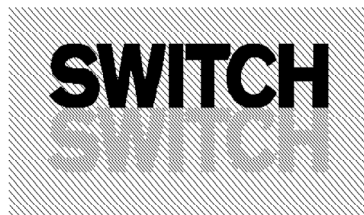
- **Established in 1987**
- **SWITCH is a foundation of the Swiss Confederation and 8 cantons hosting universities**
- **Aim: To promote modern methods of data transmission and to set up and run an academic and research network in Switzerland**
- **Head office located in Zurich, Switzerland**
- **SWITCH operates the domain name registration for the .ch zone**

- **The AA problem**
- **Earlier activities: AAI roadmap**
- **Present activity: AAI preparatory study**
- **A generic view on AAI**
- **Recommendations**
- **Outlook: AAI pilot phase**
- **Final remarks**

AA-Problem (1)



AA-Problem (2)



AA-Problem (3)

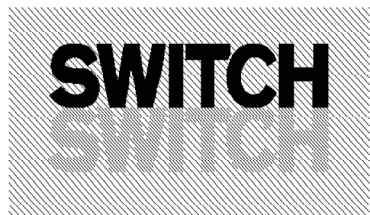
- **User registration per resource**
 - **Considerable overhead, both for the user and the resource provider**
 - **Difficult in the case of remote resources**
 - **Often not needed by access policy, but not easy enforceable without user registration (e.g. only students are allowed)**
- **Preexisting trust is not taken into account**
 - **Existing trust relationships might make the re-registration completely redundant**
- **Authentication is up to the resource**
 - **The user might be faced with different technologies for different resources**
 - **The resource provider is faced with a potential support problem**

Authentication and Authorization Infrastructure (AAI)

- **Registration at user's home organization only**
 - **needs to be done there for other purposes anyway**
- **Trust relationship**
 - **Resource providers need not re-register users, if they trust the registration process of the user's home organization**
- **Authentication method**
 - **The user's home organization chooses their method of choice**
 - **One interface for the user**

- **SWITCH applies for Swiss Virtual Campus mandate in Nov '99: “Evaluation and Implementation of an Authentication and Authorization Infrastructure”**
- **SVC-mandate “AAI” granted to SWITCH in Dec '00**
- **Workshop dedicated to AAI in Nov '00 in Gerzensee**
- **Inter-university working group formed to propose a road map towards an AAI at the Gerzensee workshop (AAI-TF)**
- **Final report of AAI gets published in Sep '01 titled: “Concept for an Electronic Academic Community in Switzerland and the Creation of a Common Authentication and Authorization Infrastructure (AAI) for the Swiss Higher Education System” (AAI-Concept). The concept receives the blessing of CRUS (Conférence des Recteurs des Universités Suisses). Report is available at: <http://www.switch.ch/aai/>**

Roadmap “AAI-Concept”



 preparatory study
(October 2001 - mid 2002)

 Decision: Entering pilot phase
(mid 2002)

 Pilot project
(mid 2002 - mid 2003)

 Decision: Implementation
(mid 2003)

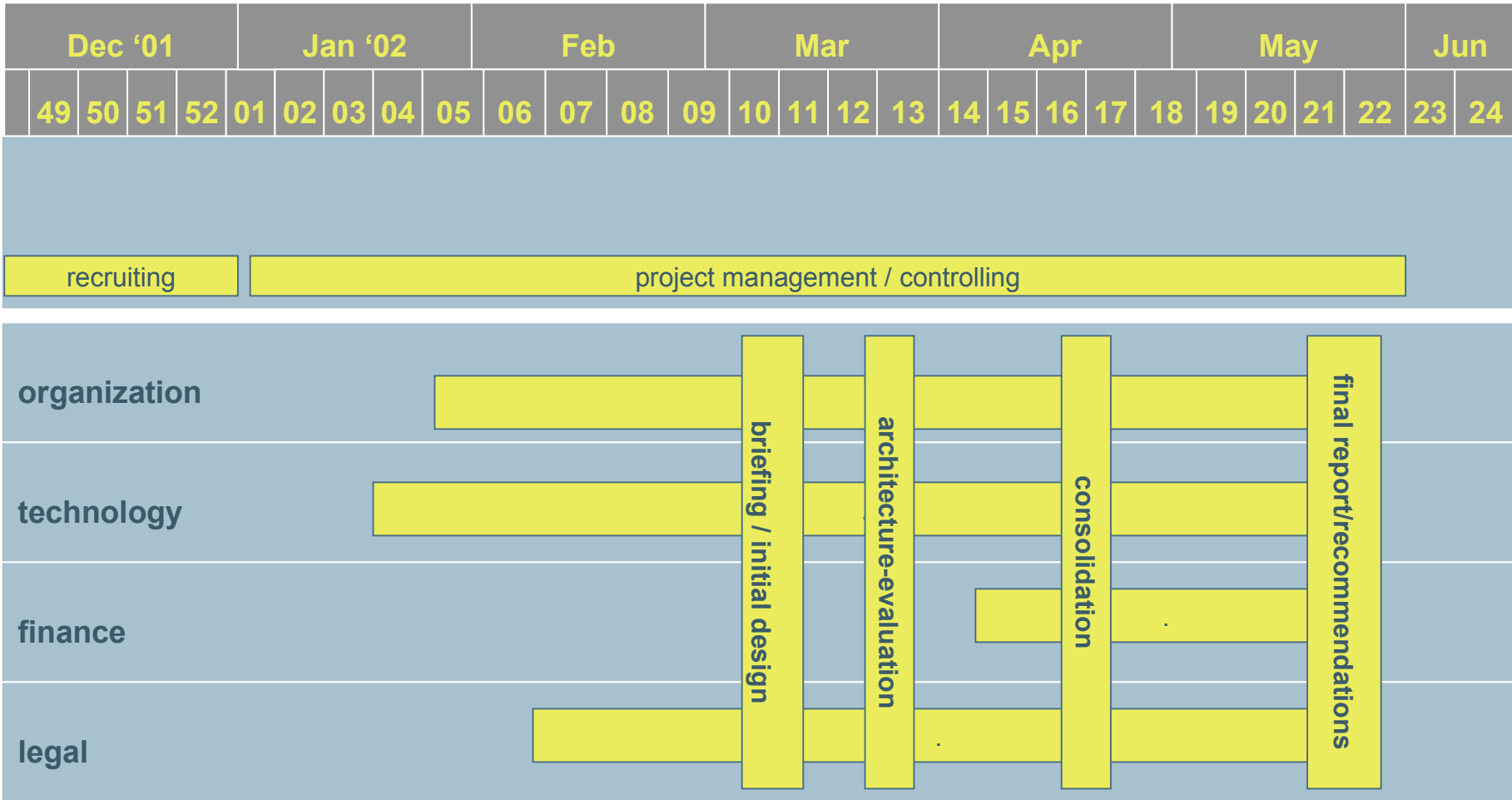
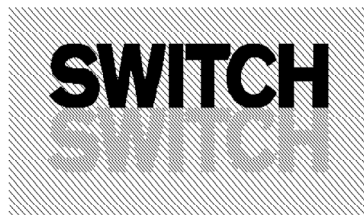
 Implementation
(mid 2003 - mid 2005)

Current Activity and Outlook

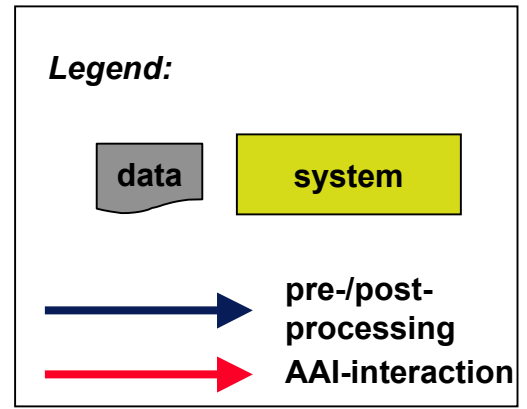
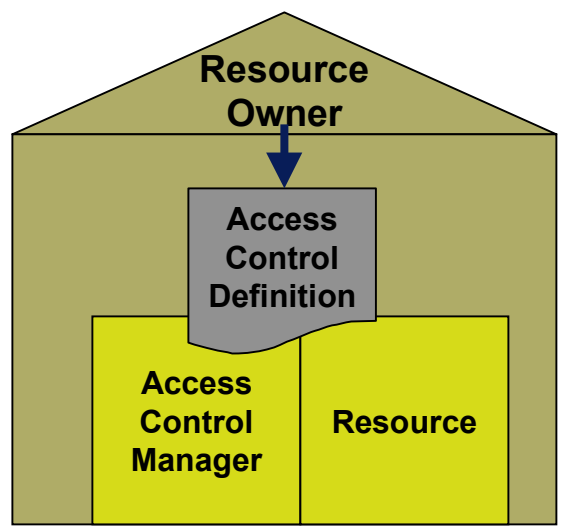
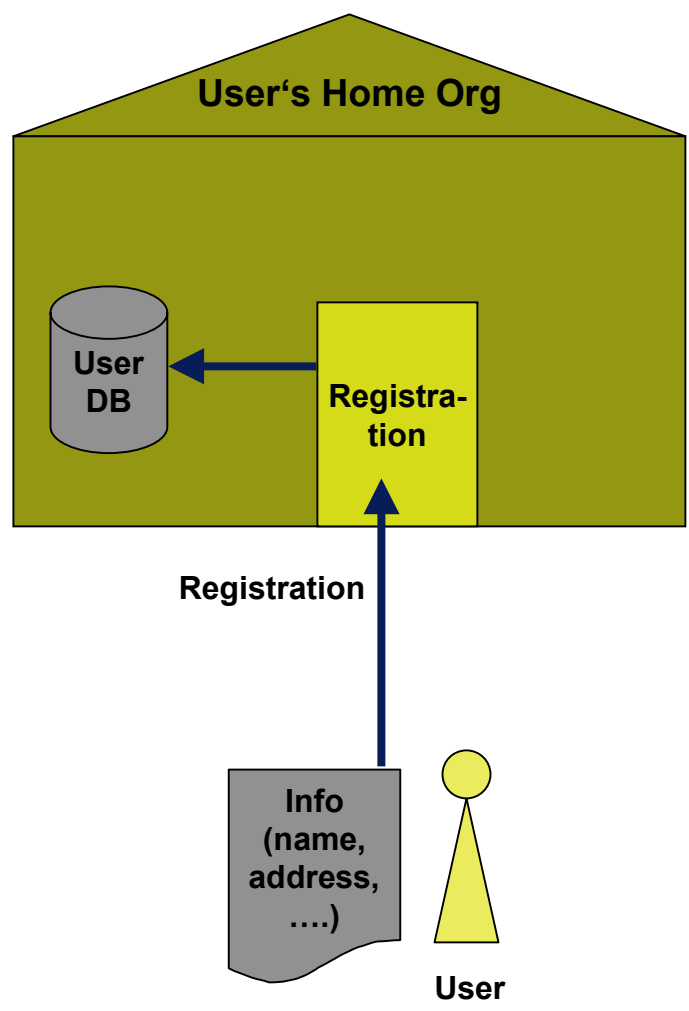
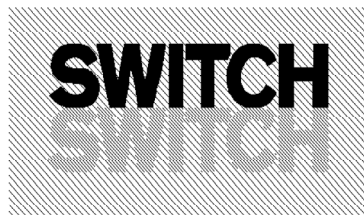


- **Oct '01: SWITCH starts implementing the first step proposed in the roadmap, the “AAI preparatory study” and invites experts from the Swiss higher education community**
- **The final report of the AAI-project is expected mid 2002**
- **SWITCH plans to go ahead and implement the next step as proposed in the AAI-Concept: a 1 year “AAI Pilot Phase”, starting mid 2002**

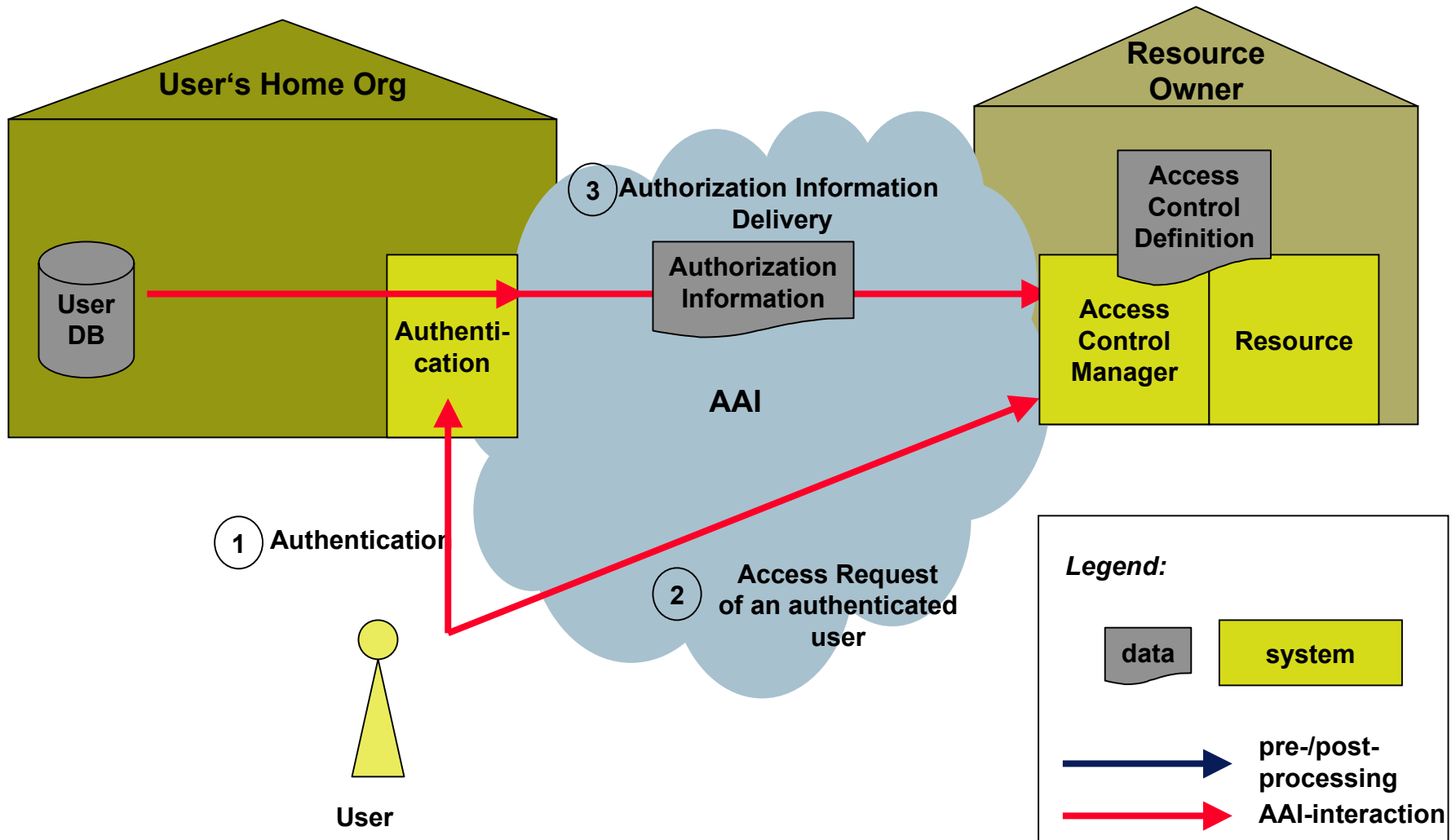
Project Plan “AAI Preparatory Study”



Generic AAI design (1): Preparation

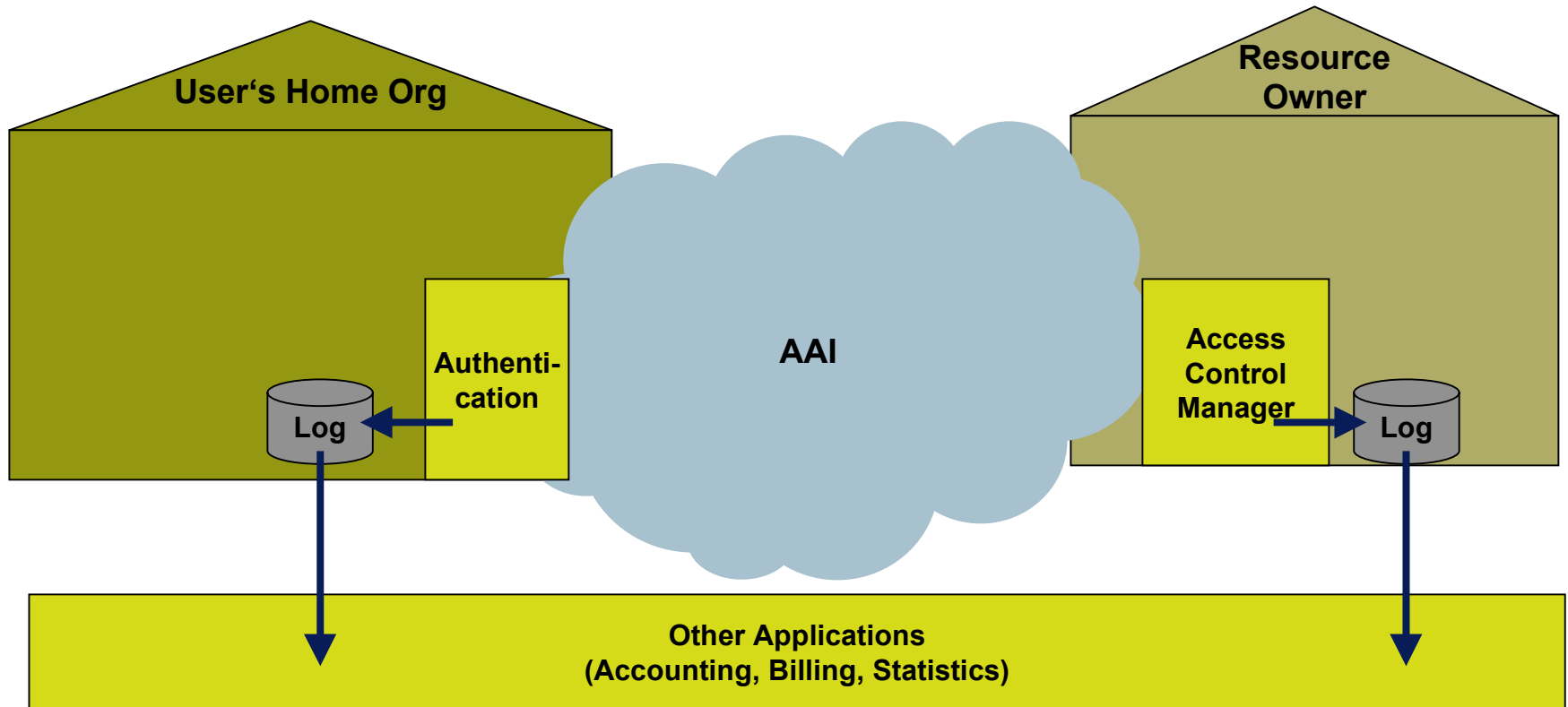


Generic AAI design (2): Authentication and authorization phase



Generic AAI design (3): Post Processing

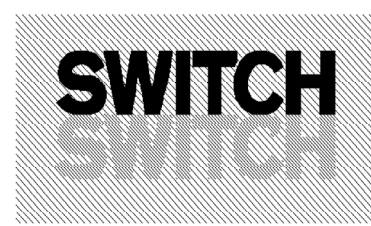
SWITCH
SWITCH



Scope:

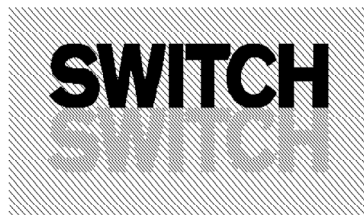
- Applications, like accounting and billing are not part of the AAI's basic functionality
- Hooks will be provided to link such applications to the AAI

Findings and Recommendations



- **ORG: involved processes / attributes exchanged**
- **JUR: legal framework / sample policy statements**
- **TEC: AAI architecture recommendations**
- **FIN: pilot phase financing**

ORG: Processes involved



Registration

Access Control Initialization

Authenticatio
n Authorization
Info Delivery Access
Cntrl
Decision

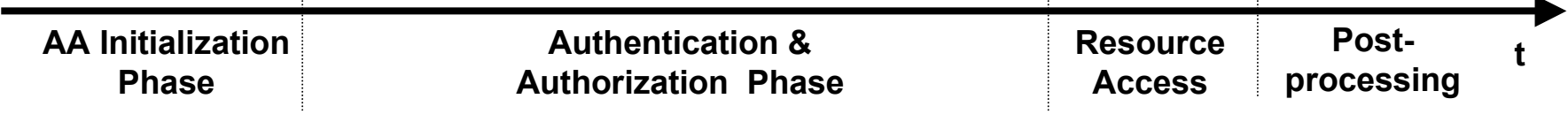
Resource
Access

Legend:

- Home Org
- Resource Owner
- AAI

Update
Author. Info

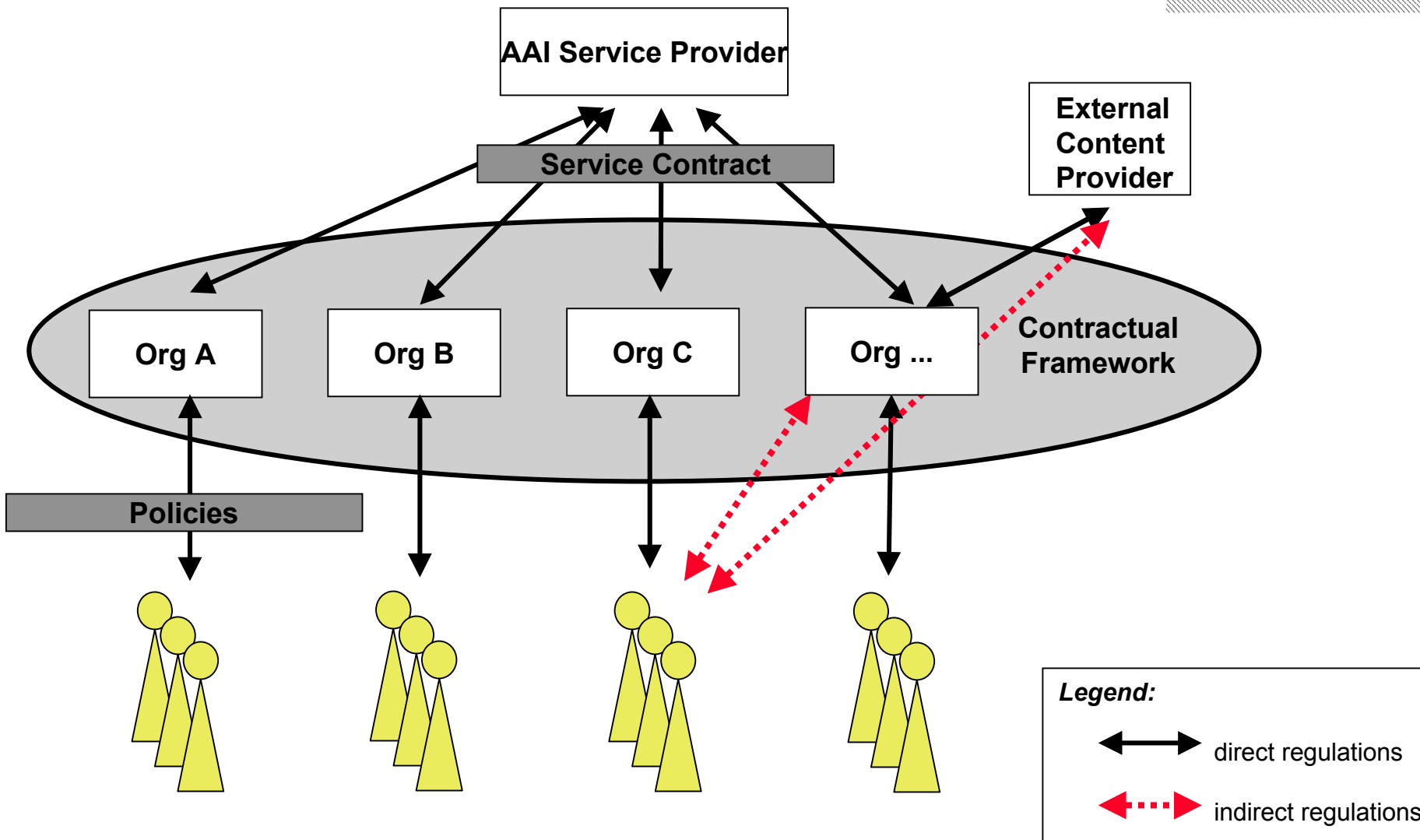
Accounting,
Billing,
Statistics



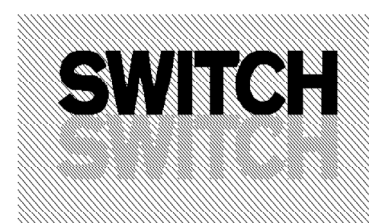
ORG: Attributes exchanged

Personal attributes	Membership/role attributes
<ul style="list-style-type: none">• Unique identifier• Name• Given name• Date of birth• Sex• E-mail• Postal address• etc.	<ul style="list-style-type: none">• Home organization• Type (student, staff, professor, etc.)• Faculty• etc.

JUR: Legal framework

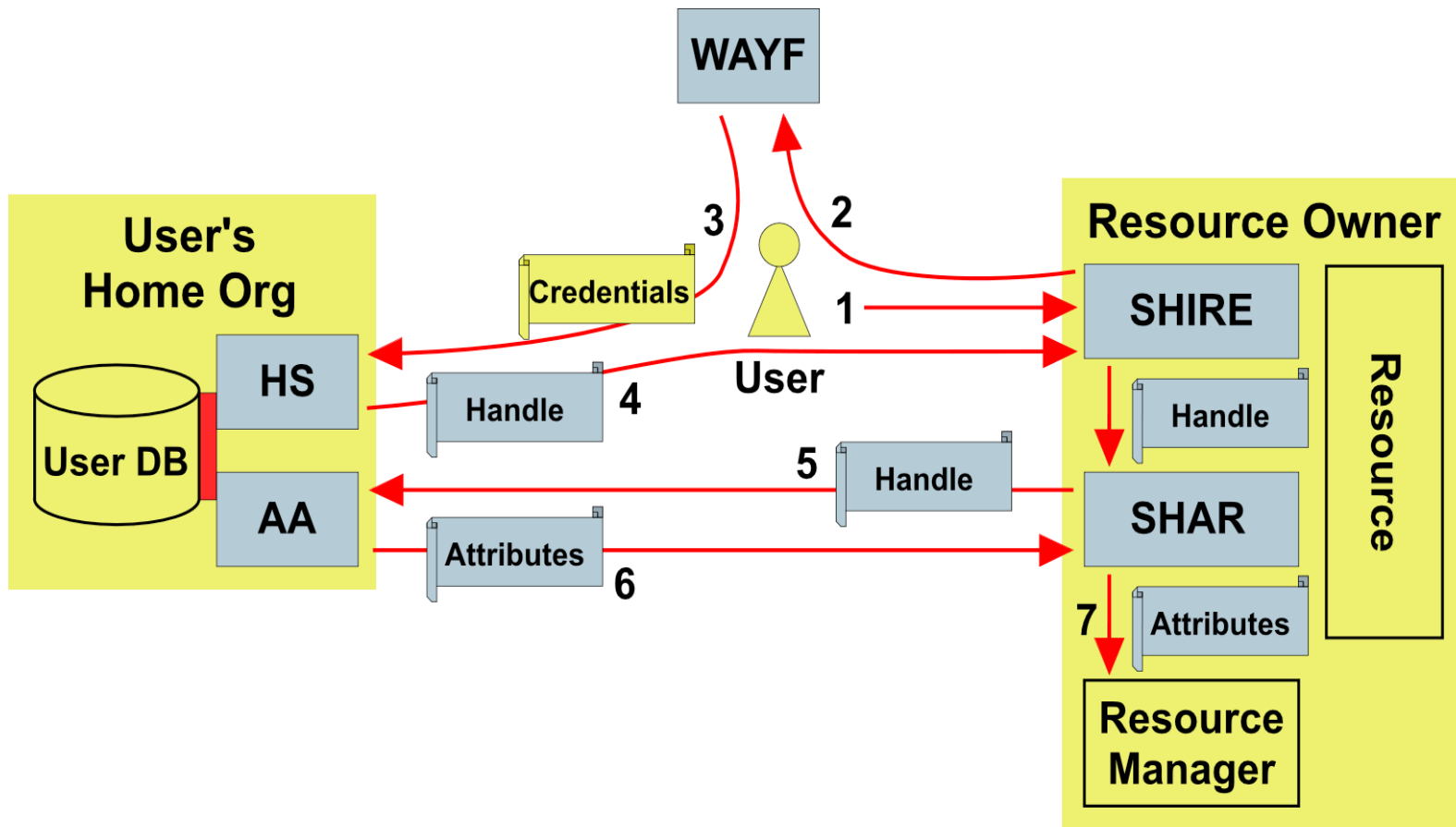
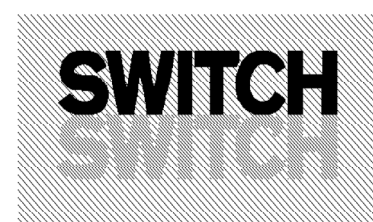


TEC: Recommended Architectures

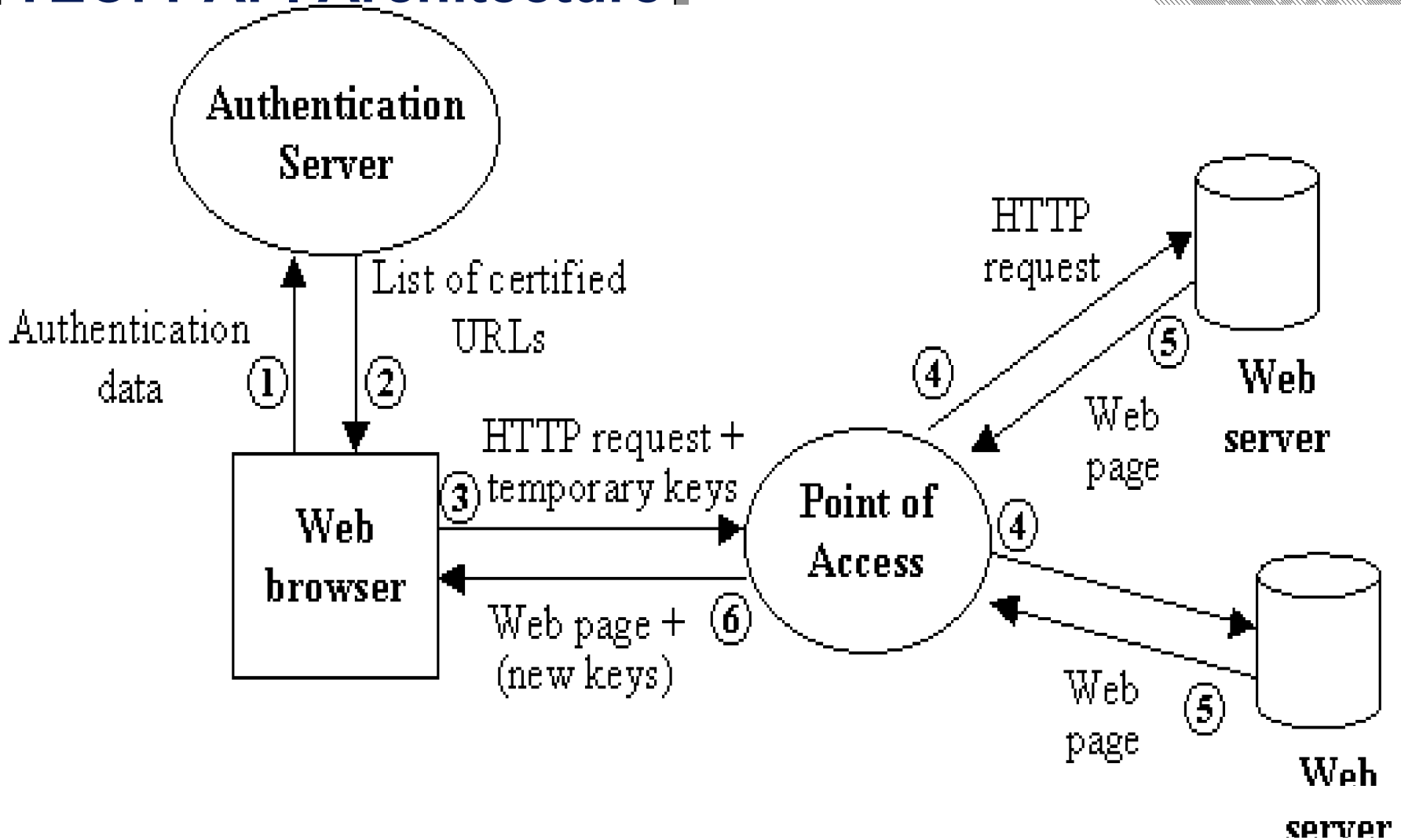


	Shibboleth (Internet2)	PAPI (Rediris, Spain)
INFO	Common project of Internet2/MACE and IBM with the goal to offer controlled inter-organizational access to protected web resources.	Tool for inter-organizational sharing of protected web based resources. Originally designed for external content providers to the Spanish universities.
+	<ul style="list-style-type: none"> • User privacy was an important initial design criterion • Minimal requirements towards user 	<ul style="list-style-type: none"> • Being actively deployed • User privacy was an important initial design criterion • Minimal requirements towards user
-	First software release expected mid 2002	Serious doubts remain regarding scalability, if used as a general purpose AAI
	Start piloting to gain operational experience	Start piloting to gain operational experience

TEC: Shibboleth Architecture



TEC: PAPI Architecture

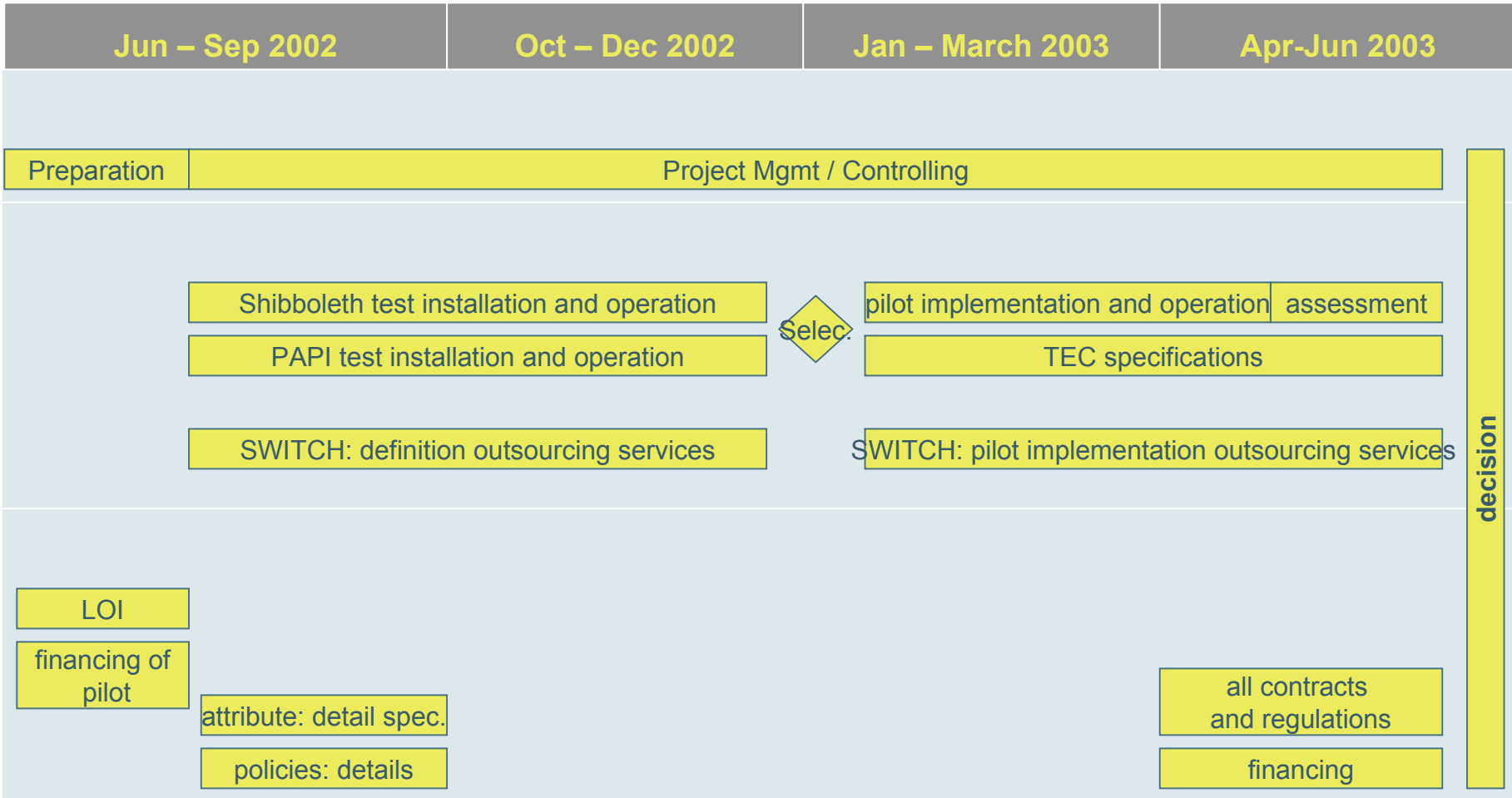
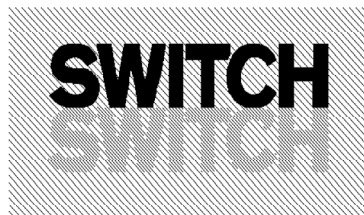


FIN: Pilot Phase Financing



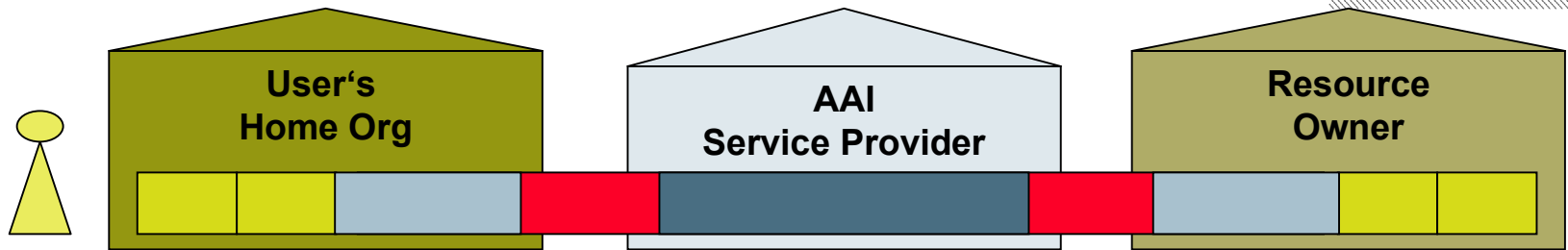
- **Very simple financing model: basically the same as in current project:**
 - **SWITCH is proposed to carry on with advance financing project management and marketing**
 - **Pilot projects financed by participants**

Project plan “AAI Pilot Phase”



decision

AAI-Rollout: Different Roles



Strategy and Marketing

AAI Business Alignment, Marketing, Financing, Contracting, Policies

Center of Competence

- Interface to Developers of AAI Kernel, international organizations, etc.
- Implementation of sample solutions
- Education: Knowledge base, best practices
- Test lab
- Change and release management
- Attribute specifications

Home Organization	Service Provider	Resource Owner
<ul style="list-style-type: none"> • Registration and authentication services • User directories 	<ul style="list-style-type: none"> • Provider of central AAI services 	<ul style="list-style-type: none"> • Resources • Access Control

Outsourcing Provider(s)

- Outsourcing of Home Org's Services (e.g. user directory, authentication)
- Outsourcing of resource owner's Services (e.g. AAI enabled portals)

Some final statements



- **Currently, there is no urgent need for the AAI, but...**
- **Some buzzwords: mobility, distributed resources, inter-organizational collaboration, distance learning**
- **Those believing in a growing importance of those buzzwords should be very much interested in the AAI**
- **The unprepared might face hard times...**
- **Watch out for the final AAI-project report in June '02:
<http://www.switch.ch/aai/>**
- **SWITCH is again prepared to co-ordinate and drive the next phase**