SWITCH

The Swiss Education & Research Network

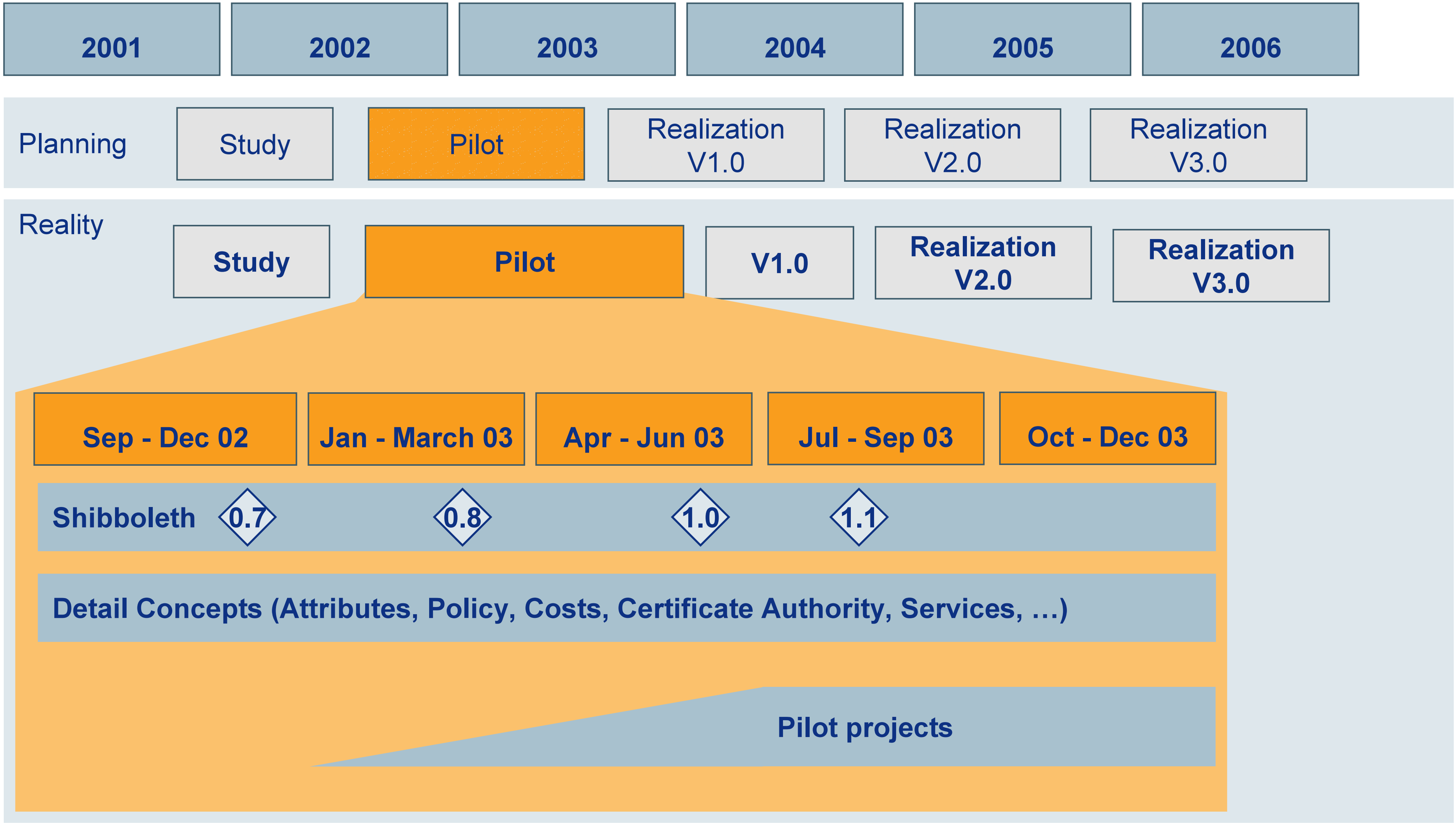
Results of the pilot phase

Christoph Graf, SWITCH
Thomas Leggenhager, SWITCH

December 3, 2003

SWITCH aai

The last 12 Months



2001 | 2002 | 2003 | 2004 | 2005 | 2006

Planning: Study – Pilot – Realization V1.0 – Realization V2.0 – Realization V3.0

Reality: **Study** – **Pilot** – **V1.0** – **Realization V2.0** – **Realization V3.0**

Sep - Dec 02 | **Jan - March 03** | **Apr - Jun 03** | **Jul - Sep 03** | **Oct - Dec 03**

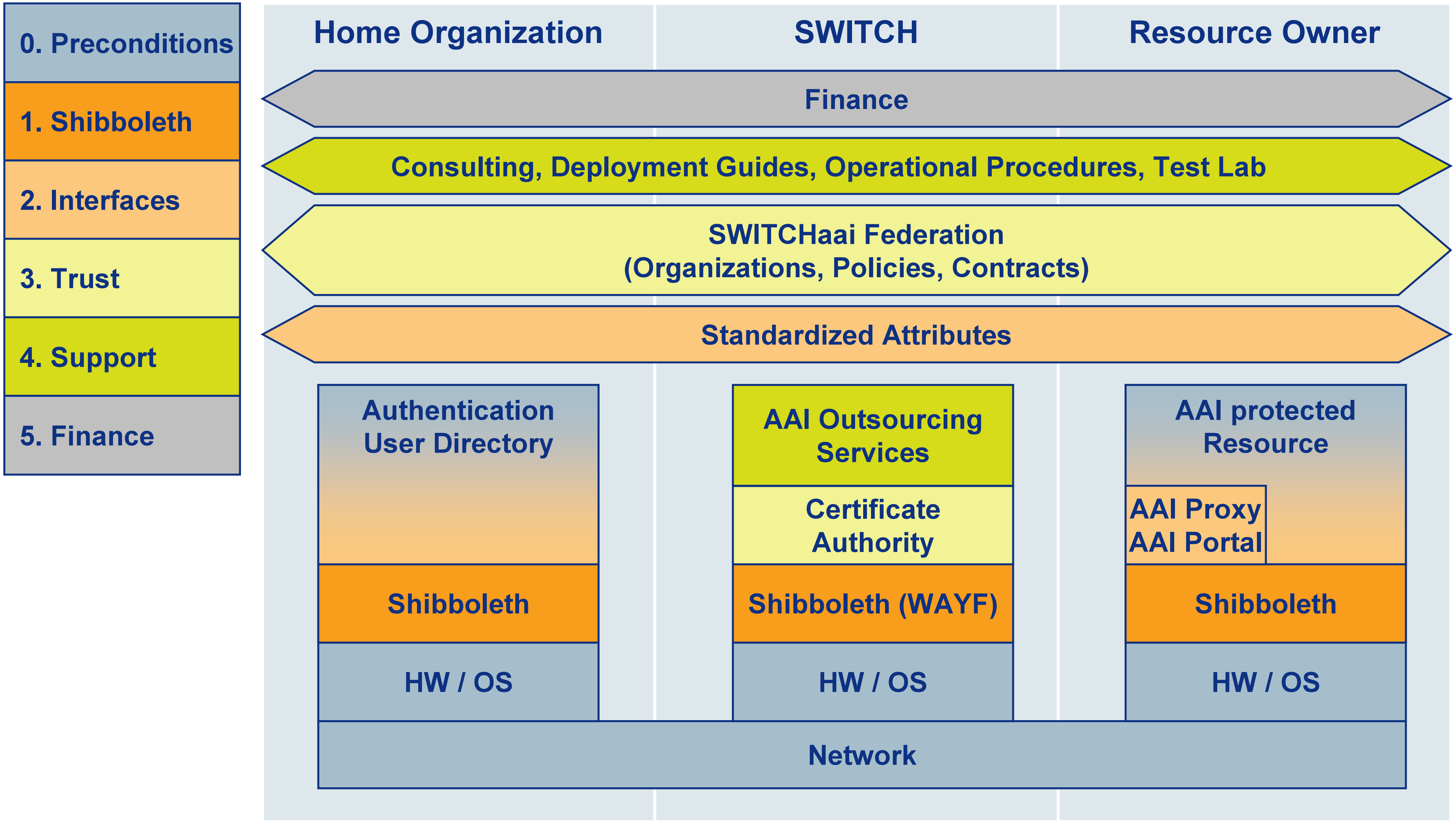
Shibboleth 0.7 – 0.8 – 1.0 – 1.1

Detail Concepts (Attributes, Policy, Costs, Certificate Authority, Services, …)

Pilot projects

AAI Framework

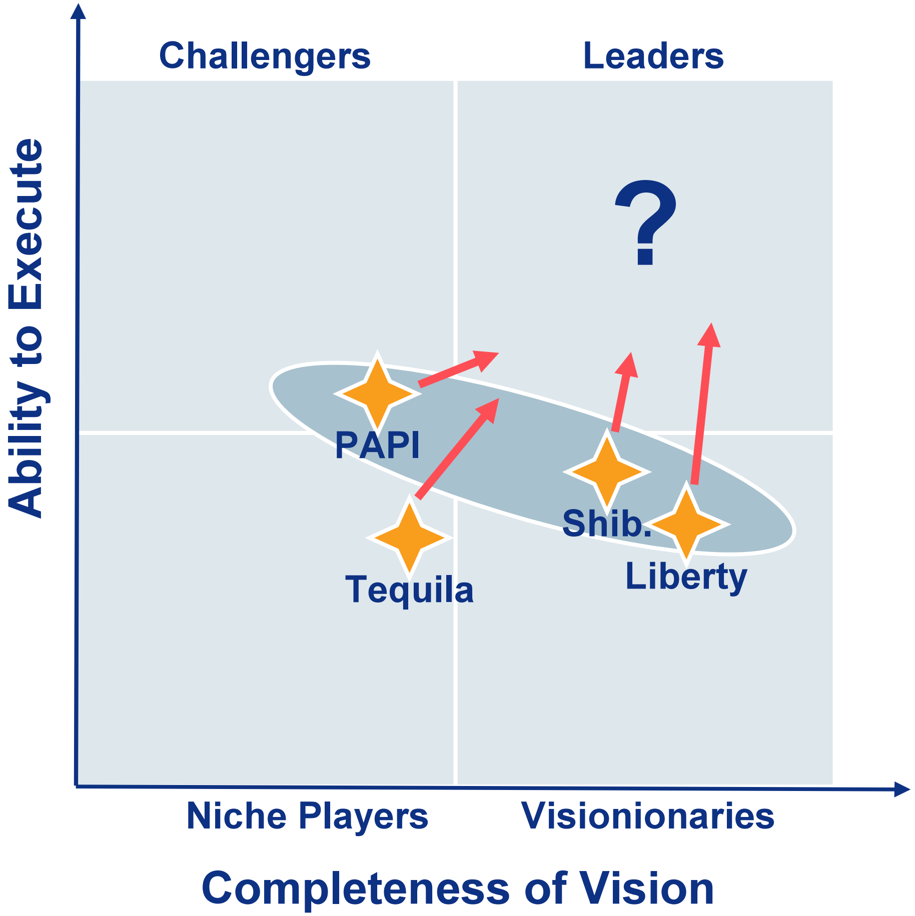
SWITCH
The Swiss Education & Research Network



Shibboleth (1): Architecture Evaluation

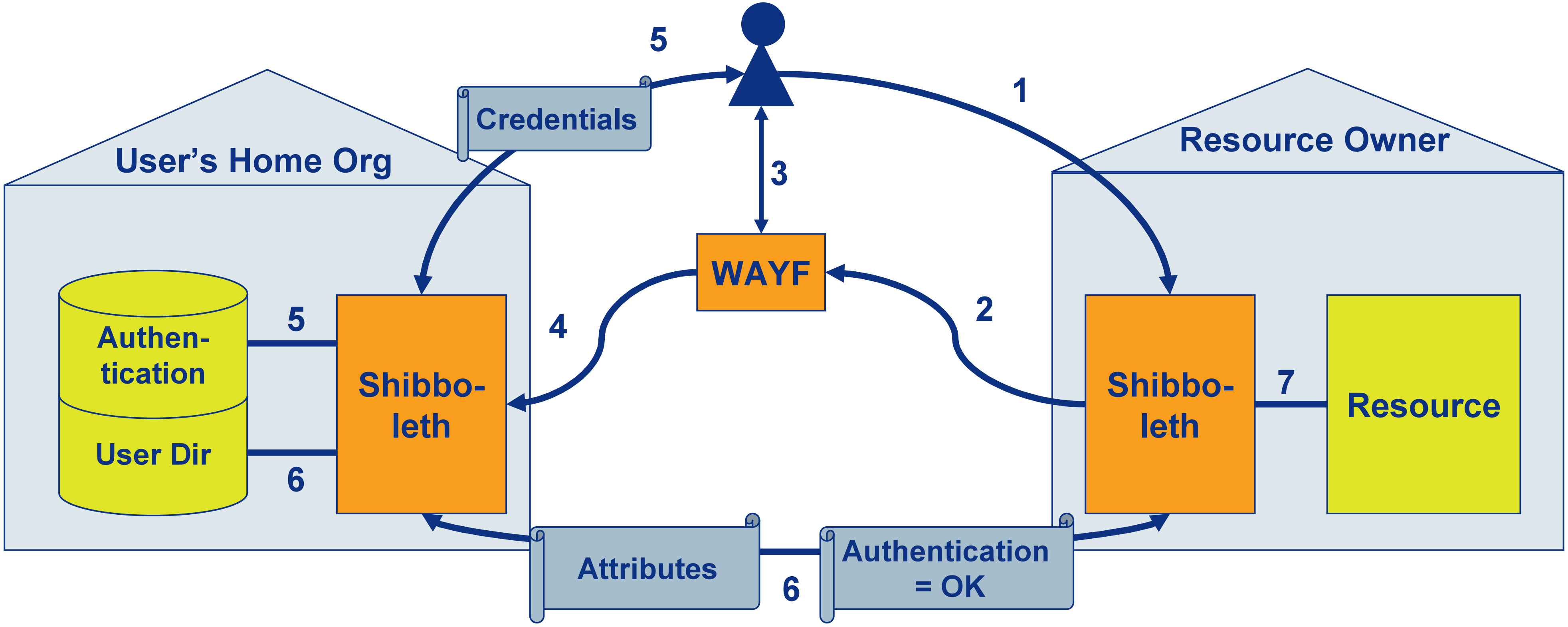
SWITCH
The Swiss Education & Research Network

Status as of January 2003



- No leader in the AAI market
- Selection of Shibboleth because of
  - international reference architecture
  - cooperating with Liberty Alliance, PAPI, Oasis (SAML), content providers, software vendors (WebCT, Blackboard, …)
  - large community

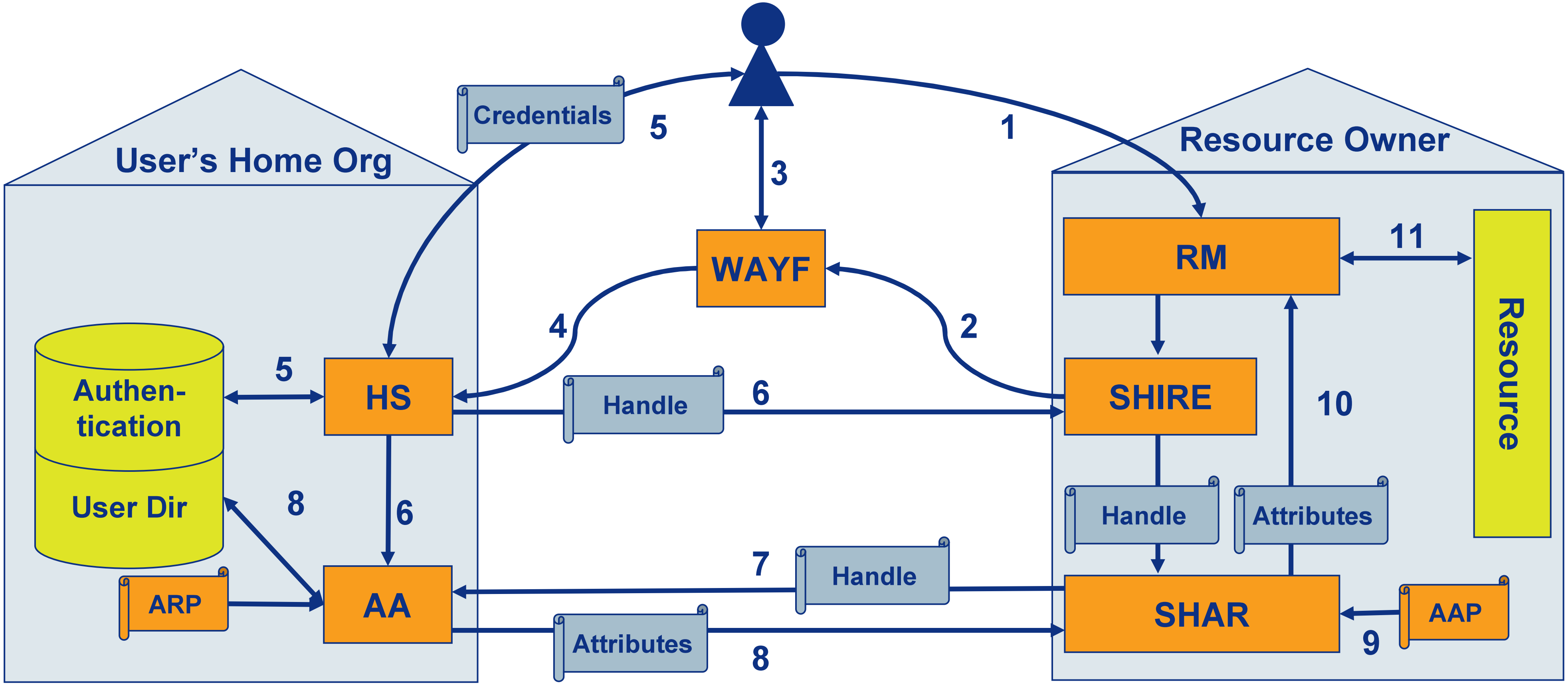
Shibboleth (2): Interactions



🟧	Shibboleth AAI Components
WAYF	'Where Are You From'-Server

Shibboleth (2a): The Details

SWITCH
The Swiss Education & Research Network



HS	Handle Server
AA	Attribute Authority
WAYF	'Where Are You From'-Server
SHIRE	Shibboleth Indexical Reference Establisher
SHAR	Shibboleth Attribute Requestor
RM	Resource Manager

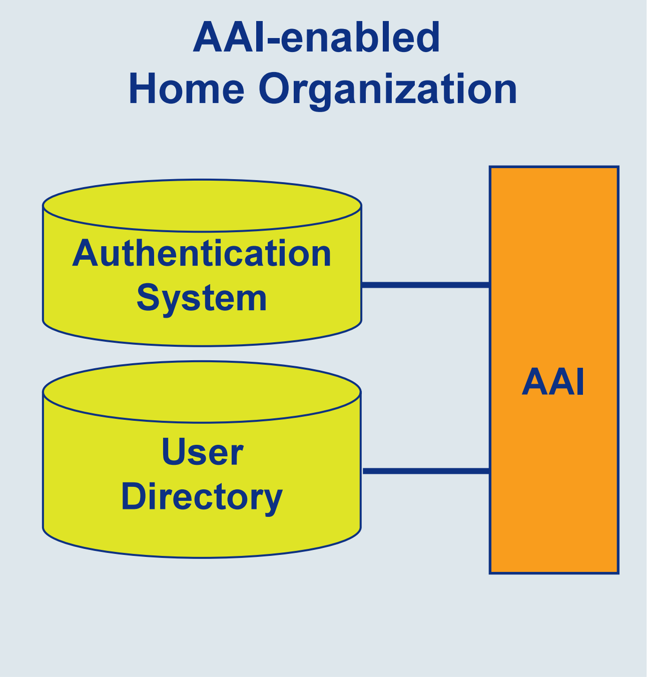
🟧 Shibboleth AAI Components

Shibboleth (3): Status and Future of Shibboleth

SWITCH
The Swiss Education & Research Network

Shibboleth 1.1 (1 August 2003)	• Productive release available for various platforms • Home Organizations (origin): Solaris, Red Hat, Debian (SWITCH) • Resources (target): • Apache on Solaris, Red Hat, Debian (SWITCH), WinNT-Win2003, • IIS 4.0+ on WinNT-Win2003 • Test infrastructure, deployment guides, configuration files
Future of Shibboleth	• Improved platform support, Java API for resource integration • Improved administration tools • Home Orgs: web-based GUI for managing Attribute Release Policy • Resource Owners: tool for managing Access Policy, Support for XACML (eXtensible Access Markup Language) • Support for new use cases • non-browser scenarios, web services • n-tier situations (e.g. portals) • Benefits from cooperation with OASIS (Organization for the Advancement of Structured Information Standards): SAML 2.0 • Support for multiple federations (circles of trust)

Interfaces (1): Home Organization Integration



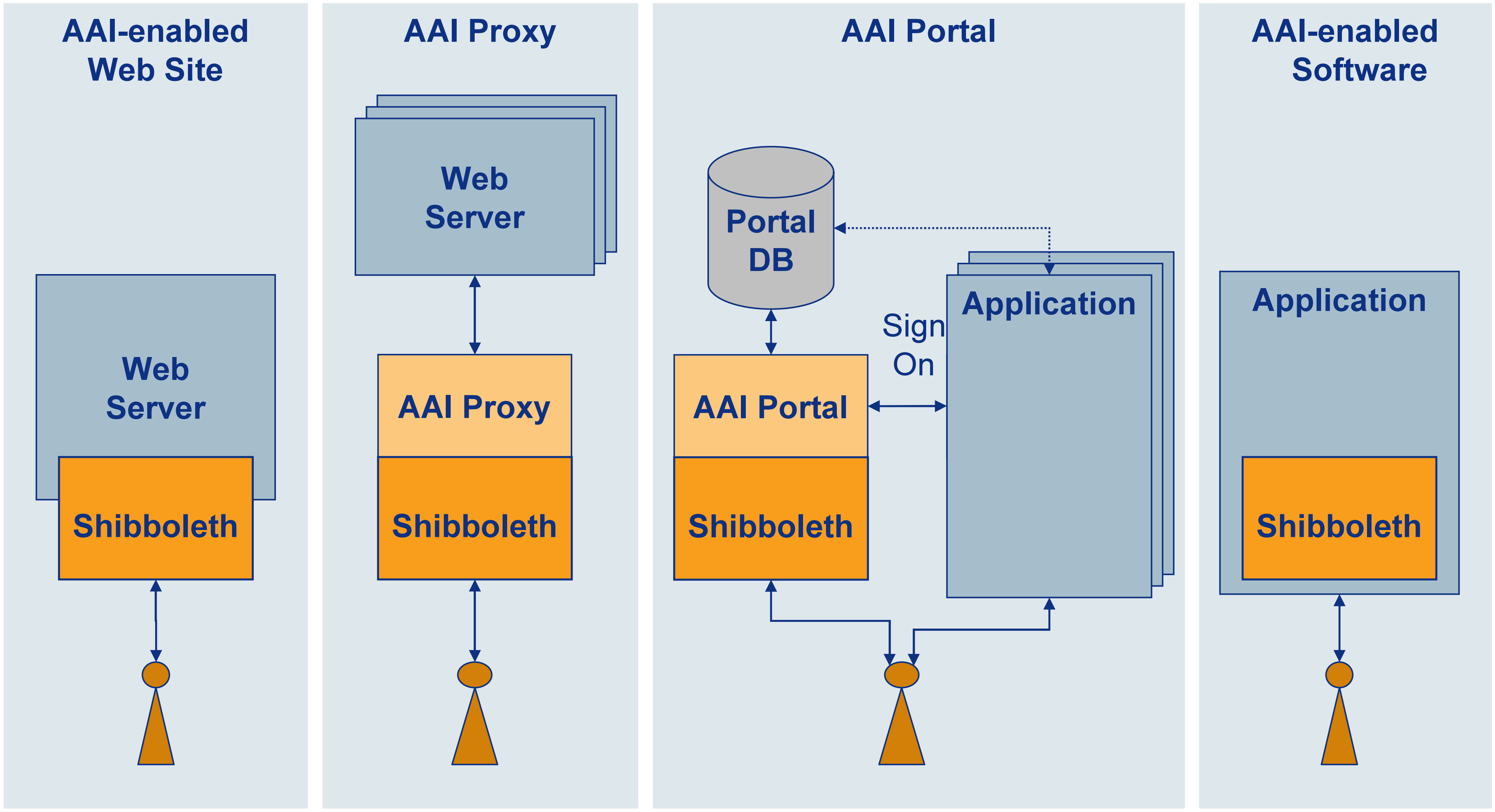
Preconditions for a Home Organization:

- can register its users
- offers secure authentication
- has a coordinated user directory
- can provide minimal set of user attributes to AAI

Interfaces

- Integration with Authentication Systems:
  - any of the authentication methods known by the Apache web server (e.g. LDAP, PAM, RADIUS, TACACS, end-user certificates)
- Integration with User Directory
  - native LDAP support
  - Java API
  - native SQL support (planned)

Interfaces (2): Resource Integration



Interfaces (3): Resource Integration

SWITCH
The Swiss Education & Research Network

	AAI-enabled Web Site	AAI Proxy	AAI Portal	AAI-enabled Software
Description	Standard web servers	Web Proxy, transparent for user	Portal with user mgmt and resource mgmt	Shibboleth-integrated software
	• Microsoft or Apache web server • access rights per group of users • static web pages or dynamic web pages (CGI, PHP, Perl, etc.)	• not-personalized websites which cannot be integrated with AAI (black-boxes)	• personalized web-sites which cannot be integrated within AAI (black-boxes) • personalized web sites which require community management functionality	• Standard applications • Content providers
Examples	• Intranet server with non-public content	• ERL (ETH Library)	• e-learning applications (Vitels, nanoWorld, …)	• e-learning: WebCT Vista, BlackBoard, WebAssign, … • Content Provider: JSTOR, EBSCO, SFX, …

Interfaces (4): Authorization Attributes

Personal attributes

Mandatory

- **Unique Identifier (pseudo)**
- **Surname**
- **Given Name**

Optional

- **Date of birth**
- **Gender**
- **E-mail**
- **Address(es)**
- **Phone number(s)**
- **Preferred language**

Group membership

Mandatory

- **Name of Home Organization**
- **Type of Home Organization**
- **Affiliation (student, staff, faculty, …)**

Optional

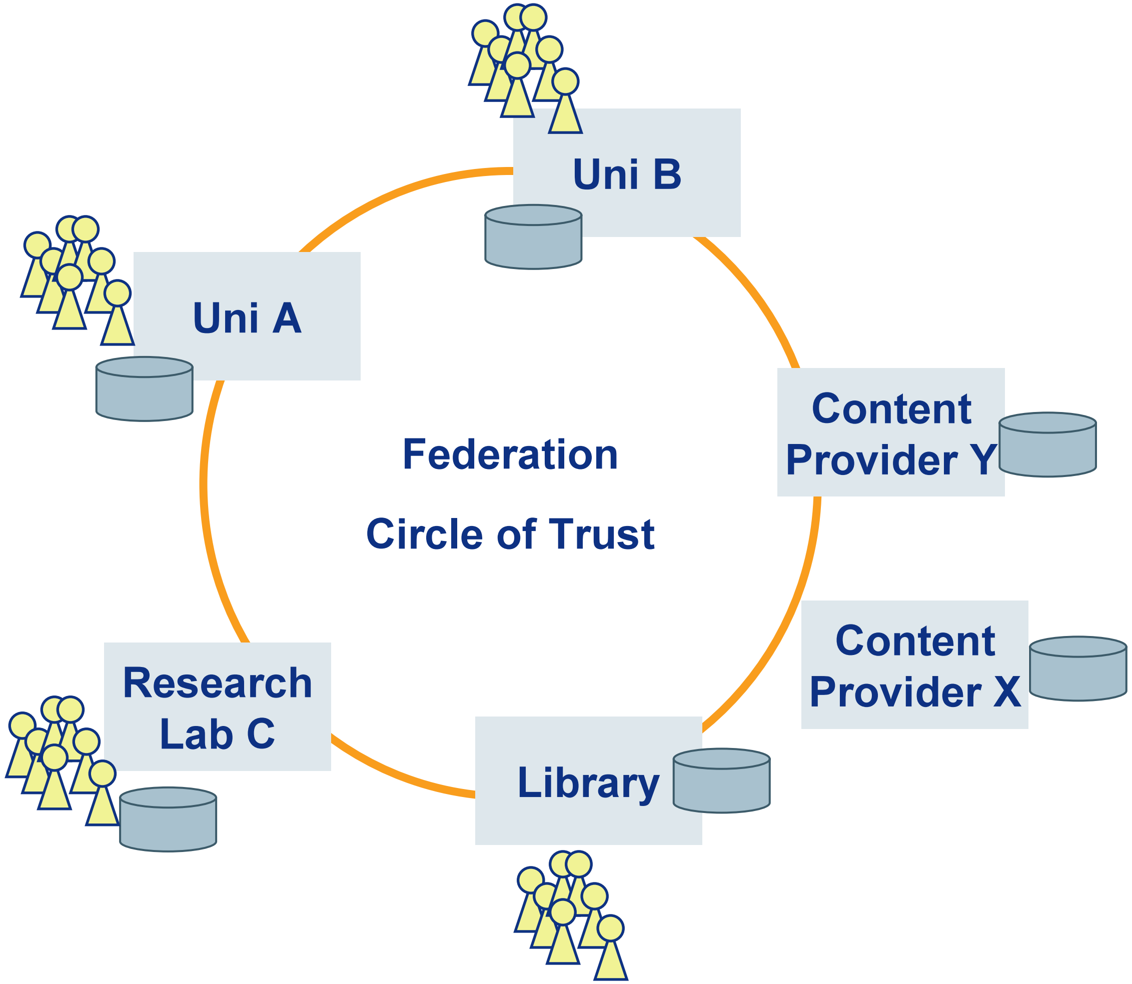
- **Study branch**
- **Study level**
- **Staff category**
- **Organization Path**
- **Organization Unit Path**
- **Group membership**

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 standard-ized change process, depending on the requirements of Resource Owners and Home Organizations

Version 1.0 of the attribute specification has been available since 12 December 2002 and has been implemented by ETH Zurich, Universities of Berne, Lausanne and Zurich

Trust (1): How to Establish Trust?



Who?

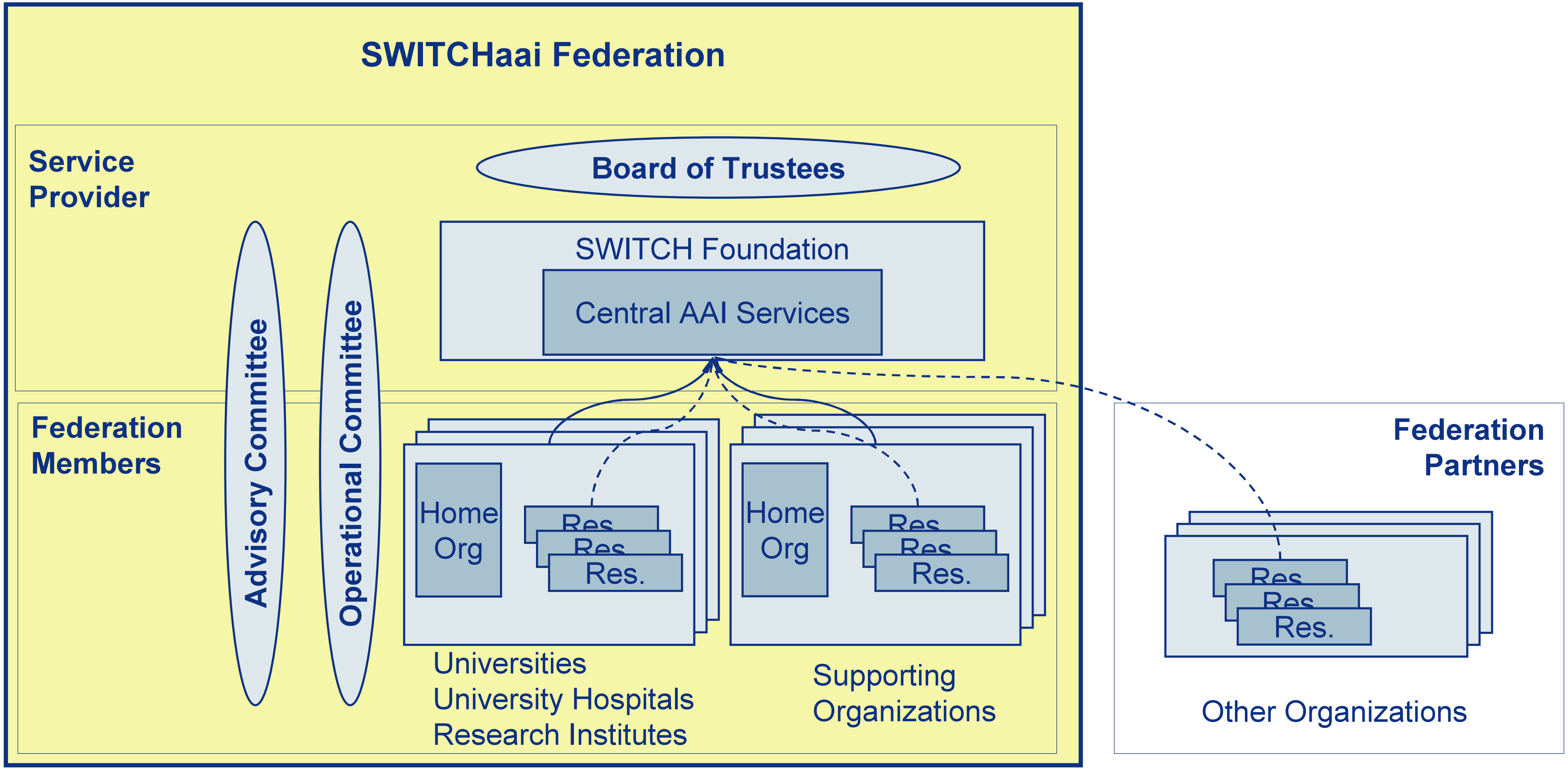
- Between end-users and organizations
- Between organizations

How?

- Known group of participants
- Common set of Policies and Procedures
- Contracts
- Technology
- Transparency
- Traceability

Trust (2): SWITCHaai Federation

SWITCH
The Swiss Education & Research Network



——> **Service subscription**

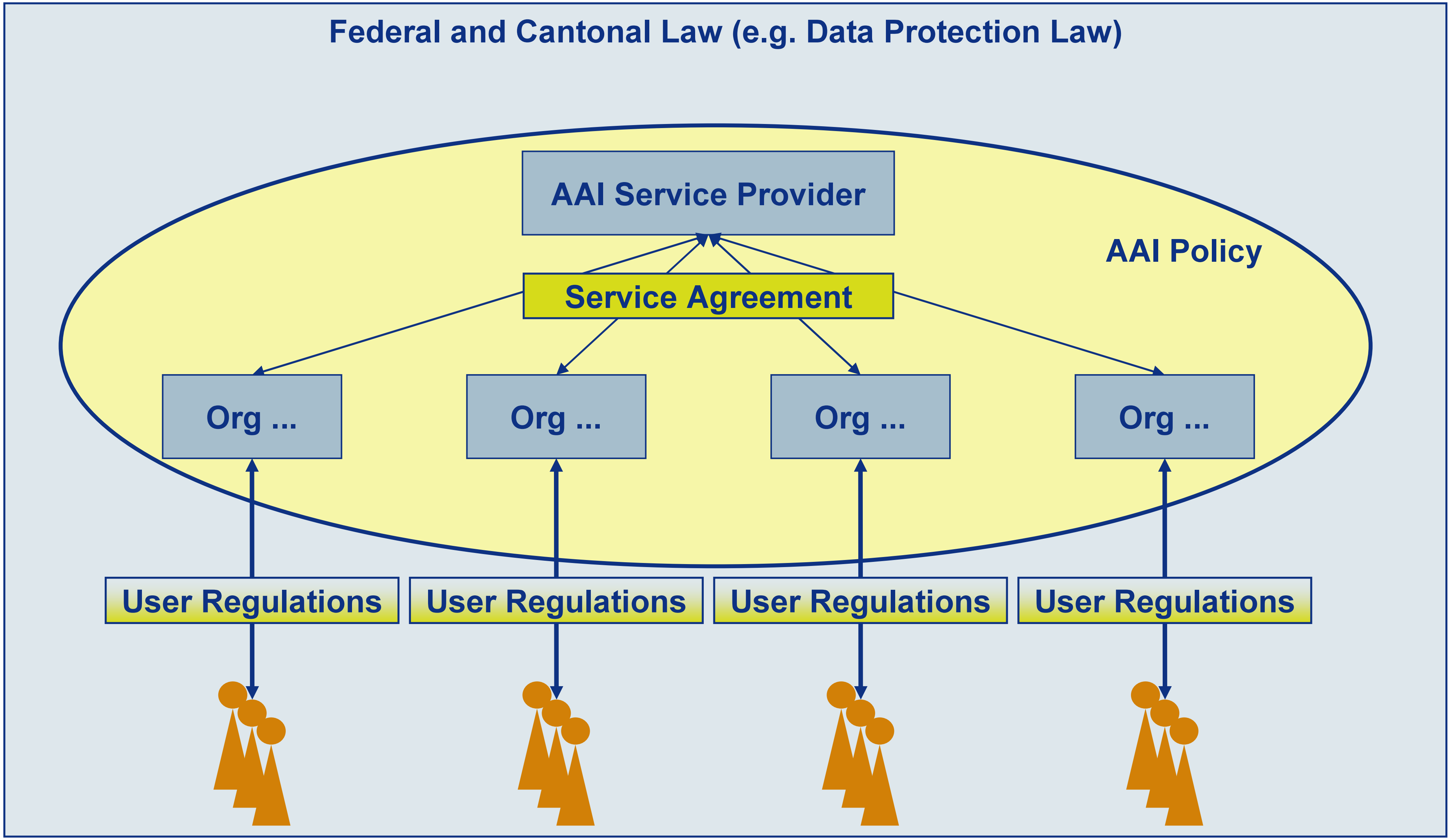
- - - - -> **Resource registration**

Trust (3): SWITCHaai Federation

SWITCHaai Federation	• Group of organizations that agree to cooperate in the area of inter-organizational authentication and authorization • Operate a Shibboleth-based AAI • Agree to abide by a common set of policies and practices
Federation Members	• Universities, universities of applied sciences, public research institutes, teaching hospitals and "Supporting Organizations“ (e.g. libaries) • Act as Home Organization and/or Resource Owner
Federation Partners	• Organizations offering AAI-enabled Resources to federation members • Cannot act as Home Organization (i.e. do not represent user community)
Service Provider SWITCH	• Provides the central AAI Services
Advisory Committee	• Committee representing the Federation members and SWITCH • Acting in an advisory capacity as regards the management of inter-institutional AAI projects and the long-term AAI strategy (architecture, functionality, federation membership, policies and business rules)
Operational Committee	• Committee representing the Federation members and SWITCH • Responsible for short-term decisions and operational or technical issues (attributes, release planning, security audits, best practices)

Trust (4): The Legal Basis of the AAI

SWITCH
The Swiss Education & Research Network



Federal and Cantonal Law (e.g. Data Protection Law)

AAI Service Provider

AAI Policy

Service Agreement

Org ...

Org ...

Org ...

Org ...

User Regulations

User Regulations

User Regulations

User Regulations

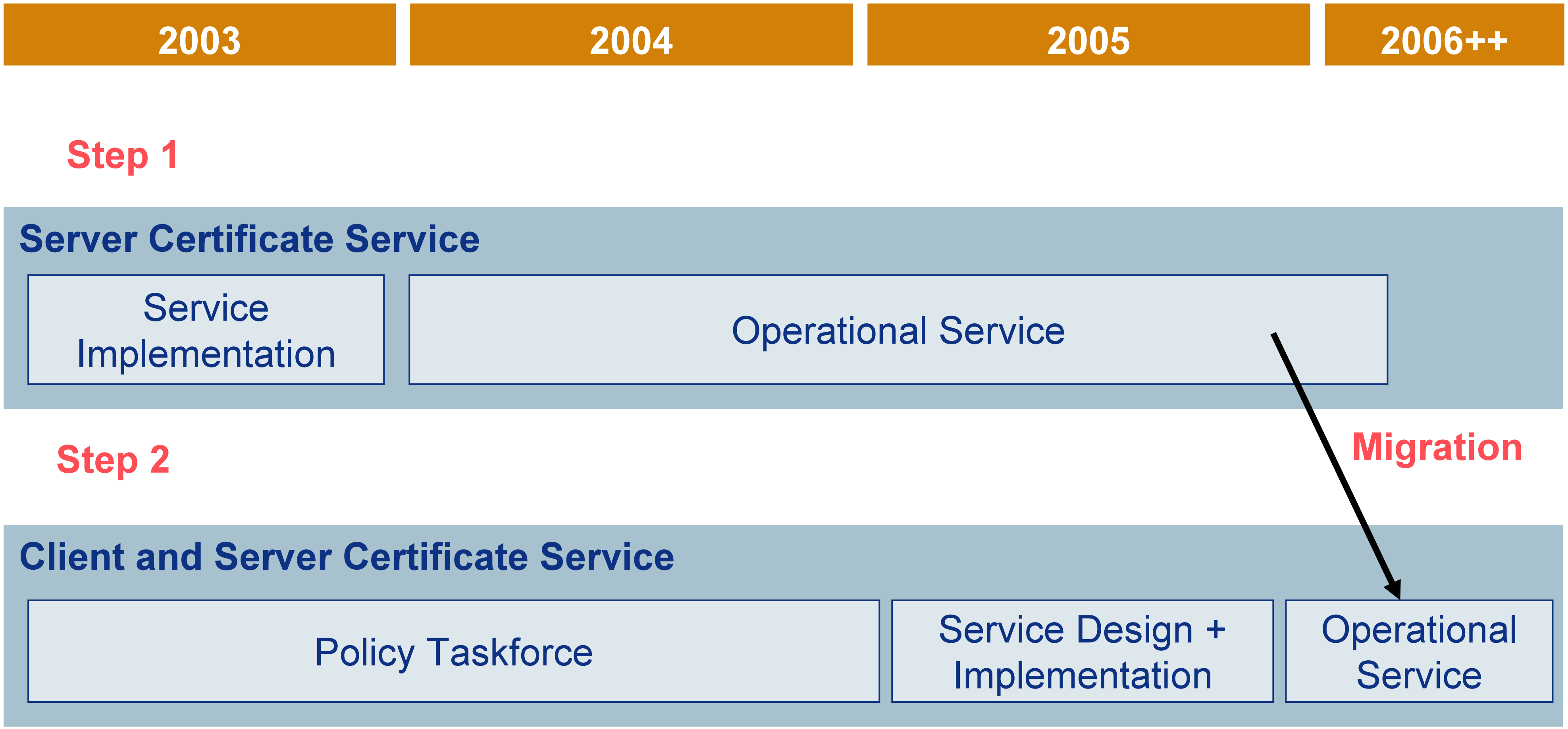
Legal Framework

Service Agreement between SWITCH and Organisation including:

- Service Description (existing document)
- Authorizations Attribute Specs (existing document)
- Policy Document (relevant for the relationship between the Organisations) (existing document)
- Software Licenses (Curl etc.) (existing document)
- Sample Data Protection Clause (existing wording)

Status: Draft version 0.1 (not yet reviewed by SWITCH)

CA Roadmap



2003 | 2004 | 2005 | 2006++

Step 1

Server Certificate Service

Service Implementation

Operational Service

Migration

Step 2

Client and Server Certificate Service

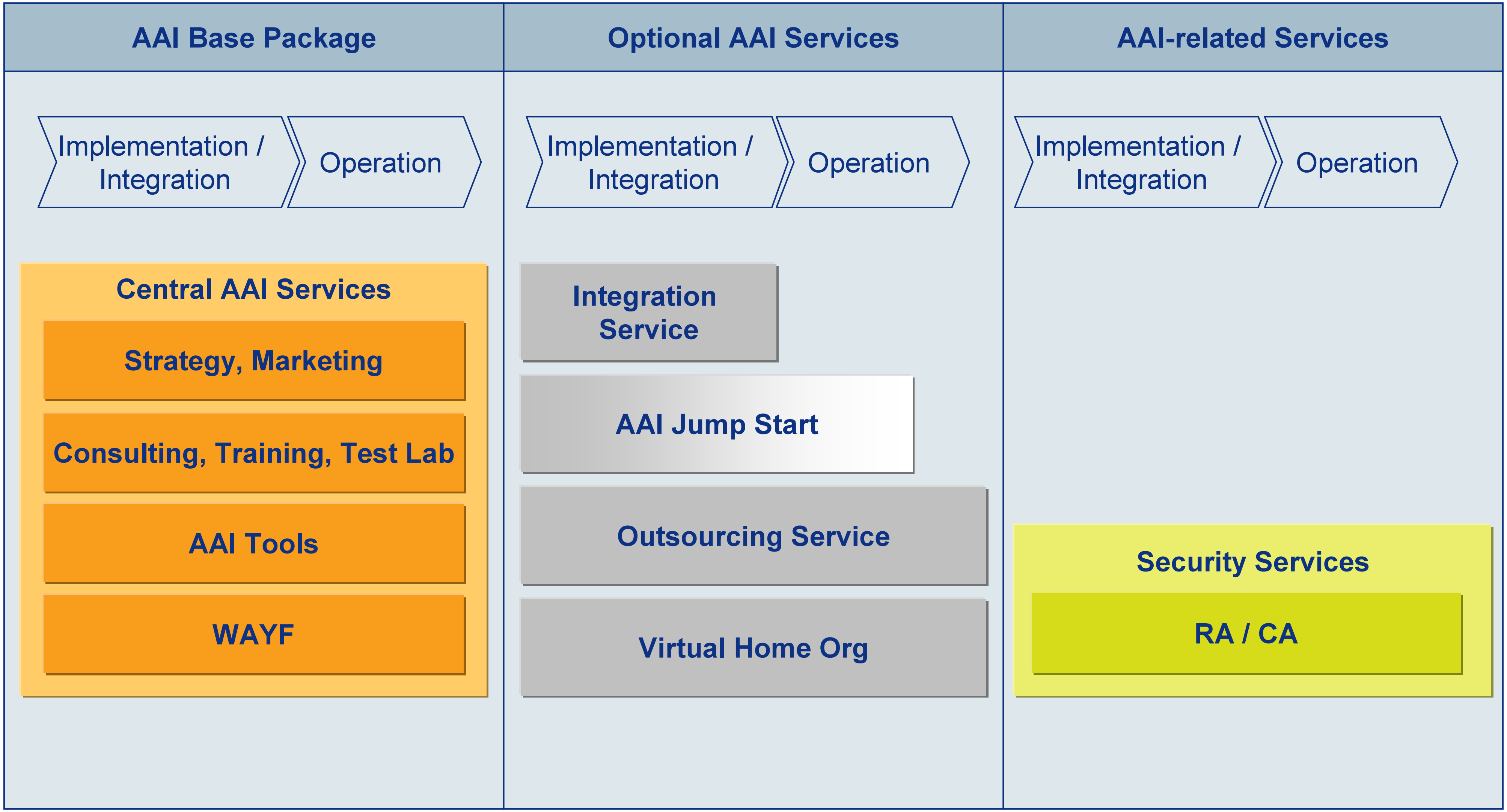
Policy Taskforce

Service Design + Implementation

Operational Service

Support (1) SWITCH's AAI Services

SWITCH
The Swiss Education & Research Network



AAI Base Package

Implementation / Integration → Operation

Central AAI Services

- Strategy, Marketing
- Consulting, Training, Test Lab
- AAI Tools
- WAYF

Optional AAI Services

Implementation / Integration → Operation

- Integration Service
- AAI Jump Start
- Outsourcing Service
- Virtual Home Org

AAI-related Services

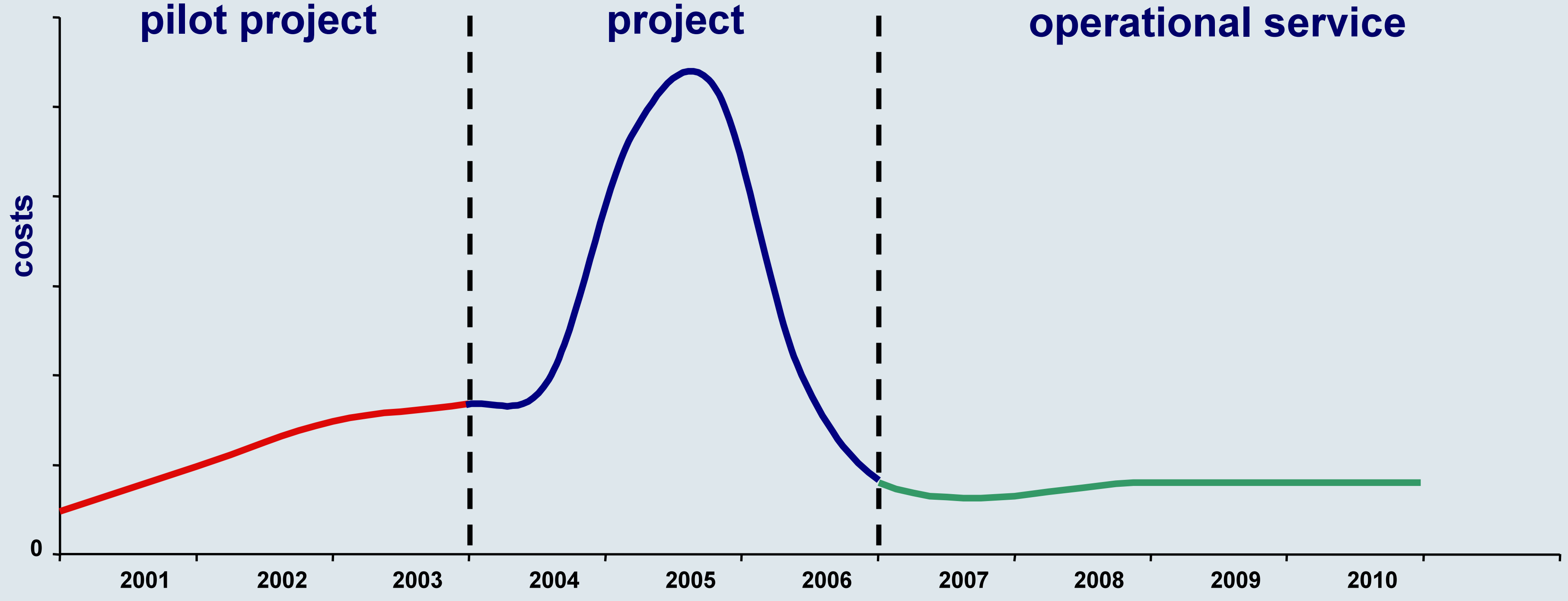
Implementation / Integration → Operation

Security Services

- RA / CA

Finance (1): Life Cycle of Services

Service innovation: from a project to a service



funded by SWITCH and participants

funded by subsidies and participants

funded by tariffs

Finance (2): Cost Estimation

Task Force “Finance”

- **Cost estimation model for Home Organizations and Resource Owners**
- **Cost estimation for typical tasks**

SWITCH

- **Has applied for subsidies for the implementation phase 2004-2006**

		Initial Cost				Recurring Cost			
		Purchase kFr.	Work kFr.	Total kFr.	Per User Fr.	Purchase kFr.	Work kFr.	Total kFr,	Per User Fr.
HomeOrg	from	15	50	**65**	**3**	5	10	**15**	**1**
	to	25	100	**125**	**8**	10	40	**50**	**3**
Resource	simple	--	25	**25**		--	5	5	
	complex	15	50	**65**		5	20	**25**	