RedIRIS

Building and (inter)operating AA services. A tour into reality

TERENA Mini Symposium on AA

Prague, 24 October 2002

Outline

- An introduction to AA technologies
- A reference model: Shibboleth
- A practical implementation: PAPI
- A review of enabling technologies
- An harmonization effort: TF-AACE

Current interrealm access control

- Ad hoc, non-scalable, difficult to maintain, and restrictive approaches:
  - Single ID and shared passwords are distributed
  - Content providers limit access by IP address
  - Proxy services or VPNs
  - Load user identities into vendor databases
- And PKIs are not a solution per-se
  - Identity, not rights
  - Although PKI is a base technology

Privacy preservation

- Privacy can only degrade as information about a certain user flows
  - Personal data has to be confined to the realm where it is strictly required
- Passive vs. active privacy:
  - Passive: Users pass identity to the target
    - Rely on target's privacy policy
    - Targets have significant regulatory requirements
  - Active: Users release the attributes to the target that are appropriate and necessary
    - The user can decide which attrinbutes and to which target are released

Federated administration

- Information providers need to keep control on resources and use their own accounting procedures:
  - Enforcing provider access policies
  - Accounting information
  - Extracting usage patterns
- Source organizations already operate authentication services
- Federated administration permits their coexistence
  - And requires trust management

Application scenarios

- Mobility has to be guaranteed
  - A user should be able to access any resource (s)he has right to anytime anywhere
  - Not only hardware mobility
- Transparency to the user
  - Seamless integration with existing usage paradigms
  - Do noot require extra technologies at the user side
- Web oriented, although extensible to other access technologies
  - Grids, multimedia contents and interactions,...

The Shibboleth model

- A MACE/Internet2 initiative
- Shift from passive towards active privacy
  - Develop an architecture, policy framework, and practical technologies to support inter-institutional sharing of resources
    - Based on the federated administration principles
  - Propose and validate standard formats for:
    - Secure exchange of interoperable attributes which can be used in access control decisions
    - Controlled dissemination of attribute information, based on administrative defaults and user preferences
- A model plus a reference implementation

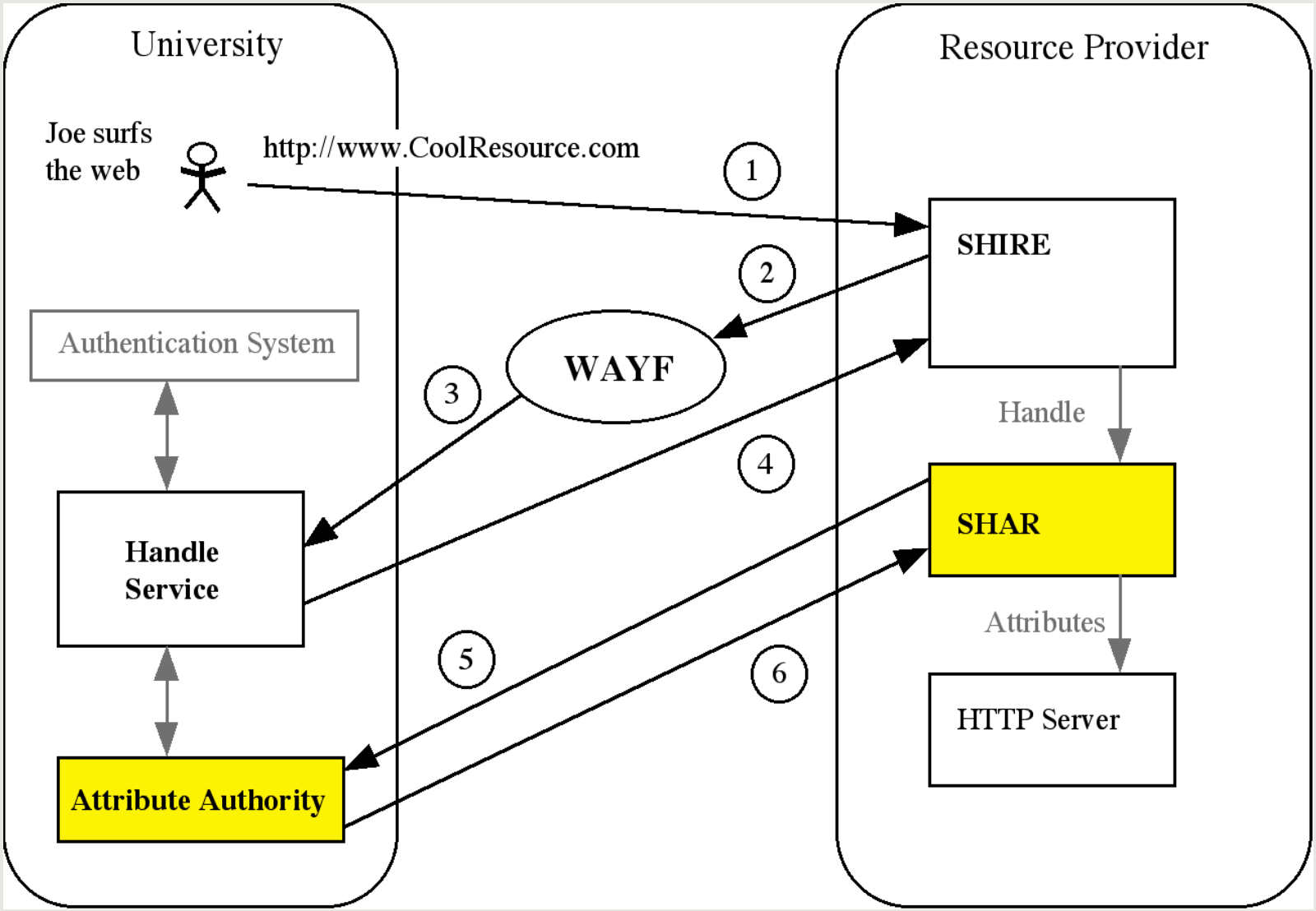
Shibboleth components

- Target site
  - The SHIRE determines the initial context, and redirects the user to their AuthN point, if needed
  - The WAYF locates the appropriate AuthN point for the user
  - The SHAR requires the user attributes as specified by the AuthZ policies
  - The RM performs actual resource access control once the AuthZ decision has been made

Shibboleth components

- Origin site
  - The HS generates a (anonymized) handle to be used by the target SHAR for attribute requests
    - Associates this handle to the user
    - Actual AuthN procedures are left to the site
  - The AA receives attribute queries from the target SHAR
    - Evaluates these queries in terms of its ARP (Attribute Release Policies)
- All the interactions use the SAML language

Shibboleth: AuthZ decision



What is PAPI

- PAPI is a distributed access control system for Internet information resources
  - Usable for intra- an interrealm scenarios
  - Based on the federated administration and active privacy principles
  - Based on standard HTTP procedures and public key cryptography
- Is the only system able to support federated AA currently in operation

PAPI and the Shibboleth model

- The current version simplifies some parts of the Shibboleth model
  - The SHIRE is simplified to an error document in the Web server
  - The HS and AA are combined within the Authentication Server
  - Assertions are pre-defined and sent along with the user handle
    - Proprietary (non-SAML) format
- Fully Shibboleth support is on its way
  - PAPI 2.0, planned for the end this year

The components of PAPI

- The Authentication Server (AS)
  - Provides users with a (local) single authentication point
- The Point of Access (PoA)
  - Performs actual access control by means of temporary cryptographic tokens, encoded as HTTP cookies
- The Group-wide Point of Access (GPoA)
  - Combines a group of PoAs with similar access policies
  - Intended to simplify AS-PoA interactions

The Authentication Server

- Verifies user identity and rights
  - Each of these verifications is independently performed
  - Directories play a key role in rights management
- Builds a set of digitally signed assertions about the user
  - According to privacy preservation rules
- Sends the assertions to the appropriate (G)PoAs
  - By means of references to objects embedded in HTML

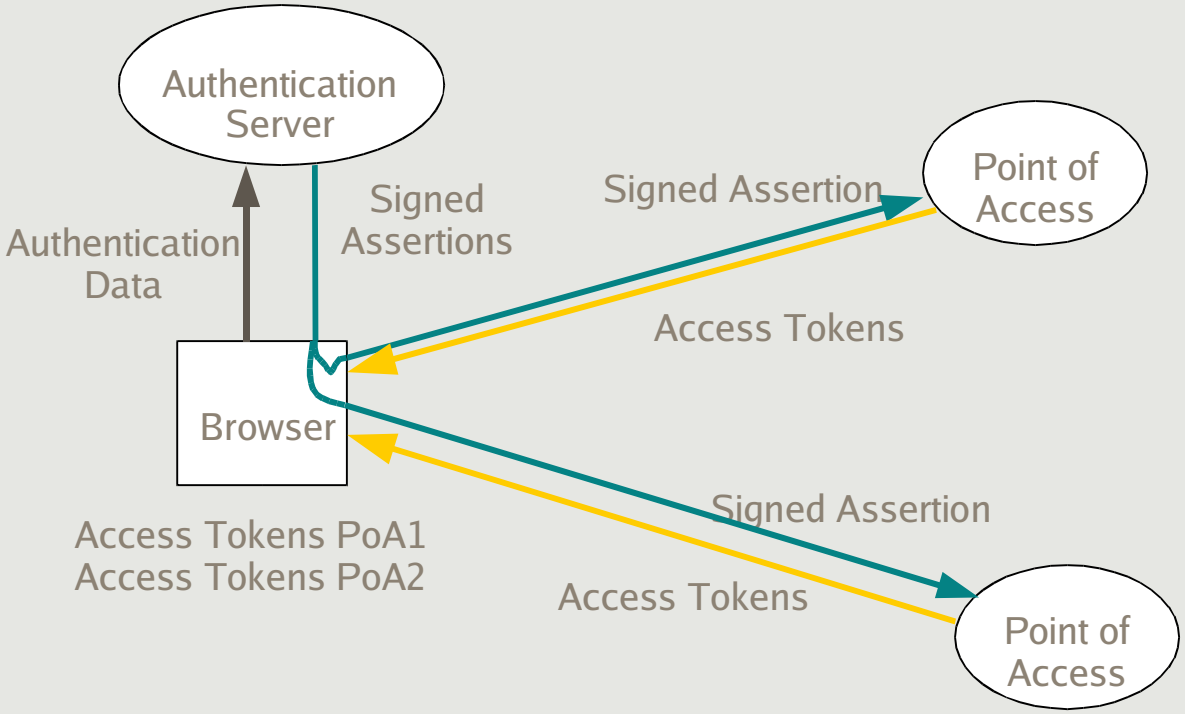
The Point of Access

- Evaluates assertions received from the AS
  - Verifying the signature and matching against any defined filter
  - If the assertion is acceptable, produces a initial couple of access tokens
- If the request comes with access tokens, evaluates them
  - Access is granted only to requests carrying valid tokens
  - Two classes of tokens (long- and short-lived) to avoid unauthorized access by cookie copying
- The PoA is able to work as a proxy to access a plain Web server

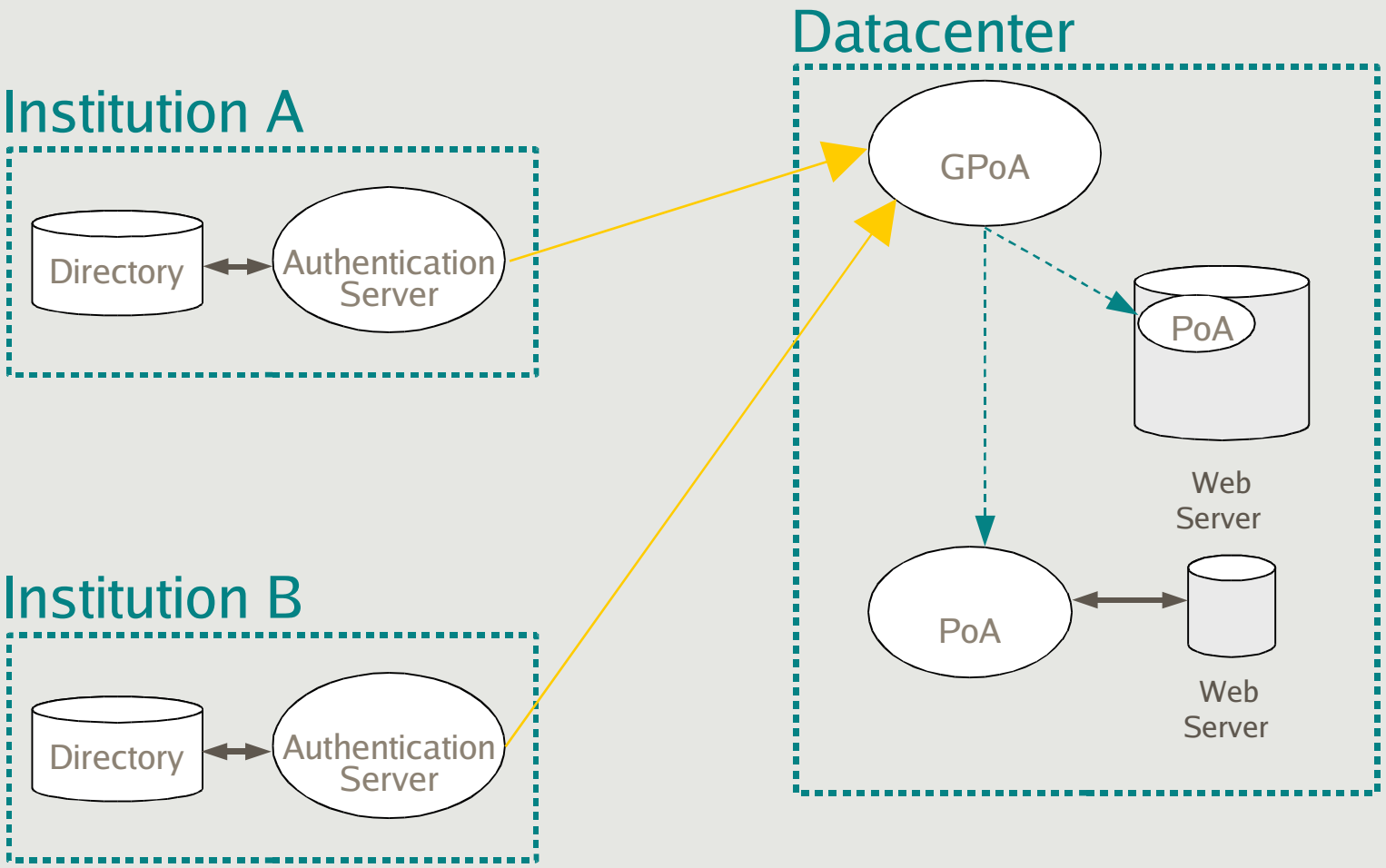
The Group-wide Point of Access

- A PoA that receives a request without access tokens can redirect it to a GPoA
- The GPoA analyzes these requests
  - If valid, the PoA receives a signed assertion from its GPoA
  - The PoA process it as coming from any other AS
  - The hierarchy may be indefinitely extended
- Trust management is simplified
  - An AS needs only to know about the GPoA
  - PoAs may be added under a GPoA without configuring them for valid ASes

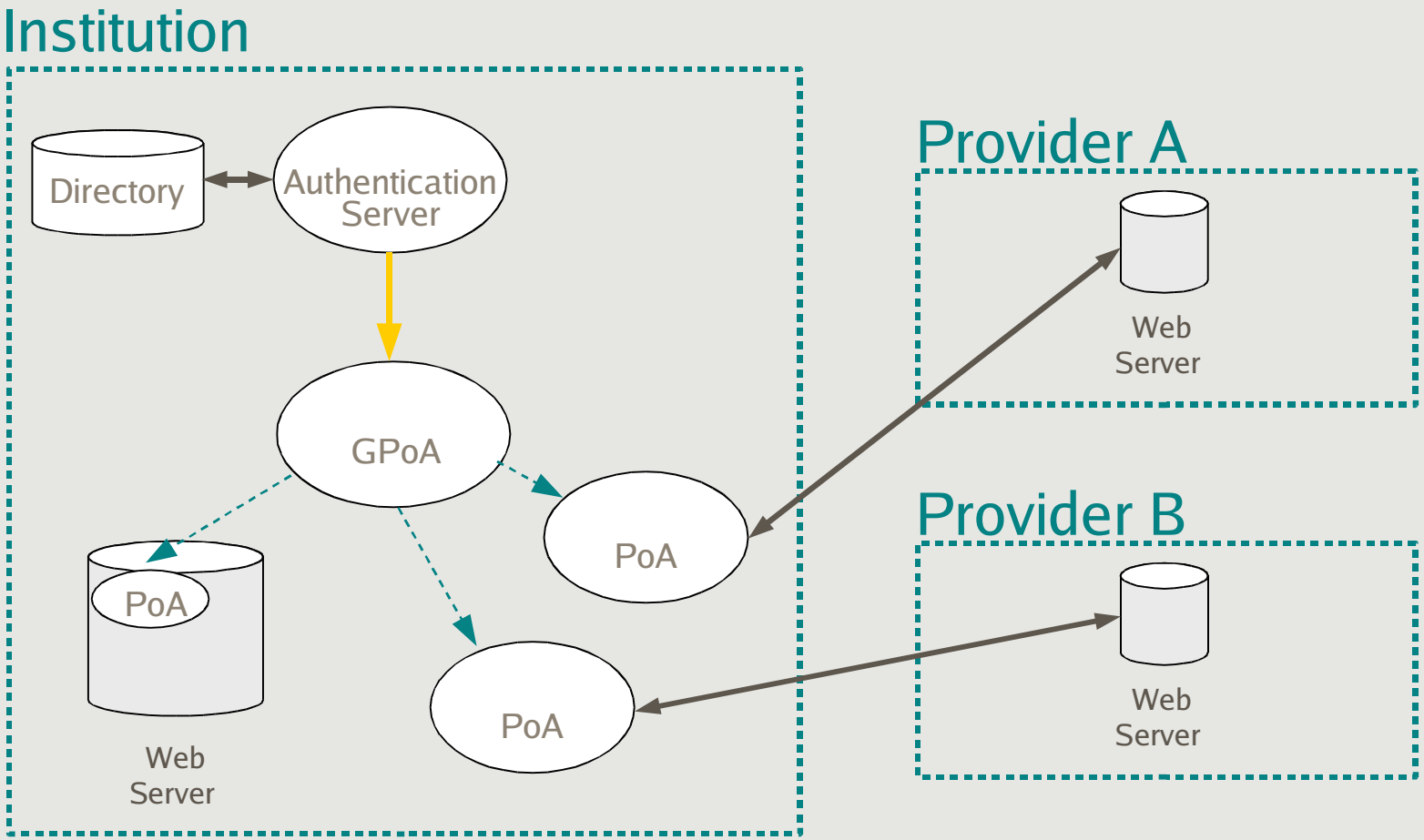
The PAPI base protocol



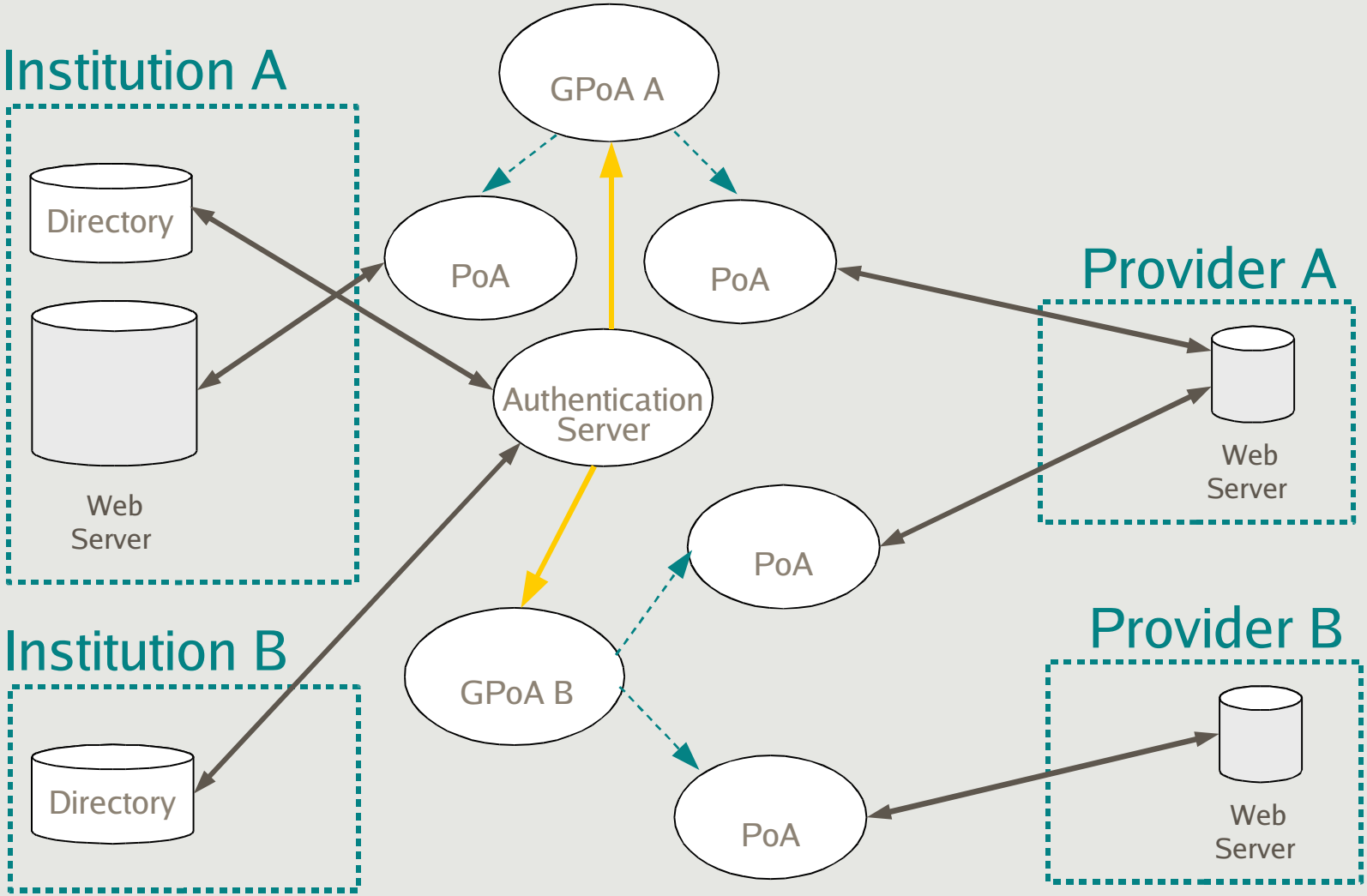
Application scenarios
Datacenter



Application scenarios
Access to local and remote services



Application scenarios
Centralized service



Enabling technologies - PKI

- Not only required for user authentication
  - Actually, this may be the more marginal use
- Trust must be established among agents in federated administration
  - Proposed formats vary from direct TLS use to XML Signature
  - All of them rely on public key cryptography
- Without a Public Key Infrastructure none of these proposal will scale
  - Revocations and different trust anchors are key issues

Enabling technologies - Directories

- Required at the origin sites
  - User authentication
  - User rights evaluation
  - Attribute release policies
- Required at the target sites
  - Centralized policies
- Required for interconnecting both sides
  - Indexes as enhanced WAYF services
  - Key repositories
- Common syntax and semantics
  - eduPerson (Internet2)
  - DEEP proposal (TERENA)

Enabling technologies - AuthZ engines

- Independent components, able to perform a decision according to user attributes and defined policy
- Not only required at target sites
  - Source sites must decide on attribute release
- Current development:
  - S-expressions
    - SPOCP, University of Umea
  - Attribute certificates
    - PERMIS, The PERMIS Consortium, University of Salford

Enabling technologies - Web Services

- They seem the most natural way of interaction for components of an AAI
  - Instead of current practices like URL piggybacking and HTTP redirects
  - Ability to freely combine different components
    - Better interoperability
    - Cleaner interfaces
- WS may also benefit from the use of AAI
  - Industry has realized this
    - The IBM/Microsoft roadmap to WS security
  - WS also become an *enabled service*

TF-AACE: Objectives

- To provide a forum for exchanging experience and knowledge in the areas of AA technologies
- To encourage the deployment of interoperable (inter-institutional) AA infrastructures and services in the TERENA community
- To coordinate the TERENA community contribution to standardization processes in this area

TF-AACE: Infrastructure interoperability

- Many European AAI initiatives
  - UK, Spain, Netherlands, Switzerland, Nordic countries, Germany, ...
- The goal is to ensure that these AAIs:
  - Can interoperate
  - Constitute a reference for commercial information providers
- Define the components and protocols to guarantee a harmonized operation of AAIs
- Establish a reference implementation
  - Validate the harmonized design
  - Provide a means for evaluating interoperability

TF-AACE: Coordination

- Other Task Forces
  - TF-LSD - Directories
  - TF-NGN - Network applications
  - Mobilty
  - Videoconferencing, streaming
- Internet2: Shibboleth and VidMid
- Grid communities
- Industry initiatives
  - MS Passport
  - Liberty Alliance
  - WebServices security initiatives