Red IRIS

Ubiquitous Internet Access Control: The PAPI System

Trustbus02 – Aix-en-Provence, September 2002

Outline

- Requirements on AA (Authentication and Authorization) technologies
- The PAPI components
- The PAPI protocol
- Application scenarios
- Current status and ongoing work

Requirements on AA technologies

- Preserve user privacy
- Do not interfere with provider rights and accounting procedures
- Do not impose management burdens either to providers or consumers
- Fully permit user mobility
- Transparency to the user
- Compatibility with other access control systems
- Web based, although extensible to other access technologies

What is PAPI

- PAPI enables distributed access control to information resources accross the Internet
  - Authentication is locally performed at the organization the user belongs to
  - Authorization is fully controlled by the provider
- Based on standard HTTP procedures and public key cryptography
  - Does not require specific hardware or software

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

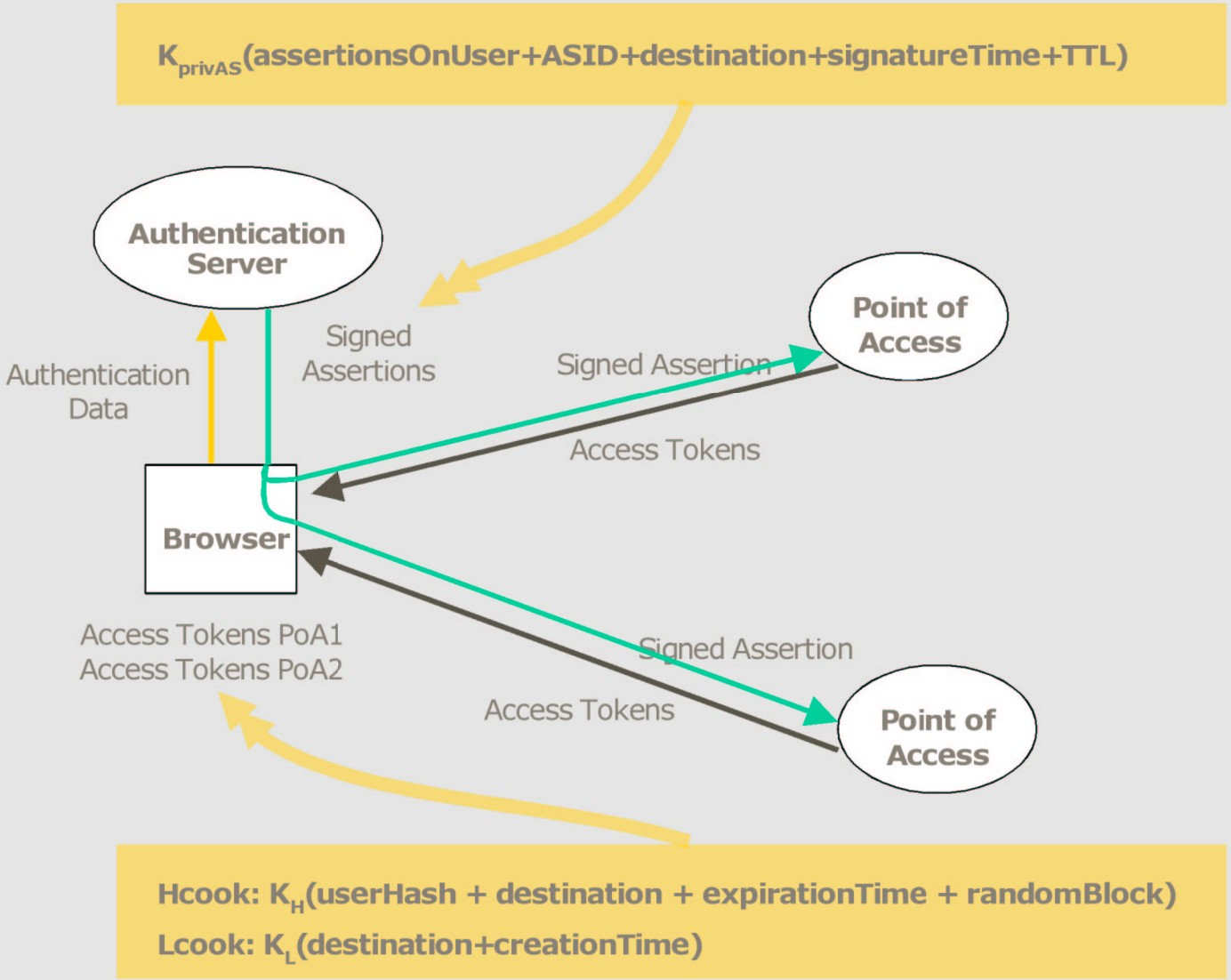
The Point of Access

- 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

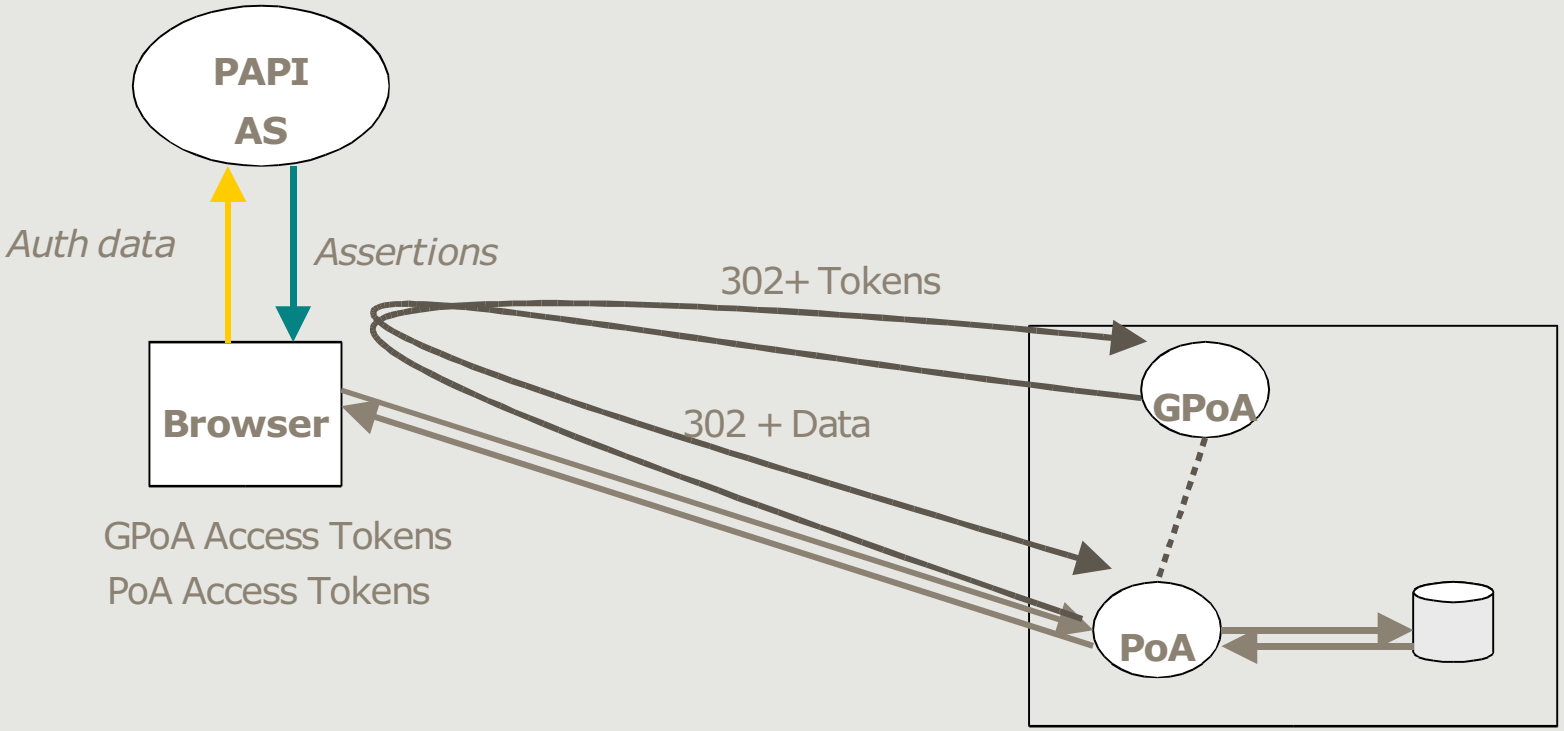
The Group-wide Point of Access

- 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

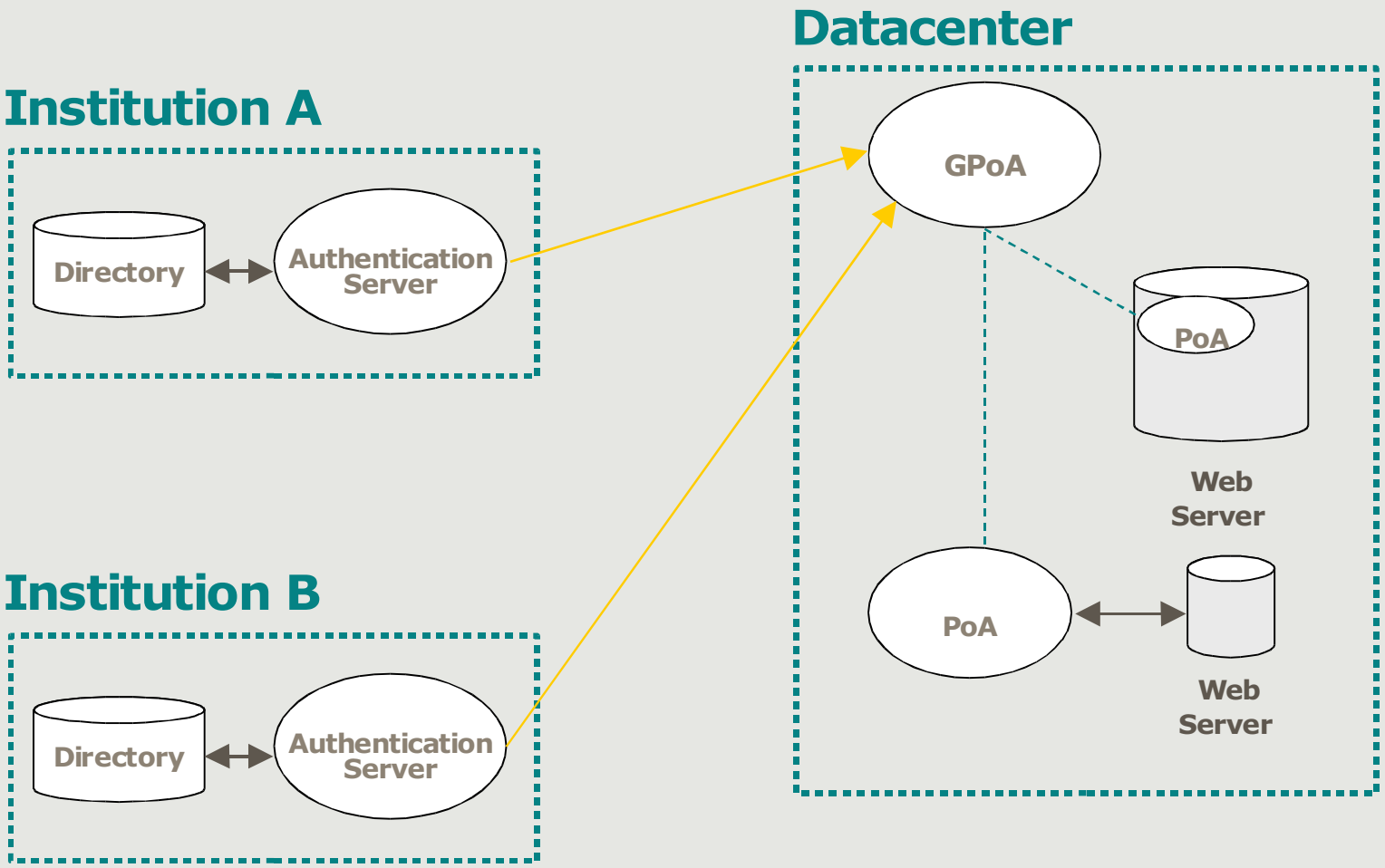
The PAPI base protocol



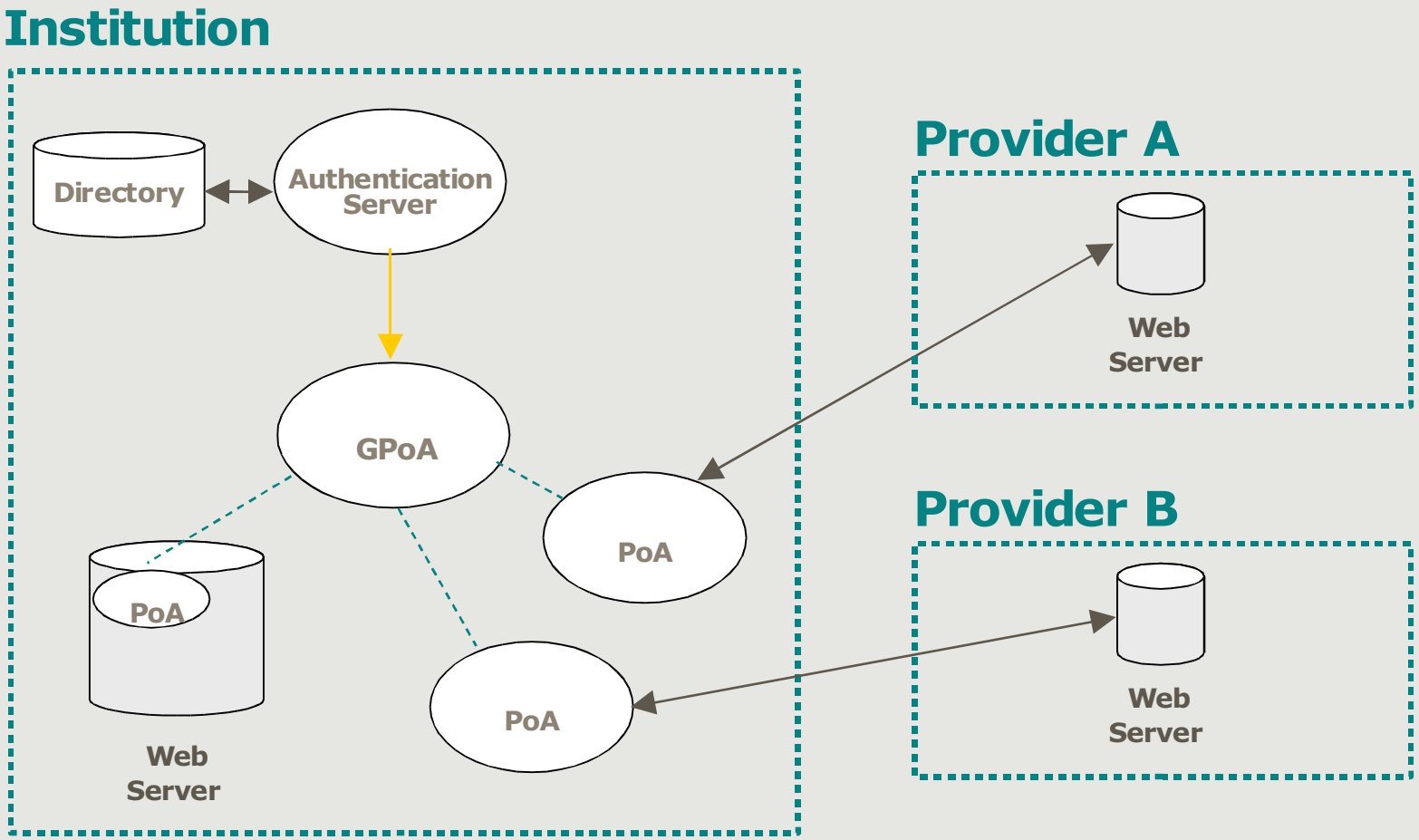
The GPoA protocol



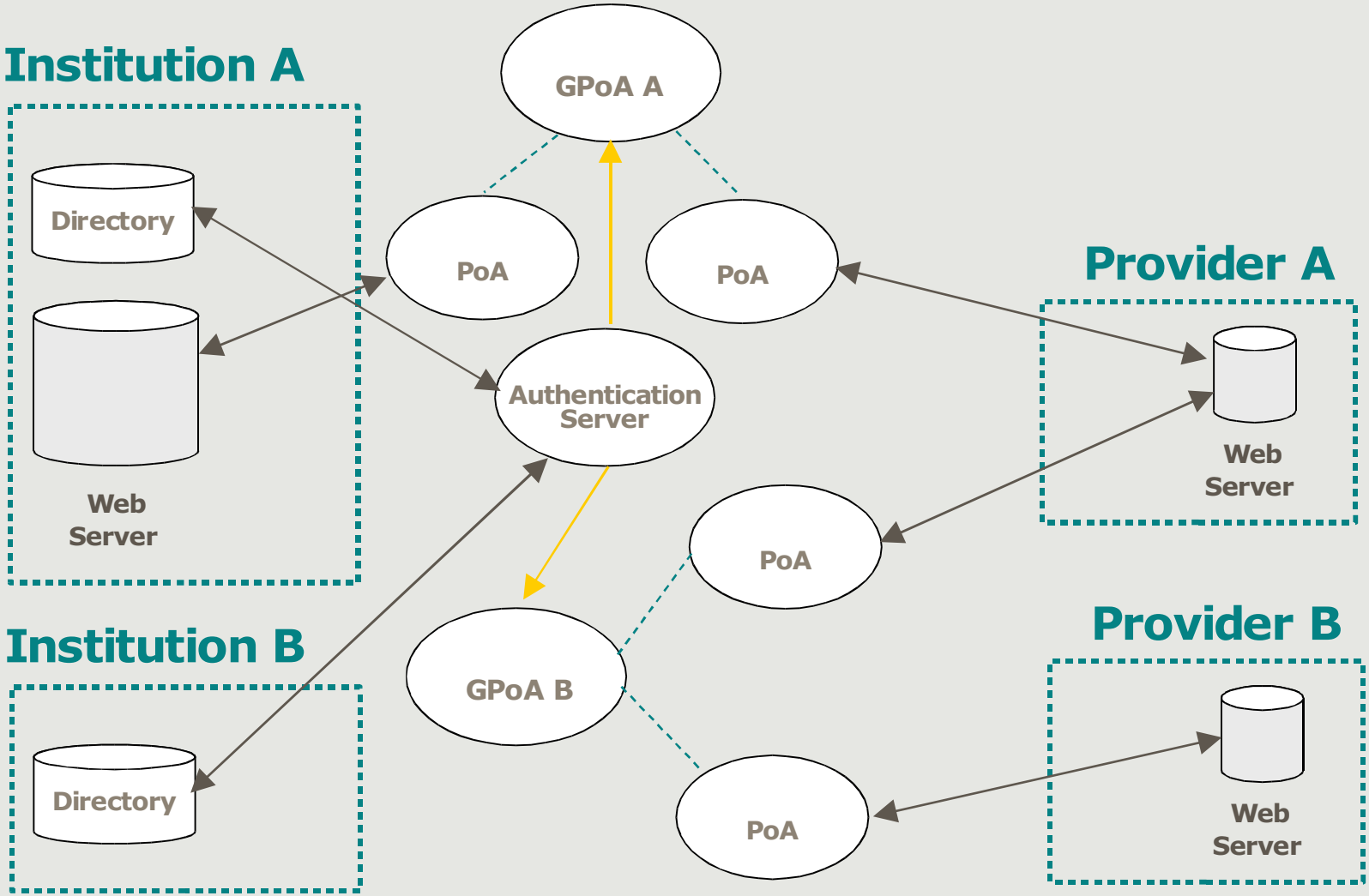
Application scenarios
Datacenter



Application scenarios
Access to local and remote services



Application scenarios
Centralized service



Current status

- Version 1.1 in production
  - Available in open source from http://www.rediris.es/app/papi/
  - Runs on Apache servers
  - Authentication modules based on POP3, LDAP and index files
- Version 1.2 nearly to be released
  - Includes ISAPI (Microsoft IIS) support
  - Enhanced proxy functionality
  - Simpler configuration
- Growing installed base
  - Gaining experience on requirements and applicability

Ongoing work

- Alignment with other AA initiatives
  - Use of standard languages (SAML) for assertions and normalization of attributes
  - In the framework of the TF-AACE group
    - In collaboration with Internet2 (Shibboleth)
- Dynamic assertion evaluation
  - Based on attribute queries made by (G)PoAs and answered by the AS
  - Running on top of WebServices (SOAP)
- Performance enhancements
- Going beyond the Web
  - Use of the AA model for other applications: videoconferencing, Grid services,...