RedIRIS

# Application of the PAPI authN and authZ system to the TJ-II Remote Participation environment

Madrid, 21 March 2003

# Outline

- An introduction to PAPI
- A short tour on PAPI internals
- Applying PAPI in the TJ-II Remote Participation

# Basic requirements

- 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 not require extra technologies at the user side
- Web oriented, although extensible to other access technologies
  - Grids, multimedia contents and interactions,...

# 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 authN/authZ currently in operation

# 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

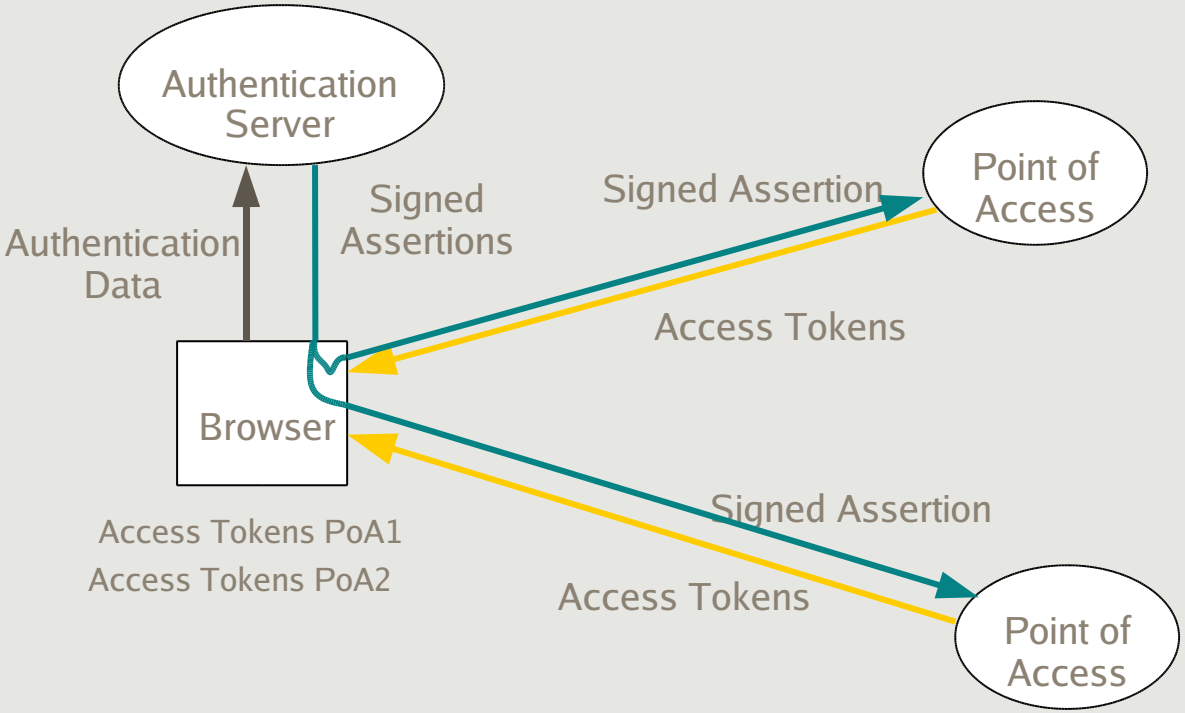
# The Authentication Server

- Verifies user identity and rights
  - Each of these verifications is independently performed
  - Multiple authentication methods: POP-3, LDAP, X.509 certificates, databases,...
- 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

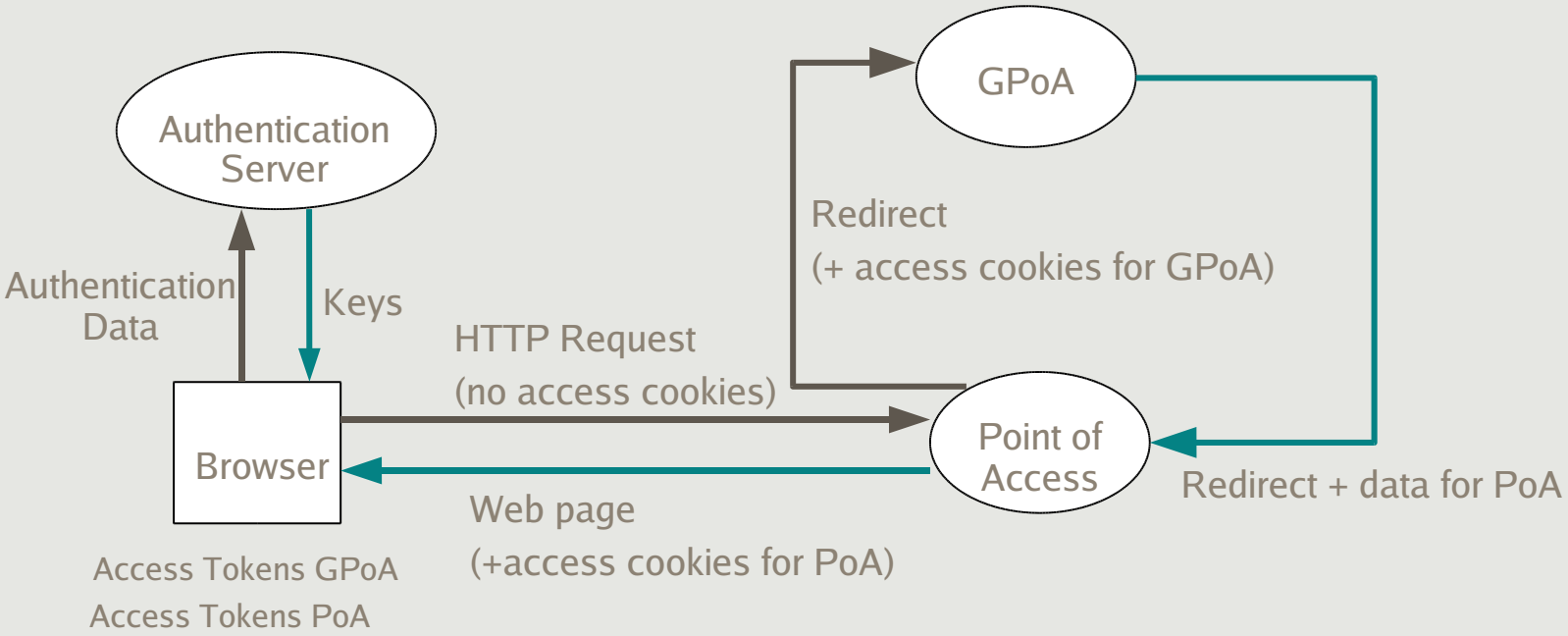
# The PAPI base protocol



# 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 processes 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

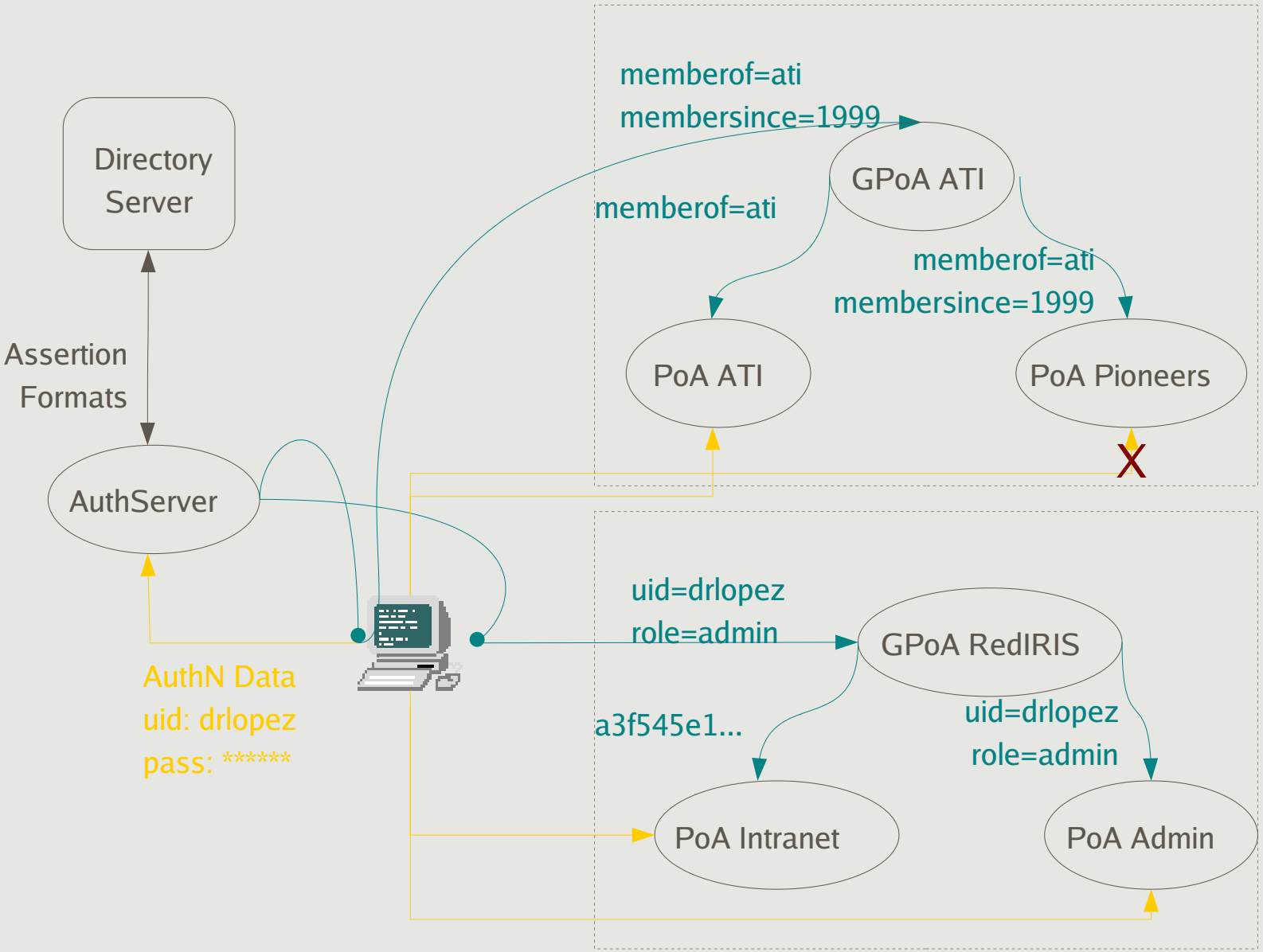
# GPoA and PoA interactions



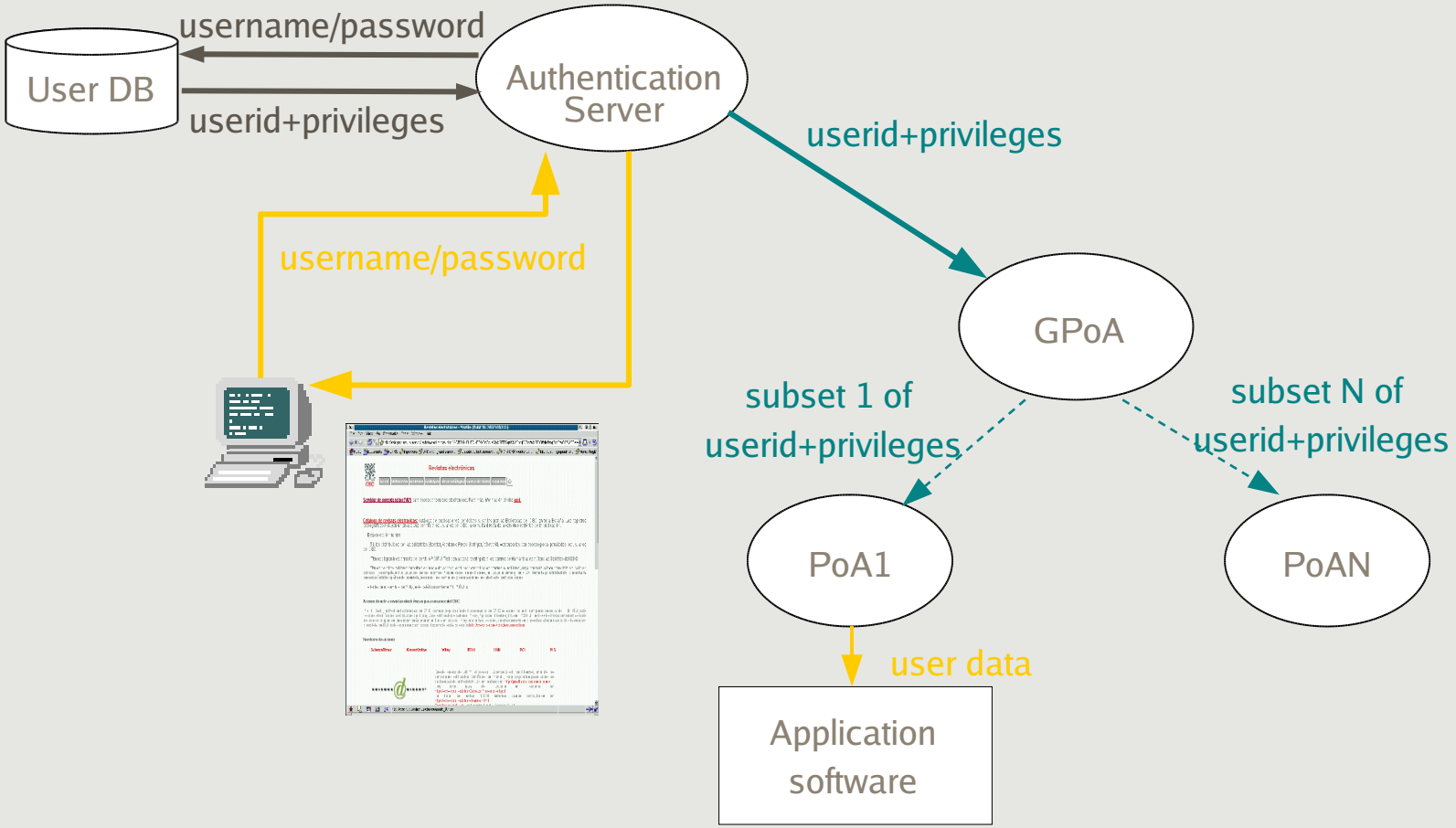
# Support for attribute-based authZ

- The AS builds an assertion string to be sent to (G)PoAs it knows about
  - Inside the assertion string, the AS can substitute
    - Connection variables: username, a nonce, anything else in HTML forms or the configuration
    - Attributes of the user entry
- When a (G)PoA receives a request for tokens can apply filters
  - Even (and specially) when it comes from a parent GPoA

# Support for attribute-based authZ



# Application scenario
# TJ-II Remote Participation



# Going further - AuthZ engines and WS

- AuthZ engines are external elements, performing decissions according to user attributes and defined policies
  - Richer semantics
  - Out of the strict Web server scope
  - SPOCP, University of Umea (integrated)
  - PERMIS
- Web Services constitute the base of new generation Grids
  - Collaborative scientific computing
  - Require distributed AA more than ever
  - Experiments on PAPI/WS interactions