EdelWeb

Peter Sylvester - EdelWeb

A standard for authorization management for secure interoperability of multi-organisation information systems

6th European Forum on Electronic Signatures

June 7-9, 2006, Amber Baltic Hotel, Miedzyzdroje

peter.sylvester@edelweb.fr *http://www.edelweb.fr*

EFPE 2006 EUROPEAN FORUM

The actors in the play

- **The French social security organisations**
  - **distributed services for retirement management**
  - **CNAM, CNAF, CANAM, MSA, CANCAVA/ORGANSIC ACOSS, …**
- **Ministry of health and social Security**
- **The Prime Minister's Agency for the Development of the Electronic Administration**
  - **ADAE now DGME**
- **EdelWeb**

EdelWeb – www.edelweb.fr

- Spin-off from French INRIA and German GMD, created in 1994
- 20 consultants, experts or engineers
- Branch of ON-X Group (220 people)
- One of the first French companies specialized in IT Security
  - Technical audits and penetration tests
  - Security architecture and technology experts
  - Cryptography
  - R&D lab for operational evaluations and specific developments
- Many references within telecom operators, banks, organizations, administrations, civil and military industries
- Quality certification ISO9001:2000

The problem space

- **Implement client/server applications between consenting but independent organisations**
  - **Allow certain persons determined by one organisation access to applications in other organisations**
- **Each organisation is responsible for its personnel and rights and duty attribution**
  - **Authentication techniques, roles, access management are specific in each organisation**
  - **A radical change or harmonisation is not a realistic approach**
- **Centralized management does not work.**
  - **Distance between interested parties to large**
  - **Problem of responsibility in case of errors**

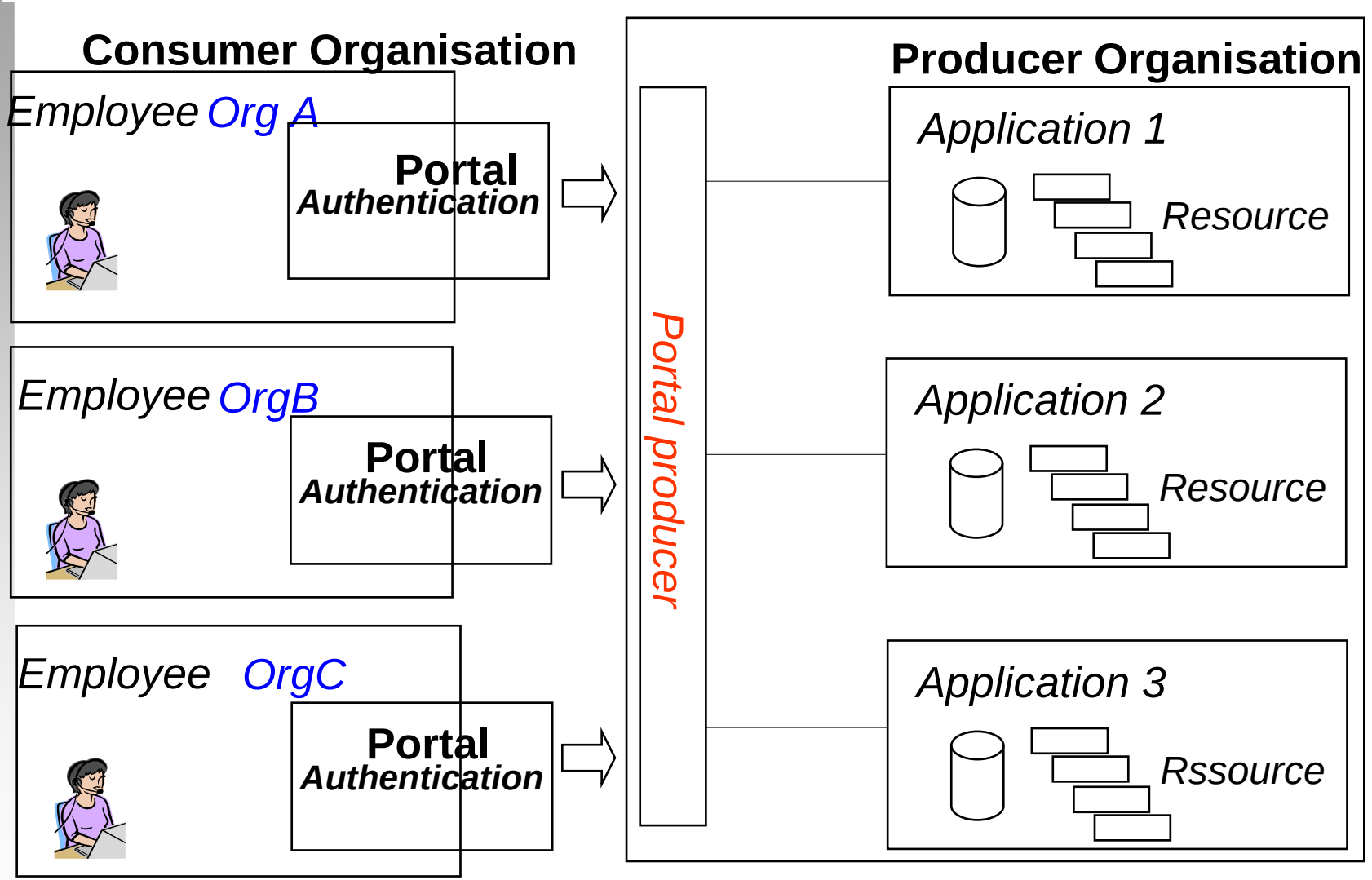
Interactions between organisations

- Communication between two different information systems – consumer and provider
- Two types of interactions
  - Web portals
  - Application to application – web services
- Context of explicit and controllable trust
- Professional actors (persons) are clearly identified
  - Vs federation of identity of « clients »
- Roles, rights, application profiles are specific and not compatible in each organisation

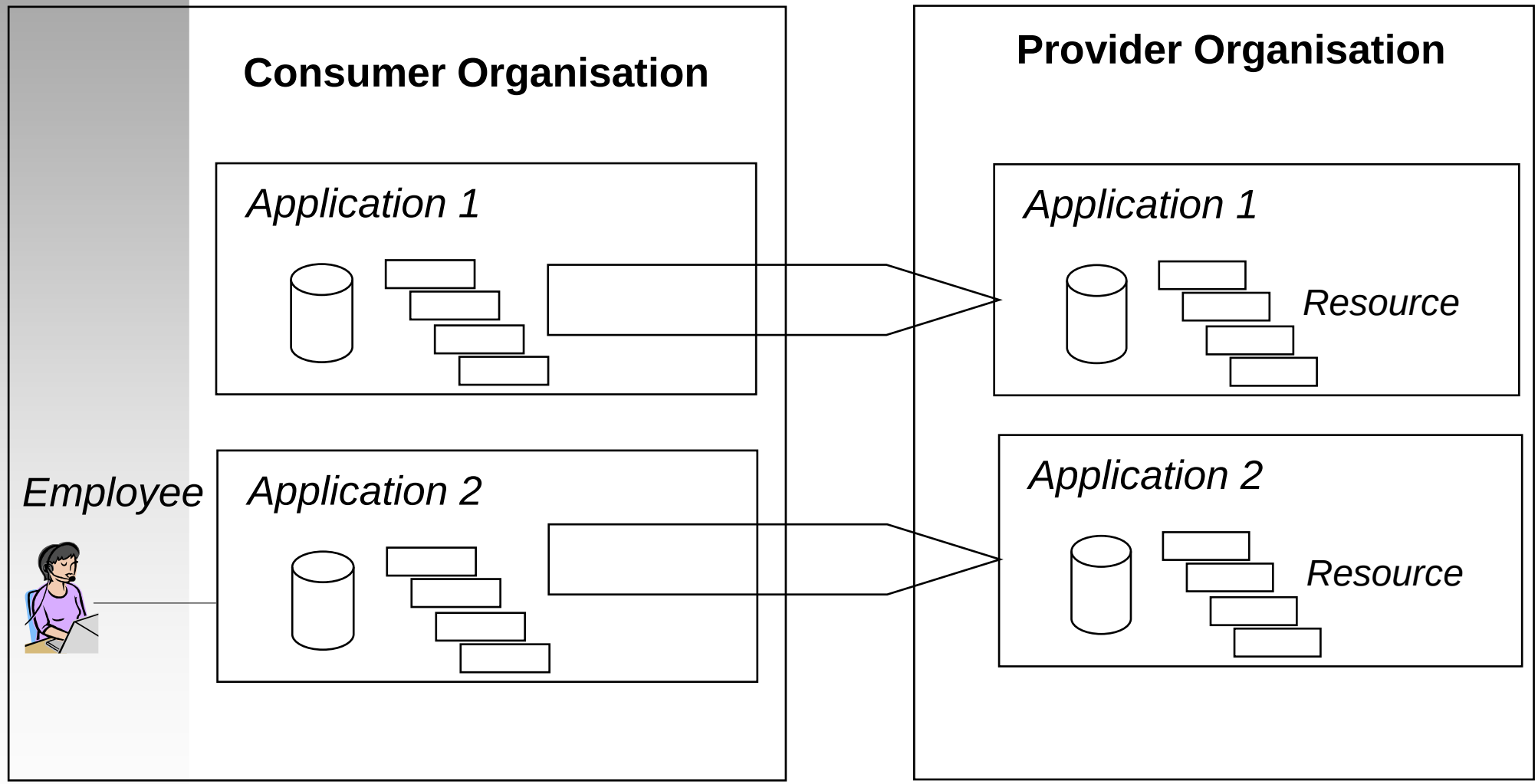
Objectif of the standard

- **Establishment of a service and a contract among organisations permitting each partner to remain « master at home » and to assume his responsibilities.**
  - **The consumer organisation manages the attribution of rights to access an application.**
  - **An assertion/attestation of this attribution is propagated to the producer**
- **Guaranty of a sufficient general security level**
  - **Authentication, traceability**
  - **A priori trust with a posterior control**

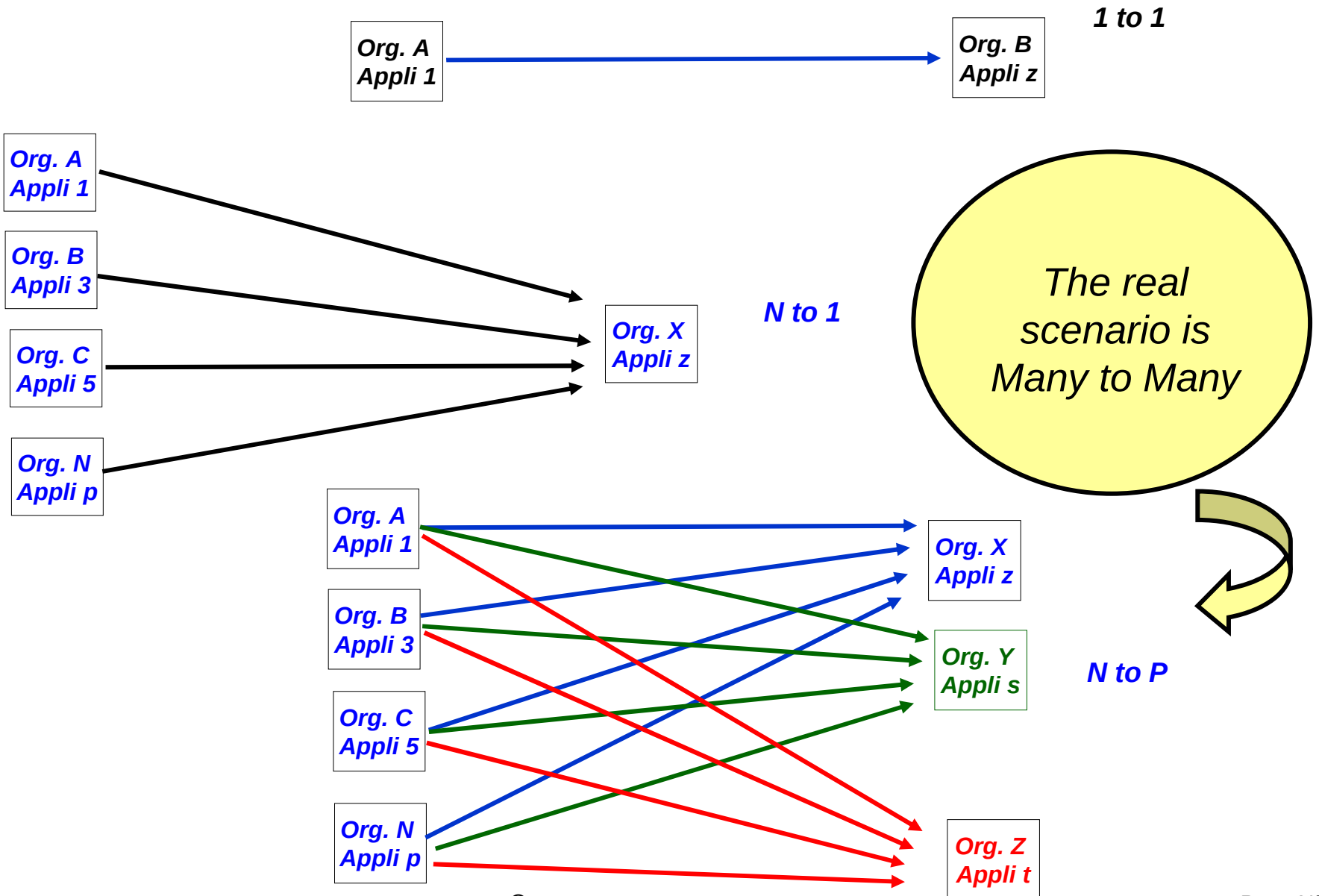
Web Portal Scenario



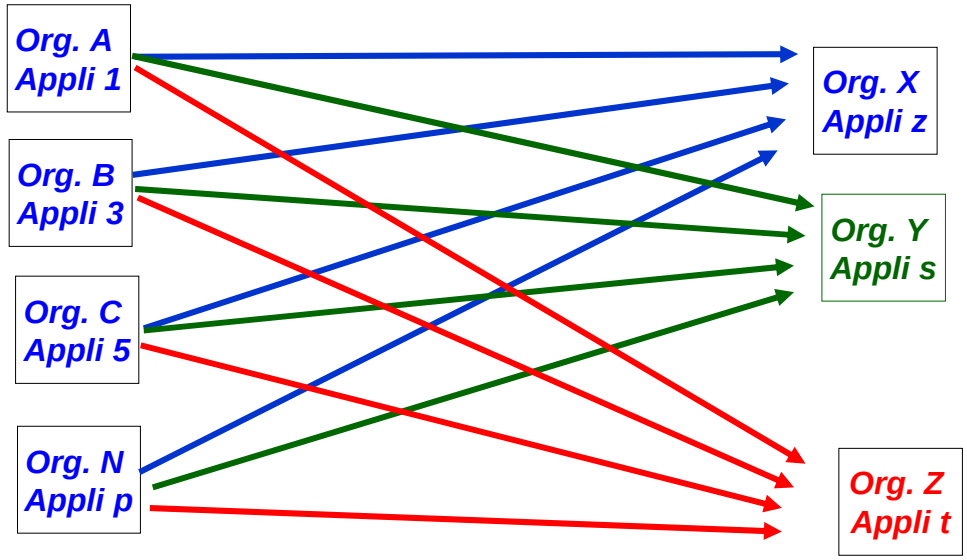
Scenarion Web Services



Communication scenarii



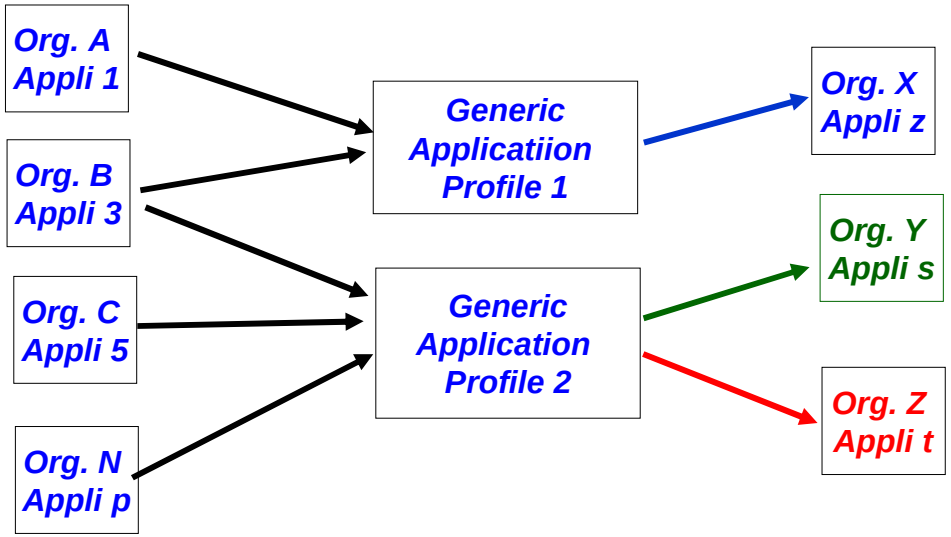
Roles and profiles



Many Different Roles

N to P

Many Different Application Profiles



N to P

Generic Application Profile (PAGM)

Profil Applicatif Générique Métier

The selected approach

Séparation of duties and responsibilities in a context of trust delegation

Right management
Towards target service

Identification vector
*transmission of a commonly defined **PAGM***
Asserted by l'organisation A

Application profile

Access rights

Right 1
Resource 2

Authentication

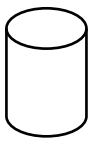
Responsability organisation A

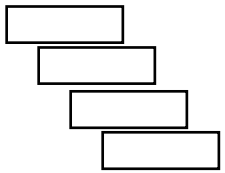
Responsibility organisation B

Agent

Organisme A

Application *Organisme B*



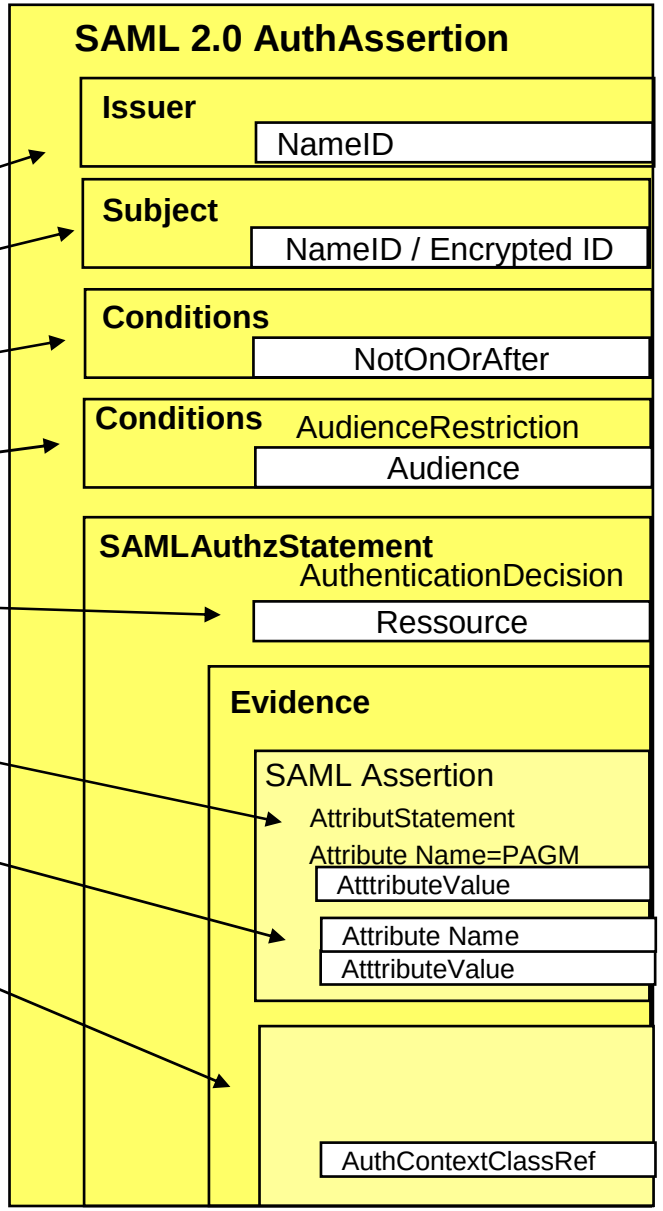


Ressources

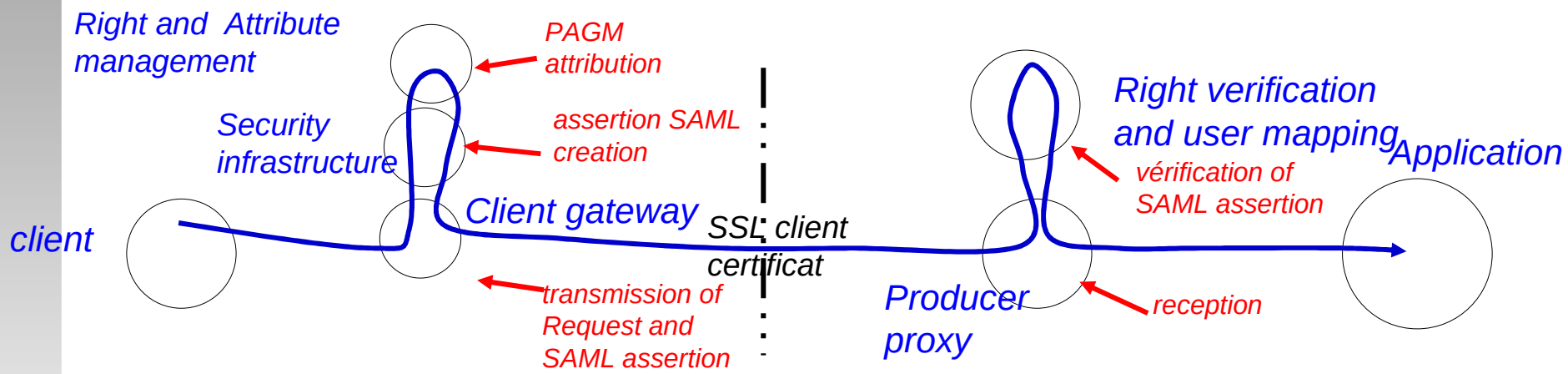
The Indentification Vector

Identification Vector

Client organisation ID
Client ID
Validity period
Target organisation ID
Target Service
PAGM (one or more)
Other attributs
Level of authentication



Data flow scenario web portals



All security control is done in the two organisations

- *no third party*
- *using gateways (client) et proxies (producer)*

Functional decomposition

Configuration and contract preparation

Administration of contracts

EbXML

Opérational Systems

Client Gateway

Apache and modules

Producer Proxy

Security Infrastructures

Right management SSO, etc.

Existing

Creation and verifictaion Identification vector service

Open SAML

Traces

IGC

Dedicated for Gateway to proxy authentication

EFPE 2006 EUROPEAN FORUM

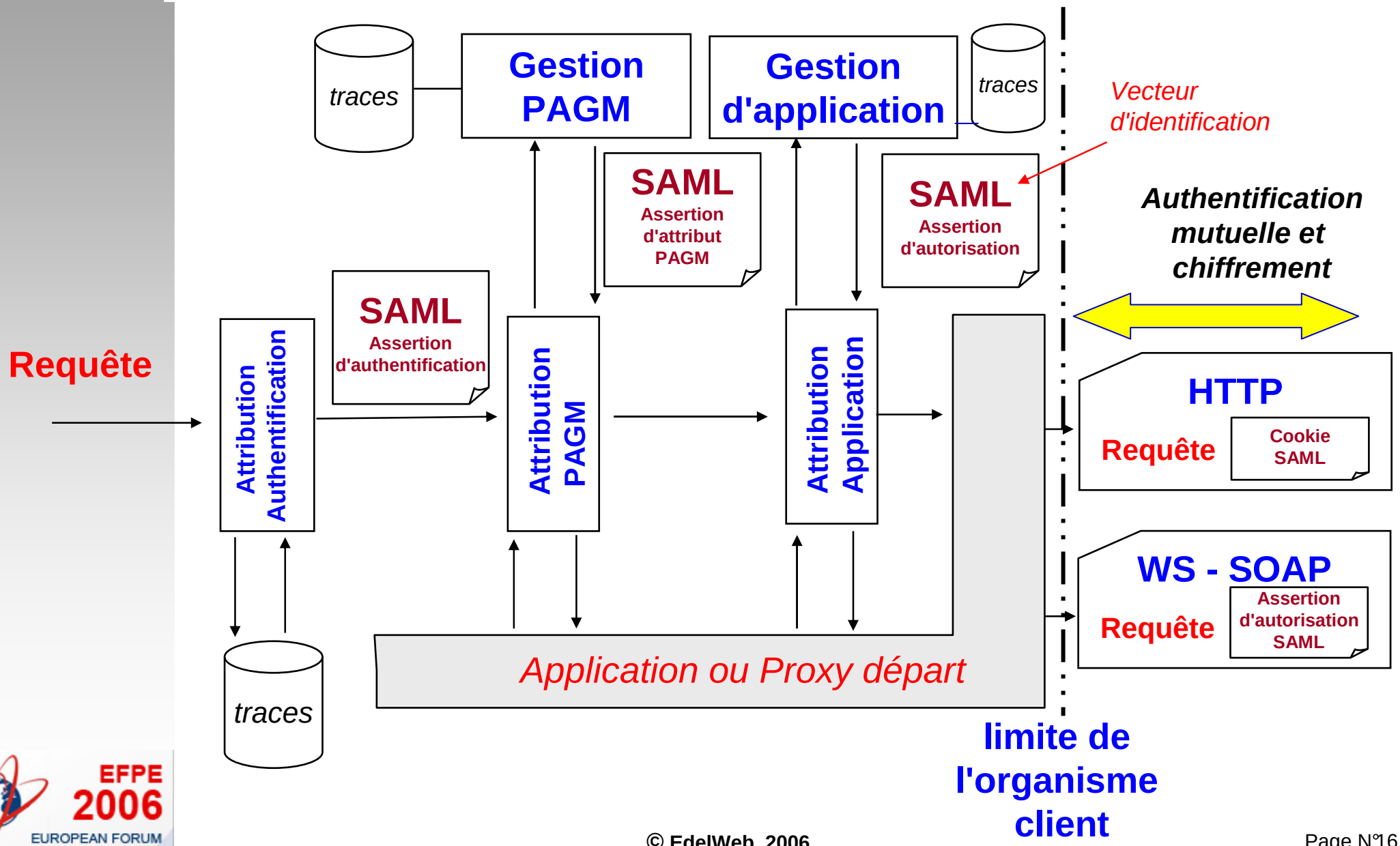
EdelWeb

Technical choices summary

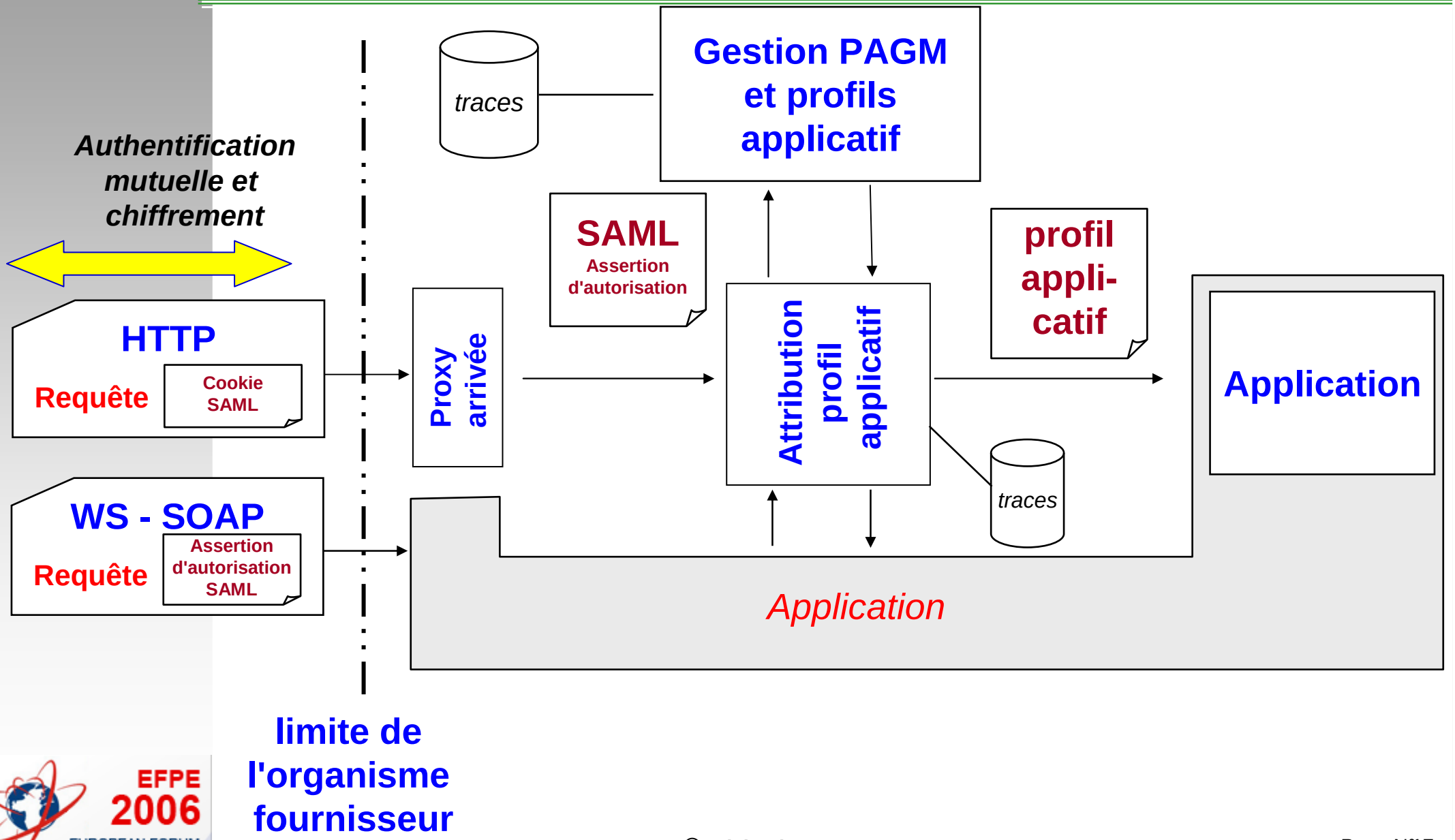
- **Base technologies**
  - SAML for the format of the identification vector
  - SSL between organisations' gateways and proxies
  - Study ebXML for the administration of the contracts
  - Simple interface to tracing and journaling service
- **No need to change the local authentication and authorisation systems**
  - For the client add PAGM management (role mapping)
  - For the consumer mapping to some local user.
- **Preference for open source technologies and standards**

EFPE 2006 EUROPEAN FORUM

Creation of identification vector



Consumer Treatment of Identification Vector



EdelWeb

Actual situation

- Standard and detailed description defined and published
- Comments from the public included
- ADAE/DGME supports activity as a possible solution for the whole administration
- Social sphere actors have started implementation experiment
- Large parts of the standard can be implemented with existing open source technology

EFPE 2006 EUROPEAN FORUM