An Access Control Framework for Business Processes for Web Services

Hristo Koshutanski, PhD Student

hristo@dit.unitn.it.

Department of Information and Communication Technology

University of Trento, ITALY

December 18, 2003

Doctoral Consortium, ICSOC-2003

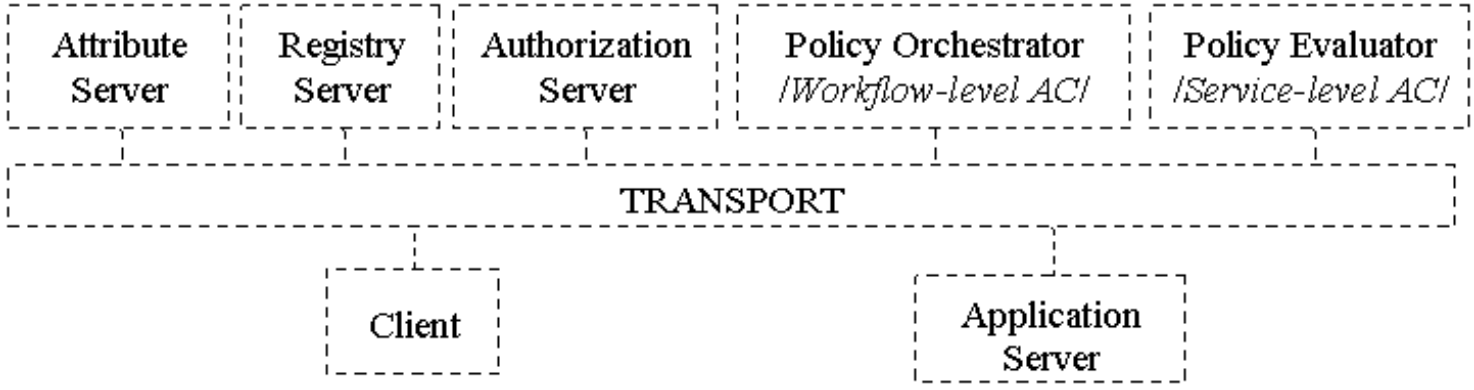
Web Services & Processes

- Web Service – an interface that describes a collection of operations that are network-accessible through standardized XML messaging.
- Web Services Process – an extension of Web Services for complex business and workflow processes.
- Virtual Enterprise – a collection of *partners* that offer their services on the Web and cooperate each other efforts into coherent business processes.

Differences with Traditional Access Control

- *credential* vs. *user-based* access control;
- *orchestrating* vs. *combining* security policies;
  - orchestrator may *not* have the policy of partners.
- *interactive* vs. *one-off* evaluation of credentials;
  - tell user to supply additional credentials.
- *controlled disclosure* of information vs. *all-or-nothing* decision;
  - information on missing credentials may *not* be sent to anyone.
- *abducing* missing credentials for fulfilling requests vs. *deducing* entailment of valid requests.

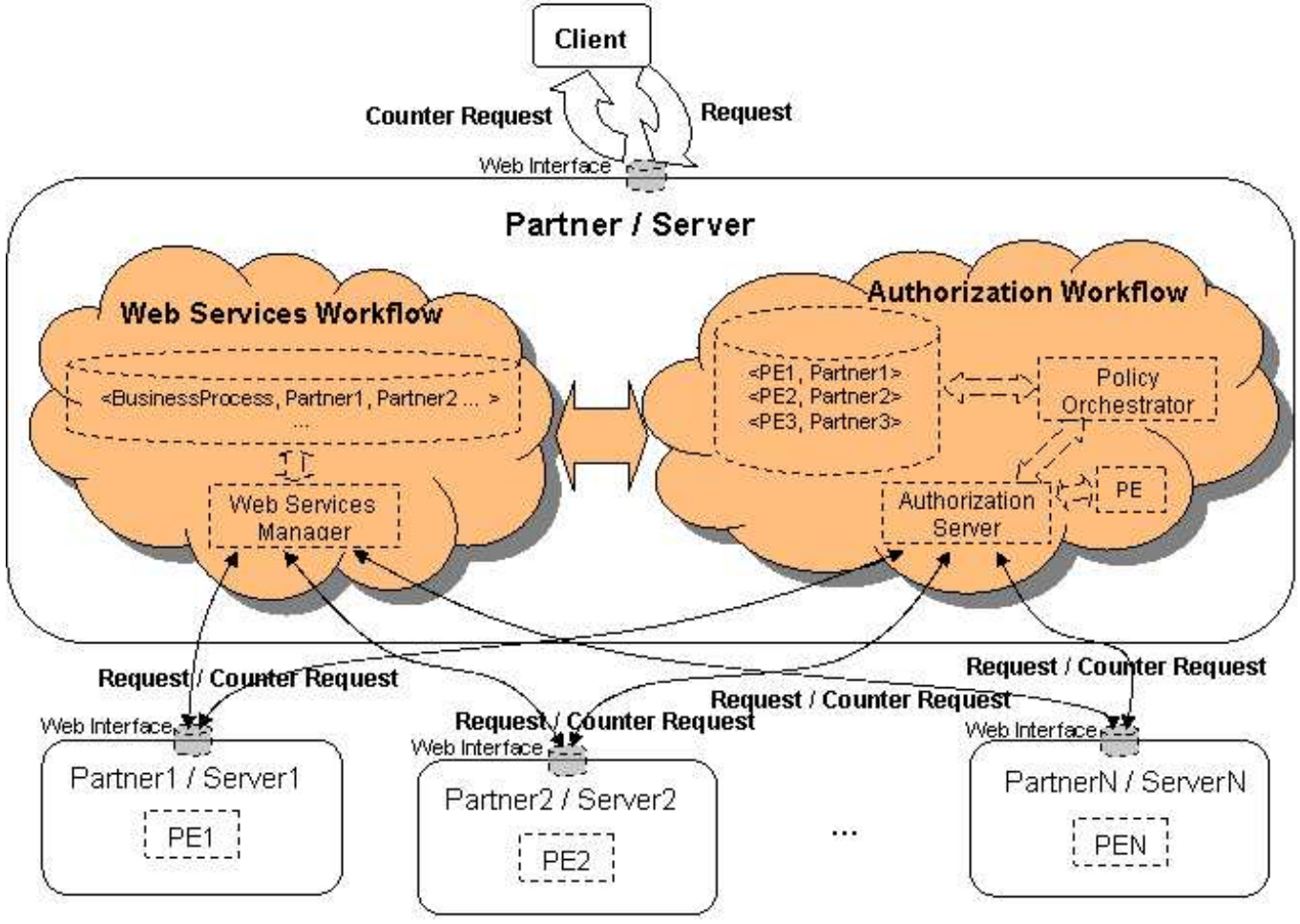
Architecture



Assumption: authentication, confidentiality and integrity on lower levels:

- Transport level – *WS-Security* by Microsoft and IBM;
- Message level – *XML-Signature* by W3C and IETF, *XML-Encryption* by W3C.

Horizontal View of the Architecture



Communicating "Mobile" Processes

- Authorization process is a business process,
- Mobility of authorization processes
  - entities send authorization business processes to other entities to execute them,
- Flexibility and simplicity of entities in the system,
- Quick and simple implementation of the Authorization Server,
- Communication with clients for interactive requests
  - want this ... do that!
  - provide information on context where credential is required.

Interactive Access Control

1. first, compute the set of disclosable credentials, then
2. use abduction to find a minimal set of missing credentials (among the disclosable ones) that entail the service, and
3. send them back to the client.

Example

$\mathcal{P}_{\mathcal{A}}$: $r_1 \leftarrow C_A, C_B$; $r_1 \leftarrow C_A, C_C$; $r_2 \leftarrow r_1, C_D$

$\mathcal{P}_{\mathcal{I}}$: $C_B \leftarrow C_A$; $C_C \leftarrow C_A$

Request	Credentials	Result
r_1	C_A, C_B	grant
r_1	C_A	send C_B or send C_C
r_2	C_A	deny
r_2	C_A, C_D	send C_B or send C_C

Access Control for Stateful Business Processes

1. first, check presented/past credentials that must be revoked (they make policy inconsistent), then
2. check for the missing credentials on the top of the not revoked ones, and
3. send the resulting two sets back to the client.

Remark. *The check for revocable credentials can be transformed back into an abduction problem.*

Ongoing and Future Work

1. Implementation of basic system entities using Collaxa server (www.collaxa.com),
2. Experimental assessments using DLV system (www.dlvsystem.com) as a background formal engine for the basic functionalities of deduction and abduction,
3. Syntactic condition for fast computation,
4. Formal relation with trust negotiation.