

# Context-based Access Control for Ubiquitous Service Provisioning

**Antonio Corradi, Rebecca Montanari, *Daniela Tibaldi***

{acorradi, rmontanari, dtibaldi}@deis.unibo.it

DEIS - Department of Electronics, Computer Science and Systems

University of Bologna - Italy

Hong Kong: September 28-30, 2004



- **Access Control Issues** in Ubiquitous Environments
- **UbiCOSM** Security Framework
  - Security Model
  - Access Control Middleware
- **Case Study:** Mobile Office Application
- Conclusions and Future Work



- Wireless network connectivity and portable devices  
⇒ *anywhere* and at *anytime* access from *various* access devices

Novel access control challenges:

⇒ **Paradigm shift** from *subject-centric* to *context-centric* access control

- Un-informative identity or not trustworthy
- Traditional identity-based access control models are inadequate for Ubiquitous Environments
- Static characterization of context
- Context as a trigger for policy evaluation



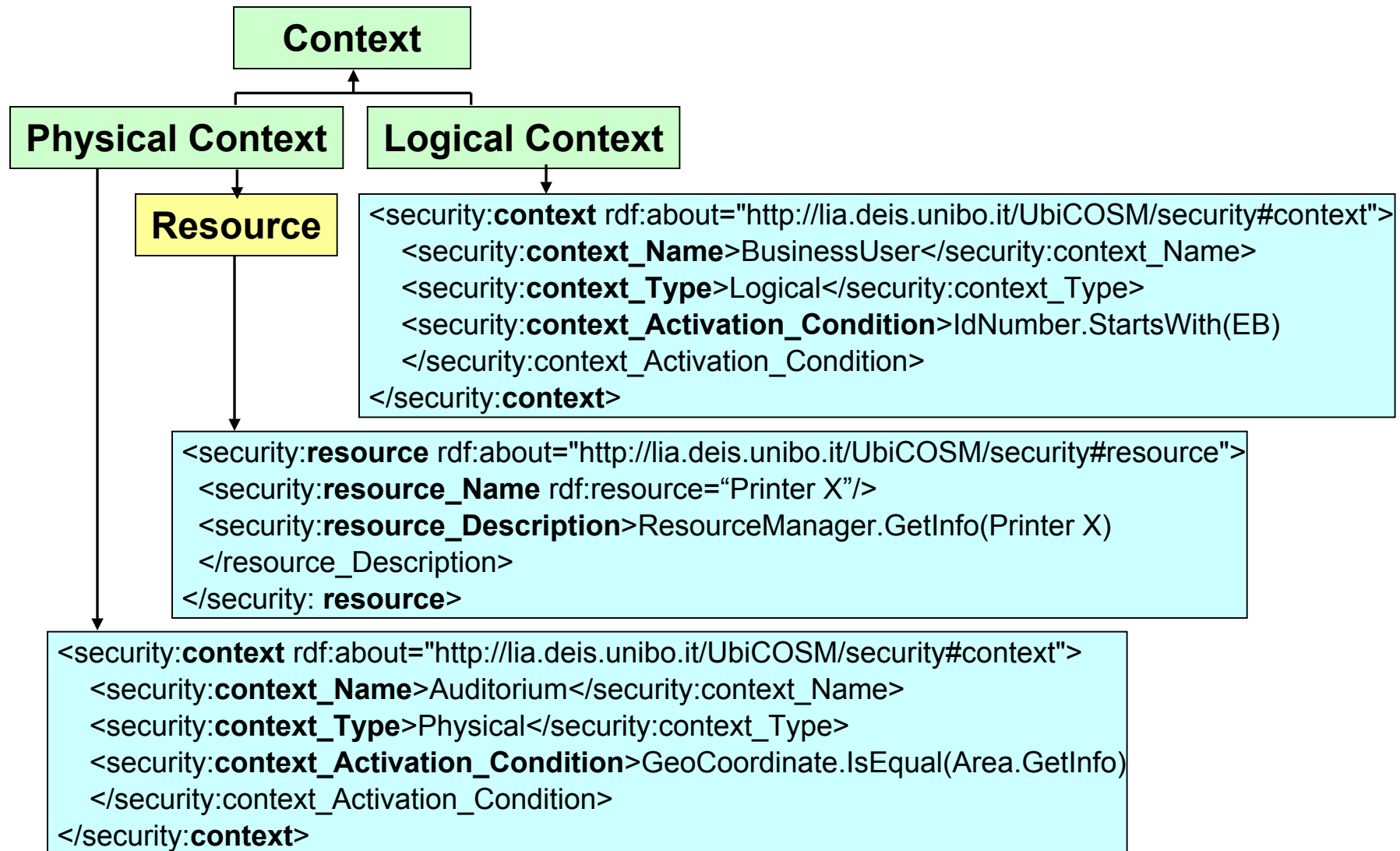
## UbiCOSM

(Ubiquitous Context-based Security Middleware)

- Permissions directly associated with contexts
- **Context** = grouping mechanism for applicable permissions

**Goal:** Immediate **controlled visibility** of accessible resources and of other mobile users locally executing







## Access Control Policies:

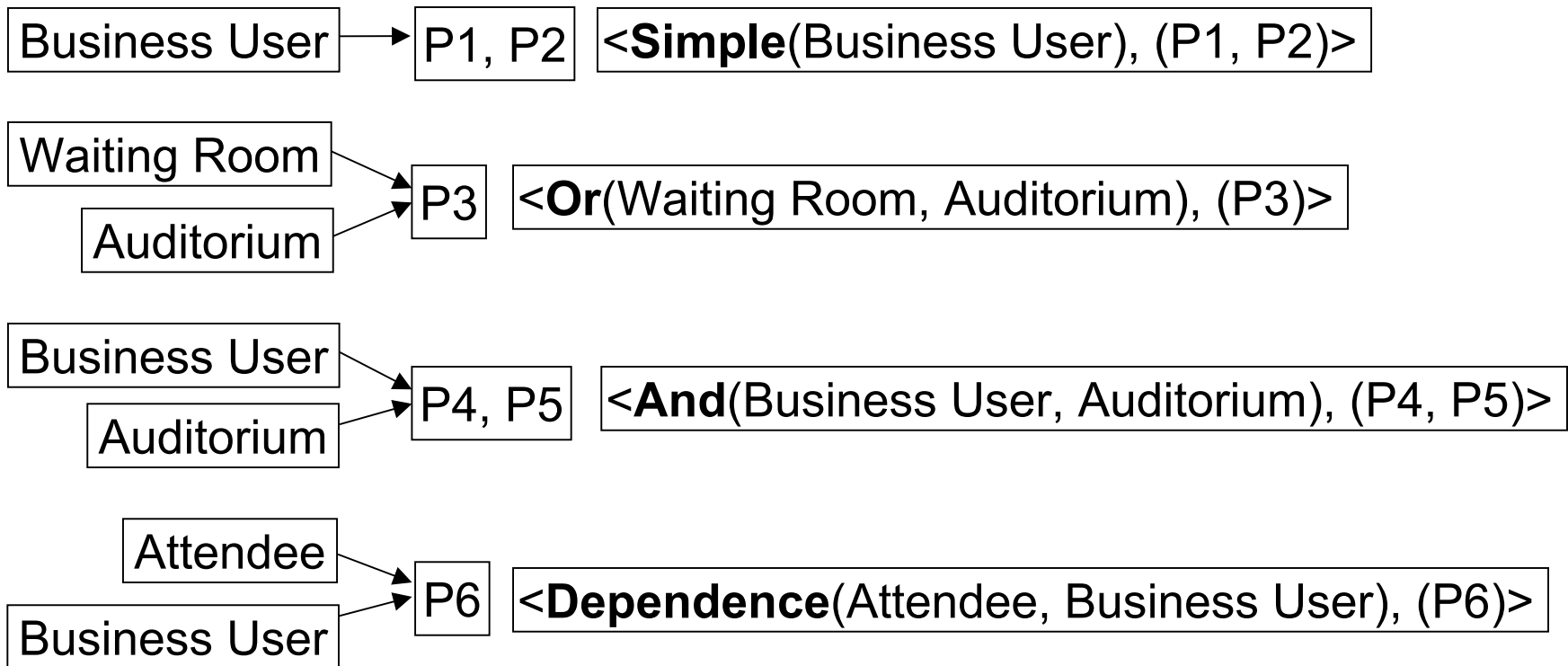
Specific context conditions  specific permissions

<association\_Name(context\_collection), permissions>

```
<security:permission
  rdf:about="http://lia.deis.unibo.it/UbiCOSM/security#permission">
  <security:Name>P1</security:Name>
  <security:Target rdf:resource="Printer X"/>
  <security:Action>print</security:Action>
</security:permission>
```

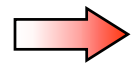


<association\_Name(context\_collection), permissions>





<association\_Name(context\_collection), permissions>

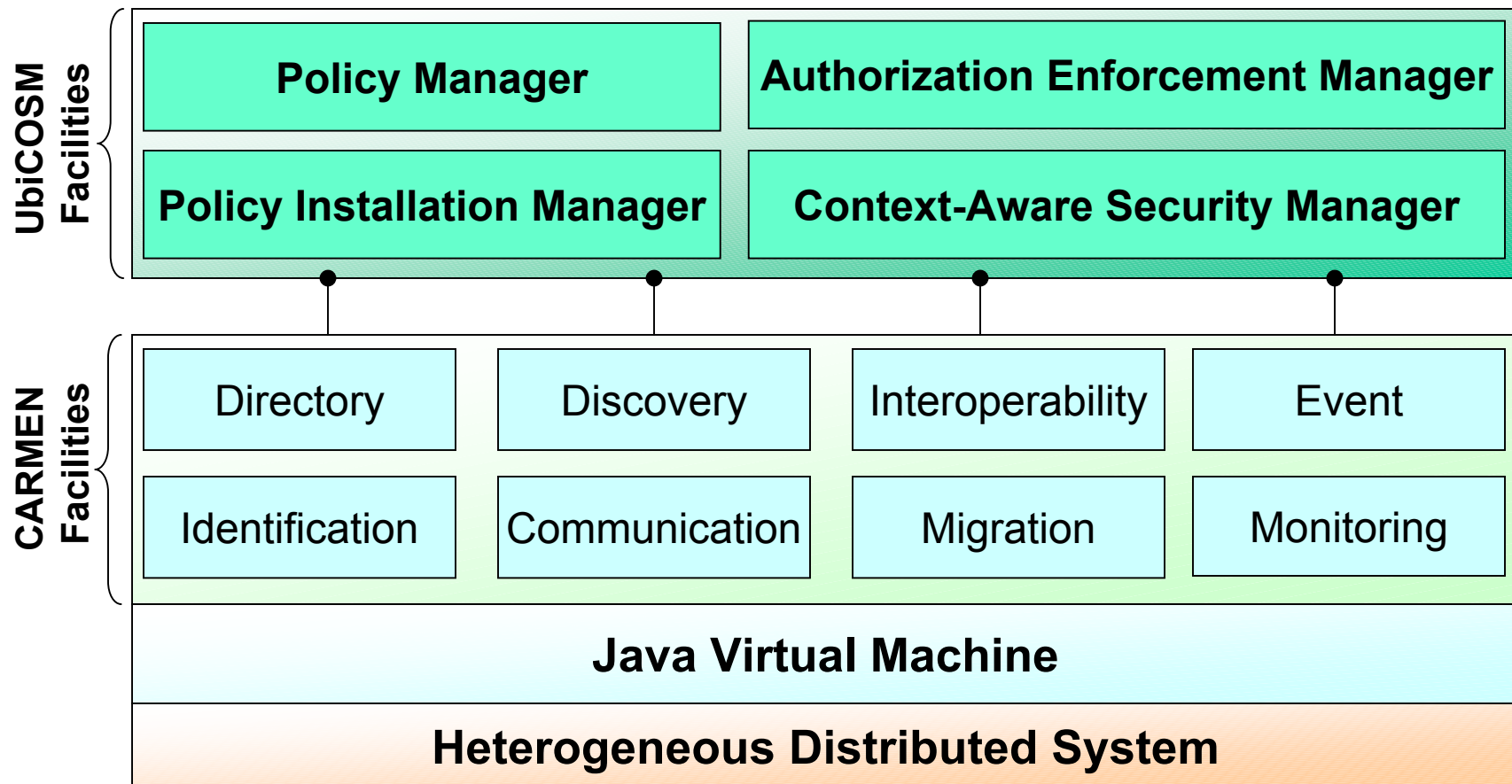


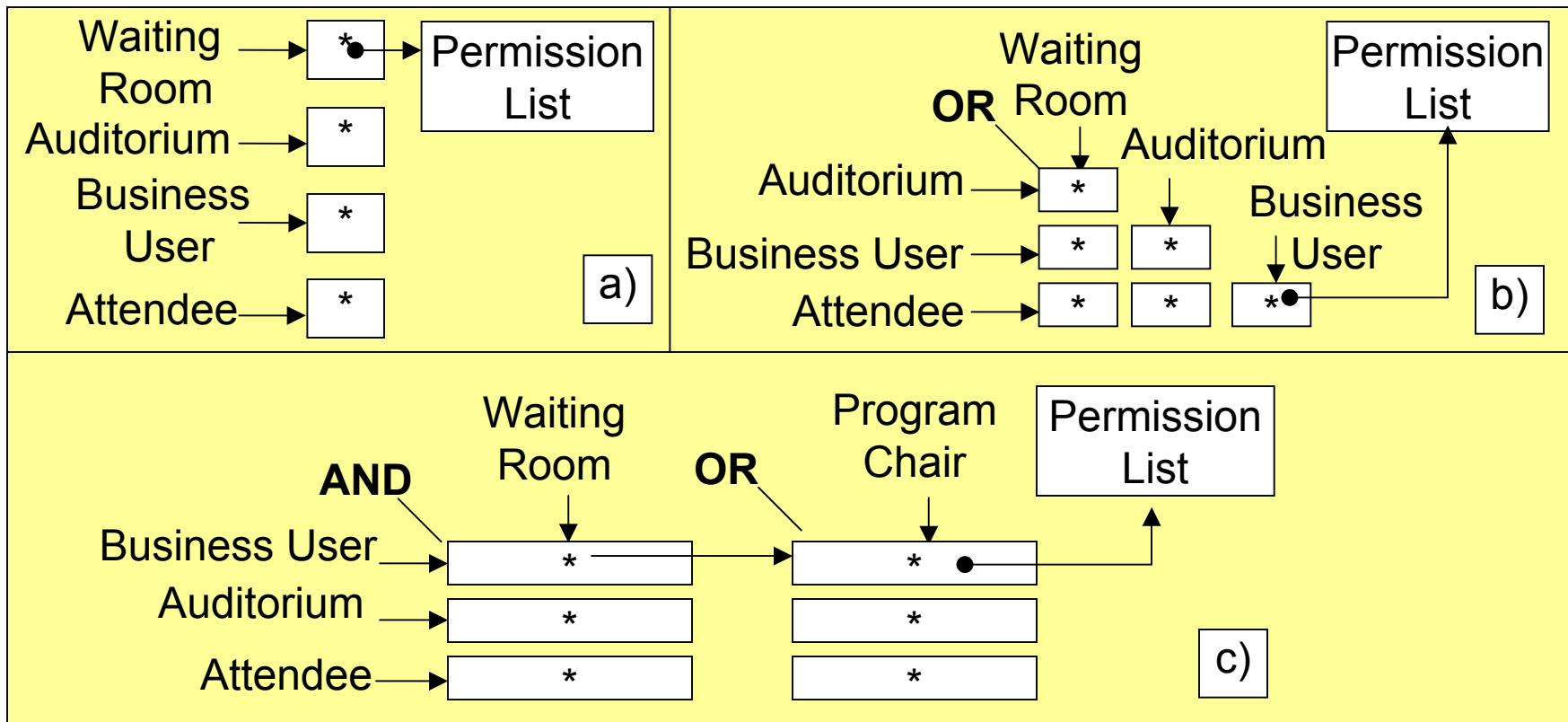
- Easy specification/update/revocation of permissions as the system evolves
- Permissions are dynamically applied simply adding/removing user association with context
- Context activation implies immediate permission activation





# UbiCOSM Architecture





OR(Program Chair, AND(Waiting Room, Business User))



## Mobile Office Application

### Objectives

- provide familiar office environment visibility
- enrich mobile office interacting with local resources

### Network Deployment Setting

- Wireless building network composed by several 802.11 network localities
- Wireless access devices: Toshiba e740 Pocket PCs



## *Access Control Policy*

<And(Auditorium, Conference in Action, Business User), P1>

```
<security:permission
  rdf:about="http://lia.deis.unibo.it/UbiCOSM/security#permission">
  <security:Name>P1</security:Name>
  <security:Type>authorization.</security:Type>
  <security:Target rdf:resource="Spider Game"/>
  <security:Action>Access</security:Action>
</security:permission>
```

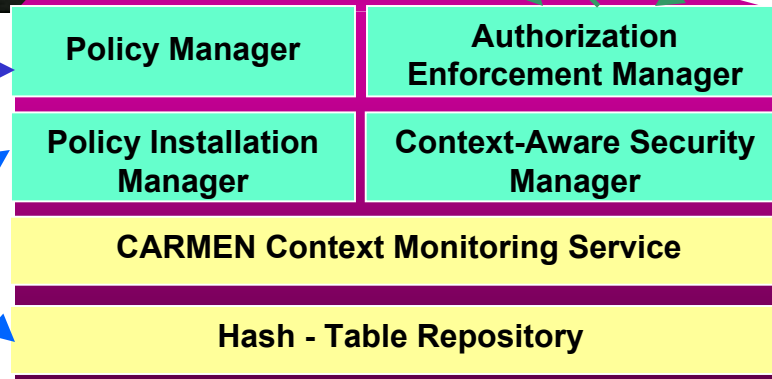


**Physical Context**

**Grants/Denies**

**Permission View**

**Request**





Performance overhead to **compute** a permission view

L	t(msec)
10	0.26
20	0.48
30	0.75
40	0.96
50	1.25
60	1.50
70	1.75
80	1.93
90	2.13
100	2.52

L = Number of Logical Context



- UbiCOSM: a *context-driven access control* framework
  - to apply in Ubiquitous Environments
  - to *protect resource access*

## Future Work

- Policy conflict detection
- Integration of UbiCOSM with mechanisms for inter-cell mobility prediction to anticipate user migration



ALMA MATER STUDIORUM  
UNIVERSITA DI BOLOGNA

# Thank You!

Hong Kong: September 28-30, 2004