Peces
Pervasive computing in embedded systems

Contract:
FP7- 224342-ICT-2007-2
PECES Technology

Outline

• Goal and Approach
• Role Assignment
  o Role Specification
  o Context Ontology
  o Classes of Rules
  o Trust and Security
  o Automatic Assignment
  o Role-based Mechanisms
• PECES Middleware
  o Architecture
  o Interaction
• Summary
PECES
Goal and Approach

• Goal
  ▪ Implementation of a middleware to ease development of applications that adapt automatically to their context
    • Within a single smart space
    • Across smart spaces

• Validation Applications
  ▪ eHealth
  ▪ Localization and navigation
  ▪ Automated parking system

• Approach
  ▪ Creation of uniform abstraction for adaptation → role assignment
  ▪ Provisioning of middleware mechanisms on top of this abstraction

Dynamically interact with other spaces depending on context (e.g. destination)

Dynamically form smart space from devices in vicinity (e.g. PDA and CAR) depending on context (e.g. same user)
Role Assignment

Overview

- Devices know parts of their context (e.g. location, equipment, etc.) and make it accessible to other devices
- Applications can „address“ a set of devices based on constraints on their context (e.g. devices with big screen or devices belonging to John) → specified within a role specification
- Generic middleware service computes the sets of devices that match the specified constraints → and assigns so-called roles
- Constraints can reference each other hierarchically to improve efficiency and to increase the flexibility → by referring to a role within another role specification

Both, applications and middleware services can use assigned roles to interact with a set of devices
Role Assignment
Role Specification

- Roles are used to create a higher abstraction from context
- Roles are defined in a role specification which contains
  - queries to define constraints on context
  - usage tags to indicate a meaning
- Usage of web standards for portability of context information
  - Context represented using RDF statements
  - Selected subset of SPARQL to implement queries
  - Context ontology (OWL subset) to provide data model with support for reasoning

[Diagram showing SPARQL queries for role:presenter and role:audience]
Role Assignment
Context Ontologies

- PECES context ontology artefacts (http://www.ict-peces.eu/ont/{xyz})
  - Smart space ontology: smartspace.owl
  - Device ontology profile: device.owl
  - Measurement ontology: measurement.owl
  - User profile: userprofile.owl
  - Event: event.owl
Role Assignment
Sparql Queries

- Query language : SPARQL-SELECT
- Basic graph pattern (BGP)
  PREFIX rdf: http://xmlns.com/foaf/0.1/
  PREFIX device: http://www.ict-peces.eu/ont/device.owl#
  SELECT ?accessory
  WHERE { ?accessory rdf:type device:Accessory }
- Conjunctive query form
  SELECT ?accessory ?property ?value
  WHERE { ?device smartspace:carriedBy <john>.
          ?device rdf:type device:PDA.
          ?device device:has_Accessory ?accessory.
  }
- Query patterns can be extended and combined on development scenarios basis

A “machine” can determine the specification of the device, and then tailor its service to that device.

list all property and value pairs associated with the PDA carried by John
Role Assignment
Further Usage of Context

- Besides from role assignment
- Context ontologies and queries can also be used in applications
  - Example: Select a service based on context

```
SELECT ?device
FROM <useCaseETRA.owl>
WHERE
{
  {?
    device <http://www.daml.org/services/owl-s/1.1/Service.owl#provides>
    ?vehicle <http://www.ict-peces.eu/ont/smartspace.owl#isOwnedBy>
      <http://www.ict-peces.eu/ont/smartspace.owl#JohnSmith>}

  UNION
  {
    ?location <http://www.w3.org/2003/01/geo/wgs84_pos#location> ?address.
    ?address <http://www.ict-peces.eu/ont/smartspace.owl#country> 'Spain'.
    ?address <http://www.ict-peces.eu/ont/smartspace.owl#city> 'Valencia'.
    ?address <http://www.ict-peces.eu/ont/smartspace.owl#street> 'Tres Forques'.
    ?device <http://www.daml.org/services/owl-s/1.1/Service.owl#provides>
      <http://www.ict-peces.eu/ont/smartspace.owl#accessControlRegService>.
  }
```
Role Assignment
Classes of Assignment Rules

- **Three classes to support a wide range of applications**

- **Filter Rules**
  - Constraint over context
  - Defined using SPARQL
  - Allows restriction to specific set of devices

- **Reference Rules**
  - Constraints over roles, e.g. “must have role X from specification Y”
  - Allows hierarchical composition of specifications

- **Authentication Rules**
  - Constraints over meta information, e.g. “context must have been gathered by sensor X”, “context must not be older than 1 hour”
  - Allows usage of roles in security critical applications

PECES Technology

```sql
SELECT ?device
WHERE
{
  ?device hasUser Alice
  ?device attached Projector
  ?device attached ?screen
  ?screen isA Screen
  ?screen hasWidth ?width
  FILTER(?width > 1000)
}
```
Role Assignment
Automatic Assignment

- Roles are tags that are automatically assigned to matching devices
  - Multiple devices might have the same role (i.e. several group members)
  - One device might have multiple roles (i.e. member of several groups)
- To automate role assignment PECES introduces some assumptions
  - All smart spaces have a limited physical size
  - Size does not exceed k-hop neighborhood (k~3)
  - A smart space is represented by one device
    - Device is acting as coordinator
    - Periodically (re-)assigns the roles in the smart space
- A role assignment can be exported to a central registry on the Internet
  - Registry can be queried to enable hierarchical role assignment
Role Assignment
Trust and Security

- Use of certificates to model trust
  - Flexible: supports asymmetric relationships
  - Distributed: no central point of trust
- Use of certificates to bootstrap keys
  - Fast: high performance due to caching
- Different key distribution schemes
  - One-to-one and group communication
- Approach
  - Devices equipped with asym. key pair (ECC)
  - Key pairs signed by other entities to represent „groups“
  - Resulting hierarchy of certificates enables fine-grained trust-definition
  - Categorization of certificates in different levels of trust
  - Trust levels are used to restrict data sharing and role assignment
Role Assignment
Role-based Mechanisms

- **Group Communication**
  - A role is used to identify group members

- **Smart Space Formation**
  - Roles identify members of the smart space
  - Roles identify devices with special abilities (e.g. gateways)

- **Smart Space Interaction**
  - Smart spaces are exported to a registry on the Internet
  - Roles are used to combine smart spaces hierarchically

PECES Technology
PECES Middleware Architecture

- **BASE Middleware**
  - Device Discovery
  - Device Interaction
  - Service Abstraction
    - System Services
    - Application Services

- **PECES Extensions**
  - Context Management
  - Security Mechanisms
  - Role Assignment
  - Role-based Mechanisms
PECES Middleware
Interaction (Space Formation)

- Role assignment layer is implemented as a number of generic system services
  - **ContextStorage**: enables execution of context queries
  - **Coordinator**: issues queries and computes assignments
  - **Notification**: signals changes to role assignment

- Further services can be used to provide mechanisms
  - **Member**: manages smart space membership

peces technology
For access control, role assignment is done reactively but basic concepts are identical → reuse of generic abstraction to facilitate device interaction.
PECES Technology

Summary

Goal
• PECES middleware to ease development of adaptive applications
  – Support for interaction within a single smart space
  – Support for interaction across different smart spaces

Approach
• Creation of uniform abstraction for adaptation \(\rightarrow\) role assignment
• Flexible context model based on Web standards to ensure data portability
• Security and trust mechanisms to enable trustworthy interaction
• Provisioning of middleware mechanisms built on top of role assignment
  – Smart space formation and interaction
  – Role-based communication and service interaction
  – Role-based Access Control
PECES Technology
Availability

- **Open Source**
  - All middleware components are available at peces.googlecode.com
    - Device-specific interoperable communication, role assignment, context storage, ontologies, security, …
  - BSD license to facilitate pickup in academic and commercial projects
  - Apache Maven to enable simple yet modular reuse on heterogeneous devices

- **Documentation**
  - Detailed specifications available at PECES project website
  - Walk-throughs and (simple) example applications at Googlecode website

- **Development Tools**
  - Comprehensive suite of tools implemented on top of Eclipse
    - Point-and-click device and security configuration
    - Context and query specification and compilation
    - Scenario emulation and testing

- **Test it yourself, it is all freely available!**
PECES Technology

• Questions?