April 25, 2013

Context-Aware Access Control Model for Smart-M3 Platform

Alexey Kashevnik, Nikolay Teslya

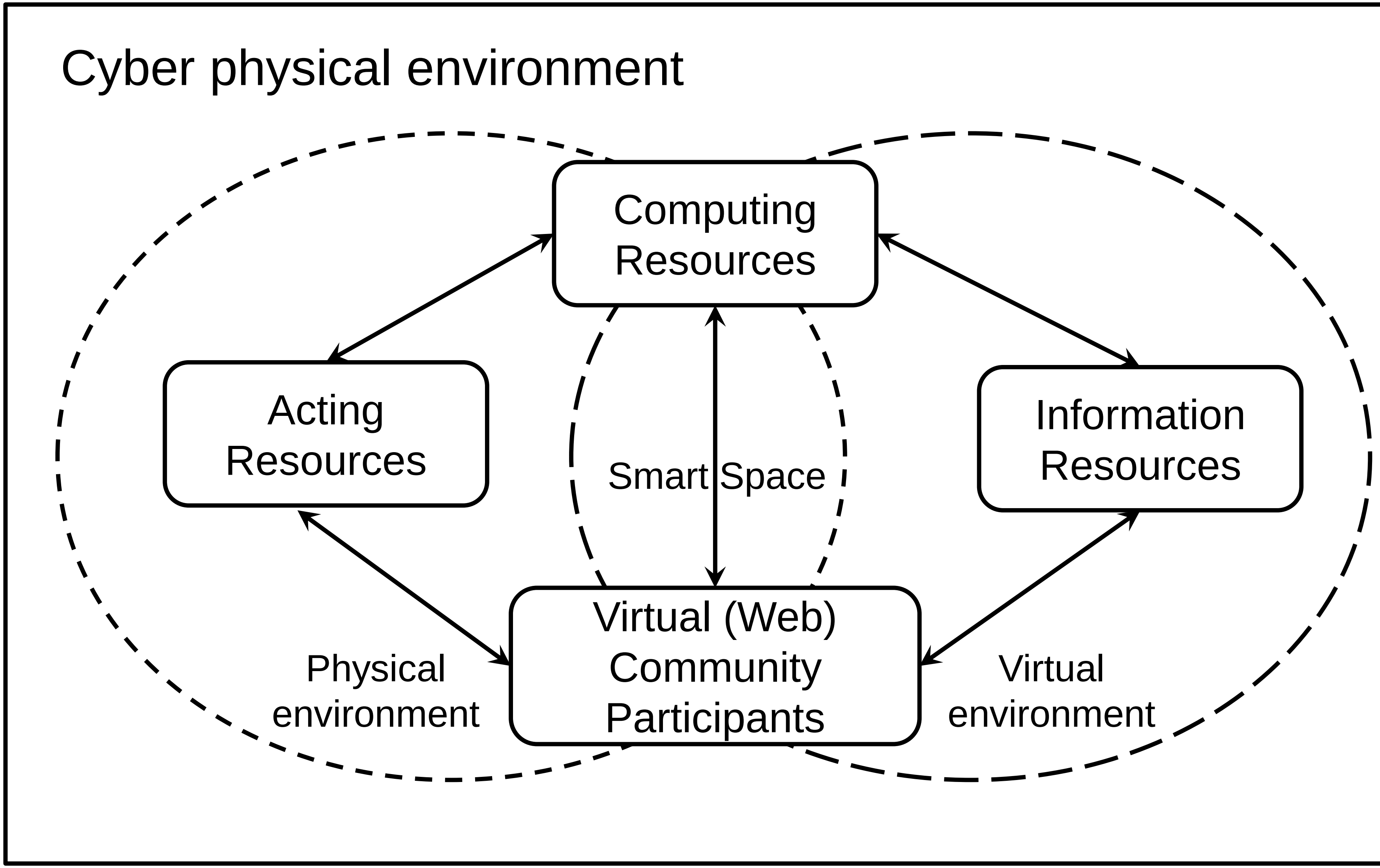
Laboratory of Computer Aided Integrated Systems

St.-Petersburg Institute for Informatics and Automation of RAS (SPIIRAS)

Introduction

- **Motivation**
  - All of the information of smart space is available for every participant
  - Leaks of confidential information are possible
  - An approach to access control for confidential information is needed
- **Table of contents**
  - Smart space as a part of the cyber-physical environment
  - Context based security model
  - Conceptual model of security module
  - Implementation of smart space access control security module

Smart Space



Cyber physical environment
Computing Resources
Acting Resources
Smart Space
Information Resources
Virtual (Web) Community Participants
Physical environment
Virtual environment

The Main Features of Smart Spaces That Affect the Information Security

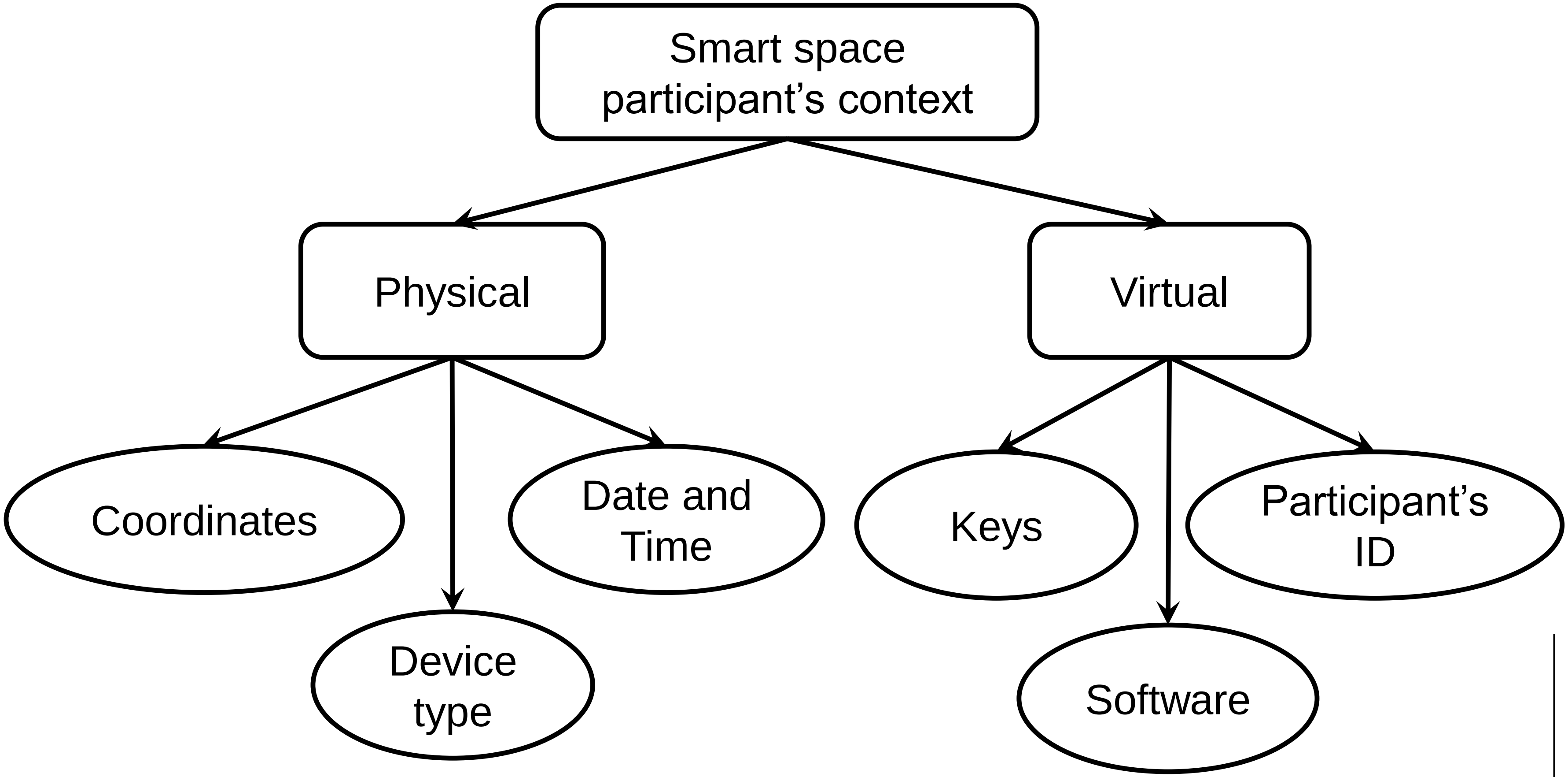
Features	Information Security Problems
Distribution across space devices.	It is difficult to provide access to resources using the existing classical access control models, such as DAC, MAC, and RBAC.
Data privacy and ownership issues	It is hard to trust the shared information, when it is impossible to find its source.
Computational and storage capacities are limited by those of space devices and services (but can extend to clouds)	Devices can be the object of denial of service (DoS) attacks
Great amount of different services in smart space	May include unknown vulnerabilities or backdoors, which may enable access to private information for unauthorized participants
Smart space is personal and user controlled	People can provide access to personal information because of forgetfulness, negligence, carelessness or ignorance

Proposed Security Mechanisms for the Smart Space

Smart Space Specific Features	Security mechanisms
Distribution across user devices	Share encoded information
Ownership issues	Context management
User controlled	Context management

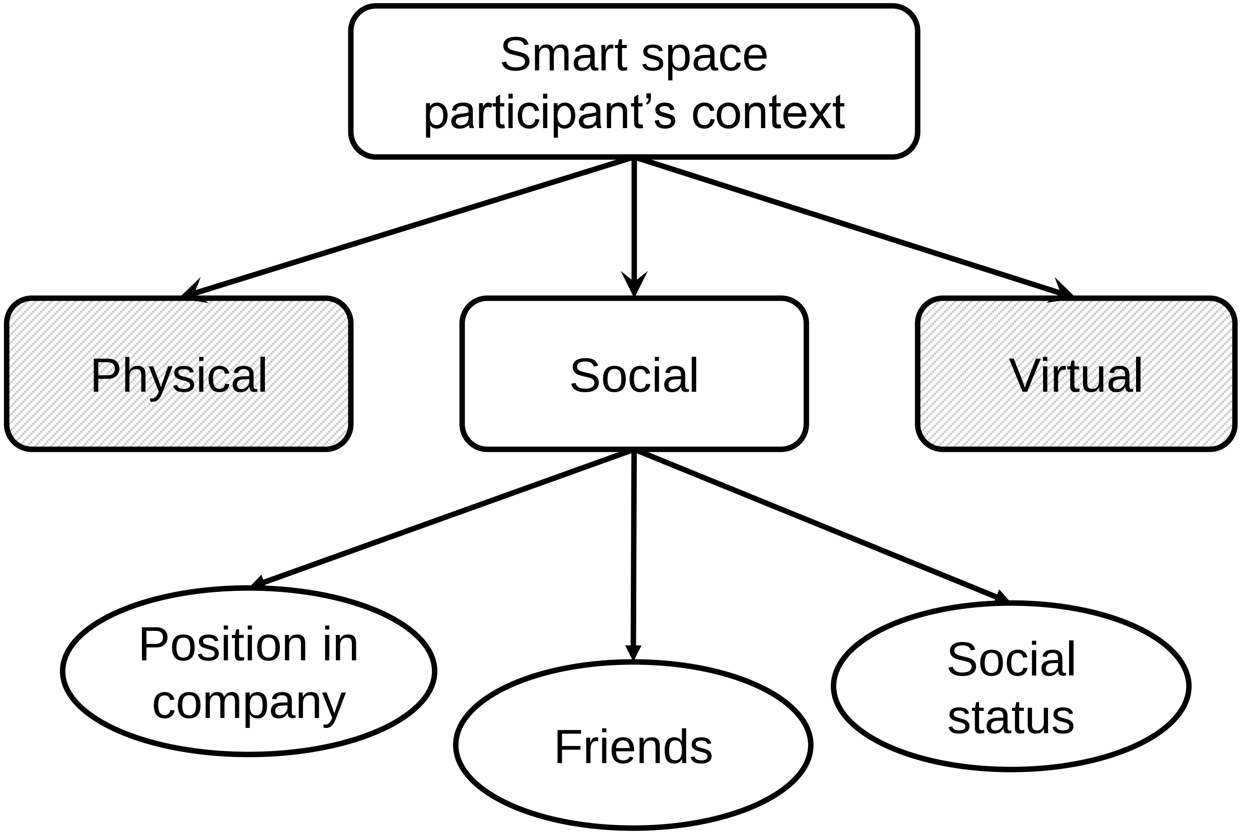
- All these mechanisms require introduction of the identification and authentication techniques for the services which request information. For example, it can be identifier and pair of public and private key for EDS or another authentication technique.

Smart Space Participant’s Context Model (1/2)



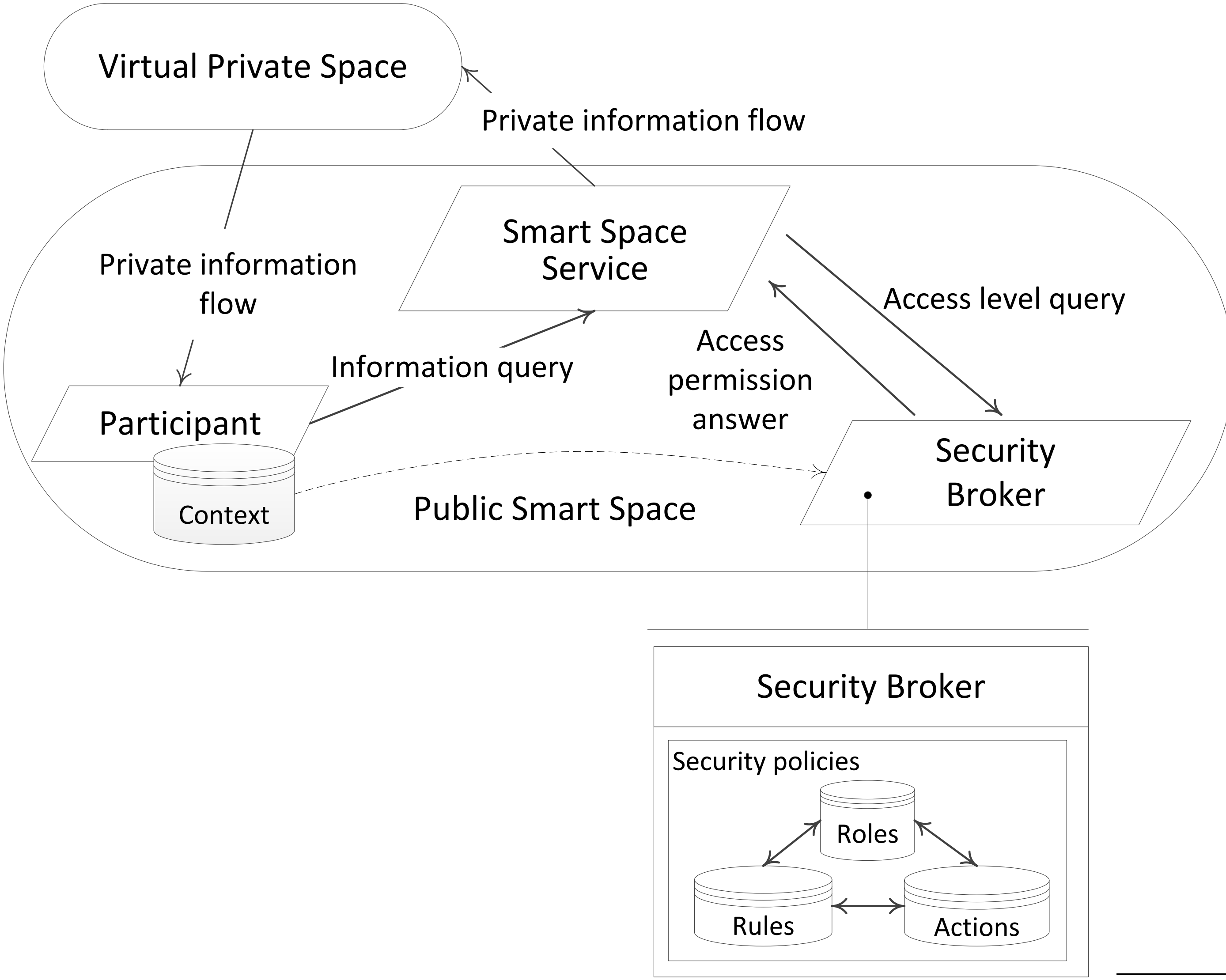
- This variant of context model can be used to describe of any smart space participant.

Smart Space Participant's Context Model (2/2)

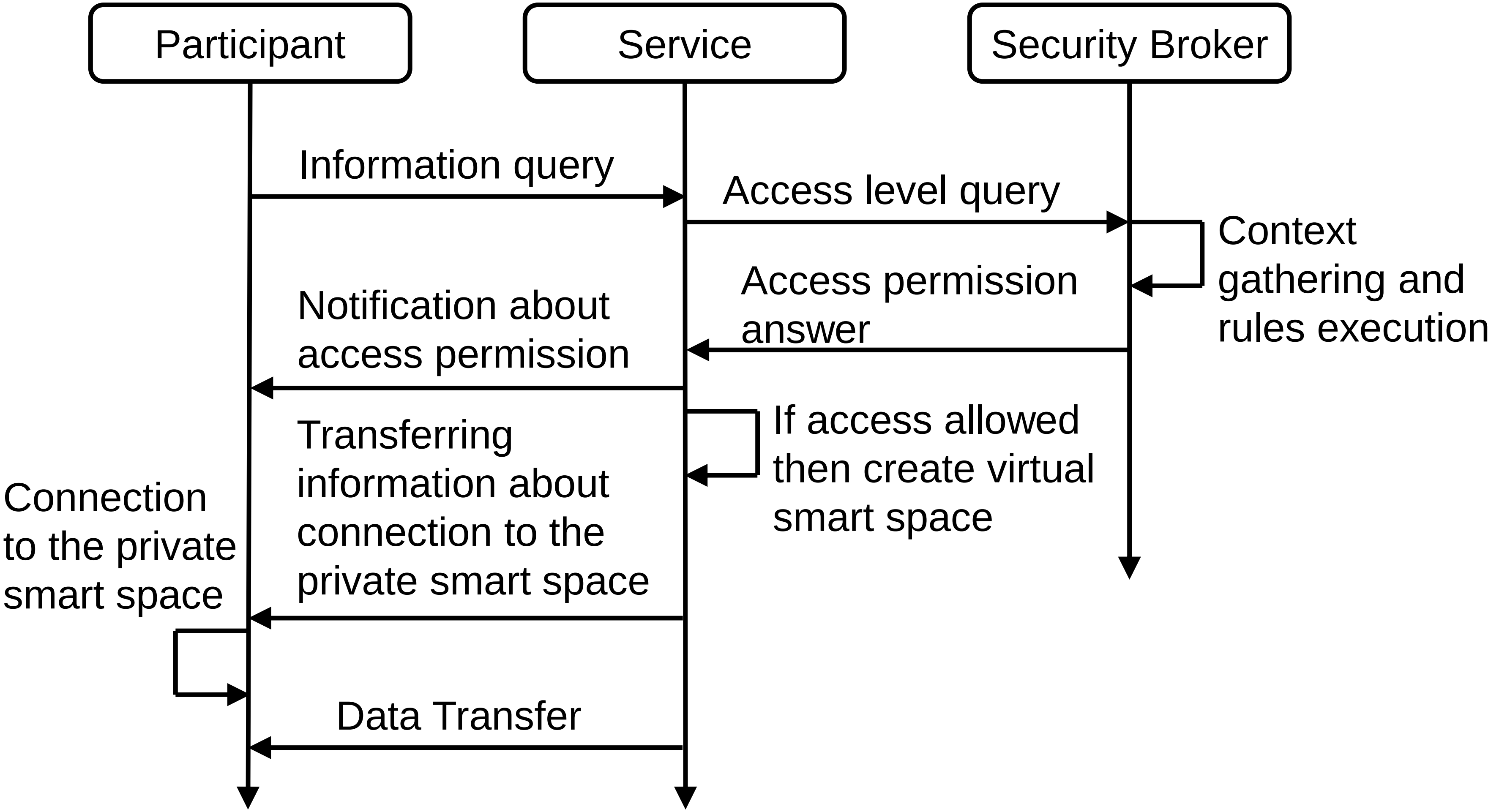


- This variant of context model can be used to describe of smart space participants which is a virtual community members.

Conceptual Model of Smart Space Access Control Module



UML Sequence Diagram of the Information Request Process



Access Control Module Policy Rules

- Policy consists of 3 rule's types:
  1) *TrustValue* rules.
  2) *Assign_role* rules.
  3) *Permissions* rules.

TrustValue Rules

- Used to assign the numeric trust value to the context component.
- Each component of the context is associated with the trust level. The value is represented by a number in the range [0, 1].
- These values depends on the context of the current situation.
- These values are set by the access control service and based on the estimations of the access control service provider’s experts according to the features of the particular smart space service.
- Examples:
    - TrustValue(public_network) = 0.2;
    - TrustValue(“08:00” < current_time < “17:00”) = 0.6;
    - TrustValue(current_time > “17:00”) = 0.1

Assign_role Rules

- The logical function taking into account trust levels of all appropriate context components is used to assign a role to the participant.
- Example:
  - Assign_role(some_rule) = (TrustValue(network) $\in$ (0.8,1)) & (TrustValue(current_time) $\in$ (0.3, 1)) & …

Permissions Rules

- Determines whether a participant with a certain role is allowed to access a particular resource type or not.
- Examples:
    - *Permission(author) = "pdf_read","doc_read", "doc_write";*
    - *Permission(coauthor) = "pdf_read","doc_read", "doc_write";*
    - *Permission(reader) = "pdf_read"*

The Main Parameters of the Access Control Module Working

Parameter	Value
Response time	20 ms
Used RAM	Client software additionally needs 1.1.Mb Access Control Service - 4.5 Мб
Network load	4 additional queries from the client software 3 queries from the Access Control Service

Conclusion

- Usually in smart spaces the information sharing is implemented without any restrictions
- The model proposes a service for smart space which makes access permission for the requested information using predefined rules.
- Model is built on the combination of the role-based and attribute-based access control models.
- All rules are human readable form and easy to set up in a fairly wide range.

Thank you for Attention
Questions are Welcome

E-mail: teslya@iias.spb.su