deepsia

Dynamic on-linE intErnet Purchasing System Based on Intelligent Agents

Dealing with Security within DEEPSIA Project

Francisco Milagres
Edson Moreira
João Paulo Pimentão
Pedro A.C. Sousa
Adolfo Steiger-Garção

WSEAS International Conference on Information Security 2002

October 15th , Rio de Janeiro, Brazil.

Outline

deepsia

- DEEPSIA's Overview
- Multi-Agents System (MAS) Security Analysis
- MAS Security Models
  - KQML – ACL Security
  - Split and Merge
- MAS Security Analysis Conclusions
- Future works

DEEPSIA Consortium

deepsia

USP Universidade de São Paulo
BRASIL

ICMC-USP Instituto de Ciências Matemáticas e de Computação

NUMA Núcleo de Manufatura Avançada

COMARCH

UNINOVA Instituto de Desenvolvimento de Novas Tecnologias

ZEUS CONSULTING S.A.

Atlante

ULB

University of Sunderland

Supported by

CNPq 50 ANOS

ist information society technologies

http://www.deepsia.com

Project Objectives

deepsia

DEEPSIA Project

Dynamic on-linE IntErnet Purchasing System based on Intelligent Agents

Assist **Small and Medium Enterprises** in the e-**commerce process** of **finding** the **most suitable offer** for their needs.

SME will find a user-friendly process for overcoming:

- **Individual purchases of items at "best" costs**
- **Finding new suppliers**

Business to Business (B2B) e-commerce models usually **focus** on **SMEs** as **suppliers** (virtual shops or marketplaces).
DEEPSIA's aim is the opposite.

Generic characteristics

deepsia

Purchaser-centred solution

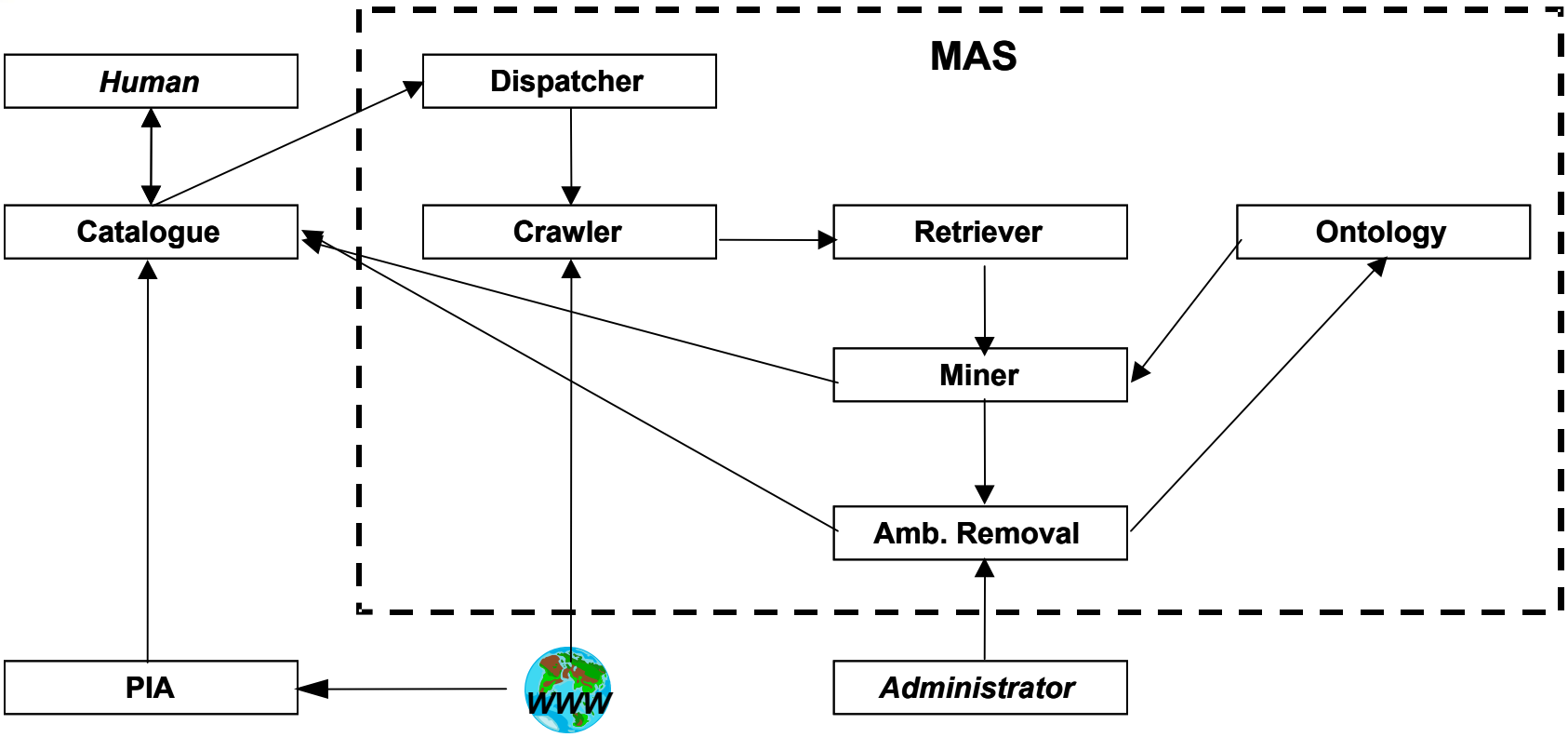
- Tailored to individual requirements
- User-friendly web interface based on a **purchaser-personalized catalogue**

The catalogue

- **Automatically updated** with information gathered from available e-business portals
- Set of **intelligent agents** which will look for data on the Web and process it

DEEPSIA's Architecture

deepsia



Security needs and approach

deepsia

Needs

Anonymity: the capacity to hide the final client from the queries he/she is performing;

Confidentiality: assure that the contents of the messages being exchanged remain hidden;

Reliability/Integrity: assure that the messages arrive intact as they left their origin;

Authentication of the sender: assure that the originator was who it was supposed to be;

Access Control: to the information beign exchanged;

Availability: of the whole system.

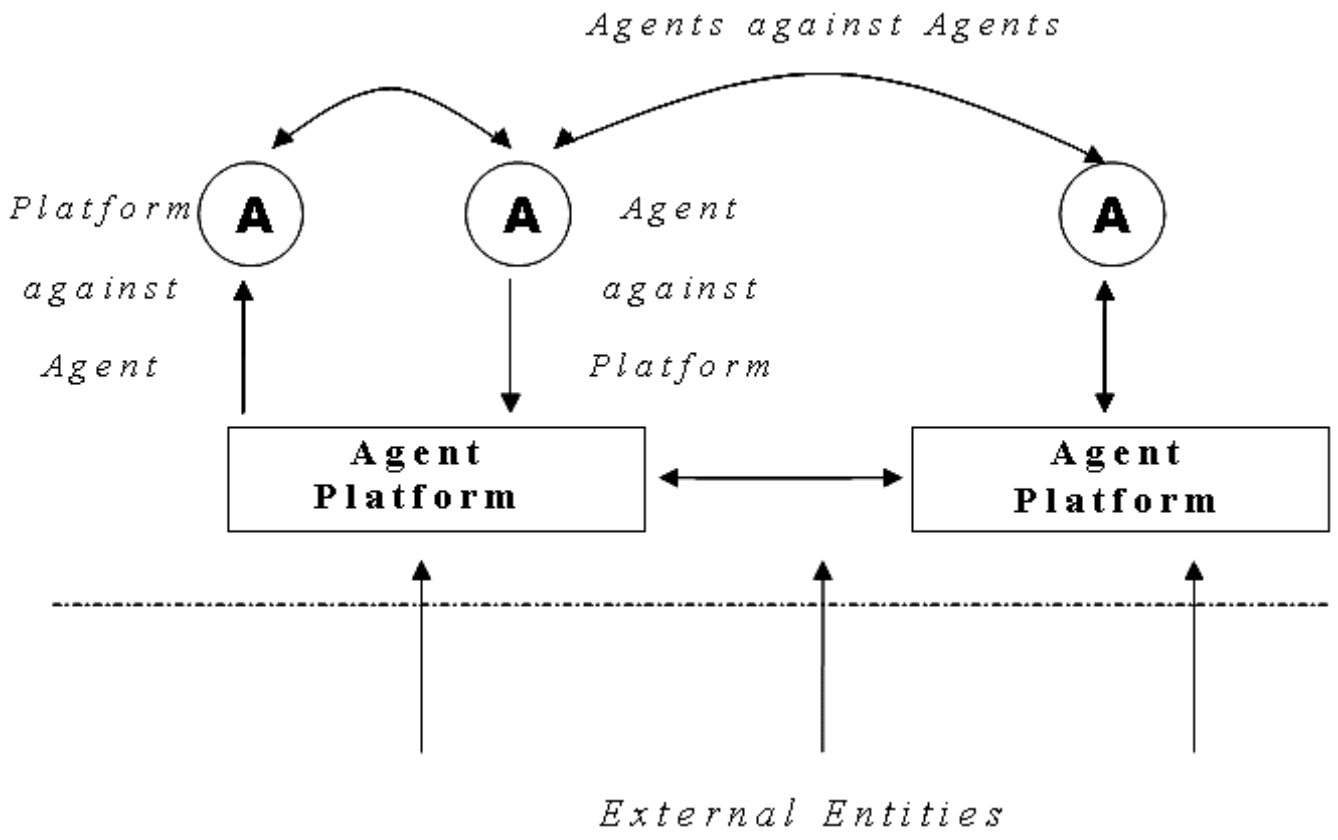
Security developments:

- *Agent Communication Lang. Security:* KQML – ACL Security, by USP
- *Message content Security:* "Split and Merge", by UNINOVA

MAS Security Analysis

deepsia

- "*DEEPSIA's MAS Security Analysis*" shown the main **threats** against **agents systems**



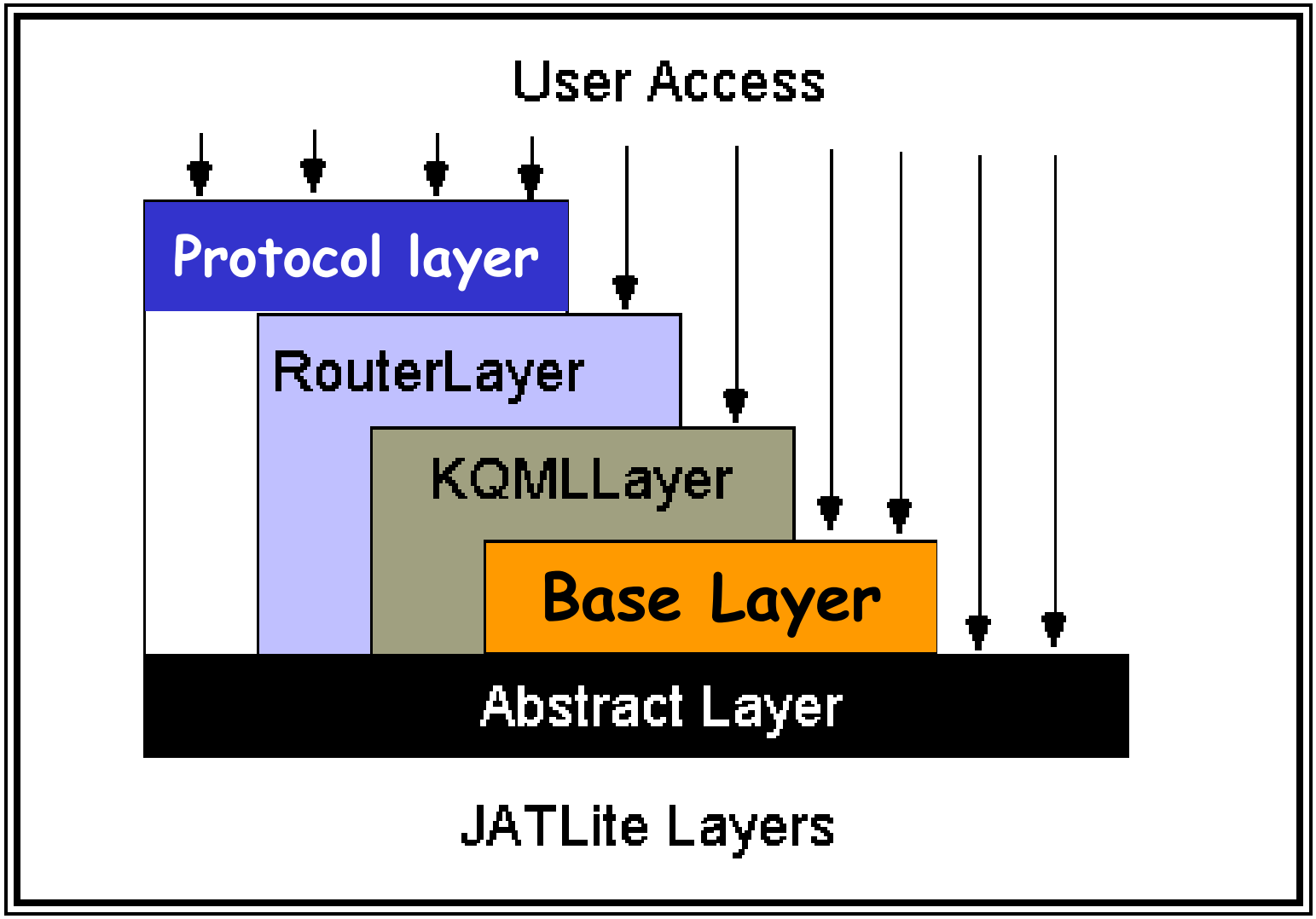
ACL Security approach

deepsia

- Based on ***Secret Agents*** proposal Finin *et al* (UMBC, 1995)
- Changes to **KQML Agents Communication Language (ACL)** in order to improve its *authentication of message sender*, *message integrity* and *privacy of data* capabilities
- Security functions implemented on **JATLite**, the KQML speaking agents platform

JATLite Layers focused

deepsia



The Split and Merge approach

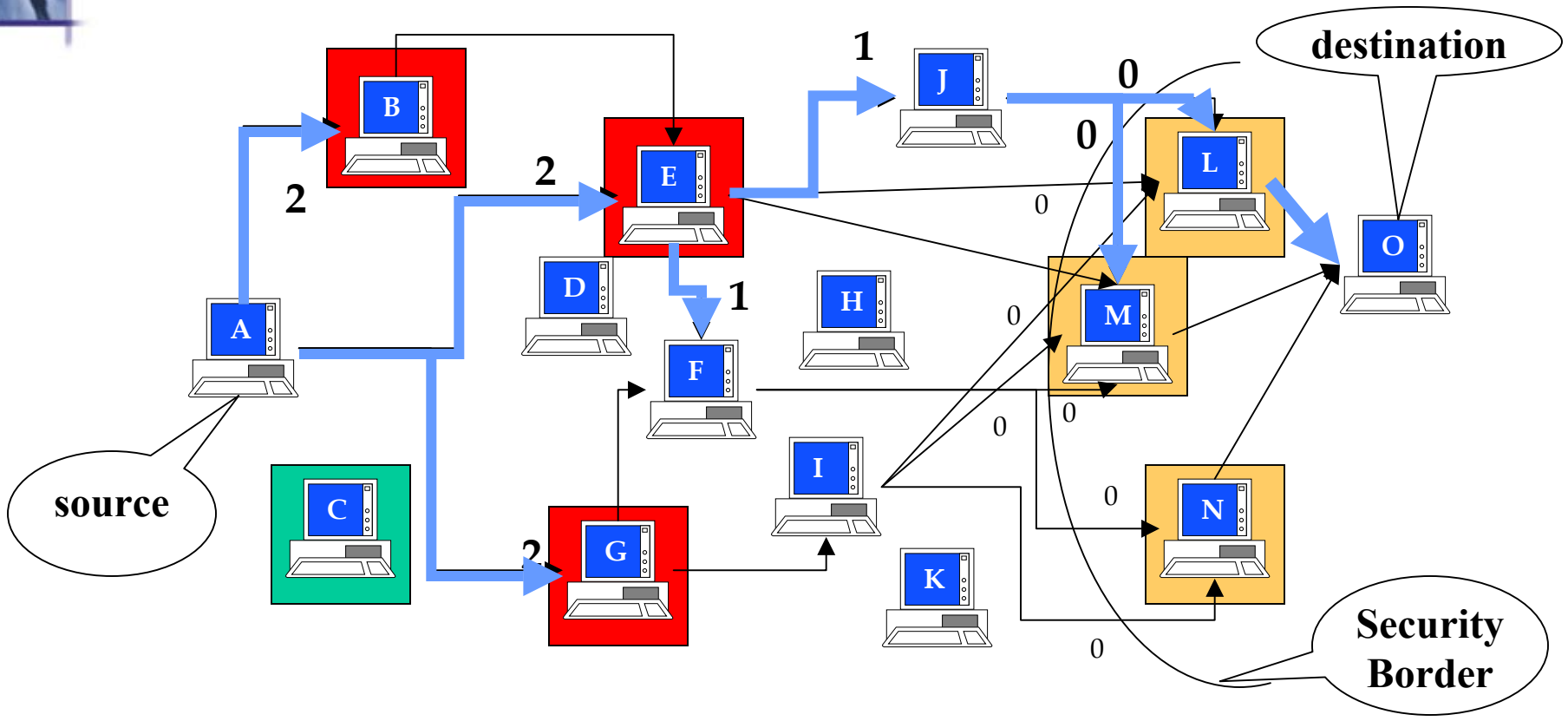
deepsia

In short:

- Split the message into fragments
- Send them through different paths
- Repeat the splitting at each node
- Reassemble the message at the destination

Split and Merge

deepsia



Faced problems

deepsia

- KQML Agents Communication Language is **outdated** and was supplanted by a new standard (**FIPA, *Foundation for Intelligent Physical Agents***)
- **JATLite** project at Stanford University and its researches were **stopped** and there is no new information about improvements on it **since 2000**
- Specific security requirements **were not defined** on original DEEPSIA Project

MAS Security Analysis

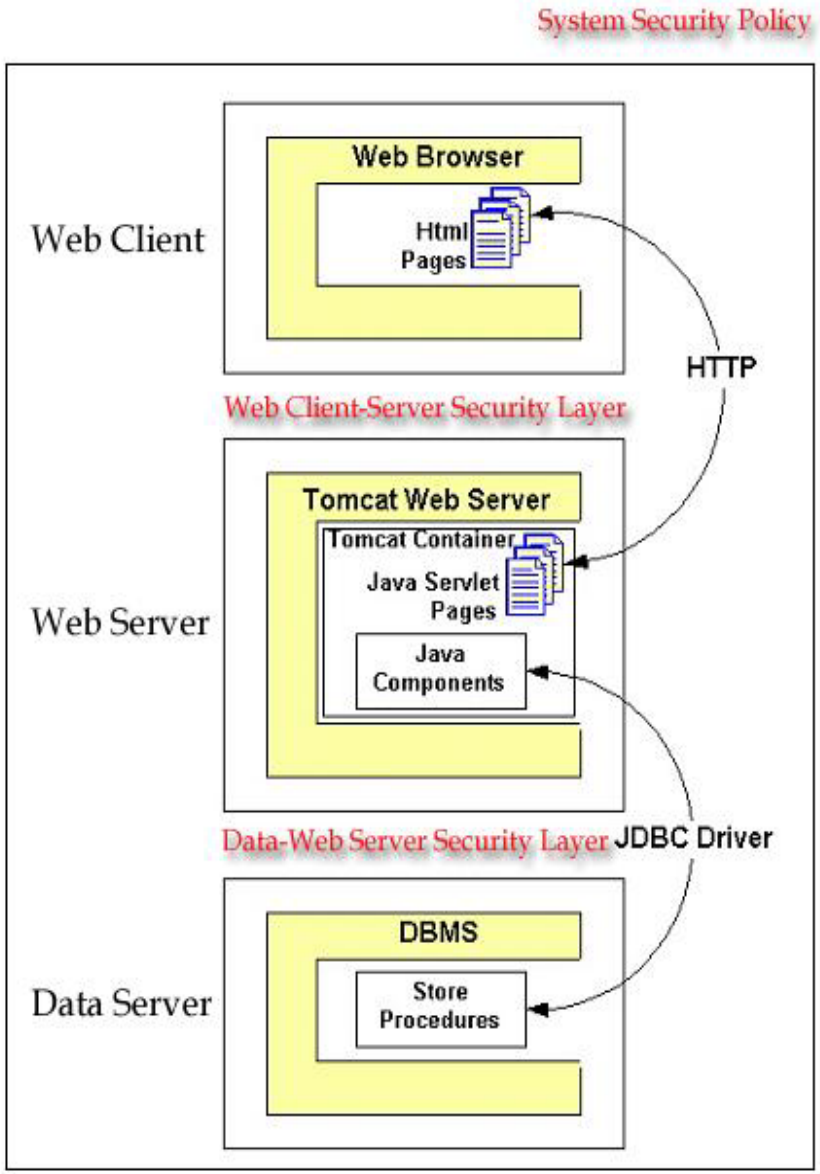
deepsia

- Conclusions of this analysis:
  - There are **security issues** on agents communication language that must be **reviewed**
  - The **KQML agents communication language** and its **messages router (JATLite)** are *outdated*
  - The **proposed model** for **KQML Security** is valid but not applicable if considered that **KQML+JATLite are not supported**

Security - future work (1/2)

deepsia

- Definition of **specific security requirements** regarding the full DEEPSIA System security and its interfaces within users and agents, using an International Security Standard (**ISO 17799**)



Security - future work (2/2)

deepsia

- **Agents Communication Language** (ACL) ***substitution*** for a better security management (**FIPA** instead of **KQML**)
- Implementation of a **hybrid security model** with a default and secure ACL in partnership with other Research Groups (e.g. **AgentCities.NET** — IST-2000-28384)

Further information

deepsia

http://www.deepsia.com

Francisco Milagres

francisco @ milagres . com