



ICMC-USP

**deepsia**

Dynamic on-line intErnet Purchasing System Based on Intelligent Agents

# *Implementação de Segurança no Sistema DEEPSIA*

*Francisco Gomes Milagres*



- O Sistema DEEPSIA
- Análise de Segurança do Sistema Multi-Agentes System (MAS)
- Resultados e publicações da análise
- Implementação do modelo proposto
- Conclusões
- Trabalho atual
- Trabalhos futuros

# Consórcio DEEPSIA

deepsia



ICMC-USP



Universidade de São Paulo  
B R A S I L



ICMC-USP

Instituto de Ciências Matemáticas e de Computação



Núcleo de Manufatura Avançada

COMARCH



UNINOVA

Instituto de Desenvolvimento de Novas Tecnologias

ZEUS CONSULTING S.A.



Atlante

ULB



University of  
Sunderland

Supported by



## Projeto DEEPSIA

Dynamic on-line Internet Purchasing System based on Intelligent Agents

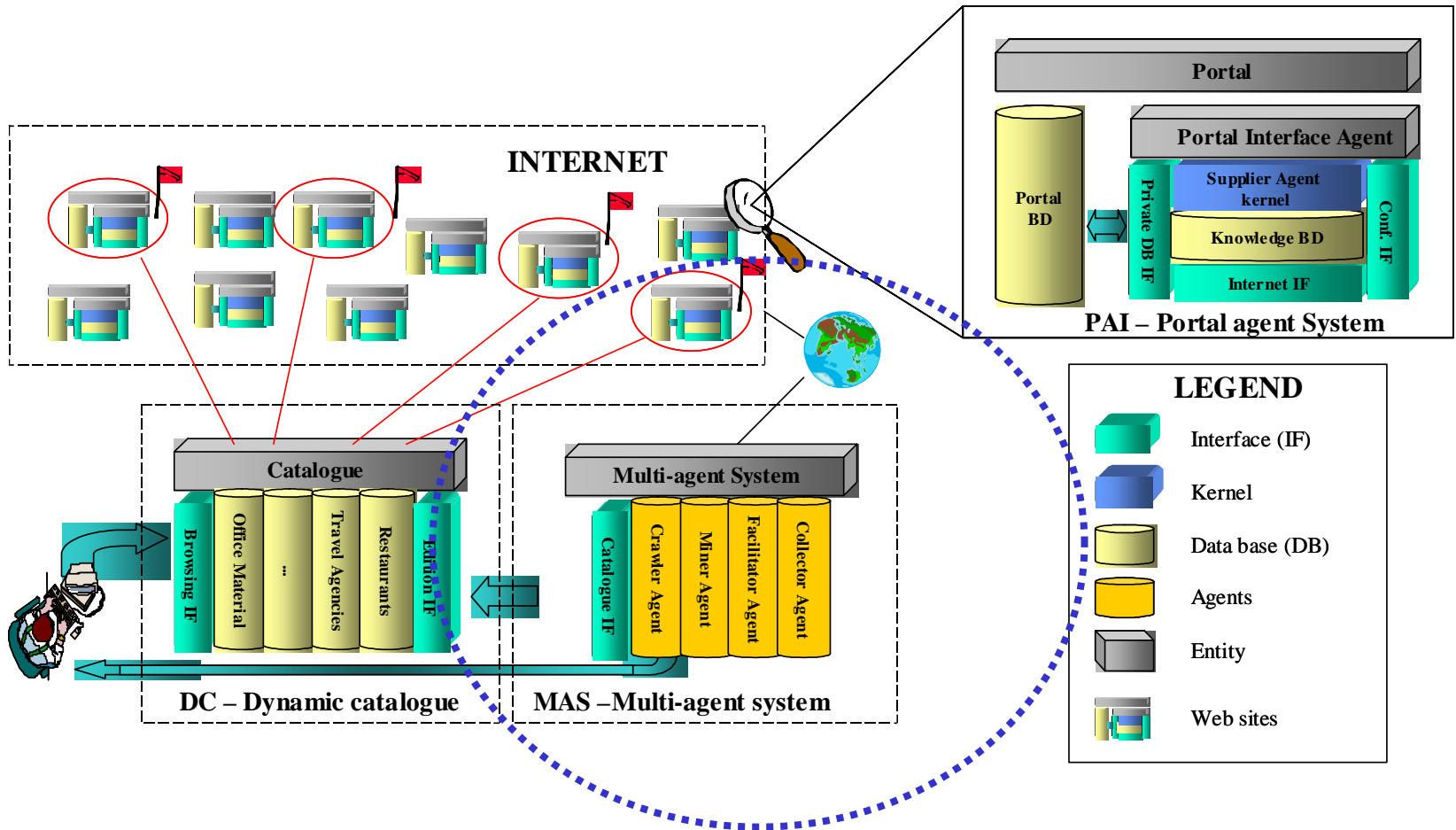
Auxiliar **Pequenas e Médias Empresas (PMEs)** em processos de **busca de ofertas** direcionadas em **comércio eletrônico**.

As **PMEs** encontrarão processos auxílio para:

- **Resultados de melhores condições de preço e pagamento**
- **Busca de fornecedores em *sites* da rede ou em parceiros**

O modelo de comércio eletrônico **Business to Business (B2B)** geralmente trata as **PMEs** como **fornecedores**  
O **foco** do DEEPSIA é o **comprador**.

# Arquitetura do DEEPSIA

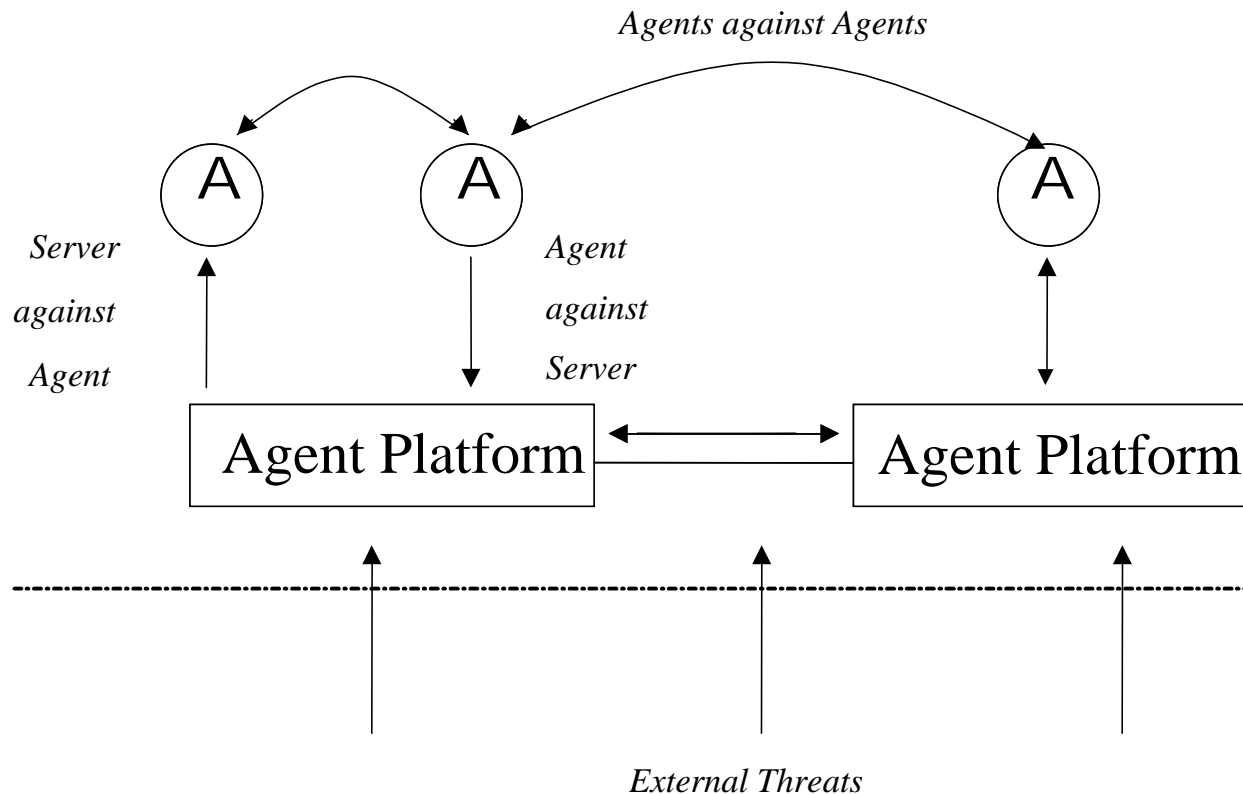


# Requisitos de Segurança



- ▶▶ *Privacidade*
- ▶▶ *Confidencialidade*
- ▶▶ *Integridade*
- ▶▶ *Autenticação*
- ▶▶ *Controle de Acesso*
- ▶▶ *Disponibilidade*

- “DEEPSIA’s MAS Security Analysis” destacou as principais vulnerabilidades







- Funções de segurança implementadas em **JATLite**, a plataforma de comunicação de agentes
- Alterações na **Agents Communication Language** para permitir *autenticação, verificação de integridade e privacidade*
- Baseada em **Secret Agents**, proposta por Finin *et al* (UMBC, 1995)





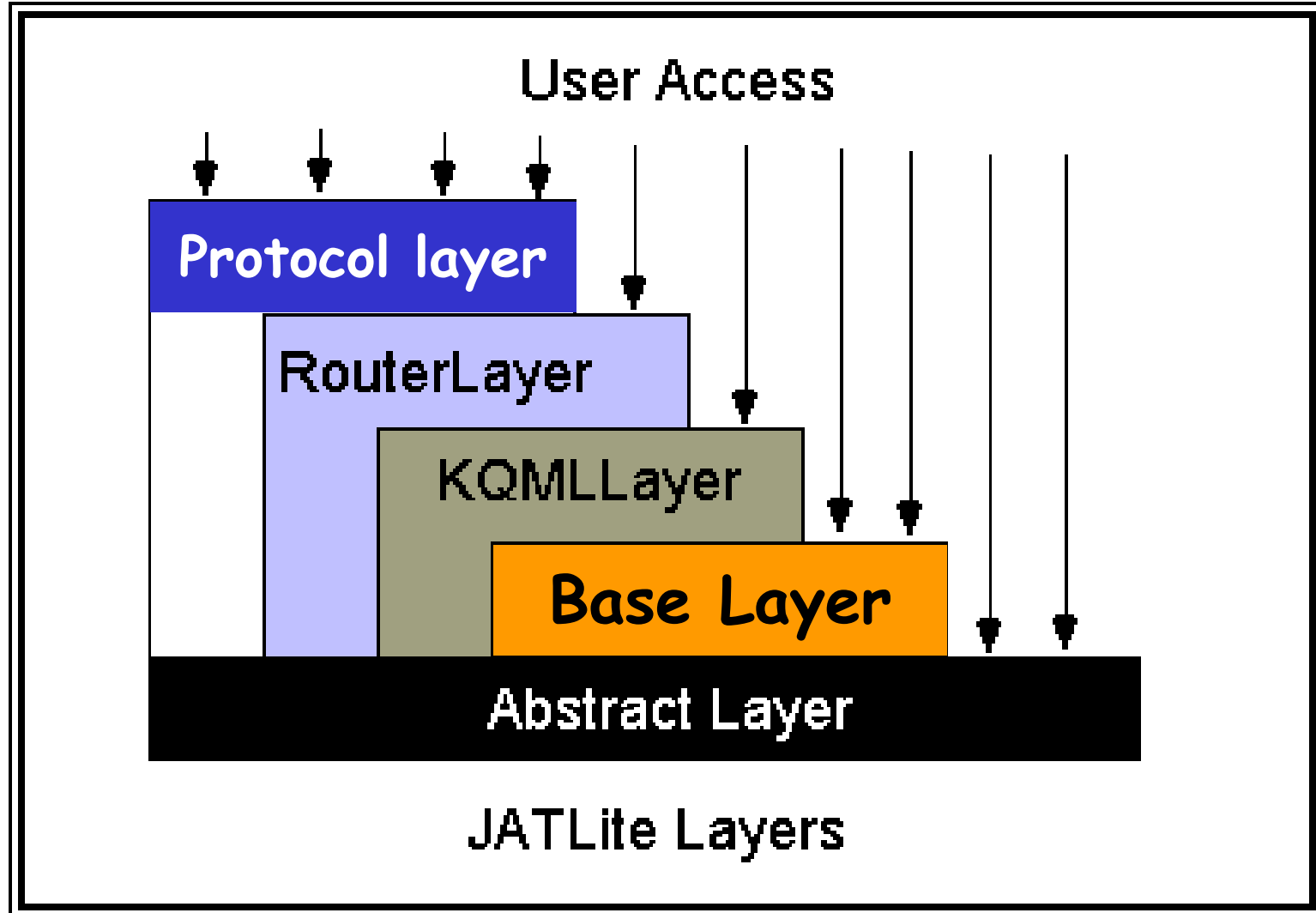
# Resultados da 1ª etapa

deepsia

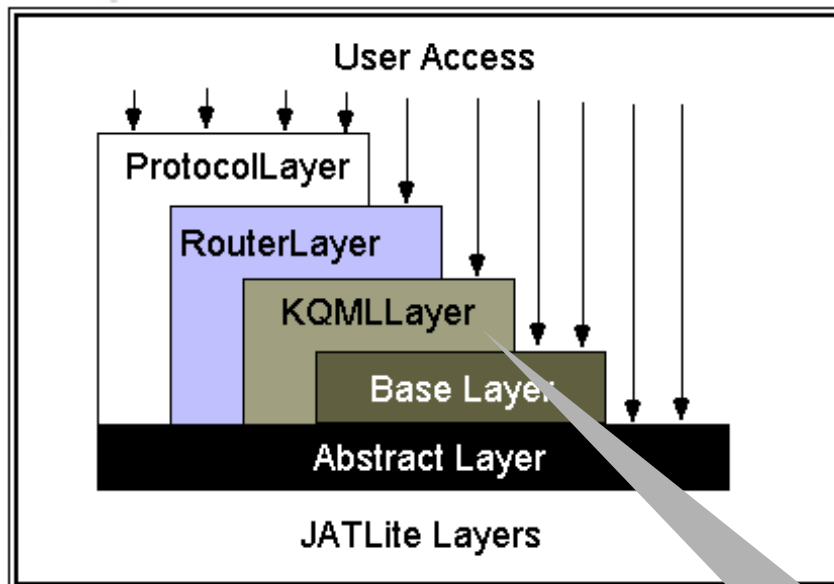


ICMC-USP

- Divulgação dos resultados da “Análise de Segurança do Sistema DEEPSIA”
  - ▶▶ WSEAS International Conference on Information Security 2002
  - ▶▶ First International Seminar on Advanced Research in E-Business
  - ▶▶ Módulo Security News
  - ▶▶ AgentCities.NET Security Workgroup Meeting (Lisboa)



# Implementação



auth-private

:sender Agent\_A

:receiver Agent\_B

:auth-key K

:auth-digest

(<digest-type>

<encrypted-digest>)

:content <KQML-msg>

**Base & KQML  
Layers**

(key <sending-agent>  
<receiving-agent>  
<master-key?>  
<key-type>  
<encrypted-key>)

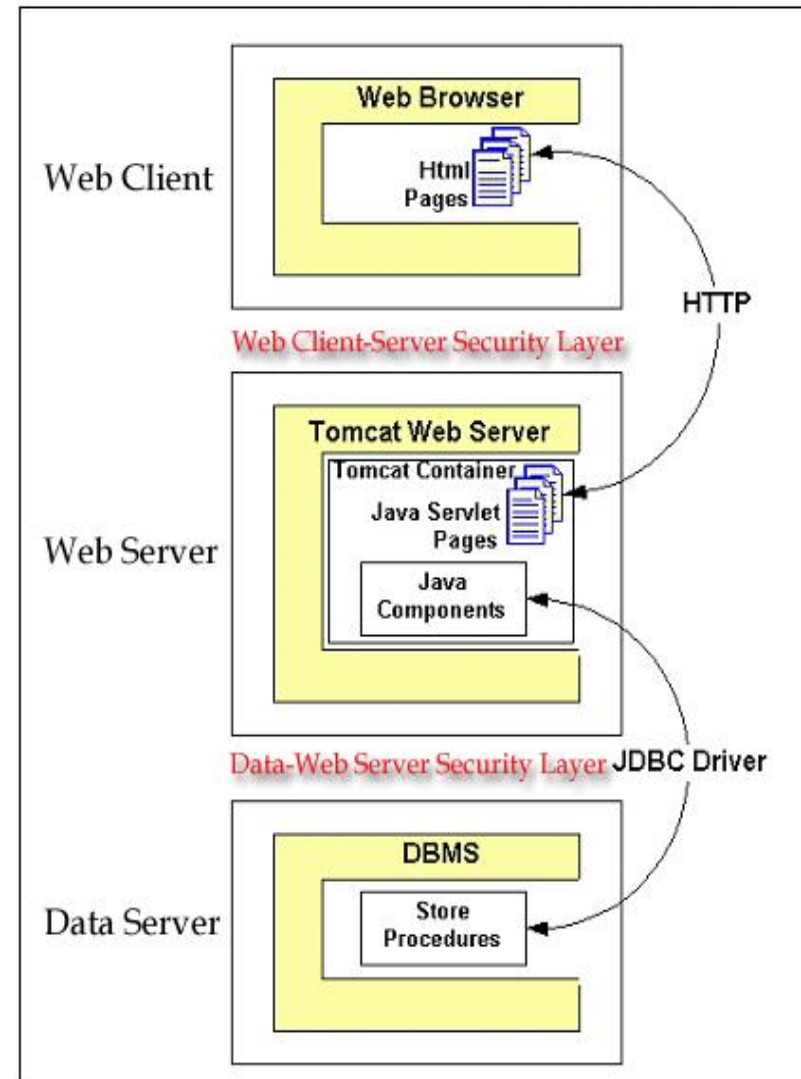


- Substituição dos agentes **KQML** por **FIPA** para a versão brasileira do sistema DEEPSIA
- Implementação de um sistema híbrido de segurança em conjunto com grupos de pesquisa em agentes na Europa (Consórcio **AgentCities.NET**)

# Trabalho futuro

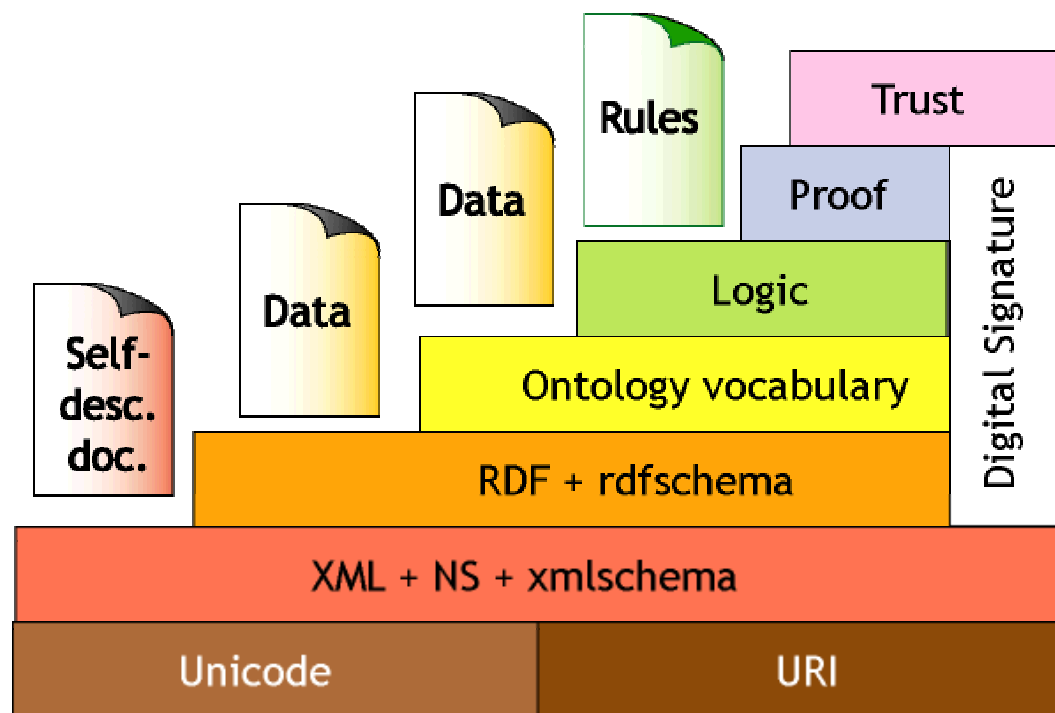


- Definição de requisitos de segurança específicos para o DEEPSIA segundo o padrão ISO 17799 de segurança



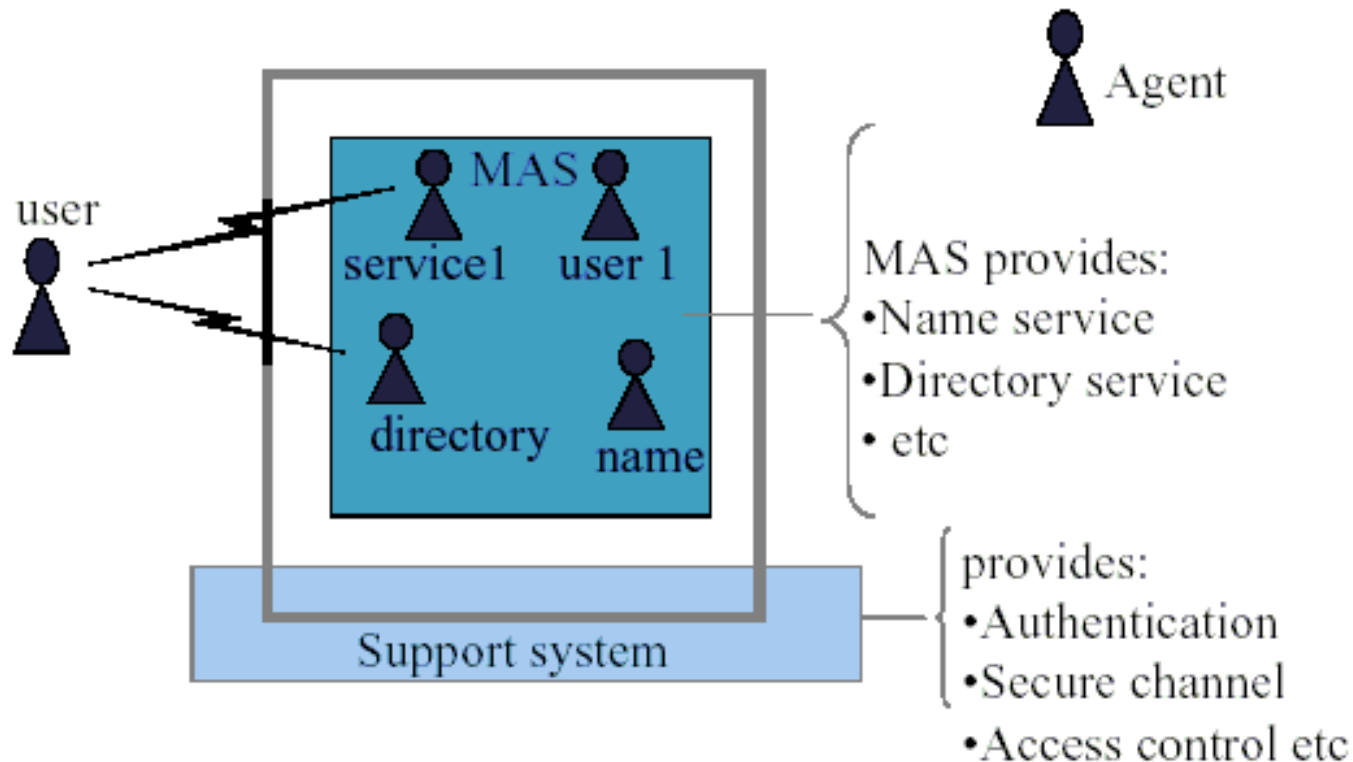
# Trabalho futuro

- Implementação dos requisitos do padrão de segurança **ISO 17799** em formato semântico





- Aplicação de política de segurança padrão **ISO 17799** em um sistema como o DEEPSIA







**deepsia**

<http://www.deepsia.com/br>

**Francisco Milagres**

milagres @ icmc.usp.br