Secure Inter-communication in Multi Agent System

Gianpiero Costantino

miniWorkshop on Security Frameworks

12 December 2006

Intelligent Agent

- **Agent definition**
  - **Object programming**: a set of passive objects that interact between them through an invoker/invoked relation
  - **Agent programming**: a set of active agents that interact between them through a p2p logic

Main characteristics

- **Goal Oriented**: an agent is programmed in order to pursue a goal
- **Autonomous**: an agent must complete its goal independently
- **Situated**: an agent woks in platforms

Obligatory characteristics for an agent

Intelligent Agent
Other characteristics

- **Reactive**: an agent reacts on the base of events that happen in the platform
- **Proactive**: an agent is able to elaborate action plans in order to obtain the goal
- **Social**: an agent is able to communicate with other agents
- **Mobile**: an agent is able to move in other platforms

Agent Platform

Two fundamental agents:

- Directory Facilitator (DF)
- Agent Management System (AMS)

Communication of the Agents

- Agent communication with ACL Message
- Most important items:

```
(inform
      :sender       (sender@platform.net)
      :receiver     (receiver@platform.net)
      :language     (FIPA-SL0)
      :content      („Text to be signed“)
```

Security in MAS

- It is inevitable to ensure security today
- Integrity, authenticity and privacy
- The existing security systems in MAS bring some disadvantages

Attacks

- Passive attacks: monitoring of network packets from malicious agent
- Active attacks : replay attacks, spoofing attacks and modification of messages

MAS needs security

Goals

- Possibility to secure not the whole ACL message but only some of its parts.
- Not to bind the security support tightly into the agent platform
- To avoid agent's core necessity to choose, set type or negotiate about algorithms used in secure communication
- All private keys and other security related data have to be available only to their owner

X-Security Prototype

- In the proposed system the function of the central authority is exerted by the **Security Certification Authority** (SCA)
- **SCA** releases certificates to agents

Certificates

- The agents use their certificates to prove their identities and to execute security related to their actions within the system
- The certificates contain mandatory information requested by SCA and they may contain additional information supplied by an agent

Certificates .2

- certificate-ident — SCA_CERTIFICATE_1
- sca-ident — (agent-identifier :name sca@platform.net)
- agent-ident — (agent-identifier :name testAgent@platform.net)
- time-from — Wed Jan 01 00:00:00 CET 2003
- time-to — Wed Dec 31 23:59:59 CET 2003
- security-level — VISITOR
- key-description
  - ident — SIGN_1
  - time-from — Wed Jan 01 00:00:00 CET 2003
  - time-to — Wed Dec 31 23:59:59 CET 2003
  - type — public-key
  - key-param — SHAwithDSA/1024
  - key-value — 56A7ED89C2……6AC54DF983
- key-description
  - ident — CRYPT_1
  - time-from — Wed Jan 01 00:00:00 CET 2003
  - time-to — Wed Dec 31 23:59:59 CET 2003
  - type — public-key
  - key-param — RSA/1024
  - key-value — 5A234DC82B……85329B76DC

Integration of Security into the message

- The message is extended to contain a new slot called **X-Security**

```
(inform
      :sender       (sender@platform.net)
      :receiver     (receiver@platform.net)
      :language     (FIPA-SL0)
      :content      („Text to be signed“)
      :X-Security   (    :type SIGN
                         :signature 48A7……20AD
                         :certificate-ident SCA_CERTIFICATE_1
                         :key-ident SIGN_1 ) )
```

Integration of Security into the message .2

- Now, X-Security slot items inform that the message content is encrypted ...

```
(inform
      :sender        (sender@platform.net)
      :receiver      (receiver@platform.net)
      :language      (FIPA-SL0)
      :content       („28AD……7BA4“)
      :X-Security    (     :type CRYPT
                           :certificate-ident SCA_CERTIFICATE_1
                           :key-ident CRYPT_1 ) )
```

Description of SCA's activity

- What does it happen when SCA fails? ...

Description of SCA's activity

- What does it happen when SCA fails? ...

...security still works!

Protected information exchange

- It usually happens through asymmetric keys but if there is a huge amount of data:
  - Symmetric session keys can be used
  - After session keys will be removed

Agent key Replacement

- It generates new keys (public and private)
- A new certificate must be created by SCA
- But what does it happen when an agent uses an old certificate?

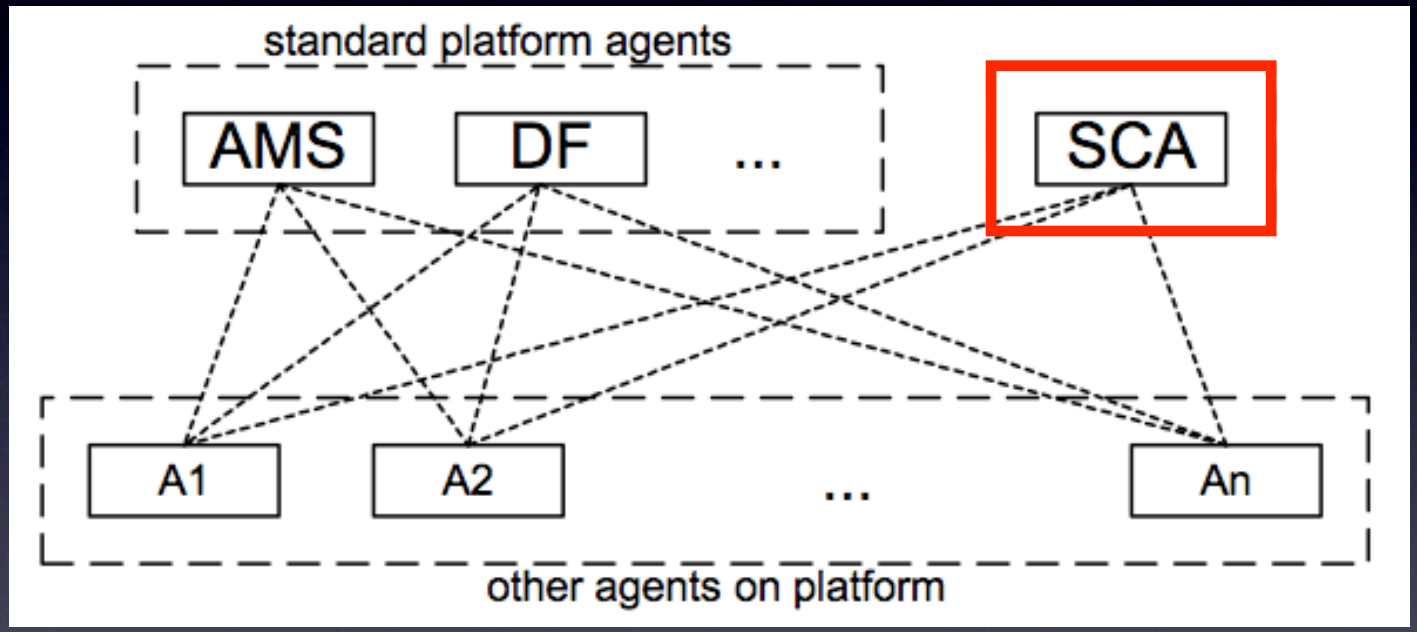
SCA key replacement

1. It generates new keys and a new certitificate
2. It sends its new certificate to the agents
3. It sends original certificates signed by the new key.

SCA Inaccessibility

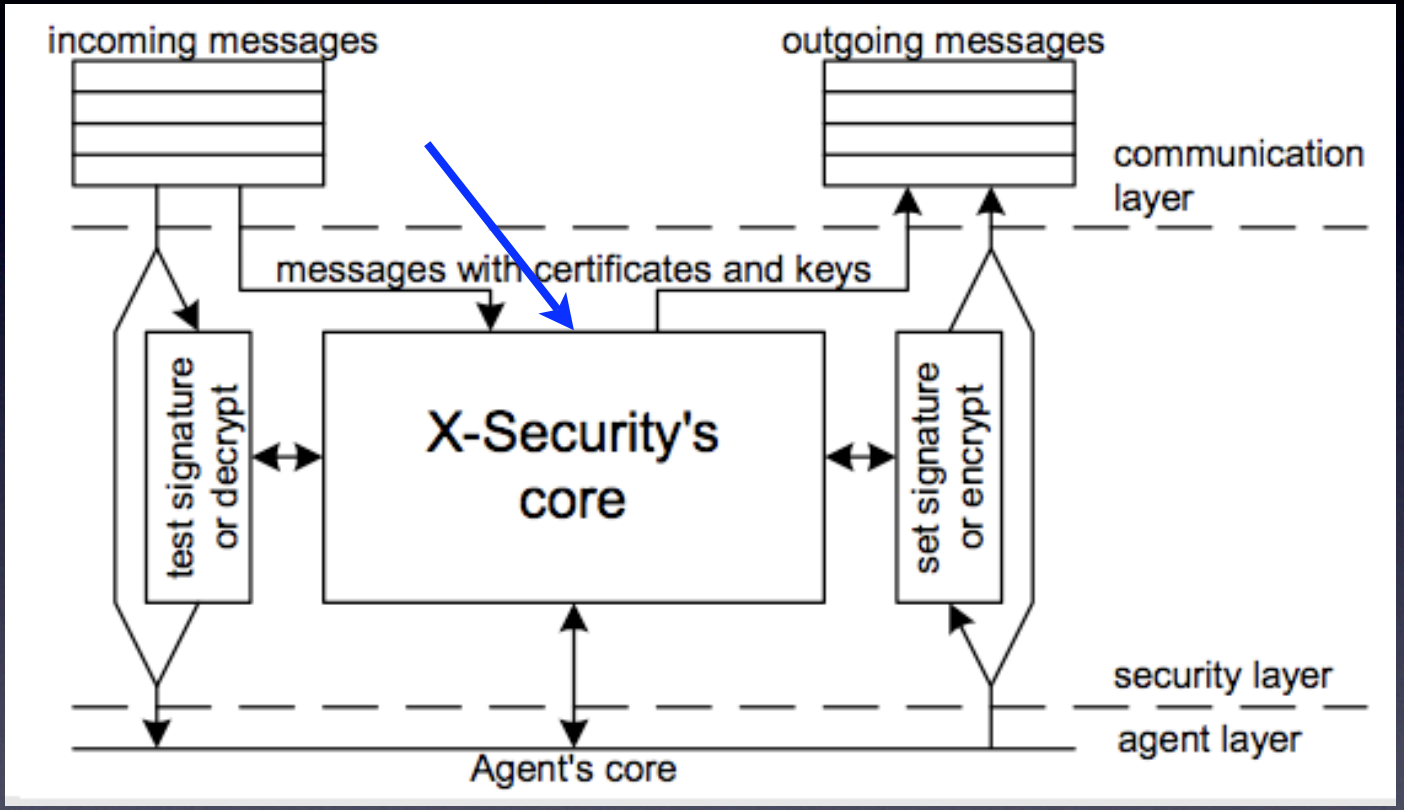
- It recovers itself from backup
- More SCA in the plattforms
- New SCA must generate new keys and a certificate for itself

Implementation



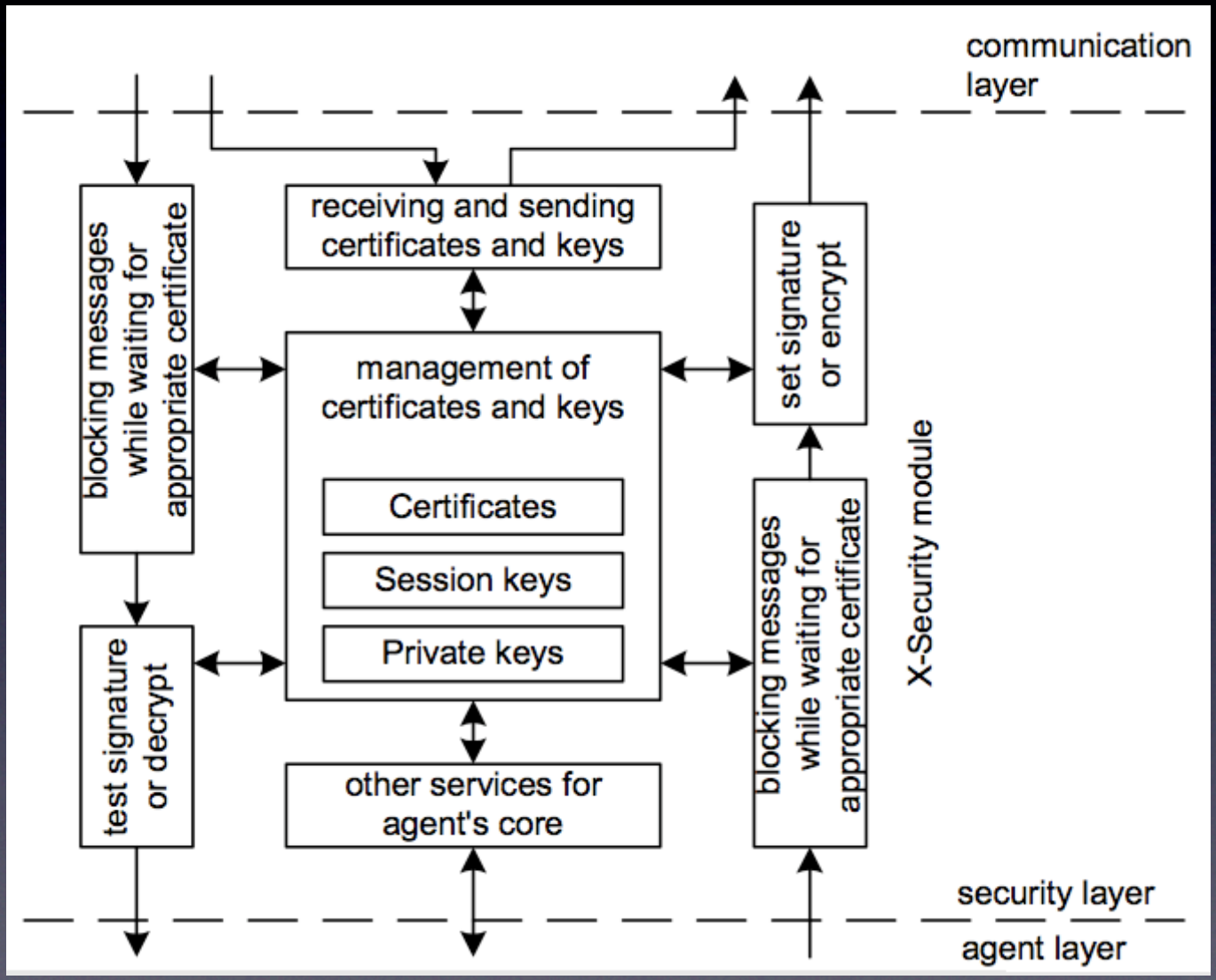
Agent platform with Security Certification Authority

Implementation .2



Integration of security module to agent

Implementation .3



Conclusions

- X-Security system is appropriate for MAS applications
- This system tries to avoid troubles during SCA inaccessibility
- Developed libraries, included SCA agent and security module, have been implemented in JAVA as an extension of JADE

References

1. **Communication Security in MAS**:

   Peter Novaàk, Milan rollo, Jiri Hodik, Tomas Vleek

2. **FIPA** http://ww.fipa.org

   Foundation for intelligent Physical Agents

3. **JADE** http://jade.cselt.it

   Java agent DEvelopment Framework

THE END