An Agent-based Framework for Identity Management The Unsuspected Relation with ISOIEC 15504 _ presentation

Gateau, Benjamin; Feltus, Christophe; Aubert, Jocelyn; Incoul, Christophe

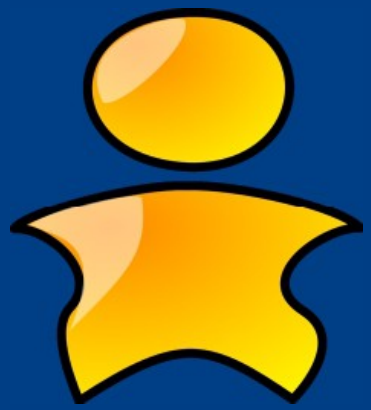
Publication date:
2008

Document Version
Peer reviewed version

CENTRE DE RECHERCHE PUBLIC
HENRI TUDOR
www.tudor.lu

IEEE International Conference on
Research Challenges in Information Science
RCIS 2008

An Agent-based Framework for Identity Management: The Unsuspected Relation with ISO/IEC 15504



Benjamin Gâteau, CRP Henri Tudor
Christophe Feltus, CRP Henri Tudor
Jocelyn Aubert, CRP Henri Tudor
Christophe Incoul, CRP Henri Tudor

June 3-6, 2008 – Marrakech, Morocco

Outline

- Context
- SIM Project
- Policy engineering
- Policy deployment
- Multi-Agent Platform

Context

- SIM stands for « Secure Identity Management »

- R&D project
  - Achieved in collaboration with the University of Luxembourg.
  - Funded by the National Research Fund Luxembourg.

- Main goals:
  - Make right management closer with business objectives
  - Automate the policies deployment

Context

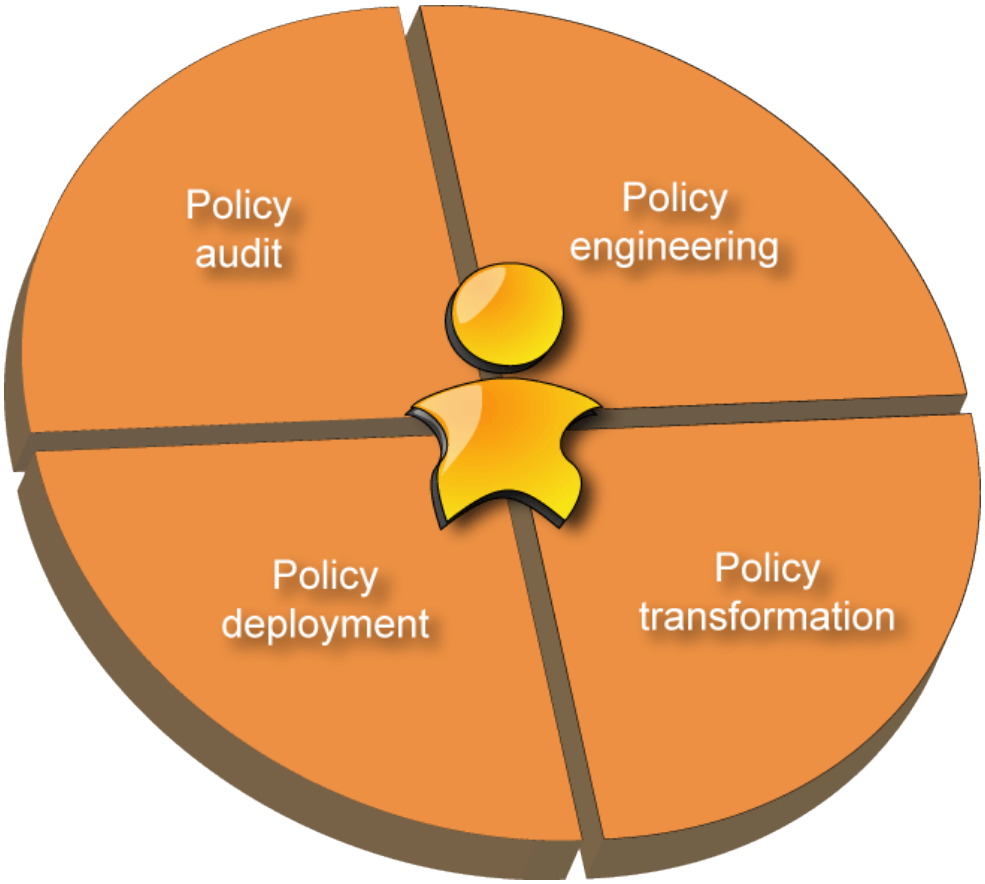
- Motivations:
  - Challenge to develop a Federated Identity Management.
    - Difficult to integrate heterogeneous applications to heterogeneous organizations
  - Existing IAM solutions are (most of time) monolithic, proprietary and non-flexible.

SIM Project

- Objectives:
  - Define responsibility concept.
  - Innovative policy engineering.
  - Develop a prototype for managing,deploying,maintaining and auditing access control policy.
  - Multi-agent system-based deployment.
  - Privilege open-source components and technologies.

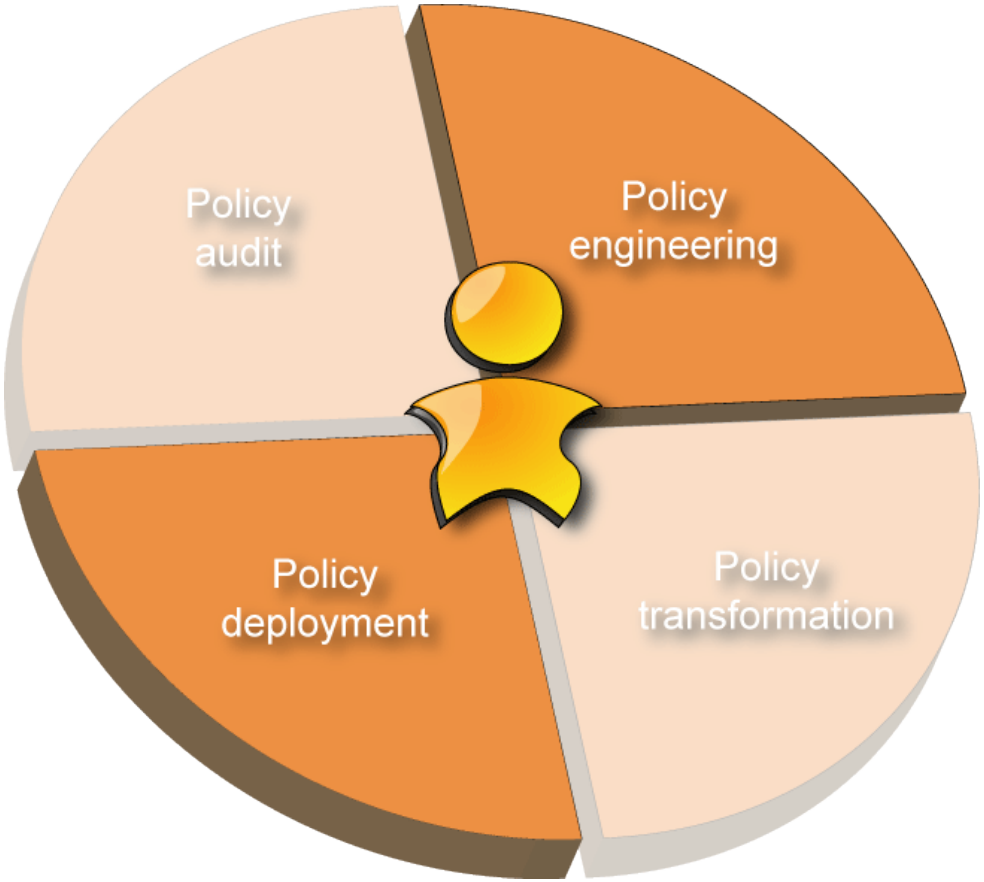
SIM Project

- Secure Identity Management



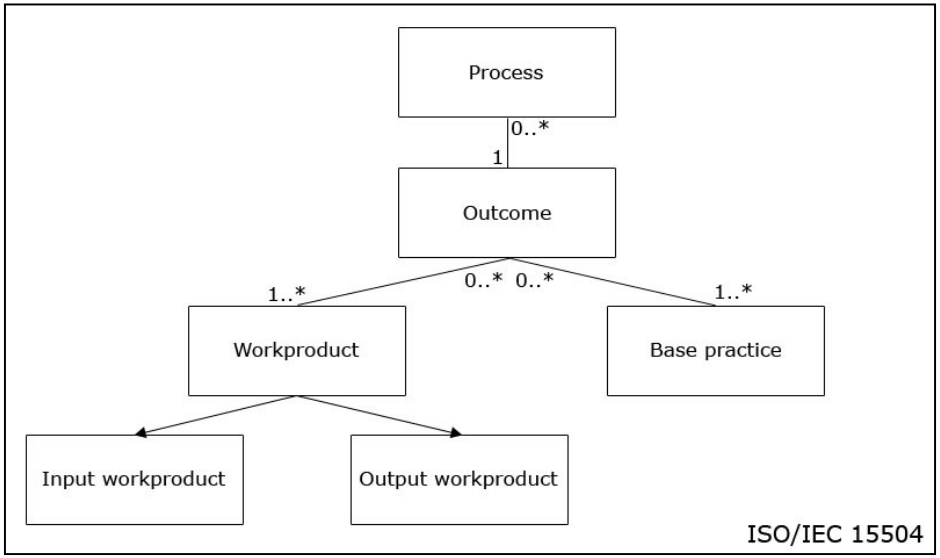
SIM Project

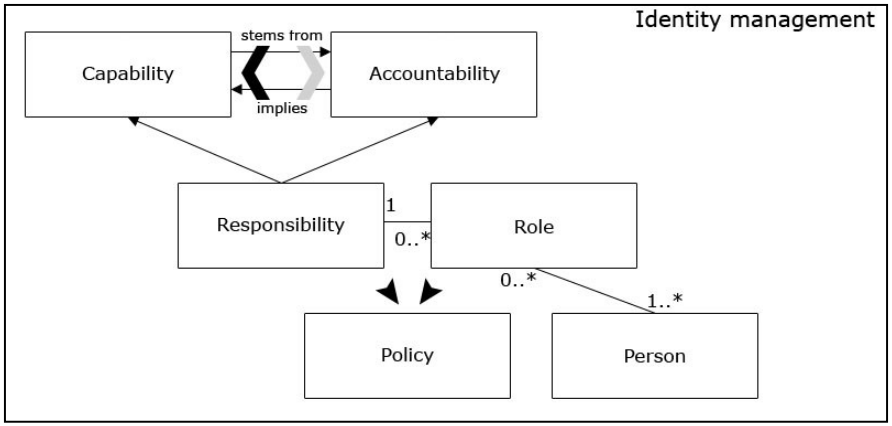
- Status:



Policy engineering

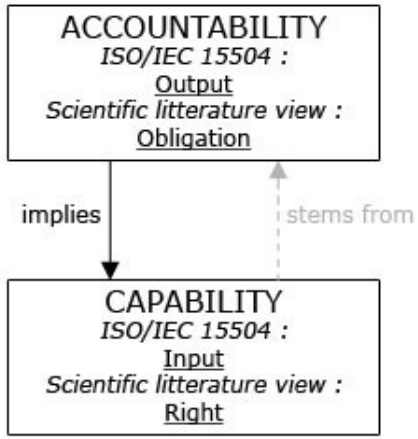
- Process-Oriented Policy Engineering
  - Combining responsibilities components to ISO/IEC 15504 concepts.



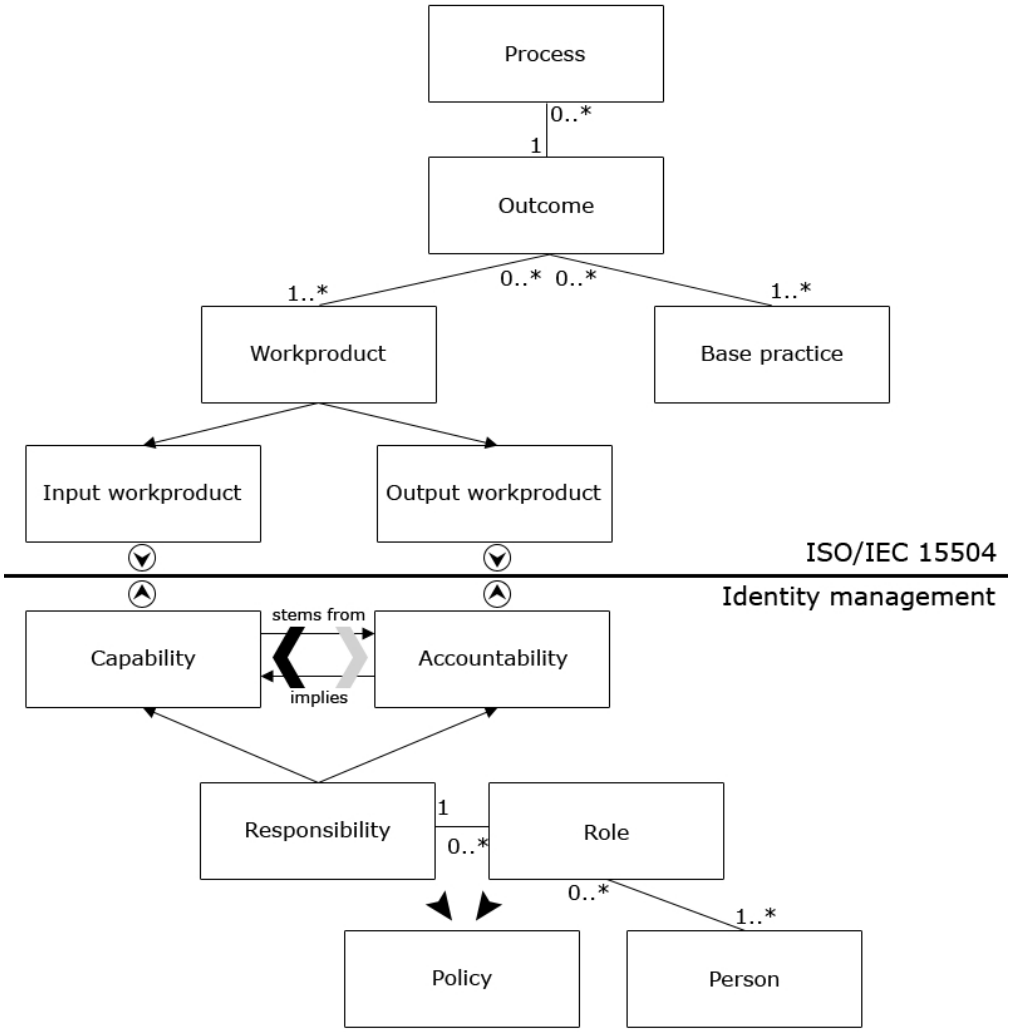


Policy engineering

- Combining responsibilities components to ISO/IEC 15504 concepts.
  - *Input Workproduct:*
    - Right for a stakeholder to perform a activity
    - → *Capability*
  - *Output Workproduct:*
    - Stakeholder's obligation to issue an activity
    - → *Accountability*



Policy engineering



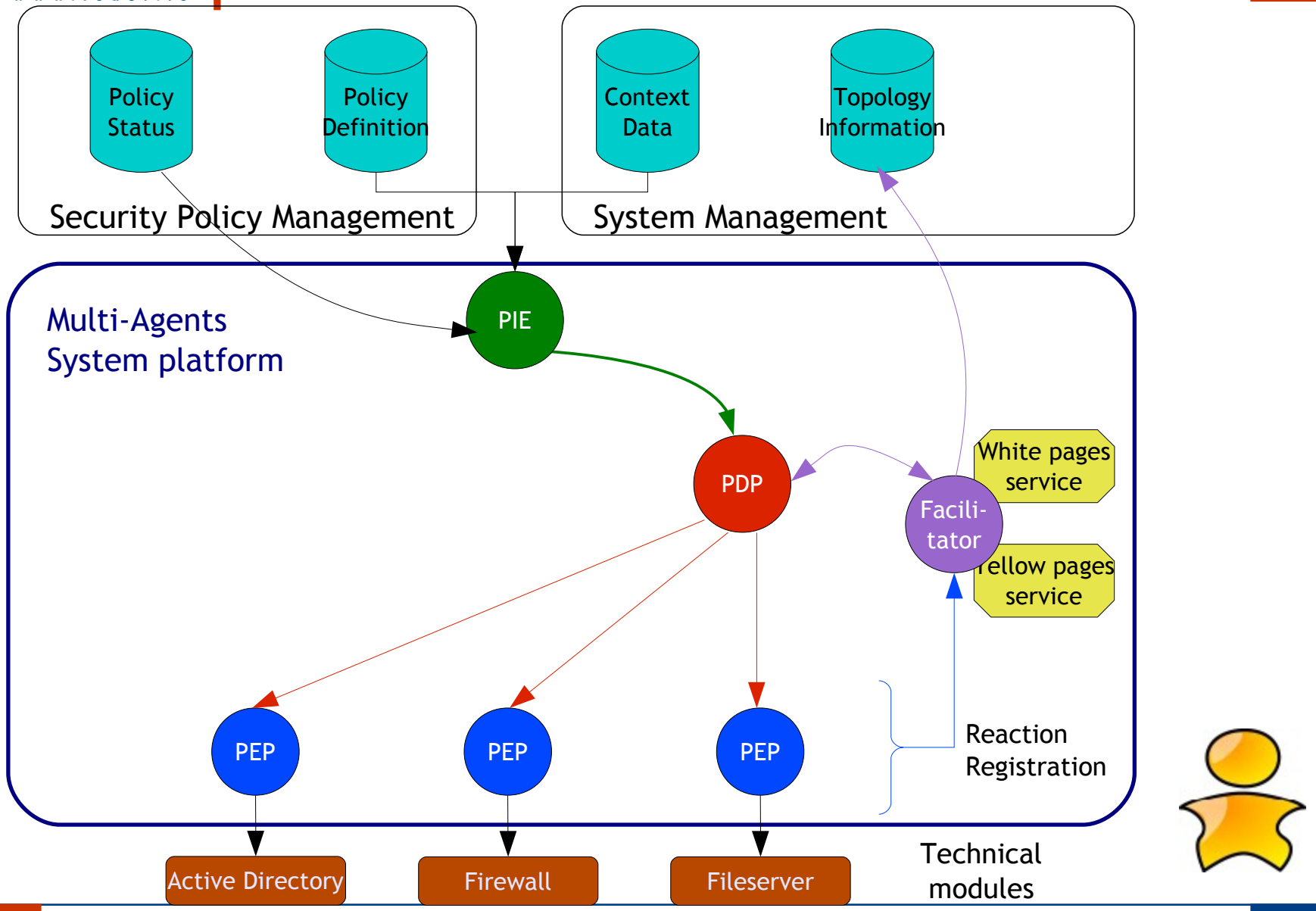
- Conceptual connection between ISO/IEC 15504 and Identity management concepts.
- Policy transformation
  - XACML format

Policy deployment

- Goal: apply policy on devices (fileserver)
  - Find all the devices concerned by the policy's rules.
  - The rules must be sent to the technical modules.
  - Each received rules must be transformed into script or command.
  - Specific scripts or commands must be executed .

- Agent-based policy deployment
  - Multi-Agent System (MAS) :
    - Several agents capable of mutual interaction,
    - Agents are proactive, reactive and social autonomous entities,
    - Agents are able to exhibit organized activity to meet their objectives.

Policy deployment



Policy deployment

- Policy Instantiation Engine (PIE)
  - Interface between Policies and the agents.
  - Instantiates the business process (policies) regarding to some context data and policies instantiation.
  - Detects policies changes.
  - Sends modified policies (to apply) to PDP agent.

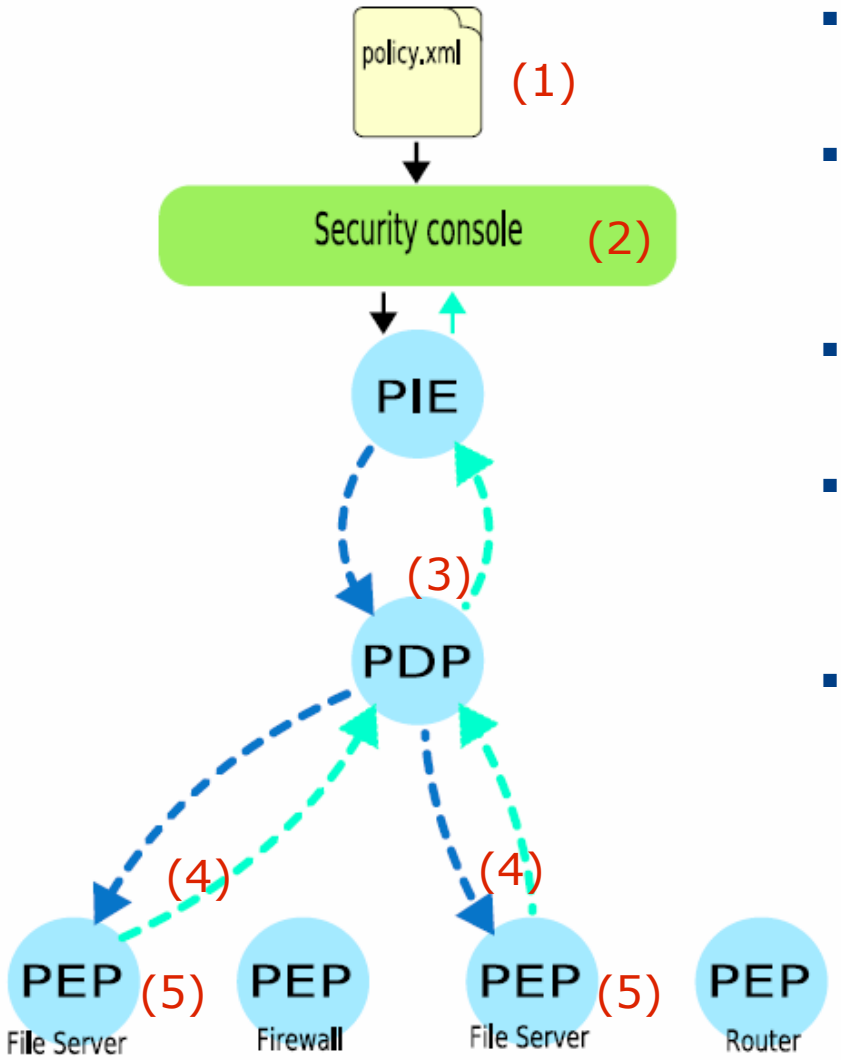
Policy deployment

- Policy Decision Point (PDP)
  - Determines PEP agents concerned by the policies (with Facilitator agent help):
    - By localization (IP address, MAC address…),
    - By policy application capability (firewall, fileserver…).
  - Sends policies to concerned PEP.

Policy deployment

- Policy Enforcement Point (PEP)
  - Must manage each device being part of SIM's technical layer.
  - Specific to the kind of devices or services offered by the device.
  - Transforms policies from abstract policy description format (e.g. XACML) in applicable scripts or rules.

Policy deployment



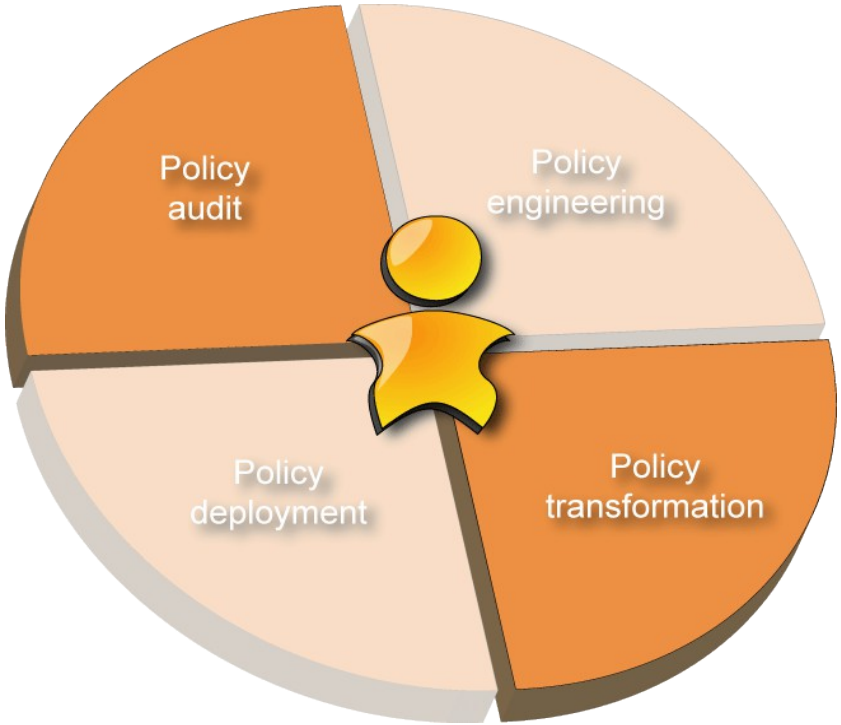
- (1) An xml file containing policy type and policy rules is created.
- (2) The policy is sent to the PIE through the security console (a policy editor).
- (3) The PIE sends the policy to the PDP.
- (4) The PDP dispatches the policy to the concerned PEP regarding the policy type
- (5) The PEP receive the policy and regarding the policy format map it to a set of corresponding commands and execute them.

Summary

- Right management facilitated by using a process approach based on business goals.
- Business-oriented approach facilitated by using ISO/IEC 15504 and Identity Management concepts.
- Obtained policies are deployed through a multi-agent system which provides:
  - Flexibility
    - dynamically addition of new PEP
  - Heterogeneity
    - if the associate agent is developed and configured correctly, all kind of system can be managed by SIM
- FIPA-ACL keep free agents to build messages with specific content (XACML for the moment).

Future works

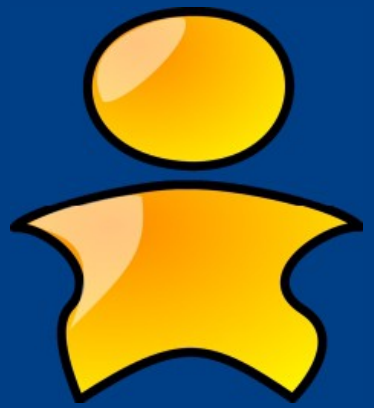
- Policy transformation
  - Policy deduction strategy from the organizational layer
    - XACML
    - CIM-SPL
    - OrBAC
  - Access to MAS platform through Web Service



- Policy Audit
  - Feedback about deployment
  - Policy application status
    - Avoid differences between organizational & technical point of view

Thanks for your attention!
Questions?

Contact: benjamin.gateau@tudor.lu
Web: www.tudor.lu



References

D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn and R. Chandramouli, “Proposed NIST standard for role-based access control”, ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001, Pages 224-274.
J. Park, R. Sandhu, “Originator control in usage control”, Policy 2002: IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, Monterey, California, U.S.A.
J. Park, R. Sandhu, “Towards usage control models: beyond traditional access control”, SACMAT’02, June 3-4, 2002, California, USA.
R. K. Thomas, “Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments”, RBAC '97: Proceedings of the second ACM workshop on Role-based access control, 1997.
A. Abou El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, and al., “Organization based access control.” IEEE 4th International Workshop on Policies for Distributed Systems and Networks (Policy 2003), Lake Come, Italy, June 4-6, 2003.
A. I. Antón, J. B. Earp, “Strategies for developing policies and requirements for secure electronic commerce systems”, 1st Workshop on Security and Privacy in E-Commerce at CCS2000.
P. Samarati, S. De Capitani di Vimercat, « Access control: policies, models, and mechanisms », IFIP WG 1.7 Int’l School on Foundations of Security Analysis and Design (FOSAD 2000), LNCS 2171, pp. 137-196, 2001.
R. Crook, D. Ince, B. Nuseibeh, “Modelling access policies using roles in requirements engineering”, Information and Software Technology 45 (2003) 979-991.
N. Dulay, E. Lupu, M. Solman, N. Damianou, “A policy deployment model for the ponder language », An extended version of paper in Proc. IEEE/IFIP International Symposium on Integrated Network Management, (IM’2001), Seattle, May 2001, IEEE Press.
Basel Committee on Banking Supervision, “International convergence of capital measurement and capital standards”; BIS; Basel, June 2004.
C. Camerer, “Redirecting research in business policy and strategy, Strategic Management Journal, Vol.6, No. 1. (Jan. – Mar., 1985), pp. 1-15.
D. Marriott and M. Sloman, "Implementation of a management agent for interpreting obligation policy", IFIP/IEEE 7th international workshop on distributed systems operations and management (DSOM), 1996.
R. J. Witty, A. Allan, J. Enck, R. Wagner, "Identity and access management defined", Publication Date: 4 November 2003, Gartner Research.
Official eGroupWare community website, http://www.egroupware.org, December 5, 2007.
C. Feltus and A. Rifaut, “An ontology for requirements analysis of managers’ policies in Financial Institutions”, I-ESA07, 2007.
R. S. Savén, Process modelling for enterprise integration: review and framework, 13th International Working Seminar on Production Economics, Igls/Innsbruck, Austria, February 18-22, 2002.
CEN/ENV 12204: Advanced manufacturing technology - Systems architecture - Constructs for enterprise modelling, CEN TC 310/WG1, 1996.
ISO/IEC 15504, “Information Technology – Process assessment”, (parts 1-5), 2003-2006.
Md. Zabid A. Rashid, M. Sambasivan, J. Johari, “The influence of corporate culture and organisational commitment on performance”, Journal of Management Development, ISSN: 0262-1711, Vol, 22., issue 8, pp. 708 – 728.
J. G. March and J. P. Olsen, The logic of Appropriateness, ARENA Working Papers WP 04/09.
J-P. Briot and Y. Demazeau, “Principes et architectures des systèmes multi-agents”, Hermés-Lavoisier, 2001.
N. R. Jennings and M. J. Wooldridge, “Applications of intelligent agents”, Agent Technology Foundations, Applications, and Markets, Springer-Verlag, 1998.
S. Godik, T. Moses, et al, “eXtensible Access Control Markup Language (XACML) Version 1.0”, OASIS Standard, February 18th, 2003.
ISO 9000:2005, Quality management systems - Fundamentals and vocabulary.
eXtensible Access Control Markup Language (XACML) homepage, , December 12, 2007.
XACML 2.0 Specifications, , December 12, 2007.
Organization for the Advancement of Structured Information Standards (OASIS) homepage, , December 12, 2007.
D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry, “The COPS (Common Open Policy Service) protocol”, IETF RFC 2748, January 2000.
R. Enns, “NETCONF configuration protocol”, IETF RFC 4741, december 2006.
D. Harrington, R. Presuhn, B. Wijnen, “An architecture for describing Simple Network Management Protocol (SNMP) management frameworks”, IETF RFC 3411, December 2002.
P. Novàak, M. Rollo, J. Hodìk and T. Vlcek, “Communication security in multi-agent systems”, Multi-Agent Systems and Applications III, Lecture Notes in Computer Science 2691,pp 454-463, 2003.