

# **A Policy-Based Security Mechanism for Distributed Health Networks**

**A. Onabajo, C. Obry and J. H. Jahnke**

netlab Research Group<sup>1</sup>  
Dept of Computer Science  
University of Victoria,  
Victoria, BC,  
Canada

# Outline

- Motivation
- Background
- Policy-Based Security Mechanism
- A Scenario
- Future work

# Motivation

- Knowledge valuable asset of organizations
- Trend towards Distributed/Integrated Health Information
- Sensitive patient information has to be protected
- Facilitate secured information exchange
  - Flexible and adaptable approach
  - Regulations and individual consents
  - Patient care should still be paramount

# Background

- Research into middleware solution for integrated medical information systems
- Based on domain and technological standards
  - HL7 Standards e.g. RIM and CDA
- Policy-Based Systems
  - Offer adaptability and easier system modification
- Encryption
  - Public Key Infrastructure (PKI)

# Policy-Based Security Mechanism

## ■ Policies

- Provide the rules for information handling and exchange
- Types
  - Patient
  - Organizational
  - Document Type
- Encoding
  - eXtensible Access Control Markup Language (XACML)<sup>2</sup>
    - OASIS standard
    - Provides languages for defining policies and requests

# Policy-Based Mechanism (cont'd)

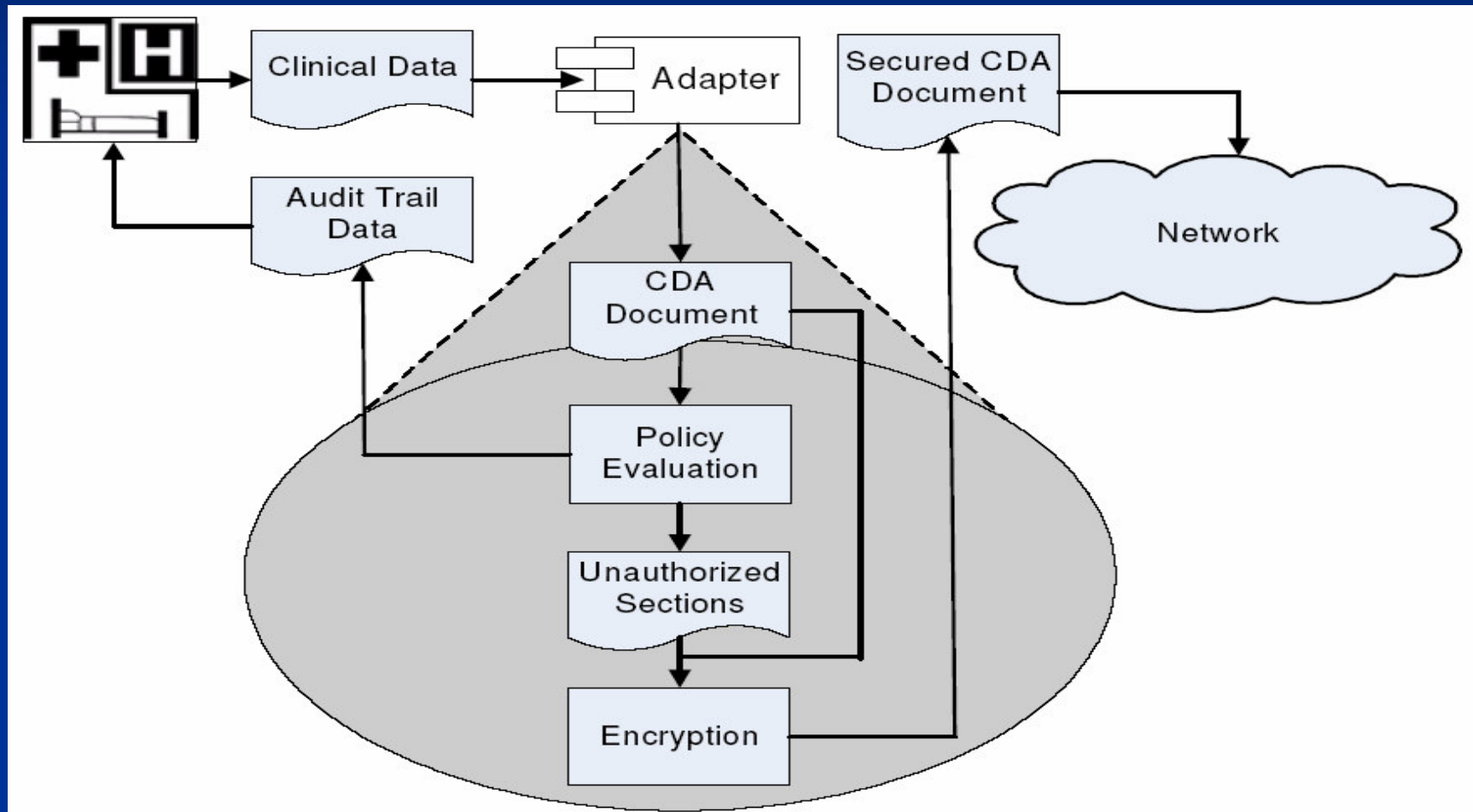
- Policy Evaluation Approach
  - Match policies to document
  - Evaluate the rule(s) of policies
  - Apply effects (deny or permit) of rules
    - Rule combination
    - Conflict resolution
      - Precedence by specificity<sup>3</sup>

# Policy-Based Mechanism (cont'd)

## ■ Encryption

- Applied after policy evaluation and before transmission
- Non-authorized sections are not transmitted
- Document will be encrypted with a symmetric key
- Encrypted document and symmetric key will be encrypted with recipients public key

# A Scenario





# Future Work

- Currently at initial stage of development
- Integration of a Role-based access mechanism
- Further refinement of conflict resolution of policies

# Resources

1. [www.netlab.uvic.ca](http://www.netlab.uvic.ca)
2. OASIS eXtensible Access Control Markup Language. Available online at [http://www.oasisopen.org/committees/tc\\_home.php?wg\\_abbrev=xacml](http://www.oasisopen.org/committees/tc_home.php?wg_abbrev=xacml)
3. Lupu E.C. and Sloman M., *Conflicts in Policy-Based Distributed Systems Management* IEEE Transactions on Software Engineering, 1999;25(6) 852-869.
4. C. Obry, J.H. Jahnke, A. Onabajo and W Schafer “*Enabling Privacy in Cross-Organisational Information Mediation – An Application in Health Care*”. Proceedings 2003 Software Technology and Engineering Practice, Workshop on e-health, software, systems and networks. Amsterdam, The Netherlands. Sept. 19-21, 2003