

“A Semantic Approach to Secure Exchange of Patient Information”

WATERLOO
CHERITON SCHOOL OF
COMPUTER SCIENCE

cs.uwaterloo.ca

Presented By: Atif Khan
April 25th, 2011

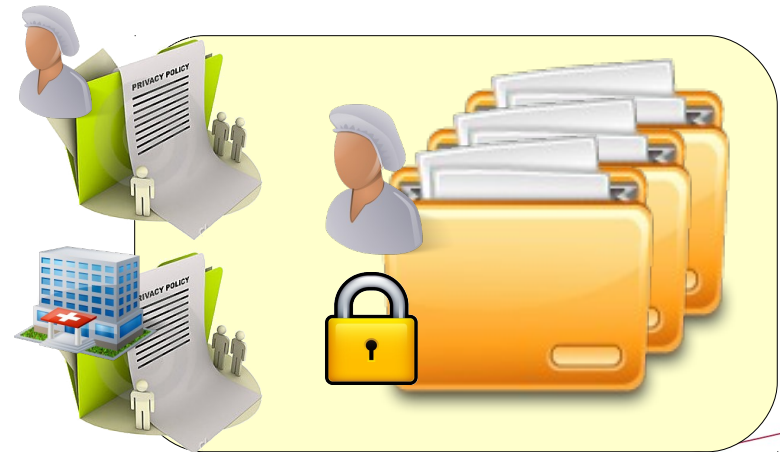


Motivation

Calgary General Hospital

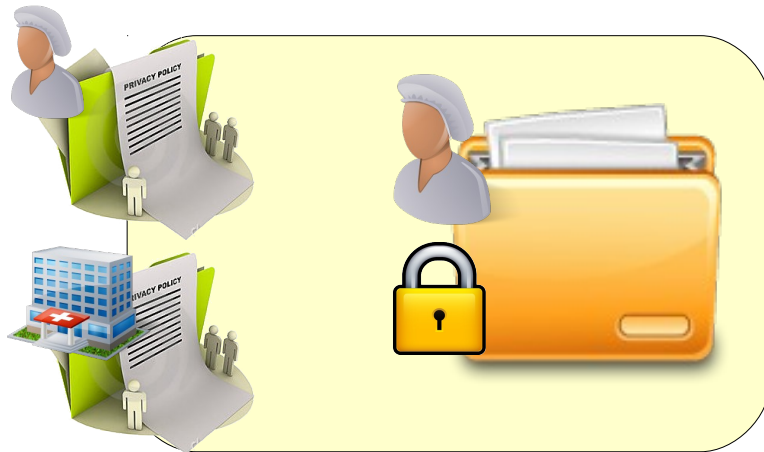


Toronto General Hospital

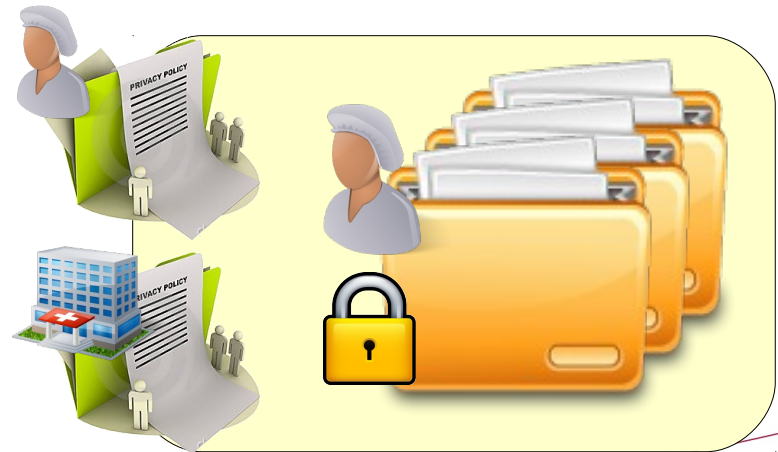


Motivation

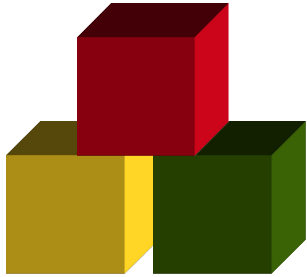
Calgary General Hospital



Toronto General Hospital



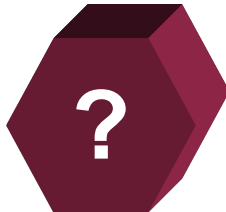
Outline



Overview
(Basic building blocks)



Framework



Future Extensions

Conclusion

Overview

Building Blocks

- Access control
 - role based access control (RBAC)
 - policy based access control
- Knowledge management
 - representation, sharing, inference & reasoning
- Multi-agent systems (MAS)

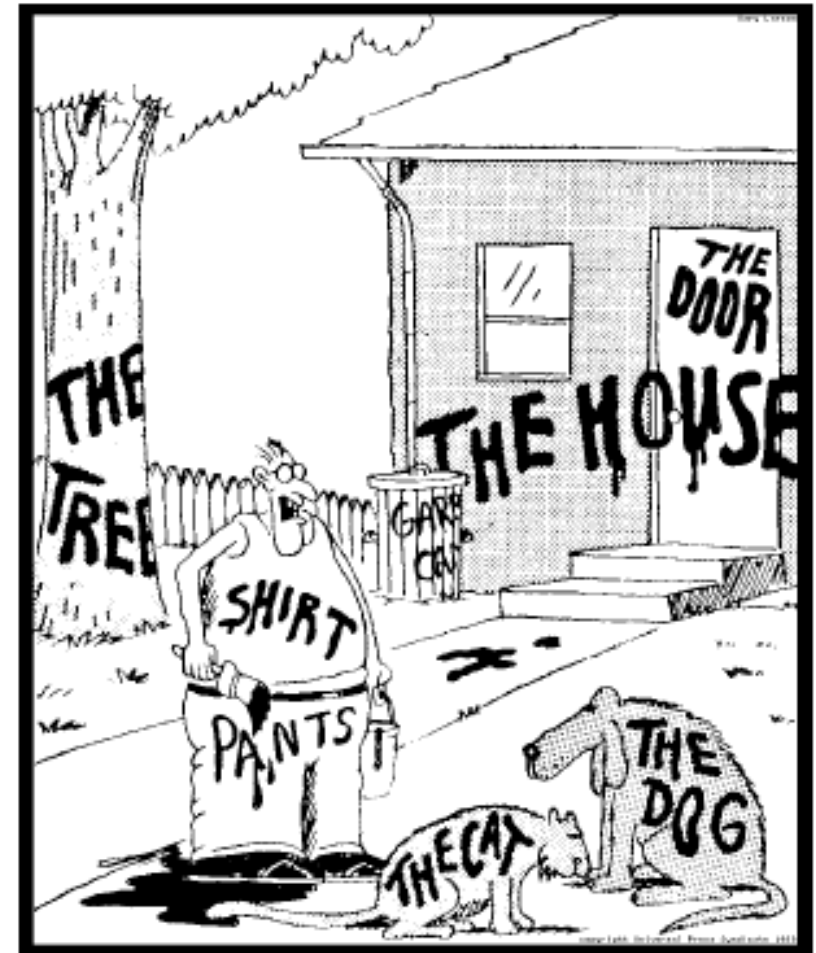
Knowledge Sharing

Representation

- **Unique** names
 - unambiguous **concepts**
 - “*universe of discourse*”
defines knowledge boundaries

Motivation

- **Easy** to work with information
 - acquire
 - maintain
 - communicate & share
 - reasoning



“Now! *That* should clear up
a few things around here!”

Knowledge Sharing

Ontology

– Definition

- “an ontology is an explicit and formal specification of a conceptualization” - Rudi Studer

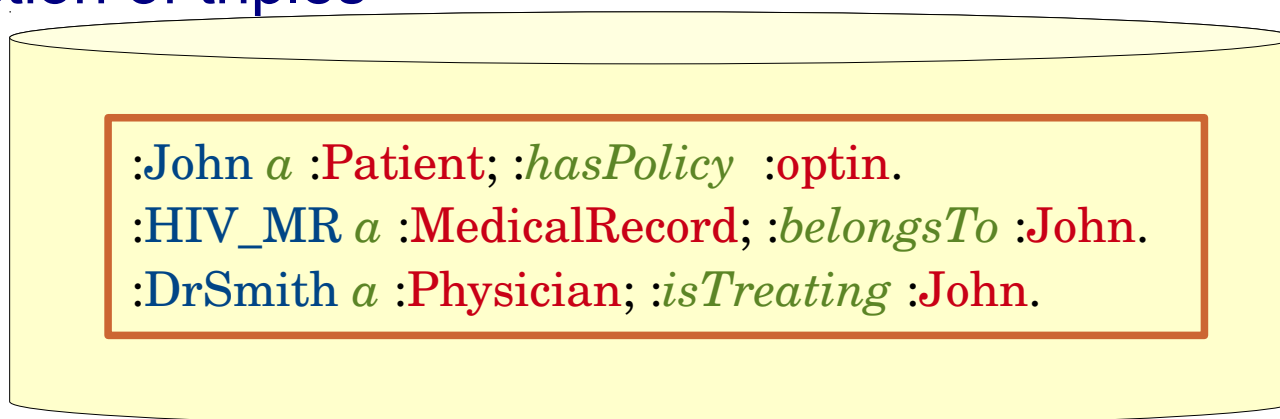
– Components

- concepts (e.g. *Patient*)
- individuals & objects (e.g. *John a patient*)
- relationships & properties (restrictions, disjointness)
 - e.g. (*John hasPolicy optin*)

Knowledge Sharing & Semantic Web

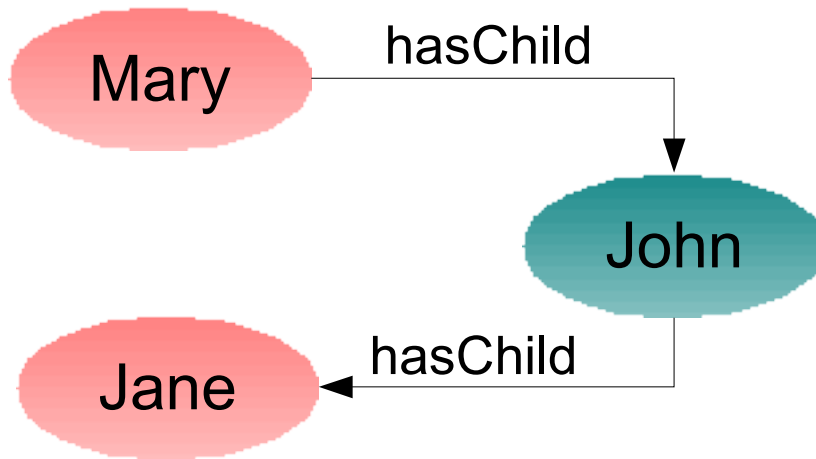
Representation & Storage

- Knowledge represented as **triple** statements
 - subject *verb* object.
 - Resource Description Framework (RDF) / Notation 3 (N3)
- Knowledge is stored in **triple stores**
 - collection of triples



N3 Triple Store

Knowledge Inference



Which statement is true

- a. Mary is a woman.
- b. Mary is a grandmother
- c. Mary is a grandparent

How do we know that Mary is a grandparent?

- *hasChild* → *parent*
- *parent of parent* → *grandparent*

Rules

- *evidence (from the knowledge store)*
 - *John is a parent & Mary is a parent of parent*
→ *Mary is a grandparent*

Result

Example (Access Control)

Knowledge-Store

:John *a* *:Patient*; *hasPolicy* *:optin*.
:HIV_MR *a* *:MedicalRecord*; *belongsTo* *:John*.
:DrSmith *a* *:Physician*; *isTreating* *:John*.

Rule

{*?P* *haspolicy* *:optin*.
?MR *belongsTo* *:?P*.
?DOC *isTreating* *?P*} \Rightarrow {*?DOC* *hasAccess* *?MR*}.

Query

_ *WHO* *hasAccess* *:HIV_MR*.

Reasoner

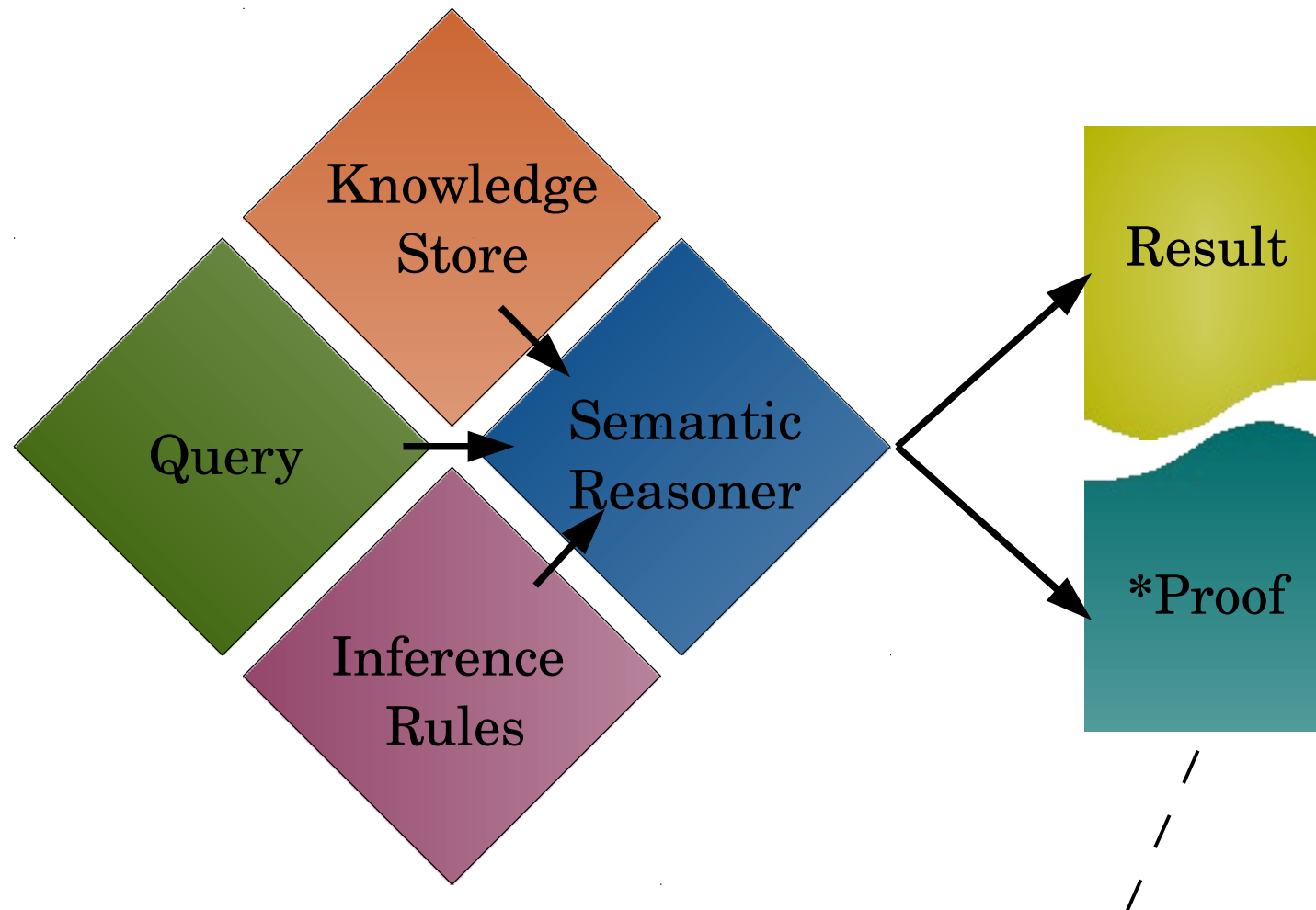
Proof

{ <i>:John</i> <i>hasPolicy</i> <i>:optin</i> }	<i>e:evidence</i> <i><knowledgebase#_2></i> .
{ <i>:HIV_MR</i> <i>belongsTo</i> <i>:John</i> }	<i>e:evidence</i> <i><knowledgebase#_4></i> .
{ <i>:DrSmith</i> <i>isTreating</i> <i>:John</i> }	<i>e:evidence</i> <i><knowledgebase#_6></i> } \Rightarrow

Result

{*:DrSmith* *hasAccess* *:HIV_MR*} *e:evidence* *<rules#_1>*}.}

System Components



can be independently verified

Multi-agent System (MAS)

Intelligent Agent (IA)

- Autonomous entity capable of acting on its own
- Interacts with its environment
 - via observations & actions
 - goal oriented (maximize utility)
 - capable of learning (using knowledge) to achieve goals

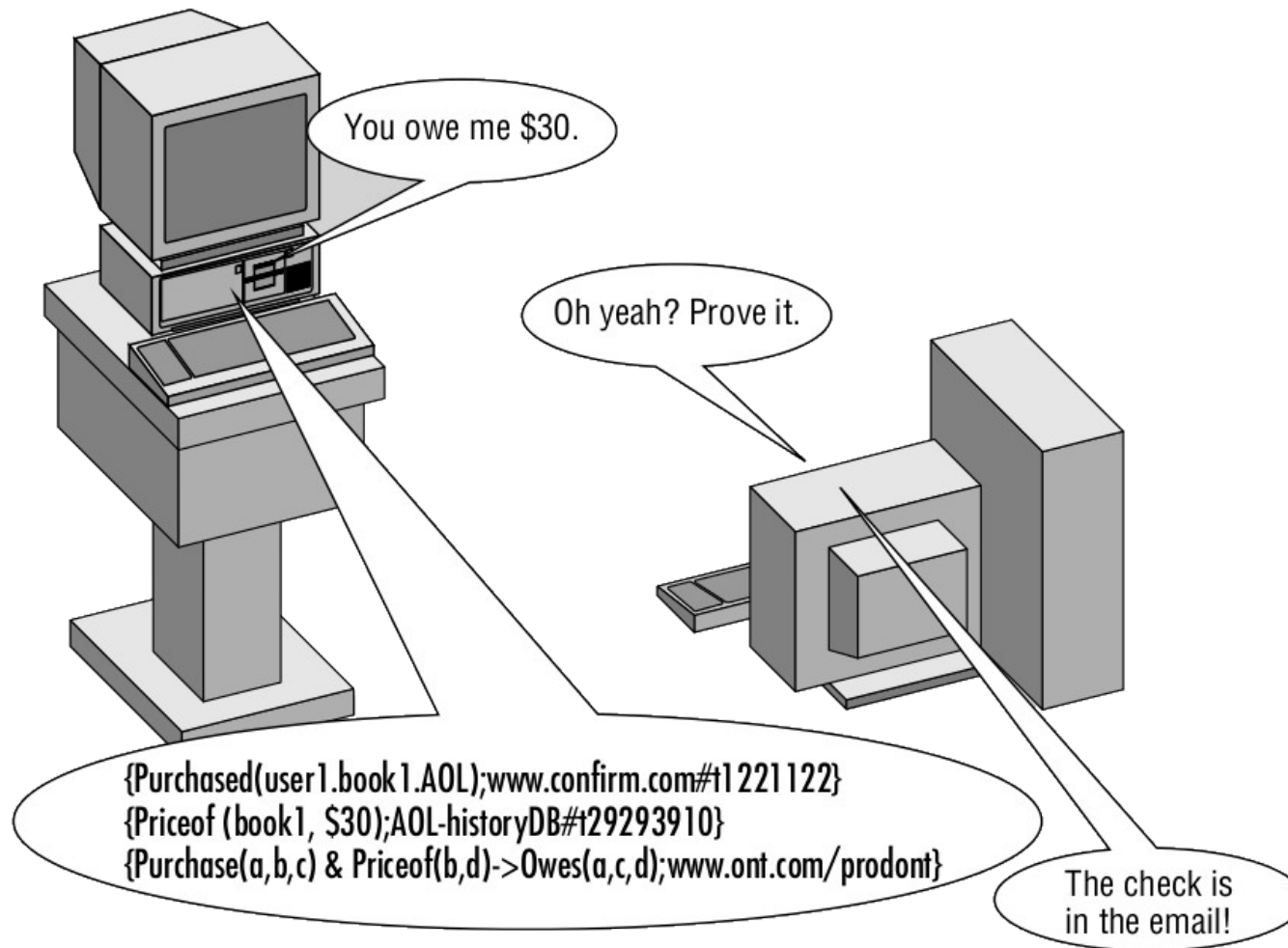
Multi-agent System (MAS)

Multi-agent System (MAS)

- Environment of interacting intelligent agents
 - IAs working towards an equilibrium
- Decision making
 - perfect vs. partial information
- Communication
 - auctions, voting, market, contract-nets
 - agent communication language (ACL)
- Types of interactions
 - cooperative interactions to maximize overall utility
 - non-cooperative interactions to maximize self utility

Multi-agent System (MAS)

Inter-agent Trust Consideration



Proposed Solution

Policy Based Access Control

- Patient consent
- Institutional security & privacy policies

Semantic Knowledge Representation

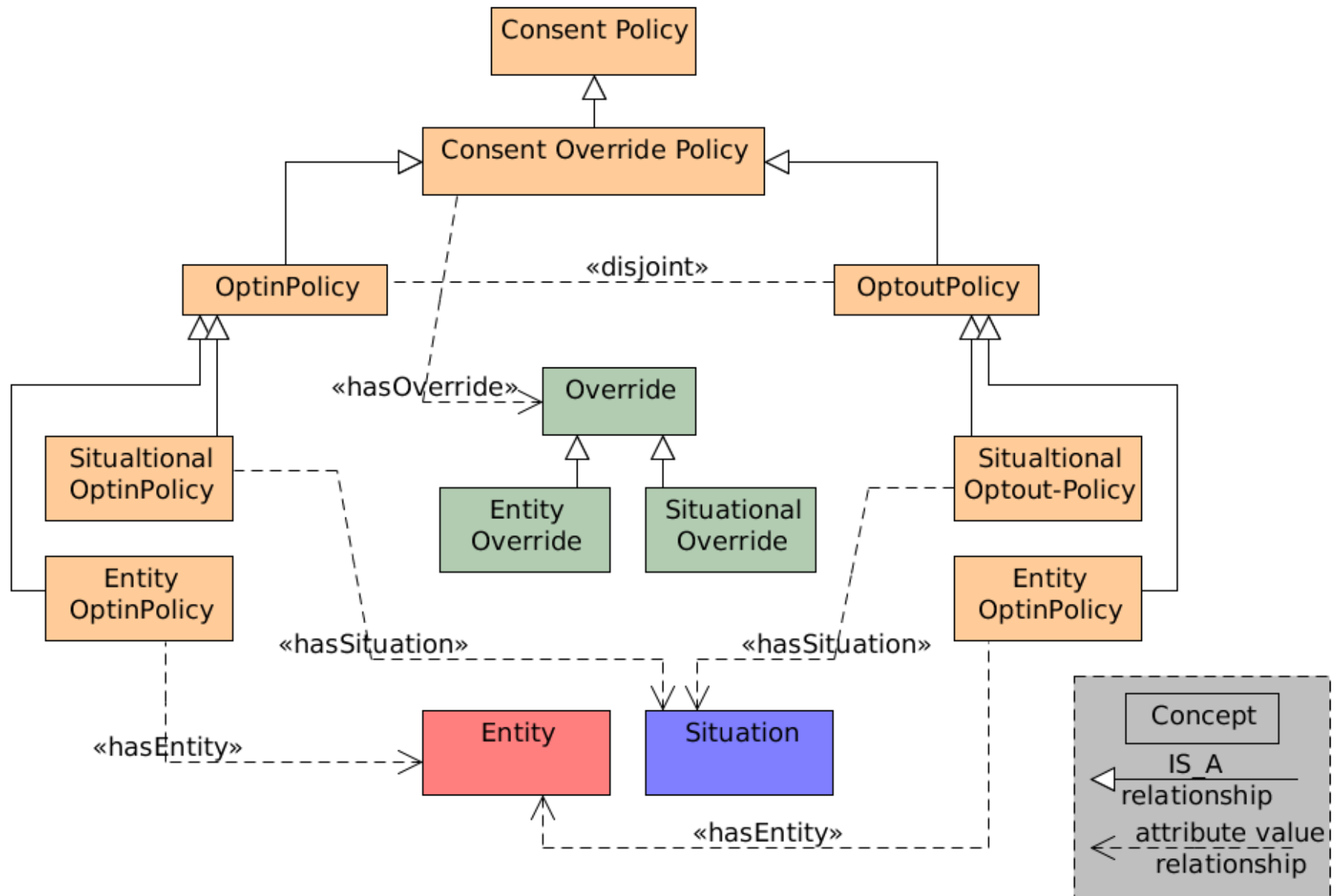
- Patient consent and other security & privacy policies
- Based on one or more ontologies (*information sharing*)
- Can be reasoned with (*knowledge inference & reasoning*)
- Machine processable

Proposed Solution

Healthcare Entities as IAs

- Ontology based agent communication language
- Cooperative environment
- Overall utility is patient centric
- Dynamic trust establishment

Representing Consent



Sample Policies

Patient Consent



Opt-out with emergency override

Institutional Policies

Toronto General Hospital



- employee has access to patient records
- employee must be treating the patient
- employee must be on shift
- employee must be a physician

Calgary General Hospital



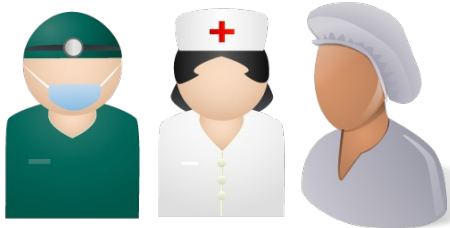
- all hospital employees have access to patient records

MAS Environment

Intelligent Agents



Institutional



Physician

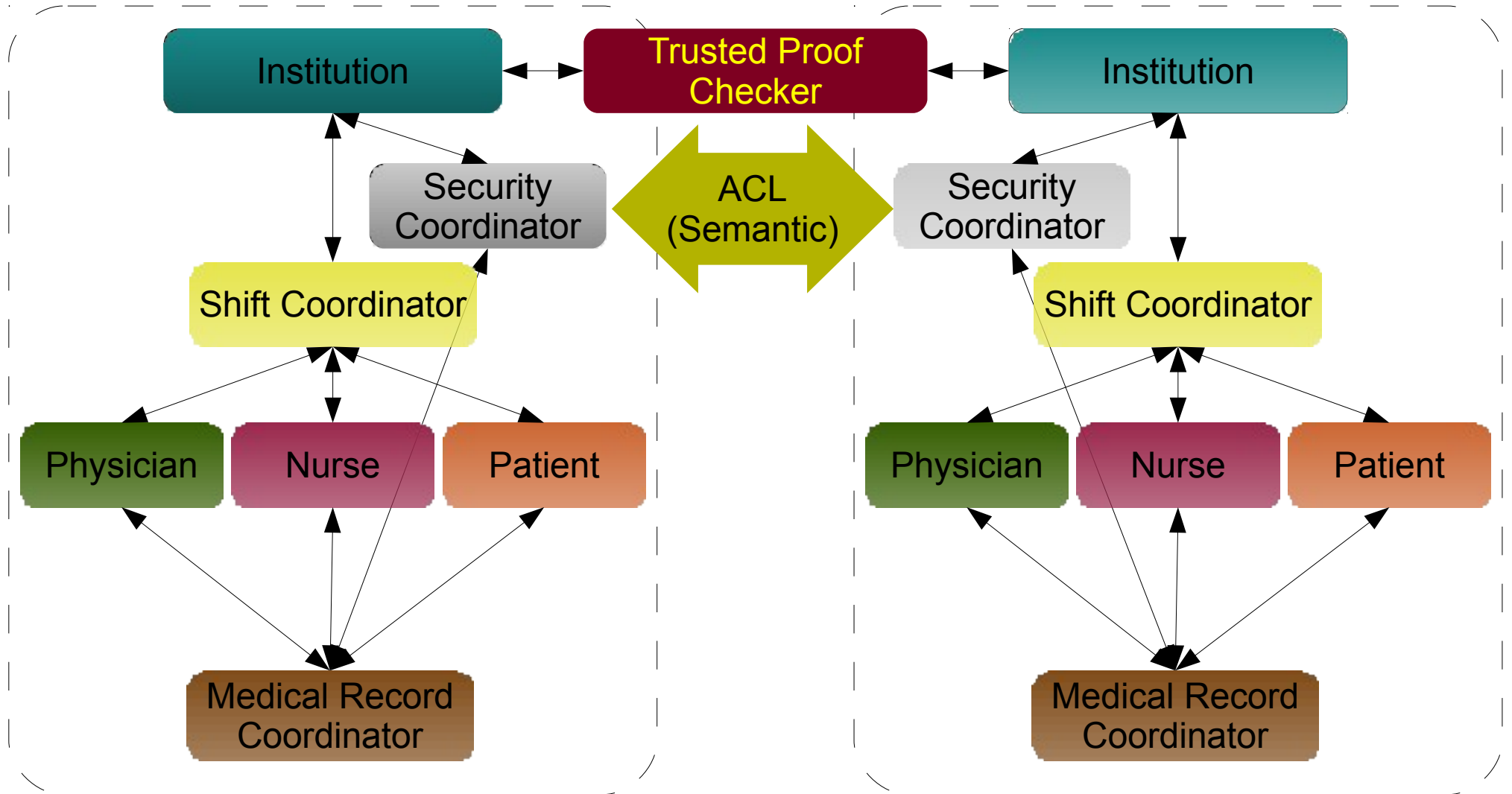
Nurse

Patient



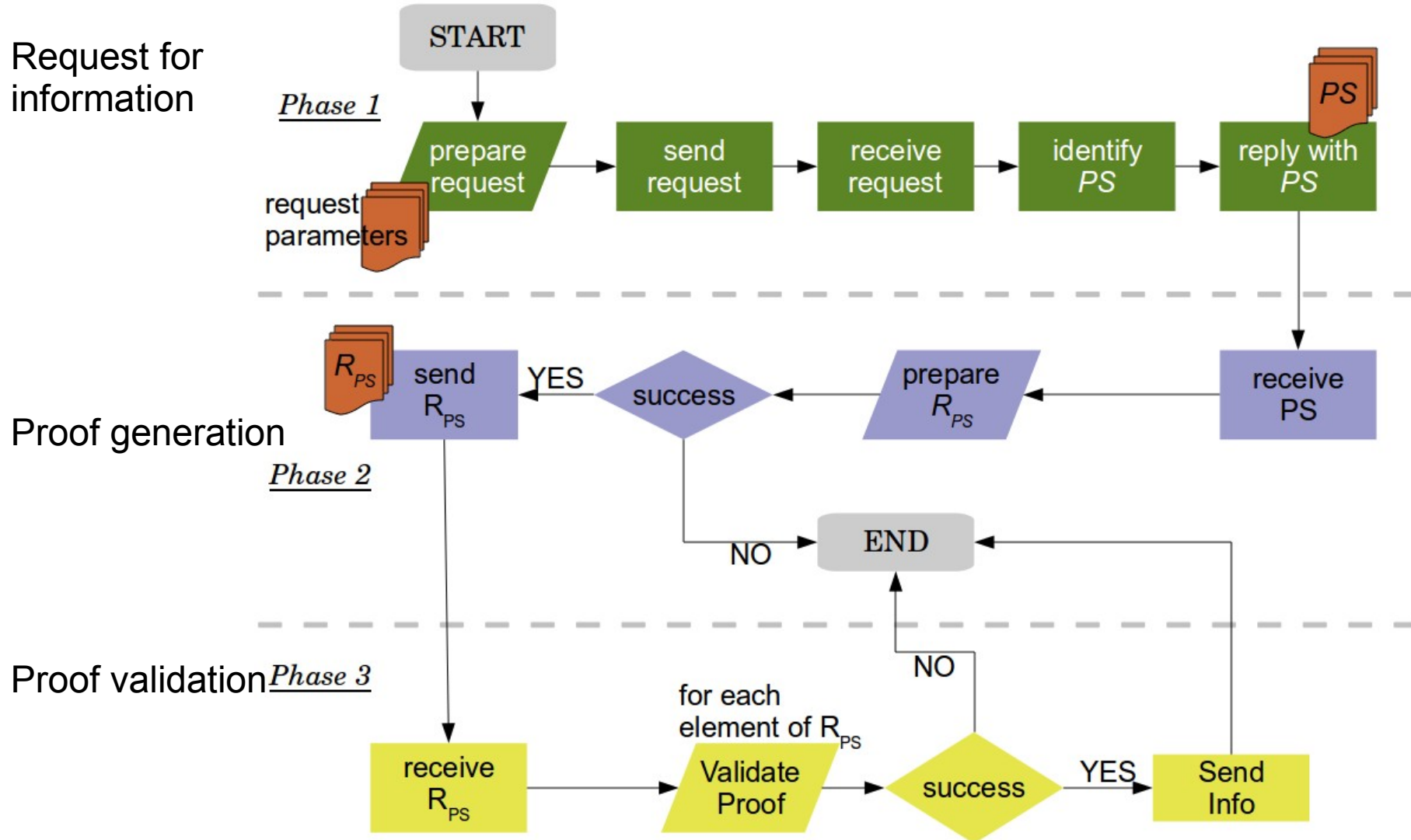
Medical Record
Coordinator

MAS Environment



Information Exchange Protocol

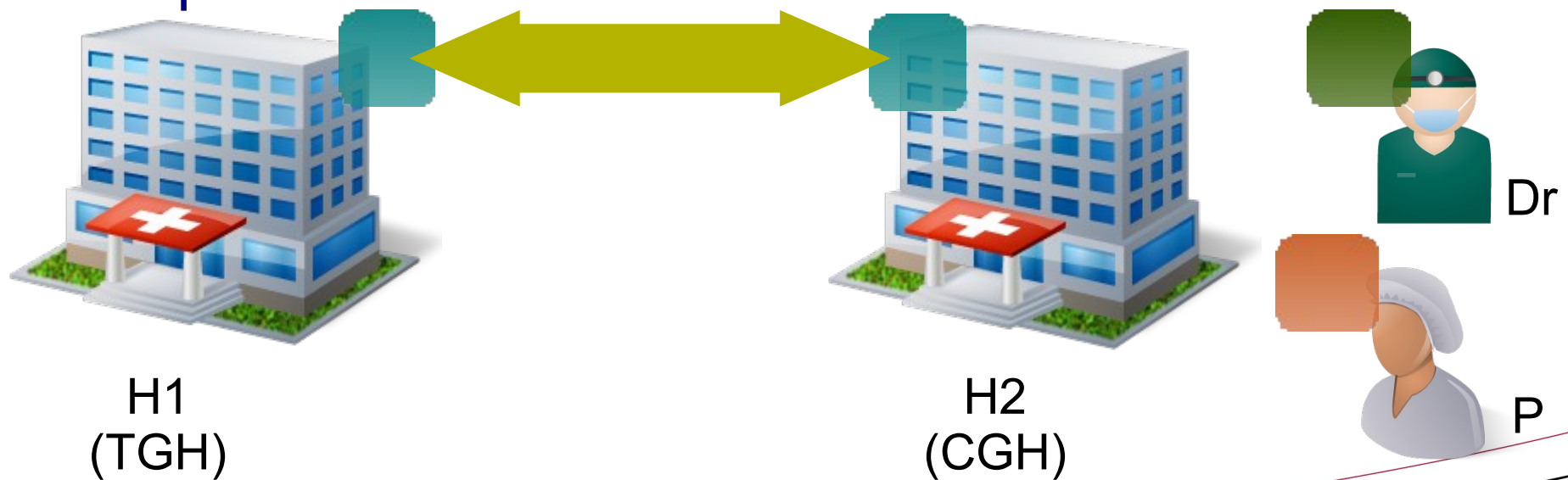
3-Phase Protocol



Information Exchange Protocol

Request for Information – Phase 1

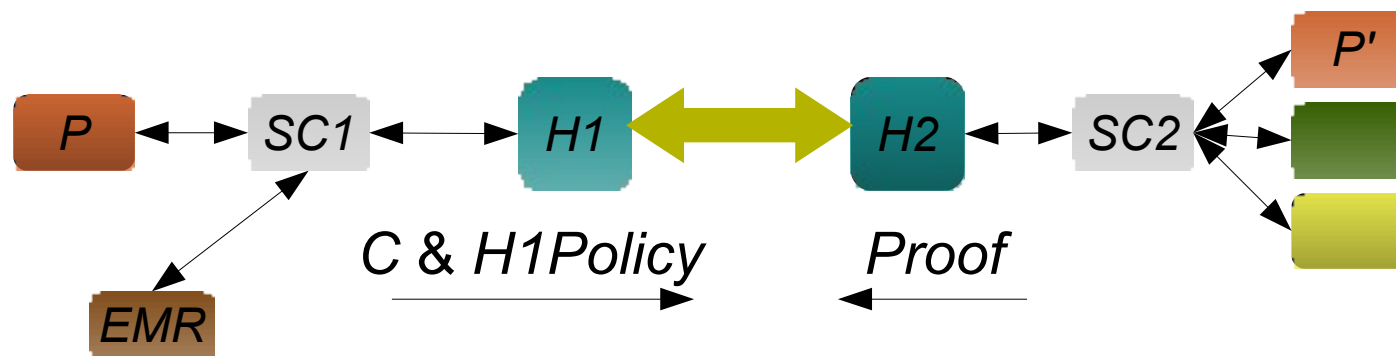
- Dr request for P's medical record from H1
- H2 (institutional agent) propagates the request to H1
- H1 (institutional agent) receives and processes the request



Information Exchange Protocol

Proof Generation – Phase 2

- H1 identifies protection set PS
 - PS {patient consent **C**, H1 privacy & security policies **H1Policy**}
- H1 requests H2 for provable validation of PS
 - **C & H1Policy**
- H2 generates the proof and returns to H1



Information Exchange Protocol

Proof Generation – Phase 2



Consent policy

Opt-out with
emergency override



TGH security & privacy policy

- employee has access to patient records
- employee must be treating the patient
- employee must be on shift
- employee must be a physician

Required Proof:

- confirm that patient is indeed in an emergency situation

Required Proof:

- DR is an employee of the hospital
- DR is treating the patient
- DR is on shift
- DR is a physician

Information Exchange Protocol

Proof Validation – Phase 3

- H1 computes the proof
 - locally
 - using a trusted third party proof checker
- Information is exchanged
 - upon **successful** validation of proof (of consent & other policies)

Future Extensions

Local Ontology

- Mapping (dynamic vs. static)

Context Based Retrieval

- Include search context to enhance access

Information Caching

- Proof attributes, patient consent, hospital policies

Privacy-aware Proof Validation

- Utilize cryptographic primitives

Conclusion

Patient Consent Management Framework

- Policy based access control
- Consent & other policies have semantic representation
 - enhanced policy exchange
 - ability to reason about access decision
- Multi-agent System
 - collaborative agent environment
 - agent utility is a function of patient utility
 - trust per request

Thank You!