

TrakChain protects Track & Trace data in the Internet of (many) Things

RFID technology enables traceability systems that capture detailed data about goods as they move in the supply chain. Securing this data requires evaluating dynamic conditions to authorize business partners that are not known in advance. Furthermore, the system must promote trust and give incentives so that each partner shares its own data.

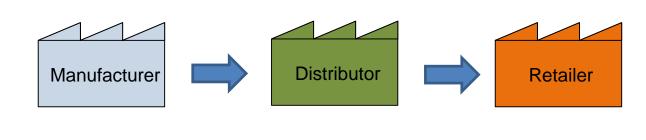
TrakChain implemented data visibility restriction policies using RDF and SPARQL. These policies can be converted to a standard format, XACML, to reuse existing enforcement infrastructures and tools. The expressiveness of the policies was evaluated against a set of requirements for a pharmaceutical traceability system.

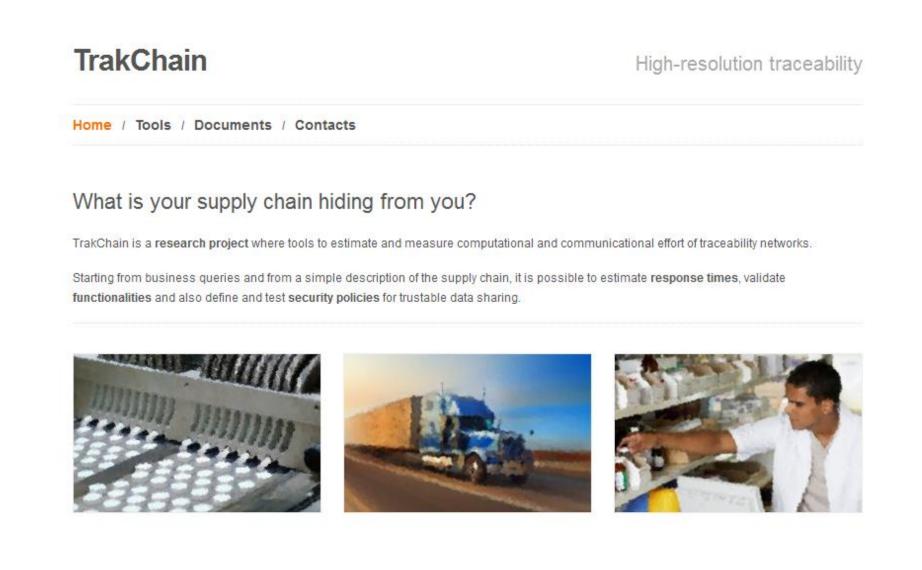
Miguel Pardal, José Alves Marques

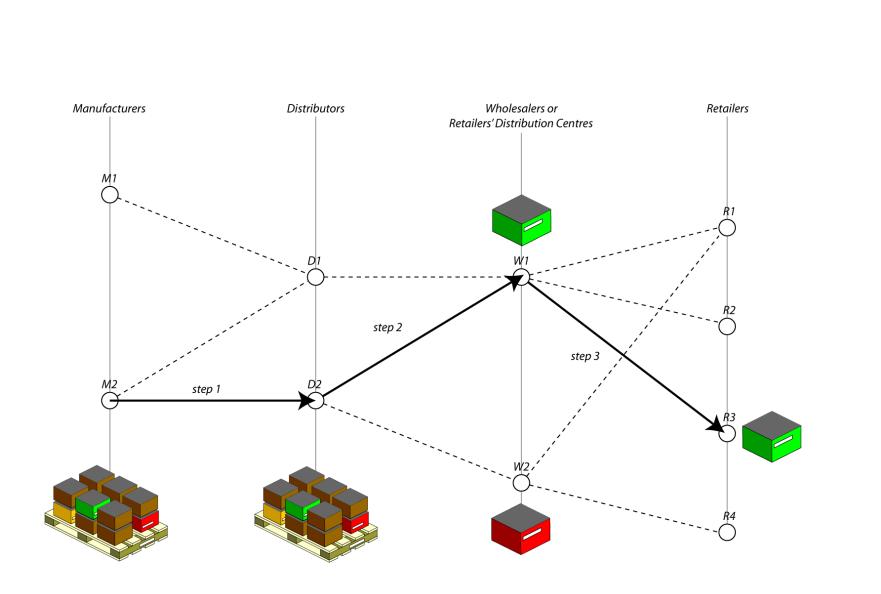
Instituto Superior Técnico, Universidade de Lisboa

http://trakchain.net

Traceability systems assessment framework



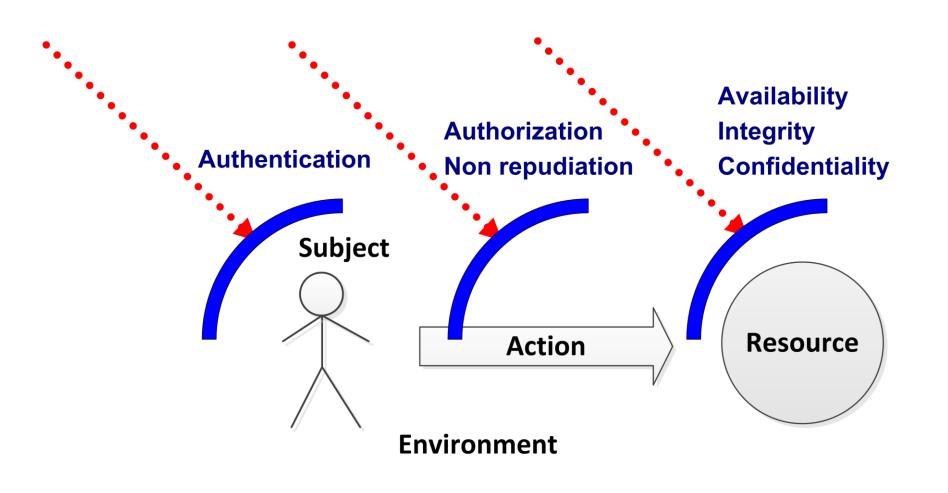






Each individual item takes a unique path...

Traceability data security



Environment

Action

Policies

Policy Admin. Point

Supply chain concepts

XACML conversion

XACML

Policies

Capability

Tokens

RDF

assertions

Resource

permit/deny

Business

Applications

Data

Messages

Docu-

ments

Policy

Enforcement

Point

Policy

Decision

Point

Subject

Policy

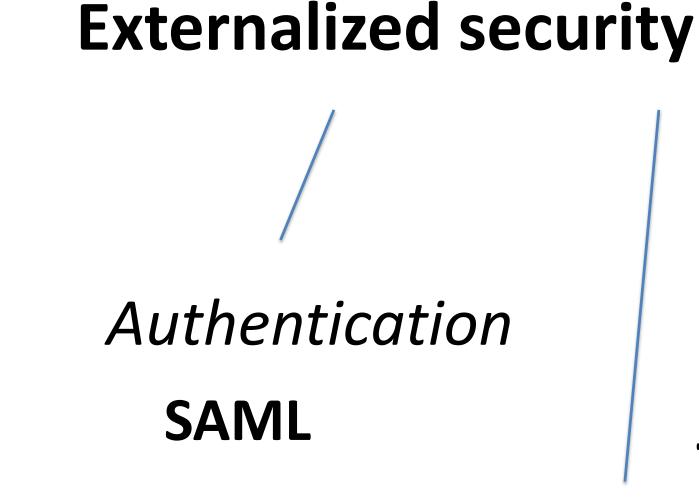
Admin.

Point

Access

Control

Lists

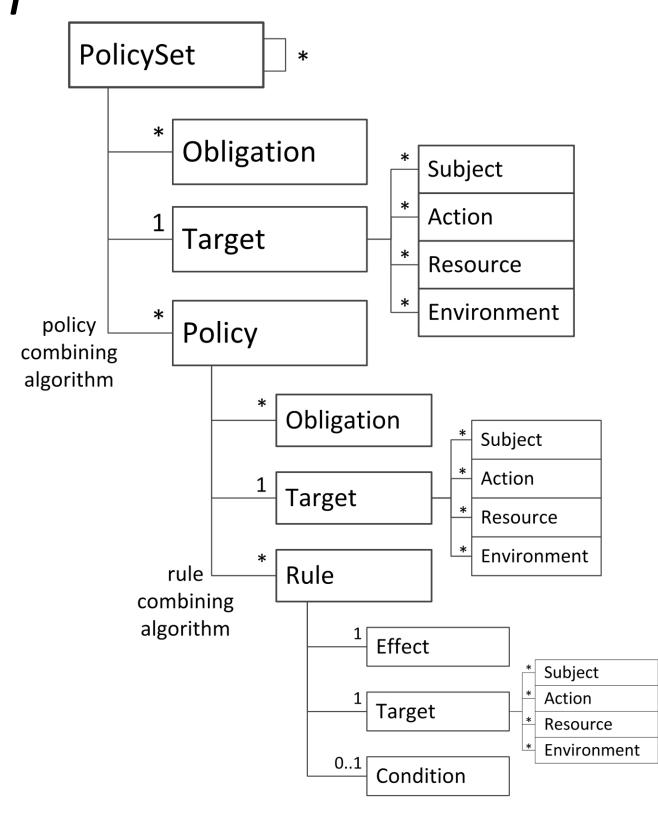


Message level (crypto) security

TLS

XACML – eXtensible **Access Control Markup Language**

Authorization



- Protect privately relevant information
- But still give access to non-

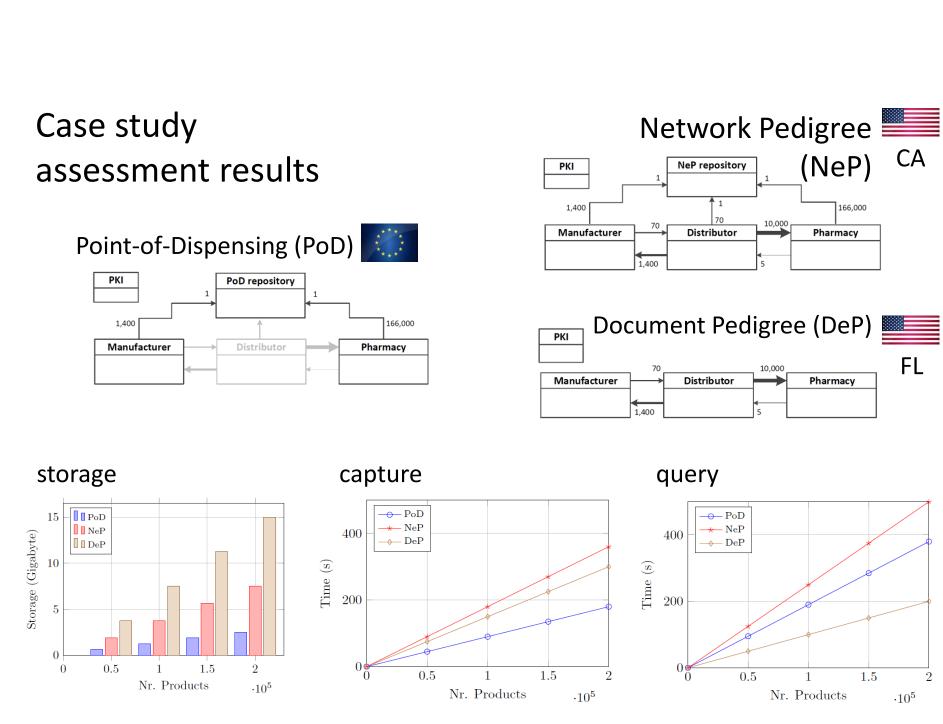
Contributions

- Data sharing policies:
- predefined participants

SCAz – Supply Chain **Authorization Language**

Chain of Trust Assertions

RDF graph for visibility policy cta:grantsRead predicate



Requirements elicited from Pharma industry prototype GHX, Abbott, McKesson, Veterans Admin. Hospital

Bulk

Service provider, manufacturer, distributor, dispenser

Rich sharing conditions expressed with assertion extensions Delegated Transitive Conditional

Future work

:company0

cta:Policy

cta:Organization

(cta:creates∖cta:grantsRead

cta:grantsRead

:company1

:policy0

cta:publishes

cta:protects

:record0

:item0

cta:Identifier

/cta:about

cta:Record

- Connect authorization with business systems
- Integrate with ERP and SCM to derive data sharing assertions
- Reduce administrative burden
- Improve performance XACML
- Find best formulations for the proposed assertion extensions

Chain-of-Trust Assertions (CTA) performance is similar to other approaches – ACLs and Tokens – but it is **extensible**

> **XACML overhead** is significant but acceptable