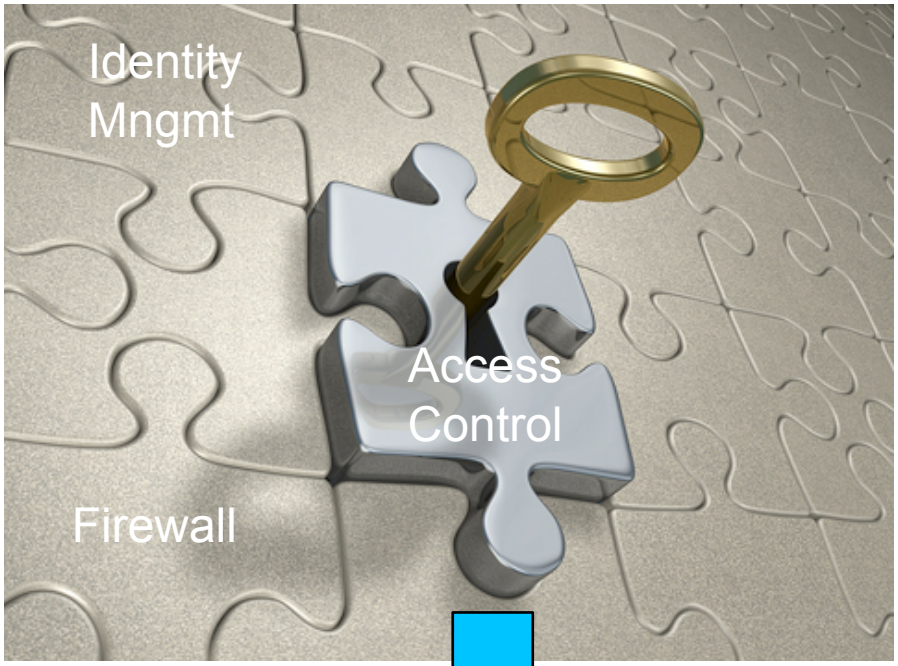
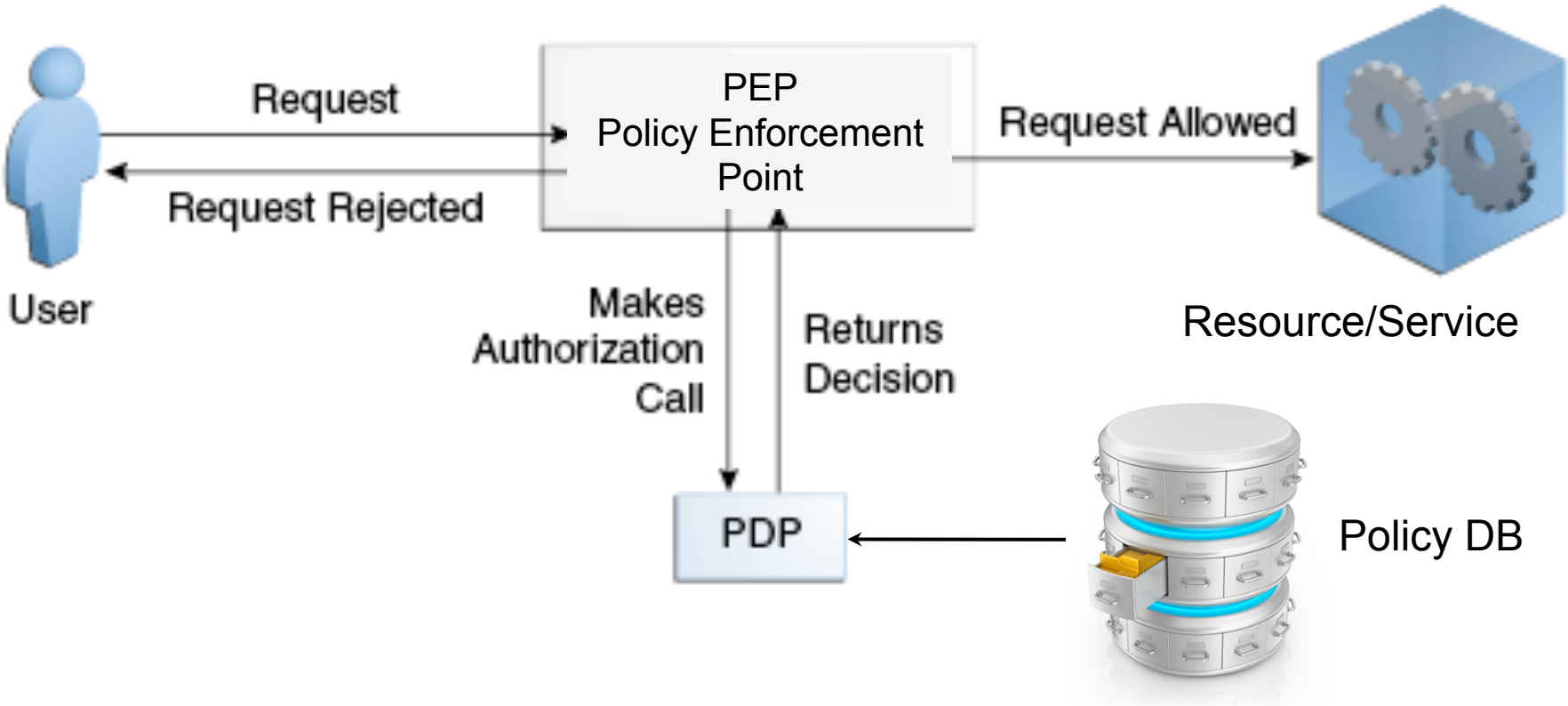
An Overview of Access Control in ST

Silvio Ranise
ranise@fbk.eu / http://st.fbk.eu/SilvioRanise

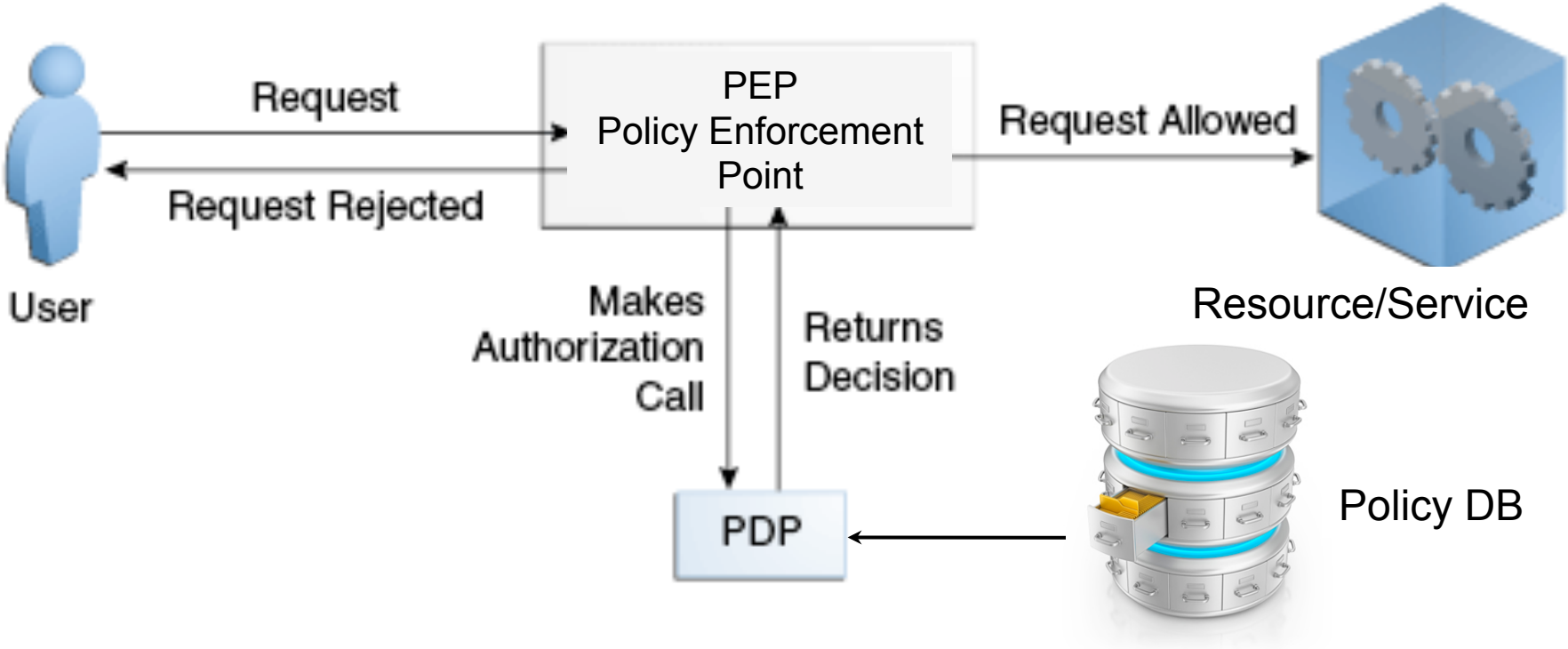
Access Control in the Security Puzzle



Access Control Mechanism



Access Control Mechanism



Security of Cloud-based and Service-oriented Applications and Infrastructures

Problems/Limitations/Difficulties

Access Control: problems

- Difficult to write policies that match designer intentions
- Required more than a simple grant/deny to maximize sharing of information while reducing risk of unintended disclosure

- Administration is complex and may give rise to safety problems

ASASPXL

ASASPTIME

- Enforcement may become very complex in presence of computation-dependent authZ constraints

SECENTIS
A European Industrial Doctorate on Security and Trust

- Lack of a uniform framework encompassing policy design and enforcement

ALPS

smart campus
OpenServices
Smart Community

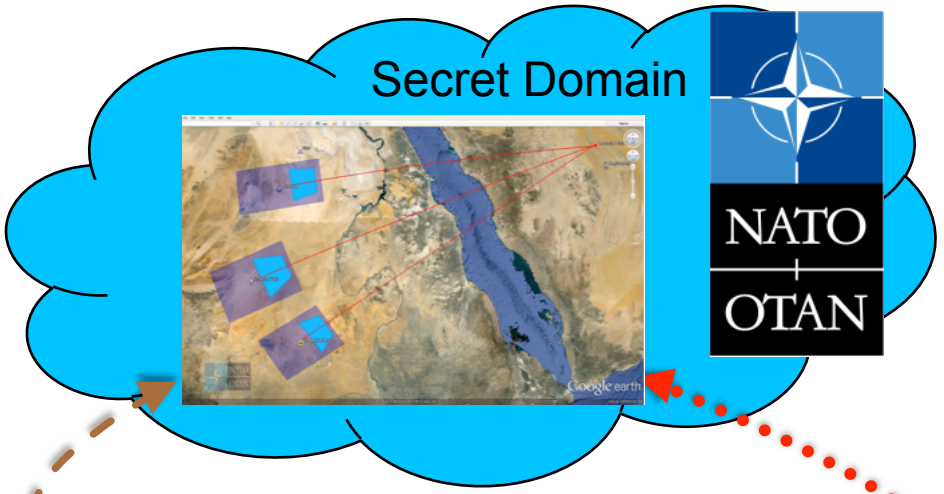
Access Control: problems

- Difficult to write policies that match designer intentions
- Required more than a simple grant/deny to maximize sharing of information while reducing risk of unintended disclosure

Passive Missile Defence (PMD) Scenario

FONDAZIONE BRUNO KESSLER

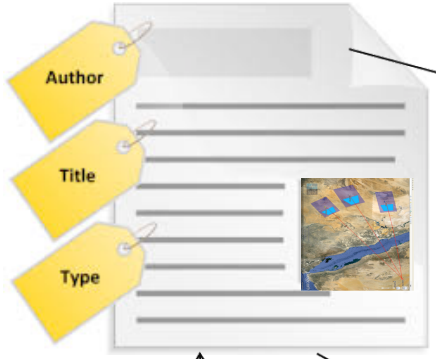
Maps with simulation on rescue mission



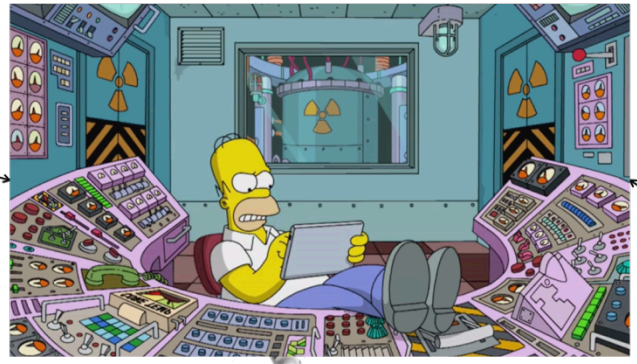
Soldier of NATO member country

Doctor of Red-Cross

Content-based Protection and Release



3. extract content metadata



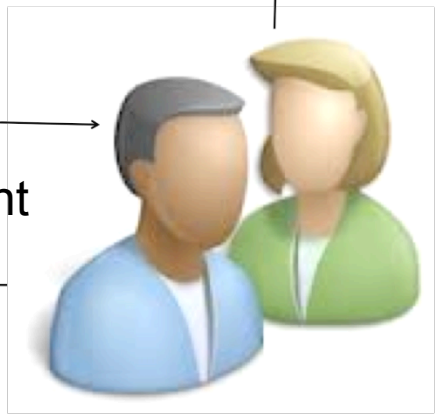
3. credentials

2. pick document

4. picked document

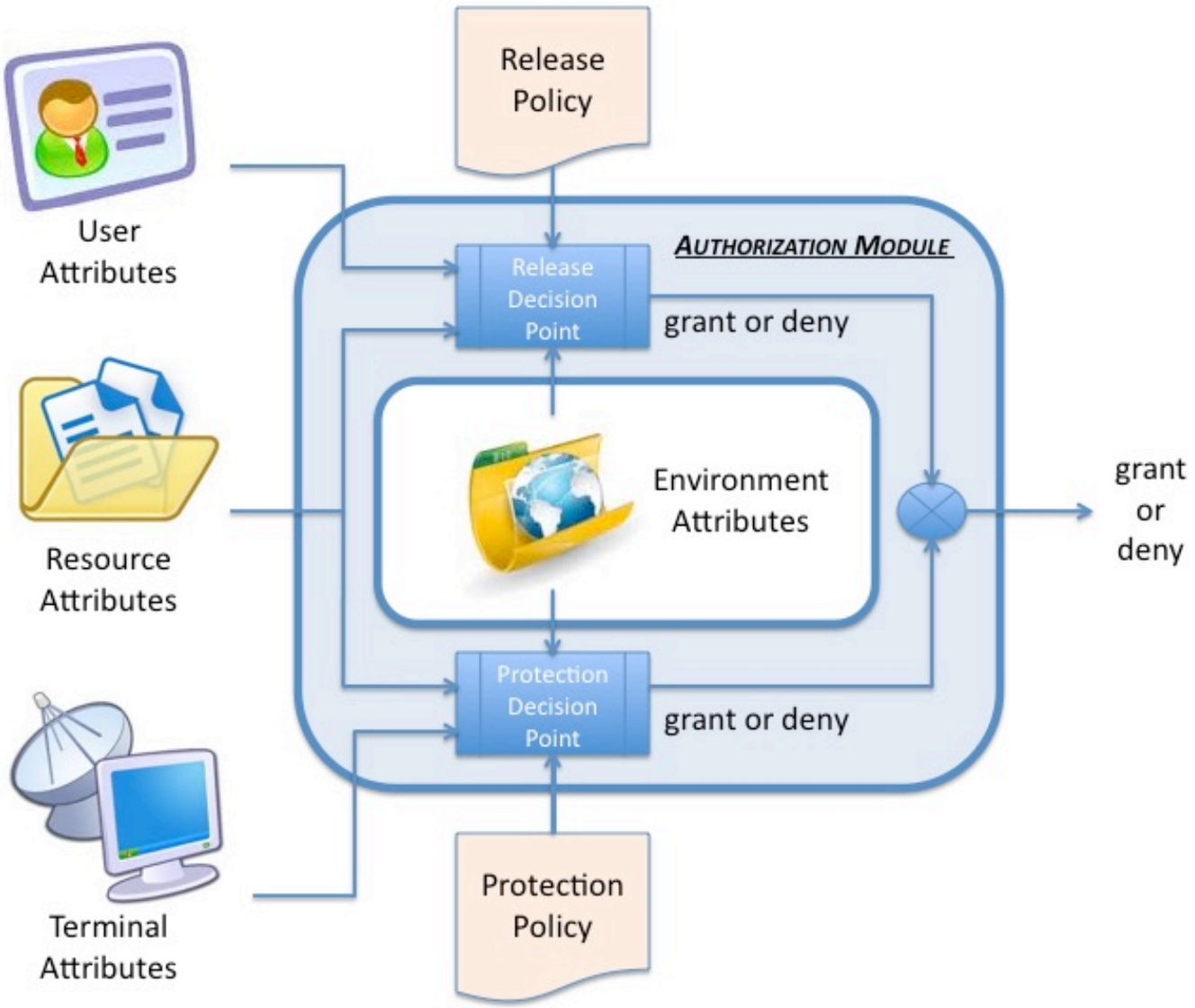
2. provide user profile

5. ***view*** of picked document

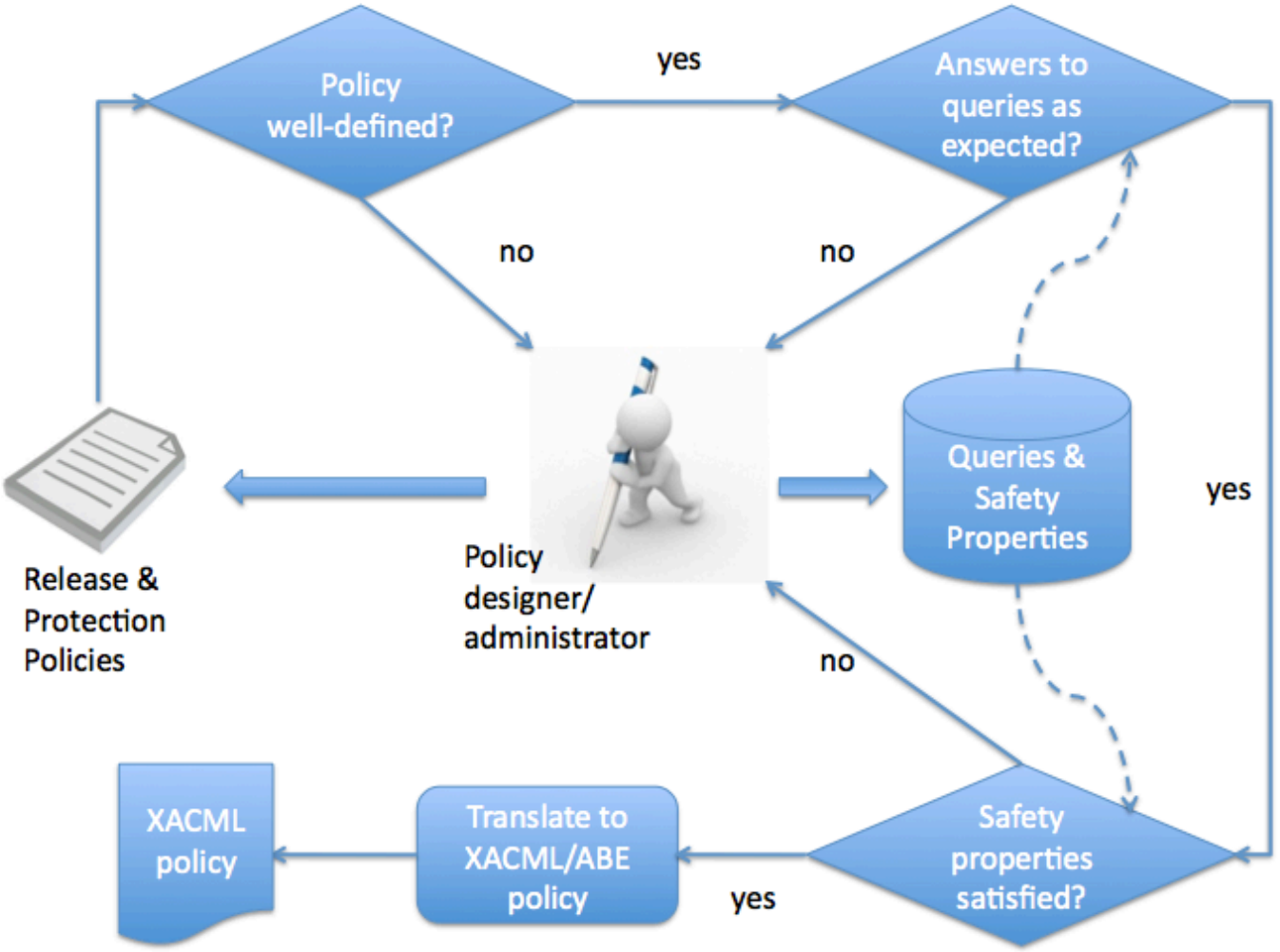


1. ask for a document

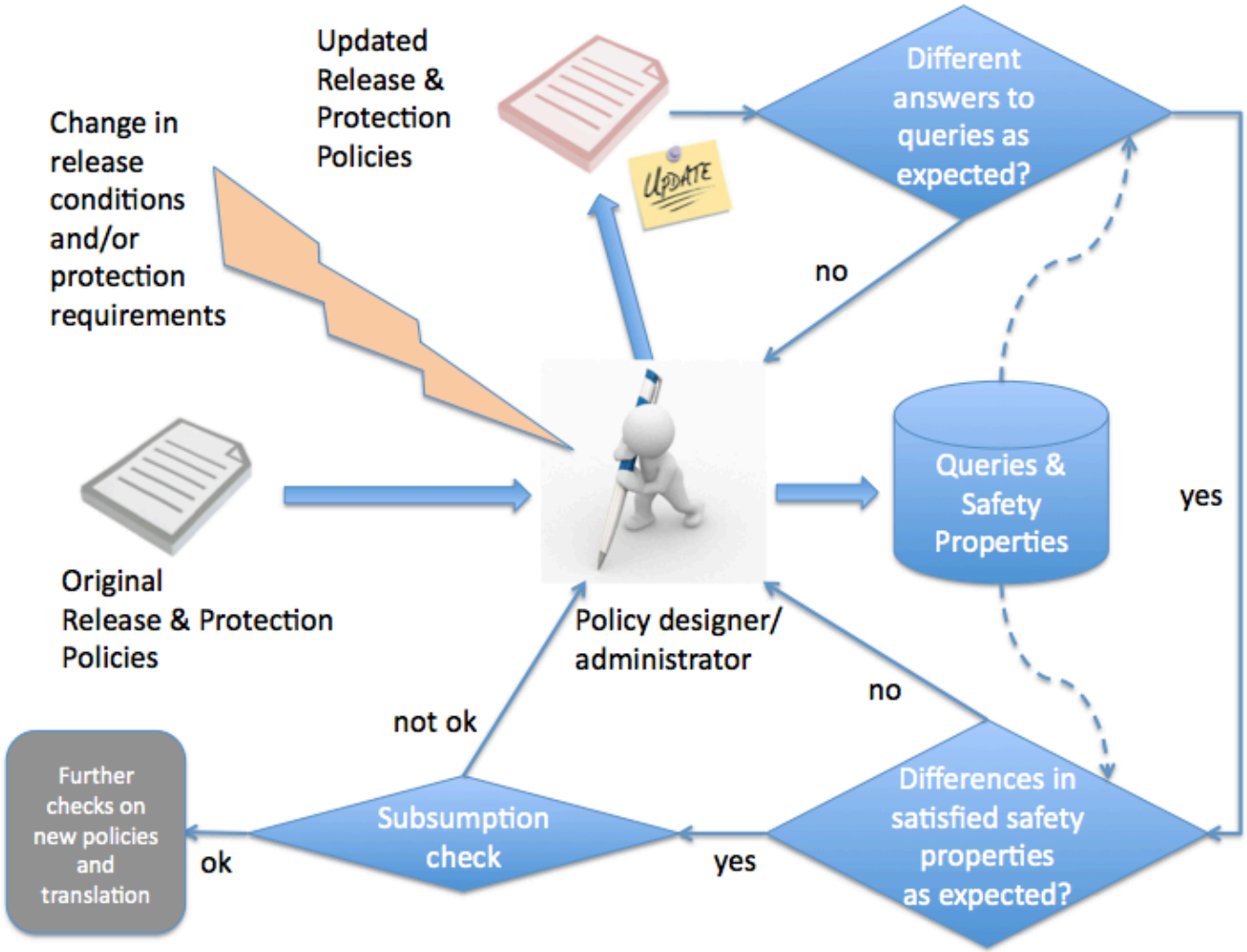
Content-based Protection and Release



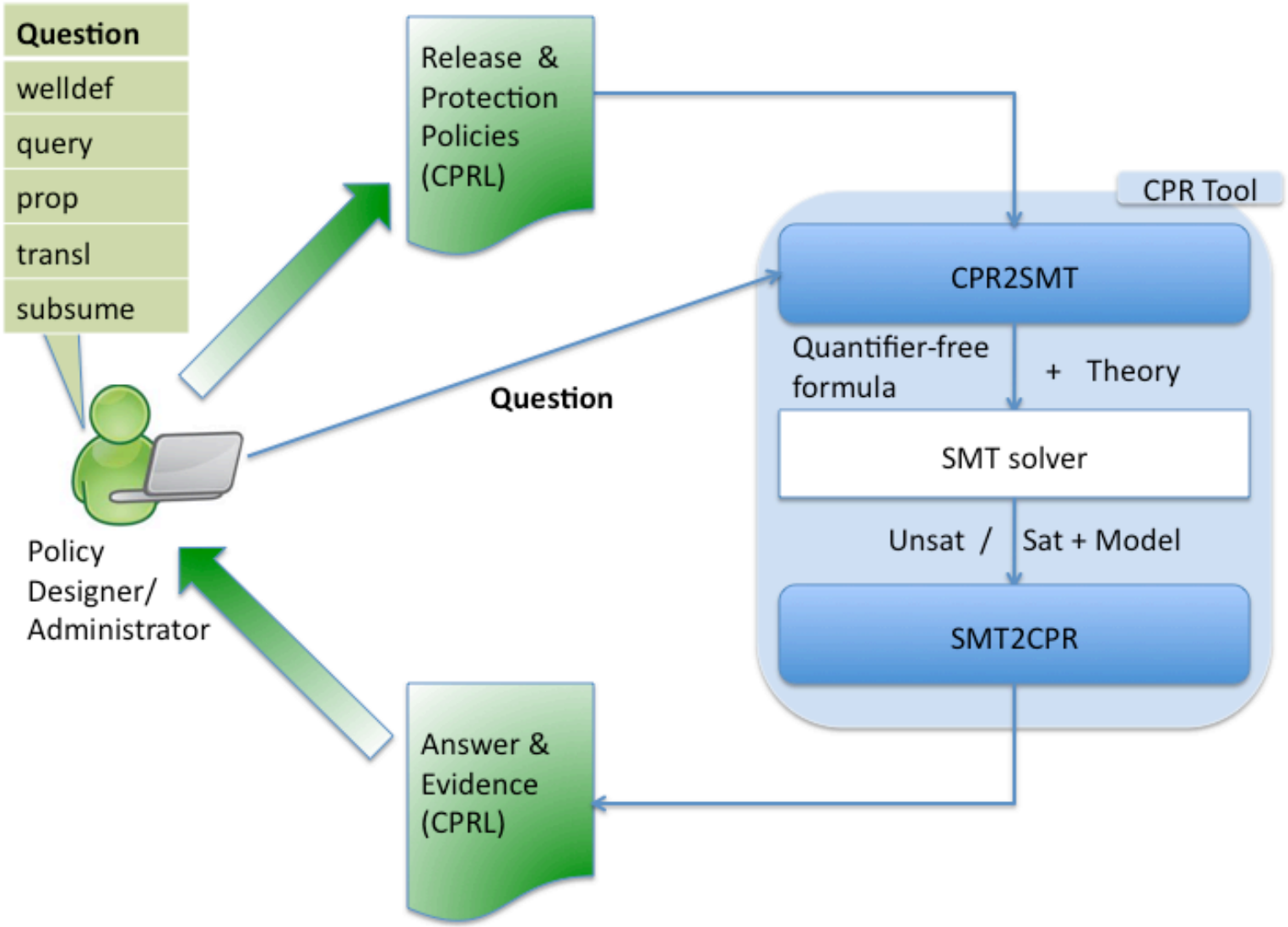
Policy Management Life Cycle (1)



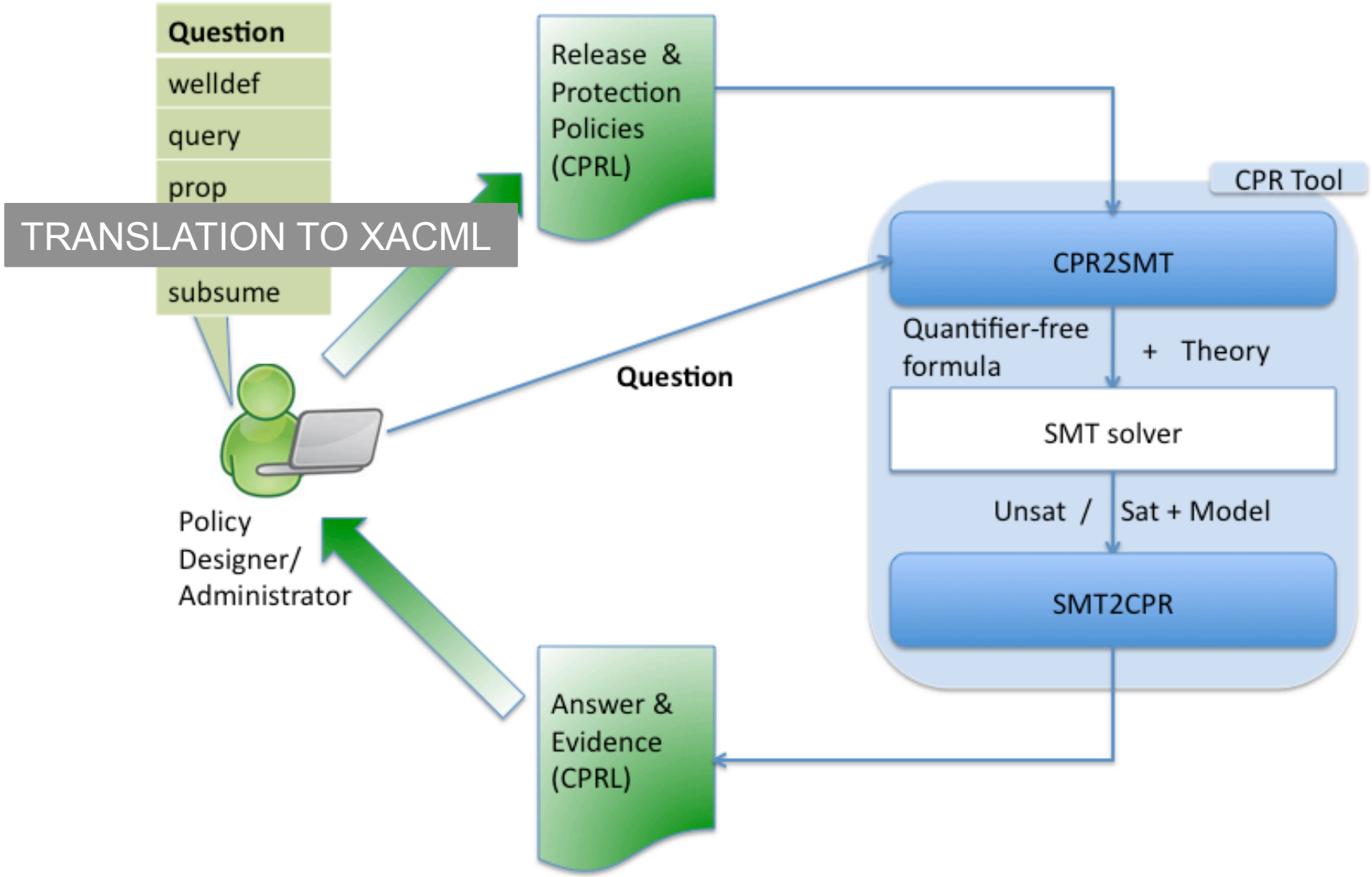
Policy Management Life Cycle (2)



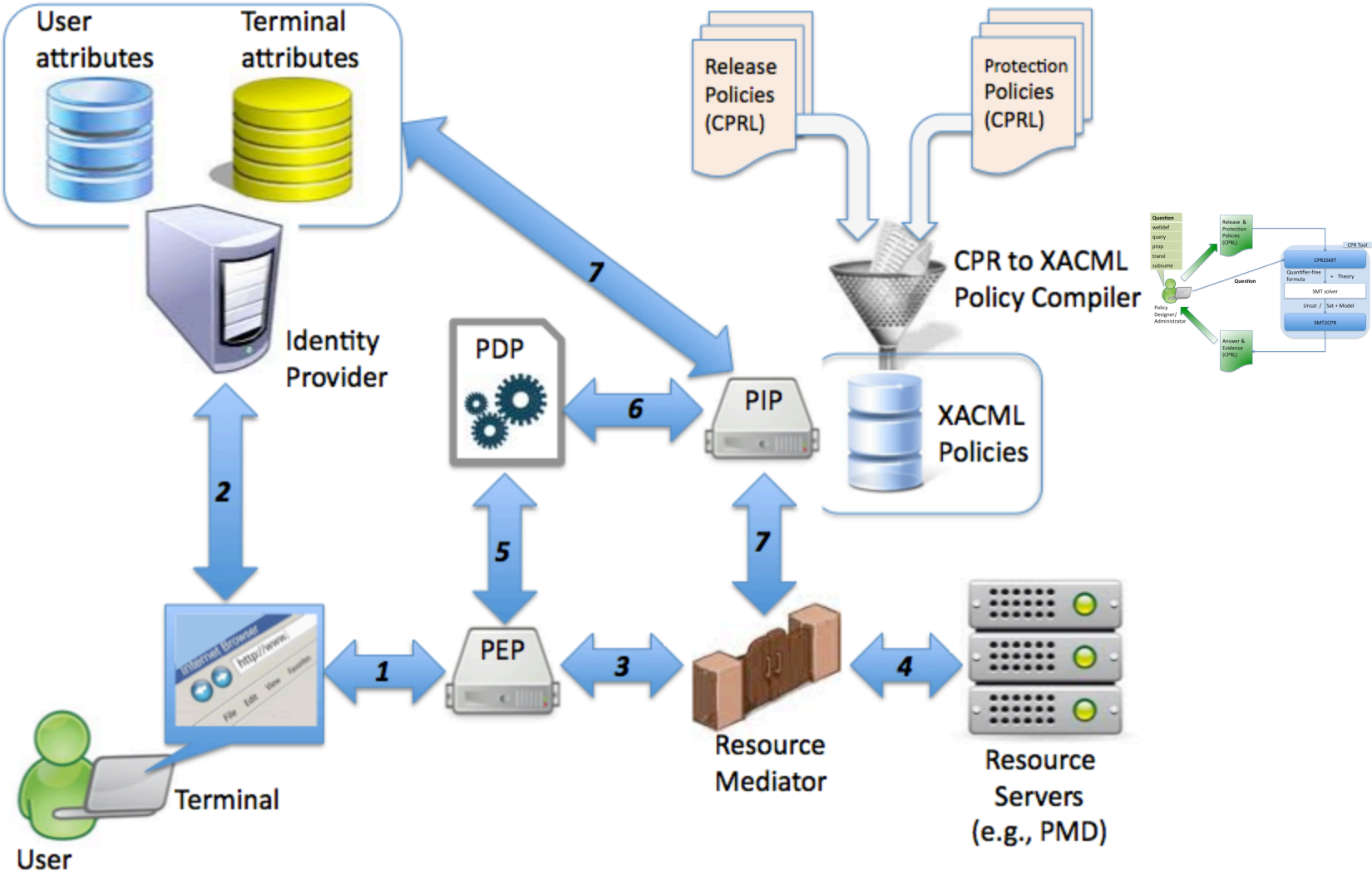
The CPR Tool: architecture



The CPR Tool: architecture



Architecture of the NATO enforcement tool



Automated analysis of NATO policies

FONDAZIONE BRUNO KESSLER

- SMT-based verification
  - Encoding of verification problems as logic problems
  - Theoretical: decidability of verification by decidability of logical problems
  - Practical: integration of state-of-the-art SMT solvers for scalability
- SMT-based enforcement
  - Enforcement of policies by translation to XACML

Access Control: problems

Administration is complex and may give rise to safety problems

ASASPXL

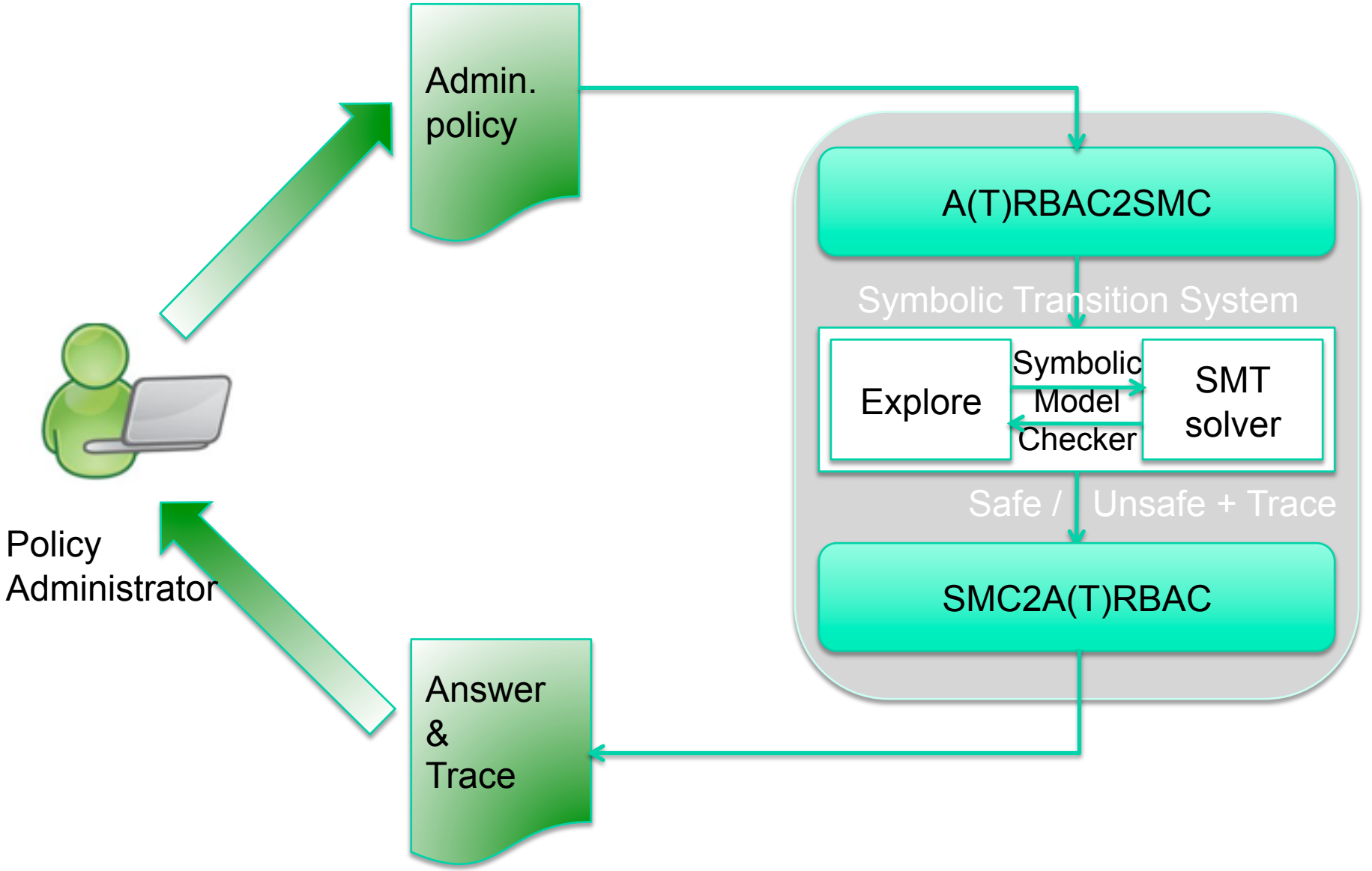
ASASPTIME

Automated analysis of Administrative Policies

FONDAZIONE BRUNO KESSLER

- Administration of policies in (extensions of) RBAC model by SMT-based model checking ASASPXL
  - Theoretical: decidability of safety wrt a ***FIXED BUT UNKNOWN NUMBER OF USERS***
  - Practical: development of a scalable tool, ***COMPETITIVE WITH*** other state-of-the-art tools such as Mohawk, VAC, PMS
- Extensions to temporal RBAC model
  - First decidability result ASASPTIME
  - Scalable tool ***BETTER THAN COMPETITOR***
  - SACMAT paper shortlisted for best paper award

ASASPXL/ASASPTIME: architecture

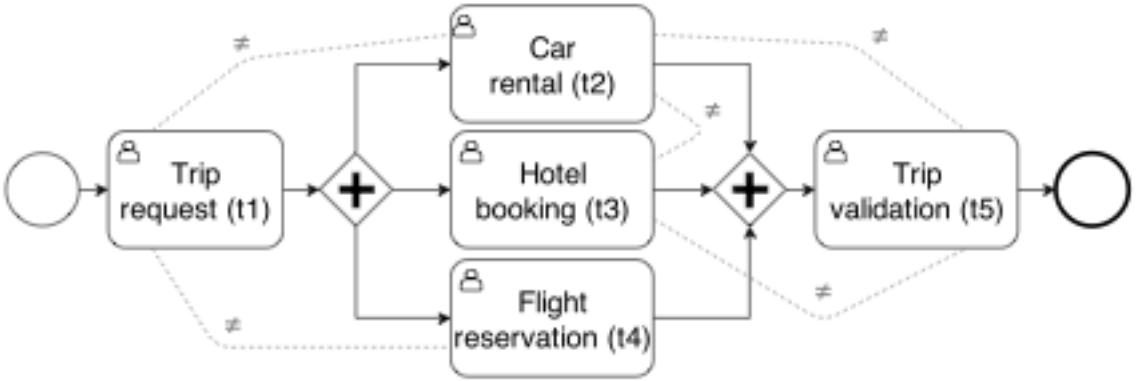


Access Control: problems

- Enforcement may become very complex in presence of computation-dependent authZ constraints

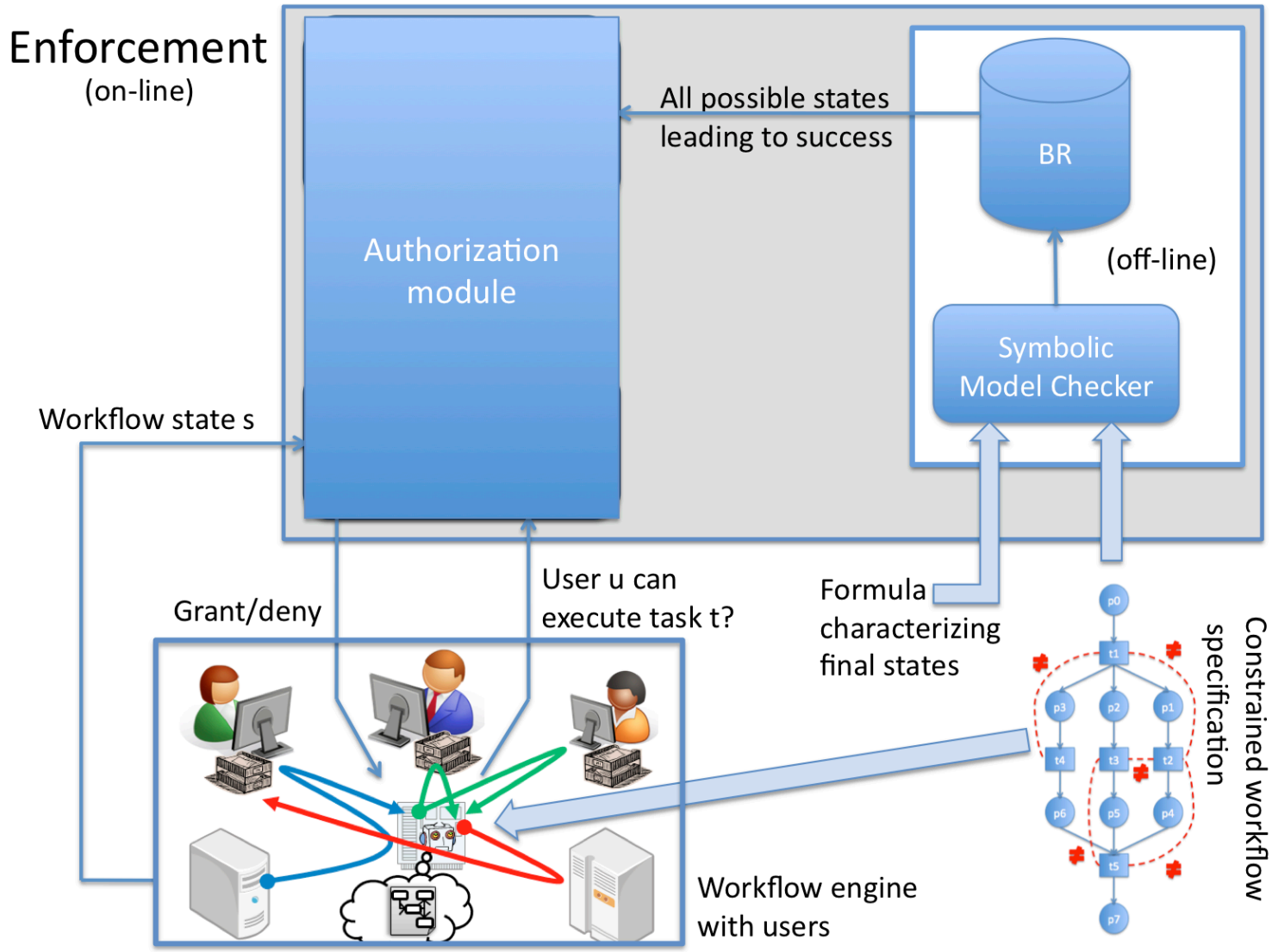
SECENTIS
A European Industrial Doctorate on Security and Trust

Synthesis of run-time monitors: problem



- Two types of authZ constraints
  - Local: user can execute a task under a policy
  - Global: Separation/Bound of Duties
- Workflow Satisfiability Problem: ensure termination while satisfying both control and authZ constraints

Synthesis of run-time monitors: solution



Access Control: problems

- Lack of a uniform framework encompassing policy design, enforcement, and extensions such as purpose for privacy

ALPS

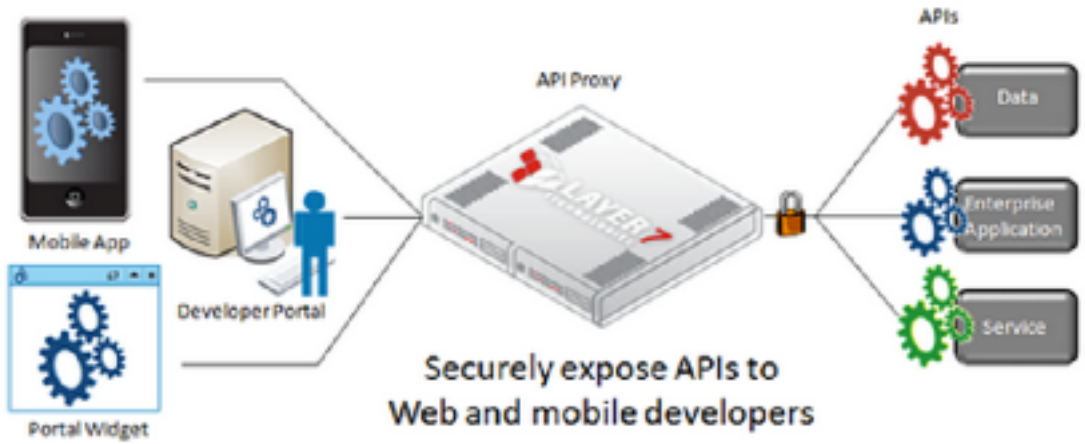
smart campus

OpenServices
Smart Community

ALPS: a uniform framework for reasoning and enforcing access control policies

- Intermediate language
  - Precise semantics
  - Expressive for encoding variety of policies
- Reuse of theoretical results (e.g., from planning) and available verification tools (e.g., model checkers)

ALPS will be used in SmartCommunity: OpenServices platform



- API-based service access
- Variety of authZ requirements
- Users becoming more and more important
    - Besides authZ also privacy constraints