Center for Information Technology - IRST

SMT for Authorization
or
How Logic and Automated Reasoning can help securing your applications

Silvio Ranise

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

&

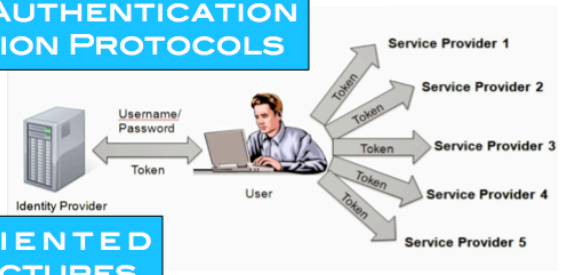
Who are I work (I): FBK Research Unit

FONDAZIONE BRUNO KESSLER

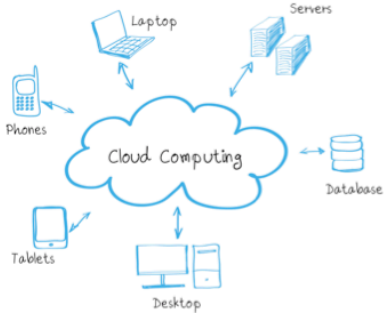
ST SECURITY & TRUST

FONDAZIONE BRUNO KESSLER

WEB-BASED AUTHENTICATION & AUTHORIZATION PROTOCOLS

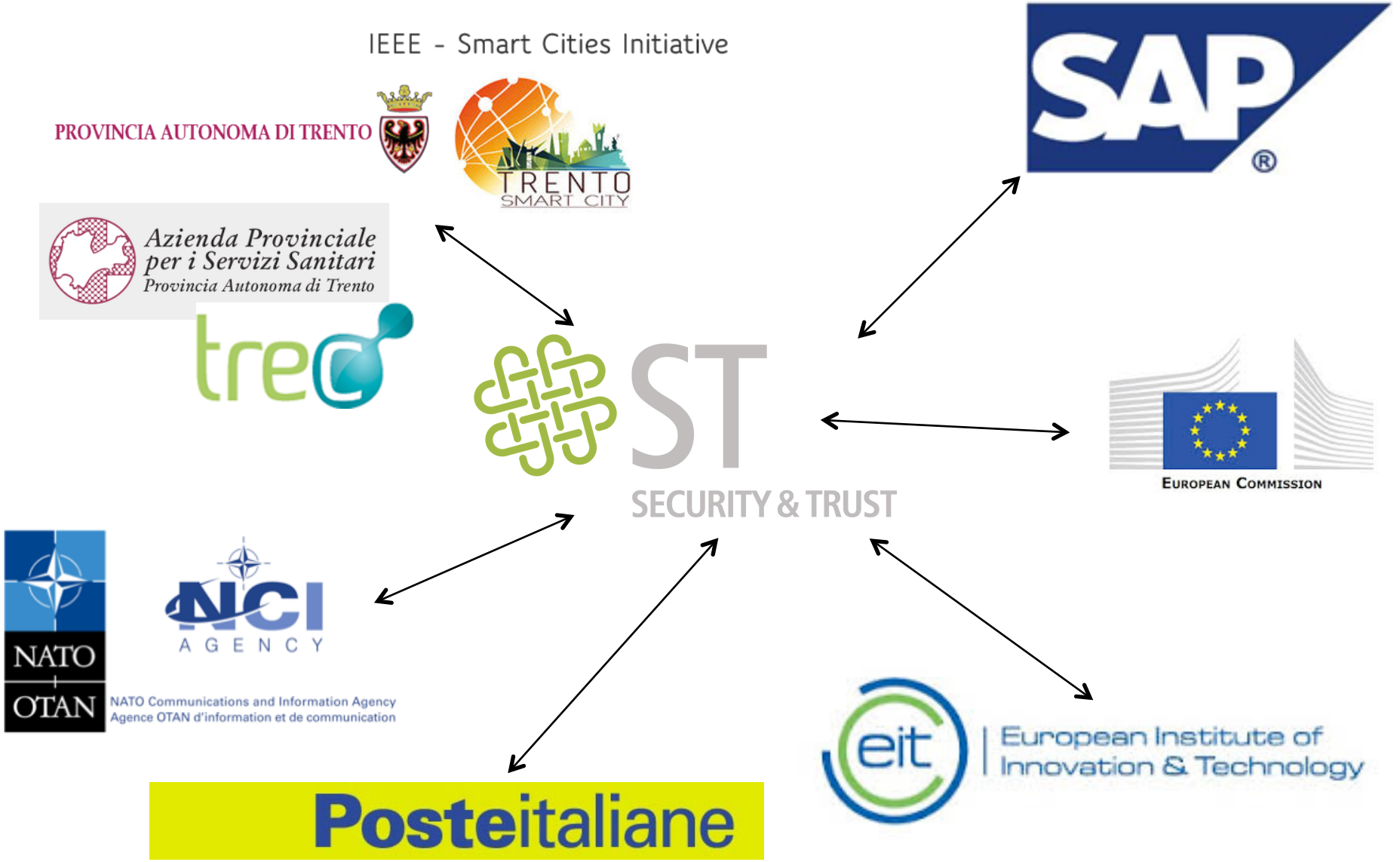


CLOUD & SERVICE-ORIENTED APPLICATIONS & INFRASTRUCTURES



MOBILE APPLICATIONS

Some Academic, PA, and Industrial collabs



Where I work (II): FBK-Poste Italiane joint lab

FONDAZIONE BRUNO KESSLER

Cyber Security Innovation Lab
Laboratorio di ricerca su tematiche di Cyber Security nato dalla collaborazione tra Poste Italiane e l'associazione Trento RISE.

ST SECURITY & TRUST

CSI Cyber Security Innovation Lab

Computer Emergency Response Team
Centro operativo di prevenzione e risposta agli incidenti informatici.

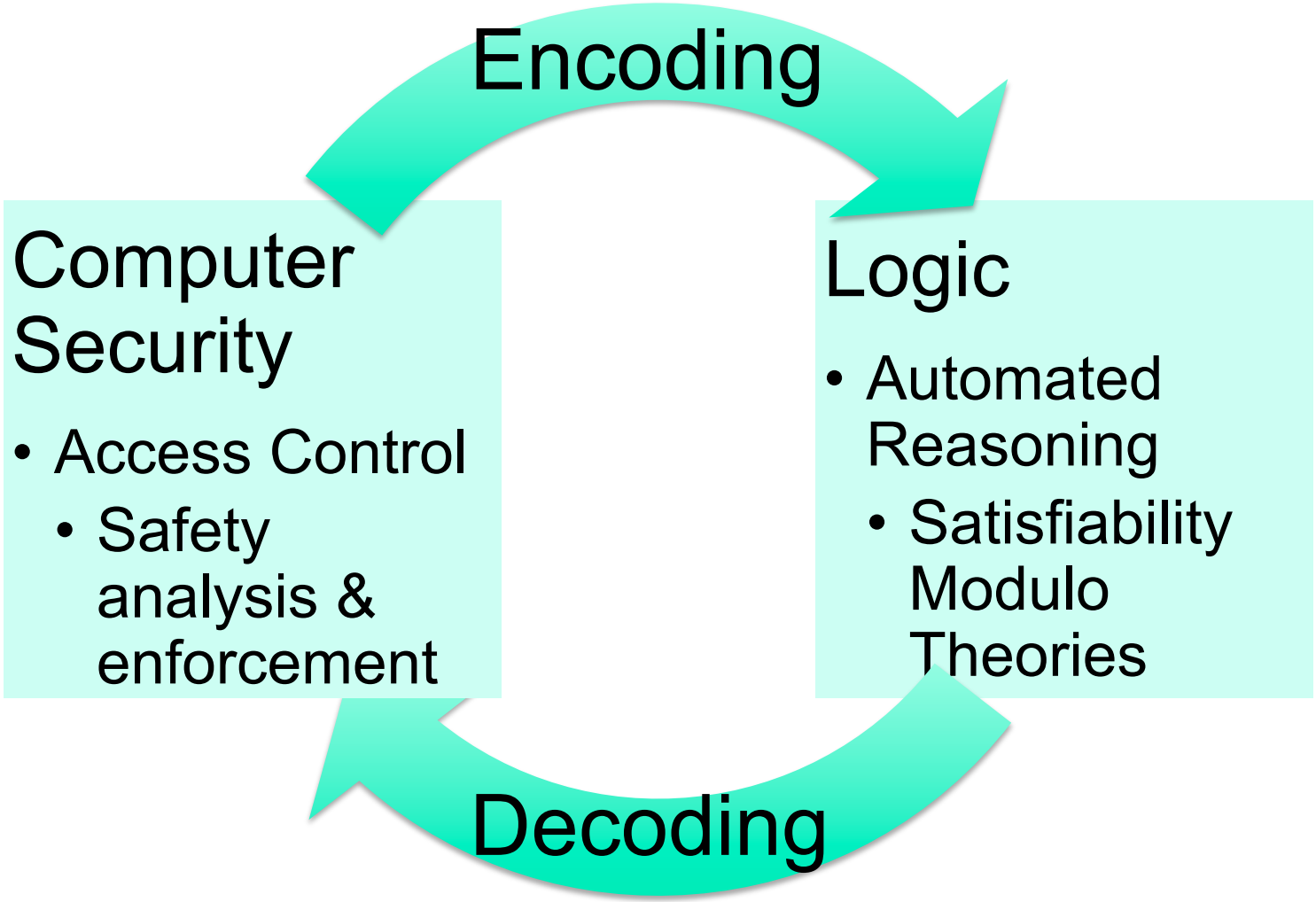
CERT Posteitaliane

Distretto di Cyber Security
Polo tecnologico per la ricerca industriale e lo sviluppo di soluzioni di sicurezza orientate alla protezione dell'end user, dei pagamenti elettronici e della dematerializzazione dei documenti. Nasce dal progetto PON finanziato dal MIUR.

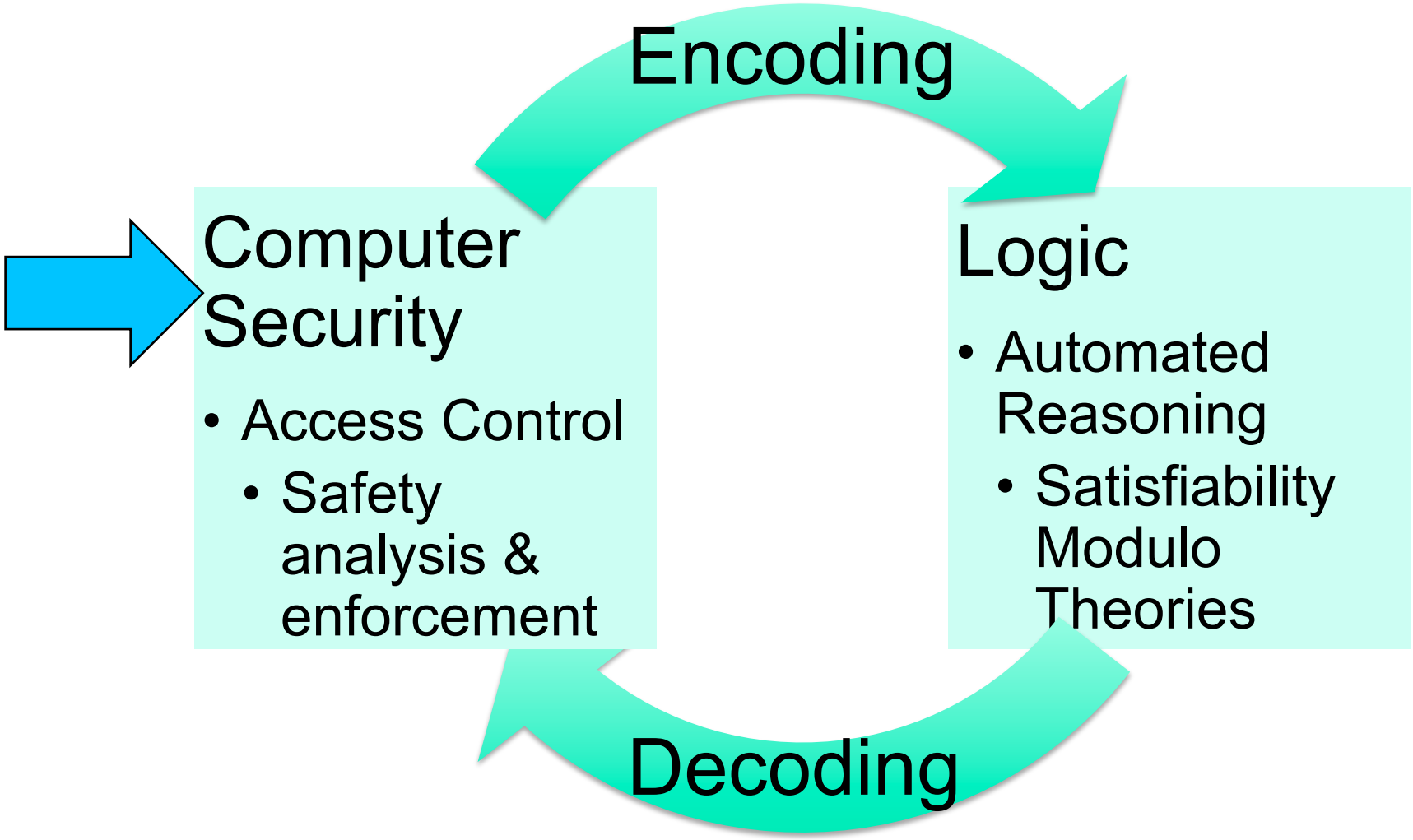
DCS Distretto Cyber Security

spid

This talk


Encoding
Computer Security
• Access Control
• Safety analysis & enforcement
Logic
• Automated Reasoning
• Satisfiability Modulo Theories
Decoding

Plan of the talk

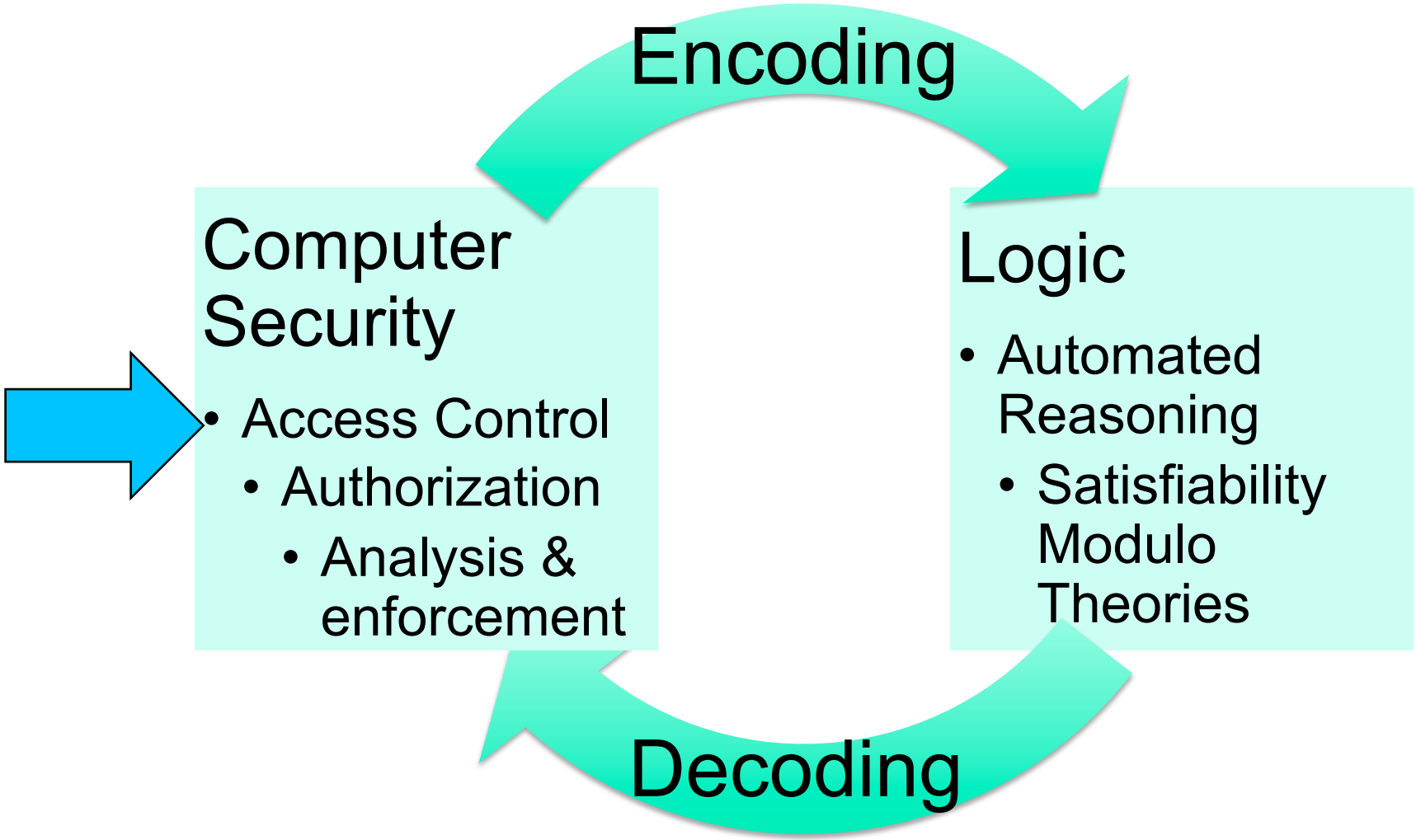


Computer Security

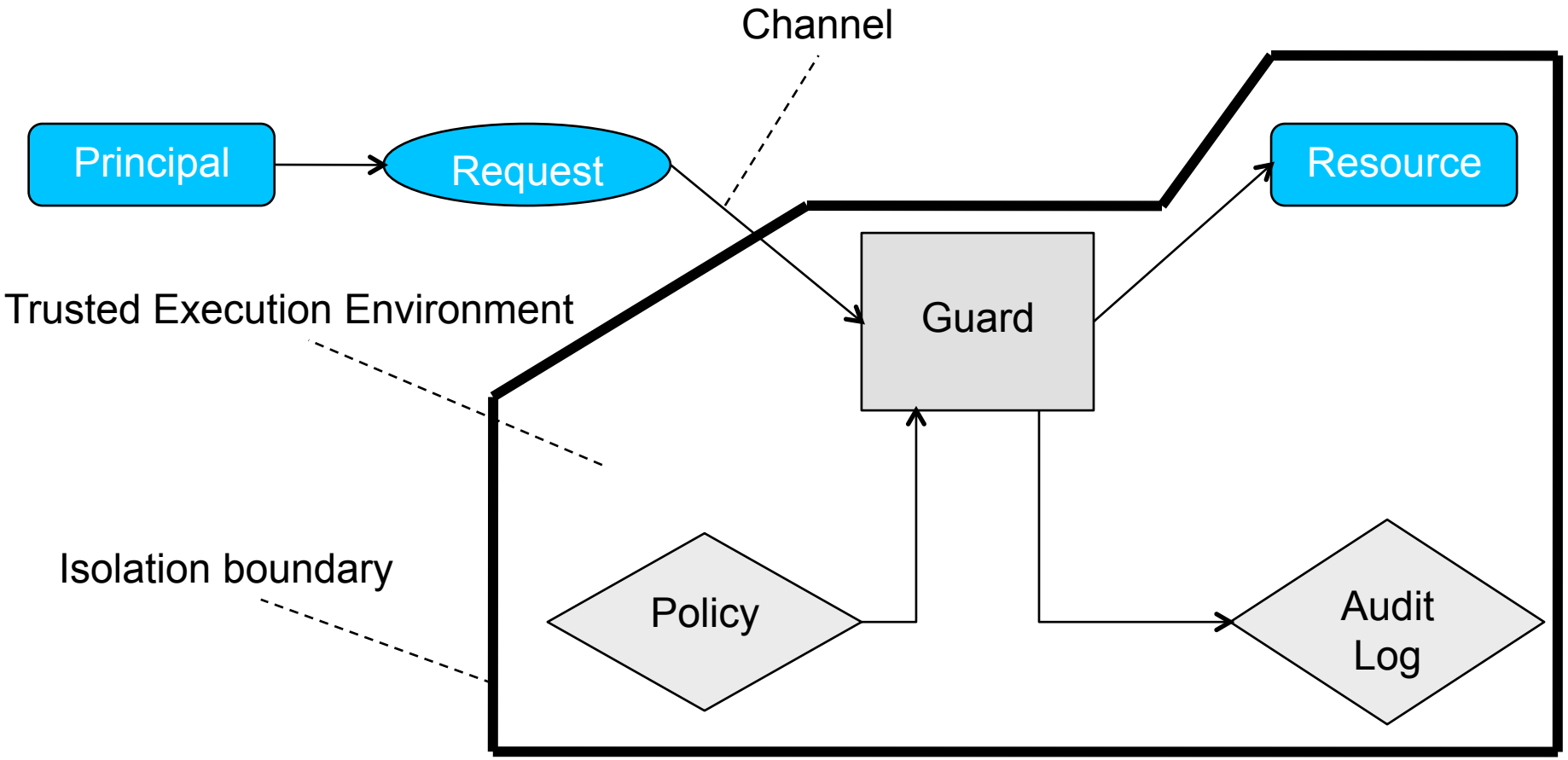
FONDAZIONE BRUNO KESSLER

- Goal of Computer Security: to defend against vulnerabilities
  - 3 types of vulnerabilities
    - Bad (buggy/hostile) programs
    - Bad (careless/hostile) agents, programs or people, giving bad instructions to good but gullible programs
    - Bad agents tapping or spoofing communications
- 5 possible defense strategies
  - Isolate: keep everyone out (best security, impractical in most cases)
  - Exclude: keep bad guys out (e.g., firewalls)
  - Restrict: keep bad guys from doing damage (e.g., sanbox)
  - Recover: undo damages done by bad guys (e.g., backup)
  - Punish: catch & prosecute bad guys (e.g., auditing)

Plan of the talk

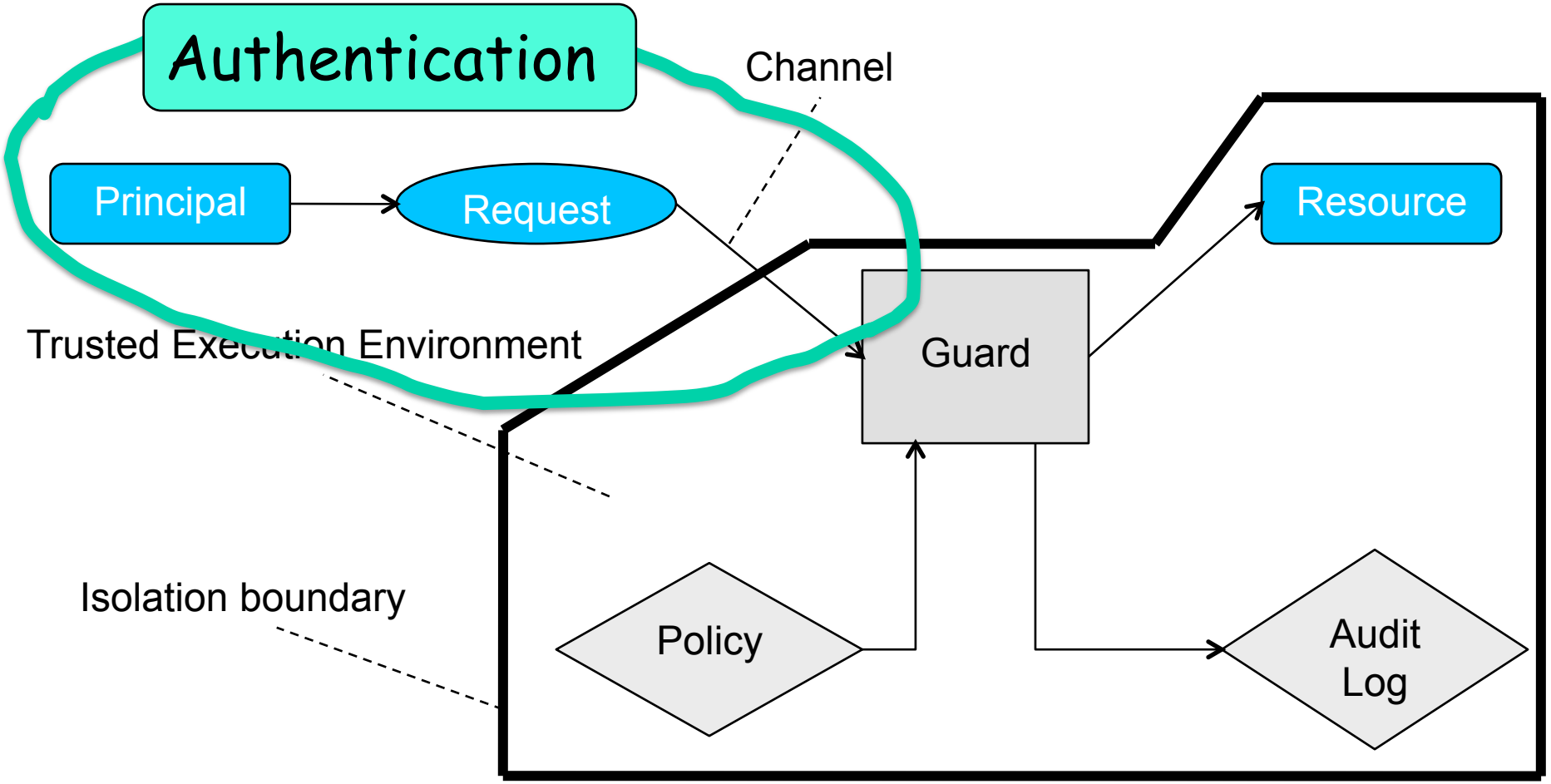


Access control



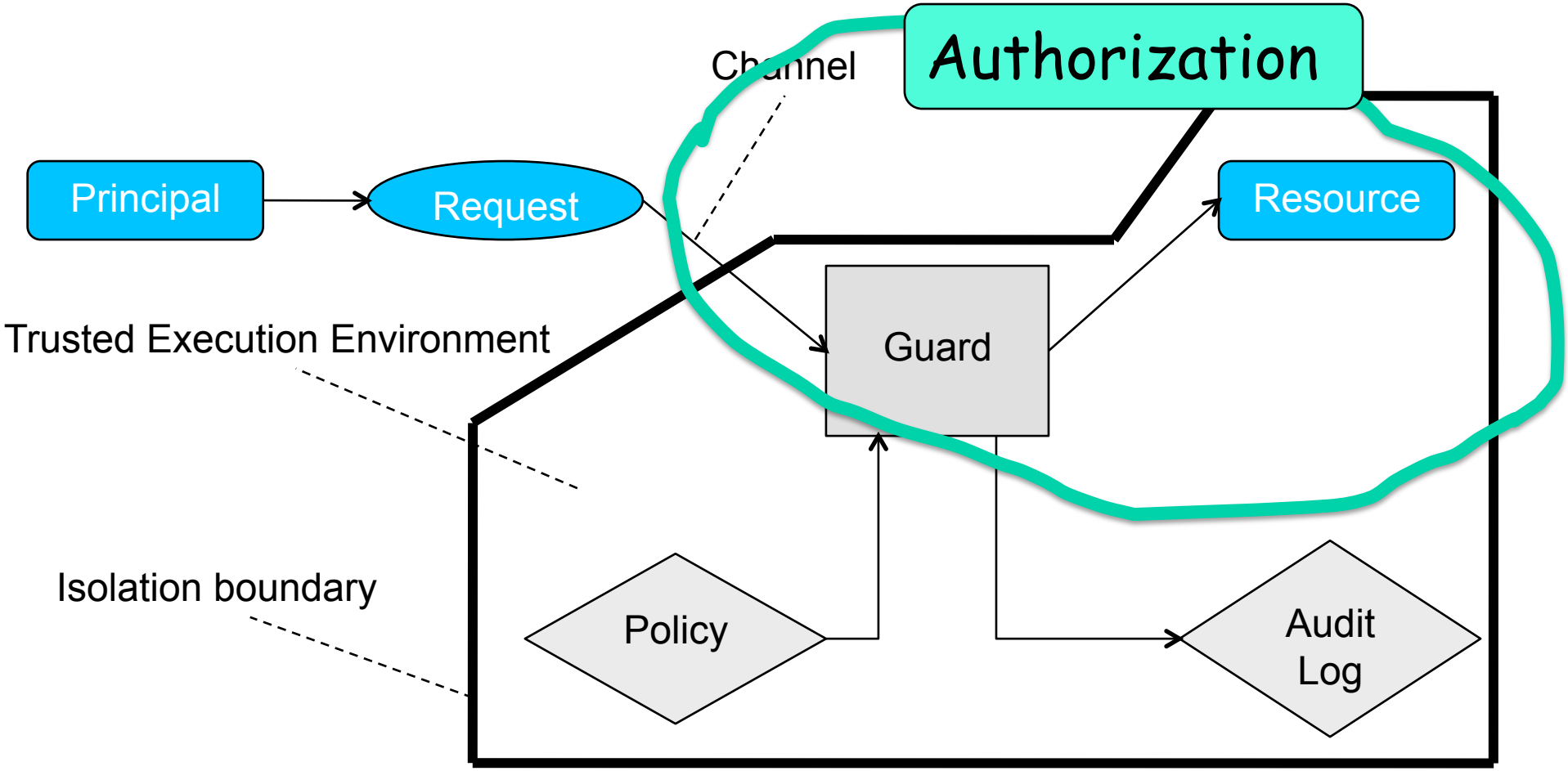
- Key security mechanism to implement 5 strategies above

Access control



- Key security mechanism to implement 5 strategies above

Access control



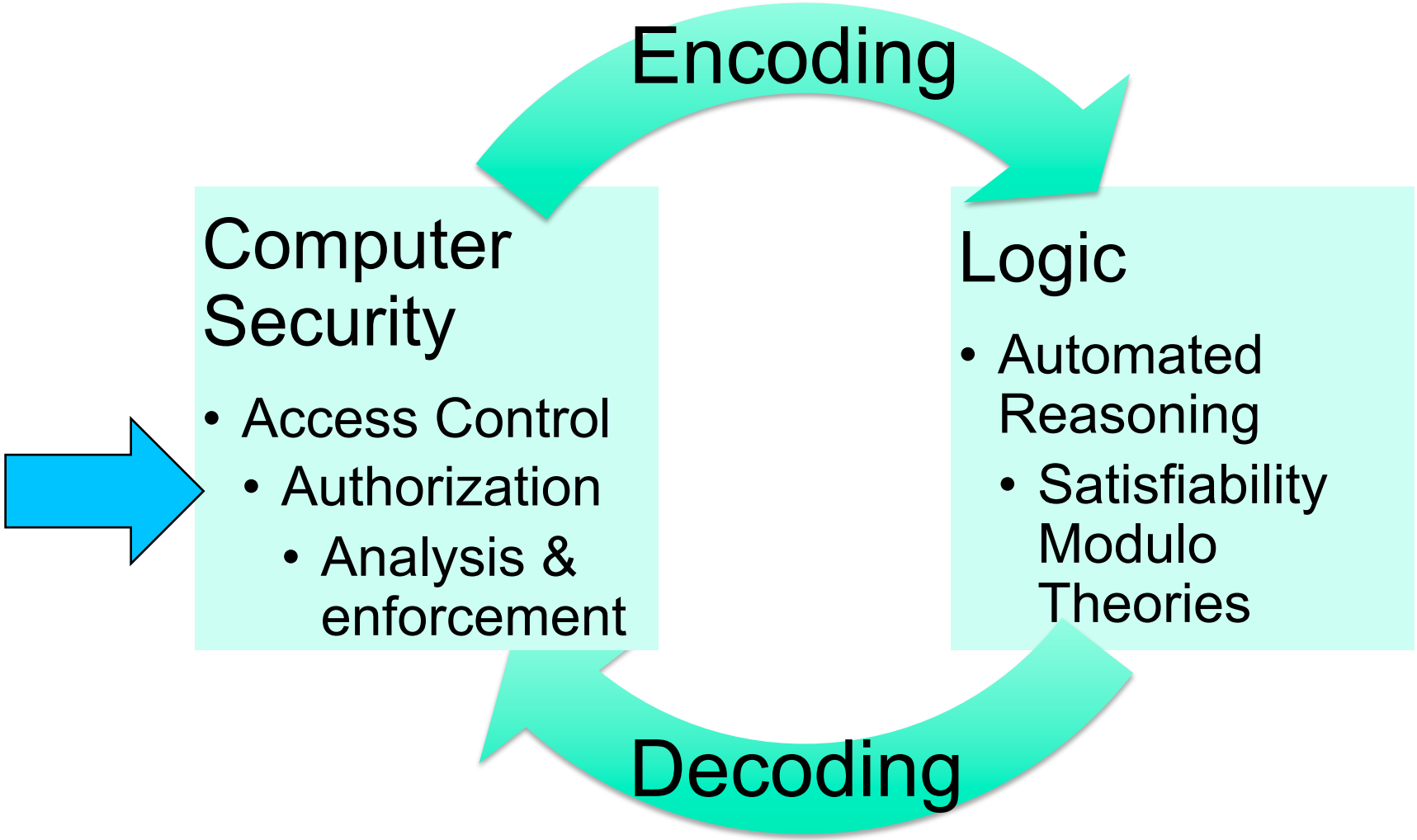
- Key security mechanism to implement 5 strategies above

AC = Authentication + Authorization + Auditing

FONDAZIONE BRUNO KESSLER

- Guard must decide whether the principal/subject (source of request) can do the operation on the resource/object
- To decide, guard uses
  - Authentication information = Who is getting info?
  - Authorization information = Who is trusted to do which operations on objects?
- Auditing = What happened and why?
- Crucial: the guard must see every request on object
  - Isolation boundary blocks all access to object except over the channel passing through the guard
- Policy = set of rules specifying conditions for principal to access resource based on features of principals, resources, and contextual information (e.g., time, location, …)

Plan of the talk



Authorization

- Authorization = Who is trusted to access a resource?
  - Confidentiality
    - Who can read the info stored in a resource?
  - Integrity
    - Who can write/update the info stored in a resource?
  - Availability
    - Are resources available when needed by trusted users?

- Note: boundary between authentication and authorization blurred, especially in modern applications

A framework for authorization

FONDAZIONE BRUNO KESSLER

Policy

- Rules specifying what actions principals may perform

Model

- Mathematical representation of the policy and its workings

Enforcement

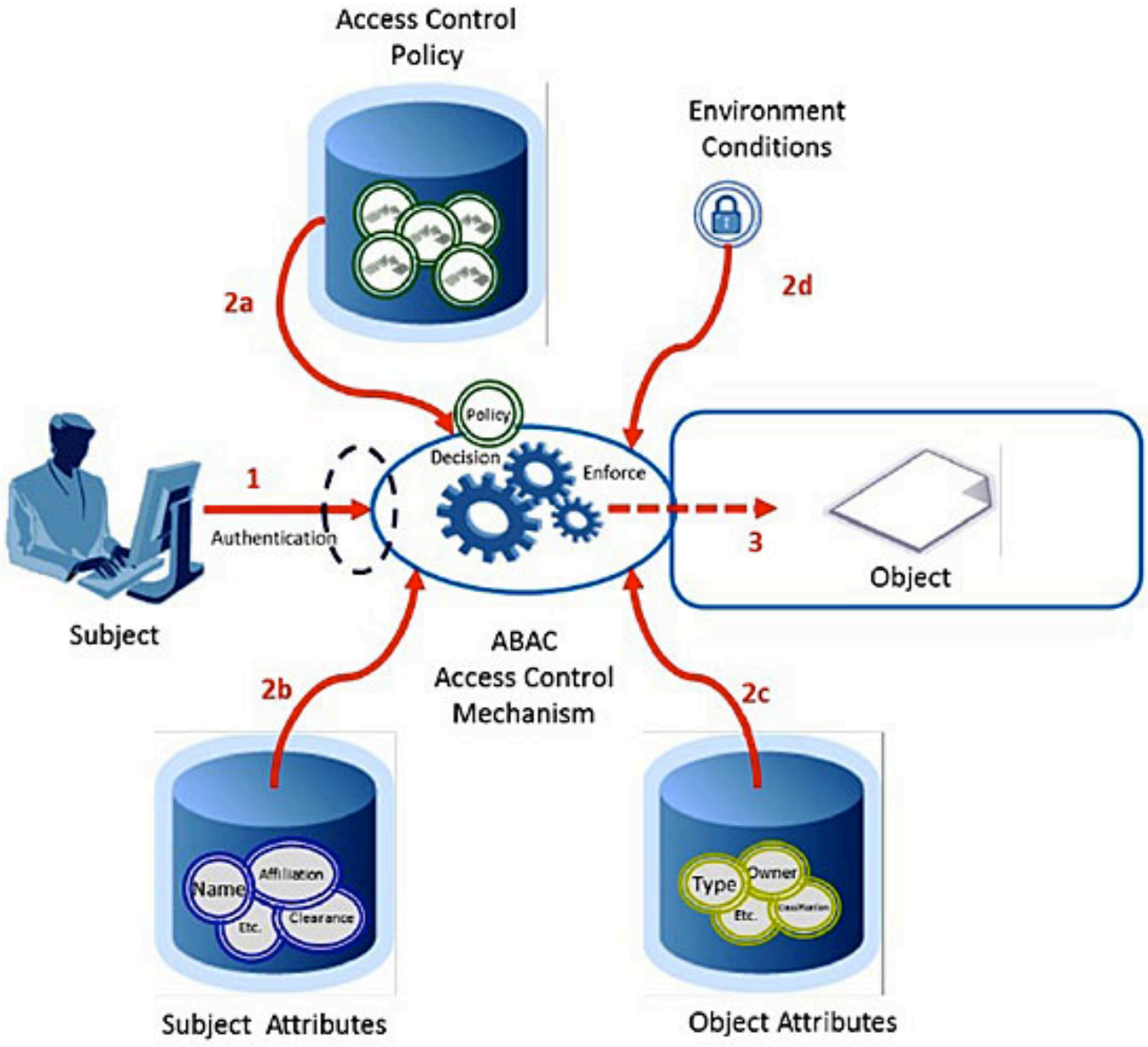
- Low level (SW/HW) functions implementing control imposed by policy and formally stated in the model

Attribute Based Access Control (ABAC)

FONDAZIONE BRUNO KESSLER

- Entities: Subjects, Actions, Objects, Environments
- Each entity has a set of attributes
  - Attribute = typed variable taking values on a domain
  - "e.a" is the attribute "a" of the entity "e"
- Attribute predicate = Boolean predicate on attributes
  - Can be specified by Boolean expressions on attributes and operators of the appropriate type, e.g.
    - Alice.Credit >= 100 & File.Classification = Secret
    - Alice.Credit >= Ebook.Value || …
- Policy = attribute predicate on the attributes of subject, action, object, and environment
- Request = list of pairs (attribute,value) for subject, action, object, and environment

ABAC: overview



ABAC: answering queries

- Policy P(s,a,o,e): predicate on attributes of s,a,o,e
- Query q=(s*,a*,o*,e*)
  - Encodes “Can s* perform a* on o* in e*?”
- Answering query q:

  “s* can perform a* on o* in e*” iff P(s*,a*,o*,e*) = TRUE
- Problem: which queries are allowed/denied by P?
- Problem: is a given set of queries allowed/denied by P?
- Problem: which queries are allowed/denied by two policies?
  - Difficult because policies can be specified by large & complex Boolean expressions
  - Answer should be found regardless of the enforcement mechanism

A framework for authorization

FONDAZIONE BRUNO KESSLER

Policy

- Rules specifying what actions principals may perform

Model

- Mathematical representation of the policy and its workings

Logical pbs, **independent of enforcement**

- Large number of rules
- Conditions depending on several features
- Evolving policies

A framework for authorization

Implementation pbs, **dependent from enforcement**

- Several technological scenarios
- Different security assumptions
- Authorization may depend on user device

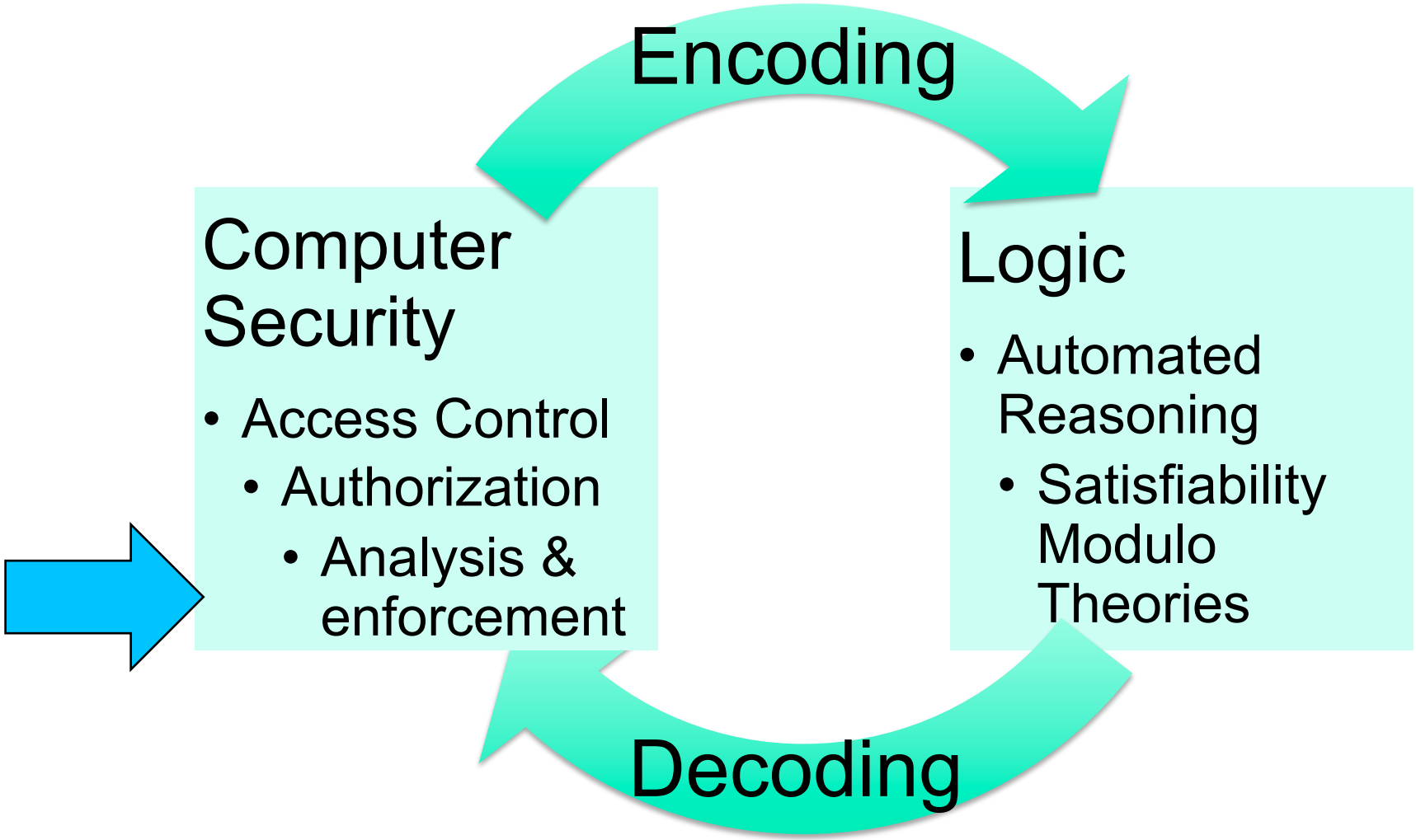
Model

- Mathematical representation of the policy and its workings

Enforcement

- Low level (SW/HW) functions implementing control imposed by policy and formally stated in the model

Plan of the talk

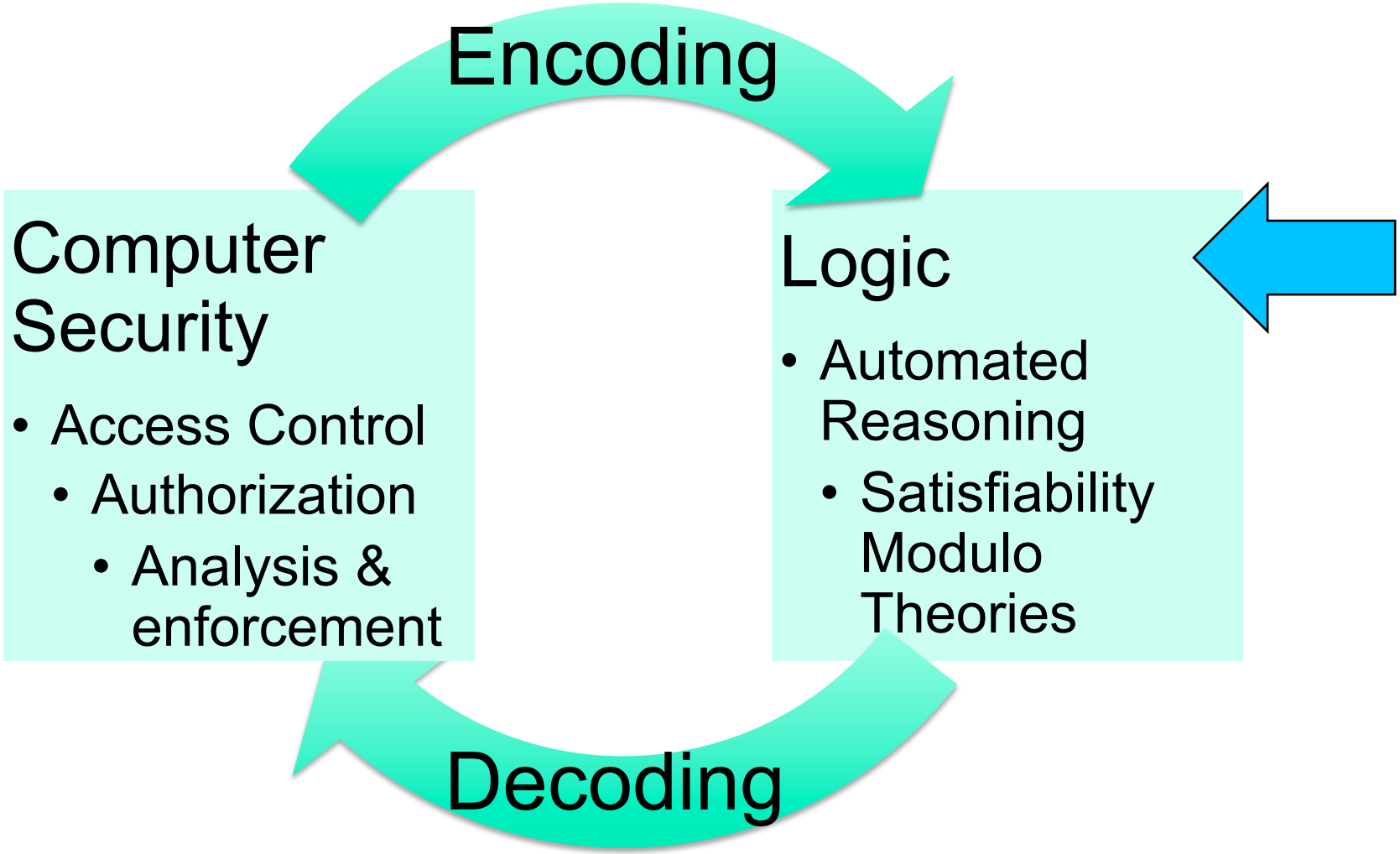


To get authorization right…

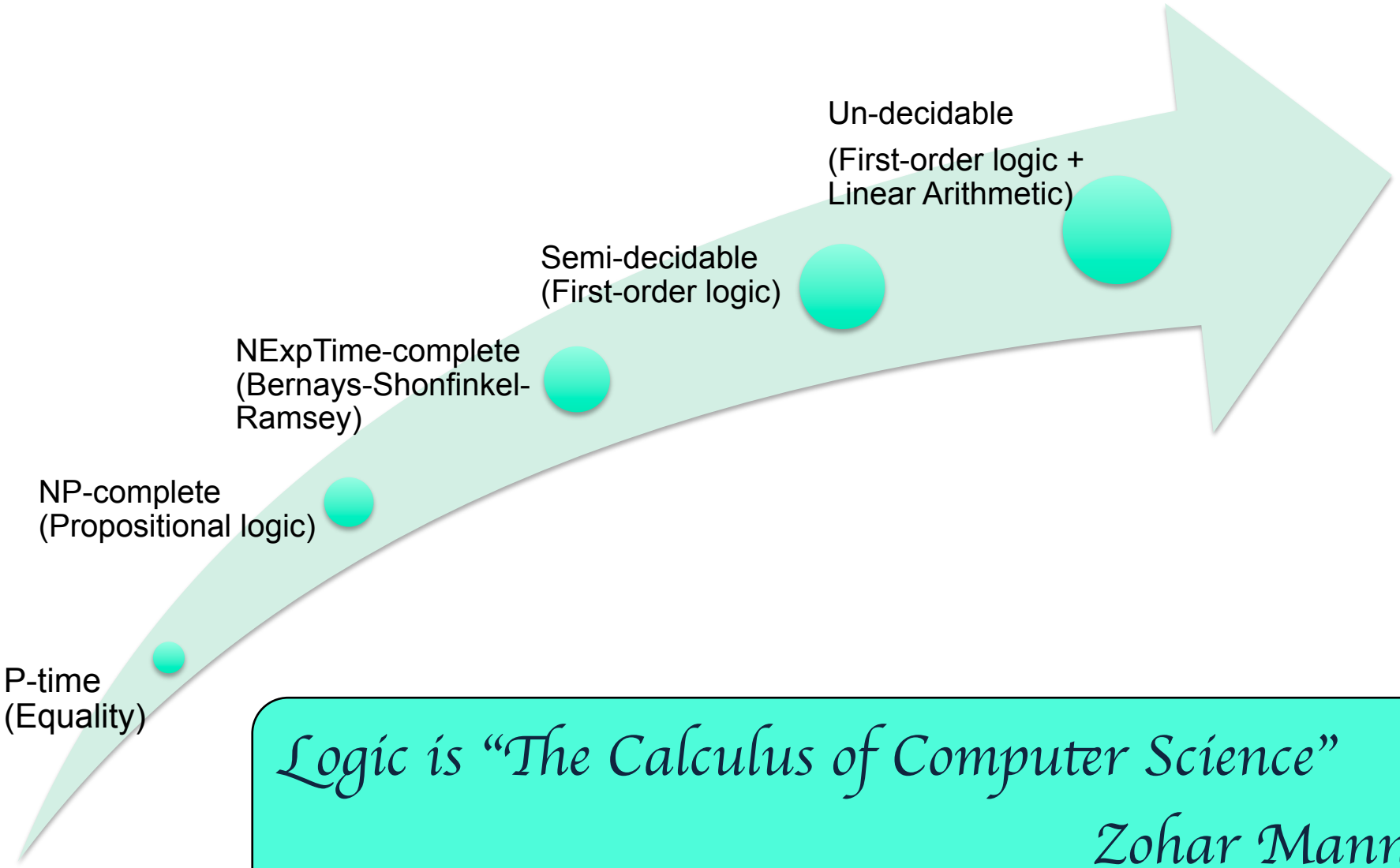
Need of automated techniques for

- Analysis @ design time for policy validation
  - scenarios, safety, …
  - change impact, refinement
- Enforcement @ deployment time for information sharing
  - from unique/coherent policy
  - in different technological scenarios and on different devices

Plan of the talk



Logic (First Order)



Logic is "The Calculus of Computer Science"

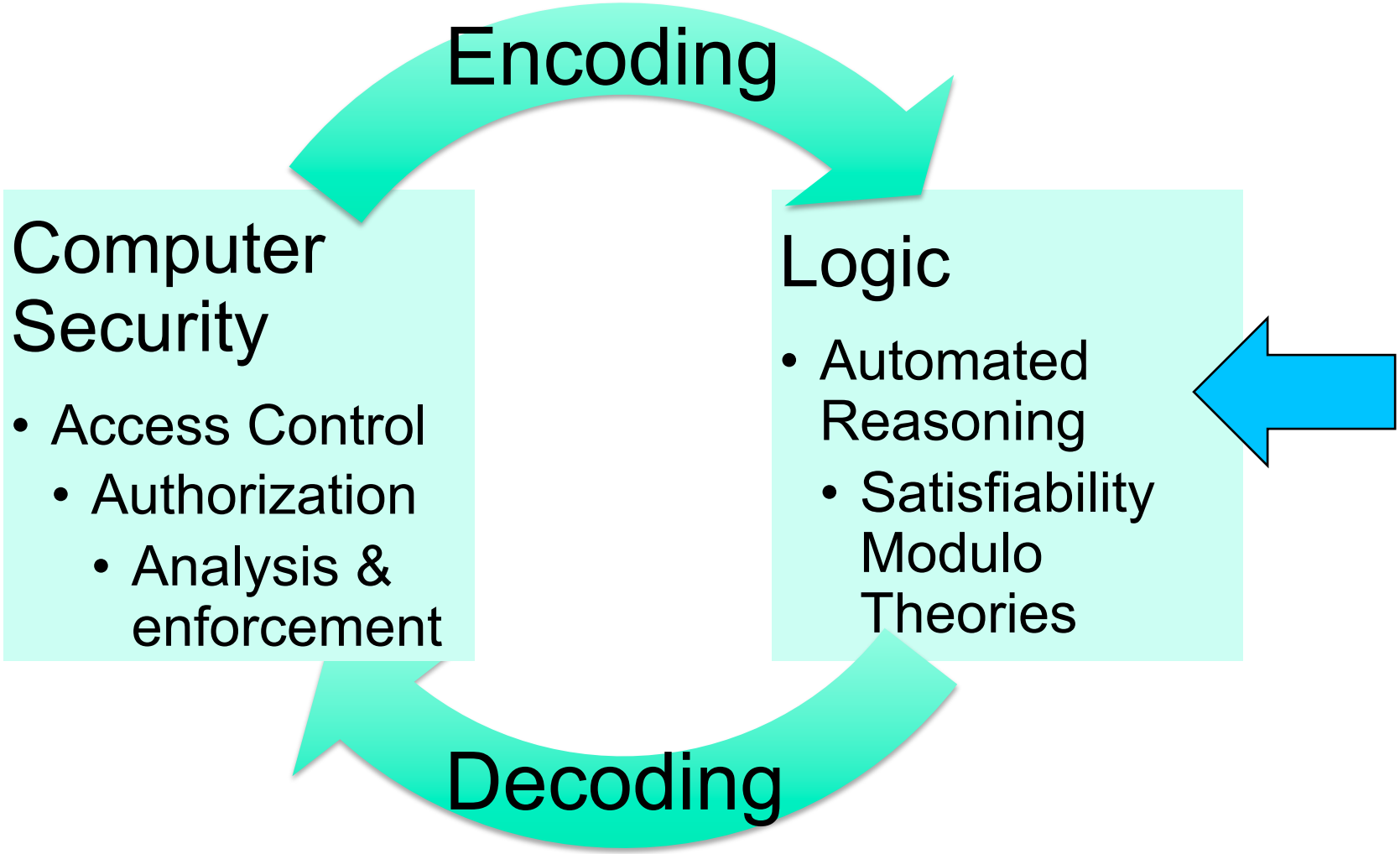
Zohar Manna

Problems in First Order Logic

FONDAZIONE BRUNO KESSLER

- Validity
  - Does formula φ hold in all models?
- Satisfiability
  - Is there a model in which formula φ holds?
- Formula φ is valid iff the negation of φ is unsatisfiable
- From now, we focus on satisfiability in FOL…

Plan of the talk



Automated Reasoning for **First Order Logic**

FONDAZIONE BRUNO KESSLER

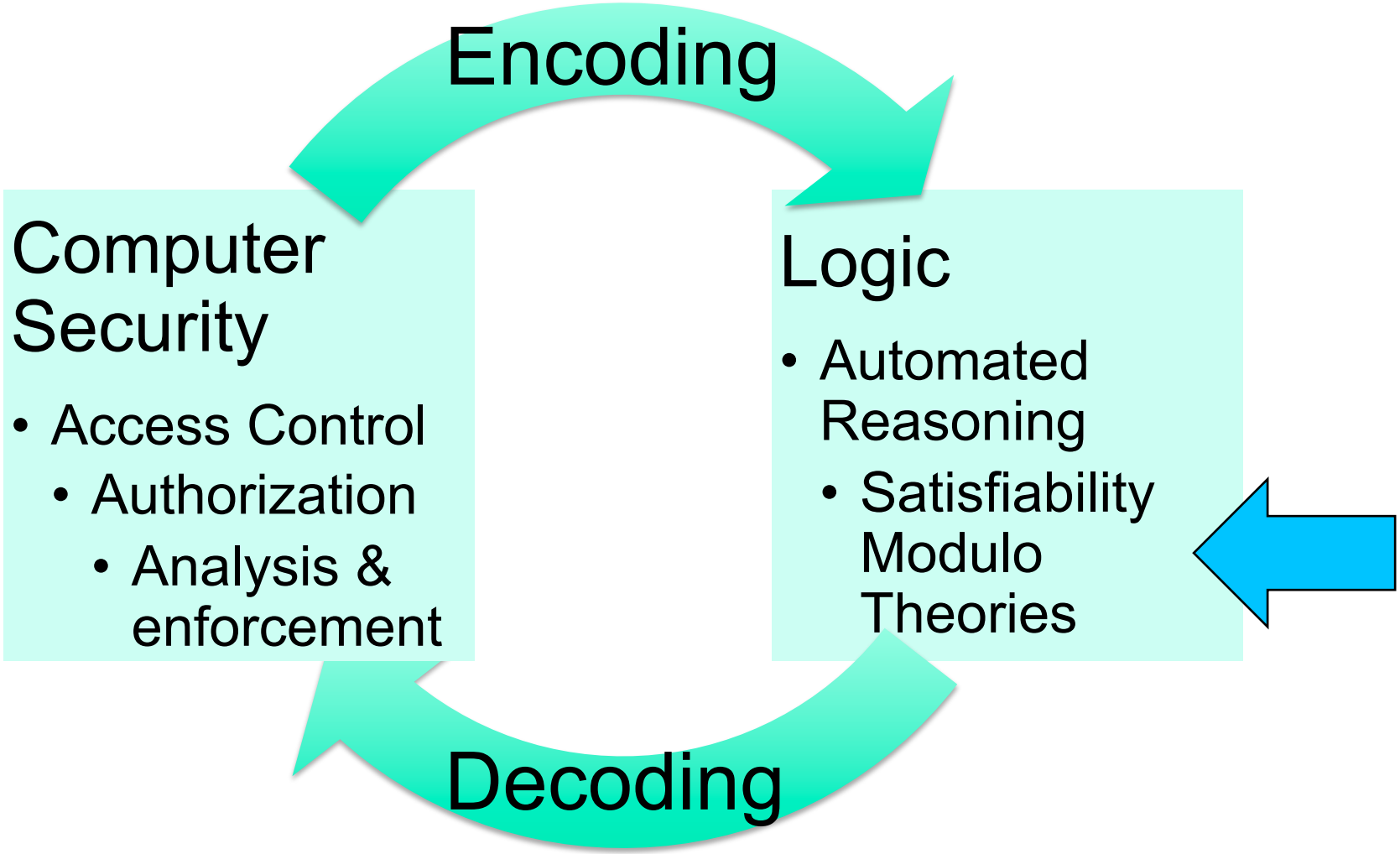
Expressivity

- Propositional
- Quantifier-free
- Quantifier prefix
- Full
- …

Decidability

- DPLL
- Resolution
- Decision procedures
- Quantifier instantiation & elimination
- Superposition
- …

Plan of the talk



Satisfiability Modulo Theories (SMT)

FONDAZIONE BRUNO KESSLER

- Satisfiability problem = determining whether a formula φ has a model
  - If φ is propositional, a model is a truth assignment to Boolean variables
  - If φ is a first-order formula, a model assigns values to variables and interpretations to the function and predicate symbols
- For some theories the problem is decidable (e.g., equality, linear arithmetic, arrays, …)

SMT in a nutshell

FONDAZIONE BRUNO KESSLER

- SMT framework = FOL + Theories
- Theory = Language + Class of Interpretations
- Examples:
  - Equality
  - Linear Arithmetic
  - Records
  - Lists
  - Combinations
  - …

SMT in a nutshell (cont'd)

FONDAZIONE BRUNO KESSLER

- Theories can be used to model many data types used in Computer Science
- SMT solving subsumes SAT solving but…
- … in practice, heuristics significantly improve on worst-case complexity…
- SMT-Lib initiative
- SMT solvers can be easily integrated in other tools

SMT solvers eat NP for lunch!
Byron Cook

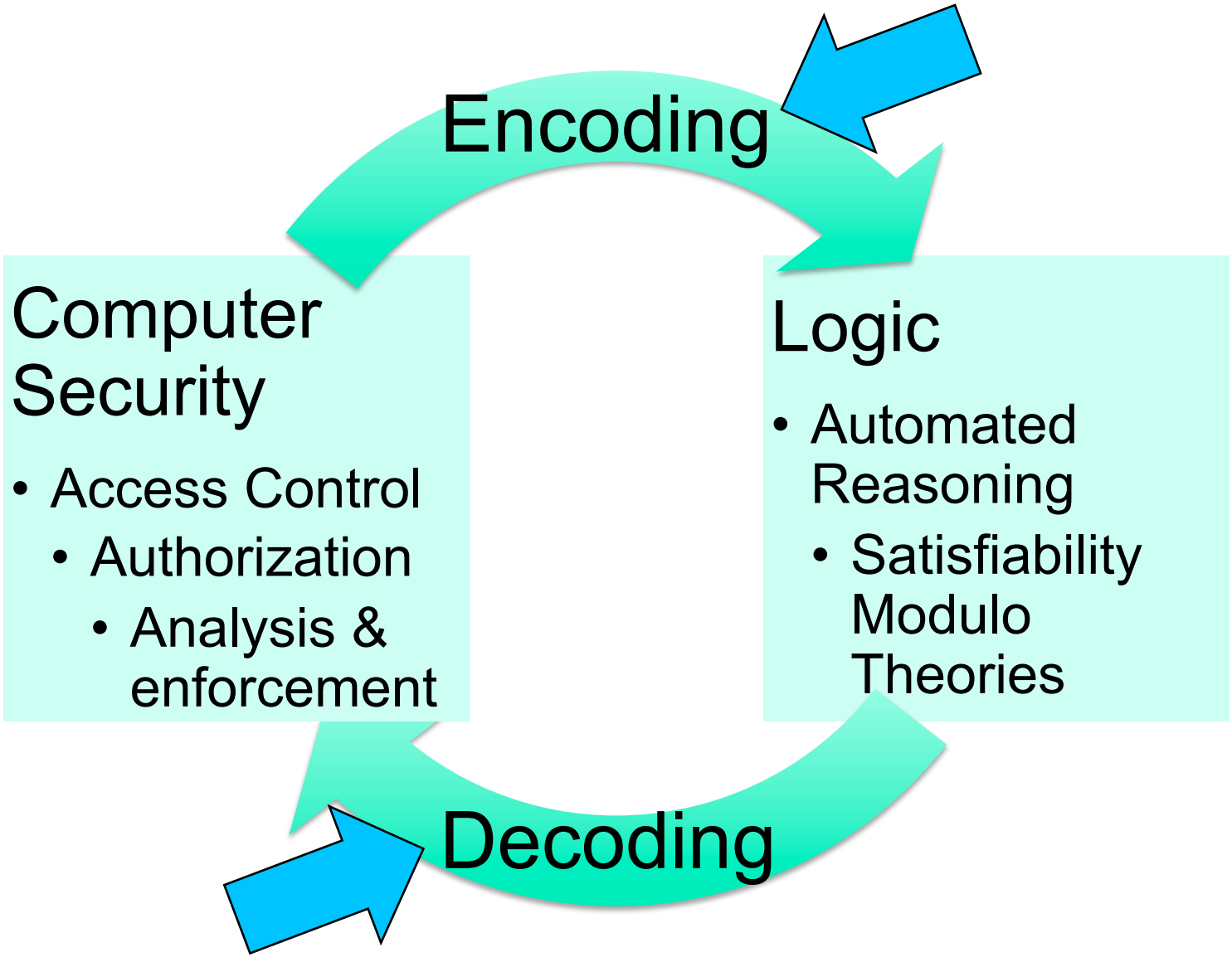
SMT: why is it useful

FONDAZIONE BRUNO KESSLER

- Many combinatorial problems can be translated to satisfiability problems in (fragments of) FOL and …
- … available SMT solvers can efficiently solve such problems*!*

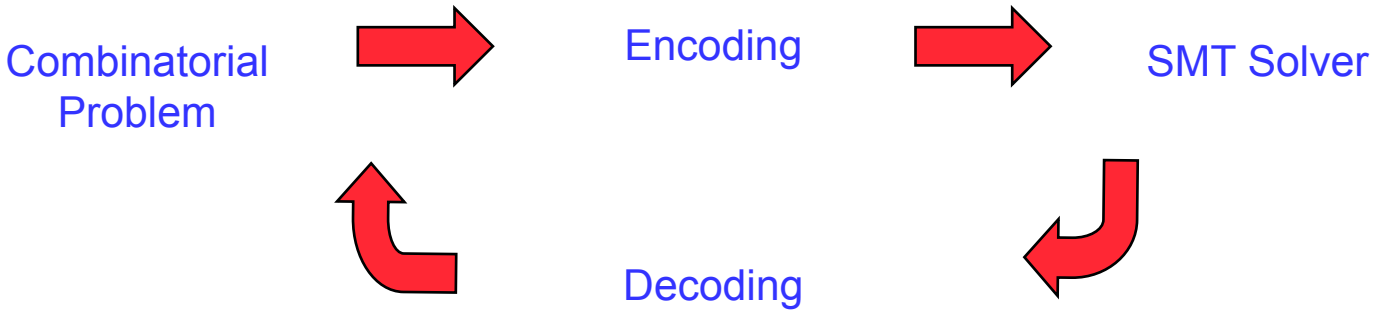
- For instance, SMT solving has been adopted in industrial verification
  - Z3 @ Microsoft
  - MathSat @ Intel, UTC
  - Yices @ Galois
  - others @ GrammaTech, NVIDIA, Dassault Aviation, …

Plan of the talk



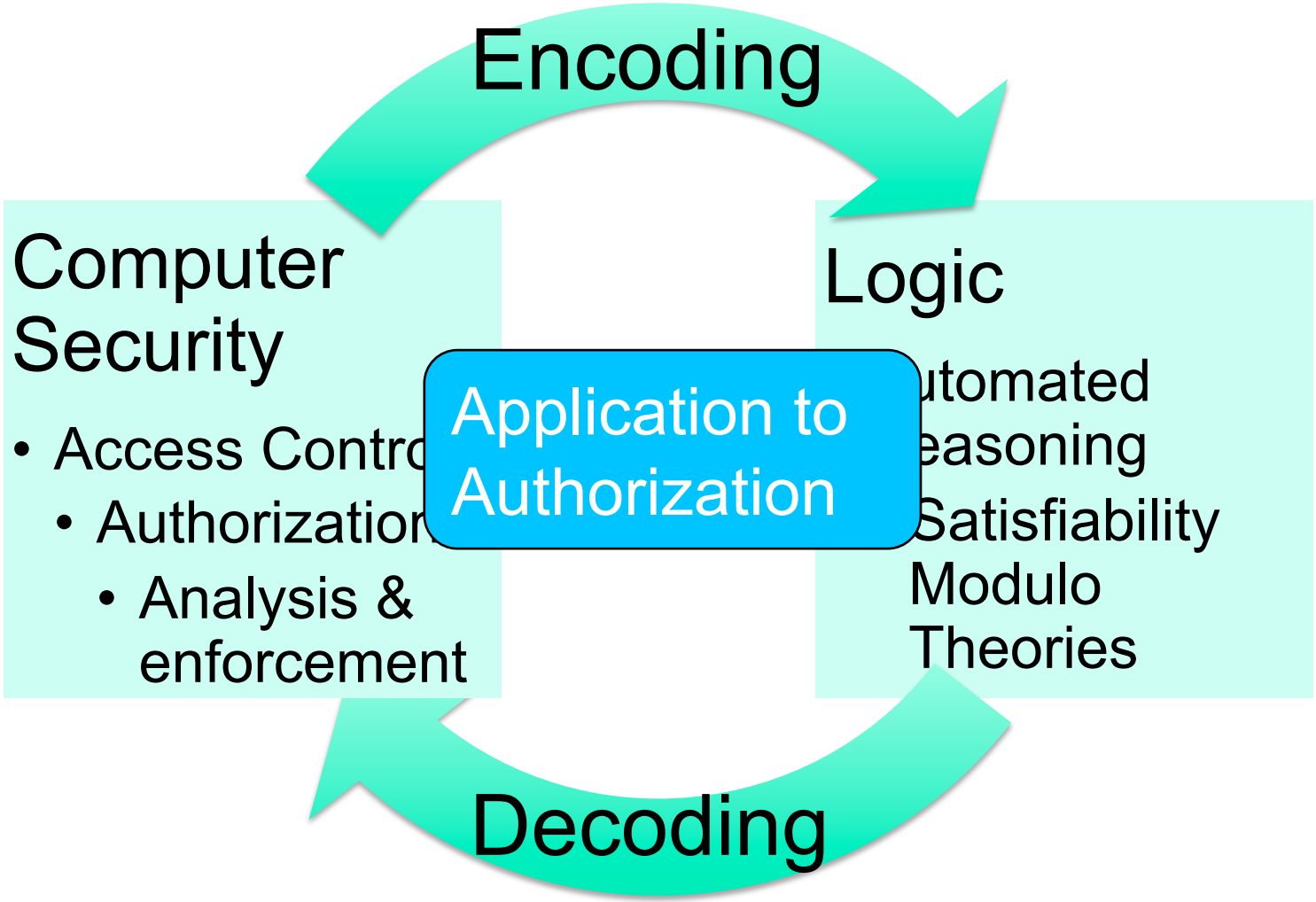
SMT: why is it useful (cont'd)

- Instead of developing specialized tools for solving combinatorial problems, …

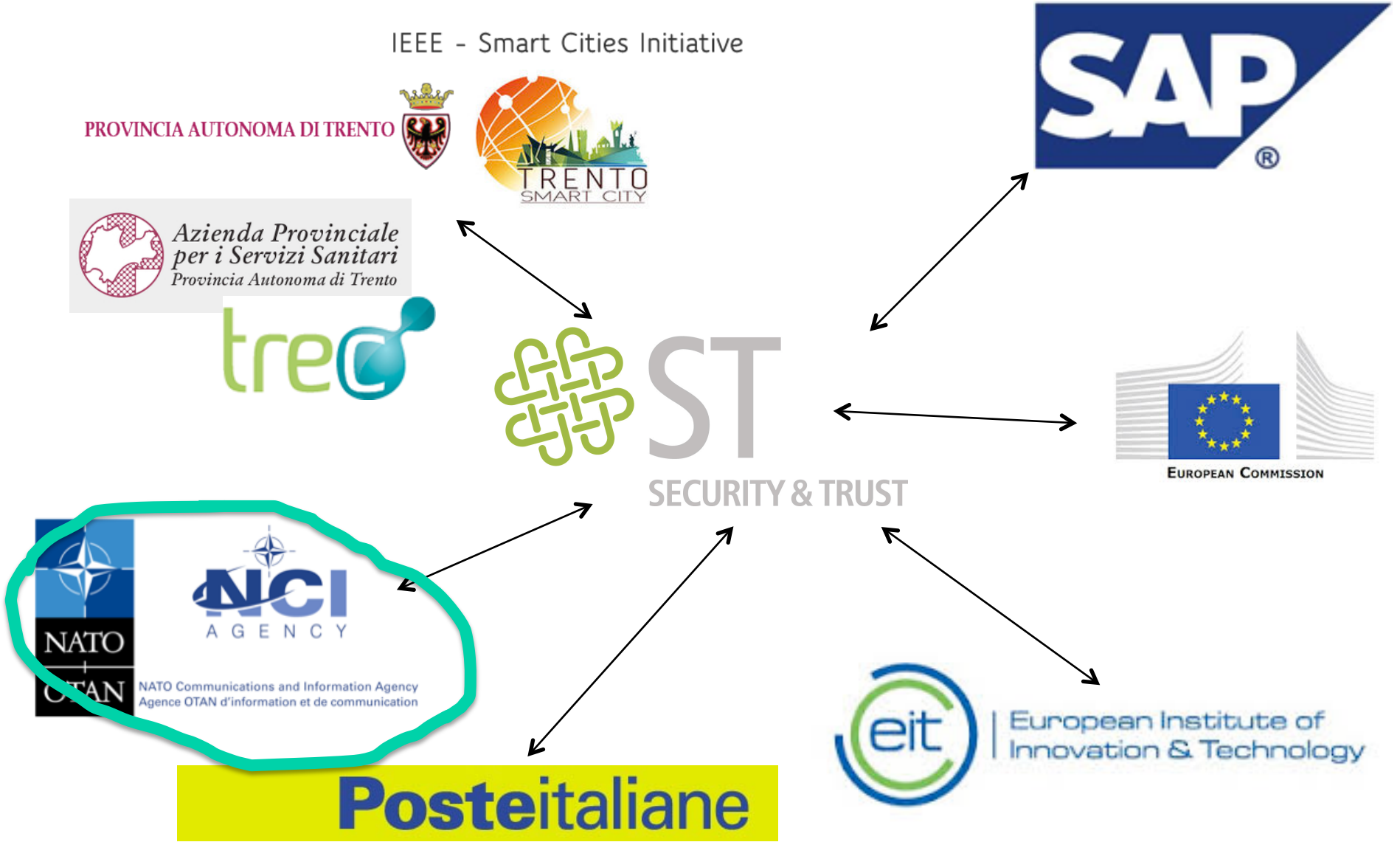


- Reuse of available knowledge about "Encoding" and "Decoding"

Plan of the talk



Our project with NATO-NCIA (2012-2015)



Context

- NATO network enabled capability and future mission network
  - High Assurance Automated Guard (HAAG)
- Selective information sharing for NATO operations
  - not only NATO members but also other governmental / humanitarian organizations
  - crucial for civil-military interaction, cyber defense information infrastructure, logistics support in the theatre
  - maximize effectiveness of operations and minimize disclosure with negative impact
- Variety of resources: Word documents, KML (Google) maps, XML documents, …
- Creators of documents have different psychological profiles leading to over/under classification

CPR (Content-based Protection and Release)

FONDAZIONE BRUNO KESSLER

Content-based

- structured resources = data containers
- atomic data associated to descriptive pairs of the form (element, content-metadata)
- For the moment, we assume that descriptive pairs exist… we ignore how they are extracted from resources… so that access control can be agnostic of the type of resources

Thus CPR can be seen as a refinement of ABAC and can be useful to large enterprises/organizations besides NATO

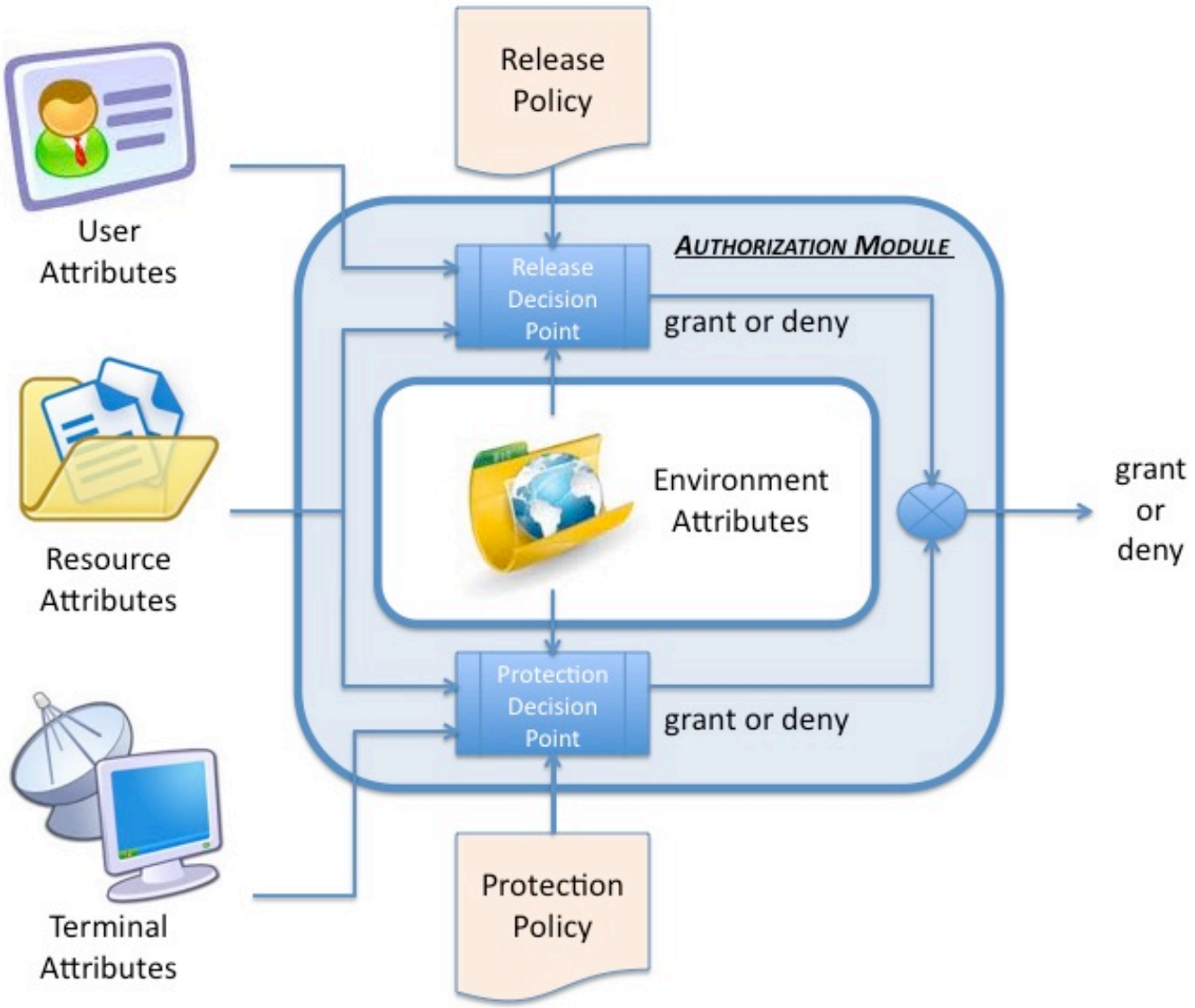
CPR (cont'd)

FONDAZIONE BRUNO KESSLER

Protection and **R**elease

- seeking the best trade-off between
  - disclosing selected parts of resources to trusted users (release)
  - ensuring use of "secure enough" terminals, i.e. device + communication channels + local data handling capabilities (protection)
- allowing for separate administration of release and protection policies
  - release policy admins = experts in matching user clearance with sensitivity of data
  - protection policy admins = experts in HW/SW requirements specified in technical directives and security settings documents

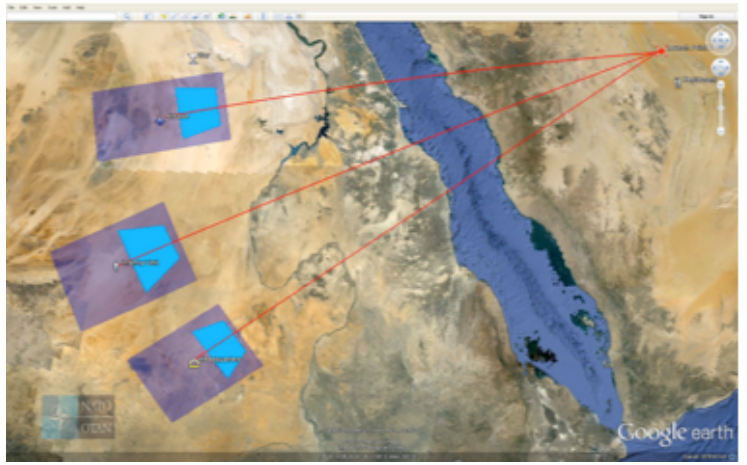
The core CPR Access Control model



An example: logistics support in the theatre

Passive Missile Defense System (PMD)

- simulates intercepting missile and consequences
- generates richly annotated KML maps



Access conditions

- NATO employees with clearance Secret can access resources whose content-metadata label category is Description… [release]
- Terminals managed by any authority with no information about their configuration can handle resources whose content-metadata label category is Public Information [protection]

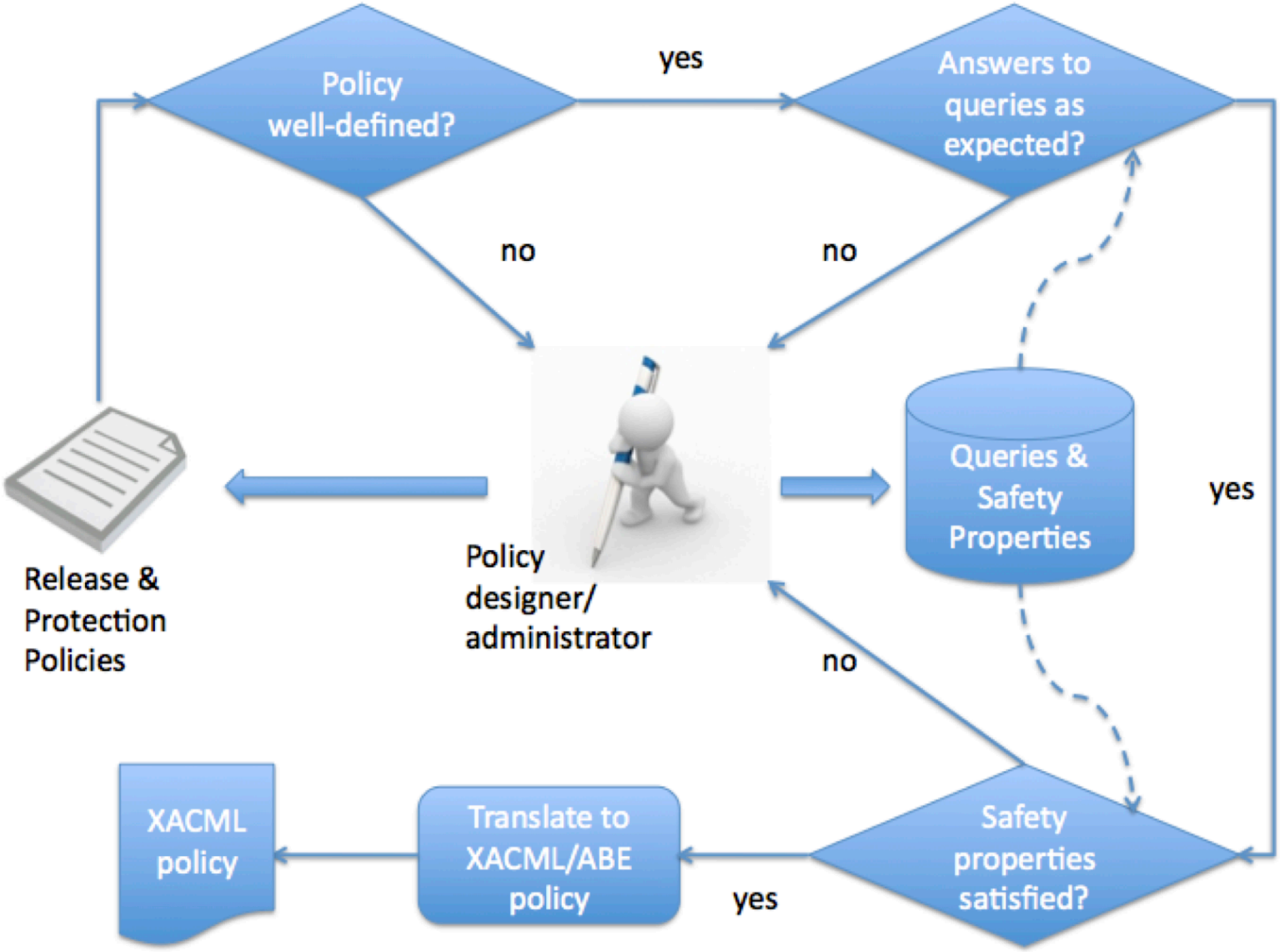
Result of access control is **more than grant/deny**:

it is a **view of the document** according to policies

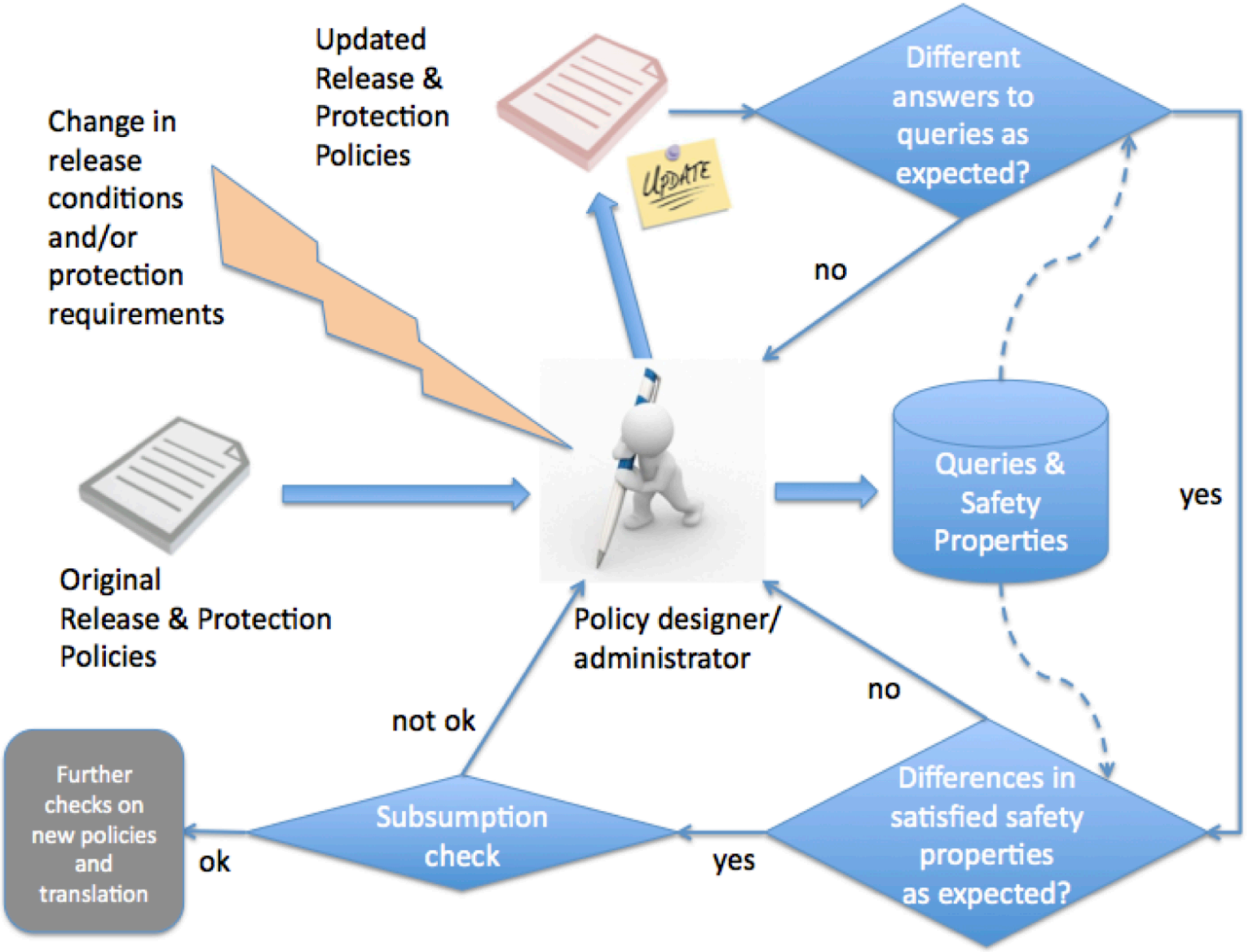
FONDAZIONE BRUNO KESSLER

Demo with CPR Tool

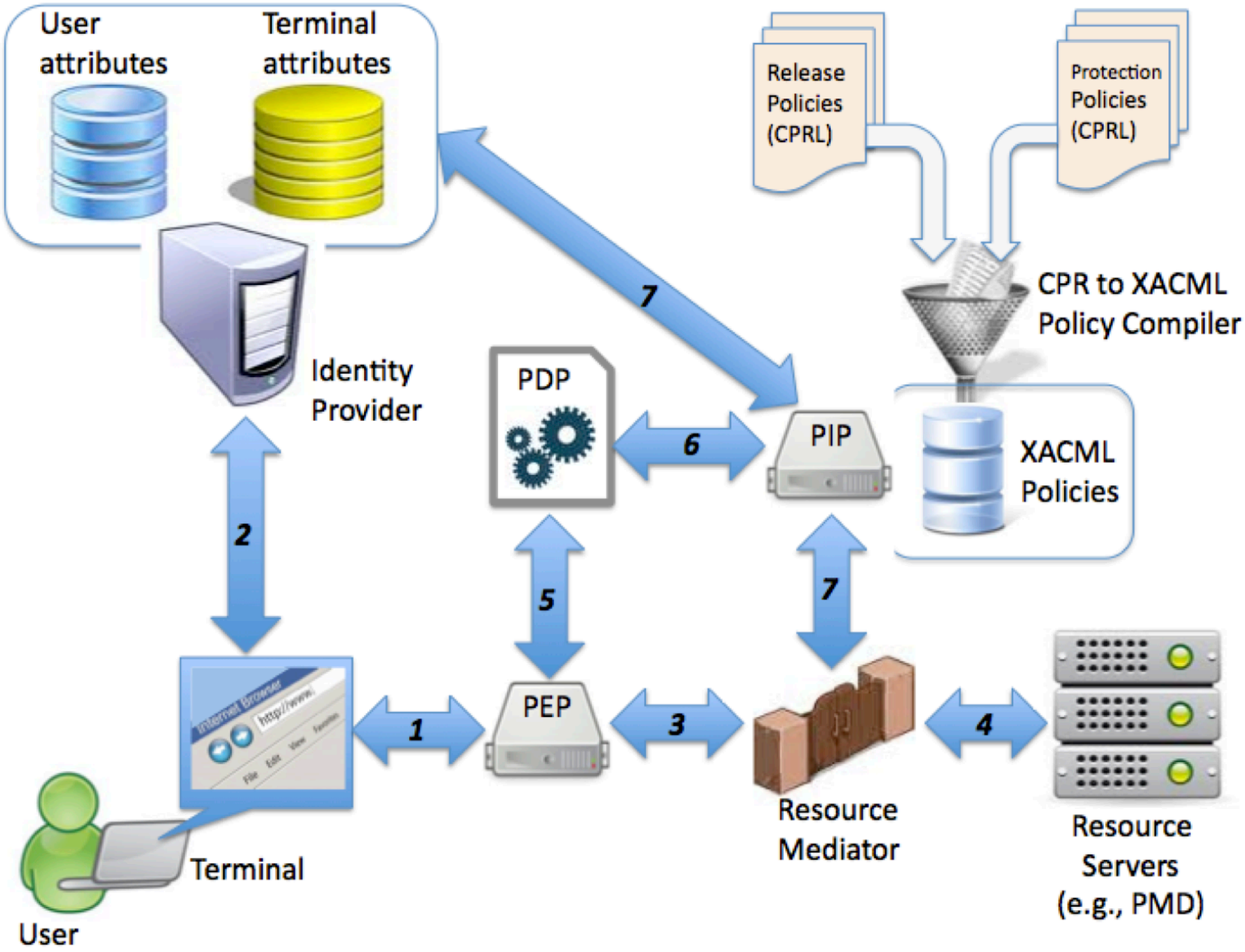
CPR Tool in the policy development lifecycle (I)



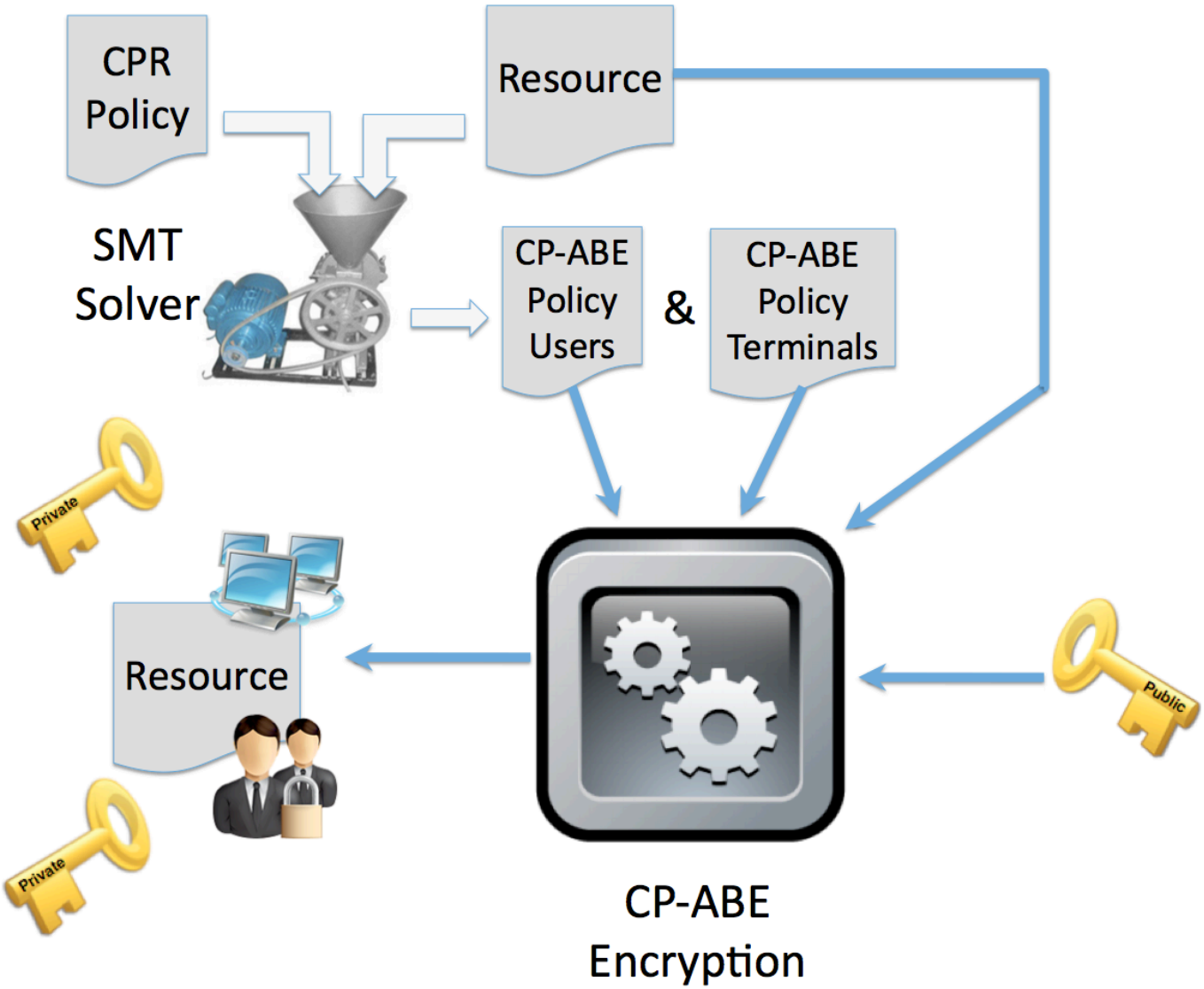
CPR Tool in the policy development lifecycle (II)



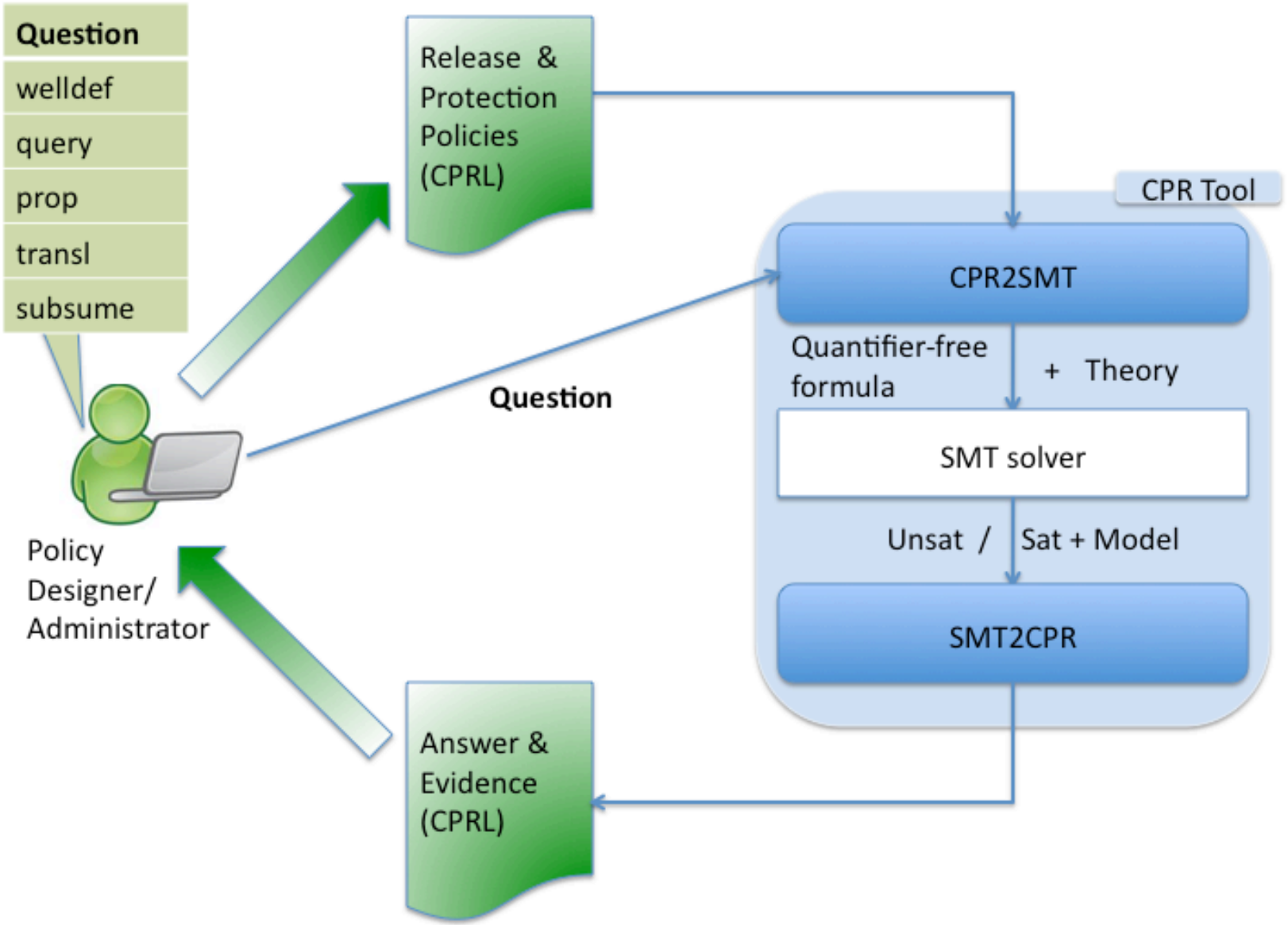
CPR Tool: Enforcement (XACML)



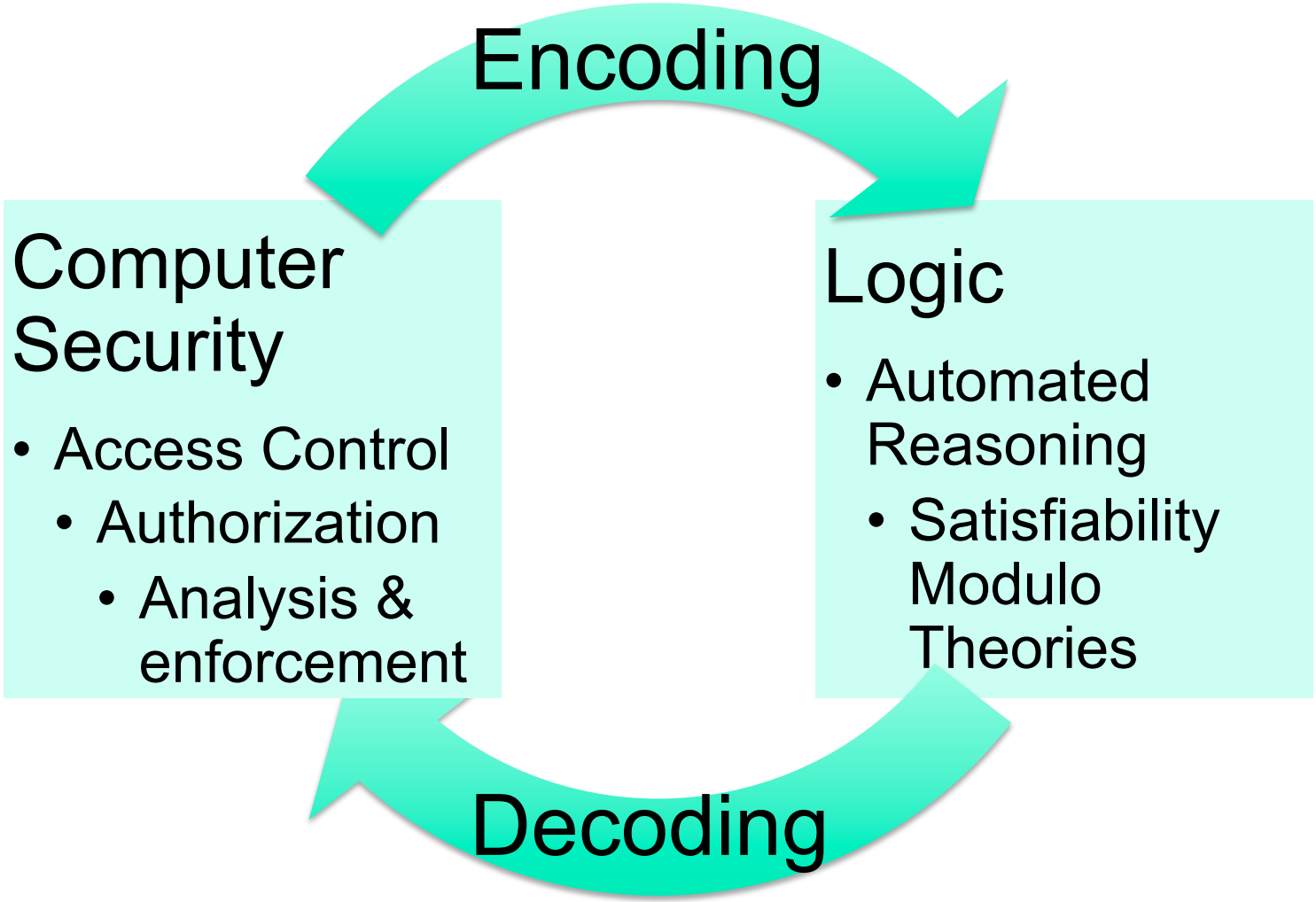
CPR Tool: Enforcement (Cloud)



CPR Tool: Architecture



Summary of the talk



Key takeways: CS side

FONDAZIONE BRUNO KESSLER

① Separate design and implementation

- Design pbs are already difficult to handle and a great source of vulnerabilities [recurring phenomenon in CS]
- Minimize implementation pbs by designing compilation to various enforcement mechanisms for different technological scenarios

② Use push-button tools for design, maintenance, and enforcement

- No need to know details of analysis techniques
- Support for wide range of analyses to support entire life-cycle

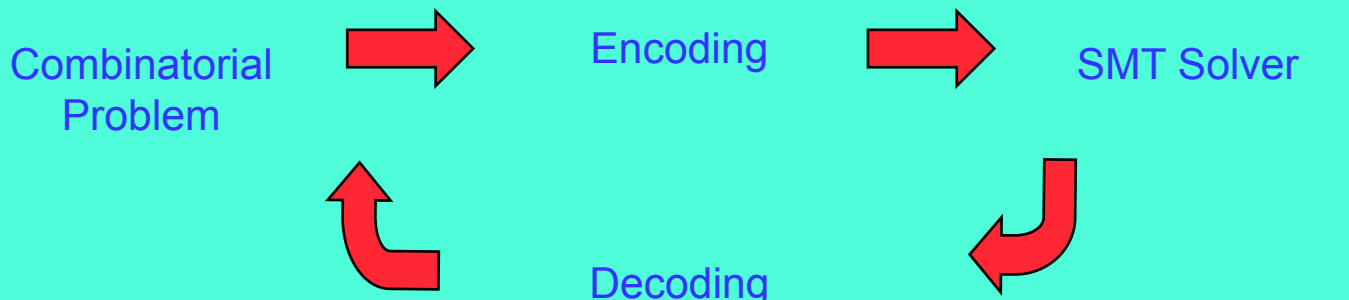
Key takeways: SMT side

Be lazy when developing analysis tools!

Don't build a new tool, try to use someone else!

Adapted from L. C. Paulson

Here is the recipe to do this:



Adapted from H. Kautz

Want to join?

FONDAZIONE BRUNO KESSLER

Drop me an email!

ranise@fbk.eu

ST
SECURITY & TRUST

Bibliography (about NATO project)

- A. Armando, S. Ranise, R. Traverso, and K. Wrona. *SMT-based Enforcement and Analysis of NATO Content-based Protection and Release Policies*. In Proceedings of the 2016 ACM International Work- shop on Attribute Based Access Control, New Orleans, Louisiana, USA. Pages 35–46, ACM, 2016.
- A. Armando, S. Ranise, R. Traverso, K. Wrona. *Compiling NATO authorization policies for enforcement in the cloud and SDNs*. IEEE Conference on Communications and Network Security, CNS 2015, Florence, Italy, September 28-30, 2015. IEEE 2015.
- A. Armando, S. Oudkerk, S. Ranise, and K. Wrona. *Formal modelling of content-based protection and release for access control in NATO operations*. In Foundations and Practice of Security (FPS) - 6th International Symposium, La Rochelle, France, October 21-22, volume 8352 of Lecture Notes in Computer Science, pages 227–244. Springer, 2013.
- A. Armando, M. Grasso, S. Oudkerk, S. Ranise, and K. Wrona. *Content-based information protection and release in NATO operations*. In 18th ACM Symposium on Access Control Models and Technologies (SACMAT), Amsterdam, The Netherlands, June 12-14, 2013, pages 261–264. ACM, 2013.

Selected bibliography (about policy analysis)

- F. Turkmen, J. den Hartog, S. Ranise, and N. Zannone. *Analysis of XACML policies with SMT*. In Principles of Security and Trust (POST) - 4th International Conference, Held as Part of ETAPS 2015, London, UK, April 11-18, 2015, volume 9036 of Lecture Notes in Computer Science, pages 115–134. Springer, 2015.
- S. Ranise and R. Traverso. *ALPS: an action language for policy specification and automated safety analysis*. In Security and Trust Management (STM) - 10th International Workshop, Wroclaw, Poland, September 10-11, 2014. volume 8743 of Lecture Notes in Computer Science, pages 146–161. Springer, 2014.
- A. Armando, S. Ranise, F. Turkmen, and B. Crispo. *Efficient run-time solving of RBAC user authorization queries: pushing the envelope*. In 2nd ACM Conference on Data and Application Security and Privacy (CODASPY), San Antonio, TX, USA, February 7-9, 2012, pages 241–248. ACM, 2012.
- A. Armando and S. Ranise. *Automated and efficient analysis of role-based access control with attributes*. In Data and Applications Security and Privacy (DBSec) XXVI - 26th Annual IFIP WG 11.3 Conference, Paris, France, July 11-13, 2012, volume 7371 of LNCS, pages 25–40. Springer.