Autenticazione e Autorizzazione nelle Piattaforme Cloud

Silvio Ranise

FONDAZIONE BRUNO KESSLER

SECURITY & TRUST

Security & Trust Research Unit @ FBK

- Fondazione Bruno Kessler

- S&T Research Unit (born in 2010)
    - 3 researchers
    - 1 visiting researcher
    - 1 junior researcher
    - 2 PhD students

- Involved in local, national, and international research projects
    - some of which I am going to present in the following…

- Coordinators of an educational project in the security of an industrial cloud computing platform…

European Industrial Doctorate

SECENTIS

A European Industrial Doctorate on Security and Trust

Goal: Train new generation of security experts capable to tackle scientific and technical challenges raised by combination of new technologies (**cloud** computing, **mobile** applications, and the **SaaS** paradigm)

Consortium:

- Fondazione Bruno Kessler (coordinator),
- Security & Trust Practice, SAP Research
- University of Trento, and TrentoRISE

FONDAZIONE
BRUNO KESSLER

SAP ®

UNIVERSITAS ATHESINA STUDIORUM

trentorise

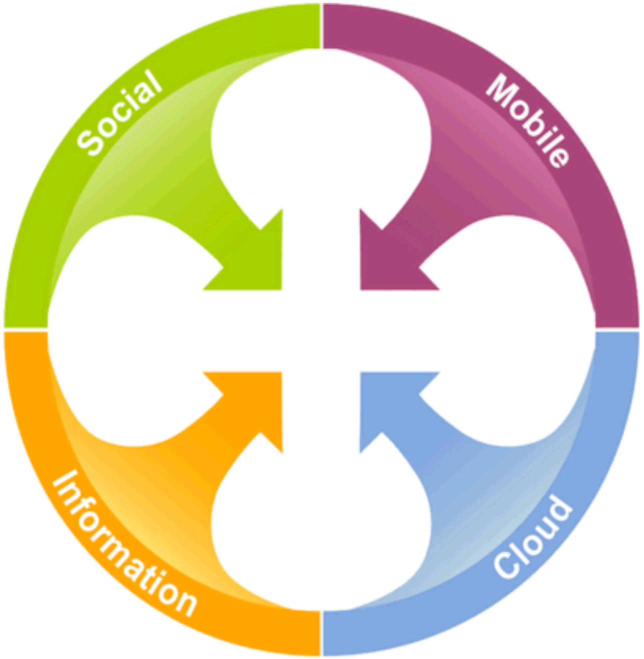
Open Innovation rooted in Research and Education

Recruitment: Currently seeking 5 young researchers willing to undertake a PhD in an international, collaborative environment.

Cloud IAM (Identity and Access Management)

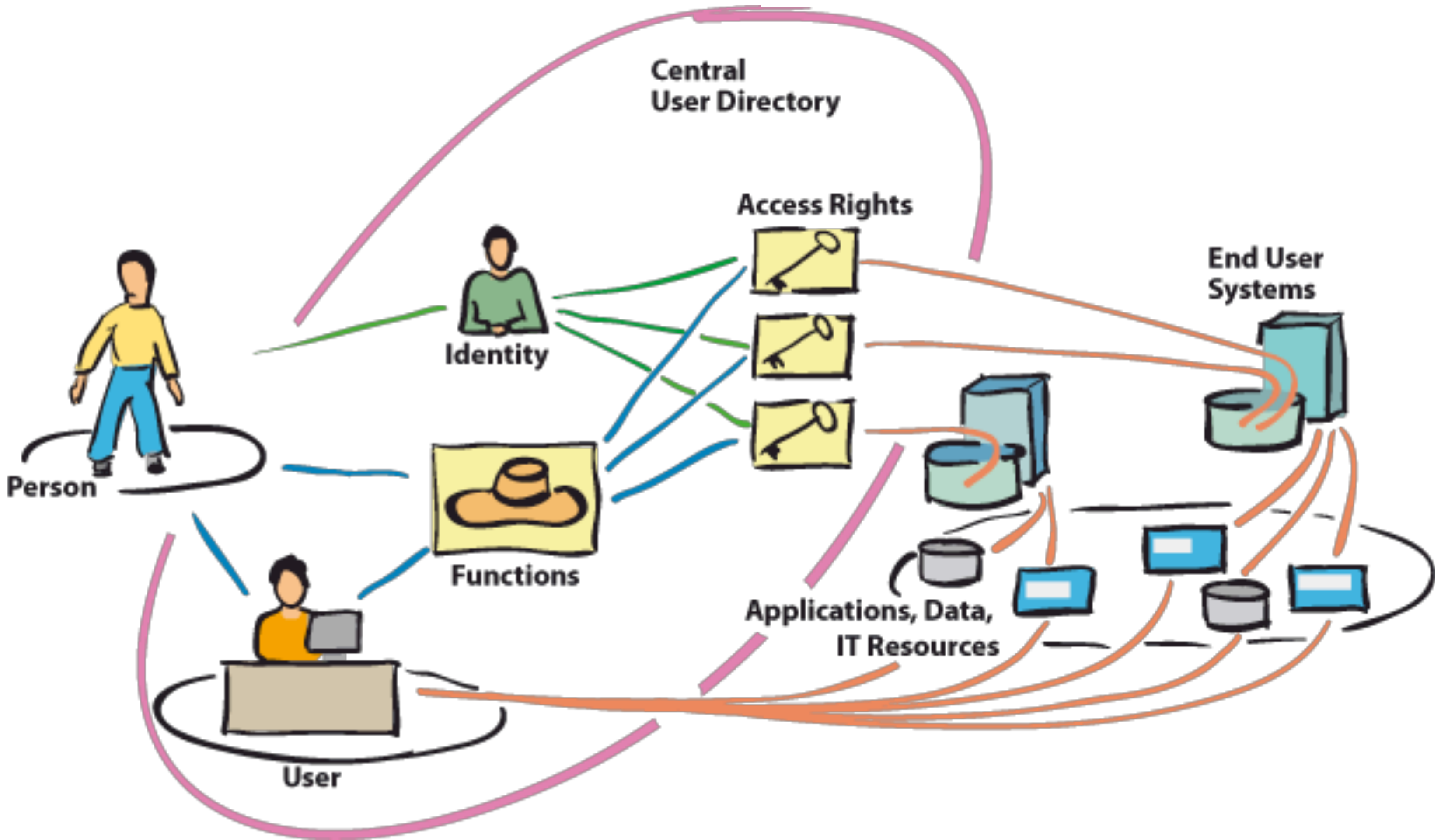
In 2012, Gartner said

- "*Cloud IAM will grow 500% by 2015*"
- IDaaS will account for 25% of all IAM sales by 2014 (in 2012, only 5%)
- Why? 4 converging forces

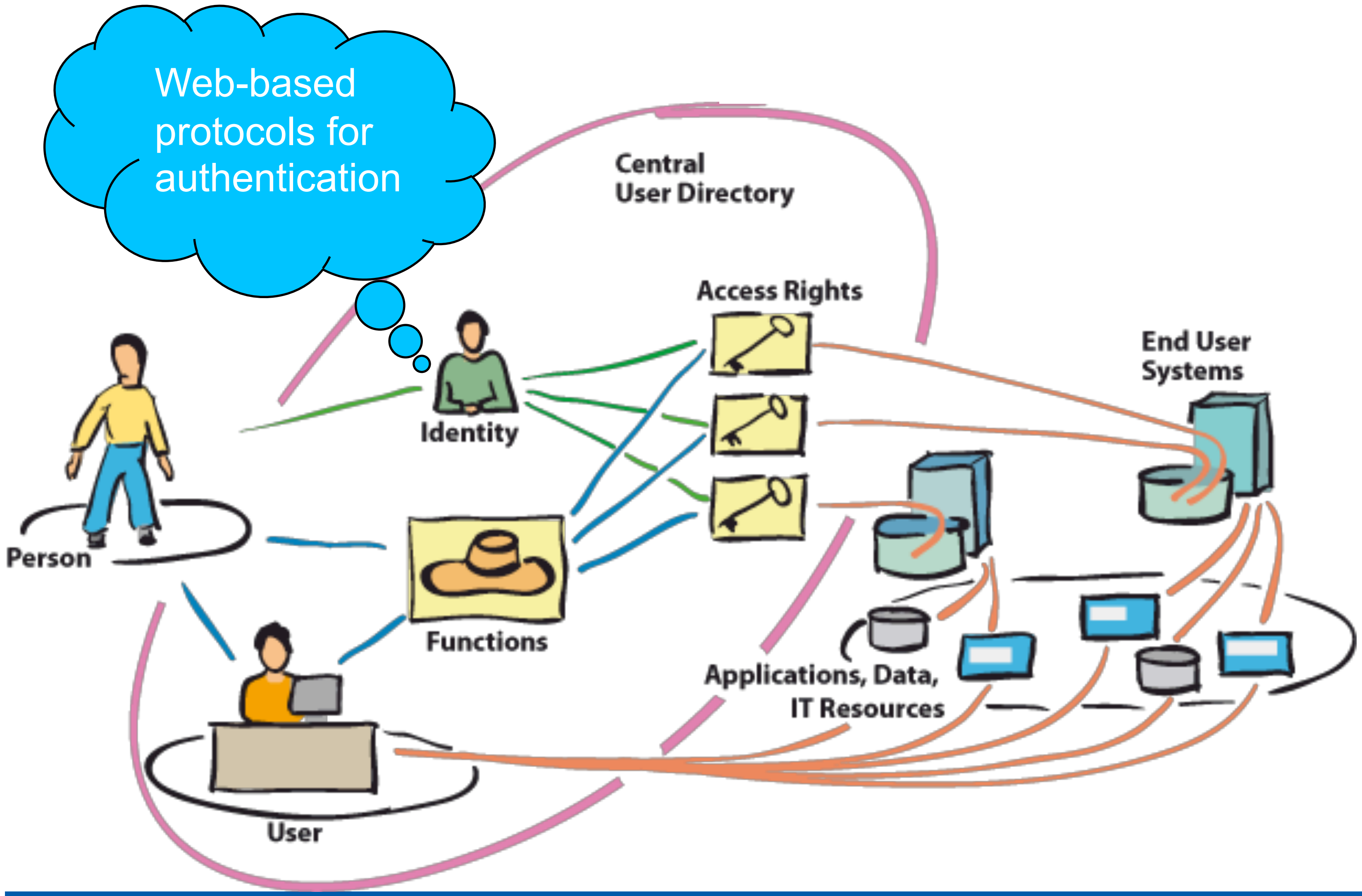


1. **social platforms** for both customers and employees
2. **mobile devices** used by employees to access corporate data
   - Bring-Your-Own-Device (BYOD)
3. **information** spread over several systems
4. **cloud SaaS** is being widely accessed and adopted

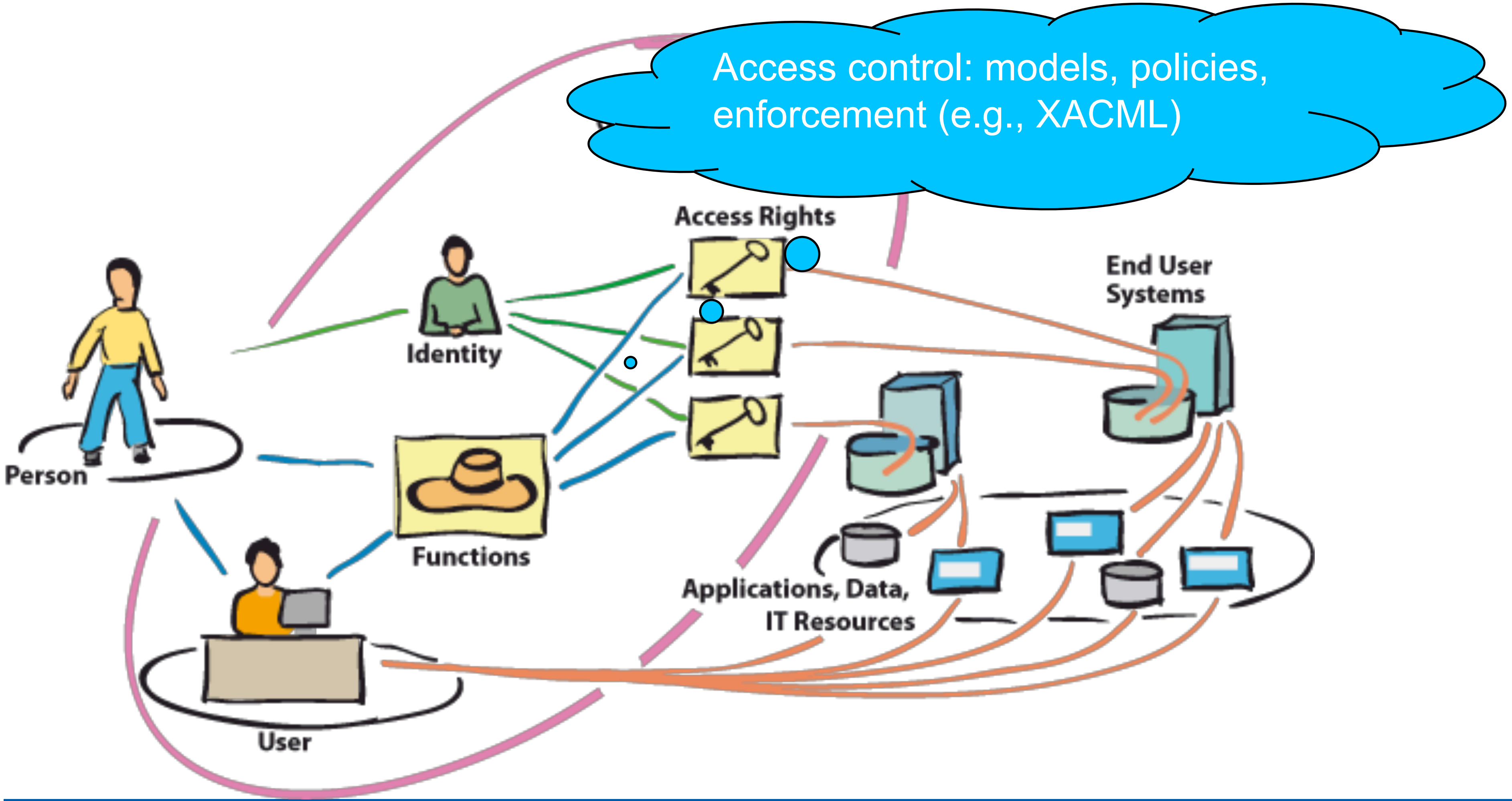
An abstract view on IAM systems



An abstract view on IAM systems



An abstract view on IAM systems


Access control: models, policies, enforcement (e.g., XACML)
Access Rights
End User Systems
Identity
Person
Functions
Applications, Data, IT Resources
User

Some scenarios

↓

smart
campus

treC

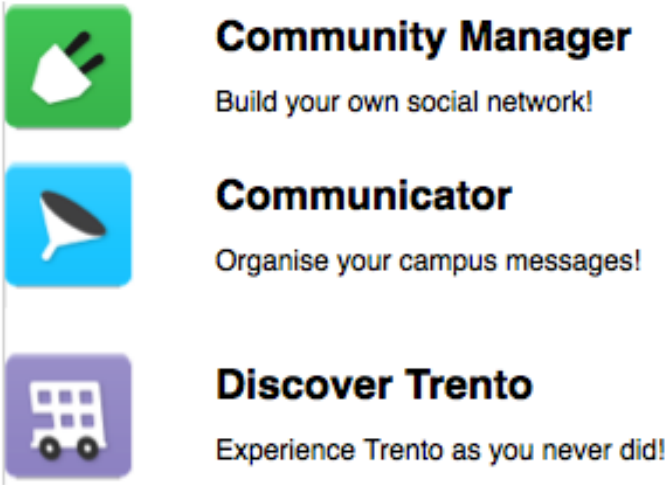
NATO
OTAN

NCI
AGENCY

NATO Communications and Information Agency
Agence OTAN d'information et de communication

Overview

- **Social platform** (FBK, UNITN, …)
- **Several devices**: laptops, tablets, smart-phones, …
- **Mobile apps:** Android
- Authentication: Single-Sign-On
- Authorization based on single user profile
- **Apps accessing data handled by other apps/ services with user consent**
    - OAuth: next slides

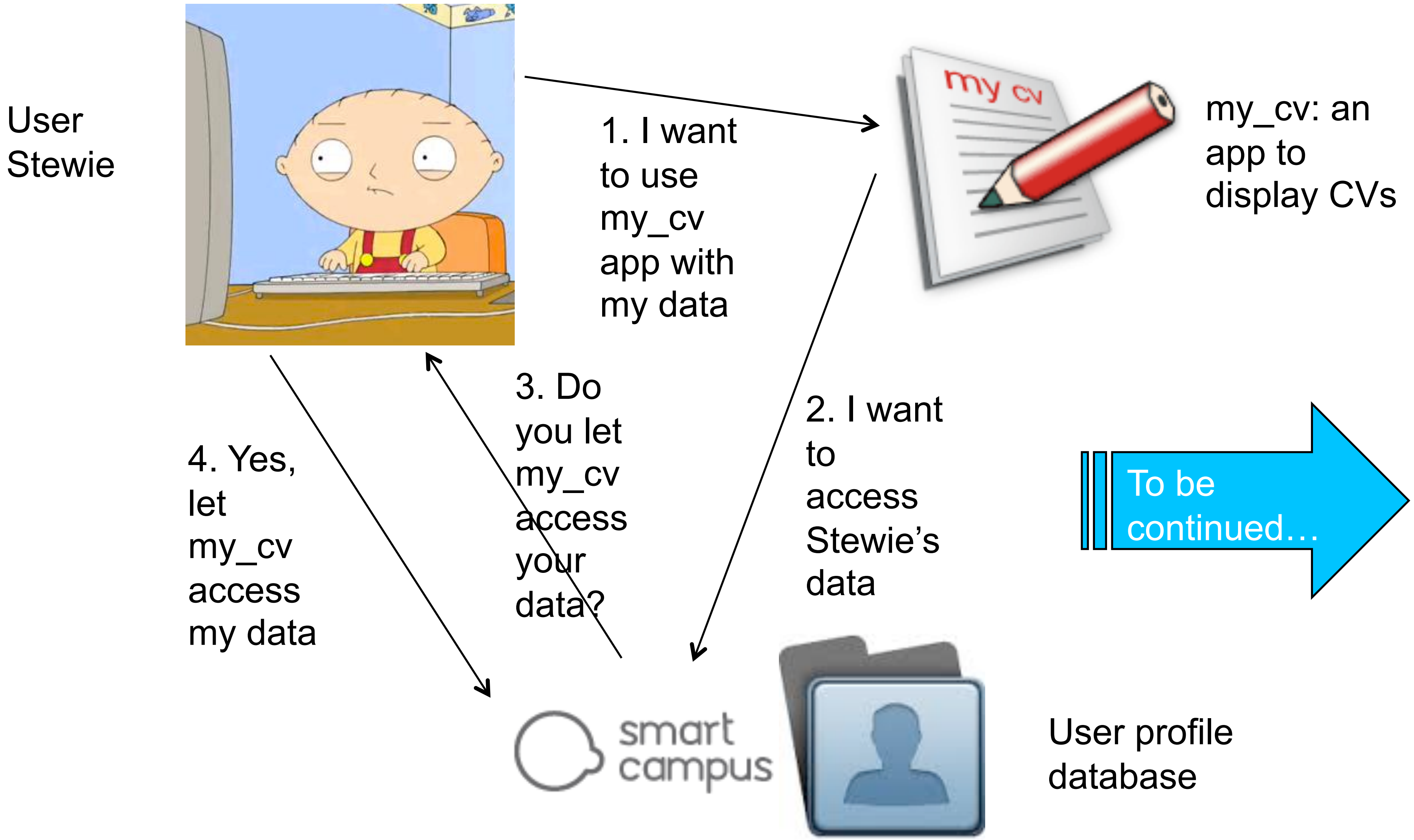


Community Manager
Build your own social network!

Communicator
Organise your campus messages!

Discover Trento
Experience Trento as you never did!

OAuth overview (1st part)



User Stewie

1. I want to use my_cv app with my data

my_cv: an app to display CVs

2. I want to access Stewie's data

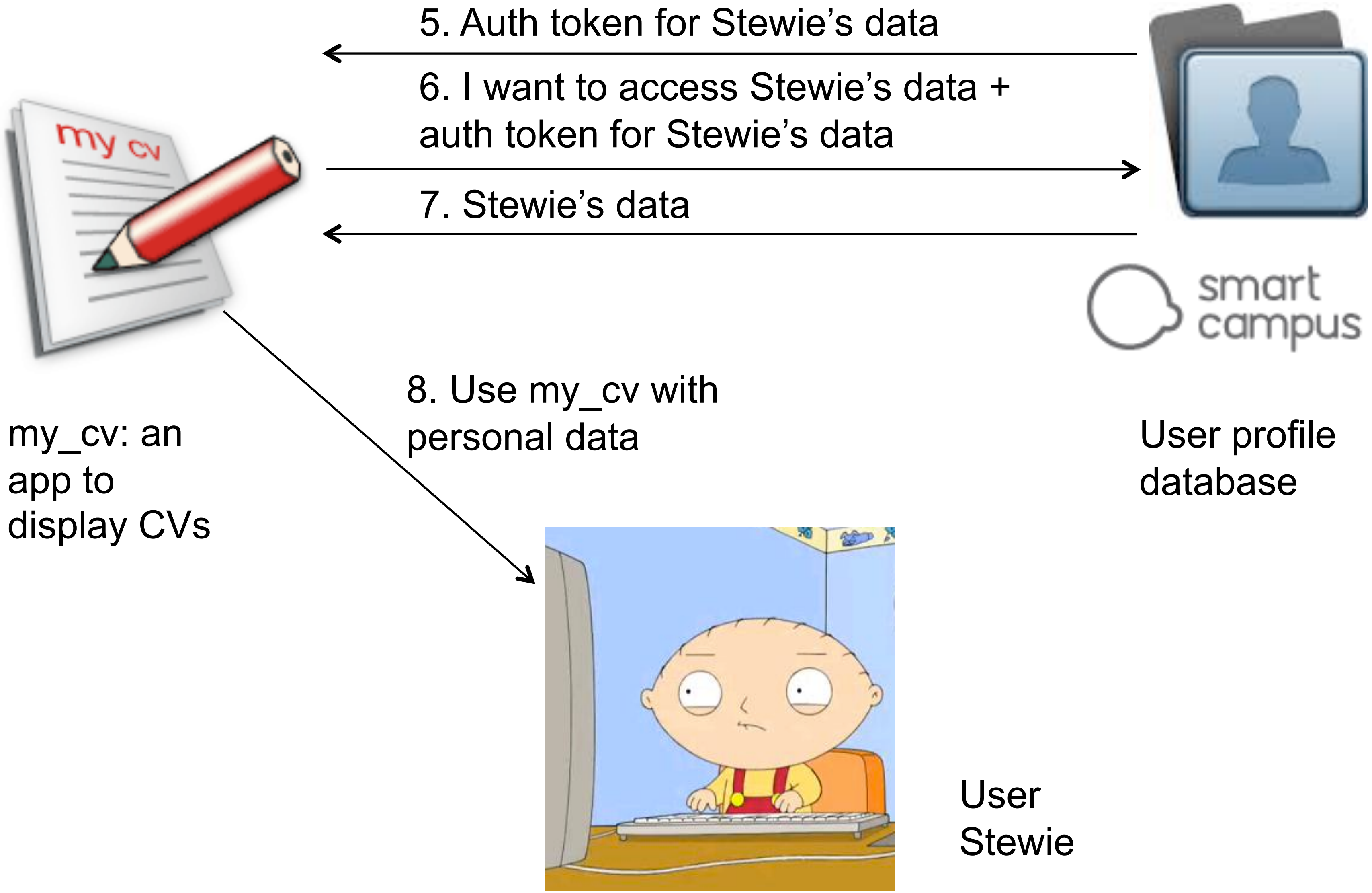
3. Do you let my_cv access your data?

4. Yes, let my_cv access my data

User profile database

To be continued…

OAuth overview (2nd part)



5. Auth token for Stewie’s data

6. I want to access Stewie’s data + auth token for Stewie’s data

7. Stewie’s data

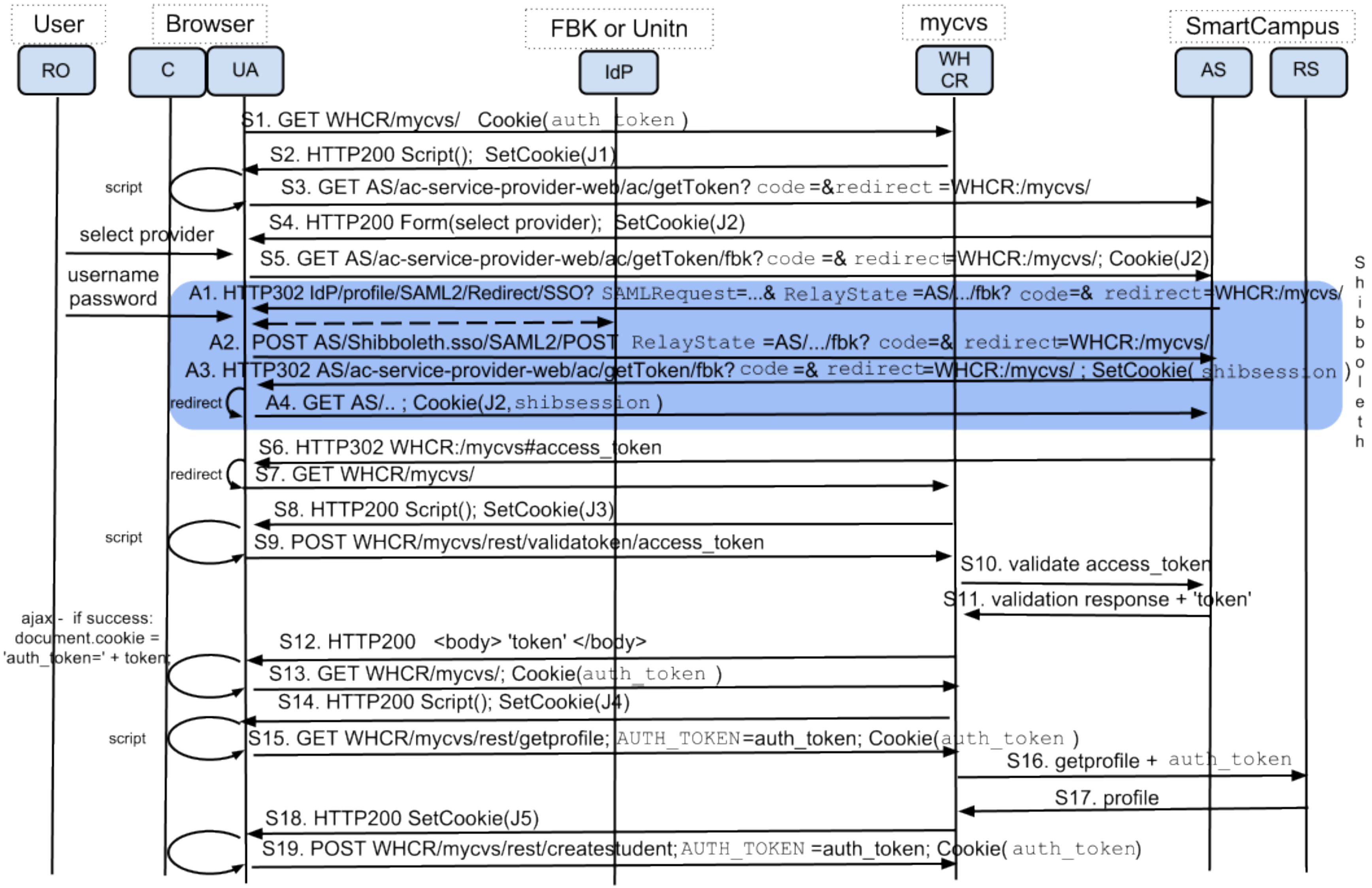
8. Use my_cv with personal data

my_cv: an app to display CVs

User profile database

User Stewie

OAuth… less abstract: MSC



User

Browser

FBK or Unitn

mycvs

SmartCampus

RO

C

UA

IdP

WH CR

AS

RS

S1. GET WHCR/mycvs/ Cookie(auth_token)

S2. HTTP200 Script(); SetCookie(J1)

script

S3. GET AS/ac-service-provider-web/ac/getToken? code =&redirect =WHCR:/mycvs/

S4. HTTP200 Form(select provider); SetCookie(J2)

select provider

S5. GET AS/ac-service-provider-web/ac/getToken/fbk? code =& redirect=WHCR:/mycvs/; Cookie(J2)

username password

A1. HTTP302 IdP/profile/SAML2/Redirect/SSO? SAMLRequest=...& RelayState =AS/.../fbk? code=& redirect=WHCR:/mycvs/

A2. POST AS/Shibboleth.sso/SAML2/POST RelayState =AS/.../fbk? code=& redirect=WHCR:/mycvs/

A3. HTTP302 AS/ac-service-provider-web/ac/getToken/fbk? code =& redirect=WHCR:/mycvs/ ; SetCookie(shibsession)

redirect

A4. GET AS/.. ; Cookie(J2, shibsession)

Shibboleth

S6. HTTP302 WHCR:/mycvs#access_token

redirect

S7. GET WHCR/mycvs/

S8. HTTP200 Script(); SetCookie(J3)

script

S9. POST WHCR/mycvs/rest/validatoken/access_token

S10. validate access_token

S11. validation response + 'token'

ajax - if success: document.cookie = 'auth_token=' + token

S12. HTTP200 <body> 'token' </body>

S13. GET WHCR/mycvs/; Cookie(auth_token)

S14. HTTP200 Script(); SetCookie(J4)

script

S15. GET WHCR/mycvs/rest/getprofile; AUTH_TOKEN=auth_token; Cookie(auth_token)

S16. getprofile + auth_token

S17. profile

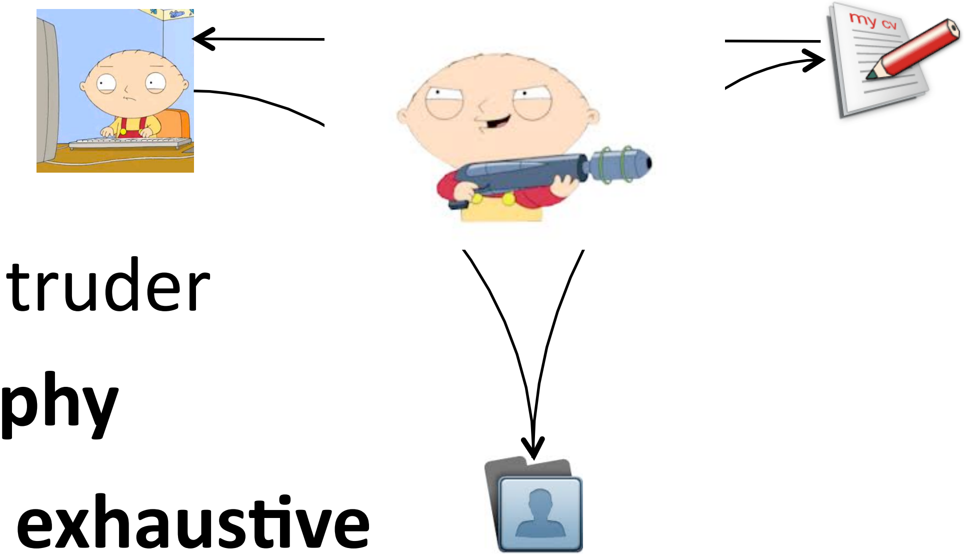
S18. HTTP200 SetCookie(J5)

S19. POST WHCR/mycvs/rest/createstudent; AUTH_TOKEN =auth_token; Cookie(auth_token)

Algorithmic analysis of smart campus OAuth

- **Model: state machine M = < I, T >**
  - I = initial states = "user is not authenticated, auth token is invalid, …"
  - T = possible transitions = arrows in MSC
- **Security property: P** = "app can access user data only after user consent"
- **Model checking: M satisfies P? M |= P**
  - Negation of P is satisfied by execution trace?
    - If so, report "security problem"
  - Enumerate all traces (1 trace = OAuth MSC!)

Some observations on algorithmic analysis



- Security w.r.t. what: *which threat model?*
  - Dolev—Yao like intruder
  - **Perfect cryptography**
- Techniques supporting **exhaustive state space exploration** of systems
  - even incomplete techniques may give better coverage than testing
- To make it practical
  - heuristics to control large/**infinite state spaces**

Some scenarios

→ treC

smart campus

NATO
OTAN

NCI
AGENCY

NATO Communications and Information Agency
Agence OTAN d'information et de communication

Cartella Clinica del Cittadino

- e-Personal Health Record (PAT, APSS, FBK)

- **Strong Authentication**
  - OTP, Smart cards
- **Access Control**: enable citizens to protect or disclose information stored in PHR
  - Italian legislation, Trento province legislation
  - Secure information sharing: citizen, doctors, …

- Geo-localisation via mobile device

Our results

- **Strong Authentication**
  - Found flaw in two factors authentication protocol by model checking (SATMC)
- **Access Control**
  - design of AC mechanism and prototype implementation for enforcement
  - issues in modeling with Italian legislation about
    - **delegation**
    - parental handling of certain data (e.g., pregnancy tests)
  - Law Dep. UniTn -> Garante della privacy

Observations on Access Control

- **Finding the “right” model is non trivial**
  - several models in the literature:
    - DAC, MAC, RBAC, ABAC, GTRBAC, STRBAC, …
  - small “quid” always lacking
  - Difficulties in incorporating regulations and legislations

Some scenarios

treC

smart
campus

NATO
OTAN

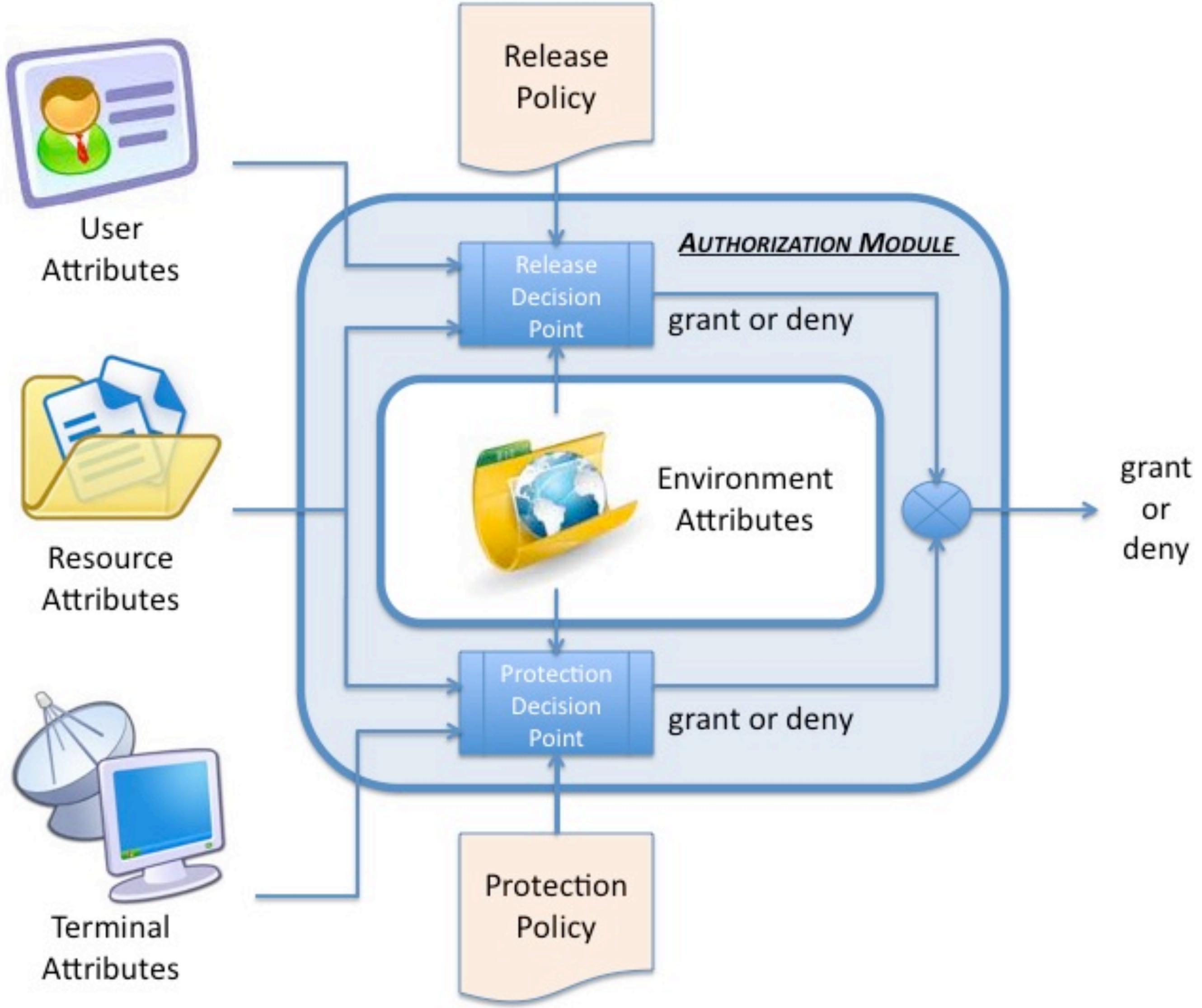
NCI
AGENCY

NATO Communications and Information Agency
Agence OTAN d'information et de communication

Access Control for NATO

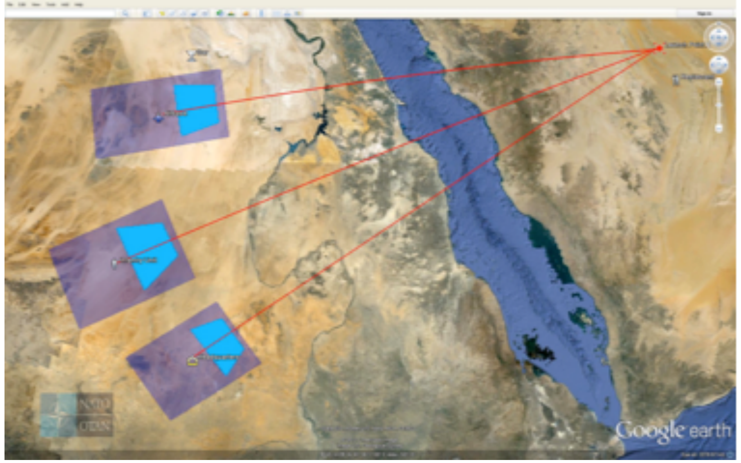
- Security model for the High Assurance Automated Guard (HAAG)
- Information sharing in NATO operations
- Not only NATO members but also other governmental and humanitarian organizations
- **Selective release of information** to
  - maximize effectiveness of operations and
  - minimize disclosure with negative impact
- Access decision based on more than user **clearance** and resource **sensitivity**

Overview of NATO Access Control model



Variety of documents: an example

- Passive Missile Defense System (PMD)
  - simulates intercepting missile and consequences
  - generates richly annotated KML maps



- Policy
  - colonel (head of mission) can see all around his position for 10 miles
  - Red Cross doctor can see wounded soldiers around his position for 2 miles
- Result of access control **more than grant/deny**: it is a **view of the document** according to policies

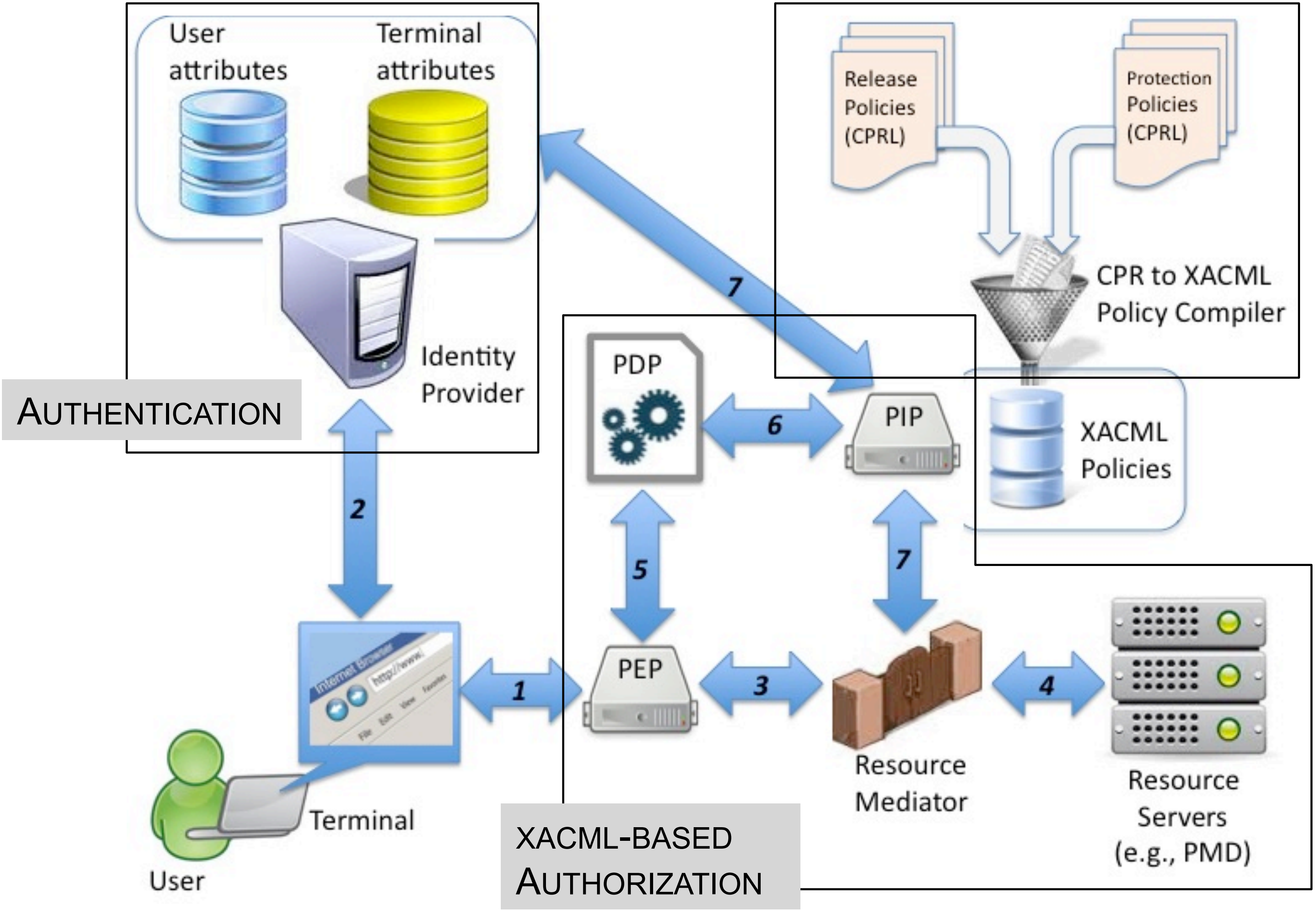
Expressive policies

- colonel (head of mission) can see all around his position for 10 miles
  - User.rank = colonel /\ User.id = Map.mission_head /\ Obj in Map /\ | Obj.loc – User.loc | < 10
- Red Cross doctor can see wounded soldiers around his position for 2 miles
  - User.org = RedCross /\ User.role = doctor /\ Obj in Map /\ Obj.type = soldier /\ Obj.wounded = true /\ | Obj.loc – User.loc | < 2
- Understand consequences of policies is difficult because of
  - hierarchic nesting of resources
  - number of attributes: hundreds to thousands
  - large/infinite attribute domains (e.g., the real numbers)

Deductive analysis of NATO policies

- **First-order logic to represent**
  - P = policies (previous slide)
  - Q = query = "can user with the following attributes access the resource with these attributes?"
- **Reduce query answering to logical problem (sat)**
  - Use state-of-the-art deductive tools
    - **Satisfiability Modulo Theories (SMT)** solvers
    - capable of reasoning in several domains (e.g., Reals)
- Note: **Q can contain symbolic values for attributes**
  - not only User.loc = (10,10) but also | User.loc – (10,10) |<3
- **Policy designers can check their intuitions** (i.e. given queries should/should not be granted) **on sets of queries**

Enforcement of CPR policies [run-time]



Further observations on Access Control

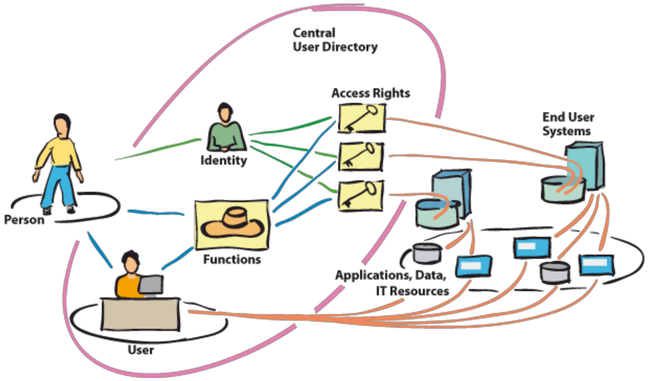
- Access control may
  - depend on several factors: users, resources, **context** (e.g., location, time, …), even **devices**!

- Separation of concerns
  - **Policies:** rules to grant/deny access
  - **Model:** semantics to policies
  - **Enforcement** of policies according to semantics

Trust in NATO access control

- **Coalitions are dynamic**
- As a result: granting/denying access may change
    - Head of mission appoints "field lieutenants" with some permissions
    - If head changes, then role "field lieutenants" from soldiers previously appointed so they cannot use associated permissions
- **Use first-order logic to express trust relations** (e.g., DKAL)
    - Agent1 ***trusts*** Agent2 ***on*** issuing certain certificates
- Combine formulae expressing trust relations with formulae expressing access control policies
- Use same deductive approach as before

Conclusions



- Cloud IAM is gaining importance
  - authentication, authorization, and trust
  - increasing complexity of systems
  - severe security pbs
- Automated security analysis tools dramatically needed
  - security certification w.r.t. given threat model
  - difficulties in access control models due to variety of requirements: technological, business, legislation
  - separation of concerns
    - Web-protocols: perfect cryptography
    - Access control: policies, model, enforcement
      - abstract analysis of policies w.r.t. model
      - analysis of enforcement w.r.t. model