Security for all: network-based protection for personal devices

Antonio Lioy

Politecnico di Torino

< lioy @ polito.it >

Cybersecurity & Privacy Innovation Forum *2015*

Brussels, 28/4/2015

SEVENTH FRAMEWORK PROGRAMME

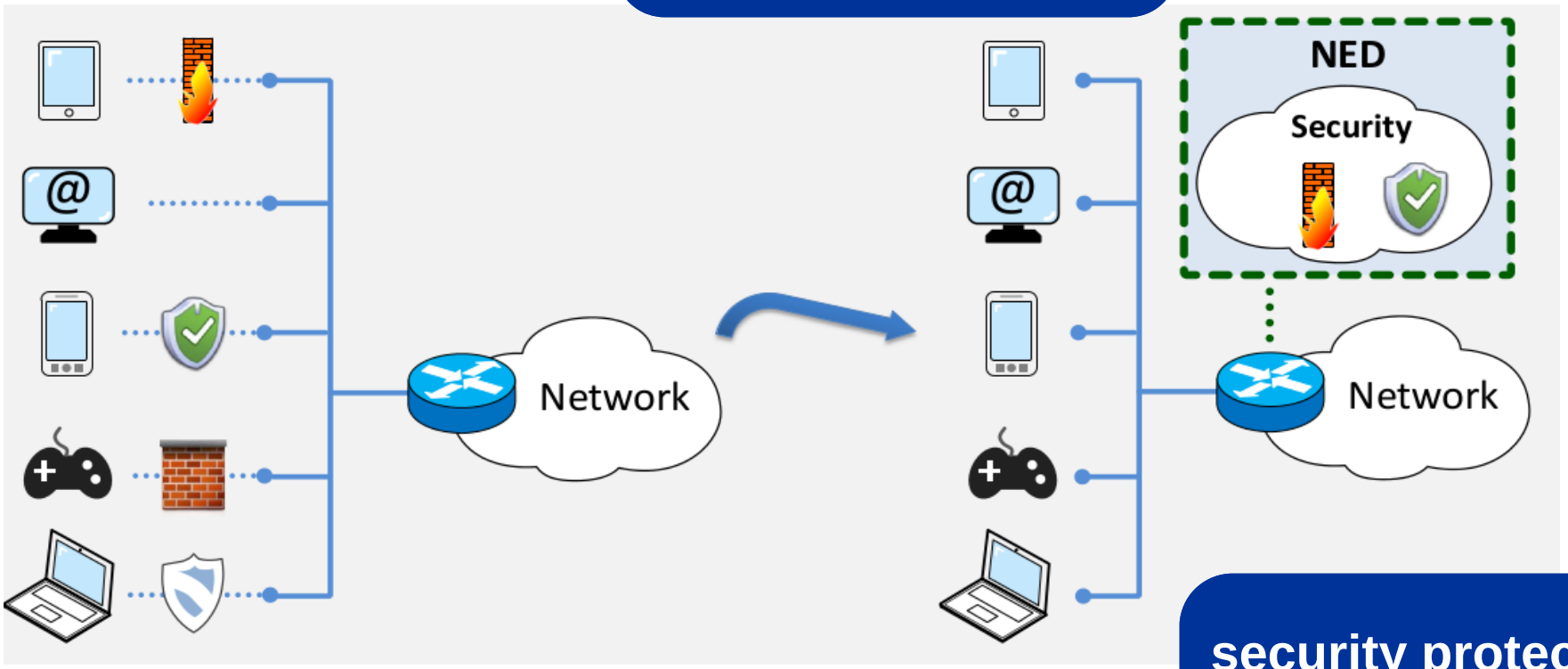
Why SECURity at the network EDge

- **users deal with many "terminals" (laptop, desktop, tablet, smartphone, Internet-connected TV, car infosystem, …**
  - with very different **security levels**
    - complex management of security controls for so many platforms with so different characteristics
  - withdifferent **network connection**
    - can't consistently rely on network border protection
  - with different policy requirements
    - mobile devices at home vs BYOD at work

SECURED = offload security controls from the user terminals to a trusted and secure network node

From heterogeneous to uniform security

security applications independent from user terminals



security protection independent from user location

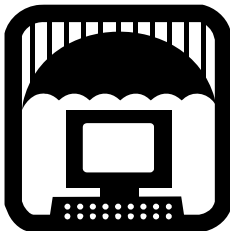
Use cases

- **home**
  - home gateway, protection of family (and visitors') devices
- **enterprise**
  - wired/wireless access, protection of hosts (including servers?)
- **public hotspot**
  - WiFi access, protection of visitors
- **mobile**
  - 3G/4G access, protection of subscriber's device
- **IoT**
  - wireless access point, protection of IoT node
- **NOTE: first hop not "SECURED"? then create a secure connection to a SECURED-node somewhere in the network**

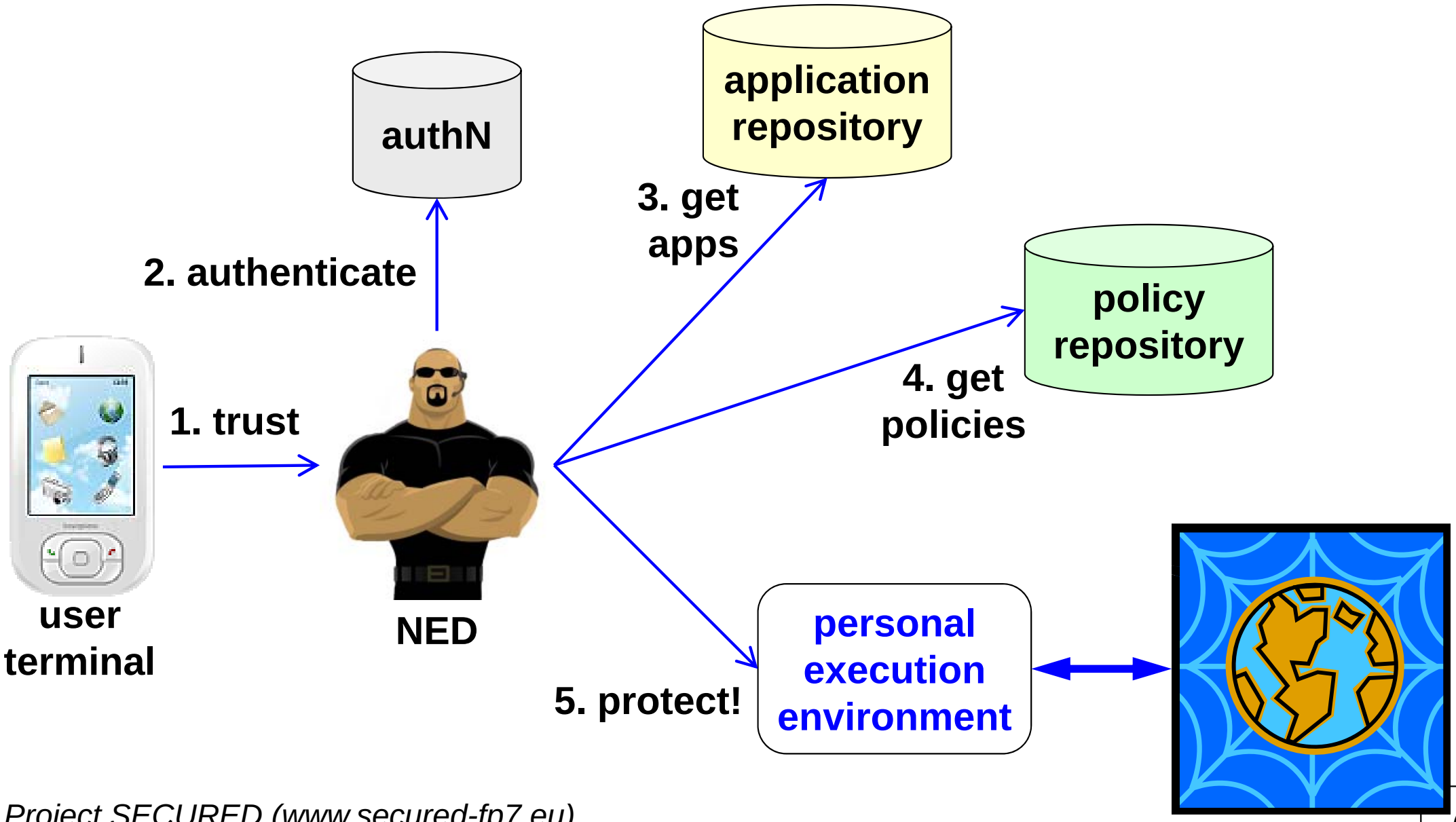
The SECURED components

- **NED (Network Edge Device)**
  - trusted node (with TC techniques)
  - provides a Trusted Virtual Domain per user
  - e.g. home gateway, corporate router, wireless AP, GGSN
- **Personal Security Applications (PSA)**
  - executed at the NED
  - specific tasks (packet filter, parental control, anti-phishing, content inspection, …)
  - chained according to security policies

- **security policies**
  - simplify configuration of PSAs and share "best practice"
  - flexibility (users care about policy, not implementation)



The SECURED framework architecture



The SECURED trust fabric

NED (Network Edge Device

policy

app(s)

TPM

user terminal

secure & trusted channel

measures

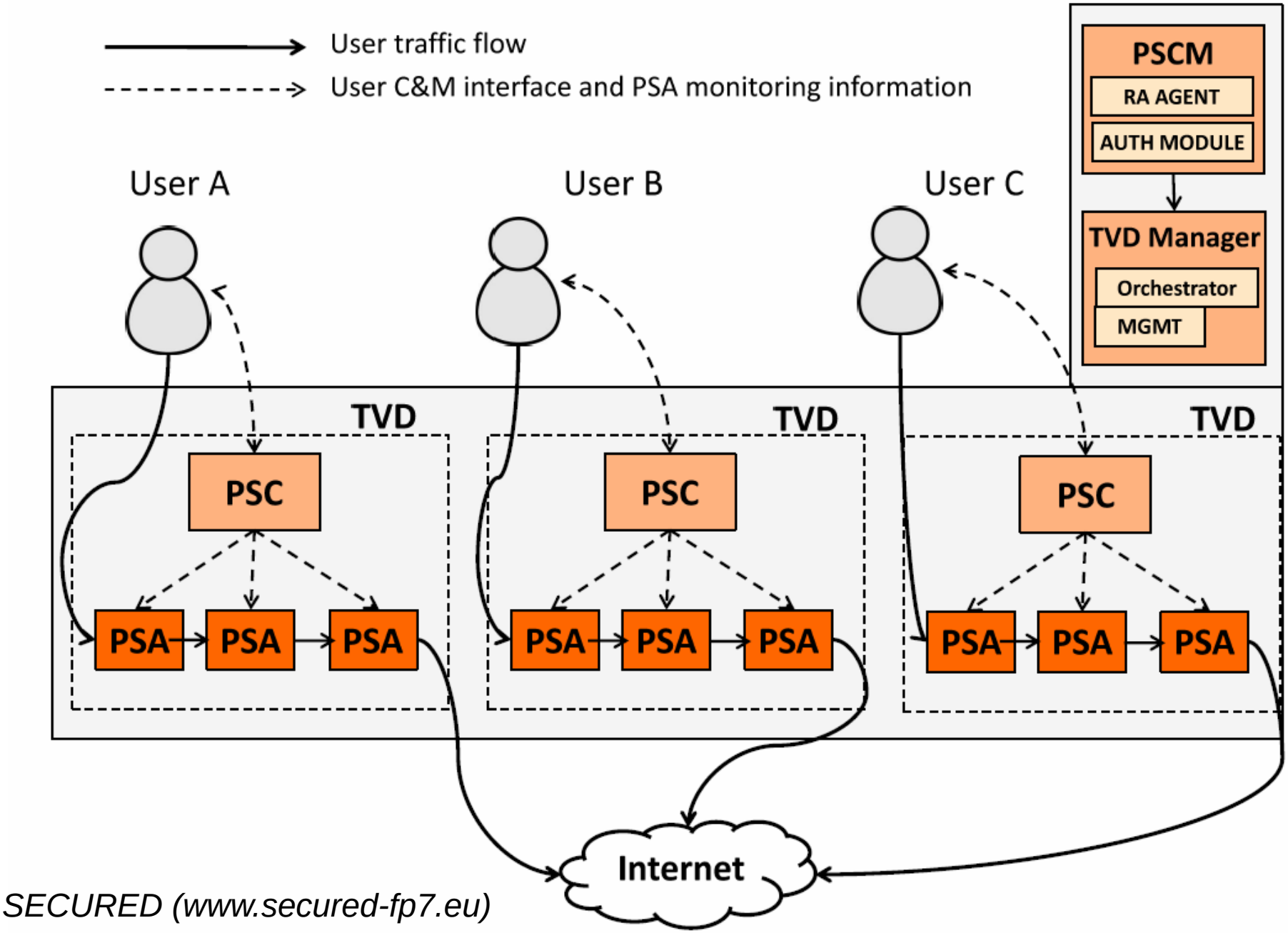
certification of "good" state (cryptographically bound to the secure channel)

verifier

The NED components

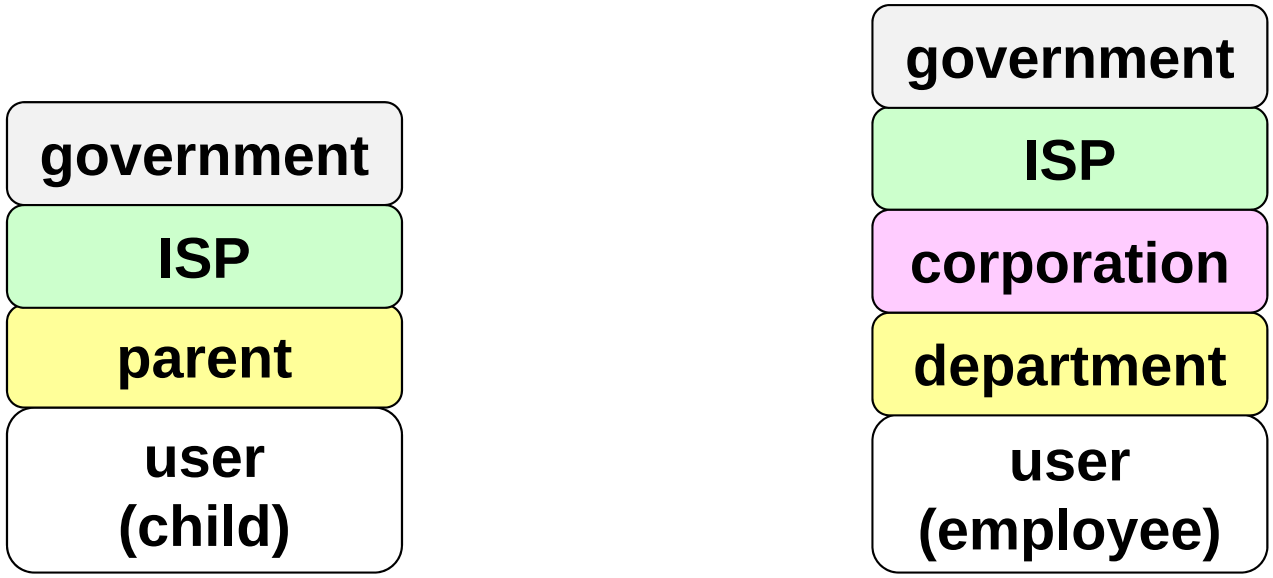
- **PSCM**
  - NED front-end, performs attestation, authN, policy analysis…
- **TVD Manager**
  - manages the network topology of a NED
  - configures the infrastructure
  - controls TVD lifecycle
- **Personal Security Controller (PSC)**
  - stores the user service graph (PSAs and interconnections)
  - determines the TVD topology from PSA and policy requirements
  - monitors the status of the TVD

The NED components at play



Multilayered security policies

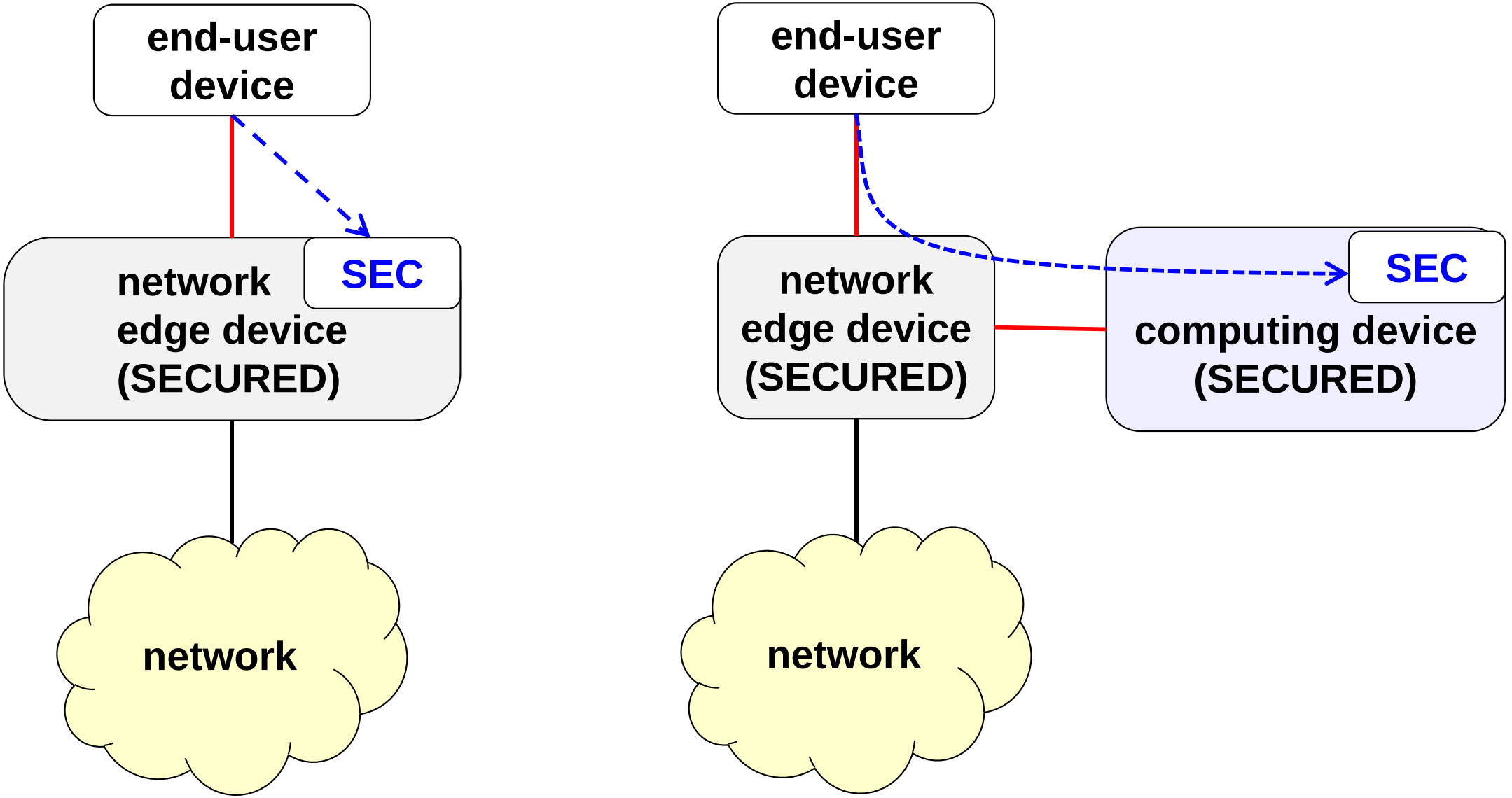
- **the same connection may be subject to constraints from different tenants (depending on the network environment)**
- **policies are applied in a hierarchical way (according to the user and connection profiles)**
- **user is informed of the overall policy applied to her connection (and may refuse connecting to the network)**



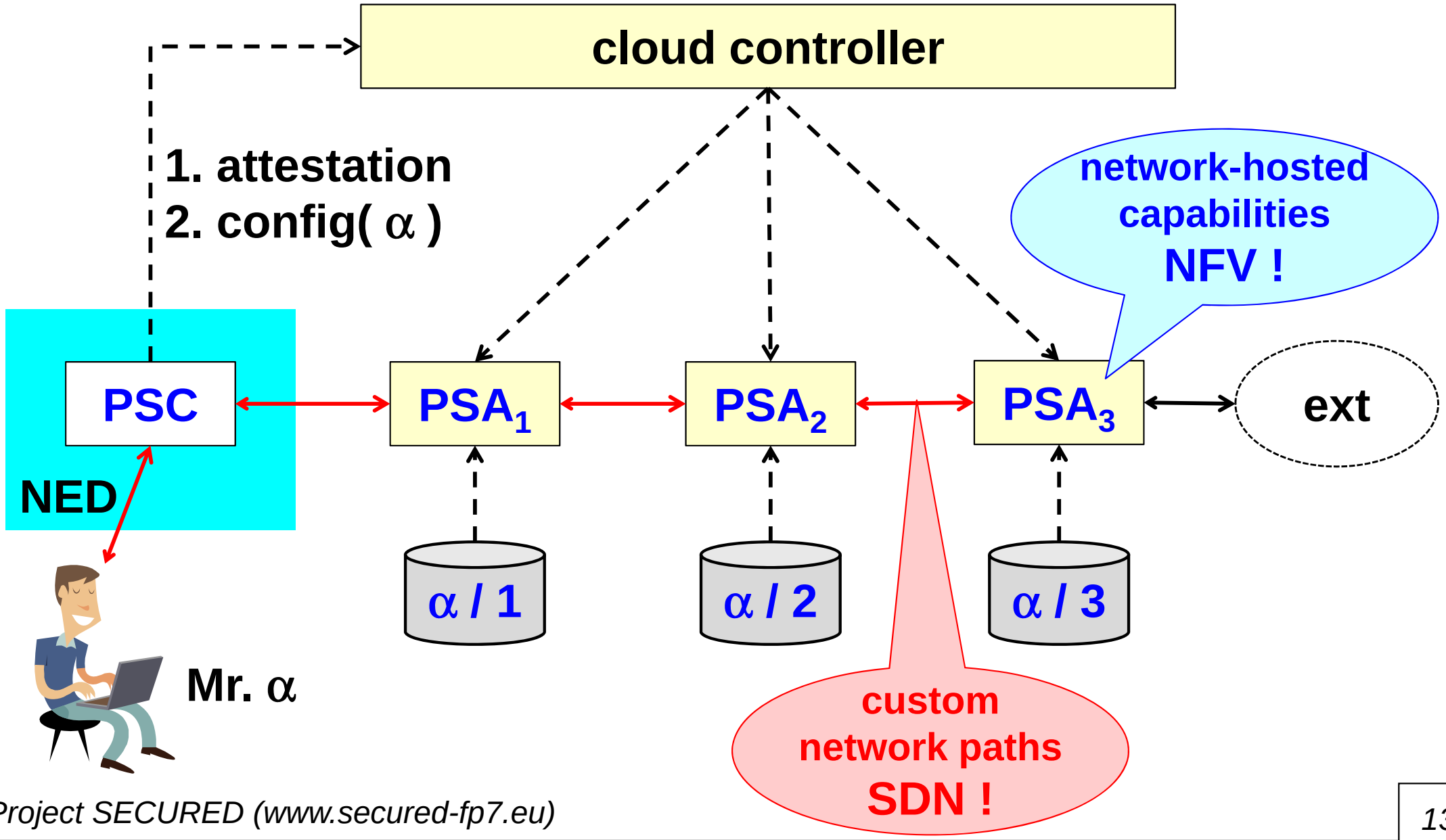
Expressing security policies

- **HSPL ~ high-level security policies**
  - for expressing the general end-user security requirements
    - Alice is not authorized to access Internet traffic (type of content,{illegal websites})
    - Bob wants email scanning (purpose,{malware})
- **MSPL ~ security capabilities**
  - to express configuration requests in an application-independent format
  - based on capabilities (atomic features of a security function)
  - capabilities grouped into categories, following an ontology
  - each PSA declares the categories it provides
- **automatic translation from HSPL to MSPL (and then to PSA)**

Monolithic vs split NED



Cloud / SDN / NFV for SECURED



The SECURED FP7 project

- **FP7 call 10 Collaborative Project (FP7-ICT-2013-10)**
- **grant agreement no. 611458**
- **duration: 3 years (1/10/2013 – 30/9/2016)**
- **EC contribution: 2.7 M Euro**
- **web: www.secured–fp7.eu**
- **mail: coordinator@secured–fp7.eu**

The Consortium (I)

- **Politecnico di Torino – Italy**
  - coordinator = Prof. Antonio Lioy (lioy@polito.it)
  - networking, trusted computing, security policies
- **HP Laboratory Bristol – United Kingdom**
  - networking, trusted computing
- **Primetel PLC – Cyprus**
  - telco, network and content provider (regional)
- **Telefonica Investigacion y Desarrollo – Spain**
  - telco and network provider (worldwide)

The Consortium (II)

- **United Nations Interregional Crime and Justice Institute – Italy**
  - social and policy aspects of security
- **Universitat Politecnica de Catalunya – Spain**
  - networking, mobility
- **(Barcelona Supercomputing Center – Spain)**
  - computational architectures
- **VTT Technical Research Centre of Finland**
  - cybersecurity

THANK YOU !

Project SECURED (www.secured-fp7.eu)

SEVENTH FRAMEWORK
PROGRAMME

Disclaimer

EU disclaimer

SECURED (project no. 611458) is co-funded by the European Union (EU) via the European Commission (EC), under the Information and Communication Technologies (ICT) theme of the 7th Framework Programme for R&D (FP7).
This document does not represent the opinion of the EC and the EC is not responsible for any use that might be made of its content.

SECURED disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.