I2NSF Use Cases in Access Networks

Diego Lopez

(diego.r.lopez@telefonica.com)
Telefónica I+D

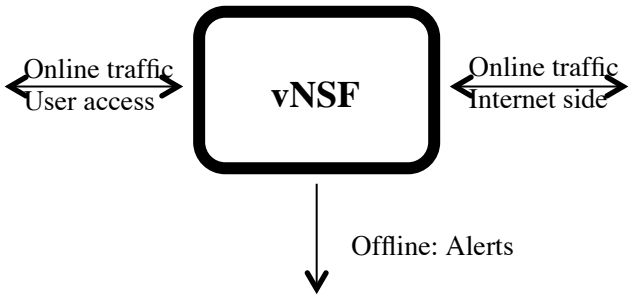
IETF91, Honolulu, 9-14 Nov.

Seeking an Open OAM Interface

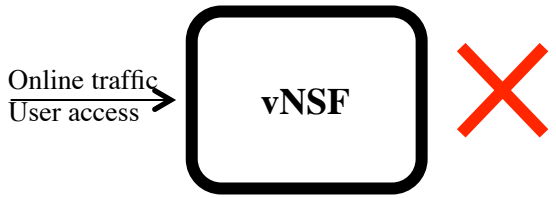
- **What?: Open OAM interface for virtualized network security services (vNSF)**
- **Who?: Actors:**
  - Network operator
  - Customer(s)
- **Where?: Access network**
  - Residential (and SME) landline network access: xDSL, FTTH
  - Mobile network Access: 2G, 3G, 4G, 5G…

A Few Examples of vNSFs

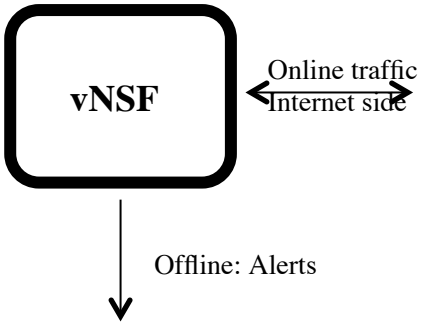
- **Traffic inspection**
  - All services that copy/analize traffic
  - E.g.: IDS,DPI,DLP



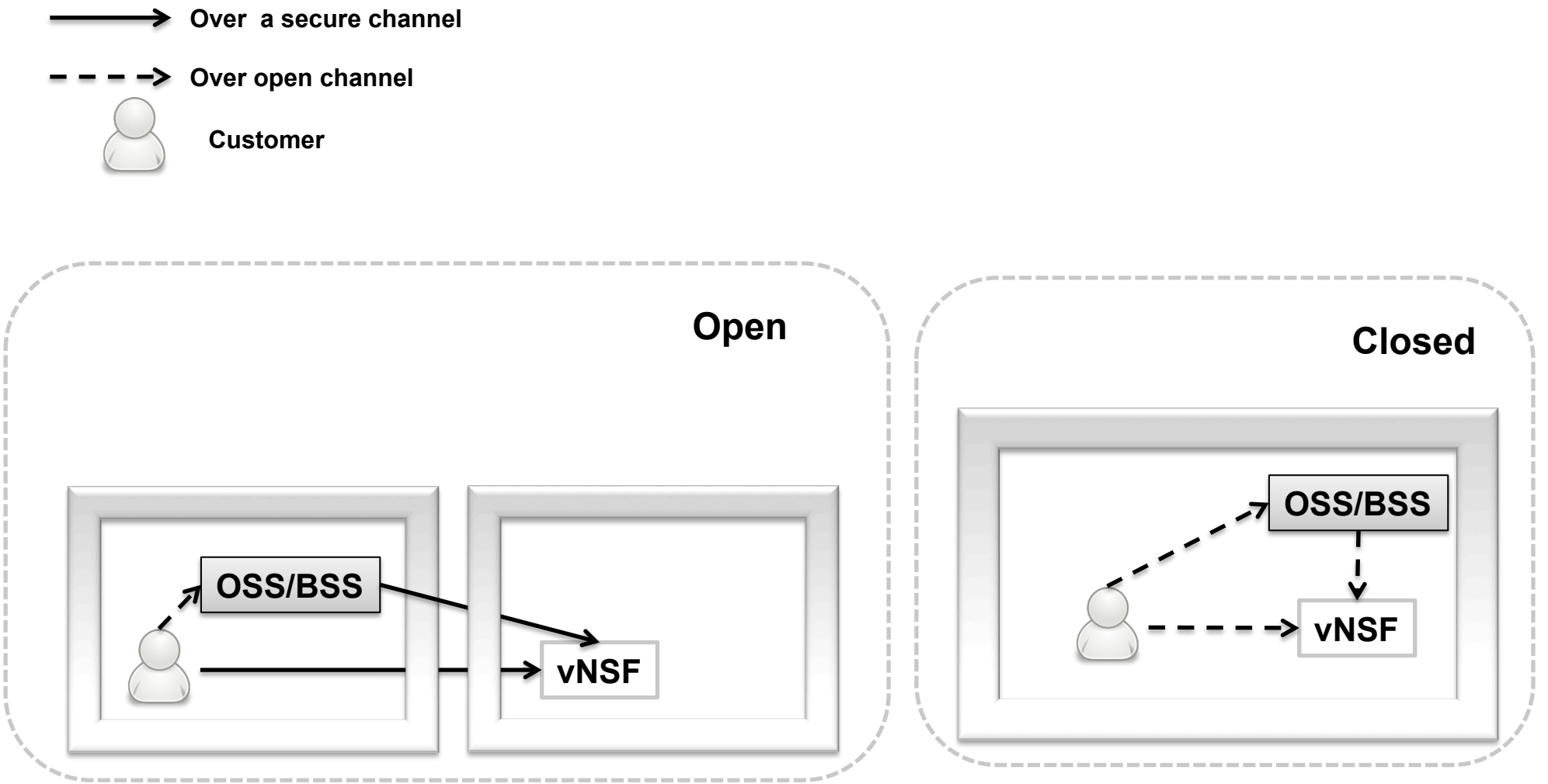
- **Traffic Manipulation**
  - Alteration of the original traffic
  - E.g.: IPS,ACL,FW,VPN



- **Traffic Impersonation**
  - Impersonate a customer device or service
  - E.g.: Honeypot



OAM Environments



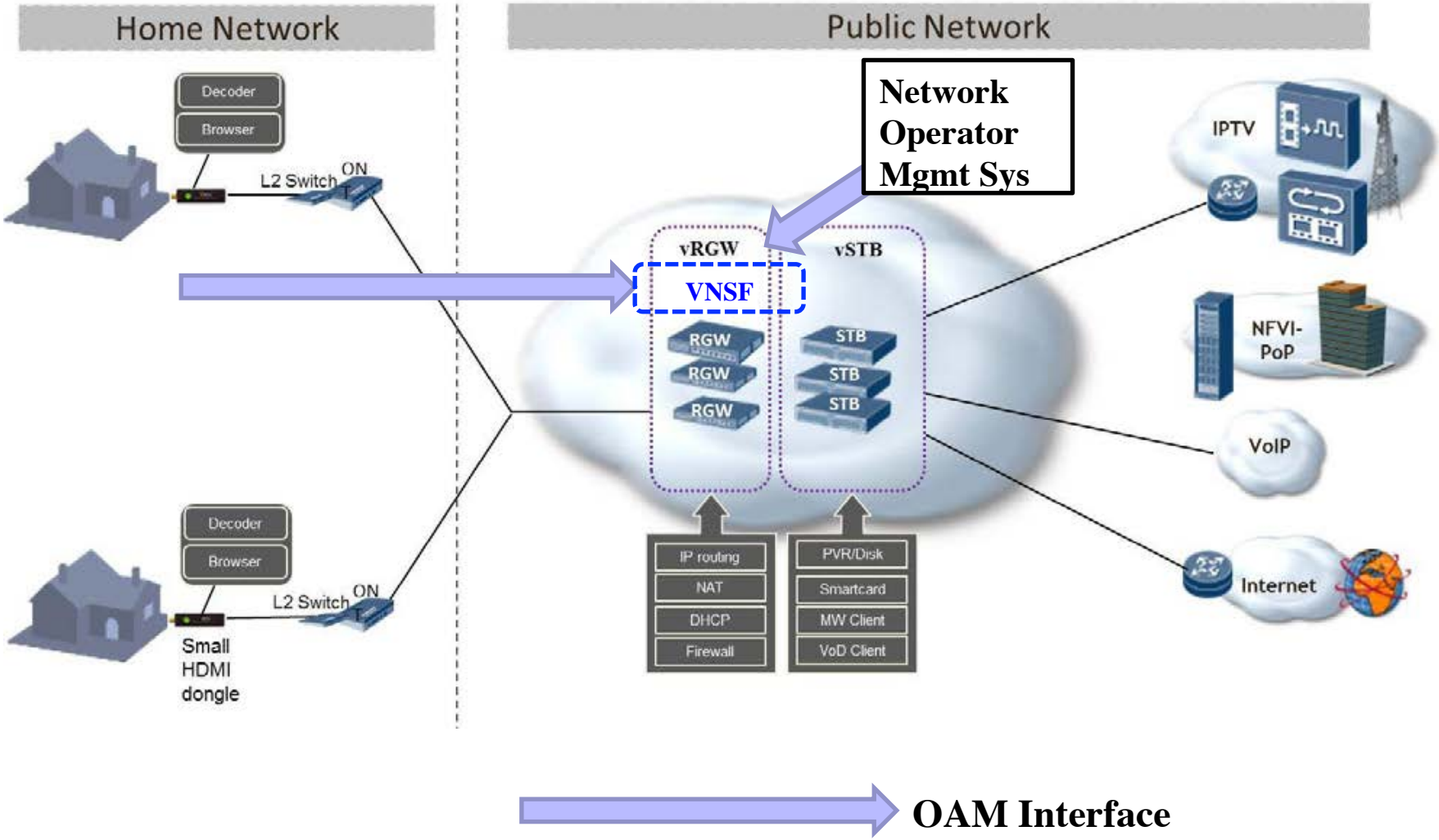
Operator-Managed

- **Network Operator interactions**
  - vNSF deployment
    - instantiating a vNSF on a NFVI
  - vNSF Customer provisioning
    - List vNSF functionalities
    - enroll/cancel subscriptions
    - vNSF configuration
      - By policy language.
      - By configuration templates/files

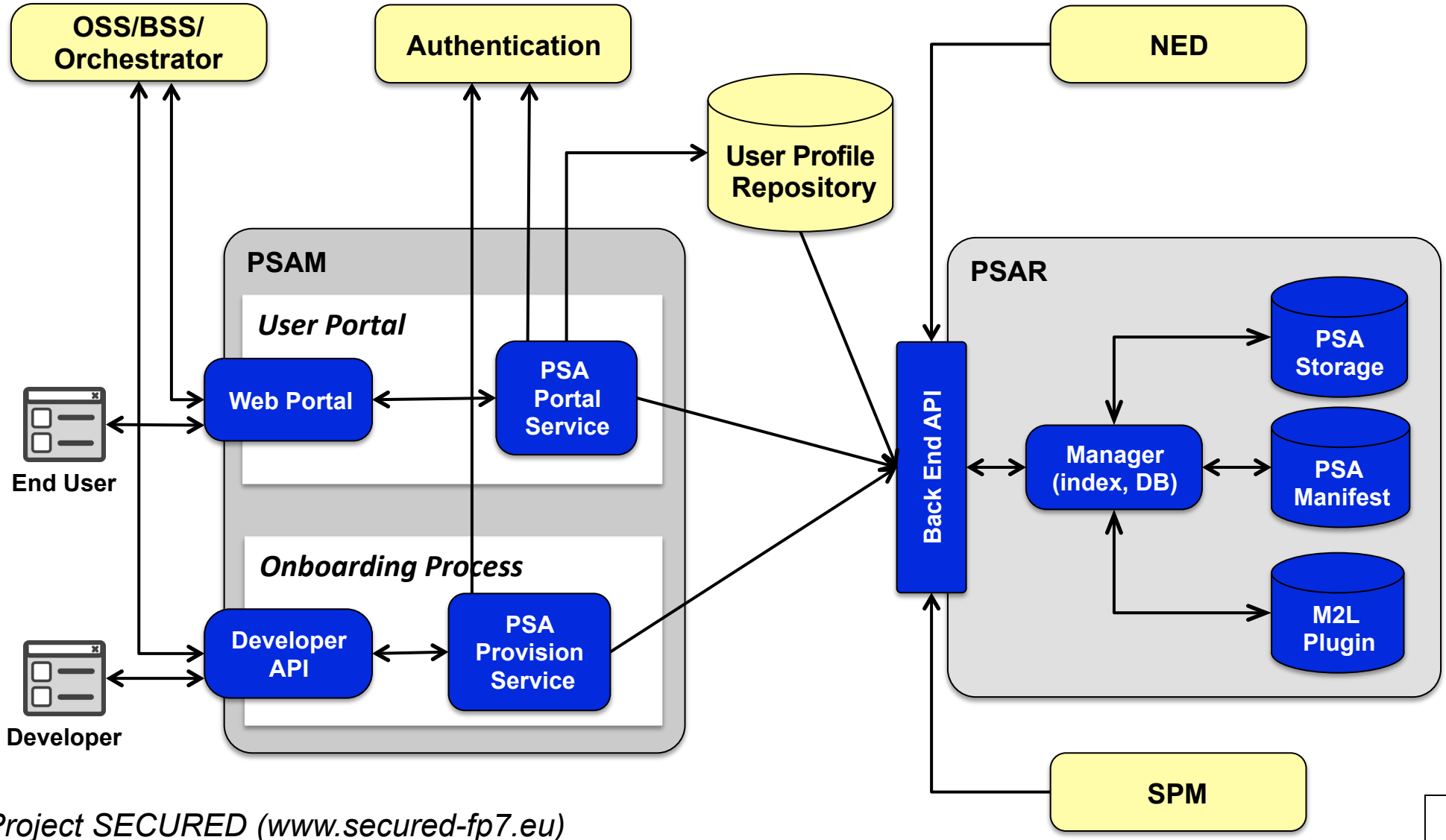
Customer-Managed

- **Customer direct interactions**
  - vNSF self-provisioning
    - enroll/cancel subscriptions
    - Probably also need a vNSF configuration
  - vNSF validation
    - Customer could require a proof of correct vNSF execution:
      - Integrity
      - Isolation & privacy
      - Confidentiality?

Example: The NFV #7 Use Case for vCPE

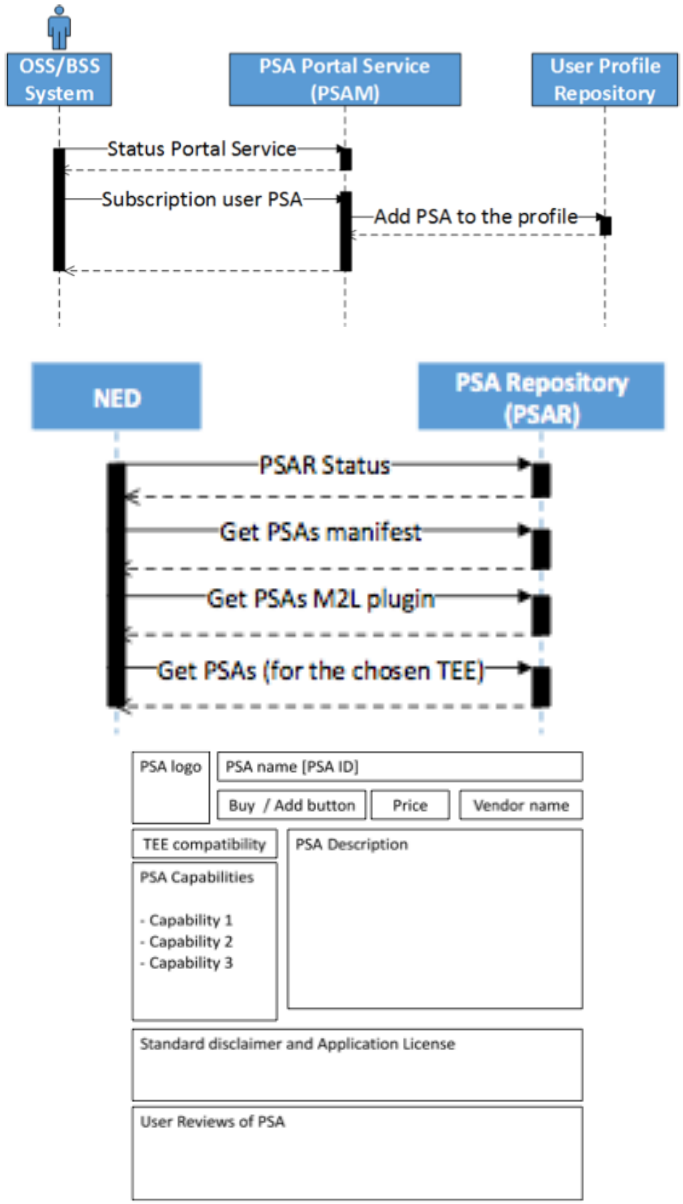


Bringing This into Reality: The SECURED Architecture



Specifying PSAM and PSAR in SECURED

- **Programmatic interfaces**
  - PSAM API
    - User provisioning
    - Load PSA in the system
  - PSAR API
    - Service support (information manager)
    - Deployment of PSA
- **User Portal**
  - Public eye area



Expressing Policies

- **vNSF configuration language**
  - Set by Operator or by Customer itself

<sbj> <*act*> <*obj*> [<(*field_type,value*)>...<(*field_type,value*)>]

- **<sbj> the subject of the policy**
  - **(e.g., employee, family member)**
  - **subject may be implicit (e.g., all devices of a customer)**
- **<*act*> the action of the policy**
  - **(e.g., block, allow, protect…)**
- **<*obj*> *the object of the policy that undergoes the action***
  - ***(e.g., email, web traffic, DNS request)***
- **[<(*field_type,value*)> condition that characterize actions**
  - **(e.g., time, type of traffic...)**

- **Examples:**

enable basic parental control
enable ”school protection control”
allow Internet traffic from 8:30 to 20:00 *[time = 8:30-20:00]*
scan email for malware detection *[check type = malware]* protect traffic to corporate network with integrity and confidentiality *[protection type = integrity AND confidentiality]*
remove tracking data from Facebook *[website = *.facebook.com]*
my son is allowed to access facebook from 18:30 to 20:00

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.