NFV and security: the necessary convergence

Antonio Pastor

Telefónica I+D

< antonio.pastorperales@telefonica.com >

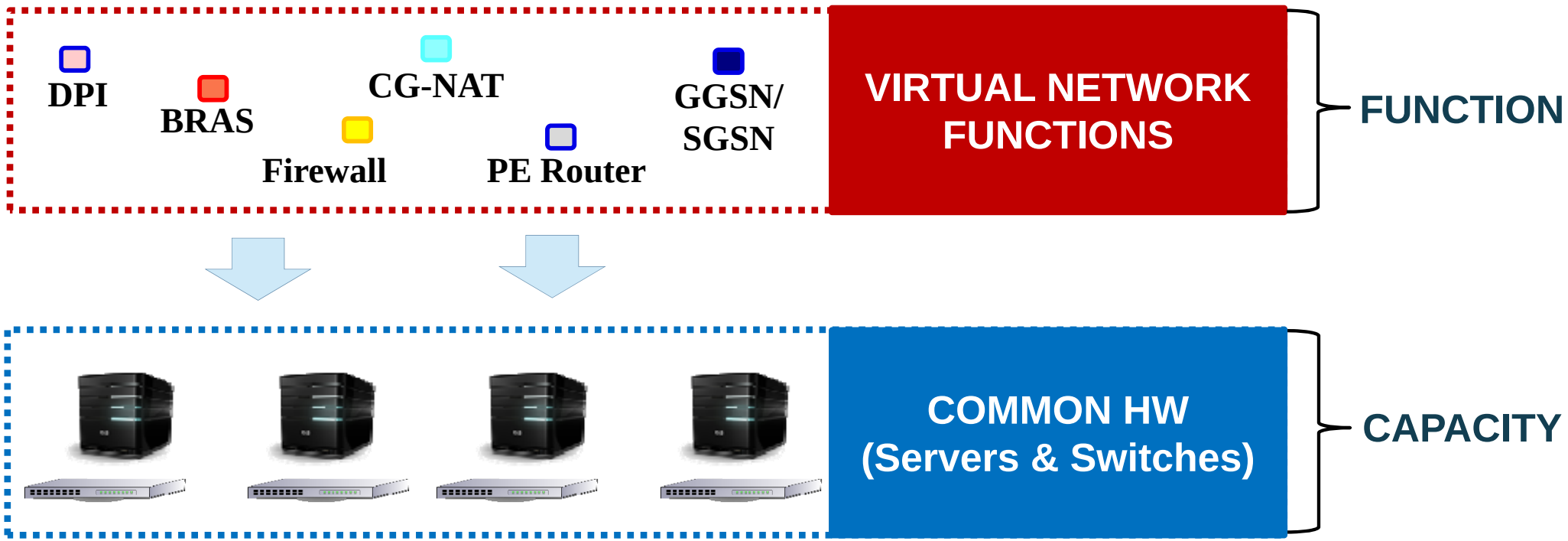
Cybersecurity & Privacy Innovation Forum 2015

Brussels, 28/4/2015

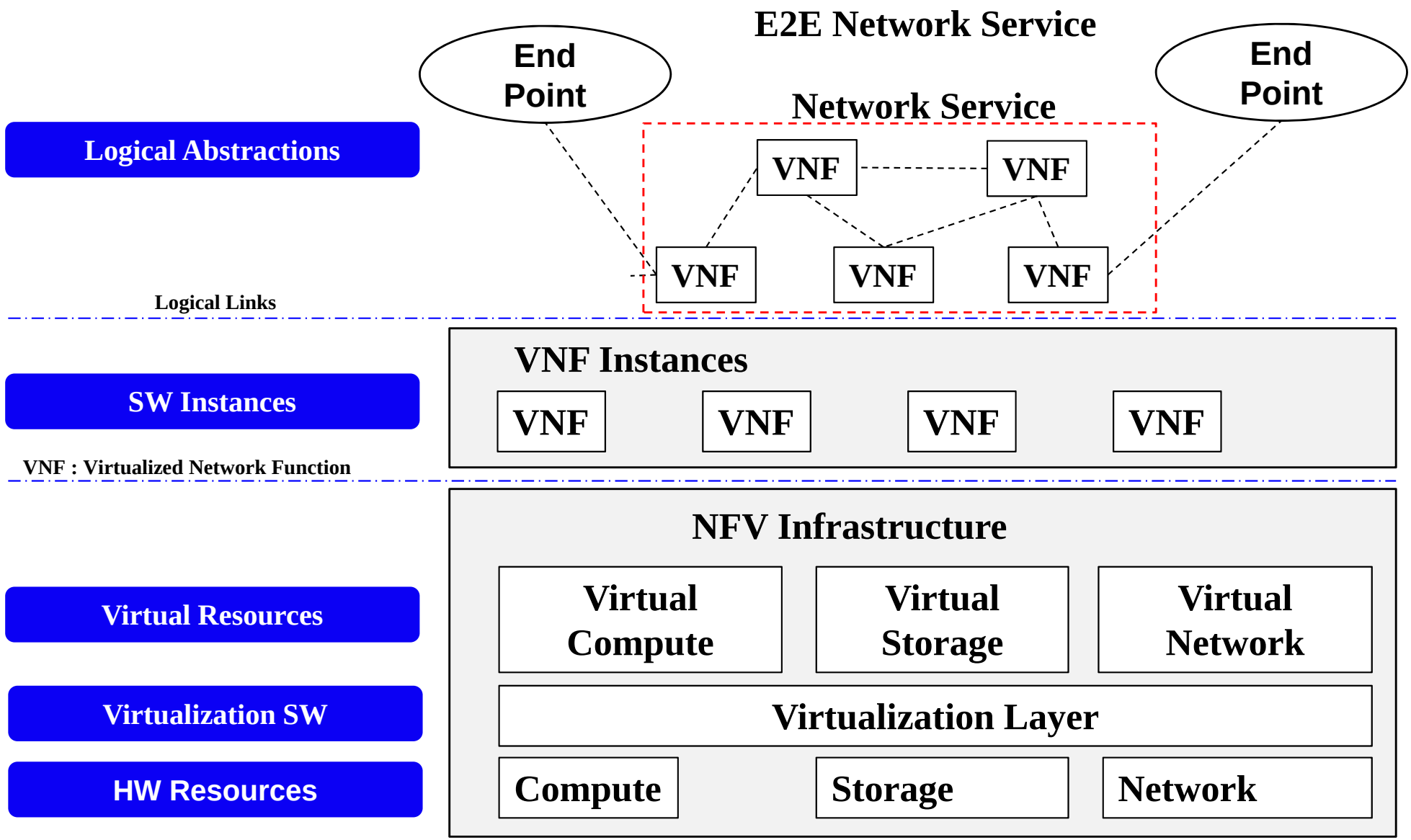
SEVENTH FRAMEWORK PROGRAMME

The NFV concept

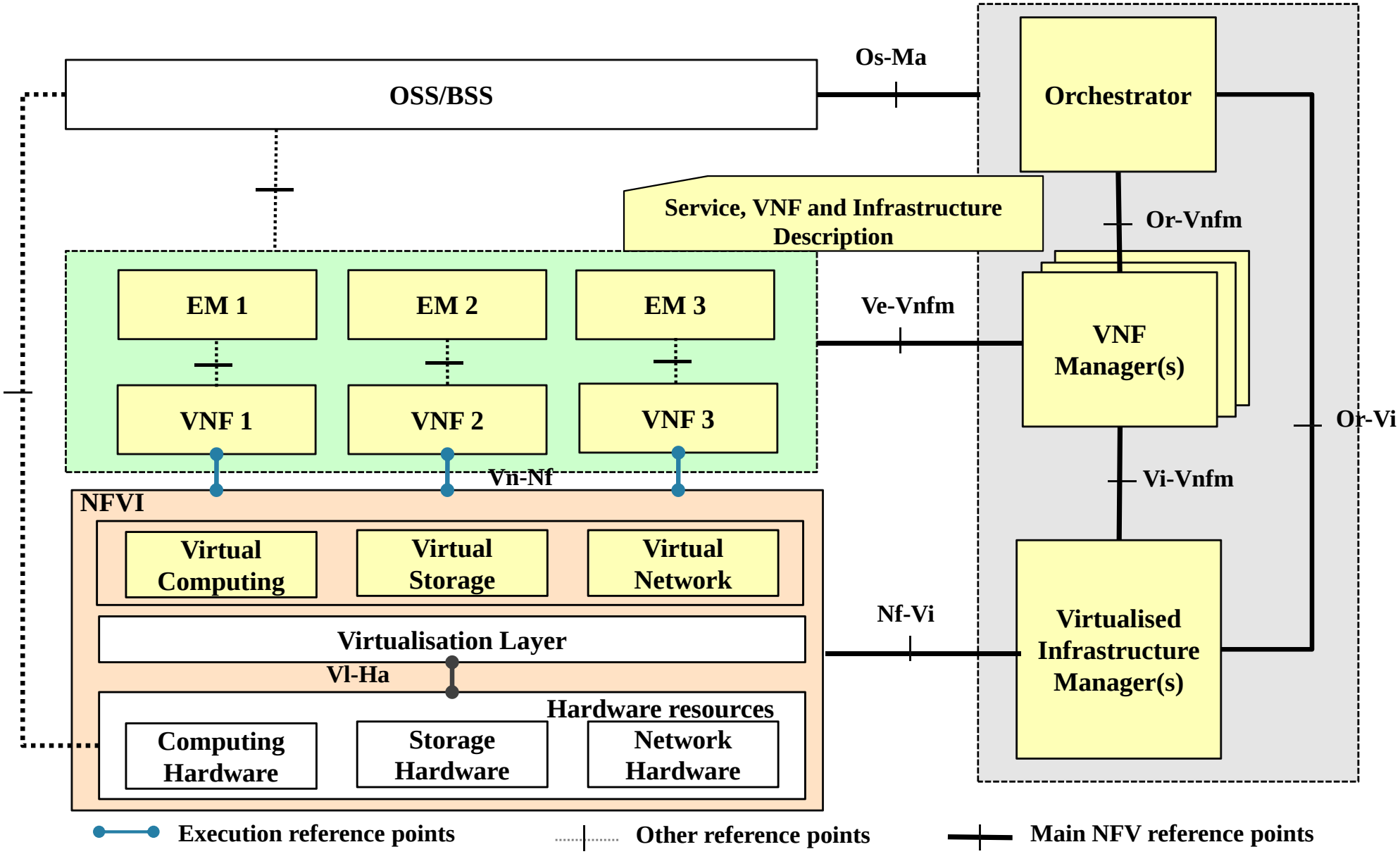
Network functions are fully defined by SW, minimising dependence on HW constraints



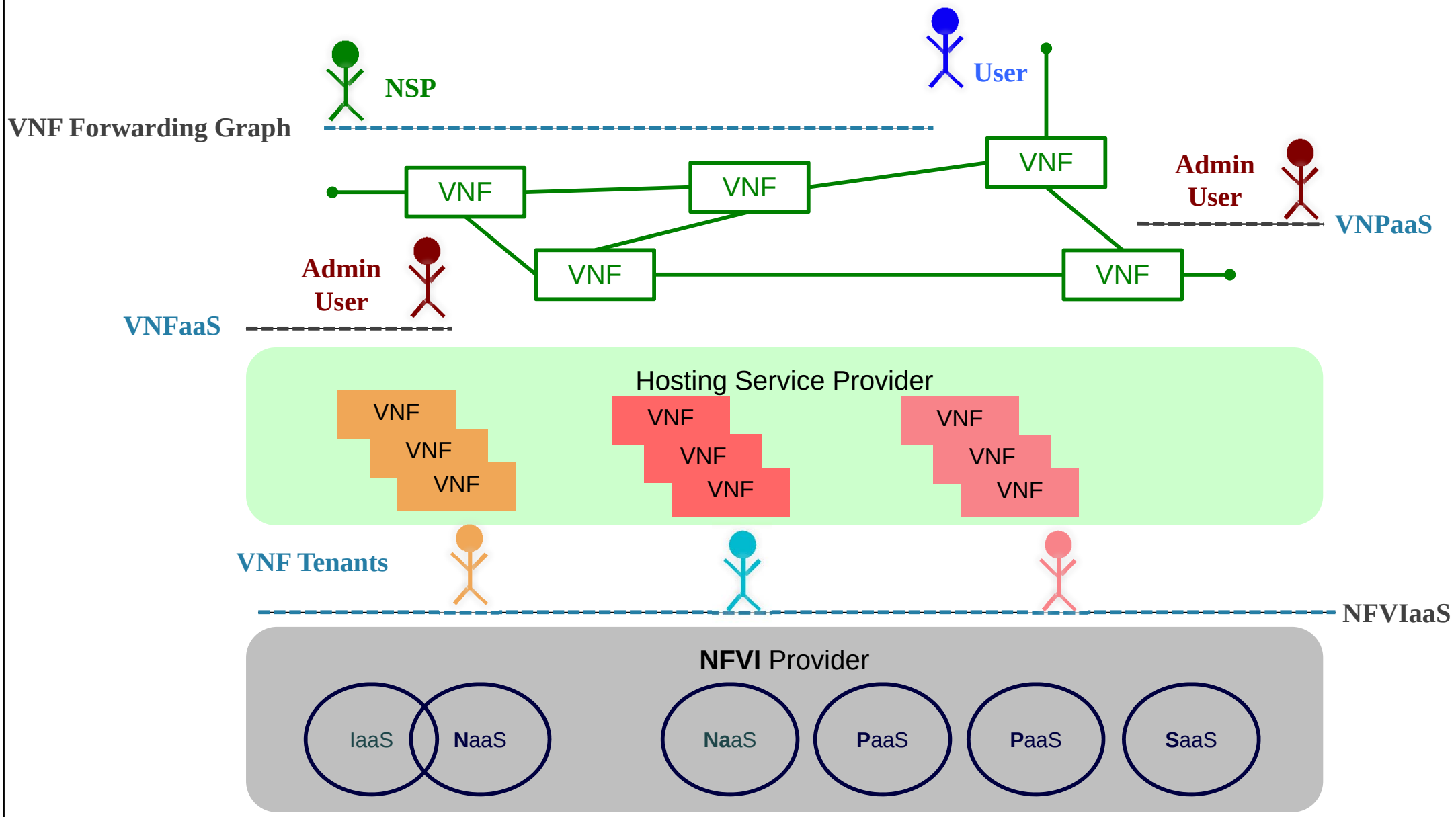
The NFV framework



The NFV reference architecture



XaaS for network services



It ain't cloud applied to carriers

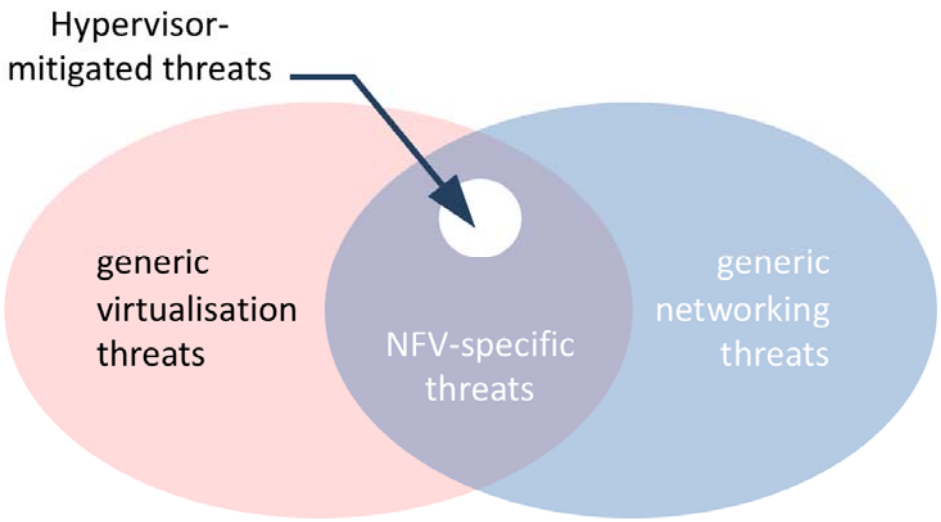
The network differs from the computing environment in 2 key factors …

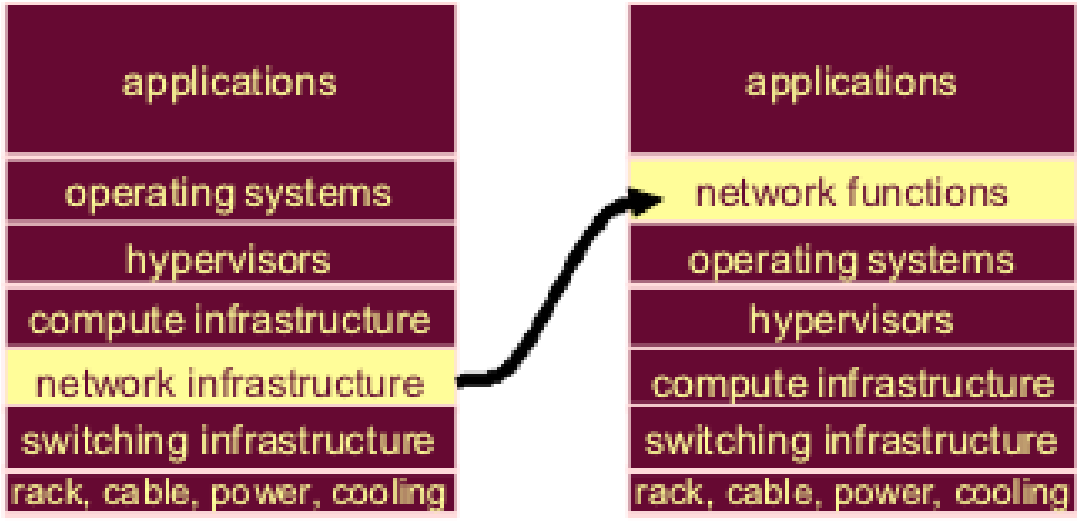
1. **Data plane workloads (which are huge!)** → **HIGH PRESSURE ON PERFORMANCE**
2. **Network requires shape (+ E2E interconnection)** → GLOBAL NETWORK VIEW IS REQUIRED FOR **MANAGEMENT**

…which are big challenges for vanilla cloud computing.

AN ADAPTED VIRTUALISATION ENVIRONMENT IS NEEDED TO OBTAIN CARRIER-CLASS BEHAVIOUR

Security for NFV





Scoping the problem

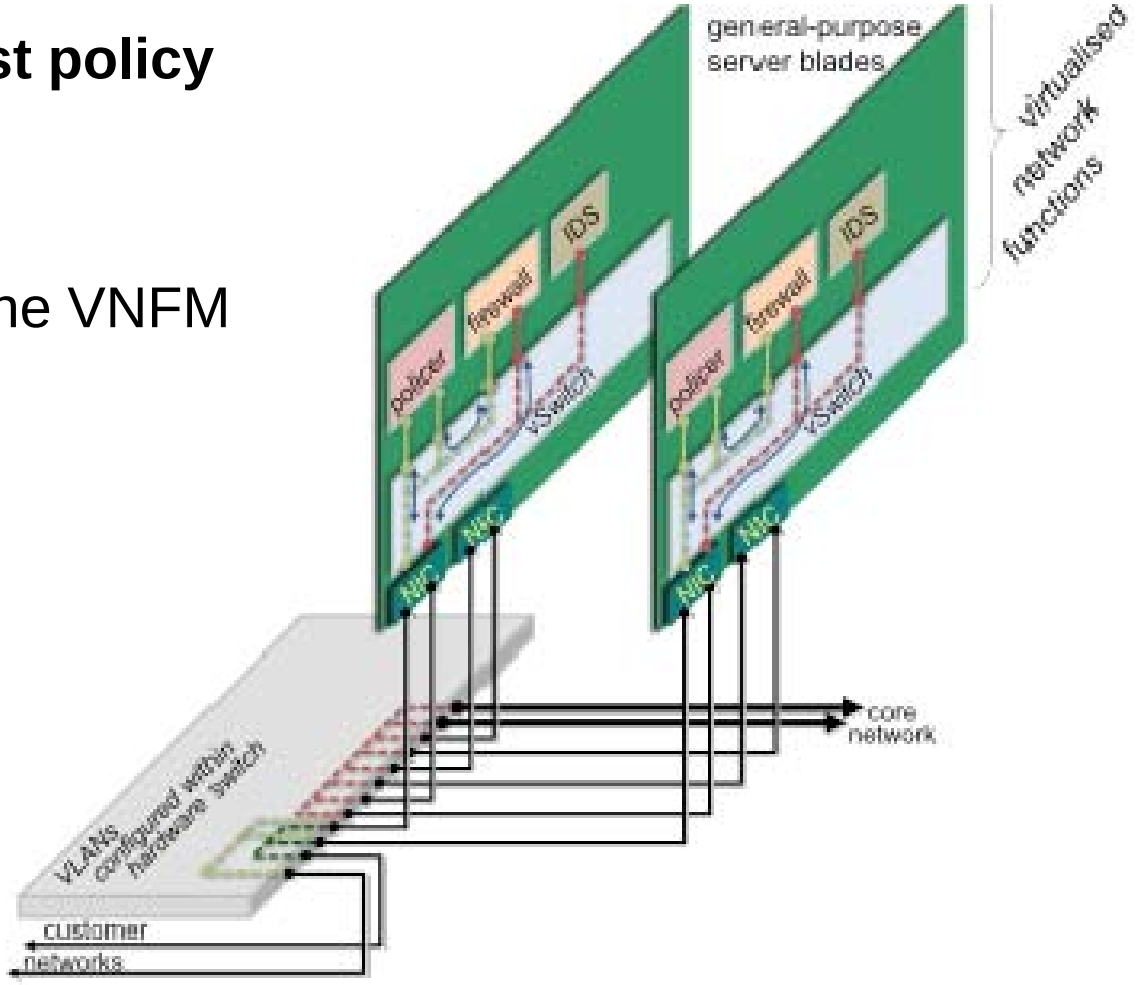
- **shrink additional threat surface**
  - general network
  - general virtualization
- **enlarge hypervisor mitigation**
  - introspection
  - containment

Consider the re-layering

- **network functions as infrastructure**
- **network functions as applications**
- **network functions as services**
- **the SDN-NFV *sandwich***

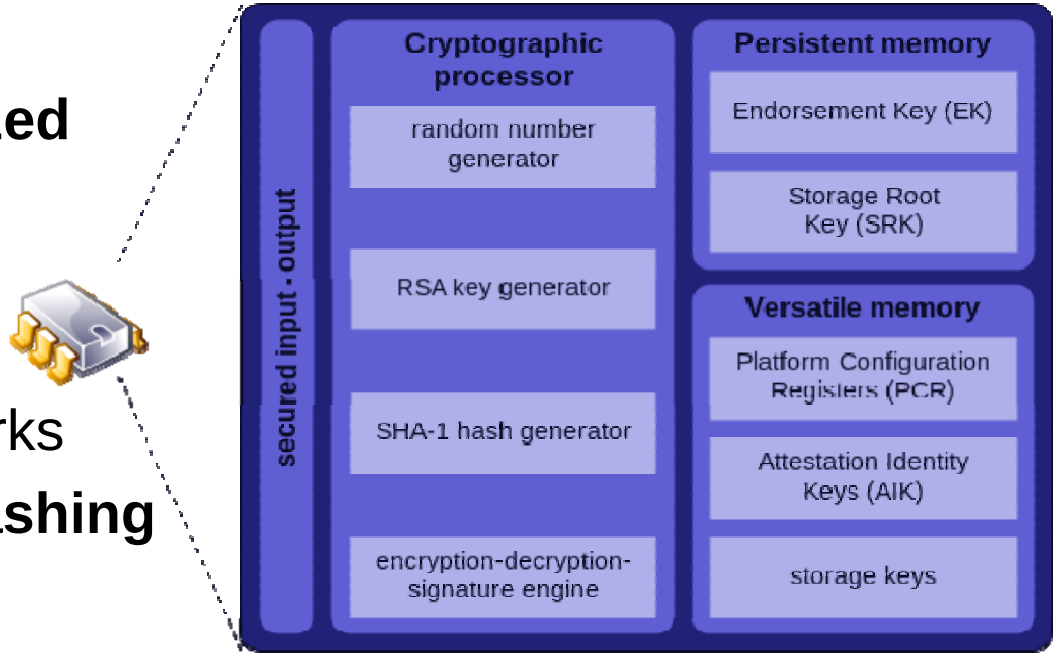
Topology and infrastructure integrity

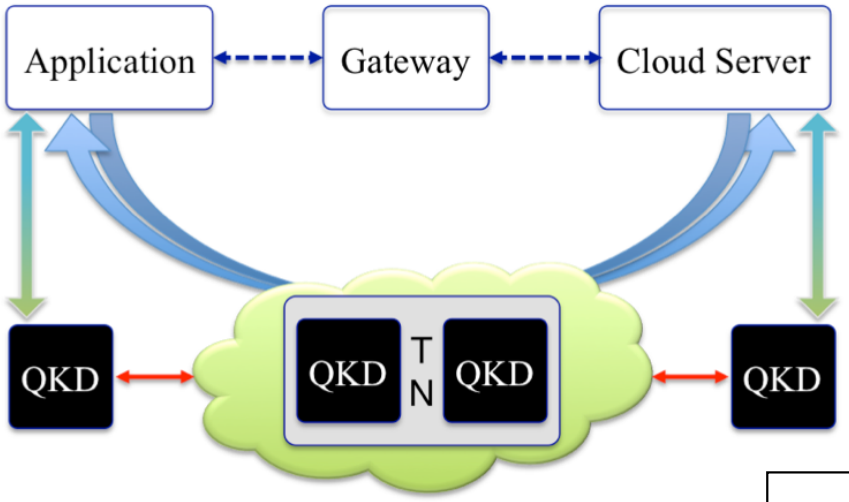
- **verify deployment topology against policy**
- **(mostly) SDN validation**
  - at the infrastructure – the VIM
  - within the virtualized functions – the VNFM
  - at the service level – the NFVO
- **tools for the first layer**
  - current practice in SDN
  - but complexity is higher
  - and beware the MiTF
- **the two upper layers need further study and development**
  - and NFV/SDN interaction models
- **out-of-band management availability**
- **integrity of clock synchronization**



Secure boot, secure crash, and key distribution

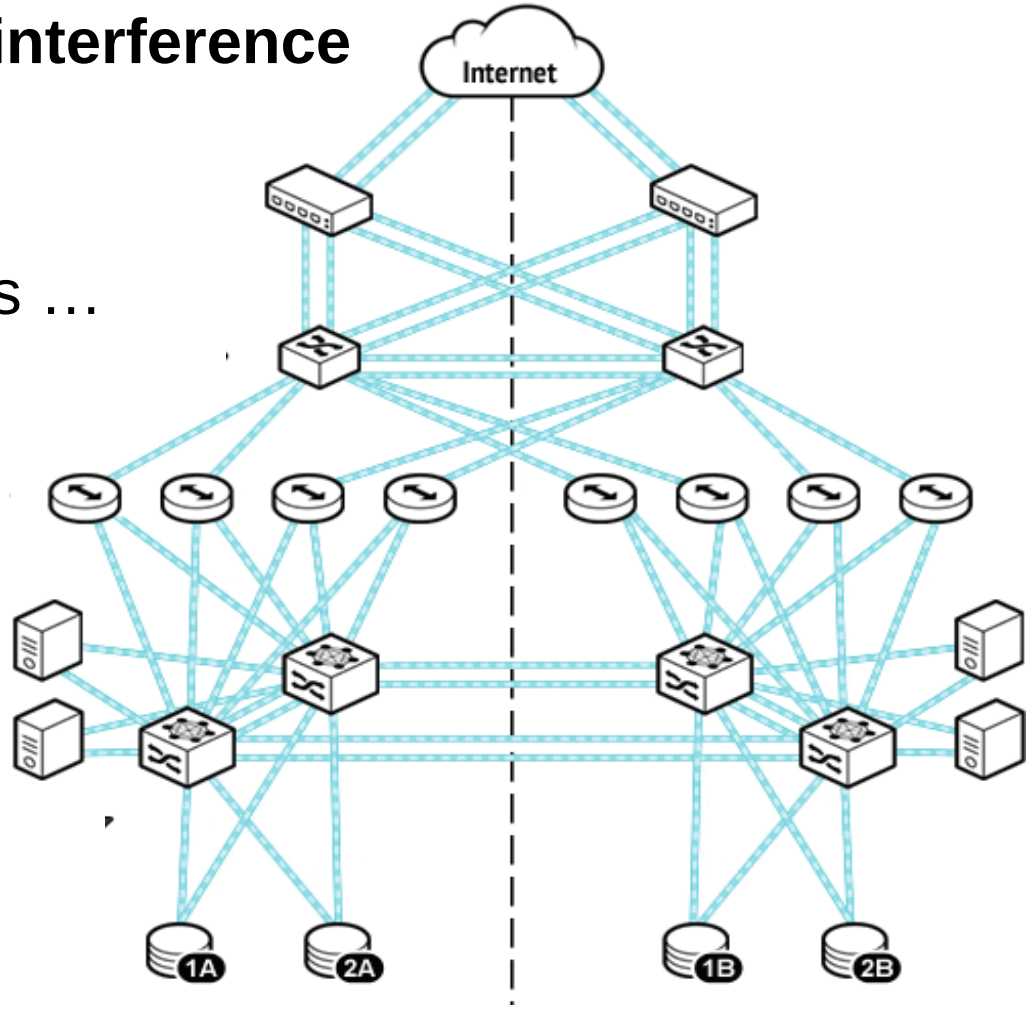
- **scaling issues applying the virtualized TPM model**
  - management system availability
  - key management robustness
  - key revocation in carrier-size networks
- **avoid information leakage by VM crashing**
  - MACs, tags…
  - and keys!!
  - distributed garbage collection
- **key distribution**
  - distribution of clone images
  - replication vs distribution of private keys
- **considering the feasibility of QKD for some of these tasks**





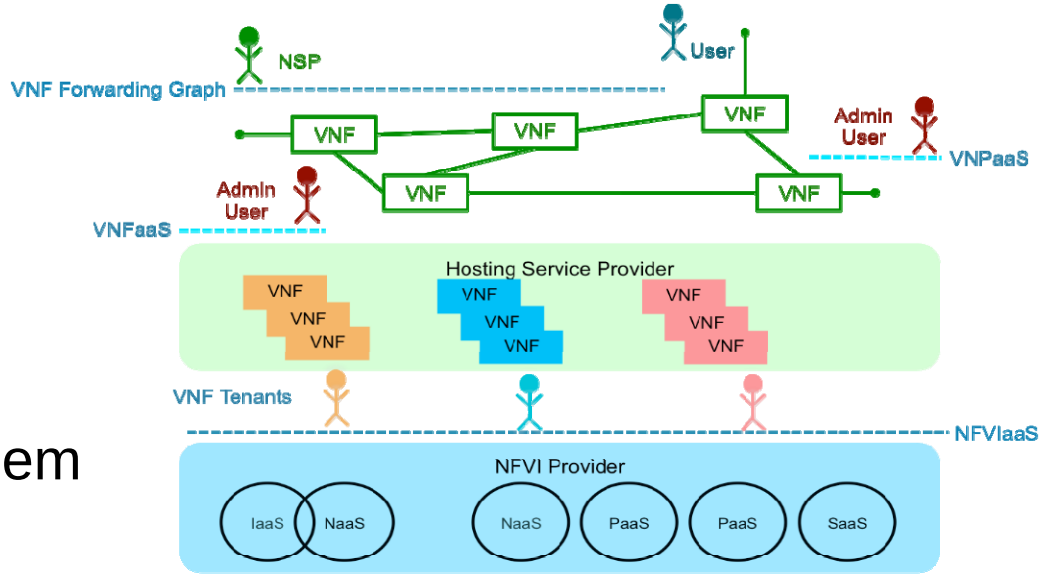
Performance isolation

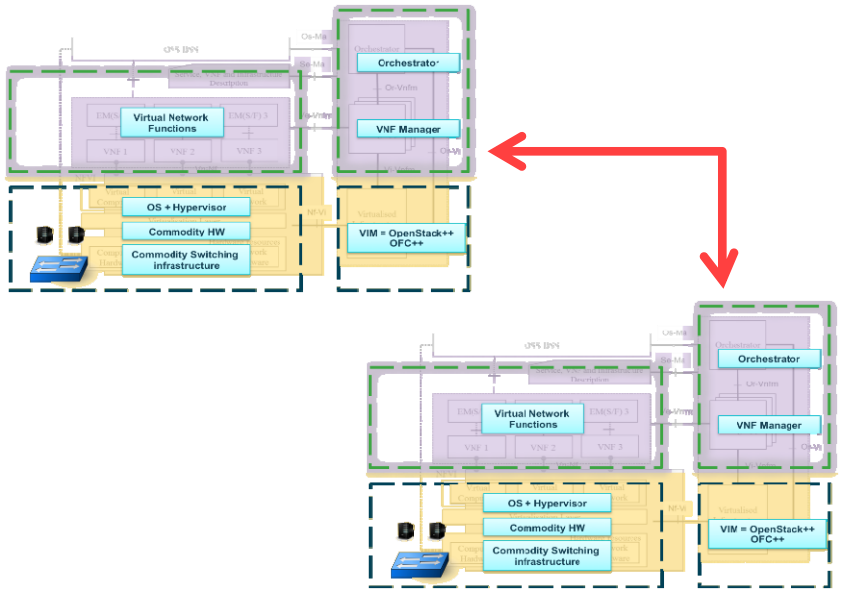
- **avoid VNFs (or VNF components) interference or eavesdropping**
- **network**
  - guaranteed QoS, full obliviousness …
- **shared cores**
  - fine-grained placement
- **the problem of hw acceleration**
  - virtualization of the non-virtualized
- **memory and storage**
  - addressed in current clouds
  - a problem of scale: real time, high distribution



User and tenant AAA

- **appropriate identity management**
  - vertical (XaaS)
  - horizontal (federation)
- **limit attribute disclosure**
  - at layers not intended to consume them
- **avoid privilege escalation**
  - wrapping unrelated identities not verifiable at a given layer
- **perform accounting at all the underlying infrastructure layer(s)**
  - beyond the granularity of virtualized applications that use the infrastructures
  - support the capability of (recursively) billing the billers





Altered procedures

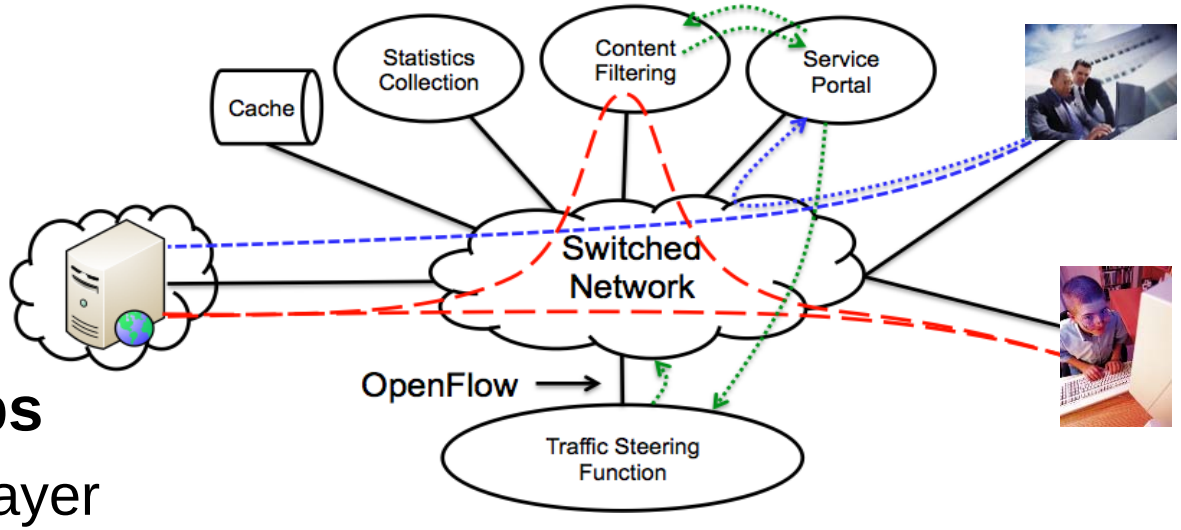
- **physical access will no longer be required to execute insider attacks**
- **functions will become executed on off-the-shelf hardware and software**
  - more reported and unreported (zero-day) vulnerabilities
  - more attack tools available, such as virus and rootkits
  - more people trying to exploit commodity software (for fun, fame, or finance)
- **NFV could be exploited to cause larger scale disruption**
  - increased motivation for attackers
  - need for virtualization to be re-assessed for critical network infrastructure
- **back-doors via VNFs**
  - a common practice for sw development, debugging, and testing
- **maintenance by patching**
  - security patches may require a reboot and imply unacceptable service disruption
  - handling of zero-day vulnerabilities

Applying NFV to the many A's in security

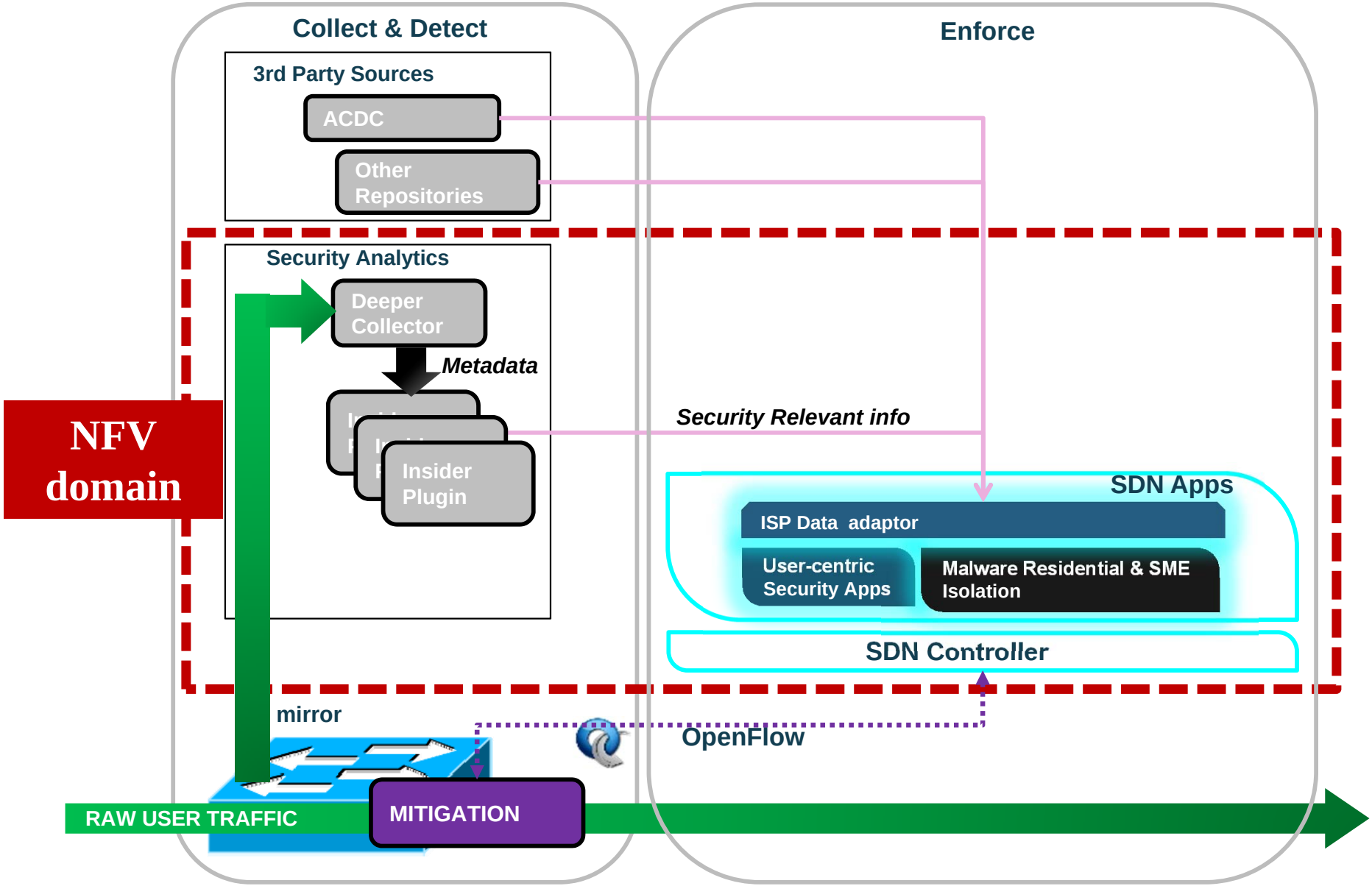
- **Authentication**
  - know who gets involved
  - go beyond the user-at-a-location
- **Authorization**
  - establish and enforce usage policies
  - go beyond the user-behind-a-portal
- **Accounting**
  - register how resources are used
  - what and by whom
- **Analysis**
  - understand usage patterns
  - identify threats and attackers
- **Action**
  - alleviate incident impact
  - collect information for further response

AAA: the Who, the What, the How

- **any starting network flow can be used to**
  - establish user identity en-route
  - apply policies
  - define sessions
- **break blind trust relationships**
  - individualized services at any layer
  - establish trust links with a variety of partners
- **mirror flows as required**
  - associated with identity
  - at any relevant level and layer
- **services can follow users**
  - identity-based service chaining



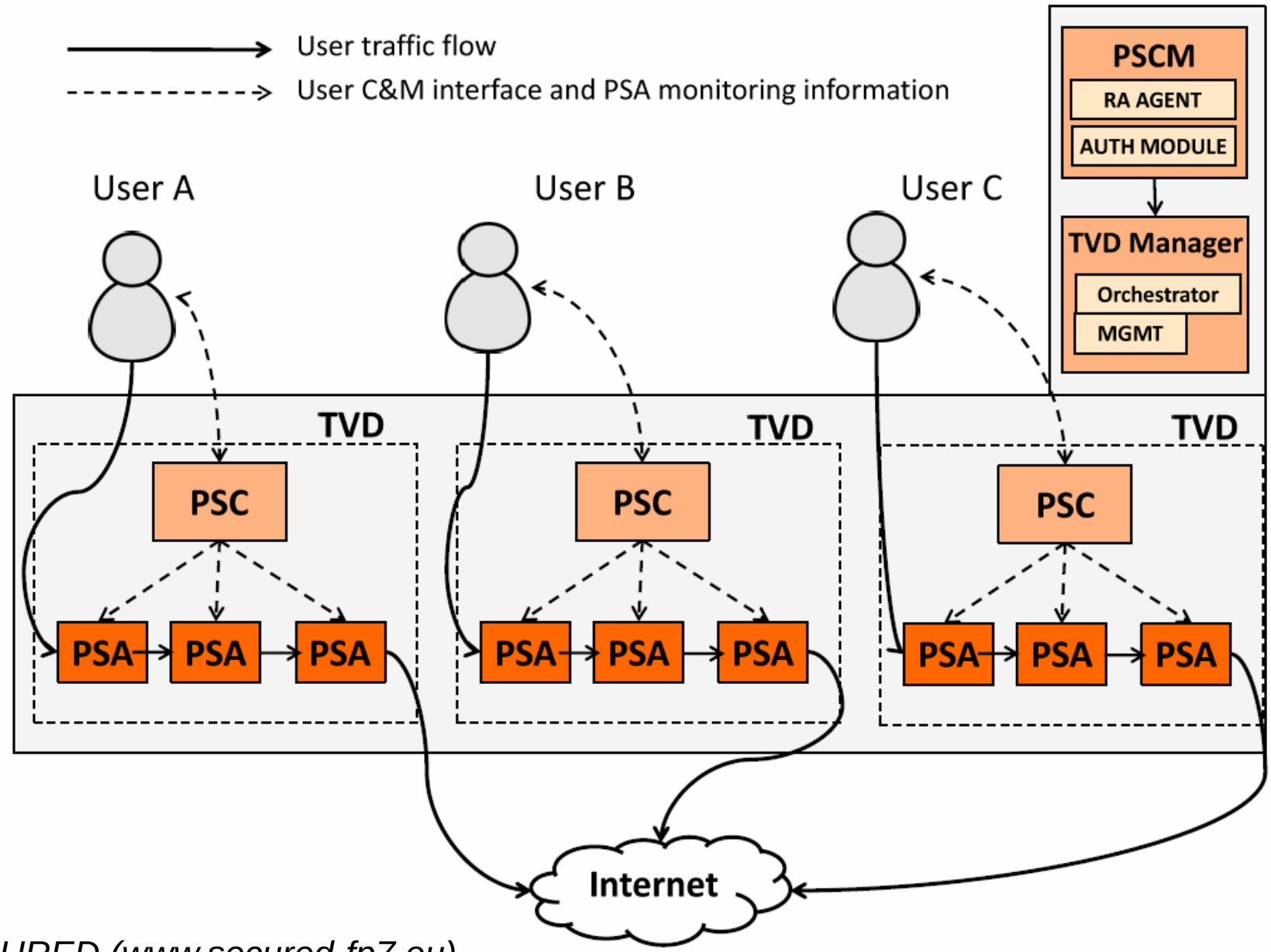
Analysis & action: infrastructural security



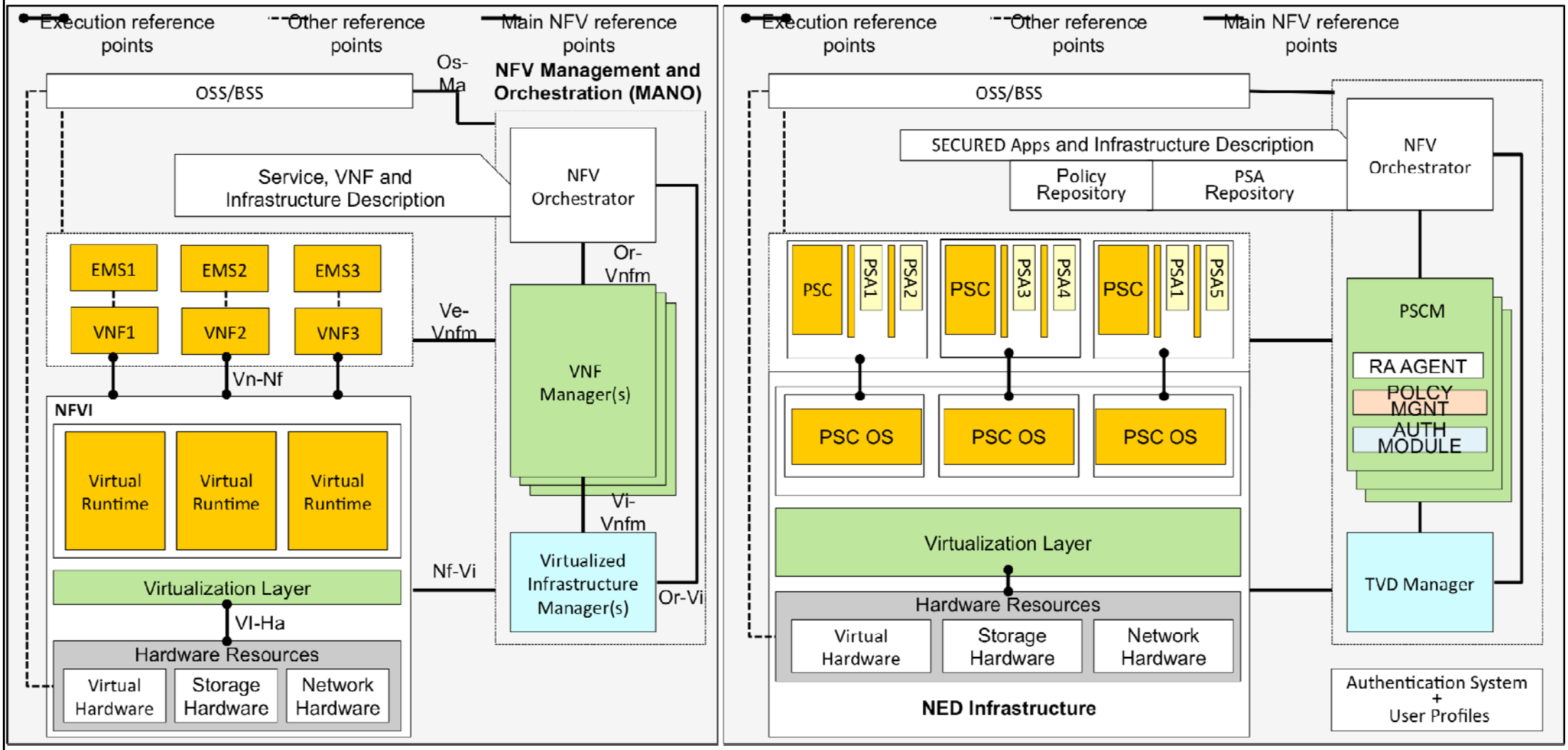
The SECURED NED components

- **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 requirements
  - monitors the status of the TVD

The SECURED NED components at play



Mapping onto the NFV framework



NFV and SECURED - more than a mapping

- **SECURED implies offloading security applications to a trusted, personalized virtual domain**
  - high level of assurance
  - based on identity
  - attestation required at all levels
    - infrastructure (trusted platform and topology)
    - functions (trusted PSA)
    - service (PSA composition)
- **not only an application of NFV to personalized security**
- **contributing results on attestation and trust fabric to the NFV ISG SEC Working Group**

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.