POLITECNICO
DI TORINO

On the establishment of trust in the cloud-based ETSI NFV framework

IEEE NFV-SDN 2017 – SN workshop

November 6th 2017, Berlin

Authors

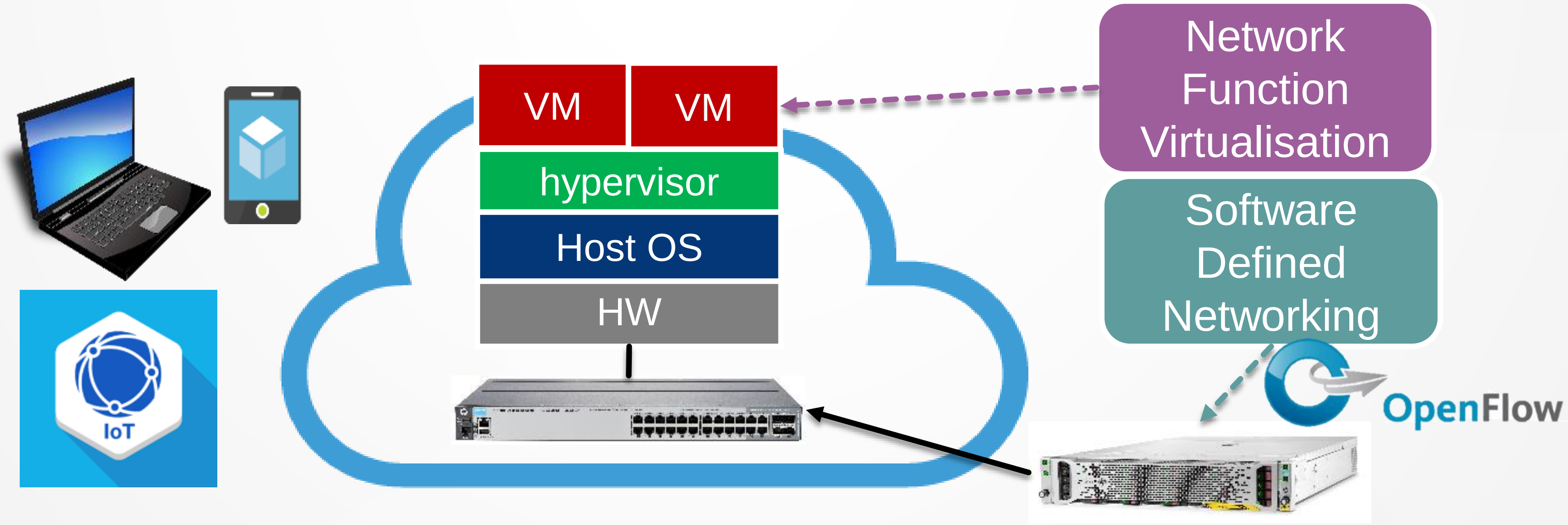
- **Marco De Benedictis** <*marco.debenedictis@polito.it*>
  - PhD Student
- **Antonio Lioy** <*lioy@polito.it*>
  - Full Professor
- **Politecnico di Torino** university in Italy
  - **TORSEC** *“Computer and Network Security Group”*

Outline

- ETSI standardisation on NFV security and trust
- An architectural proposal for assessing trust in a NFV cloud environment
- SHIELD project: leveraging big-data analytics for flexible security and trust in NFV
- Open issues and next steps
- Questions & Answers

Introduction

- Modern ICT infrastructures are evolving because of
  - **cloud** computing
  - **flexible** networking
  - **heterogenous** end-users
- High degree of **virtualisation** increases the attack surface



VM

VM

hypervisor

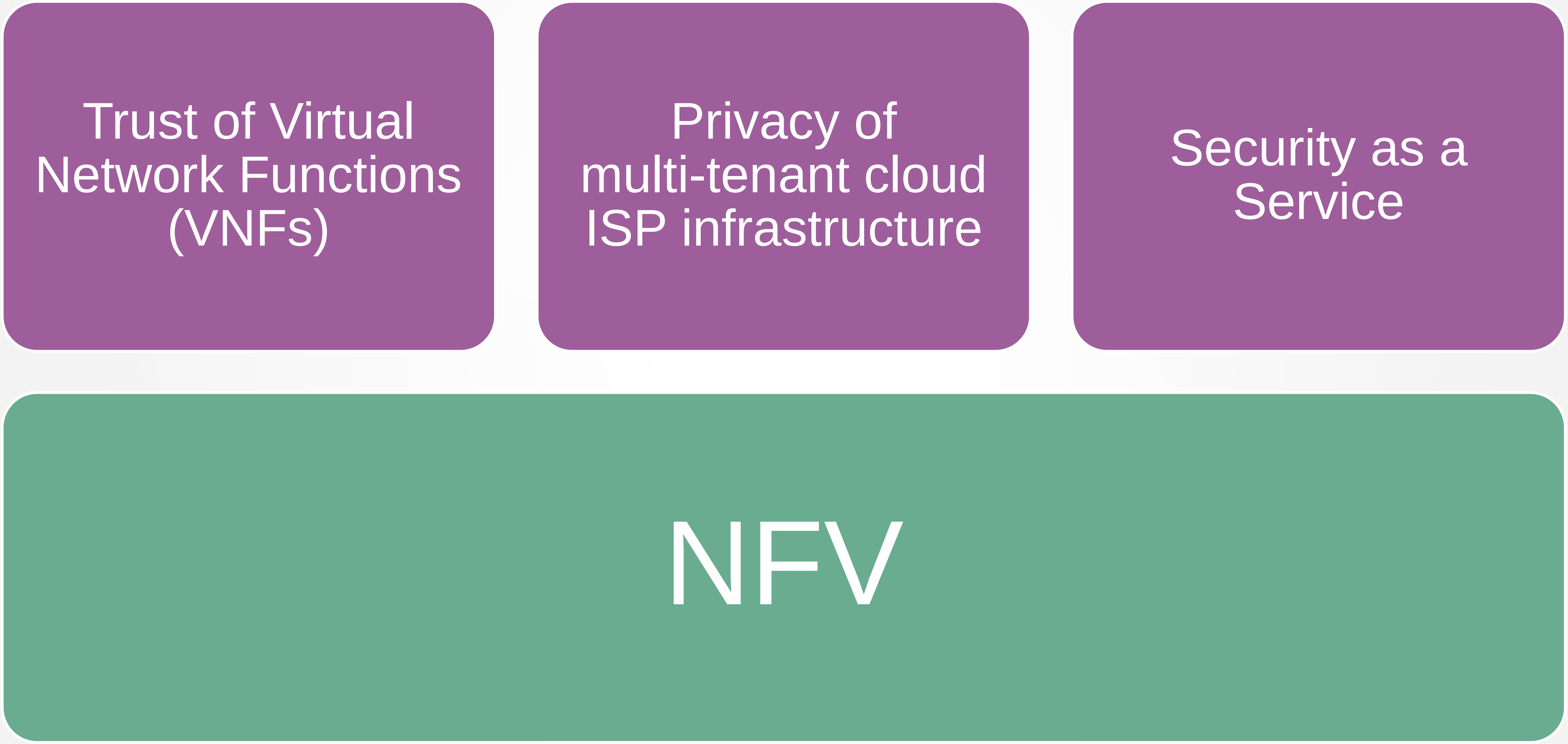
Host OS

HW

Network Function Virtualisation

Software Defined Networking

The focus on NFV security and trust



Trust of Virtual Network Functions (VNFs)

Privacy of multi-tenant cloud ISP infrastructure

Security as a Service

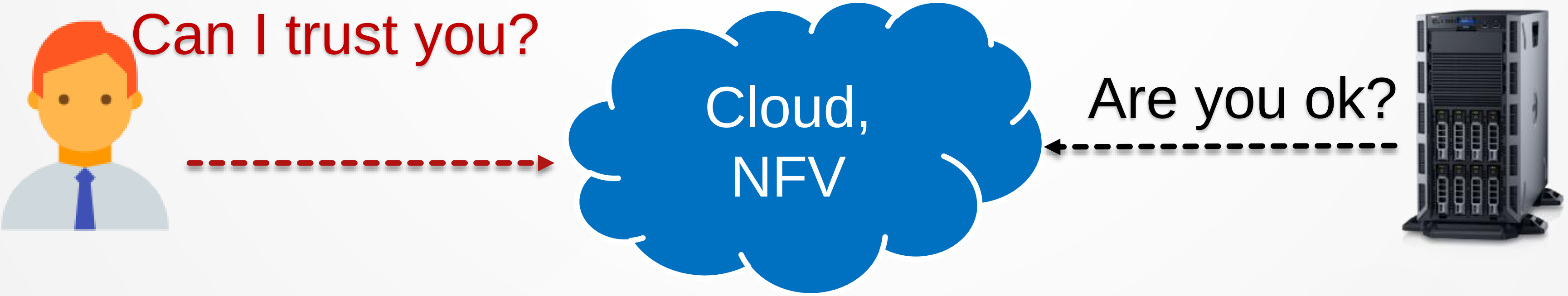
NFV

NFV standardisation activities

- *ETSI Industry Specification Group* founded in November 2012
- Defining the requirements and architecture for the NFV
- Over 60 publications up to this point
- 2-year phases
  - NFV Release 3 under way (2017-2018)
- **NFV SEC** Working Group focuses on **security** in NFV
  - analyse threats to security in virtualized environments
  - identify and specify best practices in security in NFV
  - investigate security enhancements for NFV

ETSI standardisation on trust in NFV

- Trust in a *Virtual Network Function* (VNF) derives from
  - VNF **package integrity** and provenance data
  - **Hypervisor** software **integrity** state
  - **VNF** Components software **integrity** state
- **Image** integrity check via digital signatures
- **Platform** integrity verification?
  - Trusted Computing as enabling technology

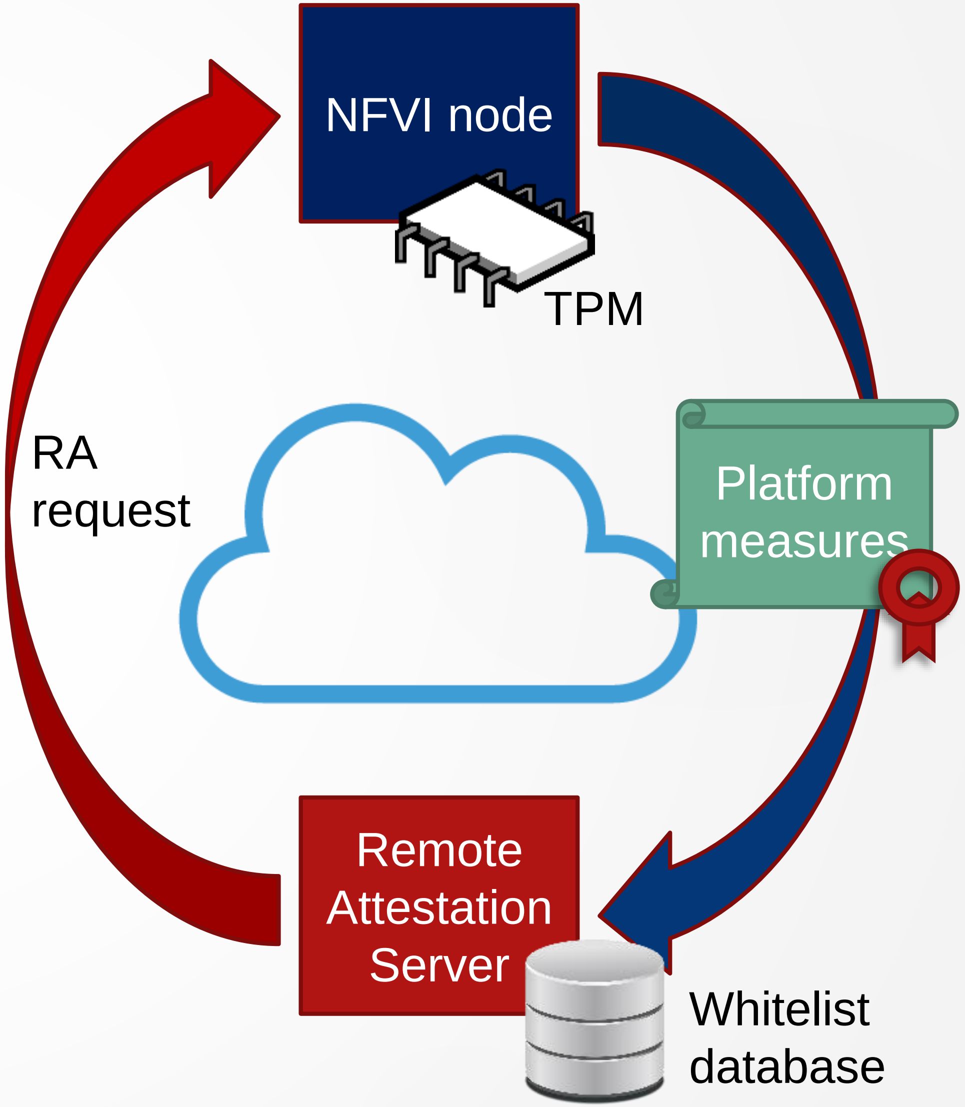


ETSI standardisation on trust in NFV

- Definition of **Trustworthy Boot**
  - encompasses technologies and methods for validation and assurance of boot integrity
    - Measured Boot
    - Secure Boot
    - Intel TBOOT
- **Trust Manager** to extend the NFV MANO administrative domain
  - centralised implementation of trust determination logic
  - interface between different administrative domains and operators
  - repository of trust around VNF packages and vendors

Trust assessment of the NFV infrastructure

- Definition of an architecture to assess the **trustworthiness** of a NFV Infrastructure (NFVI) node, based on **Trusted Computing**
  - **Remote Attestation** workflow to attest the platform integrity against a whitelist of known-good values
  - *Trusted Platform Module* (TPM) device to authenticate an hardware platform and collect its measurements (e.g. BIOS, OS, hypervisor, applications) via *Measured Boot*



Security of VNFs in the multi-tenant cloud NFV

- NFV environments leverage cloud management systems
  - physical resources **shared** among different tenants
  - **multi-tenancy** raises **privacy** issues
- Privacy may be addressed by
  - VNF image encryption
    - to ensure that VNF images cannot be accessed by non authorized users
  - secure (*and trusted*) onboarding of a VNF
    - via **digital signature/encryption** of VNF packages or images + Trusted Computing
    - to ensure that the underlying NFV Infrastructure has not been manipulated

Cloud attestation solutions for NFV

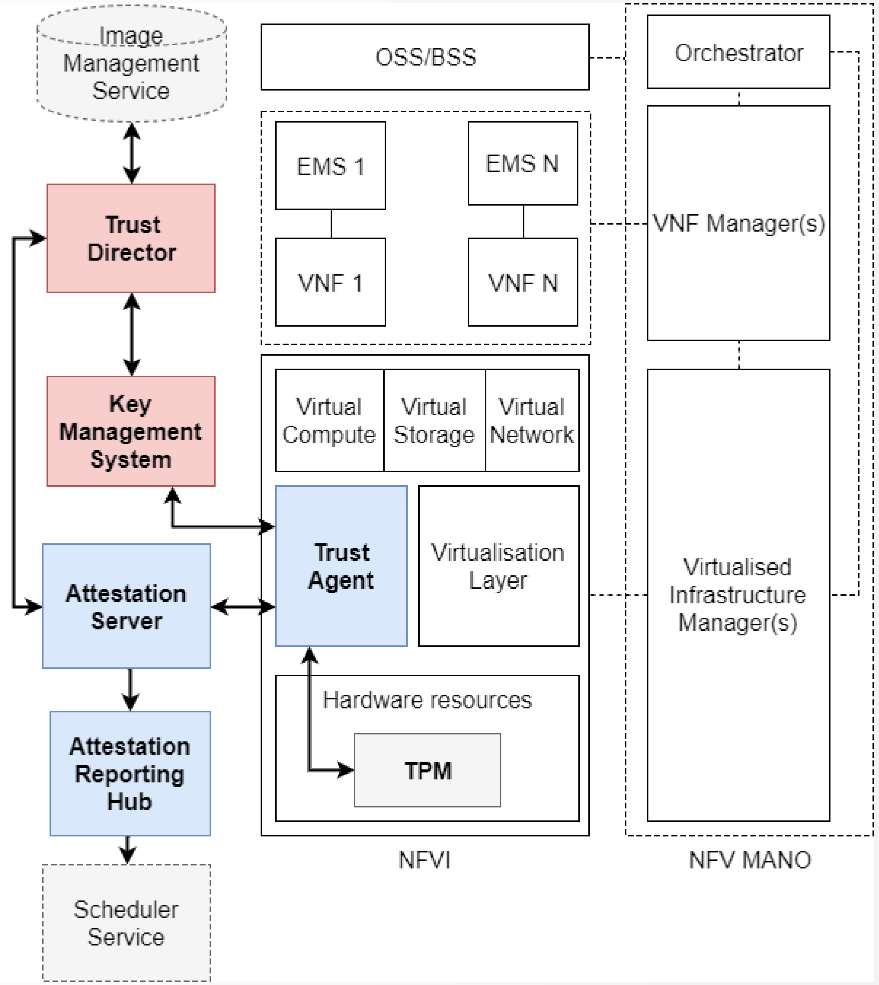
- Frameworks for **attestation** of cloud environments exist
  - Intel **OpenAttestation** (*now deprecated*)
  - Intel **Open Cloud Integrity Technology**
- Based on Trusted Computing
  - Intel *Trusted Execution Technology* (TXT)
- Focus on integrity verification of compute nodes
  - recent developments aim to **extend** trust to virtual instances
- Available solutions are not (*yet*) tailored for NFV lifecycle management

OpenAttestation

Open CIT

Extension of the NFV reference architecture

- Cloud attestation framework (**Open CIT**) as reference trust architecture
- Integrity verification of NFVI
  - **Trust Agent:** collects measurements from the NFV infrastructure nodes
  - **Attestation Server:** initiates the RA workflow
  - **Attestation Reporting Hub:** exposes attestation results to third-parties
- Secure and trusted onboarding of VNFs
  - **Key Management Service:** generates cryptographic keys
  - **Trust Director:** workflow manager



The SHIELD project

European Commission

Horizon 2020
European Union funding
for Research & Innovation

European R&D project

Co-funded by the EU under H2020 “Secure Societies” programme

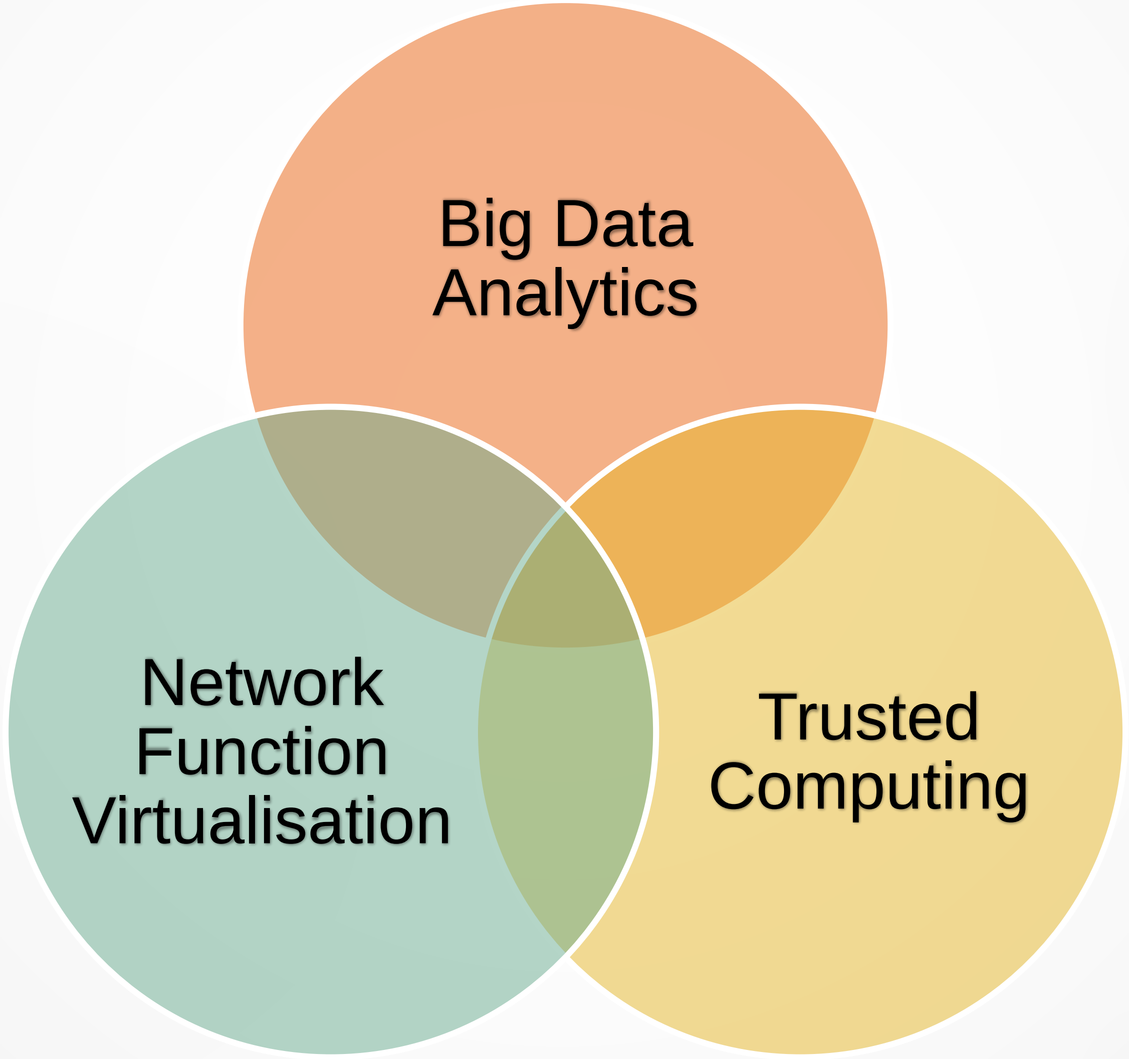
12 partners

4.56 M€ total budget

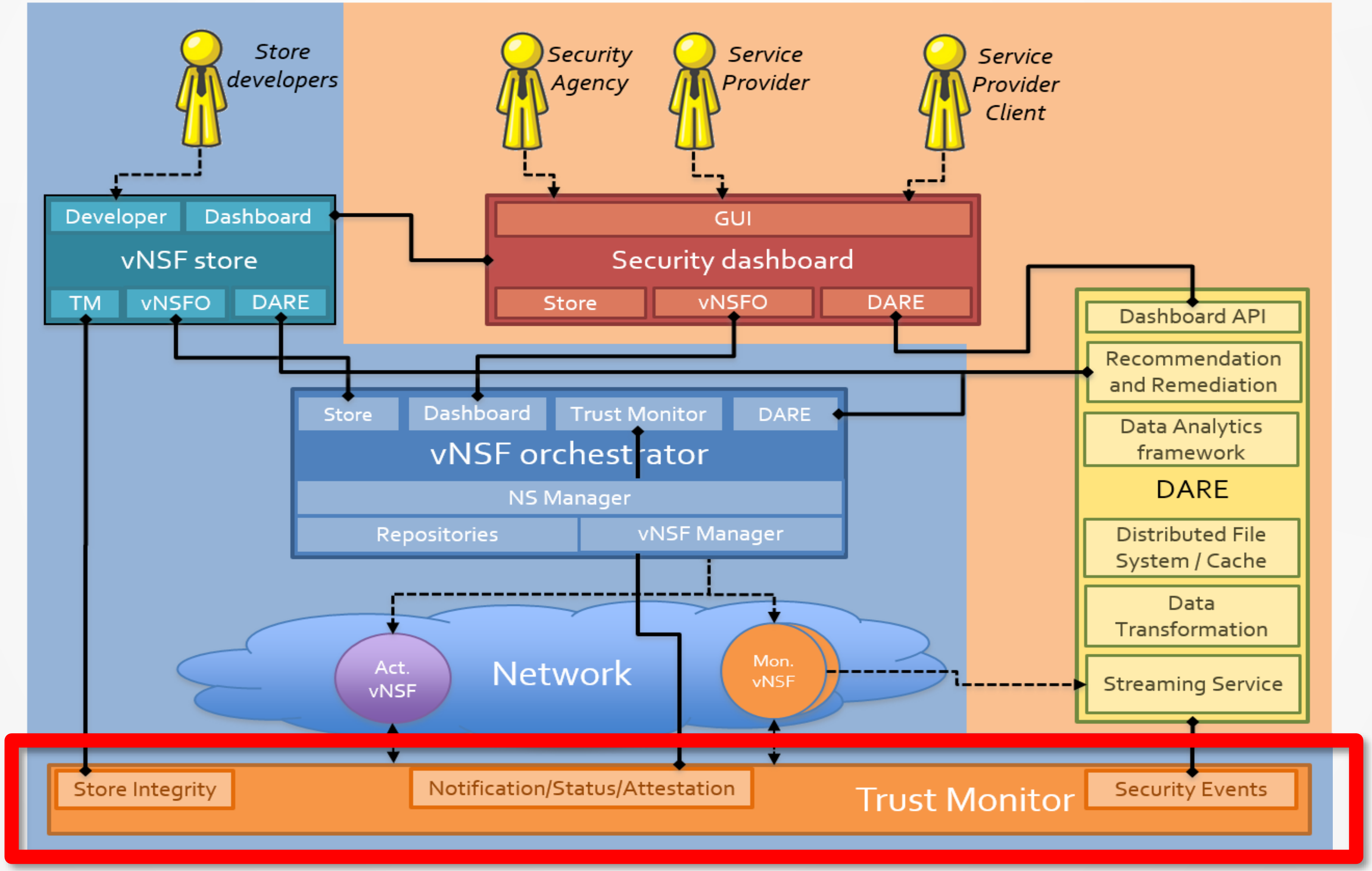
Duration: Sep 2016 – Feb 2019 (30 months)

SHIELD

The SHIELD concept



The SHIELD architecture



NFVI, vNSF attestation prototype

- Prototype based on **OpenAttestation** framework
- Attestation of a NFVI host based on CentOS 7
  - Whitelist of packages from distro repositories
- Attestation of **Docker**-based vNSFs
- *Integrity Measurement Architecture* (**IMA**)
  - run-time attestation based on a security policy
    - measure all executed binaries and scripts
    - measure all open files (read-only)
  - can detect misbehaviour in running NFVI nodes/vNSFs

Open issues and next steps

- Extension of Chain of Trust to VNFs based on different virtualisation techniques
- Application of novel **data protection** techniques to secure communication between nodes of a NFV environment
  - e.g. 802.1AE (**MACsec**) protocol for data link confidentiality and integrity
- Integration of a cloud attestation technology with a **reference** NFV framework

KVM

docker

OpenAttestation

Open CIT

Open Source MANO

POLITECNICO
DI TORINO

Thank you

marco.debenedictis@polito.it
marcoxdebenedictis
mrcdb