ENISA TELECOM SECURITY FORUM 2022
Whole System Security Challenges in Virtualised Networks

Alex Leadbeater CEng MIET, BT Plc (SECURITY)
Head of Global Obligations Futures & Standards
(BT Plc Security / Chair of ETSI TC CYBER)
29th June 2022

Context of Security Regulation and Standards

What is the purpose of National, EU or Global Security Regulation?

- Protect National, European or Global Citizens from defined threat, which the regulation aims to mitigate?
  - We must not loose sight of the fundamental purpose of security regulation through certification.

What is the purpose of Security Standards?

- Define a common minimum baseline level to address defined Security Threats / Risks.
- Security bar **must be achievable**, while adding value (current product security vs "needed" security delta).
- Must be possible to move the bar over time.

Security is a cost?

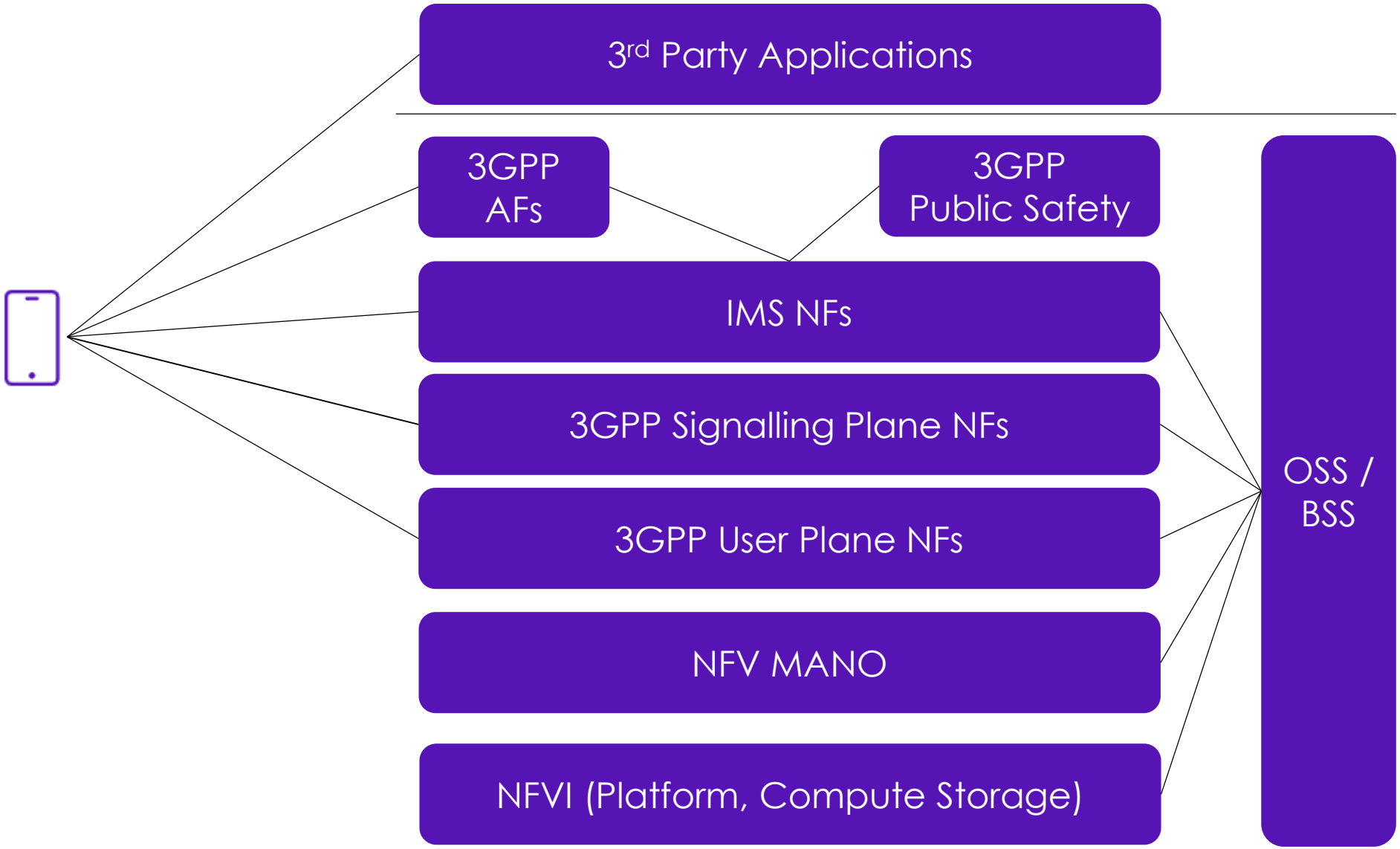
- Effective targeted Security Standards, Certification and Regulation reduce cost (e.g. financial or privacy).
- Security certification that does not mitigate intended threat / risk increases cost for little benefit.
- Multiple overlapping security mechanisms, requirements and certification obligations are inefficient.
  - End user, manufacturer or service provider rarely benefit.
  - Market agility and innovation reduced.

Overly prescriptive Regulation and Standards?

- Reduce end product market competition and security innovation?
- Barrier to market entry (including access to standards and standards creation).
- Inflexible regulation and standards are vulnerable to market or security threat landscape change.

Ultimately if the end service / product user does not receive the intended security or privacy benefit, then both regulation and security certification have failed.

“Simplified” 5G Security Layers – Multiple layers, Multiple Parties



Unwritten Legacy Security Constraints

NFV is fundamentally more secure than legacy systems if all ETSI NFV security standards and guidance are implemented. However;

Larger and more standardised attack surface responsible for larger security risks of NFV compared to legacy.

Establishing baseline security requirements for threats in NFV compared to legacy is challenging as many legacy network security approaches are not standardised.

Significant legacy security is via inherited corporate memory and varies CSP to CSP.

Physical hardware firewall legacy approaches mask many of the security risks in legacy deployments.

- NFV removes the edge, so all NFV components and protocols must be secure by default.

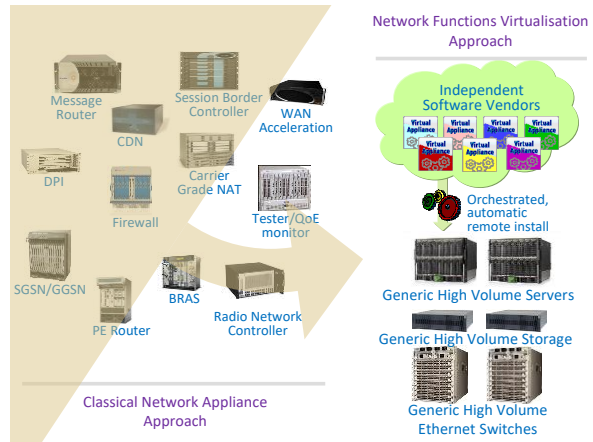
Many current Security standard approaches are not fully cloud native.

- Focus still on "link security", rather than whole platform security.

- Threat models have not fully evolved.

Strong NFV Security still highly reliant on physical host separation.

- Breakout containment and privilege escalation.

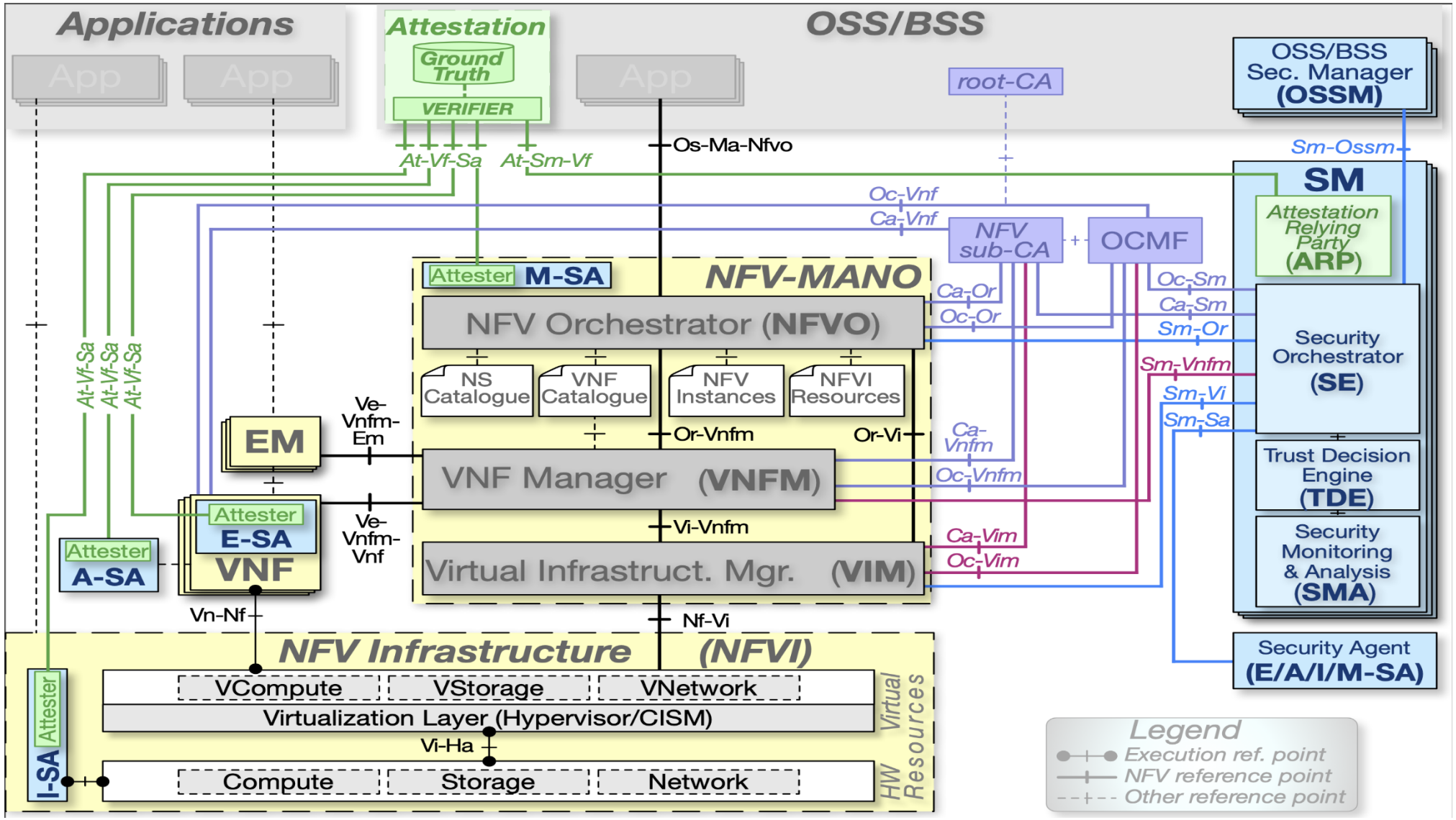


Why is Virtualised Security Hard? (Virtual Systems have more Security)

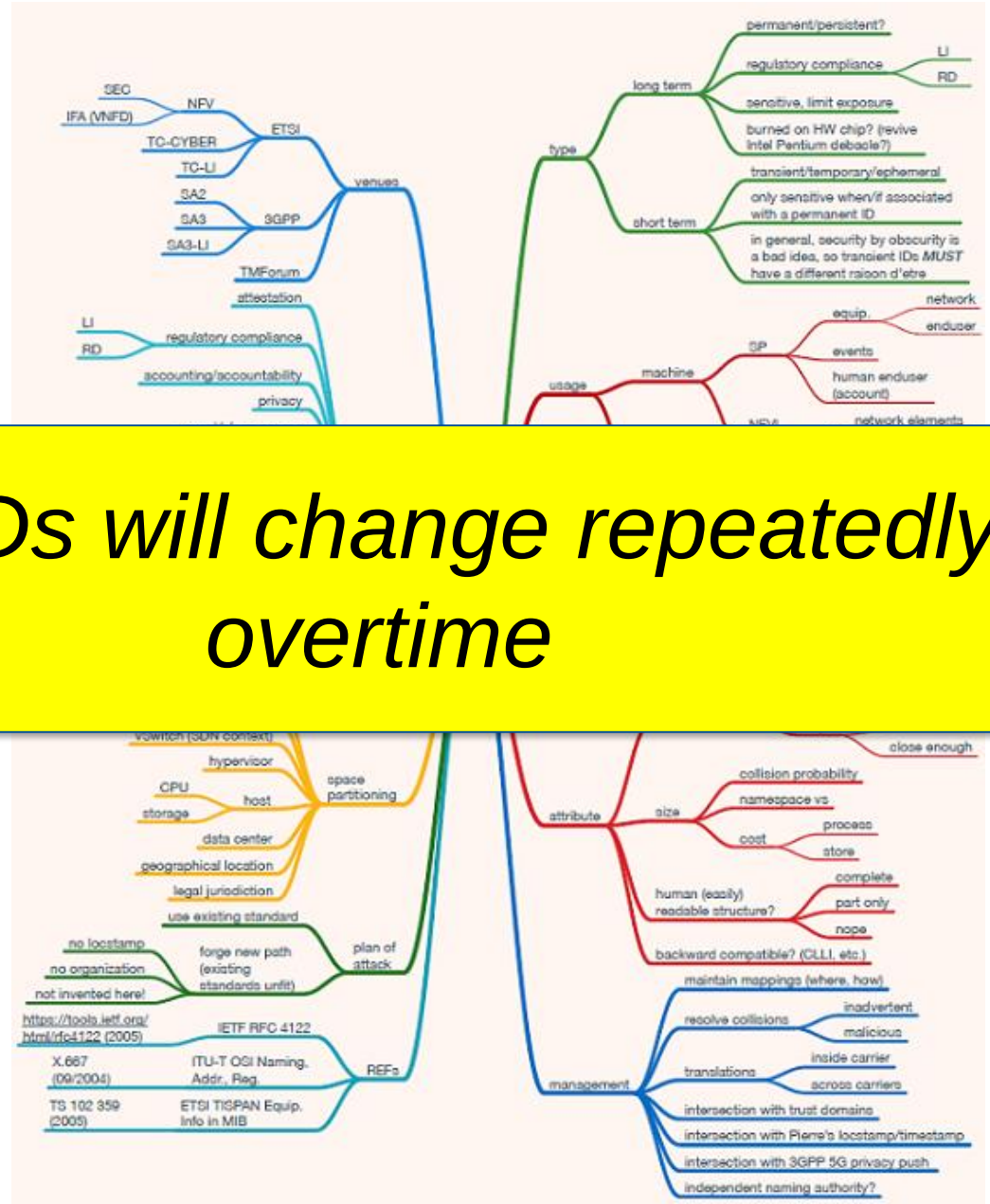
- Isolation
- Common Software Environment
- Data Location and Lifecycle
- Memory Introspection
- Test Isolation
- Defining Sensitive Functions
- Single Admin Domain
- Protecting Keys
- Function Location Assurance
- Full Attestation (Boot & Runtime)

- Physical Host Access
- VNF Host Spanning
- Encrypted Data Processing
- Limited vs Full virtualisation
- Mixed Virtual & legacy PNF Deployments
- Software Catalogue Image Exposure
- Startup Security Paradox
- Time Manipulation
- 3rd Party Hosting
- VM / Hypervisor Breakout
- IP vs App Layer Security

Whole System Attestation – ETSI ISG NFV



Identity Management in NFV – One ID becomes many



The IDs will change repeatedly overtime

Location in a Virtualised Network: Infrastructure

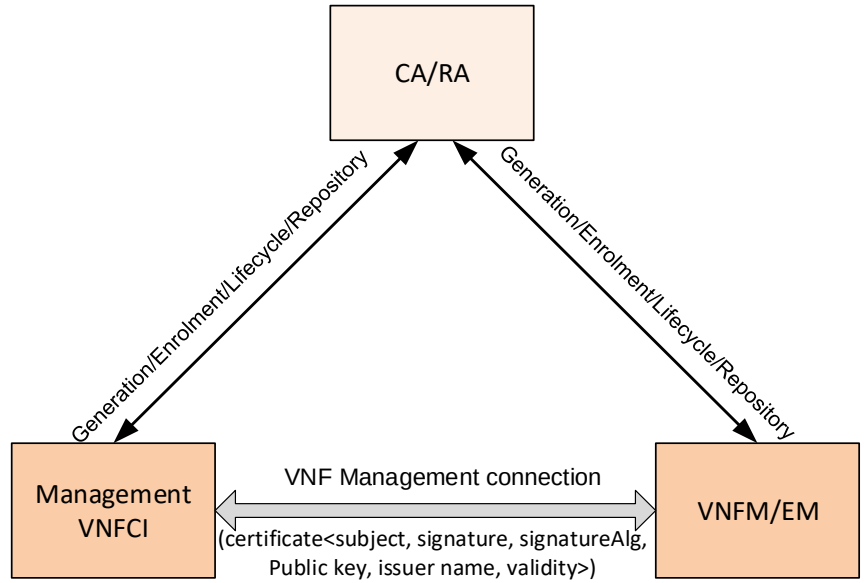
- Do you need to know the actual location of components for security or licensing reasons?
  - Virtual Machines and containers do not have a concept of physical location.
  - Not a default cloud service capability.
- Using standard commercial servers
  - Requires specific location aware hardware.
  - Requires major changes to open source software.
  - New platform Firmware and Chipset capabilities to implement securely.
- Likely sufficient for NFV MANO to attest VNFs are running as per placement rules.
  - In a specific data centre or group of host servers.
- Will need to control multiple groups of VNFs
  - Security critical VNF and supporting non critical VNFs.
- Is there a need to Retain the “location” for security purposes.
  - Very difficult if network changes 100s of times a minute.

Secure Time in NFV

- Virtual Functions can’t tell the time.
  - Reliant on host and hypervisor.
  - VMs and containers can be paused.
  - Time can be slowed or sped up.
- Security relies on accurate time for correlation and forensic integrity.
- Time of What? and Where?
  - Large VNFs may be spread over multiple hosts and locations.
- New solutions required
  - Hardware attestation at VM level.
  - External time sources (eg GNSS / GPS)
- ETSI ISG NFV 016 Report on location, timestamping of VNFs

Certificates, Certificates everywhere but are they secure?

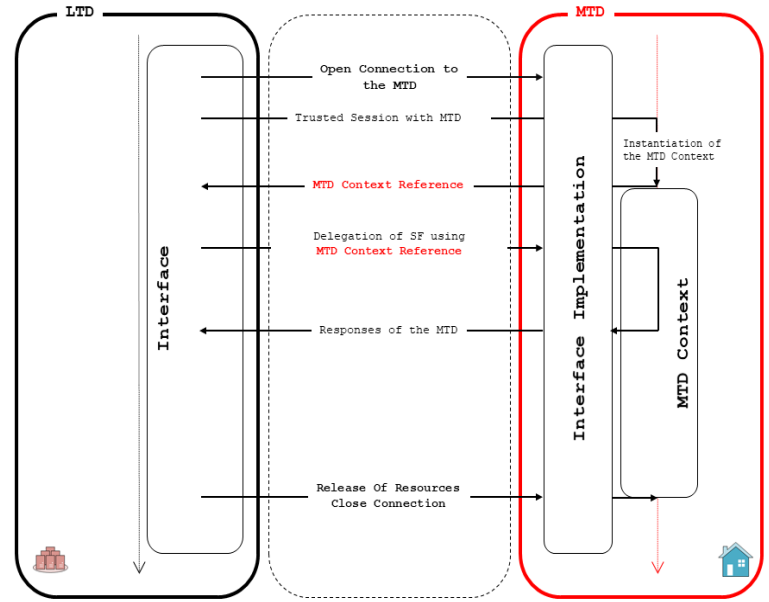
- NFV is heavily reliant on PKI techniques for security at all layers.
  - Application layer Identity and Communication certificates.
  - VNF Image Certificates (Operator and Vendor).
    - Artefact Certificates within Images.
  - VNFI Identity Certificates.
    - VNFCI Certificates within each VNFI.
  - Inter and Intra VNFI Communication Certificates.
  - NFVI Certificates.
  - MANO Certificates.
  - OSS / BSS Certificates.
  - 3rd Party Vendor Management Certificates.



- Each VNF may require 100s of certificates for different roles.
- All of these need to be stored, accessed, and deleted securely.
  - Certificate Revocation and update a major challenge.
- Is this practical in real world implementations?

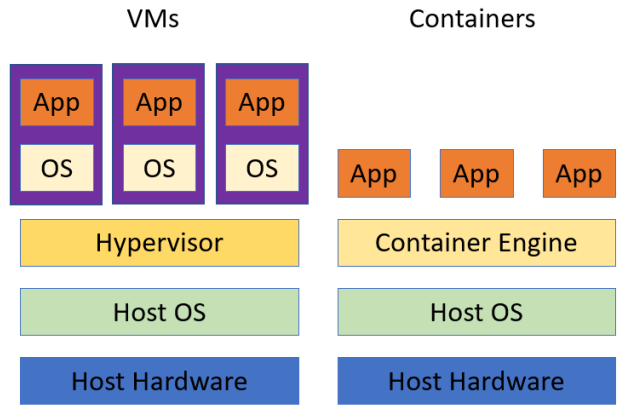
When you can’t secure Sensitive Functions, offload to a trusted domain?

- Sometimes it is not always possible to fully secure an NFV environment, sufficient to run sensitive functions.
  - What now?
- Offload the sensitive function to a trusted domain
- ETSI TS 103 457
  - How to run sensitive code in an otherwise limited security virtualised environment.
  - Uses a More Trusted Domain (MTD) to offload specific sensitive components or functionality for execution.
    - Limited security can include aspects such as lack of entropy.



Then along came containers……

- Implementing virtualised networks securely is difficult enough in a VM world
- Containers make matters worse.
  - Future of NFV / Cloud deployments
  - No native memory isolation and breakout protection
  - Very fast spawn and termination rates
  - Off function / DPI interception essentially impossible.
- Cannot secure containers across multiple trust domains with running them within VMs.
  - Container Security lacking and trailing push for deployment.
- Examples include Docker and Kubernetes.
- No Hyperviser or VM layer equivalent OS
  - Fast “boot times”.



NEPHIO – Linux Foundation (Next Generation Virtualisation Instantiation)

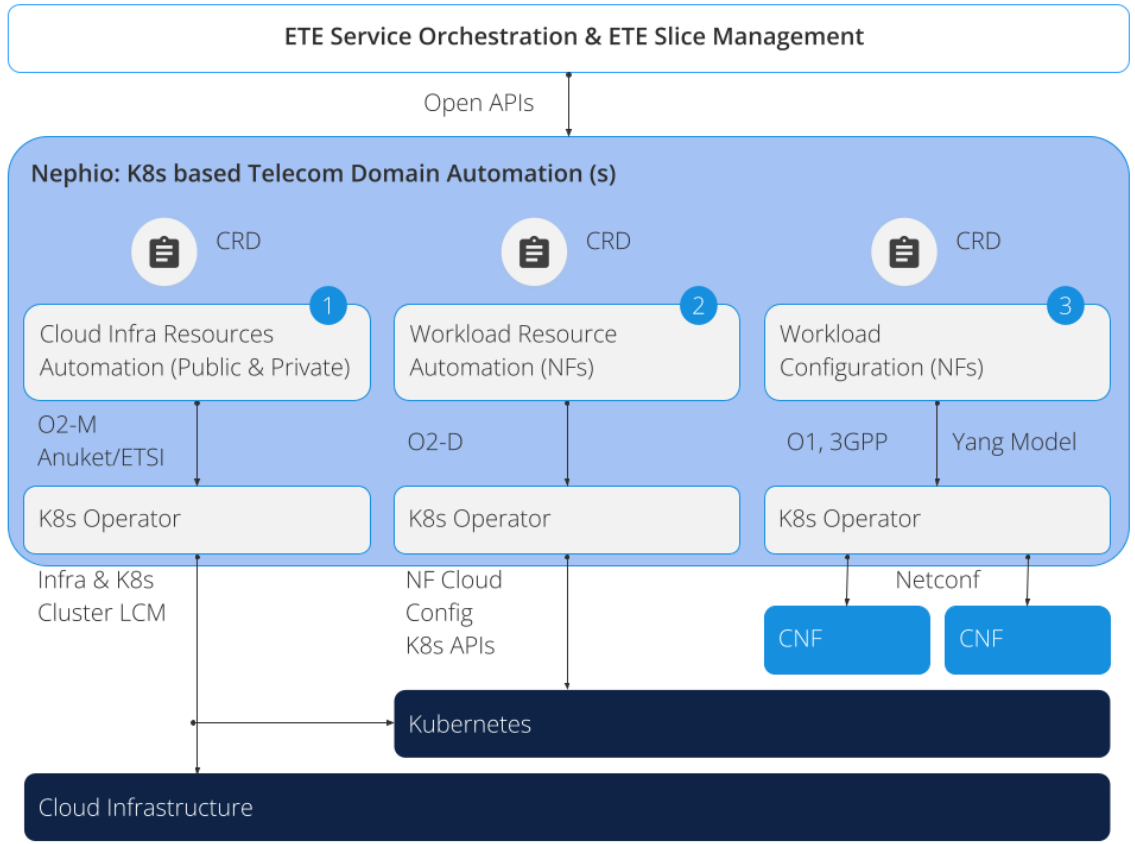
Nephio is a Kubernetes-based intent-driven automation of network functions and the underlying infrastructure that supports those functions.

It allows users to express intent, and provides declarative automation.

Much more abstract than ETSI NFV orchestration.

Current secure virtualisation approaches not fully aligned with Nephio approach.

Doesn't have the overall "telecom context awareness" of NFV MANO.



Further ETSI Cyber Security Information

ETSI's website:
www.etsi.org

TC CYBER:
www.etsi.org/technologies-clusters/technologies/cyber-security

ISG NFV:
https://www.etsi.org/technologies/nfv

ISG SAI:

https://www.etsi.org/technologies/securing-artificial-intelligence

ETSI Security Week 2022: 3rd to 5th October 2022

https://www.etsi.org/events/2068-etsi-security-conference