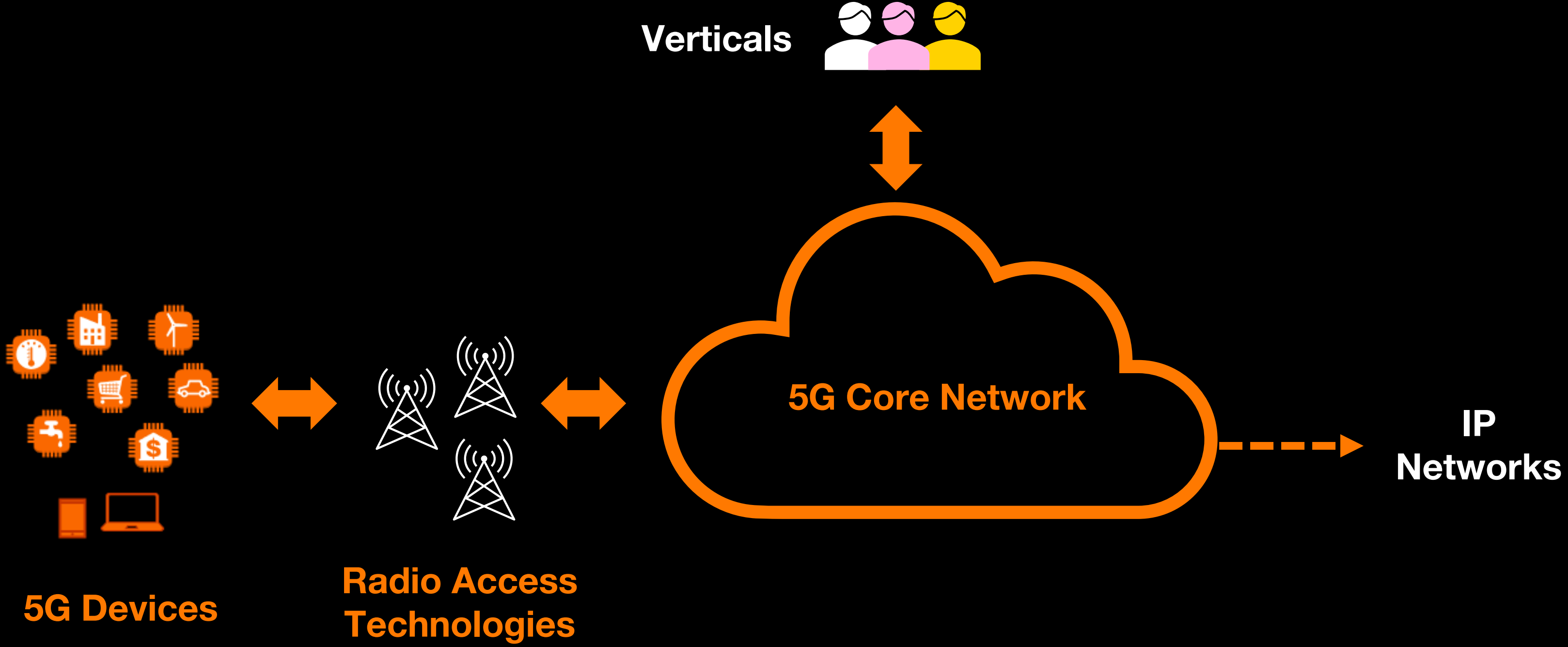
Attestation for Mobile Network

By Orange

Ghada Arfaoui, Security Research Engineer
Orange Innovation, France

March 27, 2024

Mobile Network Architecture



Verticals

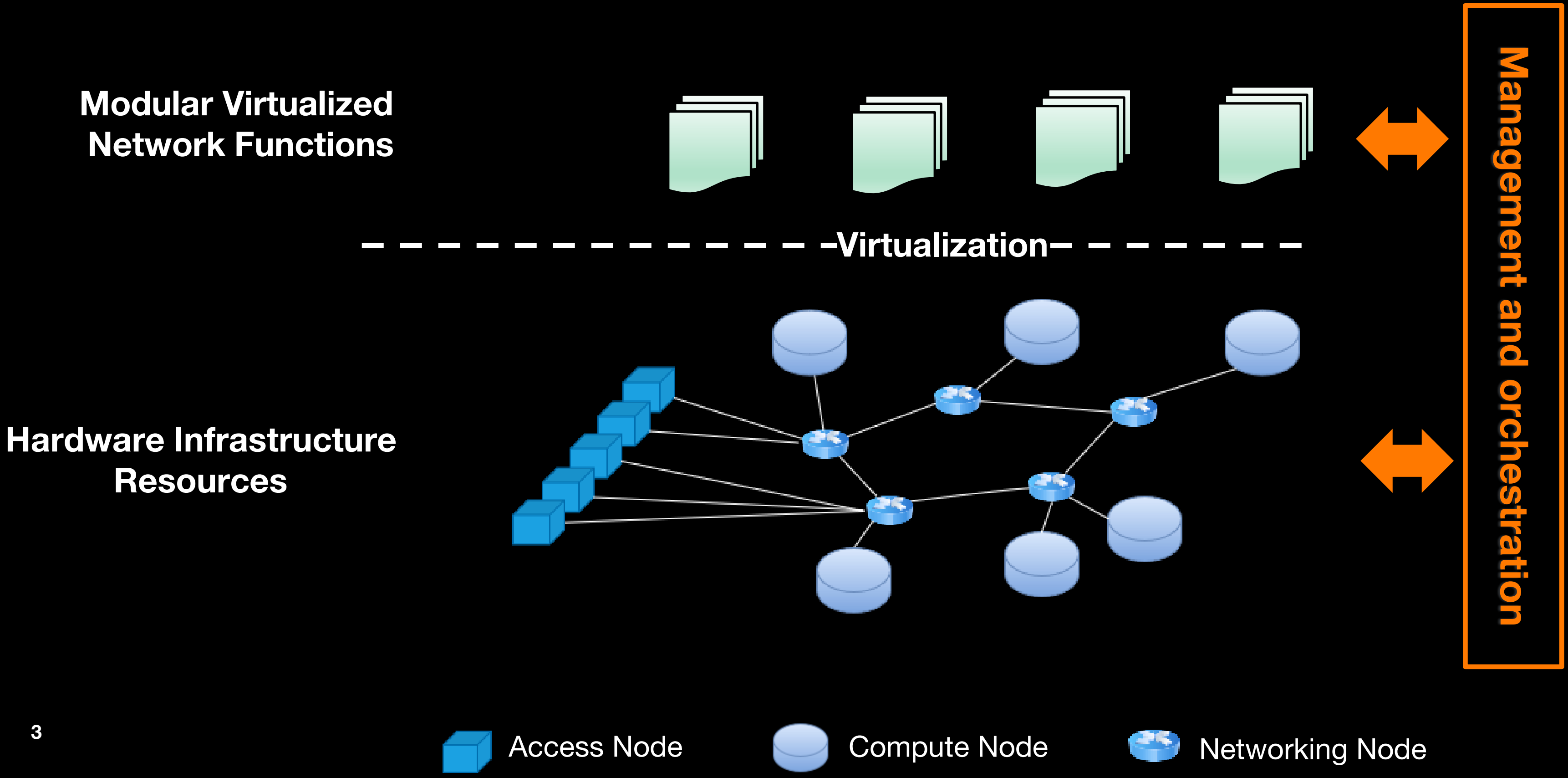
5G Core Network

IP Networks

5G Devices

Radio Access Technologies

5G Core Network



Modular Virtualized Network Functions

Virtualization

Hardware Infrastructure Resources

Management and orchestration

Access Node

Compute Node

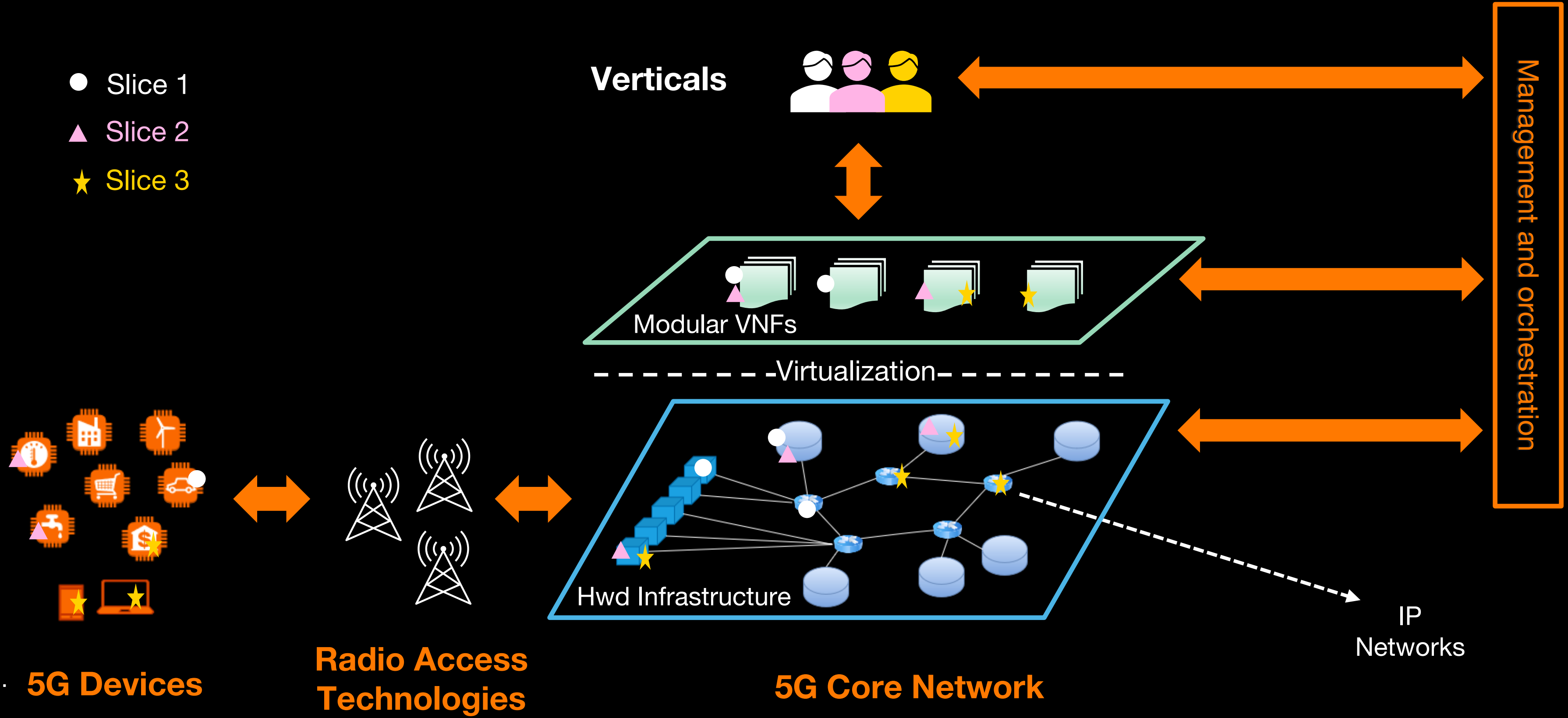
Networking Node

Mobile Network Architecture

● Slice 1

▲ Slice 2

★ Slice 3



Verticals

Management and orchestration

Modular VNFs

Virtualization

Hwd Infrastructure

IP Networks

5G Devices

Radio Access Technologies

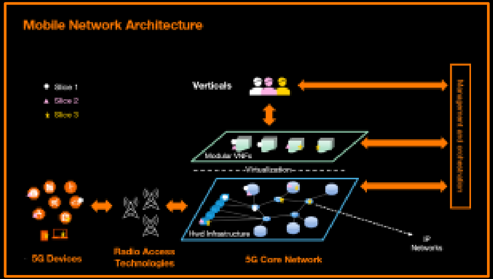
5G Core Network

Attestation: Why?

New Networks

New Ecosystem

New Trust Model



Security Challenges

Sovereignity

Measureable
Trust & Security

Stakeholder
Responsibility

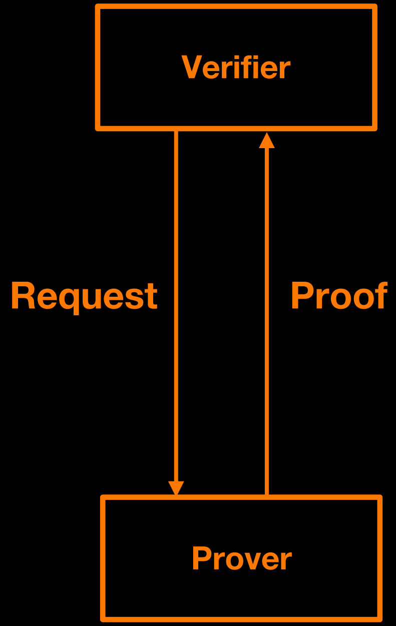
Attestation Protocol: what is it?

- **A cryptographic protocol (Challenge - Response)**

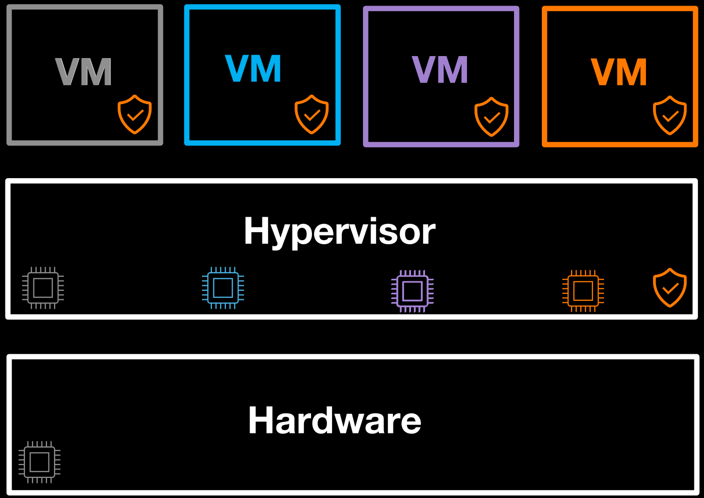
- **2 parties:**
  - Prover: Network node, a group of Network nodes
  - Verifier: Attestation Server / a Vertical

- **Objective:**

Prove one or multiple properties (e.g., integrity, location, PoT)



Deep Attestation



- Infrastructure boot integrity
  - ✓ VMs integrity
  - ✓ Hypervisor integrity

- Layer binding
  - ✓ VMs are running on top of the designated hypervisor.

🛡 An Attestation Agent

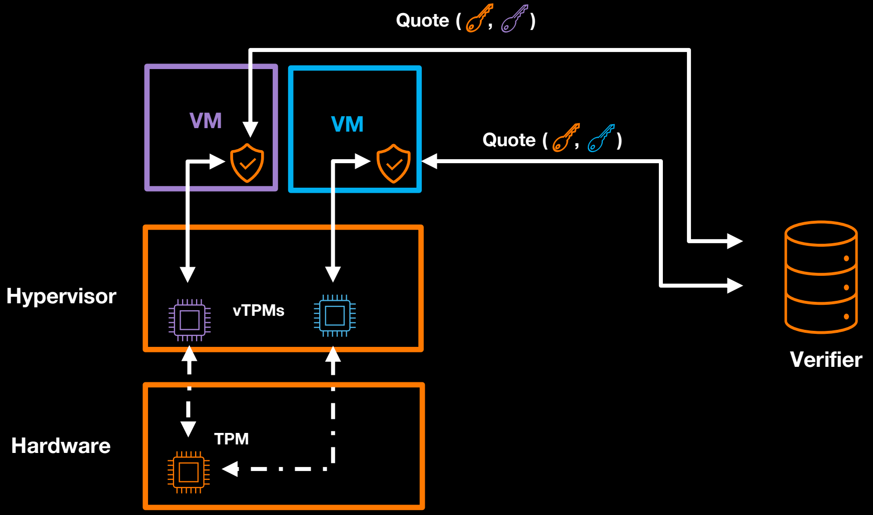
▣ A root of Trust

Deep Attestation: ETSI approaches

Single Channel

Multiple Channel

Enhanced Multiple Channel



- ☺ Infrastructure integrity
  - ✓ VMs integrity
  - ✓ Hypervisor integrity
- ☺ Layer binding
- ☹ Efficiency
- ☹ Scalability

An Attestation Agent

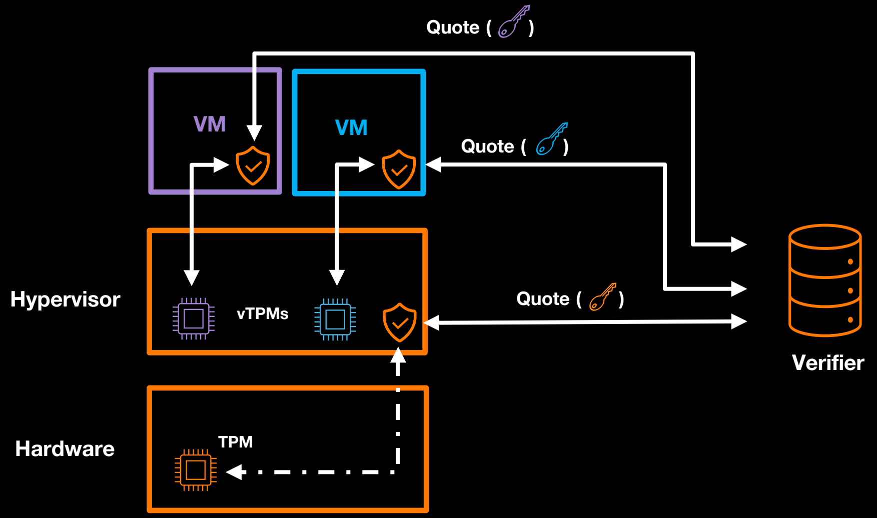
A root of Trust

Deep Attestation: ETSI approaches

Multiple Channel

Single Channel

Enhanced Multiple Channel



☺ Infrastructure integrity
- ✓ VMs integrity
- ✓ Hypervisor integrity

☹ Layer binding

☺ Efficiency

☺ Scalability

An Attestation Agent

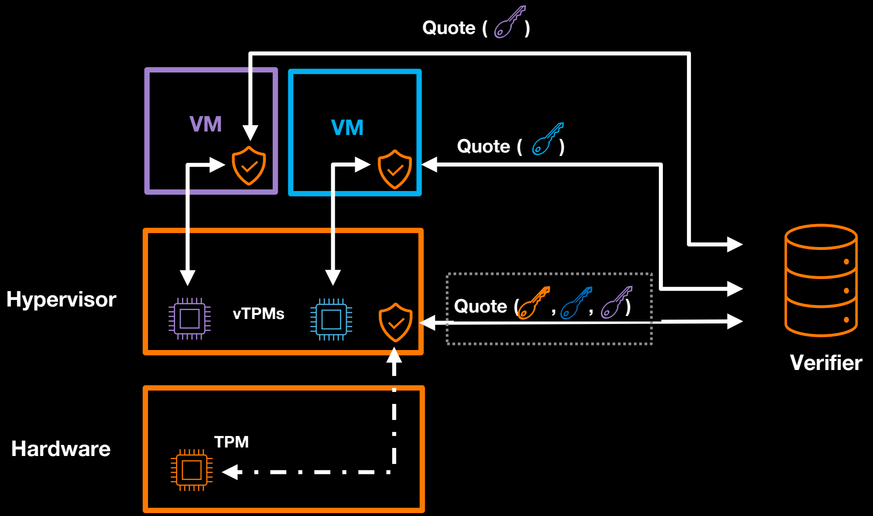
A root of Trust

Deep Attestation « revisitée » by Orange

Enhanced Multiple Channel

Single Channel

Multiple Channel

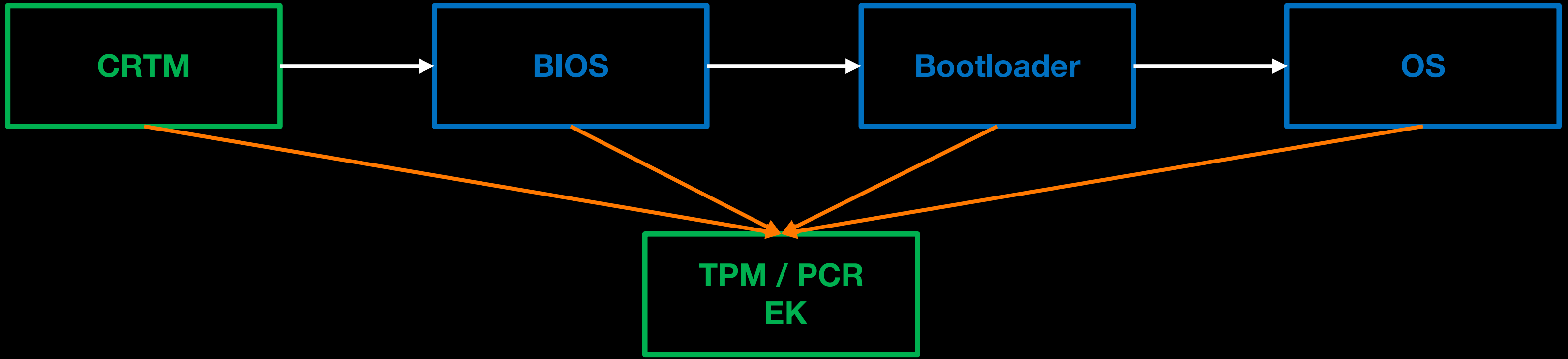


- 😊 Infrastructure integrity
  - ✓ VMs integrity
  - ✓ Hypervisor integrity
- 😊 Layer binding
- 😊 Efficiency
- 😊 Scalability

🛡 An Attestation Agent

▣ A root of Trust

TPM Attestation



→ **Measure:**

$$M = \text{Hash}(X)$$

→ **Extend:**

$$PCR_{new} = \text{Hash}(M \,||\, PCR_{old})$$

Attestation Quote

Sign (AK, PCR, nonce)

CRTM: Core Root of Trust of Measurement
PCR: Platform Configuration Register
EK: Endorsement Key
AK / AIK: Attestation Identity Key

Deep Attestation: a new quote

Intuition:

The hypervisor has access to vEKs of vTPMs. It will then securely append to its attestation a list of public keys {vEK} corresponding to the VMs physically hosted on the same device.

Hypervisor Attestation: Quote (🔑, 🔑, 🔑)

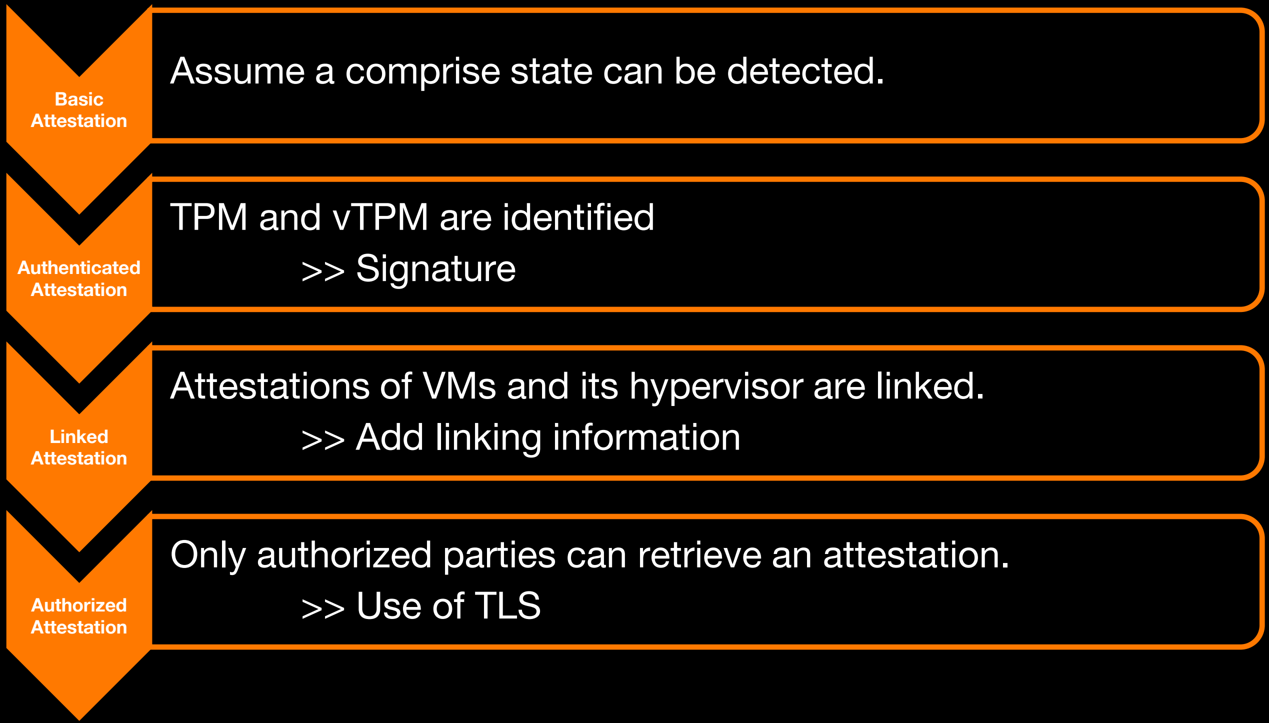
Sign (AIK, PCRs, Hash(nonce || {vEK, vEK})), {vEK, vEK}

VM Attestation: Quote (🔑)

Sign (vAIK, vPCRs, Hash(nonce || vEK)), vEK

First security model

- ✓ **Computational model**
- ✓ **Security game-based proofs**
- ✓ **Composite security**



Assume a comprise state can be detected.

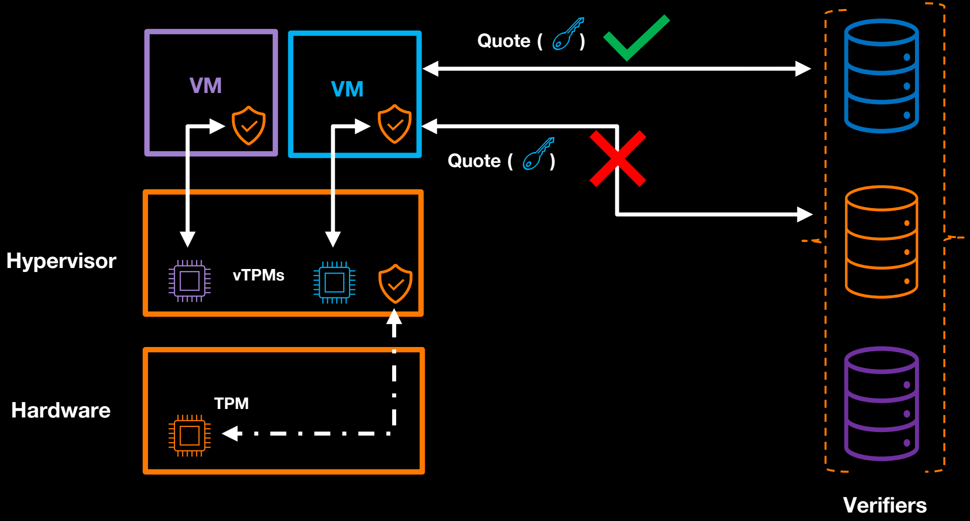
TPM and vTPM are identified
>> Signature

Attestations of VMs and its hypervisor are linked.
>> Add linking information

Only authorized parties can retrieve an attestation.
>> Use of TLS

Multi-tenant Environments Challenges

What if we apply our approach?



☹ **Security issues**

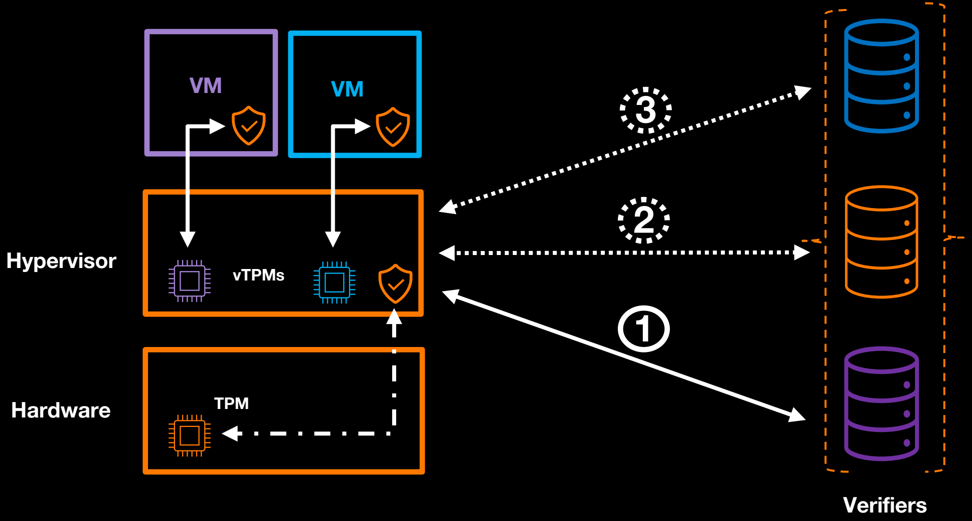
☹ **Privacy issues**

➡ **A VM must answer only to its associated verifier.**

🛡 An Attestation Agent

▣ A root of Trust

Multi-tenant Environments Challenges



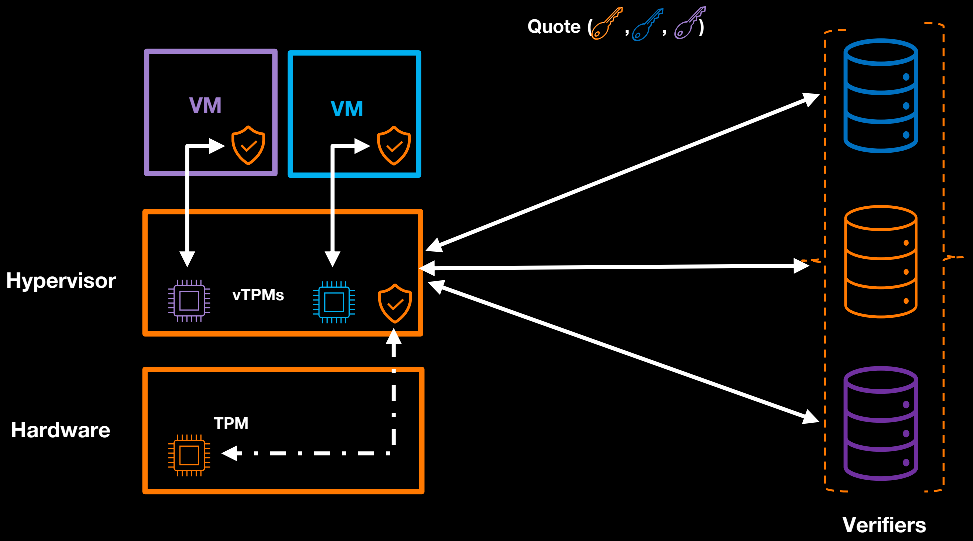
☹ Performance

➡ Batching the challenges and providing one attestation for all verifiers

An Attestation Agent

A root of Trust

Multi-tenant Environments Challenges



☹ Privacy issues

- Public keys
- Configuration

➡ Vector commitments

➡ ZK SNARKs

An Attestation Agent

A root of Trust

Our Attestation in Multi-tenant Environments

Strong privacy properties

- ✓ Responder Hiding AKE: a VM answers only its associated verifier.
- ✓ Inter-tenant privacy: a tenant can learn nothing about other tenants.
- ✓ Configuration hiding: a hypervisor proves that its configuration /state belongs to a set of valid states.

Performance

- ✓ Batching the challenges
- ✓ No TPM modification

Provable security

- ✓ Computational model
- ✓ Security game-based proofs

Next

- Collective deep attestation (submitted paper at PETS 2024)
- Other properties
- Other virtualization architectures
- Other Execution environments
- Other RoT

Conclusion: Attestation a powerful tool for continuous security

INTERNET OF TRUST

Ensuring continuity and dynamism in certification: the imperative need in the context of evolving European cybersecurity regulations

Mohamad Hajj – Internet of Trust

Attestation and its Applications Workshop - November 15, 2023

© Internet of Trust   Attestation and its Applications Workshop   1 of 25

Intel Trust Authority

Haidong Xia
Principle engineer @Intel

"An example of on demand SLA"

Jean-Philippe Wary / Orange Innovation

Orange Atalante – November 15th, 2023

CISCO SECURE

The bridge to possible

Attestations for Trusted Path Routing

Nancy Cam-Winget, Cisco Fellow
Cisco Systems, Security Business Group Office of the CTO

November 14, 2023

Attestation and its Applications Workshop, November 2023
https://crypto.orange-labs.fr/acg/workshop/workshop.php

Milestones

ACNS 2022 : A Cryptographic View of Deep-Attestation, or How to Do Provably-Secure Layer-Linking.

ESORICS 2023: Towards a Privacy-Preserving Attestation for Virtualized Networks.

- Practical and Privacy-Preserving Collective Remote Attestation for NFV (Recently submitted).

An open-source solution

Acknowledgements

- This work has been done in collaboration with Thibaut Jacques and Cristina Onete.
- H2020 INSPIRE5G+ project (EU funding)
- ANR MobiS5 project (French funding)

Thanks