



**CONFIDENTIAL
COMPUTING
SUMMIT 2024**



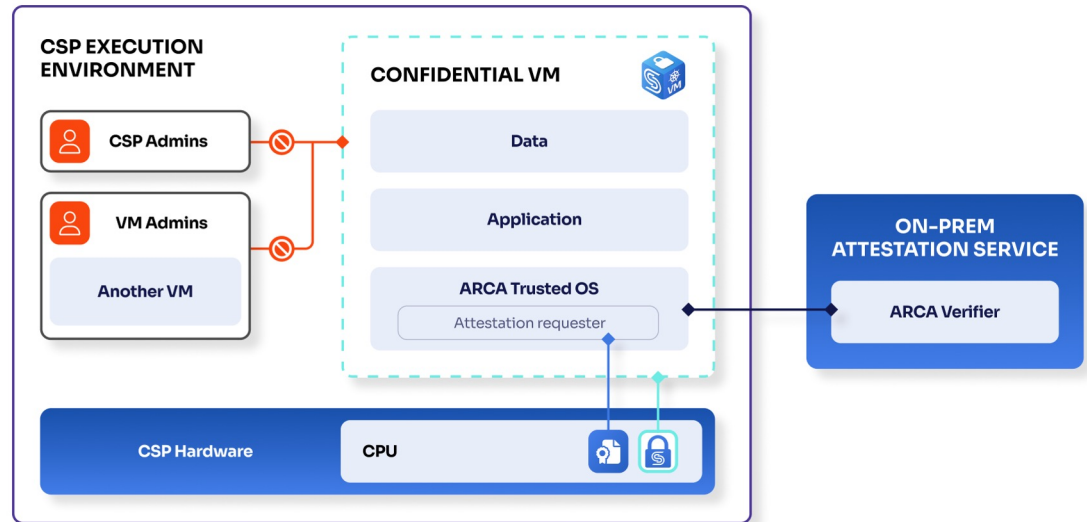
A confidential computing-based hosted private cloud for the Italian administration

Matthieu LEGRE

VP product, CYSEC SA

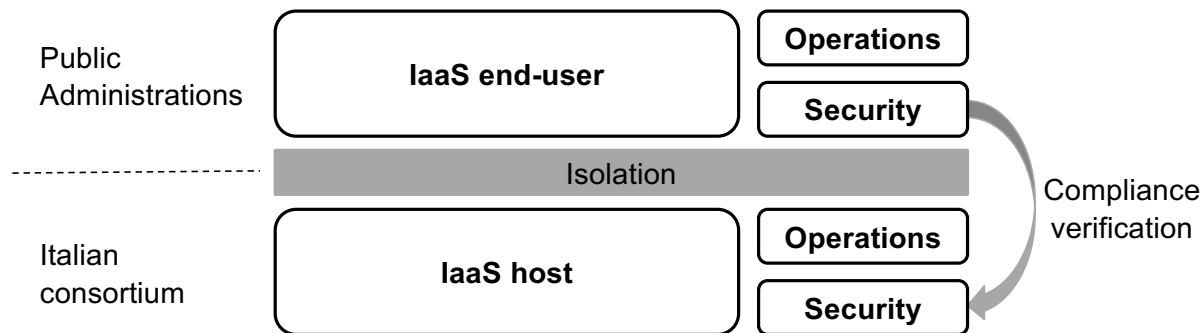
Overview of CYSEC: Expertise and Presence

- **Founded in 2018**
- **A team of +35**
- **Offices in Switzerland, France & Italy**
- **3 Lines of Products**
 - ARCA Trusted OS
 - ARCA Satlink
 - ARCA Satcom
- **Active in the following industries**

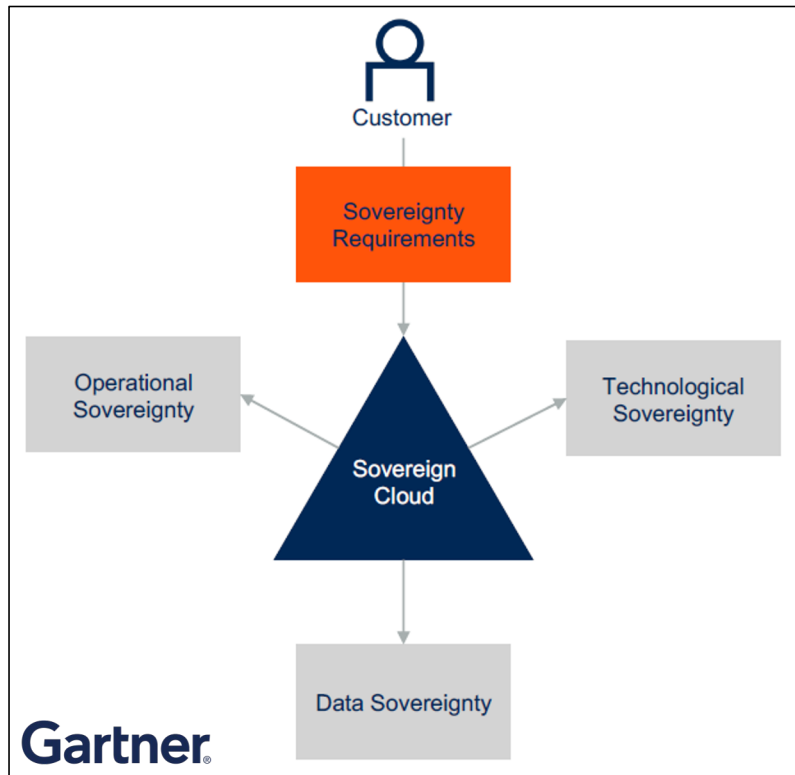


Italian Cloud Strategy: a Secure Infrastructure for Public Administrations

- 75% of Italian public administrations migrate to a cloud environment
- Hosted private cloud is one approach



Sovereign cloud: how confidential computing can help?



- Data Sovereignty
 - protection of data in-use
- Operational Sovereignty
 - attestation of VM launches
 - continuous auditing of VM instance configuration
- Technological Sovereignty

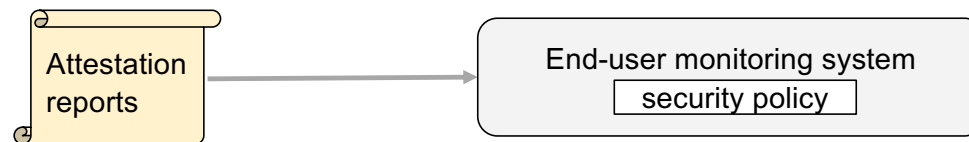
Operational Sovereignty: Attested VM launch and Continuous Auditing Needs

- Attestation of VM launches (at boot time)



→ **Authentication of a trustworthy node in a third-party IaaS by the cloud user at boot time.**

- Continuous auditing of VM instances (at run time)



→ **Technical verification of the compliance with the legal agreement between the cloud host and the cloud user**

ARCA Trusted OS: Security Features in Non-Confidential VMs

ARCA Trusted OS as guest OS

- Micro Distribution
- Immutable filesystem
- Full disk encryption of user space
- RoT OVMF & v-TPM
- Secure Boot
- 'pass or abort' boot approach

Cloud host

- CPU
- OVMF
- v-TPM

Trusted elements

CYSEC Solutions: Ensuring Confidential VM Security

CYSEC verifier (on prem)

attestation report verification

encryption key delivery

security policy definition

security event generation

ARCA Trusted OS as guest OS

Micro Distribution

Immutable filesystem

Full disk encryption

RoT Secure processor

Secure Boot

pass or abort

attestation report requester

Cloud host

CPU

patched OVMF with hardcoded SB key

CC

secure processor

data confidentiality protection

OVMF integrity verification

attestation reports

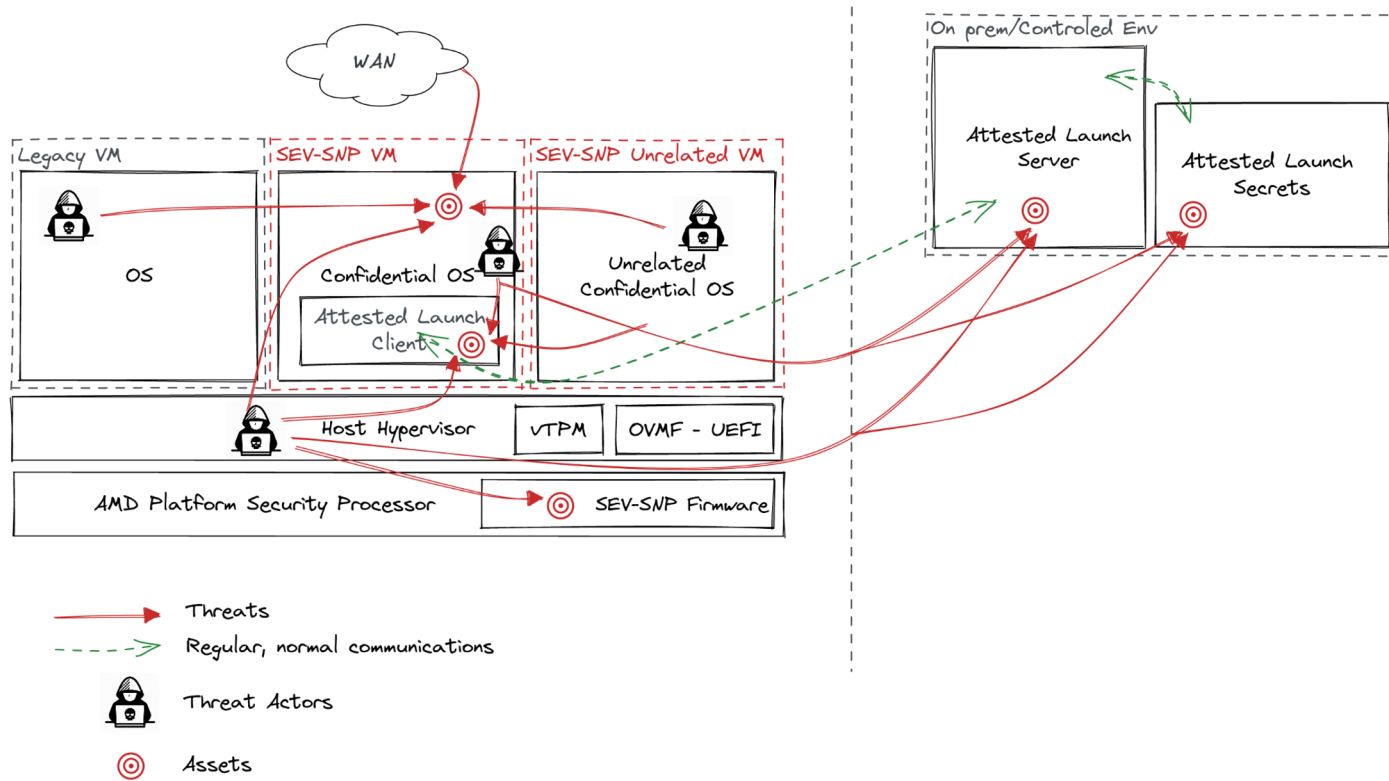
Attestation of VM launches

VM instances auditing

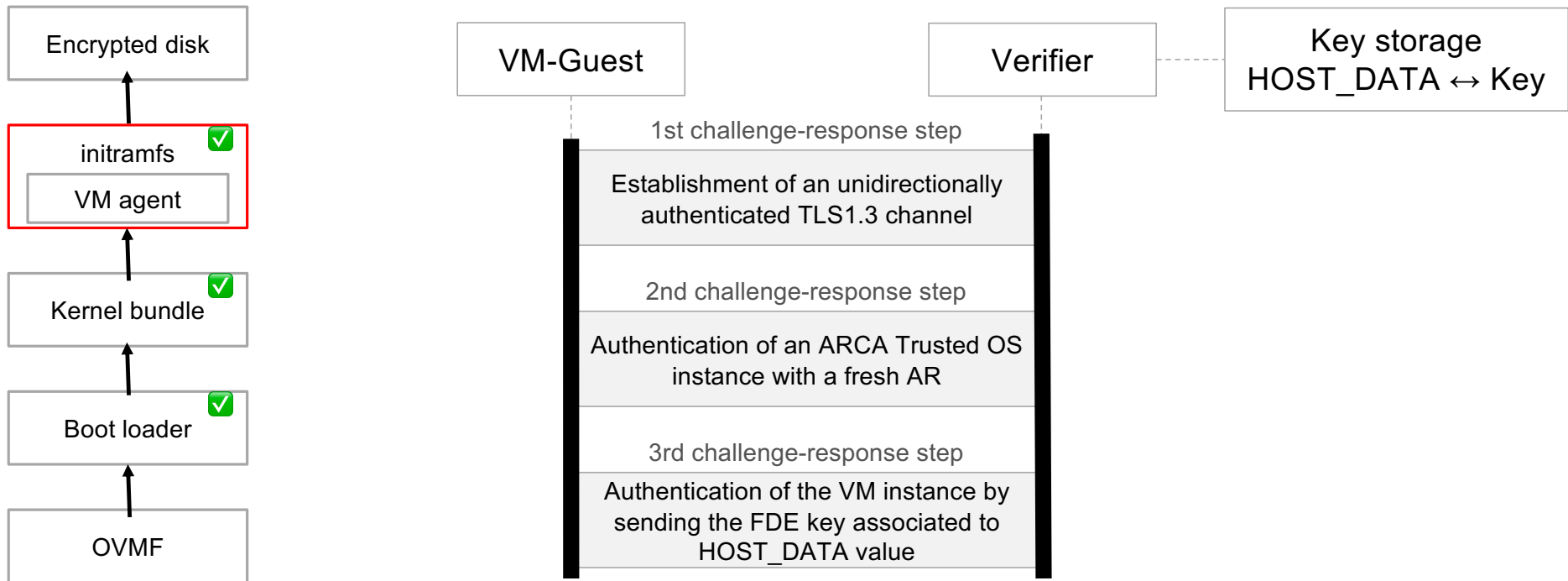
CYSEC solutions for confidential VMs

Trusted elements

Detailed Threat Model for Attested VM Launches



Attested Launch Protocol: SEV-SNP Case Study





CYSEC

Key Takeaways: Enhancing Security with Confidential Computing

- Confidential computing technology is under deployment within projects of hosted private sovereign clouds.
- CC contributes to operational sovereignty by allowing cloud users to enforce and audit the application of their security policies by their IaaS provider.
- The CC-related products for private clouds are still limited. We expect that this use-case will help to speed up the development of an ecosystem.