CONFIDENTIAL COMPUTING SUMMIT 2024

CYSEC

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

Matthieu LEGRE

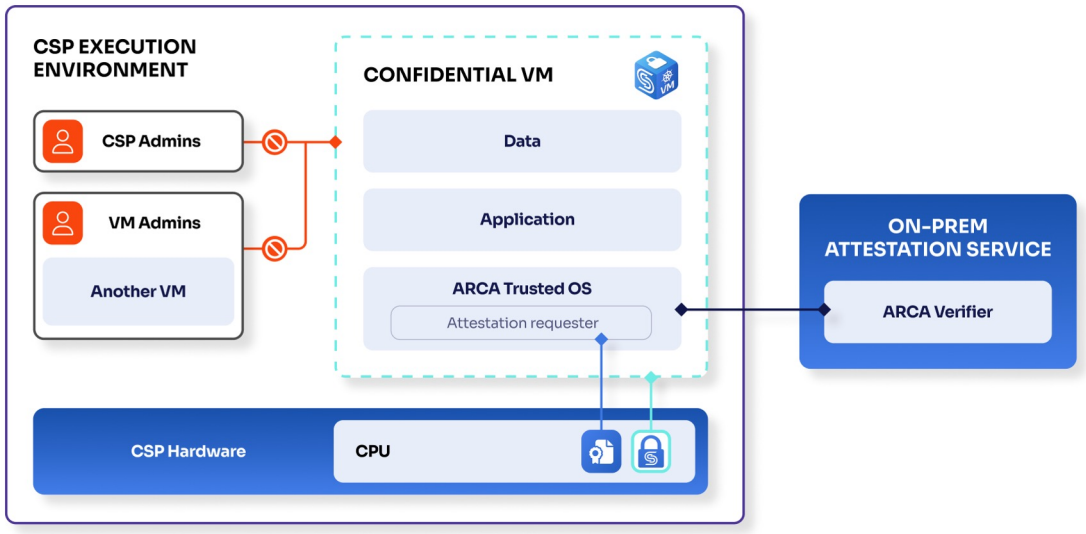
VP product, CYSEC SA

Organized by Opaque and Confidential Computing Consortium

CYSEC

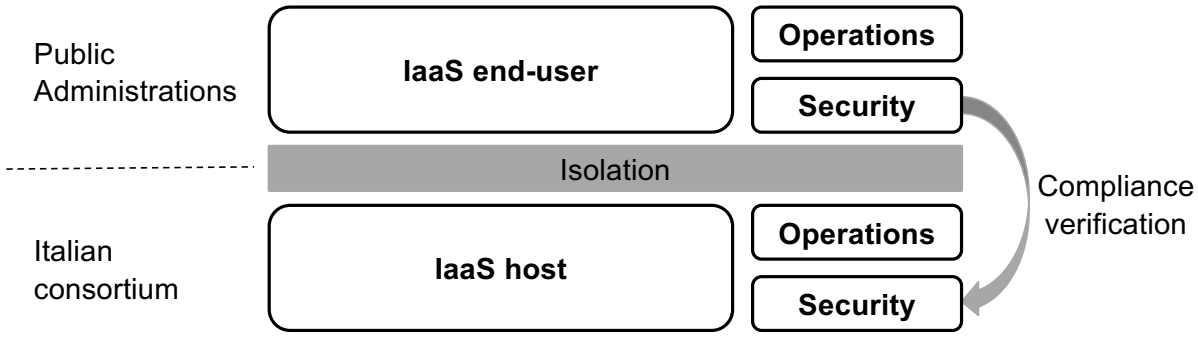
Overview of CYSEC: Expertise and Presence

- **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**

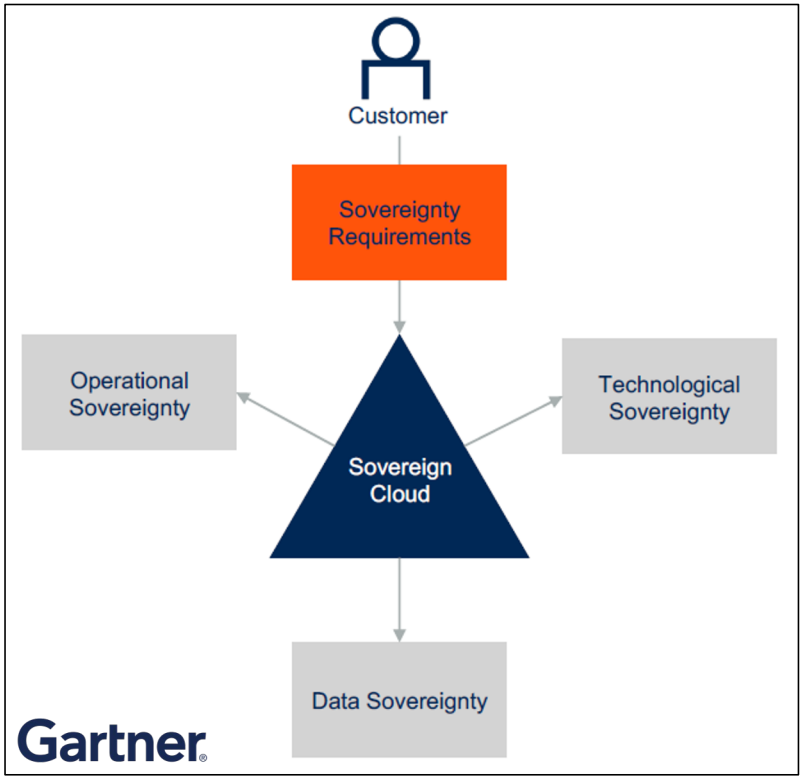


Italian Cloud Strategy: a Secure Infrastructure for Public Administrations

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



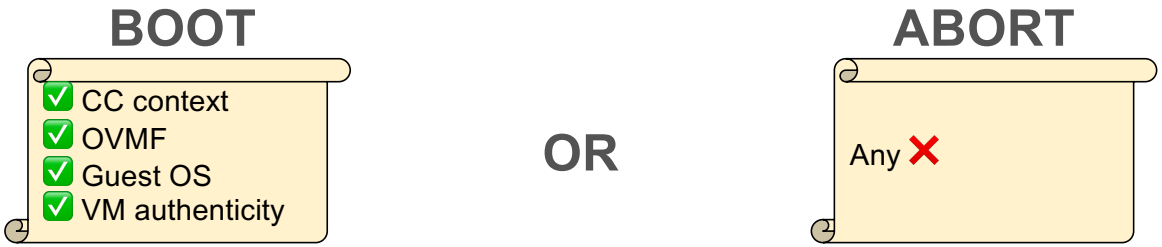
Sovereign cloud: how confidential computing can help?



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

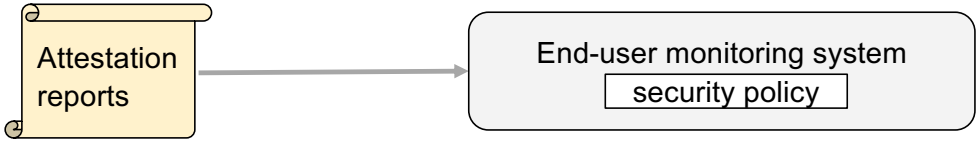
Operational Sovereignty: Attested VM launch and Continuous Auditing Needs

- Attestation of VM launches (at boot time)



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

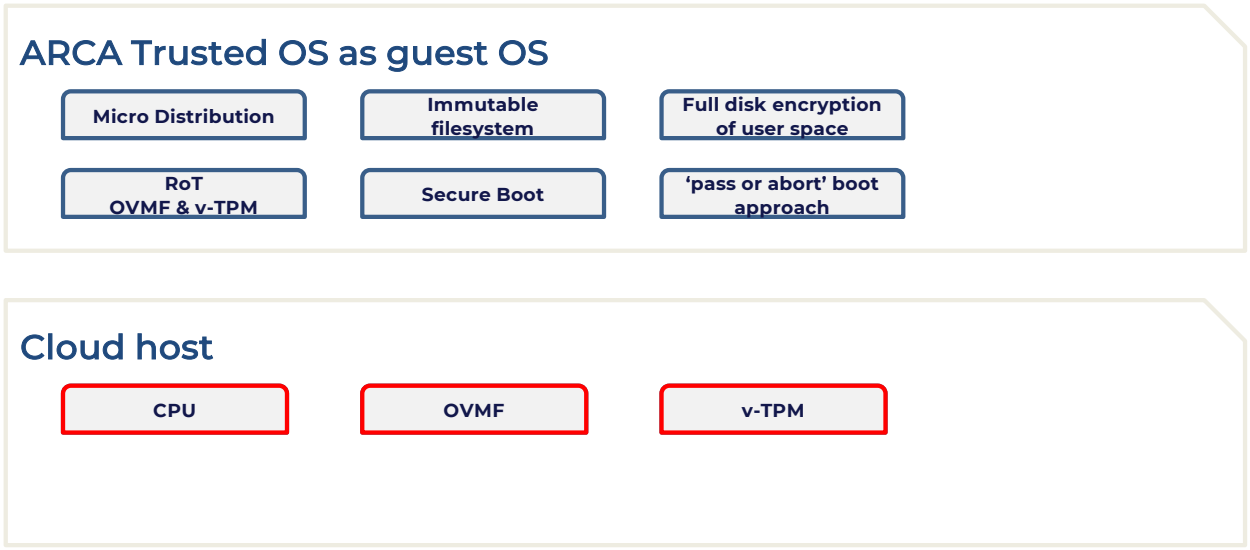
- Continuous auditing of VM instances (at run time)



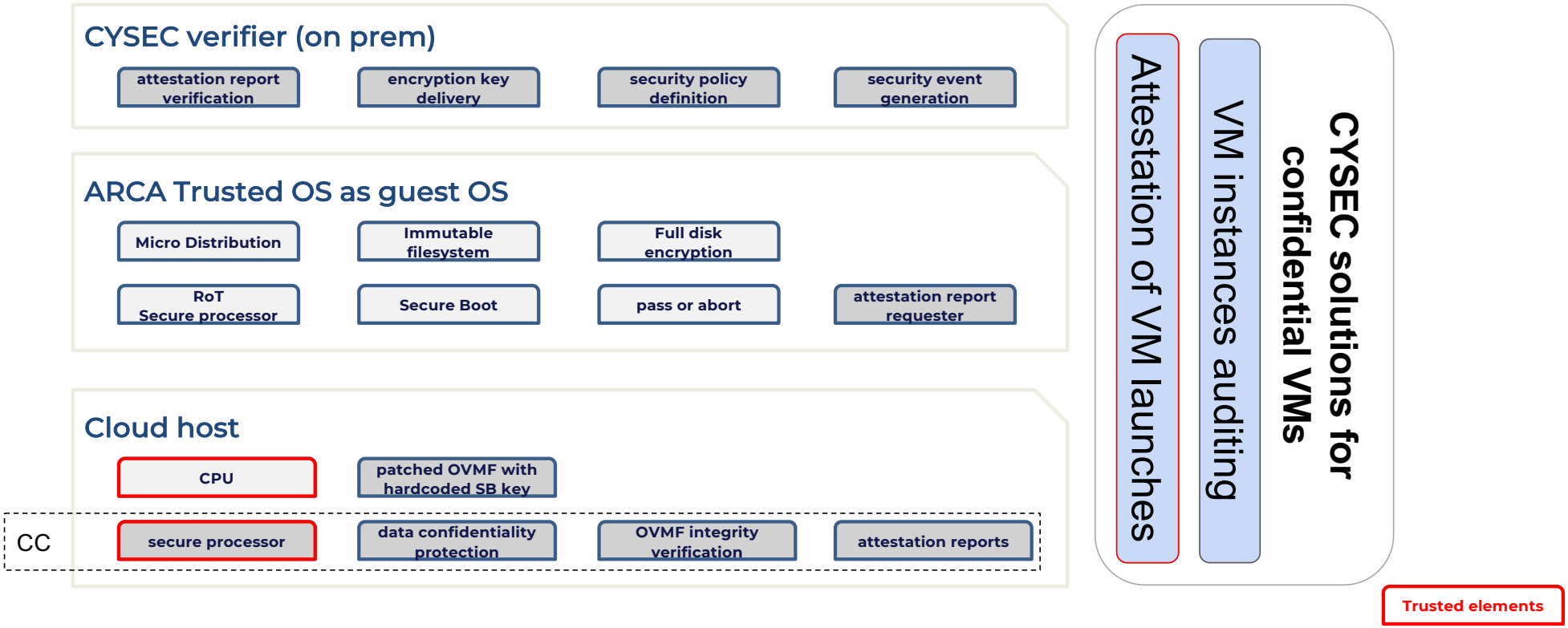
→ Technical verification of the compliance with the legal agreement between the cloud host and the cloud user

ARCA Trusted OS: Security Features in Non-Confidential VMs

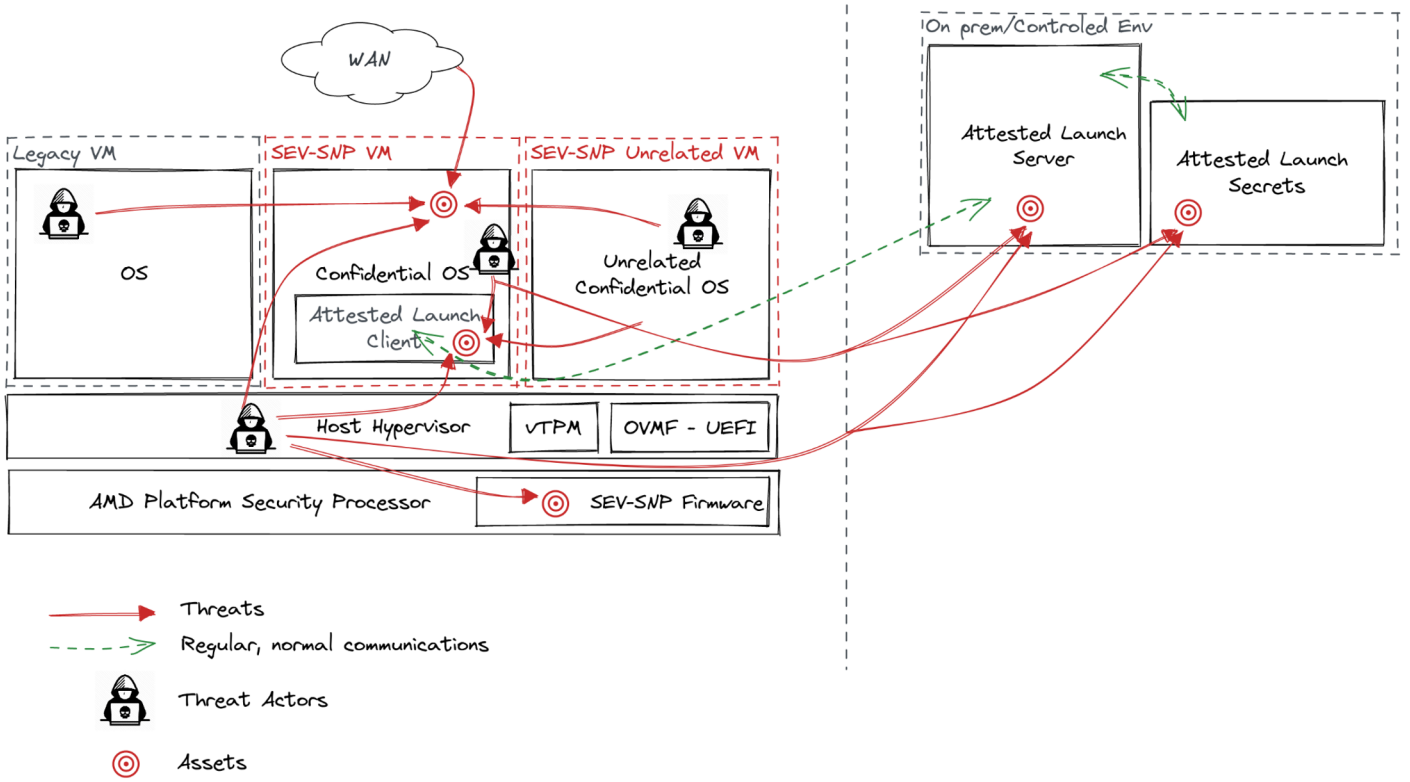
CYSEC



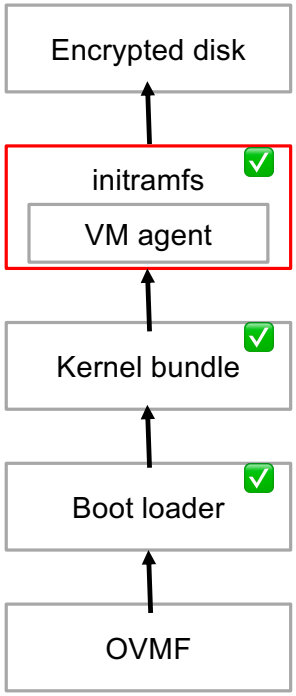
CYSEC Solutions: Ensuring Confidential VM Security

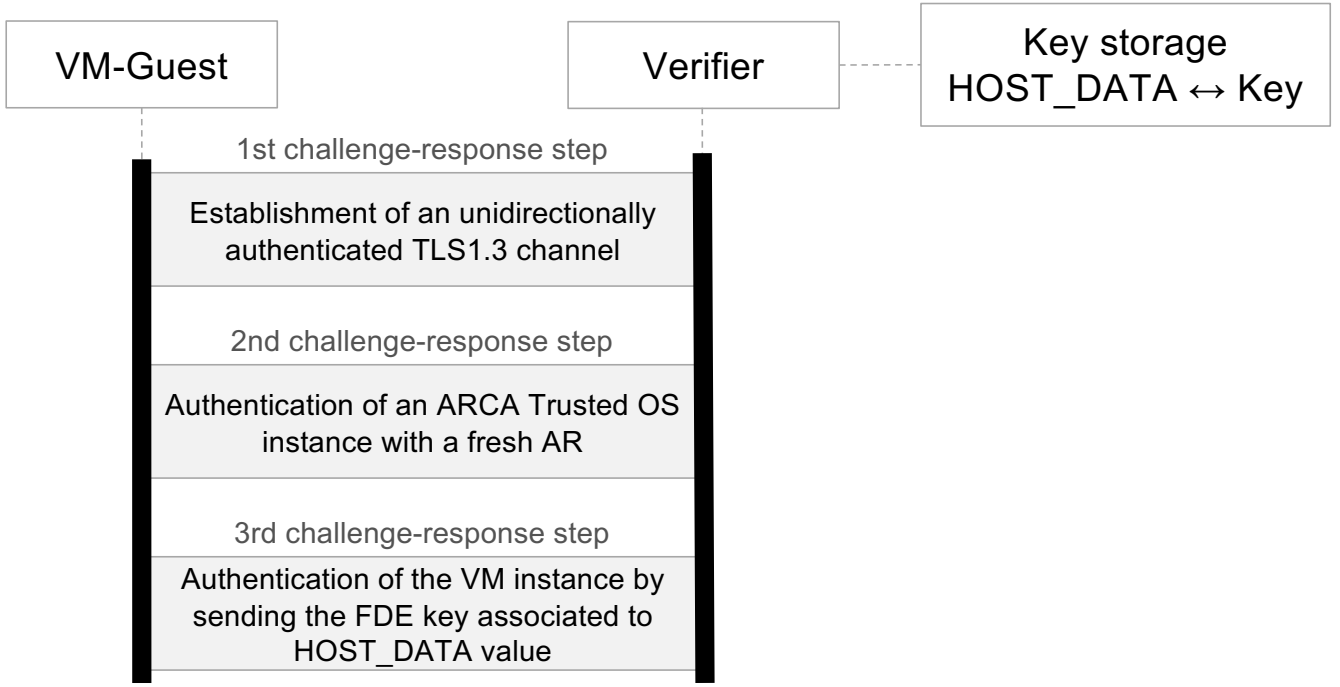


Detailed Threat Model for Attested VM Launches



Attested Launch Protocol: SEV-SNP Case Study





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.