“An example of on demand SLA”

Jean-Philippe Wary / Orange Innovation

Orange Atalante – November 15th, 2023

Business Contraints

Could « Critical Industry » constraints (regulation) become security means obligation ?

Safety requirements / objectives ←→ Security requirements / objectives

Industrials *Operators*

Evolution : 2/3/4G (Best Effort) →5G with specific security & safety means obligation ?

Addressing the Verticals real-time constraints (OT) entails / imposes real-time obligations in detection / management - mitigation / notifications of network incidents and embedded applications.

Evolution

« 5G trusted network » → « 5G trustable network »

New paradigm: on-demand security SLA

Flexible **delegation of security-related responsibilities** while optimizing costs and complexity

⇨ **Dynamic control** capabilities

Management of **on-demand SSLA responsibilities** and dynamic achievement demonstration

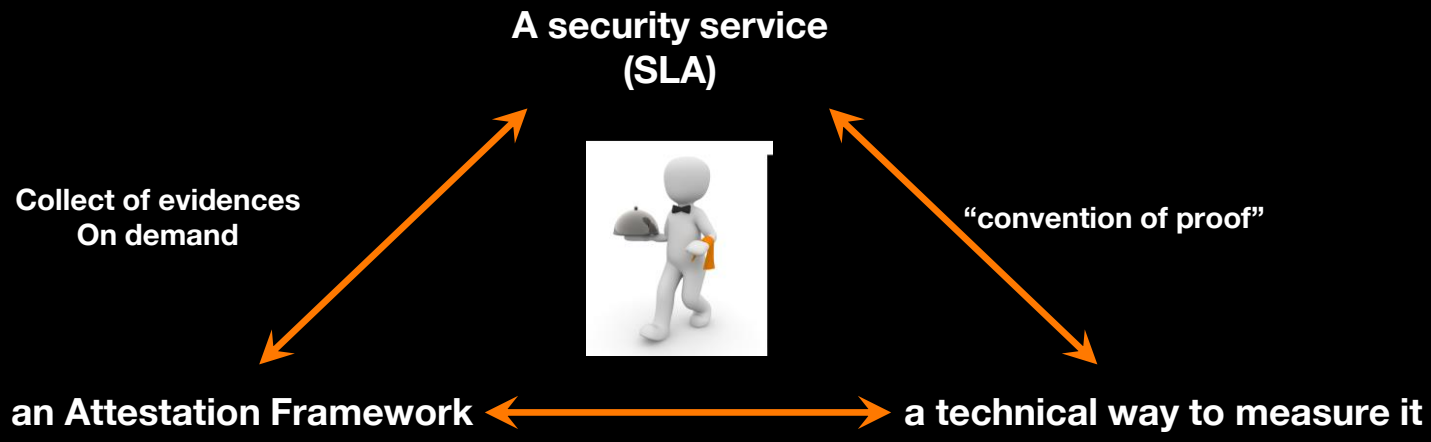
⇨ Ability to **redistribute** responsabilities

Short term availability

Mid term availability

Challenge ▸ Contract & control in a multi-party, multi-layer and evolving structure

proposition

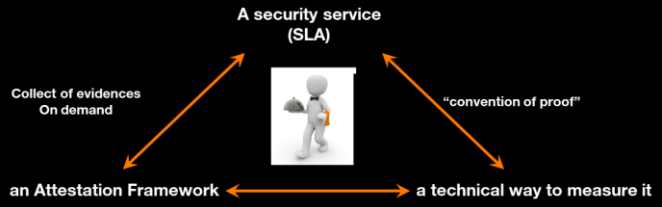


towards an industrial use of the attestation framework (2022)

H2020 INSPIRE5GPlus : demonstration of a first prototype of an obligations of 'result' for security for critical industry verticals (NIS2 & CSA)

➔ **isolation SLA on a K8S infrastructure**

"Your applications only share physical resources with applications with levels of criticality equivalent or greater"



Placement optimization under constraints for criticality and latency

INSPIRE-5Gplus MAESTRO_5G ANR MOBIS5 DEDICAT 6G

towards a catalogue of SLAs

- **isolation under constraints : criticality, latency, energy efficiency**
- **authentication of chain of components or of the underlying system** (OS, VM, containers, applications)
- **effective availability of allocated resources (CPU, memory, TPM, TEE, bandwidth) on physical servers and / or the chain of components**
  - **Only the qualified components are put in production to serve Customers.**
- **composition and insertion of additional services are effective**
- **authentification at boot-time and at run-time of critical components of the Customer**
- **critical segments of the Customer are only operated in a protected environment** (TEE / HSM).
- **software / data zoning : critical components of the Customer are only available and/or executable on identifiable target zones**
- **data security (integrity and confidentiality) during processing**

…

Merci