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

Mohamad Hajj – Internet of Trust

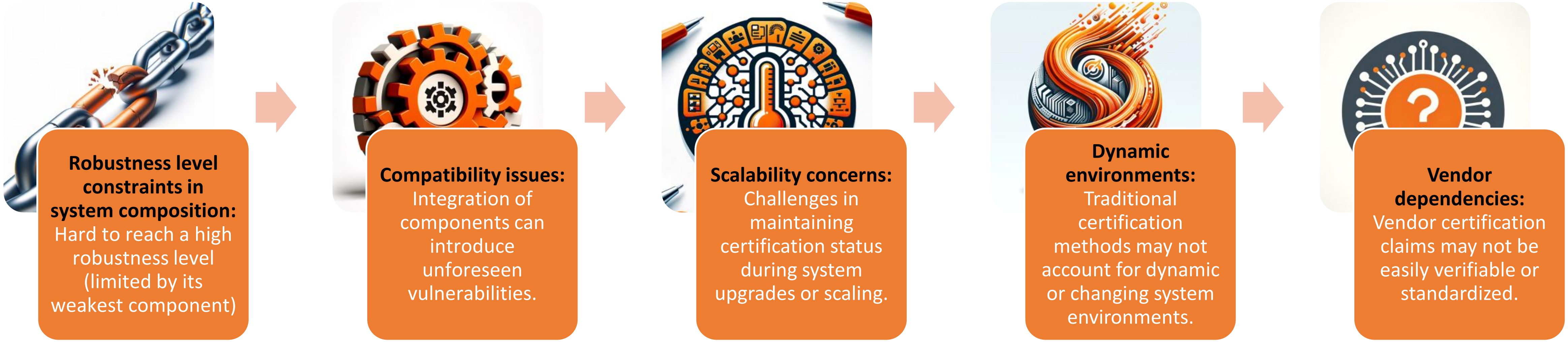
Attestation and its Applications Workshop - November 15, 2023

Agenda

- Addressing certification issues in system composition by attestation
- Lego methodology for system certification – ODSI project
- Attestation's impact on attack cotation factors
- EU CRA & Attestation role
- Focus on 5G security assurance
- Key points and conclusion

Addressing certification issues in System composition by attestation

Main current certification issues of system composition



Robustness level constraints in system composition: Hard to reach a high robustness level (limited by its weakest component)

Compatibility issues: Integration of components can introduce unforeseen vulnerabilities.

Scalability concerns: Challenges in maintaining certification status during system upgrades or scaling.

Dynamic environments: Traditional certification methods may not account for dynamic or changing system environments.

Vendor dependencies: Vendor certification claims may not be easily verifiable or standardized.

Addressing certification issues in system composition by attestation

Robustness level constraints in system composition

Attestation Role: Pinpoint and fortify the weakest system components to elevate overall robustness

Data for attestation: Interdependency data for all system components, information on the configurations of components, integrity measurements, data on the lifecycle of components

Compatibility issues

Attestation Role: Test the integration of components to identify and address unforeseen vulnerabilities

Data for attestation: Results from automated integration tests

Scalability concerns

Attestation Role: Maintain certification status more efficiently during system changes

Data for attestation: Current certification status of all components, including any conditions or limitations

Dynamic environments

Attestation Role: Real-time monitoring for dynamic system environments

Data for attestation: Data on the behavior of the system (e.g., security state, configuration data), linking information

Vendor dependencies

Attestation Role: Provide an independent verification mechanism to validate vendor certification claims

Data for attestation: Product version, security protocols, digital certificate, certification data (evaluation level, certificate ID, etc.)

Lego methodology – ODSI project

Lego methodology - ODSI project (1/2)

Reduction of the perimeter of the evaluation to only required Security Functions (SF) in a restricted configuration or well-defined use case

Possibility to increase the robustness level of those required SFs

Dynamic plug-and-play composition: possibility of adding, updating or exchanging components

Short and easy re-evaluation when loading a new component with no security requirements

Lightweight and compact approach that is targeted at IOT systems, from end-points, intermediate components such as gateways, up to integrated systems including cloud.

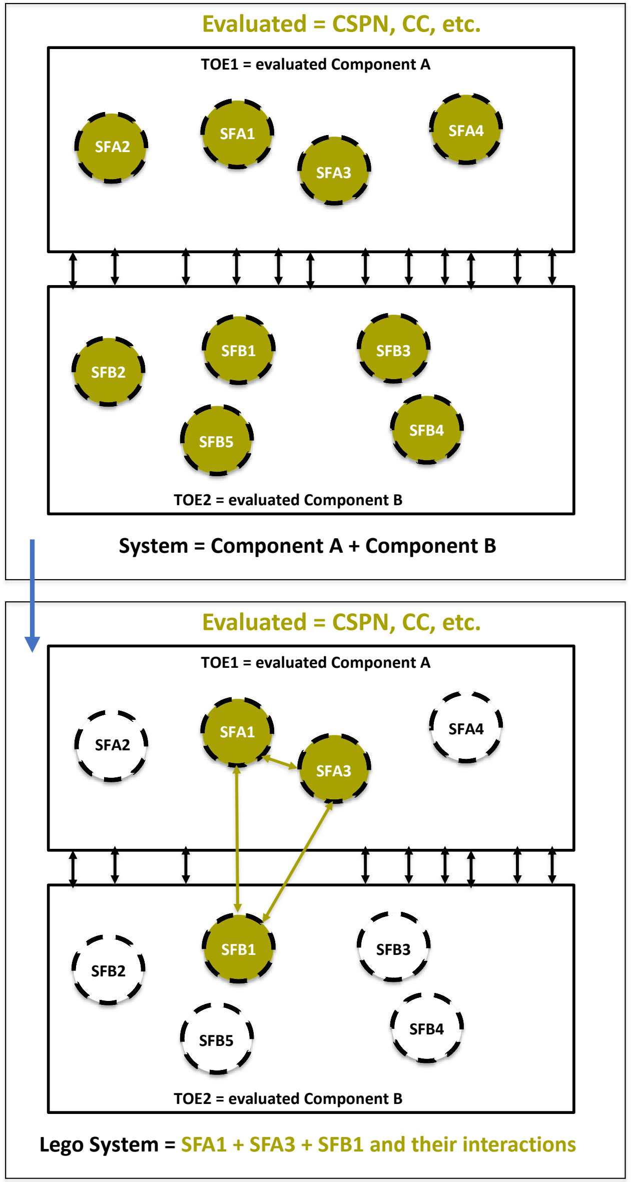
Generic approach for addressing several industry sectors

Lego methodology - ODSI project (2/2)

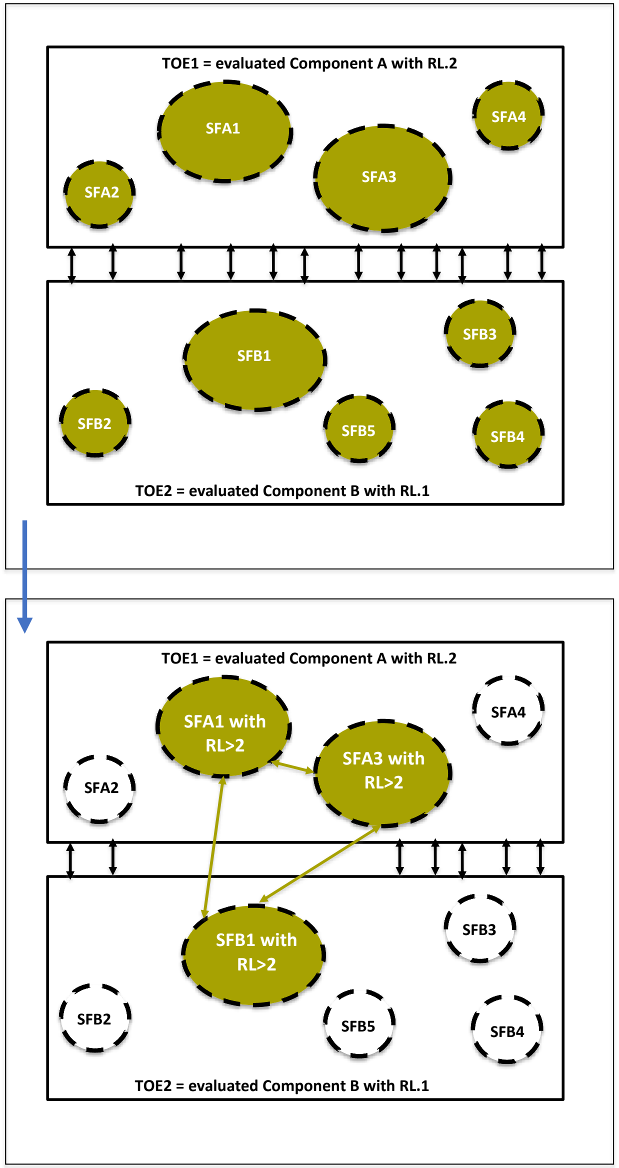
E: Evaluator
SF: Security Function
TOE: Target of Evaluation
RL: Robustness Level

Scenario of reduction of the perimeter of the evaluation

Multi-purpose Components are used in a **well-defined use case/restricted configuration** made up of **only a few required SFs**.


Evaluated = CSPN, CC, etc.
TOE1 = evaluated Component A
SFA2
SFA1
SFA3
SFA4
SFB2
SFB1
SFB3
SFB5
SFB4
TOE2 = evaluated Component B
System = Component A + Component B
Evaluated = CSPN, CC, etc.
TOE1 = evaluated Component A
SFA2
SFA1
SFA3
SFA4
SFB2
SFB1
SFB3
SFB5
SFB4
TOE2 = evaluated Component B
Lego System = SFA1 + SFA3 + SFB1 and their interactions

Scenarios of Increasing the robustness level (RL)


TOE1 = evaluated Component A with RL.2
SFA1
SFA4
SFA3
SFA2
SFB3
SFB1
SFB2
SFB5
SFB4
TOE2 = evaluated Component B with RL.1
TOE1 = evaluated Component A with RL.2
SFA1 with RL>2
SFA4
SFA2
SFA3 with RL>2
SFB1 with RL>2
SFB3
SFB2
SFB5
SFB4
TOE2 = evaluated Component B with RL.1

- Component **A with RL.2**
- Component **B with RL.1**
- Lego system = **SFA1 + SFA3 + SFB1 + interactions**
- Aim: **Achieve a robustness level of the lego system > RL.2**

Attestation’s impact on attack cotation factors

Attestation’s impact on attack cotation factors

Window of Opportunity (WoO):

- Time frame for a successful attack execution.

Attack Time (AT):

- Duration required to exploit a vulnerability.

Knowledge (K):

- Expertise needed to perform an attack.

Equipment (E):

- Tools necessary for carrying out an attack.

- Reducing window of opportunity:
  - Continuous integrity checks narrow the attack window.
- Increasing attack time:
  - Tampering detection prolongs attacker's effort.
- Elevating knowledge threshold:
  - Sophisticated attestation requires advanced attacker skills.
- Intensifying equipment requirements:
  - Hardware-based attestation demands specialized attacker tools.

EU CRA & Attestation role

EU CRA & Attestation role

EU CRA: Everybody who places digital products in the EU market will be responsible for additional obligations around reporting and compliance, such as **fixing discovered vulnerabilities, providing software updates, and auditing and certifying the products**.

CRA Req: Delivery of the products with a secure by default configuration

EUCC Gap: EUCC provides guidance to the user on modifying the initial configuration and replacing it with one that is secure.

Attestation role: can perform automated checks and real time feedback to ensure that any non-secure settings are identified and corrected before the product is deployed.

CRA Req: Regular security review of the product after its certification

EUCC gap: security review is required during certain punctual points of the evaluation timeframe, but not as a continuous regular activity.

Attestation role: can involve dynamic and ongoing assessment of the product's security.

CRA Req: Developers to disclose “unpatched” vulnerabilities to the authorities within 24 hours of the vulnerability having been discovered

EUCC gap: No gap, vulnerability handling is part of the scheme

Attestation role: can be integrated with vulnerability management processes to automatically detect and report unpatched vulnerabilities.

Focus on 5G security assurance

Challenges – 5G security assurance (1/3)

Deal with massive number of HW and SW components. (E.g. 50-100K radio equipment for a single telco operator ; 500 k-1M distribution equipment for energy in one country);

Components are diverse: PKI, HSM, TPM, PNF, Radio, Cloud, …

Components come from various vendors with multiple versions;

Components are configured and composed dynamically (slices resources, etc.)

Challenges – 5G security assurance (2/3)

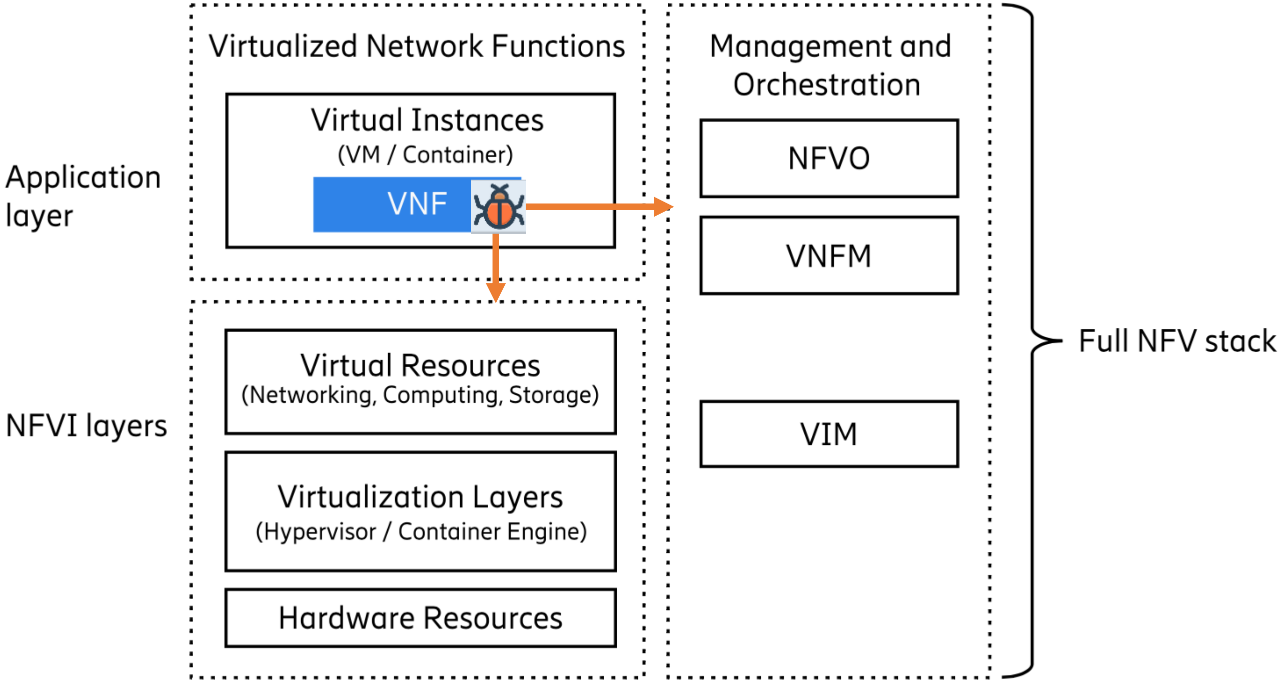
Multi-layer environment

Security protection and assurance should encompass all layers.

Security issues often need to be tackled by a coordinated coherent solution encompassing different layers.

Certified products need to be securely configured and managed by the service provider in addition

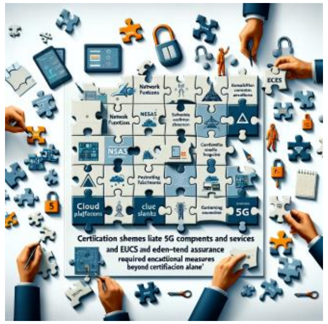
Certified products need to be operated in an assured secure environment.



Challenges – 5G security assurance (3/3)

Existing 3GPP 5G standards do not specify cybersecurity protections that support and operate the 5G system.

E.g. Cloud technologies, SDN

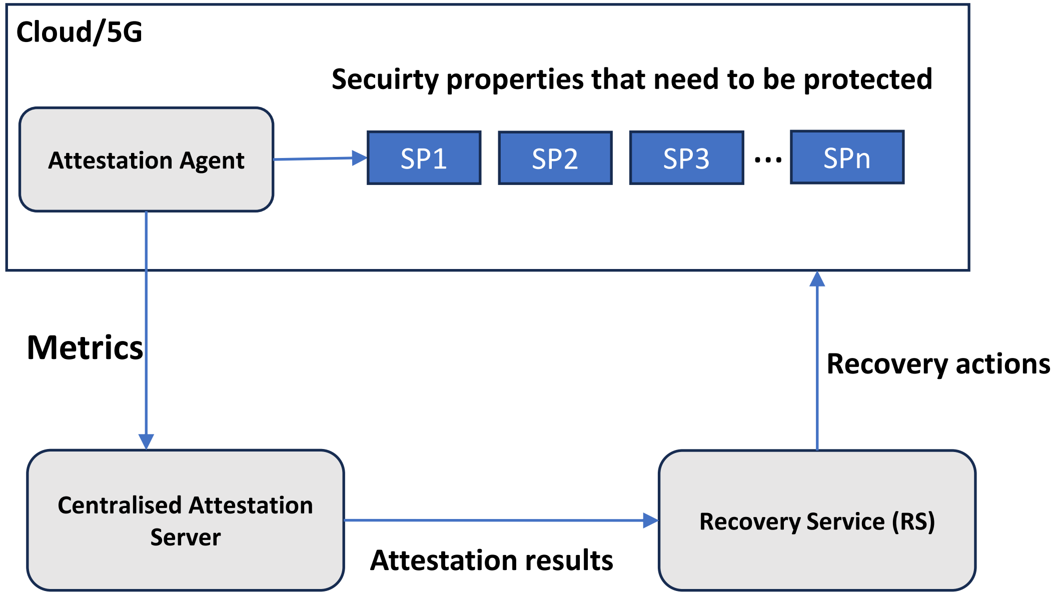

ECES
Network Fuctions
Network Function
NESAS
NSAS
Cloud plaffacons
clue slants
5G
5
Certiication shemes liate 5G compients and sevices
and EUCS and eden-tend assurance
required encadtional measures
beyond certifiacion alane'

Certification schemes like NESAS for network functions and EUCS for cloud platforms do not cover all 5G components and services, thus end-to-end assurance requires additional measures beyond certification alone.

Dynamic evaluation – Remote attestation of security properties (SP)

- Attestation framework continuously monitors the infrastructure (nodes) and SPs to detect signs of attacks or erroneous behaviour.

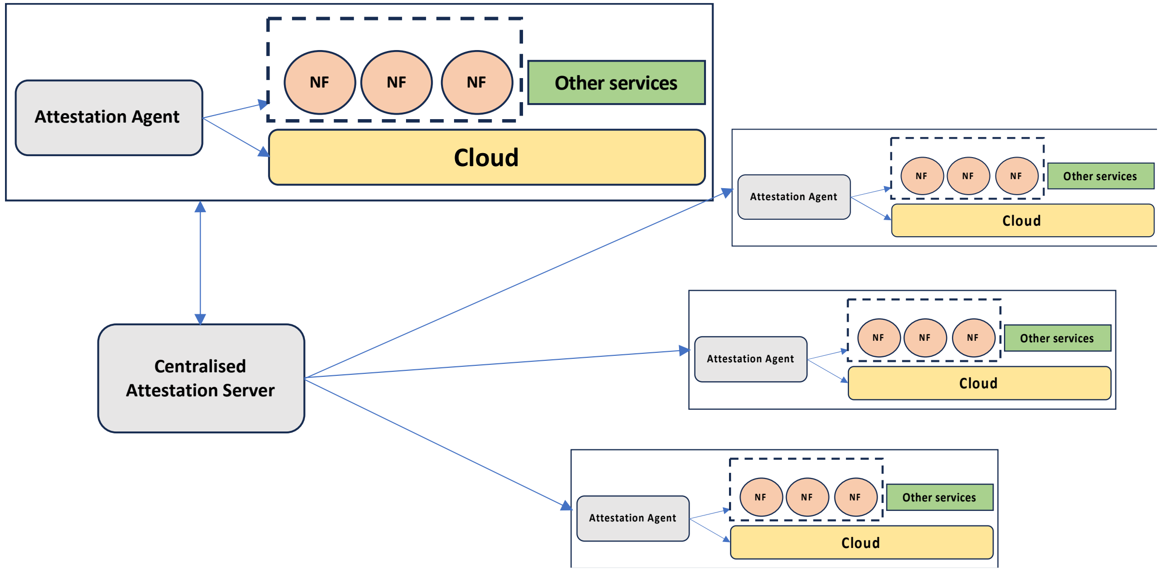
- Attestation Framework notifies the RS which will enforce a suitable remediation to recover the security posture of the system e.g.,
  - re-instantiation of the failed SC
  - Migration
  - Apply security patches

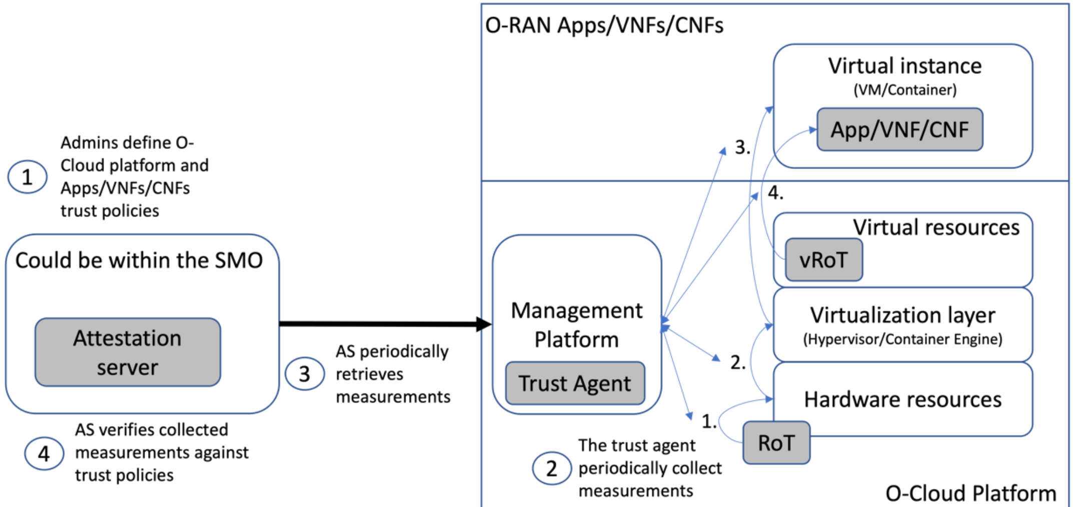


E.g., In Common Criteria, attesting the trusted execution path of SFRs (Security Functional Requirements): authentication, cryptographic operations, etc.

Dynamic evaluation – Remote attestation of 5G network

- Provide binding between NFs and Cloud
- Ensures a secure and trusted start-up for cloud infrastructure and VNFs/CNFs by validating the integrity of the boot process and authenticating software execution
- Ensure NFs and cloud operate with expected configurations at boot and run time
- Facilitates compliance by evidencing security posture; enables integrity auditing
- Provides trusted baselines for post-incident analysis and unauthorized change identification
- Authentication at boot-time and run-time of critical components
- Secure update and patch management





1 Admins define O-Cloud platform and Apps/VNFs/CNFs trust policies

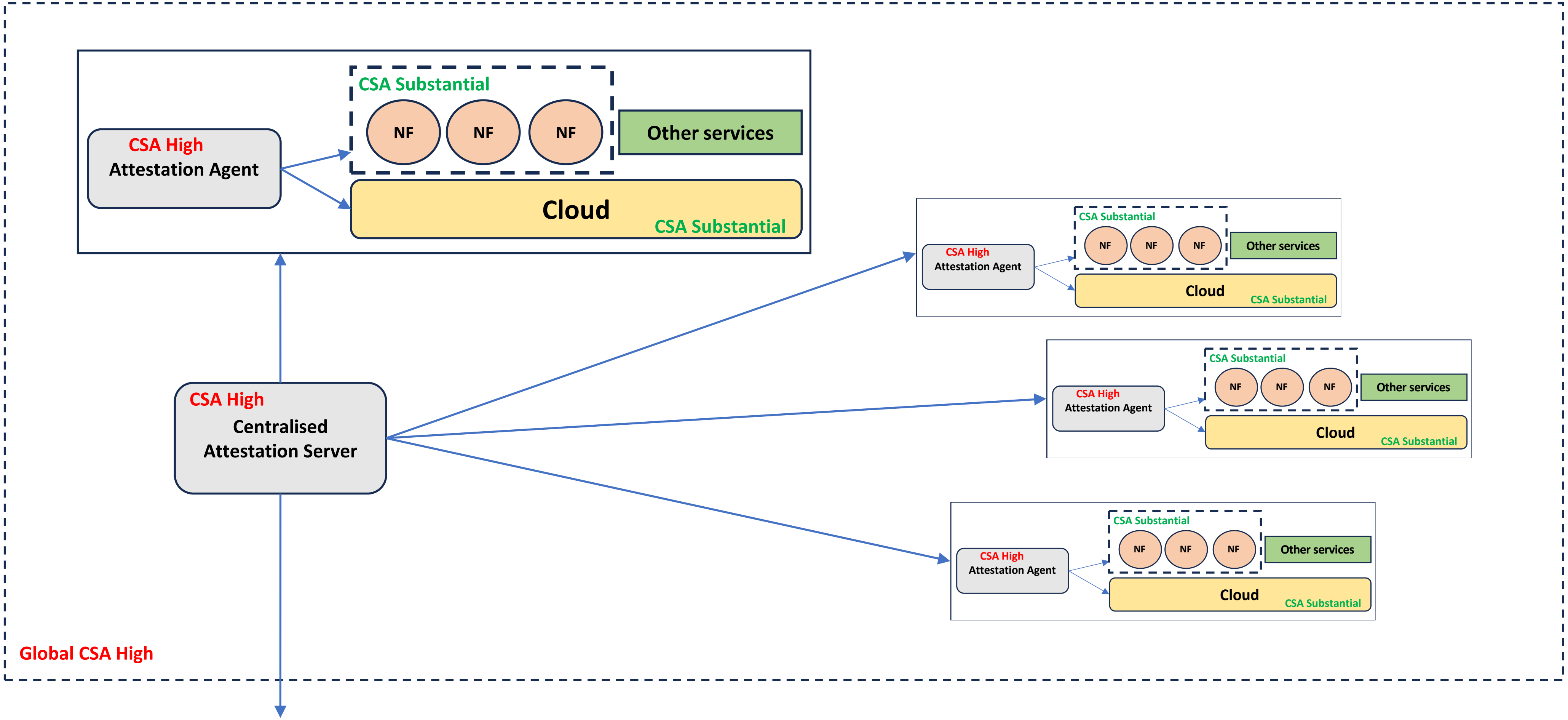
2 The trust agent periodically collect measurements

3 AS periodically retrieves measurements

4 AS verifies collected measurements against trust policies

Source: ORAN secuirty specifications v7

Dynamic evaluation – Global security level



Evidence to ENISA, Certification bodies, etc.

Key points

- EU certification schemes (e.g., EU5G, EUCS) needs to be flexible and dynamic for assessing end-to-end solution and new technologies e.g. slicing, MEC, etc.

- Need of attestation framework allowing
  - Reducing the perimeter of the certification to only required components or to specific security functions.
  - Self-assessment when required.
  - Dynamic configuration and composition to deliver contextualised assurance level

- Investigate how to trust security description/guaranty declared by each components and the way to compose those descriptors to design end-to-end systems and enable global system certification

Conclusion

- Need of more agile and adaptive approaches.
  - Attestation frameworks, with their real-time verification, automation, and adaptability, offer a promising solution.
- Attestation can play a crucial role in supporting the certification process of dynamic systems.
  - Real-time, continuous evidence that the components security functions align with the claims made in the Security Target and meet the requirements of the chosen security assurance level.
- Attestation can have a profound impact on decreasing the factors that contribute to the success of an attack.
- Attestation can enhance the security certification process and increase the security level by ensuring secure configurations, enabling continuous security monitoring, and facilitating the rapid disclosure of vulnerabilities, thus aligning with the CRA's objectives for a resilient digital market in the EU.

Questions?

INTERNET OF TRUST

www.internetoftrust.com

Get in Touch

With Us:

E-mail:

- mohamad.hajj@internetoftrust.com

77 Avenue Niel, 75017 Paris, France

Phone:

- 0619357759

IOTR Background in 5G security and certification

- Evaluation requirements and methodologies
  - SE and eUICC products in Global and European certification schemes
  - Lego certification methodology CelticPlus ODSI (Project ID: C2014/2-12, 2015-2018)

- French Operators
  - 5G core Network security requirements definition (published by FFTelecoms in February 2021)
  - Study on 5G verticals for Orange (2020)

- ORAN Alliance
  - Open RAN threat model and remediation analysis
  - O-Cloud security analysis
  - O-RAN security testing specification

- Enisa
  - Editor of ENISA 5G NFV security challenges (report published on 24 February 2022)
  - Contributor to ENISA 5G Security Controls Matrix published on May 24, 2023
  - Mohamad Hajj, member of ENISA's Ad-Hoc Working group and rapporteur on the "5G Cybersecurity Certification”

IOTR publications related to 5G security

- 2022 Collaboration with the Open Ran MoU by Deutsche Telekom, Orange, Telefónica, TIM and Vodafone - "***Open RAN Security White Paper***"
- EU Cybersecurity Act. Conference 2021 – "***5G Security – from security objectives to operational requirements***"
- ICCC 2020 - "***Trust model for verticals over 5G***"
- Orange research blog 2020 – "***How increasing the confidence in the eSIM ecosystem is essential for its adoption***"
- EU Cybersecurity Act. Conference 2019 - "***Embedded Systems for IOT Products: What is the current certification offer?***"
- ICCC 2019 - "***SIM to eSIM: what about security assurance and risks management?***"
- ICCC 2018 - "***Robustness propagation through systems of heterogeneous CC components***"