ETSI GR NFV-SEC 018 V1.1.1 (2019-11)

Network Functions Virtualisation (NFV); Security; Report on NFV Remote Attestation Architecture

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/NFV-SEC018

Keywords
NFV; security: trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document identifies and studies Remote Attestation architectures applicable to NFV systems, including the definition of attestation scope, stakeholders, interfaces and protocols required to support them. Additionally the present document identifies and discusses functional and non-functional capabilities to be supported in an NFV system and provides a set of recommendations.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR NFV-SEC 007: "Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments".

[i.2] ETSI GS NFV-IFA 026: "Network Functions Virtualisation (NFV); Management and Orchestration; Architecture enhancement for Security Management Specification".

[i.3] ETSI GS NFV-REL 005: "Network Functions Virtualisation (NFV); Accountability; Report on Quality Accountability Framework".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ACL	Access Control List
AR	Attestation Result
AS	Attestation Server
BCA	Blockchain of Certificate Authority
CPU	Central Process Unit

CRTM	Core Root of Trust for Measurement
CSC	Cloud Service Customer
CSCA	Cloud Service Customer A
CSCB	Cloud Service Customer B
CSP	Cloud Service Provider
CSU	Cloud Service User
DLT	Distributed Ledger Technology
EM	Element Management
EMS	Element Management System
FC	Functional Component
GUID	Globally Unique IDentifier
HMEE	Hardware-Mediated Execution Enclave
HSM	Hardware Security Module
HW	Hardware
IAIS	Infrastructure Attestation Information Service
II	Second
LCP	Launch Control Policies
LoA	Level of Assurance
MAC	Message Authentication Code
MANO	MANagement and Orchestration
NFVI	Network Function Virtualisation Infrastructure
NP	Network Provider
PDLT	Permissioned Distributed Ledger Technology
PKI	Public Key Infrastructure
RA	Remote Attestation
RAIC	Remote Attestation Information Customer
RAIP	Remote Attestation Information Provider
RAS	Remote Attestation Server
RATP	Remote Attestation Trusted Party
RIAP	RA Information Provider
RoT	Root of Trust
RTM	Root of Trust for Measurement
RTR	Root of Trust for Reporting
RTS	Root of Trust for Storage
SE	Security Environment
SEMS	Security EMS
SM	Security Module
SSR	System State Report
SuE	System under Evaluation
TCB	Trusted Computing Base
TEE	Trusted Execution Environment
TTL	Time to Live
TTP	Trusted Third Party
UUID	Universally Unique Identifier
VM	Virtual Machine
VMI	Virtual Machine Introspection
VNF	Virtual Network Function
VNFCI	VNF Component Instance
VNFI	Virtual Network Function Instantiation
vRoT	virtual Root of Trust

4 Motivation and Problem Description

4.1 Overview

Today's deployed systems face a huge amount of threats that have the capability to compromise them partly or fully and, in many cases, involves that an attacker modifies a system such that malicious software is executed. Execution of code that was not intended to be executed on the system is expected to be detectable. One defensive measure that addresses the malicious software execution is Remote Attestation (RA).

Remote in this context is defined as the attestation taking place outside of the immediate trusted element by a Trusted Third Party (TTP). In contrast, for local attestation, a specific hardware module might use Launch Control Policies (LCP) which are capable of halting boot (or some other action) on that device if the policies are not satisfied by the gathered measurements.

Specifically, RA is a well-known concept that is used to determine the trustworthiness of systems. Hence it might be used to facilitate the detection of unintended/malicious software. The overall process during RA is:

1) accumulation of information on a system A;

2) reporting of the accumulated information to a different system B; and

3) evaluation on basis of a comparison between the reported and well-known reference information.

Accordingly, the evaluation result is either system A is in a trusted or an untrusted state.

A TTP, i.e. the verifier, in the context of RA is the entity that holds known good values, acquires measurement reports of system state and makes the decision whether a given system, element, component etc. is trusted. What trusted is not defined means other than stating that the given system meets some a priori criteria, for example, but not limited to, that the system only loaded and executed software that is well known. How information that an element is trusted is not defined is interpreted by other elements either. Consequently, RA facilitates to assess whether a remote service is provided by a trustworthy environment. Such trust establishment is the fundamental step prior to the remote entity engaging in further interaction such as consuming services or to deliver sensitive/secret data to the remote service. For example, tenants might use RA to assess if the overall infrastructure (NFVI) is trustworthy, datacenters might use RA to assess trustworthiness of subsystems they use, and management entities might use RA to assess the trustworthiness of individual infrastructural components. Furthermore, tenants might offer RA services to its remote users and thus offer an overall assurance assessment of the end service or a service for proving compliance. For example, to demonstrate that data is stored at a correct geographical location. Hence, there are numerous use-cases and scenarios that might be considered where attestation is a fundamental step of creating an overall trustworthy system.

A trustworthy element is the entity which has a component that provides a unique identifier, certification (e.g. through cryptographic signing) and which is able to store measurements and data about the state of that element (including related sub-elements or dependent elements if necessary) in a tamperproof and verifiable form. For example, the TPM2.0 quoting mechanism using the TPMS_ATTEST data structure is an example of this.

4.2 Problems and Challenges

However, the classical RA concept and architecture was designed on basis of individual systems with clearly defined roles and assumptions. Thus, this traditional approach is not directly applicable in modern system architectures that rely on virtualisation, since it does not consider such systems from an architectural point of view. One approach that could simply overcome these problems would be to ignore the virtualisation altogether and treat each system individually. In this case, however, important information that might not be established at a later time easily gets lost and, thus, would not result in an acceptable evaluation result. Apart from the virtualisation, the NFV architecture introduces different other characteristics and constraints RA needs to adhere, for instance different roles, components, responsibilities and even visibility within the deployed systems. For these reasons, it is necessary to adopt all of the NFV related characteristics and constraints in order to derive a meaningful and applicable RA solution for NFV.

More specifically, when speaking about the attestation procedures, there are two important aspects to consider. One is the attestation protocol itself and the other is, how the information that the appraiser gets via the attestation protocol is transformed or interpreted into a statement of being trustworthy. It might be the case that this interpretation is simple but one might easily define use cases where the task of interpreting attested data is hugely complex. In any case, what is important here is that the appraiser has the knowledge how to interpret the attested data. Such knowledge is easier to arrange when the attester and appraiser are close and are, for example, aware of their environment. This leads also to the question where the appraisal takes place. One extreme is that the one that wants the information about the trustworthiness also performs the appraisal. Another extreme is that the appraisal comes from an a priori Trusted Third Party (TTP). In the latter case the one that wants to establish trustworthiness could only get a binary decision from the TTP: trusted vs not-trusted. Alternatively more complex information is provides such as levels of assurance.

The attestation protocol consists of the messages and procedures through which the attester interacts with the appraiser. The details of the protocol are coupled to the technical environment of the attester. On the other hand the purpose of the attestation protocol is to securely deliver attestation information to the appraiser, whereas the information is securely gathered in the attester's environment. This secure acquisition is necessary, so the appraiser is able to deliver a statement on the trustworthiness-state.

When using a TTP Attestation Server (AS), the semantics what trustworthiness means is hidden, and is coupled to an agreement by which one is allowed to talk to the AS, but there is typically no explicit data transferred, e.g. data that would detail what trustworthiness means for an Openstack Controller. Again, where the attestation server is located is not defined. Encapsulating the trustworthiness allows for a simpler way to adopt different implementation technologies, but it might also cause that for certain technologies fully leveraging the features of the remote attestation functions in that technology becomes limited. These consideration are the main reason why this present document distinguishes between the high level use-cases in clause 4.5.

One example of RA is that one in Openstack known as trusted compute pools. Here the launch of a VM only occurs when Openstack Controller gets the confirmation that the compute node is trustworthy from a so-called Attestation Server (AS) which performs the appraisal of the trusted compute pool that Openstack Controller wants to use for the VM.

4.3 NFV Attestation Scope

The overall NFV attestation scope comprises multiple related systems and components. From a simplified top-down view, a NFV provides a particular service to a customer. Typically, the basis of this service is provided by software running inside virtualised systems that, in turn, are instantiated on top of hypervisors. This means, ideally, the overall attestation scope comprises all of the corresponding systems and components involved, i.e. one or many hypervisors, instantiating one or multiple VMs that execute one or many different application processes, schematically depicted in Figure 4.3-1.

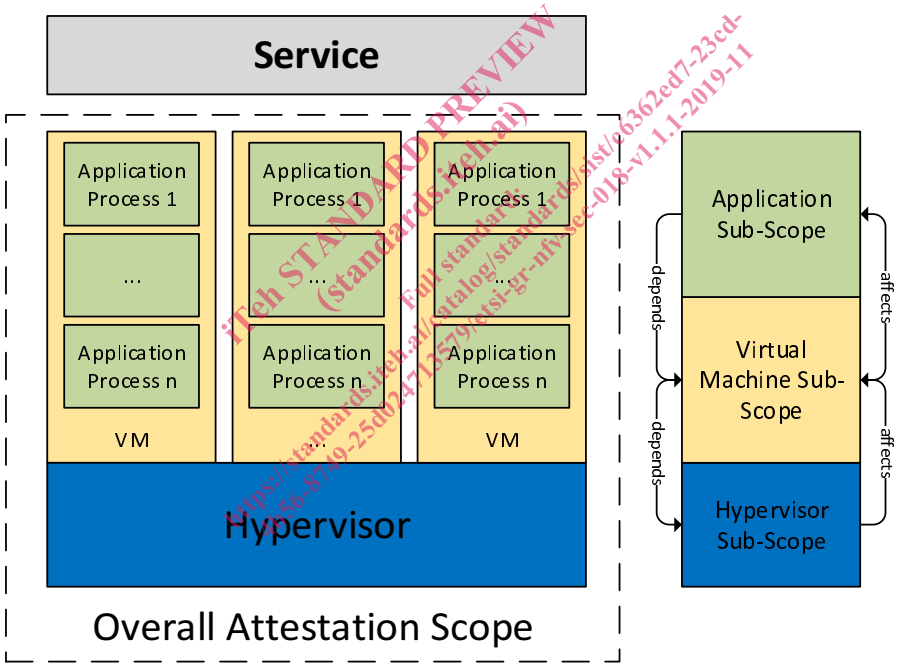

Figure 4.3-1: NFV Overall Attestation Scope

Specifically in NFV, the overall attestation scope is a composition of the described individual systems and components under the control of different roles and organizations with presumably limited visibility. Hence, the NFV attestation scope needs to be divided into multiple sub-scopes that aligns with the actual system architecture and, in addition to that, consider the mentioned additional roles, architectural components and characteristics introduced by the NFV high level architecture. These specifics are to be analysed and discussed in clause 5.3 in more detail.

In addition to the aforementioned aspects, the overall attestation scope depends also on the exact use case and, most importantly, on the agreed Level-of-Assurance (LoA) [i.1]. In particular, the LoAs define the sets of systems and components to be considered during attestation procedures and, thus, facilitate the determination of the overall attestation scope. An overview of the defined LoAs in relation to the attestation scope is depicted in Table 4.3-1.

Table 4.3-1

LoA Level	LoA defined set of attested Systems and Components	Type	Affected Attestation Sub-Scope(s)	Attestation
0	all components	None	None	None
1	Hardware and Virtualisation Platform	Loadtime	Hypervisor + Virtual Machine	Local
2	Hardware and Virtualisation Platform	Loadtime	Hypervisor + Virtual Machine	Remote
3	VNF Software Packages	Loadtime	Virtual Machine + Application	Local
4	VNF Software Packages	Loadtime	Virtual Machine + Application	Remote
5a	Hardware and Virtualisation Platform	Runtime	Hypervisor + Virtual Machine	Remote
5b	VNF Software Packages	Runtime	Virtual Machine + Application	Remote

Accordingly, the relevant LoA Levels that relate to the present document are LoA 2, 4, 5a and 5b. Important to note regarding the defined LoAs is that the corresponding attestation scope does not include the hierarchical lower layer implicitly. This means, LoA 4 does not influence the attestation information of LoA 2, although both levels share the Virtual Machine Sub-Scope. Thus, the overall attestation scope for LoA 2 and 5a relates to the Hypervisor and Virtual Machine sub-scopes and for LoA 4 and 5b the overall attestation scope relates to (1) Hypervisor and Virtual Machine sub-scopes and (2) Virtual Machine and Application sub-scopes. In the latter case (i.e. LoA 4 and 5b), two separate but interdependent RA procedures need to be applied to satisfy the requirements defined by LoA.

To conclude, the NFV RA scope depends on multiple distinct systems and components. These systems and components are under control of different organizations with different visibility. This defines natural boundaries between the involved systems and components that are represented by introduced sub-scopes. Moreover, LoA are used to determine the overall RA scope within NFV. Depending on the targeted LoA level, the overall RA scope includes multiple RA procedures that also relate to limited visibility within the system.

Regarding the present document, the targeted overall RA scope considers Hypervisor, Virtual Machine and Application sub-scopes, to satisfy the highest LoA (i.e. 4, 5a and 5b) defined. Consequently, the document discusses all RA relevant systems and components available within NFV and consider them in the design for the RA Architecture appropriately.

4.4 Stakeholders

The stakeholders relevant for RA are derived by the corresponding roles defined in ETSI GS NFV-REL 005 [i.3]. In particular, these roles are: Cloud Service User (CSU), Cloud Service Customer (CSC) and Cloud Service Provider (CSP). The CSP role is further subdivided into NFV Infrastructure (CSP: NFVI) and NFV Management and Orchestration (CSP: MANO) that might be the same or different organizations. The additional CSP roles, i.e. Functional Component (CSP: FC) and Network Provider (CSP: NP) are not considered in the present document. It is assumed that these roles are implicitly provided or not part of the NFV itself.

Accordingly, the stakeholders are identified as representatives of the mentioned roles within RA. Since NFV follows a hierarchical approach based on customer-provider relationships, each stakeholder has a particular interest in the information provided by RA. But, in turn, the information required to provide the RA information is not visible/available for all stakeholders. In addition, the hierarchical model also implies that there is no direct relationship that necessarily extends beyond a certain role boundary. For example, a CSU typically has no business relationship with the CSP and vice versa, so it might not be possible to exchange any RA information directly between them. As a result, two RA Information related roles are introduced that distinguish between an RA Information Provider (RAIP) and Customer/End-user (RAIC). More specifically, the RAIC is interested in the information provided by RIAP, but does not have the capability to acquire them; the information necessary might not be available, for instance, due to limited visibility. Accordingly, the RAIP is responsible to accumulate and provide the relevant RA information instead.

Table 4.4-1

Stakeholder	RAIC…	RAIP…
CSU	of CSC	n/a
CSC	of CSP	for CSU
CSP	n/a	for CSC

Consequently, the different stakeholders can only act as depicted in Table 4.4-1:

- CSU is RAIC of CSC
- CSC is RAIP for CSU
- CSC is RAIC of CSP
- CSP is RAIP for CSC

NOTE 1: A stakeholder with the capability of RAIP might implicitly be a RAIC of itself. For example, the CSP: NFVI could be in the role of the actual RAIP and CSP: MANO in the role of RAIC in this case.

Still, depending on the particular use-case and the exact RA model employed, the RAIP provides the accumulated information only, an already RA-evaluated result or both. Consequently, this means the RAIC either needs to conduct the RA evaluation or rely on the evaluation result provided.

Regarding the exchange of information between stakeholders, there is typically no unbound exchange of information between roles without a direct relationship in a strict hierarchical model. However, a relaxed hierarchical model could be defined that facilitates this exchange of information. Within this relaxed model, all parties provide the necessary information for the RA evaluation process without considering the hierarchical relationships altogether.

Since a completely unconstrained model might not be applicable in certain NFV RA use-cases, but a strict model would impose too many restrictions, a RA Trusted-Party (RATP) stakeholder, which might either be one of the involved parties or an additional independent party, is introduced as an alternative. The RATP is generally trusted by all RA-involved parties and has access to all information relevant to conduct an RA evaluation. Still, this does not involve the accumulation of RA information, because it is not assumed the RATP can freely access all involved systems and components on its own and acquire the information by itself. As a result, the other stakeholders do accumulate the necessary RA information by themselves, but are expected to report them to the RATP. In turn, the RATP acts as a central receiver of all accumulated RA information and conducts the RA evaluation on basis of this information. In this model, the following role-based relationships apply:

- CSP and CSC are RAIP and reports to RATP
- CSP, CSC and CSU are RAIC of RATP (evaluation result)

NOTE 2: In this model, a RAIP only accumulates the RA-information on the relevant systems and components. It does not conduct the RA-evaluation on its own. This means, in this case, a RAIP might not act as a RAIC for itself. Thus, for instance, if CSP: MANO is interested in CSP: NFVI information, it needs to ask the RATP unless it has the capability to do an RA-evaluation on its own. This is not defined or expected within this model and not considered.

4.5 Use Cases

4.5.1 Use Cases Overview

The RA use cases rely most of all on the information that is available to the involved stakeholders. In general there is a distinction between the RA information that is accumulated and the RA information necessary to check these measurement information during evaluation. As described in the previous clauses 4.3 and 4.4, the visibility of measurement information is limited to the stakeholders that control the corresponding system. But, as mentioned, this visibility only related to the actual procedure of the measurement. Hence, this does not affect the reporting of this information and neither limit the possibilities that a stakeholder might offer this information to another stakeholder by providing an interface to acquire this measurement information.

Considering that the access to the accumulated information is provided by an interface that is able to restrict the access to the information, the strict and relaxed model are equal from an architectural point of view. Similarly, the access permissions in the model involving a RATP can be restricted. For this reason, the measurement accumulation and reporting does not limit or affect the RA architecture, besides the definition of the particular interface that provides this information. As a result, the RAIP does not affect the RA Architecture and thus, plays only a minor role during the definition of use-cases. Instead, the RAIC is used to distinguish between the use-cases.

Under the pre-condition that the RA measurement information is available to RAIC, the RA Architecture needs to distinguish between a RAIC that has only limited knowledge or full knowledge during the evaluation procedure. In case this knowledge is limited, the corresponding stakeholder can only evaluate the RA measurement information partly. For instance, if the CSP has only RA evaluation information for the Hypervisor and Virtual Machine attestation scope, it can only determine the reliability of these particular scope, even if additional measurement information would be available to him. Similarly, if the CSC has only access to Virtual Machine and Application scope evaluation information, it cannot determine the reliability of the Hypervisor and Virtual Machine scope, even if the RA measurement information is available. This means, within this model, multiple distinct attestation procedures might be required, depending on the LoA that has to be satisfied.

4.5.2 Transitive Model Use Case

Multiple Independent Logical RA Servers in a single trust domain.

Assumptions:

1) It is assumed that the model satisfies LoA 4 and 5b.

Pre-Conditions:

1) Relevant RA measurement information is available. Access permissions policies are enforced by the Security Controller or available to all RAIC.

2) Role-specific RA evaluation information is available to RAIC, but limited to system and component managed directly by the corresponding RAIC.

Use-case 1 is defined as follows:

There are multiple RAICs, repressed by different stakeholders with limited RA evaluation information. Each RAIC can only evaluate the systems and components it manages and operates. In order to satisfy LoA 4 and 5b requirements, a RAIC might share its RA evaluation result with other RAICs or provide the RA evaluation result to a different system that is eligible to receive this information. In case of RAIC 1 sharing its RA evaluation result with another RAIC 2, RAIC 2 inherently trust the RAIC 1 evaluation result and might use it during its own evaluation procedure. In addition to that, a RAIC might share its evaluation results with a third independent system, eligible to receive this information. In any case, the system receiving the RA evaluation results might combine them and derive the overall reliability state based on the provided evaluation results it received. To satisfy LoA 4 and 5b, the RA evaluation results from (1) Hypervisor and Virtual Machine sub-scopes and (2) all relevant Hypervisor maintained Virtual Machines and Application sub-scopes need to be available.