# ETSI GS NFV-SEC 020 V1.1.1 (2026-04)

**GROUP SPECIFICATION**

# Network Functions Virtualisation (NFV); Security; Identity Management and Security Specification



***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
DGS/NFV-SEC020

Keywords
NFV, security

***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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

***Important notice***

The present document can be downloaded from the
ETSI Search & Browse Standards application.

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 on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.



***Notice of disclaimer & limitation of liability***

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

***Copyright Notification***

# Contents

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.



# Foreword

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



# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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 specifies requirements for secure VNF identity management and trust relationships in NFV. The present document specifies how identities are securely lifecycle managed, verified and trusted. The present document addresses both horizontal and vertical relationships and leverages existing work in ETSI GR NFV-SEC 005 [i.1], ETSI GR NFV-SEC 007 [i.2], ETSI GS NFV-SEC 009 [i.3], ETSI GS NFV-SEC 012 [1] and ETSI GS NFV-SEC 013 [i.4].

# 2 References

## 2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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 necessary for the application of the present document.


[1] ETSI GS NFV-SEC 012: "Network Functions Virtualisation (NFV) Release 5; Security; System architecture specification for execution of sensitive NFV components".

[2] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[3] IETF RFC 9334: "Remote ATtestation procedureS (RATS) Architecture".

[4] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[5] IETF RFC 9711: "The Entity Attestation Token (EAT)".

[6] OpenID4VP: "OpenID for Verifiable Presentations".

[7] GlobalPlatform Card GPC_SPE_095: "Digital Letter of Approval".

[8] W3C® Recommendation: "Verifiable Credentials Data Model v2.0".

[9] OpenID4VCI: "OpenID for Verifiable Credential Issuance".

[10] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[11] DIF: "Presentation Exchange".

[12] IETF RFC 8414: "OAuth 2.0 Authorization Server Metadata".

[13] IETF RFC 7519: "JSON Web Token (JWT)".

[14] IETF RFC 7515: "JSON Web Signature (JWS)".

[15] IETF RFC 7516: "JSON Web Encryption (JWE)".

[16] IETF RFC 7517: "JSON Web Key (JWK)".

[17] SPIFFE Federation.

[18] ETSI GS NFV-SOL 003: "Network Functions Virtualisation (NFV) Release 5; Protocols and Data Models; RESTful protocols specification for the Or-Vnfm Reference Point".

## 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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI GR NFV-SEC 005: "Network Functions Virtualisation (NFV); Trust; Report on Certificate Management".

[i.2] ETSI GR NFV-SEC 007: "Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments".

[i.3] ETSI GS NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".

[i.4] ETSI GS NFV-SEC 013: "Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification".

[i.5] ETSI TR 119 460 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects".

[i.6] ENISA Remote ID proofing report /2021-03: "Remote ID proofing; Analysis of methods to carry out identity proofing remotely ".

[i.7] ETSI GR NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.8] FIPS PUB 199: "Standards for Security Categorization of Federal Information and Information Systems".

[i.9] Gartner: "Leading the IoT, Gartner Insights on How to Lead in a Connected World".

[i.10] FIPS PUB 202: "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions".

[i.11] NIST Special Publication 800-90A Revision 1.

[i.12] ETSI GS NFV-SEC 023: "Network Functions Virtualisation (NFV) Release 5; Security; Container Security Specification".

[i.13] ETSI GR NFV-SEC 018: "Network Functions Virtualisation (NFV); Security; Report on NFV Remote Attestation Architecture".

[i.14] IETF RFC 9901: "Selective Disclosure for JSON Web Tokens".



# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in ETSI GR NFV 003 [i.7] and the following apply:

**qualified attestation of attributes:** identity credentials as Verifiable Credentials including identity attributes that have been qualified and signed by a trusted provider, a qualified attestation of attributes provider

**qualified attestation of attributes provider:** trusted provider of qualified attestation of attributes

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR NFV 003 [i.7] and the following apply:

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| ABAC | Attribute-Based Access Control |
| AUTHN | Authentication process |
| AUTHZ | Authorization process |
| CIA | Confidentiality, Integrity, Availability |
| CSR | Certificate Signing Request |
| DLOA | Digital Letter of Approval |
| ID | Identity |
| PVID | Primary Verifiable Identity Document |
| RBAC | Role-Based Access Control |
| SM | Security Manager |
| VIP | Verifiable Identity Presentation |

# 4 Overview

## 4.1 Introduction



Identity (ID) is defined as "the fact of being who or what a person or thing is" and is usually used as a parameter to uniquely distinguish one being from a group of others.

In the realm of human society, where individuals are often unknown and untrusted, passports are relied on to establish our identities across the globe.

Passports are considered trustworthy documents because they are issued by governmental authorities, universally recognized as reliable and equipped with security features to ensure the integrity of the document.

A passport includes an identifier, the passport number, which indicates the country of issuance and a unique identifier for the individual. Additionally, it includes several attributes that inherently represent the person such as their first name, family name, photograph, a fingerprint, and other physical characteristics. These claimed attributes are verified by an authoritative body during the passport issuance process to confirm they correspond with the actual person. This is the proofing process. These attributes are utilized during the verification process to ascertain that the individual presenting the passport is indeed the person they claim to be.

Similarly in the realm of zero trust and distributed environments, such as NFV, entities shall substantiate their claims to establish trust. Each of these entities require an identity document akin to a passport, which should be trustable, interpretable and verifiable by all the entities that initiate communication with it.

Every element of a telecoms network and everything or person using the network needs an identity to determine the characteristics of that individual or component. For CSPs, the identity of NFVI components, SDN routing and VNFs are key to how CSPs design, manage and operate their networks.

Identities may be self-assigned, given, inherited, derived, acquired, allocated or obtained in a large number of ways.

If an attacker obtains access to a CSP network implemented with NFV then it needs to be possible, even months after the event, to retrace the attack to establish where they got into the network, what was accessed, for how long and, as far as possible, what identity they used to achieve this access. Similarly, if a customer reports a fault it needs to be possible to trace their current and past usage of services to resolve the issue.

Therefore, in an NFV environment, it needs to be possible for identities to be trusted, structured, unique, and immutable for a given period, if networks are to be operated securely and with a low risk of fraud.

The present document describes secure identity management in the context of NFV, in terms of what an identity is, what that identity is used for, how it is assigned, how it is discovered and how it is securely managed throughout the lifecycle of that identity.

## 4.2 Identity Definition Purposes and Uses of Identity

The present document defines an ID structure that vertically spans the NFV domain and the application domain above it. Information from both domains is necessary to implement effective, real-world security policies. The ID will contain information about both the TYPE and INSTANCE of a software process. The information about the TYPE of a running INSTANCE, which is available in a higher trust domain, shall not be available in any lower trust domain. Further, information about the TYPE of a running INSTANCE available in any trust domain shall not be available in any other trust domain of equal sensitivity, unless the process in the source trust domain explicitly intends it, as expressed in the appropriate security policies.

Identity is the foundation of networks, it enables distinction among individual instances and individual types, discovery of suitable partners of a process, attachment to such partners once discovered, and, as it is also the foundation of security, identity enables the assignment, tracking and evolution of trust.

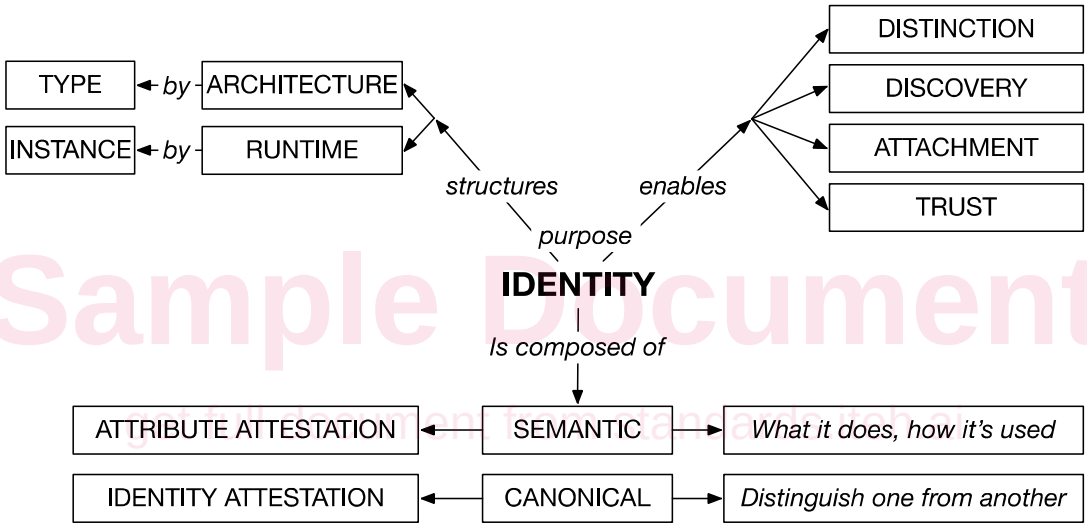


**Figure 4.2-1: Purposes and Uses of Identity**

There are two basic flavours of identity in a network: TYPE identity, through which architecture is structured, and INSTANCE identity, through which the runtime is structured.

Identity enables the development of ontologies, allowing the systems designer to make statements about an object's capabilities and uses, and based on this, allows the implementer to distinguish, manage and secure runtime instantiations of said objects.

A person's passport identifies them with a globally unique identifier, primarily defined by the passport number. It also contains information about the issuing country, allowing the assessment of trust and identifying the structure of the passport.

Similarly, an identity document for an entity in the virtualized world should possess a globally unique identifier, that includes:

- information about the issuing system (e.g. NFV system), allowing the identification of the scheme used for this identity;
- the trust domain associated with the entity; and
- a unique identifier.

This globally unique identifier is the canonical identity of figure 4.3-1, distinguishing one entity from another.

A person's passport includes attributes inherent to the person's identity verified during the proofing process before issuance. These attributes are crucial for confirming the person's identity during passport presentation, verification of fingerprint, picture, and physical characteristics such as eyes colour, height.

In the same way, an identity document for virtualized entities should include attributes inherent to the entity's identity, such as:

- Entity name (e.g. the 3GPP name of a virtual function)
- Hash of the software image
- Attestation result
- Trust domain where it is instantiated
- Identity of the NFV-MANO, and the NFVI that instantiate the entity
- ContainerID where it is instantiated
- Timestamp of instantiation
- Location instantiation
- Etc.

The list of attributes could depend on the service provider and the trust domain, as per policies.

These attributes shall undergo verification by a trusted authority during a proofing process which is synonymous with the attestation process.

Attributes, as described, correspond to the semantic identity outlined in figure 4.3-1, defining the entity's functionality and usage.



## 4.3 Hierarchy



IDs have usage and meaning that span domains. Figure 4.3-1 depicts the main elements that share usage and meaning of IDs in the larger context in which NFV exists. While the figure shows the relationships, the details of the actual interfaces themselves are outside the scope of the present document.

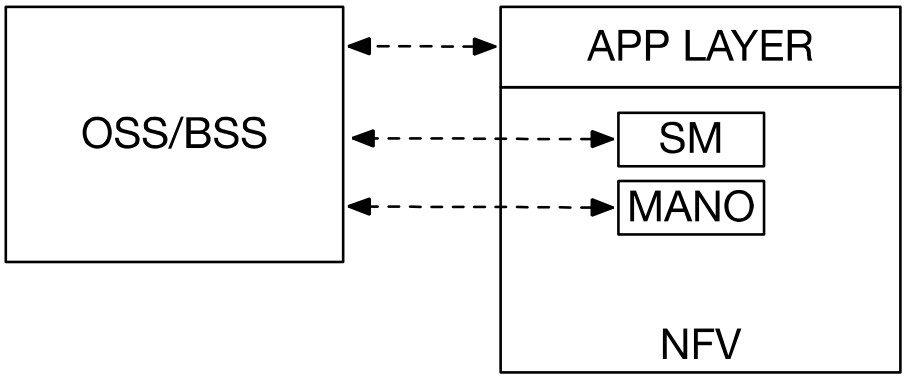


**Figure 4.3-1: NFV Context**

Operations Support Systems (OSS) and Business Support Systems (BSS) have existed, and will continue to exist, outside the NFV domain but are also intricately linked with the operation of virtualised functions. As described in the present document, some interaction will have to exist between the relationship of the OSS/BSS and the application layer function (e.g. 3GPP NF) implemented using NFV, with the relationships between OSS/BSS and both the Security Manager (SM) and MANO. The interaction, whether automated or manual, is intended to bridge the gap between the NFV infrastructure and the application layer.

The VNF instance communicates with entities at these different levels and may have different identity attributes for these different levels, even if these attributes are associated to the same VNF instance.

In the context of identity of human, depending on the domain where the identity of a person is used, the attributes presented could change. For example, an alumni could present his diploma as attribute, with the date of issuance, when he presents himself for a job. But in the context of health care, he will present an identity containing its identifier for the health care service.

In the same way, the identity of the virtual entity may include attributes that are relevant for the domain where the identity is used. For example, the identity of a VNF instance at the NFV level, communicating with the VNFM may include some attributes (e.g. role of the VNF) that are relevant at this level. The same VNF communicating with another VNF at 3GPP level may include other attributes such as the name of the VNF at 3GPP level and its role at 3GPP level.

Some attributes could be useful for both levels. This is the case for example of attestation result that is relevant at NFV level but also at 3GPP level to enable the trust.

The identity management of the VNF instance shall allow the bridge between NFV infrastructure and application layer, that could be 3GPP but also other application context.

# 5 Identity-Related Concepts and Definitions



## 5.1 General



### 5.1.1 TYPE and INSTANCE

The present document defines the software package TYPE category, which describes the particular functions a package is capable of fulfilling at the application layer (e.g. a firewall, a 3GPP-defined Serving Call Session Control Function (S-CSCF), etc.), and the VNF INSTANCE category, which identifies the running instance of a VNF and/or its component software process.

### 5.1.2 Lifecycle Events

Further, the present document defines two events in the lifetime of a software package: the ON-BOARDING event, when a software package is received from the vendor and is added to the software catalogue of the CSP, and the run-time events of INSTANTIATION, MODIFICATION, and TERMINATION, when the VNFI is executed, modified, and terminated, respectively.

### 5.1.3 Confidentiality, Integrity, and Availability

The US National Institute of Standards and Technology (NIST) in FIPS Publication 199 [i.8] defines the Confidentiality/Integrity/Availability (CIA) model, which defines LOW/MODERATE/HIGH impact to each of the three dimensions. This model has been adopted for the present document. The attributes can be applied at both ON-BOARDING time, to the TYPE of a package, and at INSTANTIATION time, to the running INSTANCE of the package.

For the purposes of the present document, the same three levels are defined (LOW, MODERATE, and HIGH) for each of the three dimensions. While all three dimensions play into ID management, the present document concentrates on the Confidentiality dimension. At the discretion of the CSP, the NFV system shall operate with at least two of the three confidentiality levels, with the Security Manager assigned to the higher confidentiality level of the two, and MANO assigned to the lower level of the two. If the CSP elects to implement all three levels, the SM shall be assigned to the HIGH confidentiality level, and MANO shall be assigned to the LOW confidentiality level.

For the purposes of the present document, the Availability dimension is expanded to encompass not only Availability but also Authorization and Authentication. Again, the same three levels are defined for these.

### 5.1.4 Trust Domains

A trust domain is defined as a set of processes running at the same sensitivity level due to the application of a common set of security policies. The CSP shall manage the flow of information across trust domains in such a way that information and attributes of a higher sensitivity trust domain shall not transfer to a lower sensitivity trust domain.

There may exist many separate trust domains of the same sensitivity level, but information contained in each is not necessarily available from any other. For example, administrators given access to the HIGH sensitivity level in one trust domain will not necessarily have access to another trust domain of HIGH sensitivity level, as dictated by the need-to-know principle. When the present document refers to a "HIGH trust zone", it is always to be read as meaning a HIGH confidentiality trust zone, unless the other two attributes are used explicitly. A consequence of this requirement is that data needs to be labelled as exportable or non-exportable.

Implementing an access control system shall be mandatory. As described in ETSI GS NFV-SEC 012 [1], security maintenance has finer granularity under the implementation of Attribute-Based Access Control (ABAC), rather than the simpler Role-Based Access Control (RBAC). A difference between the two is that ABAC also takes into consideration the context (e.g. time-of-day access restrictions to certain resources) of a resource access event, not only the accessor and the resource itself. ABAC is comparable to concepts used in multi-factor authentication, RBAC is comparable to concepts used in single-factor authentication. Segregating access to a trust domain is therefore more robust under ABAC.

# 6 Management and Structure of Identity



## 6.1 Introduction - Purpose of Identity

The purpose of VNF instance identity is to uniquely identify the VNF instance and prove that the VNF instance is really what it claims to be.



A VNF instance identity has several usages:

- **Distinction:** A same program may be deployed and scale out to a large number of nodes, in different locations, within different infrastructures and may be updated with a new version. It is also associated with an issuing authority that manages it. The identity of the workload shall enable this distinction. A mechanism to ensure the uniqueness of identity across the CSP system at any given time shall be employed.
- **Discovery:** Once identities are issued for the workloads, they can be used for the discovery of the services in a catalogue, after their registration.
- **Authentication:** Identities can be used for authentication, proving that the service is what it claims to be, and enabling establishment of secure communication with it.
- **Authorization:** Once the services have authenticated to each other, they can control access to their services and data.
- **Confidentiality:** After authentication, a secure communication may be established between the services enabling the data exchanged being kept secret.
- **Trust:** The identity document issued for the service shall be trustworthy: issued by a trusted authority after a proofing process, verifiable, and containing attributes that can be checked at the authentication or authorization time.

This clause defines the two fundamental components of the Identity management:

- The Identifier: a decentralized unique identifier of the VNF instance.
- The Verifiable Identity document: a passport for the VNF instance, that carries the Identity.

The Verifiable Identity document shall be resistant to forgery and contain information that proves that it belongs to the VNF instance that presents it, and that proves its authenticity. In addition, this Verifiable Identity document supports verification of various identity attributes of the VNF instance that have been determined during the proofing process (i.e. attestation). The simple presentation of this Verifiable Identity document gives the relevant identity information to the other party, enabling the trust.

## 6.2 Structure of Identity

### 6.2.1 Introduction

The identity of a VNF/VNFC instance shall be uniquely defined and shall identify the instance across heterogeneous environments and organizations, within a global scope and shall be interpretable consistently regardless the context. Therefore, the NFV identity of the VNF instance shall be defined as a Uniform Resource Identifier (URI) as defined by IETF RFC 3986 [2].

### 6.2.2 Scheme

The scheme name defined for the URI of NFV instance identifiers, that refers to the present document is the following:

Scheme: nfvid

NOTE: The present document defines a specific scheme name for NFV, which is to be registered with IANA. It is possible to use a scheme name already defined and used in the cloud environment if it satisfies the requirements for identity management: example: "spiffe" identity name space.

### 6.2.3 Authority



In the context of a URI the authority identifies the domains. To avoid collisions in the identifiers and be able to identify the system in which the identity has been issued, the trust domain is included in the URI as a hierarchical element. With this hierarchical element, the remainder of the URI is delegated to the authority managing this trust domain.



The trust domain is a trust root of the system and is defined by the service provider, owner of the VNF instance. There could be a trust domain for e.g. operational or test instance. This trust domain name is self-registered by the service provider. There is no centralized authority for the registration of these trust domain names. To prevent collisions the service provider shall select the trust domain name that is highly likely to be globally unique (e.g. adding a service provider DNS name as a suffix of the trust domain name or using a randomly generated name such as UUID).

The trust domain is defined as the authority component of the URI where only the host part is present.

### 6.2.4 Path

The path component is used to uniquely identify a VNF instance within the scope of the "nfvid" scheme and the trust domain controlled by the service provider. The path definition is left open to the service provider. Path may be hierarchical with e.g. the name of the network service which the VNF instance is part of, the name of the VNF instance (e.g. udm) and the last path segment shall be the vnfInstanceID as defined in ETSI GS NFV-SOL 003 [18], which is an individual path segment, and issued during the creation of a VNF instance.

Example of an identity:

nfvId://test.operator.com/vnfInstanceId

NOTE 1: How the vnfcInstanceID is incorporated into the scheme is for future study.

NOTE 2: Some information contained in the VnfInfo could be used for an automatic identification of the VNF instance: e.g. vnfInstanceName, vnfProductName, or specific data in the metadata element. How this can be incorporated is for future study.

## 6.3 Properties and Attributes of Identity

### 6.3.1 Introduction

The VNF/VNFC instances have some properties or attributes that could be used as identity attributes.

Some of these attributes inherently identify the VNF/VNFC instance, some other attributes are identity attributes applicable to some context and have a meaning within this context only (e.g. the 3GPP entity name that has a meaning at the 3GPP layer only).

Attributes that inherently identify the VNF/VNFC instance are attributes that could be verified to prove that the VNF/VNFC instance is really what it claims to be. These attributes could be verified during a proofing process, an attestation process, before the issuance of the Identity document to the VNF/VNFC instance. The attestation verification is done by an authoritative entity in the trust domain of the VNF/VNFC instance. The Security Manager (SM) of the trust domain may include the attestation verification and identity management. The choice of attributes used to inherently identify the VNF/VNFC instance is controlled by the CSP associated with this trust domain and are further called selectors. These selectors are part of policies that could be registered in the SM during a registration process of the VNF at the time of instantiation.

The selectors included in the policies depend on the use case and the service provider. For example:

- Some simple use-cases could restrict the list of selectors to the software integrity attestation as described in ETSI GS NFV-SEC 023 [i.12], clause 6.5.1.4.
- Some use cases could use HMEE Attestation and additional selectors as instantiation locstamp: e.g. Lawful Interception.

## 6.3.2 Attributes bound to Identity

Table 6.3.2-1 lists potential attributes bound to identity that shall be able to be cryptographically bound to the identity. Some attributes are fixed upon the receipt of the VNF package from the vendor, end of testing, on-boarding of a package received from the vendor to the CSP catalogue, some other attributes are fixed upon the completion of the launch procedure of a VNF instance.

**Table 6.3.2-1: List of potential attributes bound to identity**

| Attribute | Description | Fixed upon | Trust source of information | Comments | Use-case |
|---|---|---|---|---|---|
| | **Attributes that could be included in the Identity URI as hierarchical paths** | | | | |
| Manufacturer | | Package on-boarding | VnfInfo/SM | | |
| ProductName | | Package on-boarding | VnfInfo/SM | | |
| Version | | Package on-boarding | VnfInfo/SM | | |
| | **Inherent Identity Attributes for proofing process** | | | | |
| Integrity Attestation | | Instantiation | Attestor | See ETSI GS NFV-SEC 023 [i.12], clause 6.5.1.4) | |
| HMEEAttestation | | Instantiation | Quoting enclave/Attestor | | LI |
| Run-time Attestation | | | Attestor | | |
| Instantiation locstamp | | Instantiation | | | LI |
| Instantiation timestamp | | Instantiation | | | |
| LoA | | | | (1, 2, 3, 4, 5a, 5b - see ETSI GR NFV-SEC 007 [i.2], clause 5) | |
| MANO IDs | Identification of MANO function instances (e.g. NFVO, VNFM, VIM) which effected the launch | Instantiation | | | |
| Security domain/namespace | | Instantiation | | | |
| CGroup | | Instantiation | | | |
| ContainerID | | Instantiation | | | |