ETSI GS NFV-SEC 006 V1.1.1 (2016-04)

Network Functions Virtualisation (NFV);
Security Guide;
Report on Security Aspects and Regulatory Concerns

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-SEC006

Keywords
NFV, regulation, 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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 7
4 Security design guide 8
4.1 Overview and introduction 8
4.2 Risk, risk analysis, and risk management 9
4.3 Design for assurance 10
4.4 Secure by default 12
4.5 Domain of Attack model 12
4.6 Regulatory and conformance issues 13
4.7 Interoperability considerations 13
4.7.1 Syntactic interoperability 13
4.7.2 Semantic interoperability 13
4.7.3 Electrical and mechanical interoperability 14
4.7.4 Radio communication interoperability 14
Annex A (informative): Pro forma of Security and Regulatory Concerns for use in ETSI ISG NFV GSs 15
A.1 Risk analysis and assessment 15
A.2 Countermeasure deployment 16
A.2.1 Identity management 16
A.2.2 Integrity protection and verification 16
A.2.3 Confidentiality 16
A.2.4 Availability and resilience 16
A.2.5 Trust framework 16
A.3 Regulatory conformance 17
A.3.0 Introduction 17
A.3.1 Data protection and Privacy 17
A.3.2 Retention of Data 22
A.3.3 Lawful Interception 22
A.3.4 Export control of cryptographic material 22
A.3.5 Others 23
Annex B (informative): Summary of attack vectors as applied in NFV 24
B.1 Interception attacks 24
B.2 Manipulation attacks 24
B.3 Identity based attacks 24
Annex C (informative): Cryptographic measures for NFV protection 25
C.1 Cardinality of relationships 25
C.2 Algorithm selection and key size 25
Annex D (informative): Bibliography 27

Annex E (informative): Authors & contributors.....28
History.....29

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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.

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 is a guide to developers of NFV related documents and applications in means to address the security aspects and regulatory concerns as they impact the security of deployed networks that conform with these documents and applications. The present document contains detailed descriptions of security concerns, attacks, as well as an overview of regulatory concerns and how they can be treated in system design to give the highest level of assurance that the resultant system is secure and complies with current regulation and best practice. The present document is intended for use by developers of NFV documents and the guidance is given in a manner that assists non-experts in security and regulation to prepare such documents.

In addition to the guidance and explanatory text the present document contains, in annex A, a pro forma template for use in ETSI ISG NFV documents to capture the security concerns and mitigations that apply.

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 at http://docbox.etsi.org/Reference.

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.

Not applicable.

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 TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.2] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.3] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.4] Privacy Impact Assessment Handbook (2009).

NOTE: Available at http://www.piawatch.eu/node/48.

[i.5] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.6] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

[i.7] Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (recast) (Text with EEA relevance).

[i.8] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance).

NOTE: Available at http://eur-lex.europa.eu/

[i.9] ETSI GS NFV-SEC 004: "Network Functions Virtualisation (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implication".

[i.10] ETSI GS NFV-SEC 010: "Network Functions Virtualisation (NFV); NFV Security; Report on Retained Data problem statement and requirements".

[i.11] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[i.12] UK Information Commissioners Office: Conducting Privacy Impact Assessments Code of Practice.

NOTE: Available at https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

[i.13] ETSI ETR 332:"Security Techniques Advisory Group (STAG); Security requirements capture".

[i.14] ETSI ES 202 383: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets".

[i.15] ETSI ES 202 382: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".

[i.16] Domains of Attack list and descriptions.

NOTE: Available at http://www.mitre.org. Please consult this website for detailed descriptions of each attack: http://capec.mitre.org/data/graphs/3000.html.

[i.17] IEC 60906-2: "IEC system of plugs and socket-outlets for household and similar purposes - Part 2: Plugs and socket-outlets 15 A 125 V a.c. and 20 A 125 V a.c.".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TS 102 165-1 [i.1] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 102 165-1 [i.1] and the following apply:

PP Protection Profile
TVRA Threat Vulnerability Risk Analysis

4 Security design guide

4.1 Overview and introduction

Security cannot be an afterthought, and has to be considered throughout the planning/development/deployment/runtime lifecycle. Unfortunately, effective security design is not trivial and there is a constant tension between functionality and security that inherently couples the two. A significant danger is that in progressing functionality it will become harder and harder to provide deeply rooted security in system designs. As with design of any type there are a number of ways to approach security in system design. The primary starting point in much of security is to identify an attack and pair it with a means to thwart the attack, such that a tuple of {issue, mitigation} will exist across the system.

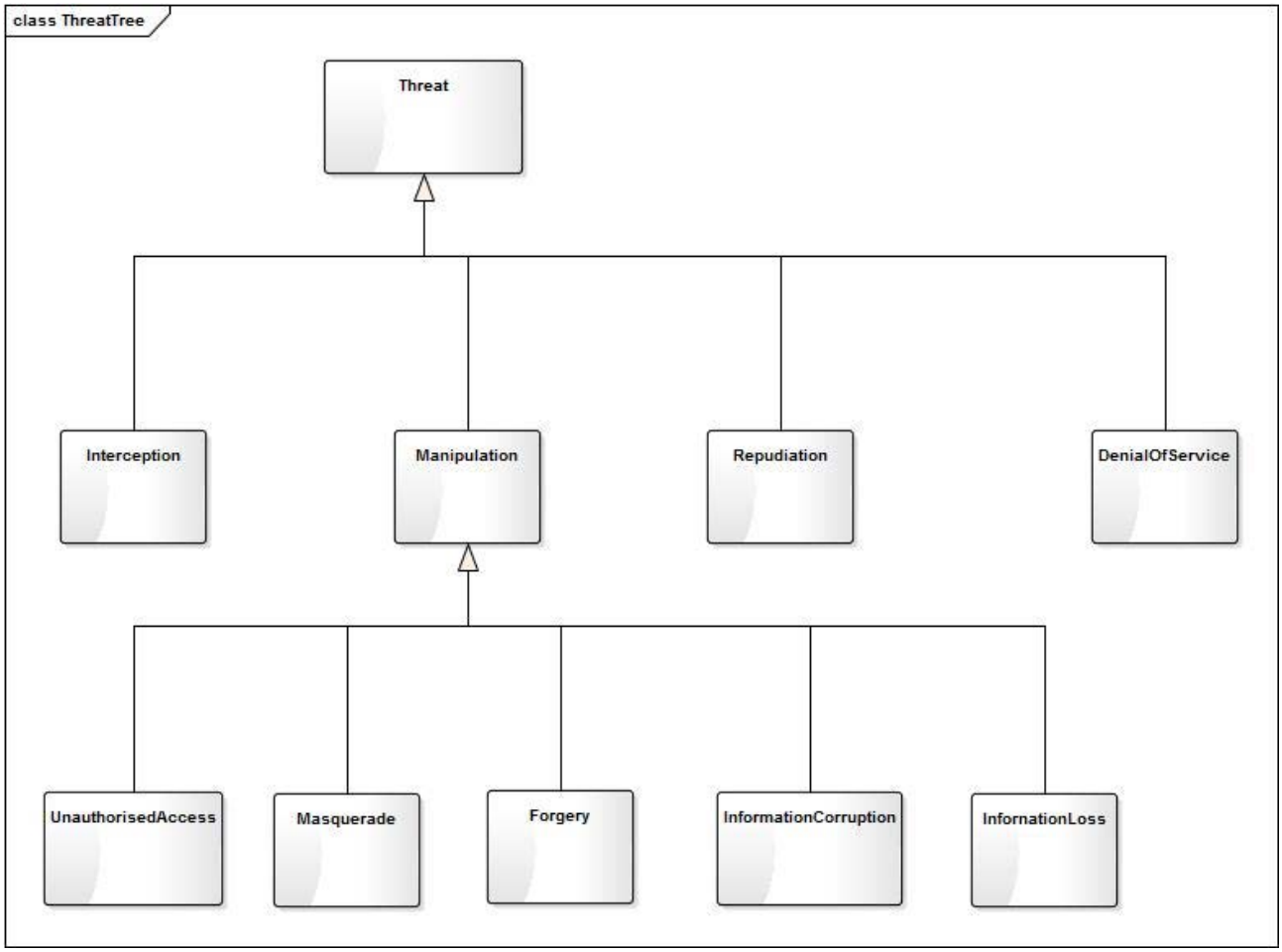

Figure 1: Illustration of a threat tree to identify forms of threat in systems

Whilst an understanding of threat trees (see figure 1) is useful it is not sufficient and has to be mapped to a wider understanding of countermeasures. For example the tuple {masquerade, authentication} suggest that if the authentication element is implemented properly it will counter masquerade, but the pre-requisites of authentication include identity management and credential management. If authentication is a cryptographic process further issues arise that include the viability of the authentication algorithms over time (and associated cryptographic strength), the means to distribute credentials (the pairing of identity and the cryptographically significant data used to assert it), and so forth.

In the regulatory domain the mind-map shown in figure 2 identifies some of the relationships between protection technology and attack types, and the relationship between privacy and regulation is highlighted. The latter is important as regulation exists to protect the obligation or right to privacy as identified in a number of acts and laws, however there are a number of exceptions to the right to privacy identified by the same broad set of acts and laws that generally give rights for law enforcement to have reasonable rights to protect the wider population sometimes with a short term risk to the individual. Such exceptions include the need to provide for Lawful Interception, and to retain data in the network in support of law enforcement.

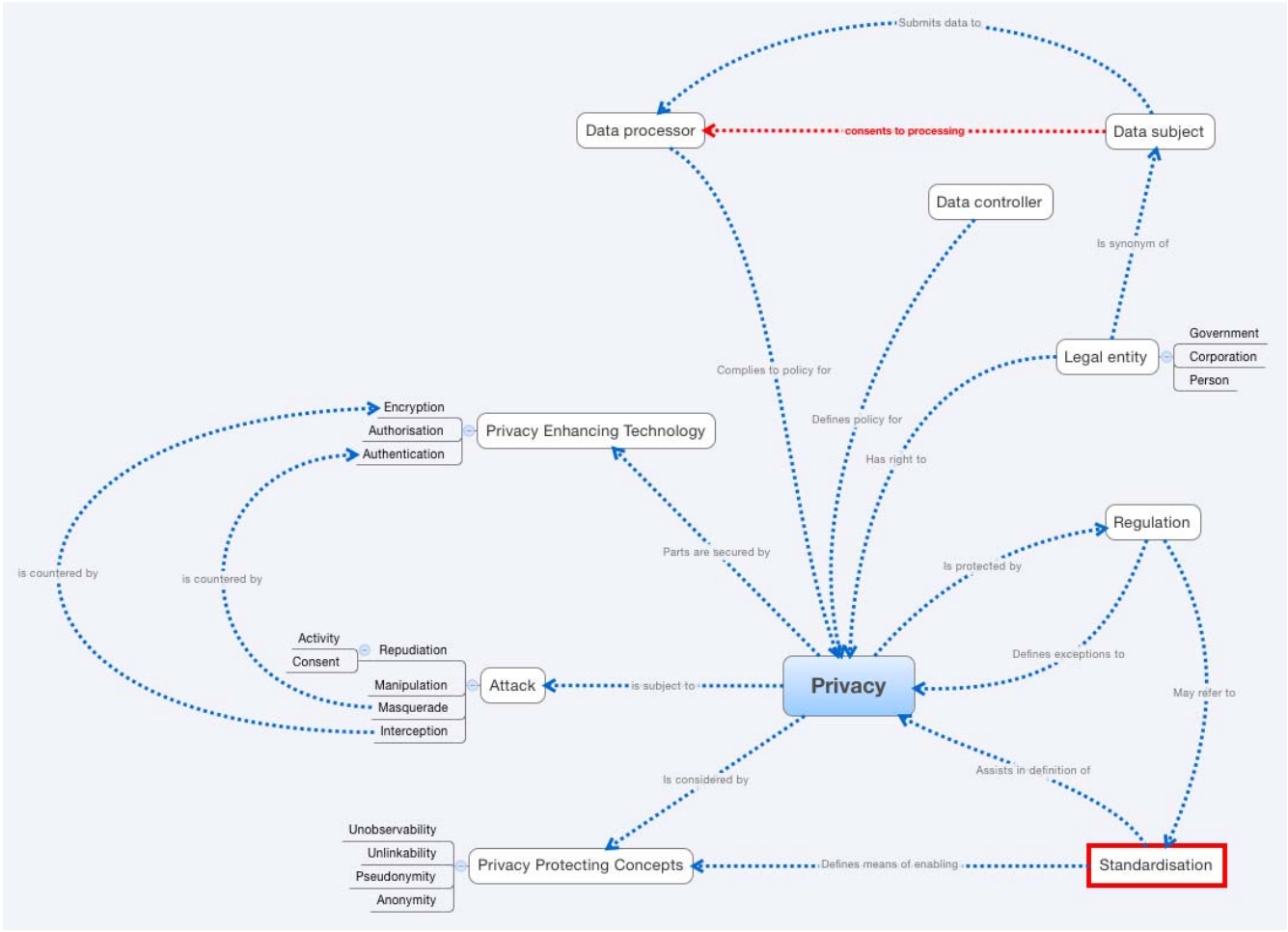

Figure 2: Mind-map illustrating complexity of privacy and privacy protection

In designing a secure system an understanding of the impact of attack has to be developed. For example, when two functions share a host, a Denial of Service attack on one may affect the other. The mitigation may be to not co-host high-priority functions with low-priority functions.

4.2 Risk, risk analysis, and risk management

Designing for the effective security of a system cannot be done without a reasonable understanding of risk, there are a large number ways of modelling security in systems that look variously at the process (Identify, Mitigate, Monitor as a continuous loop), and at the interactions of assets. The model given in ETSI TS 102 165-1 [i.1] and copied below makes a number of assumptions including:

- systems are compositions of a set of assets;
- assets may have inherent vulnerabilities;
- a vulnerability when discovered with a viable threat becomes a weakness;
- exploitation of a weakness leads to something unwanted in the system (unwanted incident); and,
- threat agents are used to enact threats and many threat agents may work together to exploit a weakness.

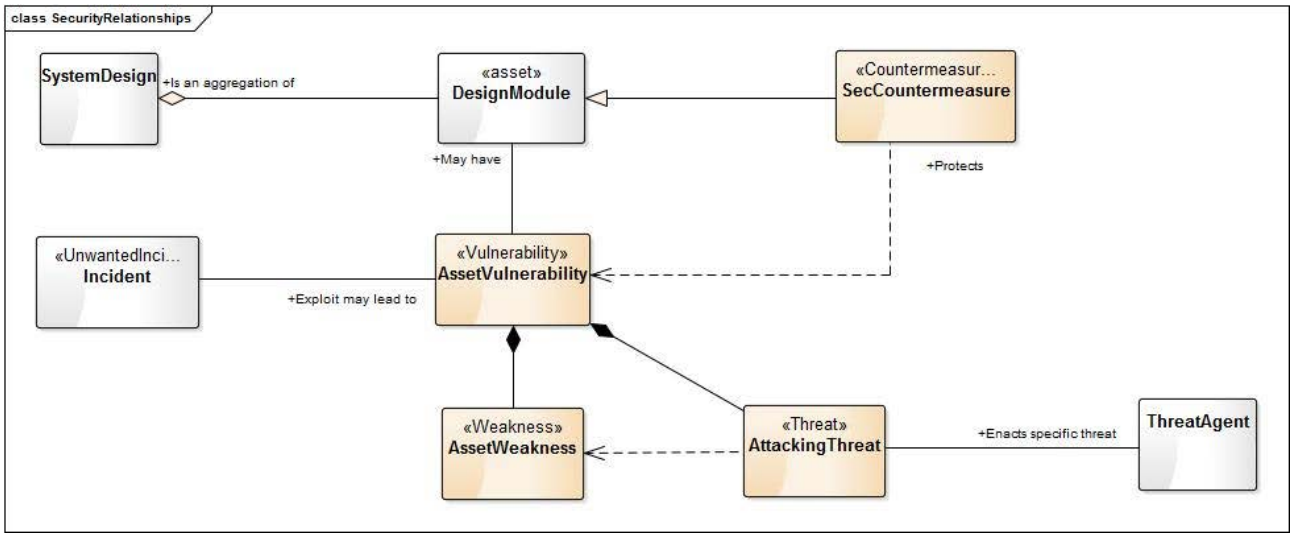

Figure 3: Generic security TVRA model from ETSI TS 102 165-1 [i.1]

There are a number of questions that arise from the generic model shown in figure 3 and these include:

- What are the assets of my system?
- How do I determine the vulnerabilities and when they become exploitable weaknesses?
- How do I protect my system?

The present document is part of the process in the identification of assets and their vulnerabilities by recommending a set of topics to be considered in every deliverable of ISG NFV.

Threats are potential events that can cause a system to respond in an unexpected or damaging way. It is useful to categorize threats to determine effective and deployable mitigation strategies. The identification and analysis of NFV relevant security threats (general and application specific) should include the following categories:

- Spoofing of identity (masquerade).
- Tampering with data (manipulation).
- Inappropriate information disclosure.
- Denial of service.
- Improper elevation of privileges.

Clauses 4.3 and 4.4 describe a number of strategies for identifying the threats in general terms in the NFV context.

4.3 Design for assurance

The Design for Assurance paradigm is closely aligned to the design for test paradigm. The aim of these paradigms is to ensure that when designing a system an independent tester can validate that the system actually performs to the design specification. The primary difference between design for test and design for assurance is that in the latter there are specific security claims that are being made and verified.

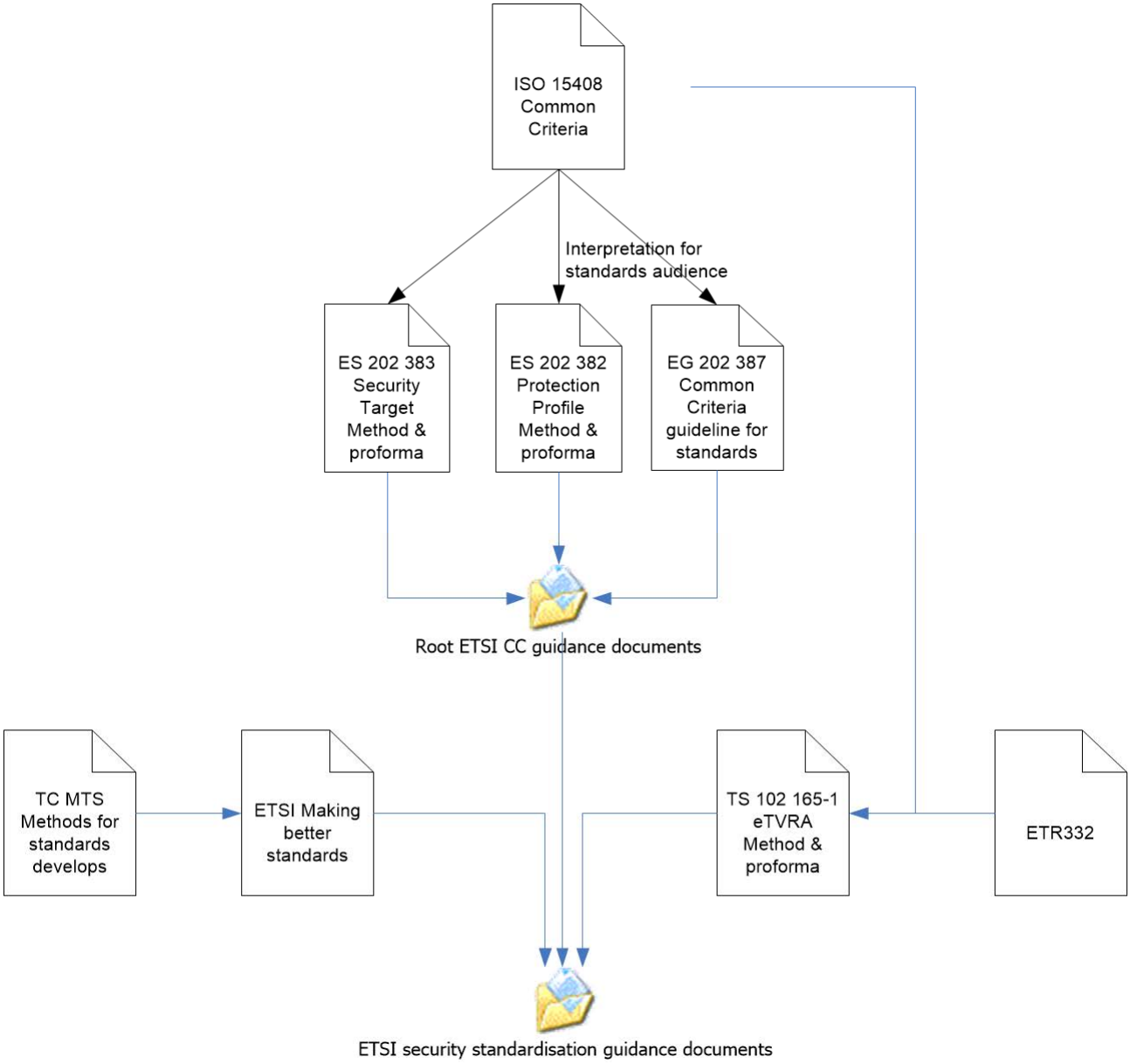

Figure 4: ETSI's Design for Assurance document suite

The core aspects of Design for Assurance are as follows: to identify the assets of the system and through a risk analysis (identified by method in ETSI TS 102 165-1 [i.1]); Identify the security architecture and functionality to eliminate critical risks and to substantially reduce the number of major risks; Reassess the risk with the assets required for risk reduction and management; repeat. In this approach Design for Assurance is thus not very far removed from any other good design practice - the core difference is that in defining a security measure there is a clear path to its justification and thus a rationale for its presence which is interpreted as a claim for the security assurance it delivers. Thus if the concern is interception across a broadcast medium (e.g. a radio link) the attack model will be expected to show the likelihood of an attacker making the interception and the impact of that attack, then in applying (say) encryption to the link it will show how the likelihood of interception or the impact of an interception modifies the risk to the user and the system. The model will also show how the countermeasure (i.e. encryption in this case) modifies the system and what, if any, new risks are introduced. This then gives a measure of the cost benefit of the provision of encryption technology and the level of increased protection in such a way that it can be, if necessary, independently validated.

There are a number of major players in the design for assurance domain and ETSI, as shown in figure 4, has developed its guidance from the Common Criteria (ISO/IEC 15408-2 [i.2] and ISO/IEC 15408-1 [i.3]) and incorporated many of the key points into the "Making Better Standards" guidance published by ETSI CTI with support from ETSI TC MTS. Since the original publication of this guidance the Common Criteria experts groups have recommended a change in approach that is more closely aligned to the approach taken by ETSI with the adoption of a principle of Community Protection Profiles (cPPs) to be developed by industry experts in a similar way to standards.

4.4 Secure by default

The secure by default initiative documented in ETSI TR 103 309 [i.5] is a philosophy in which real business problems are identified and security solutions to the problems are solved at root cause, rather than by applying patches or 'stop-gap' measures to address particular issues. The emphasis is therefore on security mechanisms embedded in core device functions; supplied literally 'by default' in products instead of being added afterwards via updates or complex configuration. It is considered that an understanding of the Domain of Attack model described in clause 4.5, the appreciation of risk described in clause 4.2, and the concept of security assurance described in clause 4.3, when taken together and applied before a system is deployed are major components and strategies that support Secure by default.

New features of this nature require fundamental changes to devices, hence development can take time. Promoting adoption may require that technical solutions be identified when they are still maturing; prototypes exist to verify the concept, however market support is required in order to justify investment in refining a product.

Finally, it is clear that simply developing technical components is almost never sufficient to solve problems in the real world. Practical guidance is needed to ensure these components can be integrated appropriately into deployed systems. As well as identifying technologies, it is necessary to point out relevant good practice guidance where it exists. This has to include the Human element as very often a technically sound and secure system is made irrelevant if a door is left open by a disgruntled or forgetful employee.

4.5 Domain of Attack model

The domain of attack model [i.16] is simple in theory and divides attack vectors into sets:

- Social Engineering:
  - The manipulation and exploitation of people to attack the system or to gather information about the system and its operation in order to perform future attacks. In most cases the adversary never comes face-to-face with the victim.
- Supply Chain:
  - Everything and anything brought into the system is part of the supply chain. The supply chain has to be trusted sufficiently that when an asset is introduced to the system it can be trusted to work. This requires understanding of not just software and hardware products, but wider issues of distribution, support, tools and so forth. Failures in the supply chain, or attacks introduced through the supply chain, have to be considered in the general security model and means to give supply chain assurance and validation defined.
- Communications:
  - The model of establishment of communication between 2 parties has to meet certain goals of confidentiality, availability and authenticity. Attacks against communication may attack the confidentiality by intercepting the communication, or attack the availability by disturbing the protocol in some way.
- Software:
  - Software is the backbone of the ISG NFV and software is one of the assets of the system that tends to exhibit a number of core vulnerabilities that when exploited lead to a number of forms of unwanted incident. The set of checks against software design to mitigate potential vulnerabilities are extensive and form the core of the checklist of the present document. Attack vectors will also often be software based and may attack on multiple paths including through operating systems, programming languages and their associated compile and link facilities.
- Physical Security:
  - Often refers to the premises and to access control for the installed NFV hardware.
- Hardware:
  - Breaking the hardware will break the NFV and anything built on it.

As the ISG NFV initiative involves hardware, software and communications this checklist of attack vectors is a useful tool to verify that all reasonable steps have been taken in managing the security and privacy risks.

4.6 Regulatory and conformance issues

Security measures often have to be implemented to give assurance of conformance to regulation. In security there are a number of regulations and restrictions that have to be borne in mind and these include (the list is indicative as national legislation may extend the items that an NFV user/deployer may have to show conformance to):

- Lawful Interception.
- Data protection.
- Privacy protection.
- Retention of data.
- Export controls of dual use technologies (i.e. cryptographic material including algorithms).

Of these issues a number of concerns arise that require particular care in defining the security solution. For LI there is a clear need for unobservability of the LI measure by unauthorised parties and this requires a multi-tier security system. For data protection and privacy protection the current legislation identifies roles of data controller and data processor in the system with explicit responsibilities to manage the processing of private data (and by inference Personal Identifying Information) with rules for accountability and for non-repudiation implicit in the requirements.

Much of the regulatory domain and the necessary compliance is non-technical in nature although in some cases conformance to cited standards is required. This is especially true for radio devices (as part of the Radio Equipment Directive [i.6]) and for certain electrical equipment (the CE marking) and for medical device (including software) marking.

NOTE: In general regulatory compliance does not recognize details of implementation such that if a feature is subject to regulation it does not matter if the feature is implemented using virtualisation or in some other manner.

4.7 Interoperability considerations

4.7.1 Syntactic interoperability

Syntax derives from the Greek word meaning ordering and arrangement. The sentence structure of subject-verb-object is a simple example of syntax, and generally in formal language syntax is the set of rules that allows a well formed expression to be formed from a fundamental set of symbols. In computing science syntax refers to the normative structure of data. In order to achieve syntactic interoperability there has to be a shared understanding of the symbol set and of the ordering of symbols. In any language the dictionary of symbols is restricted, thus in general a verb should not be misconstrued as a noun for example (although there are particularly glaring examples of misuse that have become normal use, e.g. the use of "medal" as a verb wherein the conventional text "He won a medal" has now been abused as "He medalled").

4.7.2 Semantic interoperability

Syntax cannot convey meaning and this is where semantics is introduced. Semantics derives meaning from syntactically correct statements. Semantic understanding itself is dependent on both pragmatics and context. There are a number of ways of exchanging semantic information although the success is dependent on structuring data to optimize the availability of semantic content and the transfer of contextual knowledge (although the transfer of pragmatics is less clear). Semantic interoperability is very difficult to add to a system that has not been initialized with it as

The problem that semantic interoperability attempts to solve is that of given an identifier what deterministic action should be taken (given the VNV-I's present state and any inputs, there should be only one possible action that the VNF-I takes). Semantic interoperability also provides greater richness and thus accuracy of identity of any object in the wider NFV environment.

4.7.3 Electrical and mechanical interoperability

Quite simply a device with a power connector using, for example, a Type-A IEC 60906-2 connection (USA power connector) cannot accept power from anything other than a IEC 60906-2 conforming source [i.17]. Similarly, for example, a serial port complying to USB-Type-A will not be able to connect with a USB-Type-C lead. In addition to simple mechanical compatibility there is a requirement to ensure electrical interoperability covering amongst others the voltage level, amperage level, DC or AC, frequency if AC, variation levels and so forth.

4.7.4 Radio communication interoperability

The Radio Equipment Directive 2014/53/EU [i.6] applies to any equipment that contains a radio module. The scope of the Directive is such that the entire equipment containing the radio is required to undergo conformance testing (not just the radio module) and details can be found in the RED [i.6] and in accompanying material [i.7] and [i.8].

NOTE: The RED [i.6] currently applies to equipment sold within the CEPT region, i.e. Europe, but may be extended globally.

Annex A (informative): Pro forma of Security and Regulatory Concerns for use in ETSI ISG NFV GSs

A.1 Risk analysis and assessment

A Security Environment			
a.1 Assumptions			
a.1.1	*Text of assumption*		*Citation for full text*
a.1.2			
GUIDANCE: *to be added by reference to ETSI TS 102 165-1*			
a.2 Assets			
a.2.1	*Short text describing asset*		*Citation for full text*
a.2.2			
a.3 Threat agents			
a.3.1	*Short text describing threat agent*		*Citation for full text*
a.3.2			
a.4 Threats			
a.4.1	*Short text describing threat*		*Citation for full text*
a.4.2			
a.5 Security policies (OPTIONAL)			
a.5.1	*Short text describing security policy*		*Citation for full text*
a.5.2			
B Security Objectives			
b.1 Security objectives for the asset			
b.1.1	*Short text describing objective for the asset*		*Citation for full text*
b.1.2			
b.2 Security objectives for the environment			
b.2.1	*Short text describing objective for the requirement*		*Citation for full text*
b.2.2			
C IT Security Requirements			
c.1 asset security requirements			
c.1.1 asset security functional requirements			
c.1.1.1	*Short text describing security functional requirement*	*ISO15408 class*	*Citation for full text*
c.1.1.2			
c.1.2 asset security assurance requirements			
c.1.2.1	*Short text describing security assurance requirement*	*ISO15408 class*	*Citation for full text*
c.1.2.2			
c.2 Environment security requirements (OPTIONAL)			
c.2.1	*Short text describing security environment requirement*	*ISO15408 class*	*Citation for full text*
c.2.2			
D Application notes (OPTIONAL)			
E Rationale			
The TVRA should define the full rational, if this is true only a citation (reference) to the full text is required			

In completing the pro forma above it has been shown in best practice from a number of applications in ETSI projects (including TISPAN, RRS and ITS) that the table can be built using specially crafted bookmarks and document automation although if the table scans multiple documents this is obviously more difficult.

A.2 Countermeasure deployment

A.2.1 Identity management

Successful identification is a pre-requisite for a number of security functions including authorization (verifying the right to do something) and authentication (verifying a claim of identity).

NOTE: Identity management is also considered in many domains as a precursor to protection of privacy and thus may be required for regulatory compliance under data protection and privacy regulation.

Table A.1: Summary of identity management measures

Requirement met	Identifier	Identifier attester	Attestation mechanism	Algorithm

A.2.2 Integrity protection and verification

Table A.2: Summary of Integrity protection measures

Requirement met	Data being protected	Verification source	Verifier	Protection mechanism

A.2.3 Confidentiality

Table A.3: Summary of confidentiality protection measures

Requirement met	NFV element being protected	Source	Sink	Protection mechanism

A.2.4 Availability and resilience

Table A.4: Summary of availability and resilience measures

Requirement met	Data being protected	Verification source	Verifier	Algorithm

A.2.5 Trust framework

ETSI GS NFV-SEC 003 [i.11] provides a detailed examination of the role of trust in a virtualised environment. The present clause is a simplified and re-targeted examination of the role of trust as introduced in ETSI GS NFV-SEC 003 [i.11].

Trust is defined as confidence in the integrity of an entity for reliance on that entity to fulfil specific responsibilities.

Trust is highly dynamic and contextual, and may be described in assurance levels based on specific measures that identify when and how a relationship or transaction can be relied upon. Trust measures can combine a variety of assurance elements that include identity, attribution, attestation and non-repudiation.

Trust is a complex issue, but in many cases, the decisions that are required within a particular NFV deployment will be simple.

Some myths or commonly ignored features about trust:

- Having a secured communications channel with another entity is never sufficient reason to trust that entity, even if the underlying security primitives on which that communications channel is based are trusted.
- Trust is not a binary operation. There may be various levels of trust that an entity has for another.
- Trust may be relative, not absolute. Entity A may trust Entity C more than Entity B, without trusting either absolutely.
- Trust is rarely symmetric. Entity A may trust Entity B completely, whereas the amount of trust that B has for A may be very low. This does not always matter: a schoolchild may trust a schoolteacher, for instance, without any requirement for that trust to be reciprocated.
- One of the axes for trust is almost always time, and the trust relationship between two entities may be highly dynamic over time. Just because a certain level of trust was established at point T, it does not mean that that level will be maintained at time T+ τ, as it can increase and decrease.

As noted above, trust is defined as confidence in the integrity of an entity for reliance on that entity to fulfil specific responsibilities. An entity A has no need to have a direct trust relationship with another entity B if B's operation has no direct impact on A. It may be that entity C is affected by entity B's operations, and that entity A relies on entity C, but this does not affect entity A directly, and therefore the trust relationship can be considered separate.

The core requirements related to trust in NFV that have to be addressed are the identification of the "root of trust". For each element protected within a trust relationship it is necessary to identify both the root of trust and the path from the protected element to the root of trust. It is strongly recommended (non-negotiable in some jurisdictions) that the root of trust is a trusted hardware module (that is able to store keys for example in tamper-resistant hardware).

Table A.5: Identification of root of trust

Requirement met	NFV element being protected	Root of trust	Nature of trust relationship and path to root of trust	Protection mechanism

A.3 Regulatory conformance

A.3.0 Introduction

NOTE: This clause identifies measures taken to assure that the NFV implementation conforms to applicable regulation.

A.3.1 Data protection and Privacy

The deployment of a network will require that a Privacy Impact Assessment (PIA) is carried out. The PIA process is shown in figure A.1 and is drawn from the Article 29 "Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011" [i.12] which itself is driven by the "Privacy Impact Assessment Handbook" [i.4].

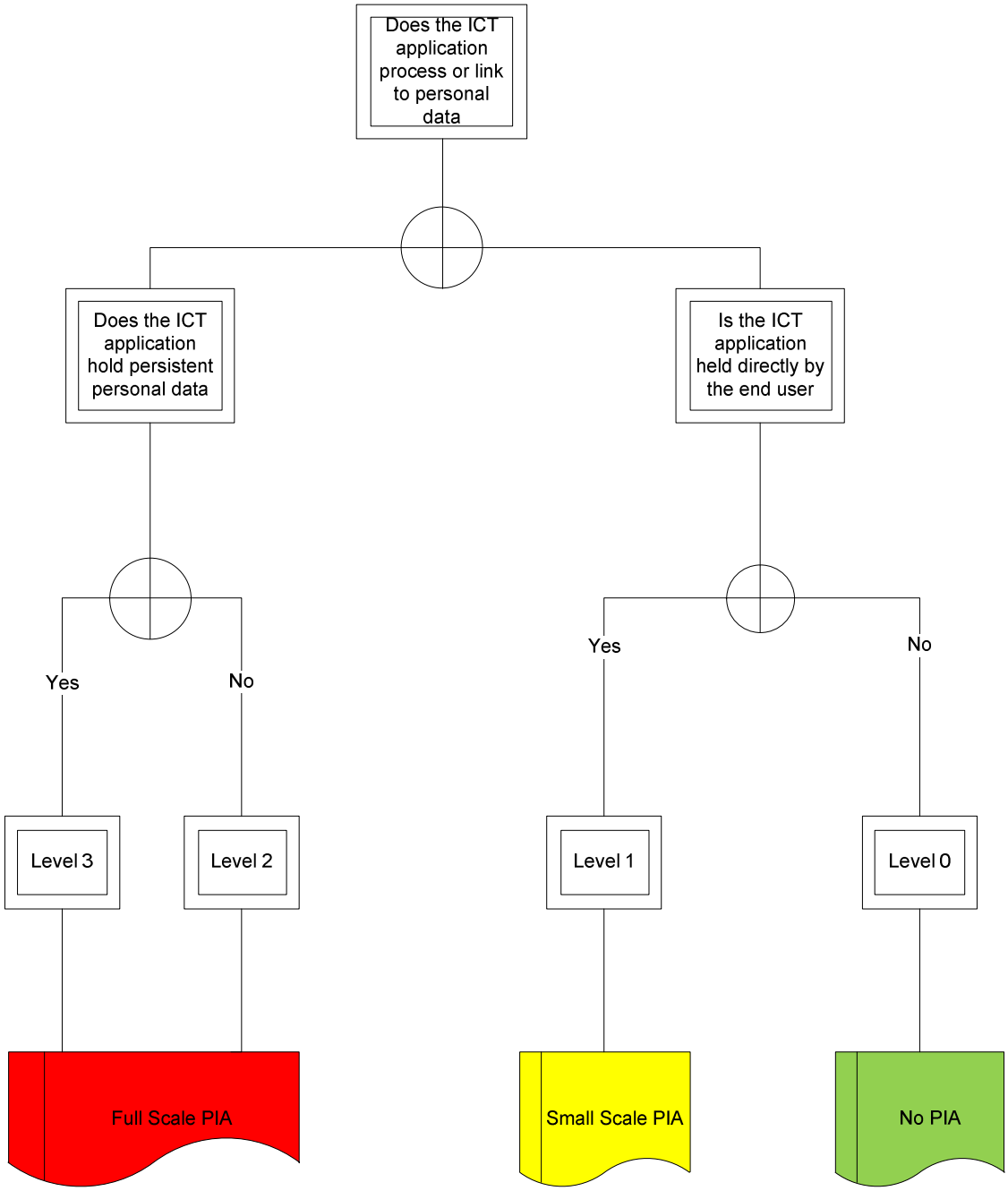

Figure A.1: Decision tree to identify form of PIA to conduct

The questions from the PIA Handbook [i.4] are structured into 5 groups:

1) Technology;
2) Identity;
3) Multiple Organizations;
4) Data; and,
5) Exemptions and exceptions.

Table A.6: PIA analysis

	Technology	
(1)	Does the technology or standard apply new or additional information technologies that have substantial potential for privacy intrusion?	Yes/No
	Identity	
(2)	Does the technology or standard involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?	Yes/No
(3)	Might the technology or standard have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	Yes/No
	Multiple organizations	
(4)	Does the technology or standard involve multiple organizations, whether they are government agencies (e.g. in 'joined-up government' initiatives) or private sector organizations (e.g. as outsourced service providers or as 'business partners')?	Yes/No
	Data	
(5)	Does the technology or standard involve new or significantly changed handling of personal data that is of particular concern to individuals?	Yes/No
(6)	Does the technology or standard involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?	Yes/No
(7)	Does the technology or standard involve new or significantly changed handling of personal data about a large number of individuals?	Yes/No
(8)	Does the technology or standard involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?	Yes/No
	Exemptions and exceptions	
(9)	Does the technology or standard relate to data processing which is in any way exempt from legislative privacy protections?	Yes/No
(10)	Does the technology or standard's justification include significant contributions to public security measures?	Yes/No
(11)	Does the technology or standard involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	Yes/No

In the data protection domain there are 2 key entities defined: The data controller; and, the data processor. There are also a number of key principles that underpin the OECD and EU approach to data collection and use, and a summary of these and the immediate impact on NFV (operators and technology) is given in table A.6.

Table A.7: DP&P Principles from OECD and EU guidelines

Root principle	Subsidiary principle	Impact on NFV
Collection limitation	Limits to data collection	Before collecting personal data - for example, when contracting with the data subject - an operator should obtain the prior and unambiguous consent of the data subject **or** inform him/her of the collection of personal data and the indicated purposes of use according to domestic regulations (see note).
		From the viewpoint of the operator, consent is always required when personal data is used in commercial services. However, in cases of safety and public services, prior explicit consent may not be required although implicit consent is likely to have been given as part of the user's contractual agreement with the service provider (see note).
	Data collection methods	An operator should not acquire personal data by fraudulent or other dishonest means.
	Data collection without consent	The limits to data collection do not apply to cases in which the handling of personal data is restricted by national regulation.
	Exclusion of data capable of identifying an individual from collected data	An operator should take reasonable measures to avoid collecting data from which an individual could be identified by referring to a database in cases where such a possibility exists.
	Confirmation of a data subject's consent about data collection	An operator should take suitable measures to confirm the consent of a data subject about data collection (see note).
Data quality		An operator should endeavour to keep personal data accurate and up to date within the scope necessary for the achievement of the purposes of use.
Purpose specification	Specification of the purposes of use	When handling personal data, the operator should specify the purposes of use of personal data.
	Limits on changing the purposes of use	An operator should not change the purposes of use beyond the scope in which new purposes can reasonably be considered to be compatible with the original purposes.
	Change of the purposes of use required prior consent	Before an operator changes the purposes of use beyond the scope in which new purposes can reasonably be considered to be compatible with the original purposes, it should inform a data subject of the change or obtain prior and unambiguous consent (see note).

Root principle	Subsidiary principle	Impact on NFV
Use limitation	Use limitation	An operator should not handle personal data, without obtaining the prior consent of the data subject, beyond the scope necessary for the achievement of the specified purposes of use (see note).
	Restriction of disclosure to third parties	An operator should not provide personal data to a third party without obtaining the prior consent of the data subject (see note).
	Use without consent	The provisions of the preceding two paragraphs do not apply to cases in which the handling of personal data is based on domestic laws. The operator should grant access only to law enforcement authorities as authorized by a domestic court order or equivalent legal instrument.
Security safeguards		Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
Openness		There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data collector.
Individual participation		An individual may have the right to: a) obtain from an operator, or otherwise, confirmation of whether or not the operator of the system has data relating to him; b) have communicated to him, data relating to him; (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; c) be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
Accountability		An operator should be accountable for complying with measures which give effect to the principles stated above.
Equality of regime		An operator should not transfer personal data across borders unless the destination has at least the same privacy regime as the origin.
Anonymity		An operator should provide the means for users to transact anonymously.
NOTE: The authorization framework to support consent does not need to be technical but may be procedural and may be both explicit (e.g. by acknowledgement of data transfer) and implicit (e.g. by means of signs and logos).		

The NFV designer/operator should complete the tables A.8 and A.9 with respect to the implementation of measures to comply to data protection and privacy regulation.

Table A.8: Identification of authority

Data controller	
Data processor	

Table A.9: Mechanisms implemented for data and privacy protection

Data controller	
Data processor	

A.3.2 Retention of Data

As noted in ETSI GS NFV-SEC 010 [i.10] the provision of facilities to support retention of data is mandatory in most deployment cases. The operator of the NFV should identify how the necessary facility is provided. In addition, the NFV operator should indicate how the handover interface to the appropriate authority is implemented by reference to the appropriate standards.

A.3.3 Lawful Interception

As noted in ETSI GS NFV-SEC 004 [i.9] the provision of facilities to support lawful interception are mandatory in most deployment cases. The operator of the NFV should identify how the LI facility is provided. In addition, the NFV operator should indicate how the handover interface to the LEMF is implemented by reference to the appropriate standards.

A.3.4 Export control of cryptographic material

Many countries in which NFV is deployed, developed or manufactured control the export of cryptography in the interests of national security. The present document does not propose to define which parts of the NFV will be subject to such controls but it is useful to note what is generally exempted. Thus the following notes may be used to guide in determining what is exempt, although it is strongly recommended that advice is sought from the appropriate national authority:

- the item is generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of over-the-counter transactions, mail order transactions, electronic transactions or telephone order transactions;
- the cryptographic functionality cannot easily be changed by the user;
- the item is designed for installation by the user without further substantial support by the supplier; and,
- when necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in the three points above.

All 4 conditions have to be met for the decontrol to apply (where decontrol refers to the non-applicability of export controls). It is essential to note that items marketed over the internet are subject to the same criteria. For example, cryptographic software and hardware products used to provide high-end backbone infrastructure services - such as high-capacity backbone routers - do not qualify as these items would normally require substantial support by the supplier.

The following interpretations of the main phases are taken from the UK but similar interpretations can be found from most countries:

- 'Retail selling points' are places where cryptographic items are readily available - e.g. high street and warehouse shops which facilitate over-the-counter sales, or companies which make sales via mail order, telephone, fax or internet transaction. Purchases from such companies are made by reference to a mail order catalogue, magazine or newspaper advertisement, website, etc. - media which are generally available in their own right.

- 'Without restriction' means that a buyer may acquire a product by paying a standard fee to the seller. 'Restriction' in this context means either that some persons are excluded from being allowed to buy, or that they are subject to conditions or limitations at the time of purchase, other than those normally arising from copyright - e.g. conditions imposed in a software licence. Other examples of forms of 'restriction' include a requirement to be an EU member state resident before purchase can be authorized, or a requirement for the purchaser to undertake that the goods will not be re-sold or given to any person or company from or in a particular country, or that installation is to be undertaken only by authorized engineers.
- 'The cryptographic functionality cannot easily be changed by the user' means that the manufacturer has taken reasonable steps to ensure that the cryptographic functionality in the product can only be used according to their specification.
- Installation by the user without further 'substantial support' - most mass-market products meet this requirement. 'Substantial support' does not include purely nominal installation support, such as provision of a telephone or an email helpline to resolve user problems.

A.3.5 Others

There are a number of additional regulatory actions to be taken for deployed equipment that may have to be taken prior to placing equipment (including software) on the market. It is essential that all stakeholders and participants in the NFV supply chain take due care to ensure that they comply.

Annex B (informative): Summary of attack vectors as applied in NFV

B.1 Interception attacks

In summary an interception attack occurs when two parties, Alice and Bob, exchange data over an open channel that is visible to the adversary Eve. If the data being exchanged by Alice and Bob is confidential (i.e. only intended to be seen by Alice and Bob), then any interception by Eve is an attack. There is also a set of conditions where whilst Alice represents an individual Bob may represent a group of users and there may be many channels between Alice and each instance of Bob but Eve is similarly multi-dimensioned.

Mitigation of interception is classically treated by encryption in order that if a channel or path is intercepted that any material gained cannot be used by an attacker to exploit the transmission content. In other words even if interception is possible the attacker cannot gain any advantage from the attack as the content will be indecipherable.

B.2 Manipulation attacks

A manipulation attack is designed to alter the function of the system. Many different vectors result in manipulation and include such things as buffer overflow, type-casting (forcing interpretation of (say) a structured element as an integer (say)), overloading of resources (denial of service attacks fall into this group).

Mitigation of manipulation is classically treated by the use of checksums or message hashes.

The requirements to be met of an integrity check function for detection of manipulation of something considered immutable can be summarized by the following requirements of a cryptographic hash function to generate a fixed length output from an arbitrary length input:

- One way function requirement
  - Given a hash h it should be difficult to find any message m such that $h = \text{hash}(m)$.
- Collision resistance requirement
  - Given an input $m1$ it should be difficult to find another input $m2$ such that $m1 \neq m2$ and $\text{hash}(m1) = \text{hash}(m2)$
- Strict Avalanche Criterion
  - if 1 bit in message m changes all other bits should change with 50 % probability
- Bit Independence Criterion
  - output bits j and k should change independently when any single input bit i is inverted, for all i, j and k

The challenge in general is to identify the immutable element of code or data over which the checksum is to be calculated and where reversal of the immutability will lead to error. When this element is correctly identified the form of function to be applied to detect manipulation has to be considered.

The algorithms used to generate a hash function should be of similar strength to any other cryptographic operation in the system but the system should ensure that it supports the concept of crypto agility in order that the algorithm can be updated over time.

B.3 Identity based attacks

The most common identity based attacks are those where a user (or device) masquerades as another user (or device) to gain access to information, an effect often termed as privilege escalation. The primary means to minimize identity based attacks are to authenticate identifiers that are non-forgeable and non-transferable with similarly non-forgeable and non-transferable verification credentials.

Annex C (informative): Cryptographic measures for NFV protection

C.1 Cardinality of relationships

The cardinality of relationships that have to be protected may be used as pre-selector for the crypto-system architecture.

- 1:1 relationships:
  - In this relationship there is only instance of each of Alice and Bob and they are able to exchange a secret in advance. For pre-established relationships all cryptographic operations for authentication, integrity and confidentiality may use symmetric key cryptography in which Alice and Bob share a single key. For relationships that are not known in advance a symmetric session key can be established using public key based authentication, or anonymous key establishment protocols where authentication is not required.
- 1:m and m:1 relationships:
  - In this case there is one instance of Alice and many instances of Bob, in such cases Alice does not need to know which particular instance of Bob. This is the common model of public key cryptography (or asymmetric cryptography). An operation with the private key can only be reversed with the public key and knowledge of the public key cannot be used to create a matching private key. The security of such cryptography is dependent on the properties of asymmetric functions and properties of particular mathematical problems. In larger systems an infrastructure is used to support the distribution of public keys in the form of public key certificates that hold the public key and some assertion by a trusted 3rd party that they public key is associated to a private key bound to an attribute of the public key holder. The most common attribute is identity but other attributes can be asserted using the same form of framework.
- m:n relationships:
  - Many to many relationships are quite simply difficult to cryptographically secure without normalizing the use case to a set of 1:m or m:1 relationships (this is somewhat similar to the normalization undertaken in the design of relational databases). If however an object (file, executable code, etc.) needs to be encrypted at all times where Alice is the initiator of the file but Bob is allowed to modify it in some way whilst it remains encrypted, and Charles is allowed to also modify it, but without any of the modifying parties being able to extract the plain-text of the object whilst at the same time assuring that future legitimate parties can perform their legitimate authorized actions on it is mathematically complex. Solutions do exist in the domain of Homorphic encryption and various schemes including attribute based encryption may satisfy the use case. Difficulties remain if the set of future parties to the encrypted data are unknown when setting out the access policy. This is an area of active cryptographic research.

In NFV the selection of crypto-architecture is dependent on identifying the cardinality of relationships between objects, and instances of objects, in the NFV.

CHECKLIST	Has the cardinality of all vulnerable relationships been defined for the NFV?	YES/NO

C.2 Algorithm selection and key size

Cryptographic algorithms for the NFV should be selected on the basis of interoperability across a wide spectrum of implementations in both hardware and software. It is strongly recommended that algorithms should be defined through their boundary conditions and taking account of the lifetime of the virtualised function being secured, the data it processes, the relevant regulations regarding the use of cryptography in the regulation of the country in which the cryptographic primitives are deployed. In all cases the system should ensure ability to support cryptographic agility, i.e. the ability to update both algorithms and keys over the lifetime of the underlying dependent functions or hardware.

Where asymmetric encryption is to be deployed there is a risk from advances in computing that may make the more common approaches invalid. Both the RSA and ECC approaches are vulnerable to Shor's and Grover's algorithms when run on a quantum computer that will break the algorithms (i.e. given knowledge of the public key certificate the private key can be found in polynomial time). The alternative for future proof digital signature is to use an approach that is considered Quantum-safe, i.e. an algorithm that is not weakened by the capabilities of a quantum computing attack. Within ETSI the impact of quantum computing is being addressed in 2 groups: ISG Quantum Safe Cryptography (QSC) with a role to identify cryptographic primitives that will be viable for reference in standards; CYBER with a role to identify business continuity requirements in transition to quantum safe cryptography.

The necessary cryptographic strength should follow best practice. Within ETSI expert guidance on such matters is offered from SAGE and should be adopted and sought.

Annex D (informative): Bibliography

- ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".
- ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.
- Recommendation ITU-T X.509: "Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks".
- ISO/IEC 27001:2005: "Information technology -- Security techniques -- Information security management systems - Requirements".
- Auguste Kerckhoffs: "La cryptographie militaire", Journal des sciences militaires, vol. IX, pp. 5-83, January 1883, pp. 161-191, February 1883.
- Shannon, Claude E. (July/October 1948). "A Mathematical Theory of Communication". Bell System Technical Journal 27 (3): 379-423.
- Computer Misuse Act 1990.

NOTE: Available at http://www.legislation.gov.uk/ukpga/1990/18/contents.

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002, p. 37.
- 52003DC0265: "Report from the Commission - First Report on the implementation of the Data Protection Directive (95/46/EC)", COM (2003) 265(01), 15.5.2003.
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
- Recommendation ITU-T X.1520 (January 2014): "Common vulnerabilities and exposures".

Annex E (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Mr Scott Cadzow, Cadzow Communications Consulting Ltd.

History

Document history		
V1.1.1	April 2016	Publication