International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(09/2021)

XSTR-XAASL
Framework for security standardization for virtualized services

Summary

This Technical Report is a document for discussion regarding the development of standards considerations, requirements and frameworks for virtualized services. These services are often known by the words "as a service" as in, "network as a service". The architecture for these virtualized services comes from work done in ITU-T Study Group 13. However, this discussion is around the security implications and considerations for those services which is within the mandate of ITU-T Study Group 17.

Keywords

Architecture, cloud, security, service, standard, virtualization.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Change Log

This document contains Version 6 of the ITU-T Technical Report on "Framework for security standardization for virtualized services". It contains revisions suggested at the Q8/17 interim meeting held virtually in July 2020 and the agreed text from the virtual Q8/17 meeting from August 2021.

Editor: Mark McFadden
DCMS
United Kingdom
Tel.: +1 608 504 7776
E-mail: mark@internetpolicyadvisors.com

Table of Contents

Technical Report ITU-T XSTR-XAASL

Framework for security standardization for virtualized services

1 Scope

This Technical Report makes no attempt to and does not suggest a revision to standards that have already been approved (with one exception). Instead, the scope of this contribution is current and future work items that address virtualization categories that are motivated by work from Study Group 13.

This contribution also suggests that, in the event it is revised in the future to reflect the current environment for cloud computing, that ITU-T Y.1601, "Security framework for cloud computing", be changed to include the considerations and recommendations proposed in this document. These include a common, consistent approach to:

- Use of the word "guidelines", and its effect on the structure of Recommendations;
- Use of the word "requirements", and its effect on the structure of Recommendations; and
- Structure for content for these documents.

2 References

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*

[ITU-T X.1602] Recommendation ITU-T X.1602 (2016), *Security requirements for software as a service application environments.*

[ITU-T X.1603] Recommendation ITU-T X.1603 (2018), *Data security requirements for the monitoring service of cloud computing.*

[ITU-T X.1604] Recommendation ITU-T X.1604 (2020), *Security requirements of Network as a Service (NaaS) in cloud computing.*

[ITU-T X.1605] Recommendation ITU-T X.1605 (2020), *Security requirements of public Infrastructure as a Service (IaaS) in cloud computing.*

[ITU-T X.1606] Recommendation ITU-T X.1606 (2020), *Security requirements for communications as a service application environments.*

[ITU-T X.1750] Recommendation ITU-T X.1750 (2020), *Guidelines on security of big data as a service for big data service providers.*

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2016), *Cloud computing – Framework and high-level requirements.*

[ITU-T Z.100] Recommendation ITU-T Z.100 (1997), *Specification and Description Language – Overview of SDL-2010.*

[ITU-T Z.150] Recommendation ITU-T Z.150 (2003), *User Requirements Notation (URN) – Language requirements and framework.*

[ITU-T Z.341] Recommendation ITU-T Z.341 (1988), *Glossary of terms.*

[ITU-T Z-Sup.1] ITU-T Z.100-series – Supplement (1997), *SDL+ methodology: Use of MSC and SDL (with ASN.1).*

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 guideline [ITU-T Z.100]: Advice to the user of this methodology on identifying decisions to be made, which can also provide reasons and direction for making a decision.

3.1.1bis guideline [ITU-T Z.341]: General directions by which the purpose of one or more phases of the methodology may be accomplished.

3.1.2 requirement [ITU-T Z.150]: A requirement is an expression of ideas to be embodied in the system or application under development.

3.1.2bis requirement [ITU-T Z.100]: Provision that conveys criteria to be fulfilled.

3.2 Terms defined in this Technical Report

None.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

CaaS Communication as a Service

IaaS Infrastructure as a Service

NaaS Network as a Service

PaaS Platform as a Service

SaaS Software as a Service

5 Introduction

Cloud computing is a model for enabling service users ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud computing model is composed of five essential characteristics (on-demand, delivery over a broad network access, resource pooling, rapid elasticity, self and measured services), five cloud computing service categories, i.e., software as a service (SaaS), communication as a service (CaaS), platform as a service (PaaS), infrastructure as a service (IaaS) and network as a service (NaaS), and different deployment models (public, private, hybrid, etc.).

The five cloud computing service categories are effectively virtualized services: instances of a service made available to a cloud service customer through a virtual, pooled resource. ITU-T Study Group 13 routinely publishes functional requirements for these virtualized services. A good example is the current work on Y.BaaS-reqts, "Cloud computing – functional requirements for blockchain as a service", or Y.MLaaS-reqts, "Cloud computing – functional requirements for machine learning as a service".

In these cases, Study Group 13 inserts a brief description of the security requirements for the virtualized service, but leaves the detailed analysis of the security requirements to Study Group 17. Question 8 in Study Group 17 has then had the responsibility for addressing the comprehensive security requirements for the virtualized services described by Study Group 13.

6 Virtualized services in ITU-T Study Group 17 Question 8

For many years, ITU-T Study Group 17 Question 8 (Q8/17) has responded to the development of requirements for virtualized services in Study Group 13 by initiating a new work item based on the Study Group 13 definition.

[ITU-T X.1601], "Security framework for cloud computing", provides the overall architecture for describing cloud computing security and acts as the foundation for all other security documents in the X-series related to cloud computing.

The X-series documents numbered between ITU-T X.1602 and ITU-T X.1639 are intended to provide specific security standards for individual classes of cloud computing applications. It is in this series where Q8/17 establishes standards for virtualized services. Besides the established security standards for virtualized services in this series, Q8/17 also has security standards, [ITU-T X.1750] and X.BaaS-sec, to respond to the development of standards for virtualized services in ITU-T Study Group 13.

7 Existing standards

Study Group 17 has published the following standards related to security of virtualized services:

- X.1602 – Security requirements for software as a service application environments
- X.1603 – Data security requirements for the monitoring service of cloud computing
- X.1604 – Security requirements of network as a service (NaaS) in cloud computing
- X.1605 – Security requirements of public infrastructure as a service (IaaS) in cloud computing
- X.1606 – Security requirements for communication as a service application environments
- X.1750 – Guidelines on security of big data as a service for big data service providers

8 ITU-T Study Group 17 Question 8 work items on virtualization

Study Group 17 also has other, approved work items in the current study period related to virtualized services. In each case, the motivation has come from the development of a service definition by Study Group 13 with no details on how to provide for security for that service. The following documents are under consideration at the current time in Q8/17:

- X.BaaS-sec – Guideline on blockchain as a service security

9 Problem statement

The content of each of the virtualized services security work items is varied. A reader is unable to expect consistent content across each of the virtualized services recommendations from Q8/17. What is needed is a common, consistent framework for documents that have "as a Service" in their title – that is, documents that attempt to provide security considerations and requirements for virtualized services.

In addition, Q8/17 has a series of work items that provide guidelines instead of requirements. Once again, the reader is unable to consistently expect the same content based on the use of these keywords. A common, consistent approach to the use of "requirements" versus "guidelines" is required for this series of documents.

10 Scope

This contribution makes no attempt and does not suggest a revision to standards that have already been approved (with one exception). Instead, the scope of this contribution is current and future work items that address virtualization categories that are motivated by work from Study Group 13.

This contribution also suggests that, in the event it is revised in the future to reflect the current environment for cloud computing, that [ITU-T X.1601], "Security Framework for cloud computing", be changed to include the considerations and recommendations proposed in this document. These include a common, consistent approach to:

- Use of the word "guidelines", and its effect on the structure of recommendations;
- Use of the work "requirements", and its effect on the structure of recommendations; and
- Structure for content for these documents.

11 Problem statement

As nouns the difference between requirement and guideline is that requirement is a necessity or prerequisite; something required or obligatory while guideline is a non-specific rule or principle that provides direction to action or behaviour.

For virtualized services, a requirement is a statement which specifies a verifiable constraint on an implementation that it shall undeniably meet or

- be deemed unacceptable, or
- result in implementation failure, or
- result in system failure.

On the other hand, a guideline is a non-specific rule or principle that provides direction to action or behaviour. It can be a plan or explanation to guide in setting standards or determining a course of action.

[ITU-T Z.150] clause 3.16 provides the following definition of "requirement":

- "*A requirement is an expression of ideas to be embodied in the system or application under development*".

[ITU-T Z-Sup.1] clause 2.33 says, simply:

- *Provision that conveys criteria to be fulfilled*.

On the other hand, [ITU-T Z-Sup.1], clause 2.23 provides the following definition of "guideline":

- *Advice to the user of this methodology on identifying decisions to be made, which can also provide reasons and direction for making decisions*.

[ITU-T Z.341] clause 2 provides the following definition of "guidelines":

- *General directions by which the purpose of one or more phases of the methodology may be accomplished*.

What is clearly intended here is that "requirements" provide specific, exact specifications for the security of a virtualized service. In contrast, "guidelines" are an overview of how to provide for security of that virtualized service and not a set of specific specifications.

12 Security requirements for virtualized services (XaaS)

12.1 Introduction

This contribution proposes a structure for future Q8/17 documents that intend to provide security requirements for virtualized services (often identified by the acronym XaaS, where X is the initial of the class of service being virtualized). These are intended to be precise specifications with normative language. The intent is to provide the reader with comprehensive instructions for providing security to an implementation of a virtual service: it should be complete, address all aspects of security for the service and use normative language to indicate the requirements.

12.2 Structure of a security requirements draft

For Q8/17, the structure of current and future security requirements documents is presented in Table 1.

Table 1 – Structure of a security requirements draft

Clause	Description	Mandatory for security requirements documents?
1. Scope	A short, one or two paragraph description of the virtualized service and the security requirements being standardized. Where appropriate, reference and refer to the methodology specified in clause 10 of [ITU-T X.1601].	Mandatory
2. References	This is the standard reference clause for all ITU-T Recommendations. A XaaS requirements document must reference [ITU-T X.1601] and [ITU-T Y.3501] at a minimum.	Mandatory
3. Definitions	This is the standard set of definitions for any ITU-T recommendation. It should include two clauses: terms that are defined elsewhere and terms that are defined within the XaaS requirements document. Note that the ITU-T Y.3500 series of documents have good definitions for XaaS services.	Mandatory
4. Abbreviations and acronyms	This should be a comprehensive list of all acronyms and abbreviations used in this XaaS requirement document.	Mandatory
5. Conventions	This is a short clause that provides the reader with an understanding of any conventions or understandings that will provide context for the requirements. For instance, if "server" is used interchangeably with "virtual server" for the purposes of the document, it should be noted in this clause. In addition, the following context should be provided in this clause: "The keywords "is required" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed. The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance. The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification. In the body of this document and its appendixes, the words shall, shall not, should and may sometimes	Mandatory

Table 1 – Structure of a security requirements draft

Clause	Description	Mandatory for security requirements documents?
	appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent."	
6. Overview of XaaS	This clause is a description of the virtualized service. It may take much of its content from the description provided by the Architectural Framework provided by the associated standard in the Y.3500 series such as for instance, [ITU-T Y.3501]. It should provide enough background for the reader to understand the virtualized service but not so much that it duplicates the material provide by the Y.3500 series of standards. It should provide an illustration of the XaaS service model.	Mandatory
7. Security threat landscape for XaaS	This is a precise description of the security threat landscape that is specific to XaaS. It should not include security threats that are generalized threats and apply to any network based service (as an example, theft of credentials). Instead, this clause should, at a minimum, identify threats in the following areas: – Architecture – Identity and access management – Software isolation and API related issues – Isolation of instances – Data protection – Availability – Incident response – Management, orchestration and deployment	Mandatory
8. Security requirements for XaaS	This is a clause that identifies, using precise normative language, the mitigations for each of the threats from the outline in clause 7. The language should be specific enough for an implementer to understand and deploy a security solution that addresses the threat landscape for XaaS. In particular, using normative language, it should be possible for the reader to have a "checklist" approach to designing, building and deploying security mitigations for the threats outlined in clause 7 above. Each requirement clause should use the normalized language format, in other words, each requirement clause uses "is required", "is recommended" or "can optionally" as the keywords. Each subsection of requirements should identify its corresponding threats, or vice versa. The mapping of security threats and challenges to security requirements can be illustrated in a table format.	Mandatory

Table 1 – Structure of a security requirements draft

Clause	Description	Mandatory for security requirements documents?
Appendices	Security requirements documents are often accompanied by appendices that assist the reader in understanding the steps needed to design, build and deploy a security solution. For XaaS, these might include checklists, case studies and examples, and lists of tools that help the reader build and deploy security solutions for XaaS. In addition, the reader may be assisted by diagrams that should show the logical relationships between functional components of security for a XaaS service.	Optional

13 Guidelines for security for XaaS

13.1 Introduction

A guideline document is very different from a requirements document. The intent of the guideline is to provide the reader with a very high-level overview of XaaS, the security threats that are specific to XaaS and the general tools, services and design criteria that can be used to address those threats. It is intended at a more general audience than a requirements document and does not provide specific, normative tasks for an implementer to use. In ITU-T Q8/17, it is possible and sometimes advisable to have both a guidelines document (for generalist readers) and a requirements document (for readers designing, building and implementing) for a XaaS service. Other than an overview of the XaaS service itself (a prerequisite for understanding the security ecosystem for XaaS), a guideline document should not duplicate material in a requirements document.

There is never any normative language in a guideline document.

13.2 Structure of a security guidelines draft

For Q8/17, the structure of current and future security guidelines documents is presented in Table 2.

Table 2 – Structure of a security guidelines draft

Clause	Description	Mandatory for security guidelines documents?
1. Scope	A short, one or two-paragraph description of the virtualized service and the security guidelines being provided.	Mandatory
2. References	This is the standard reference clause for all ITU-T recommendations. A XaaS requirements document must reference [ITU-T X.1601] and [ITU-T Y.3501] at a minimum.	Mandatory
3. Definitions	This is the standard set of definitions for any ITU-T recommendation. It should include two clauses: terms that are defined elsewhere and terms that are defined within the XaaS requirements document. Note that the Y.3500 series of documents have good definitions for XaaS services.	Mandatory

Table 2 – Structure of a security guidelines draft

Clause	Description	Mandatory for security guidelines documents?
4. Abbreviations and acronyms	This should be a comprehensive list of all acronyms and abbreviations used in this XaaS guidelines document.	Mandatory
5. Conventions	This is a short clause that provides the reader with an understanding of any conventions or understandings that will provide context for the requirements. As an example, if "server" is used interchangeably with "virtual server" for the purposes of the document, it should be noted in this clause.	Mandatory
6. Overview of XaaS	This clause is a description of the virtualized service. The goal of a guideline document is to provide a high-level understanding of the XaaS service itself, the security issues that are associated with the service, and an understanding of the general guidelines used to mitigate those issues. It should provide enough background for the reader to understand the virtualized service but not so much that it duplicates the material provide by the Y.3500 series of standards. It should provide an illustration of the XaaS service model.	Mandatory
7. Security threats and challenges for XaaS	This is a high-level description of the security threat landscape that is specific to XaaS. It should not include security threats that are generalized threats and apply to any network based service (as an example, theft of credentials). This clause should provide enough background for the reader to understand the security challenges that are unique to this XaaS service. Subsections of this clause may address challenges in the following areas: – Architecture – Identity and access management – Software isolation and API related issues – Isolation of instances – Data protection – Availability – Incident response – Management, orchestration and deployment	Mandatory
8. Security guidelines for XaaS	This is a clause that describes, at a high-level, the approaches that should be taken to mitigate against the threats identified in clause 7. The language should never be normative. Instead, the reader should be able to understand the tools, services and design criteria that help ensure that XaaS is protected against the threats in clause 7 above. This clause can be presented in two clauses instead: one is "Security requirements for XaaS" and the other is "Security controls for XaaS". Here "Security requirements for XaaS" is a clause different from that	Mandatory

Table 2 – Structure of a security guidelines draft

Clause	Description	Mandatory for security guidelines documents?
	in security requirements documents. It describes the security characteristics that XaaS should satisfy, such as confidentiality and integrity, while security requirements documents provide requirements in a detailed manner for an implementer to understand and deploy a security solution. These security characteristics are not generalized ones. Instead, this clause should explain how these security characteristics are unique to this XaaS and how these characteristics function against the threats in clause 7 above. "Security controls for XaaS" provides security mechanisms to implement the security requirements.	
Bibliography	In guidelines documents it is often very helpful to provide the reader with a list of further resources and reading that will help him/her better understand the security requirement for XaaS. A bibliography is always more helpful if it is annotated in a way specific to a reader interested in XaaS and not simply a list of links and publications.	Optional
Appendices	Security guidelines documents are often accompanied by appendices that assist the reader in understanding the steps needed to design, build and deploy a security solution. For XaaS, these might include checklists, case studies and examples, and lists of tools that help the reader build and deploy security solutions for XaaS. In addition, the reader may be assisted by diagrams that should show the logical relationships between functional components of security for a XaaS service.	Optional