International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1606

(09/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cloud computing security – Cloud computing security design

Security requirements for communications as a service application environments

Recommendation ITU-T X.1606

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	**X.1602–X.1639**
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1606

Security requirements for communications as a service application environments

Summary

Recommendation ITU-T X.1606 identifies security threats and recommends security requirements for communications as a service (CaaS) application environments. The Recommendation describes scenarios and features of CaaS containing multi-communication capabilities. Then it identifies specific threats arising from unique CaaS features and recommends appropriate CaaS security requirements.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1606	2020-09-03	17	11.1002/1000/14265

Keywords

CaaS, cloud computing, risk, security requirement.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Overview of CaaS	3
7	Security threats to CaaS	4
	7.1 Identity threats	4
	7.2 Account lifecycle management threats	5
	7.3 Orchestration threat	5
	7.4 Terminals context threat	6
	7.5 Spam threat and malware distribution	6
	7.6 Add-on threat	6
	7.7 Software development kit threat	7
	7.8 Threats from telecommunication networks vulnerabilities	7
8	Security requirements for CaaS	7
	8.1 Identity and access management	7
	8.2 Terminal security	8
	8.3 Service security	9
	8.4 Security coordination	9
Appendix I – A quick guide to the security threats and challenges listed in Recommendation ITU-T X.1601		10
Appendix II – A mapping of security threats and security requirements		12
Bibliography		13

Recommendation ITU-T X.1606

Security requirements for communications as a service application environments

1 Scope

This Recommendation focuses on security requirements of communications as a service (CaaS) application environments, which differ from those for software as a service (SaaS) in [ITU-T X.1602]. CaaS of telecommunication organizations merges the communication capabilities of telecommunications and the Internet. The convergence leads to some unique CaaS features that are subject to specific risks. These risks are identified in this Recommendation and appropriate security requirements are recommended.

These requirement measures take into account national legal and regulatory obligations in individual member states in which CaaS operates. The text is based on the methodology specified in clause 10 of [ITU-T X.1601].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [ITU-T X.1601]: Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

3.1.2 capability [b-ISO 15531-1]: Quality of being able to perform a given activity.

3.1.3 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.4 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.5 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.6 cloud service partner [b-ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

3.1.7 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.8 cloud service user [b-ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

NOTE – Examples of such entities include devices and applications.

3.1.9 communications as a service (CaaS) [b-ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is real time interaction and collaboration.

NOTE – CaaS can provide both application capabilities type and platform capabilities type.

3.1.10 multi-tenancy [b-ITU-T Y.3500]: Allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another.

3.1.11 orchestration [b-ITU-T Y.3100]: In the context of IMT-2020, the processes aiming at the automated arrangement, coordination, instantiation and use of network functions and resources for both physical and virtual infrastructures by optimization criteria.

3.1.12 software as a service (SaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CaaS Communications as a Service

CSC Cloud Service Customer

CSN Cloud Service partner

CSP Cloud Service Provider

CSU Cloud Service User

DDoS Distributed Denial of Service

GSM Global System for Mobile

IAM Identity and Access Management

IaaS Infrastructure as a Service

ID Identifier

MMS Multimedia Messaging Service

NaaS Network as a Service

OS Operating System

PaaS Platform as a Service

PC Personal Computer

QR Quick Response

SaaS Software as a Service

SDK Software Development Kit

SIM Subscriber Identity Module

SMS Short Message Service

URL Uniform Resource Locator

(U)SIM (Universal) Subscriber Identity Module

VoLTE Voice over Long-Term Evolution

VPN Virtual Private Network

5 Conventions

In this Recommendation, there is no difference between server and virtual server.

6 Overview of CaaS

Definition of CaaS is found in clause 3.1.9. The general requirements of CaaS were recommended to be communication capabilities openness, communication software support and unified communication (see clause 11 of [ITU-T Y.3501]).

According to industrial practice, these capabilities are usually implemented or supported by CaaS:

– combination of telecommunication services and internet services;
– real-time communication;
– multi-device synchronization;
– communication resources isolation;
– user presence update;
– group chat or meeting;
– embedded by other SaaSs;
– user opt in or out;
– service process customization;
– data or file sharing;
– identity and access management (IAM).

Figure 6-1 depicts a general CaaS service model. There are four layers in Figure 6-1 labelled: user; access; service; and resource.

– The user layer contains cloud service user (CSU) terminals that can run some CaaS clients and can access the Internet and even telecommunication networks.
– The access layer provides various types of tunnels, usually to allow terminal access to their targeted CaaS service.
– The service layer, which is also the CaaS layer, is owned by a cloud service provider (CSP), which relies on the necessary inside and outside resources to complete the service operation. The service layer customizes service processes and allocates resources for cloud service customers (CSCs), maintains a (virtually) dynamic service network for a CSC with its CSUs, and isolates computing resources and communication networks for any CSC.
– The resource layer provides the fundamental infrastructure resources related to data processing and communication, part of which could be infrastructure as a service (IaaS), platform as a service (PaaS) and network as a service (NaaS).

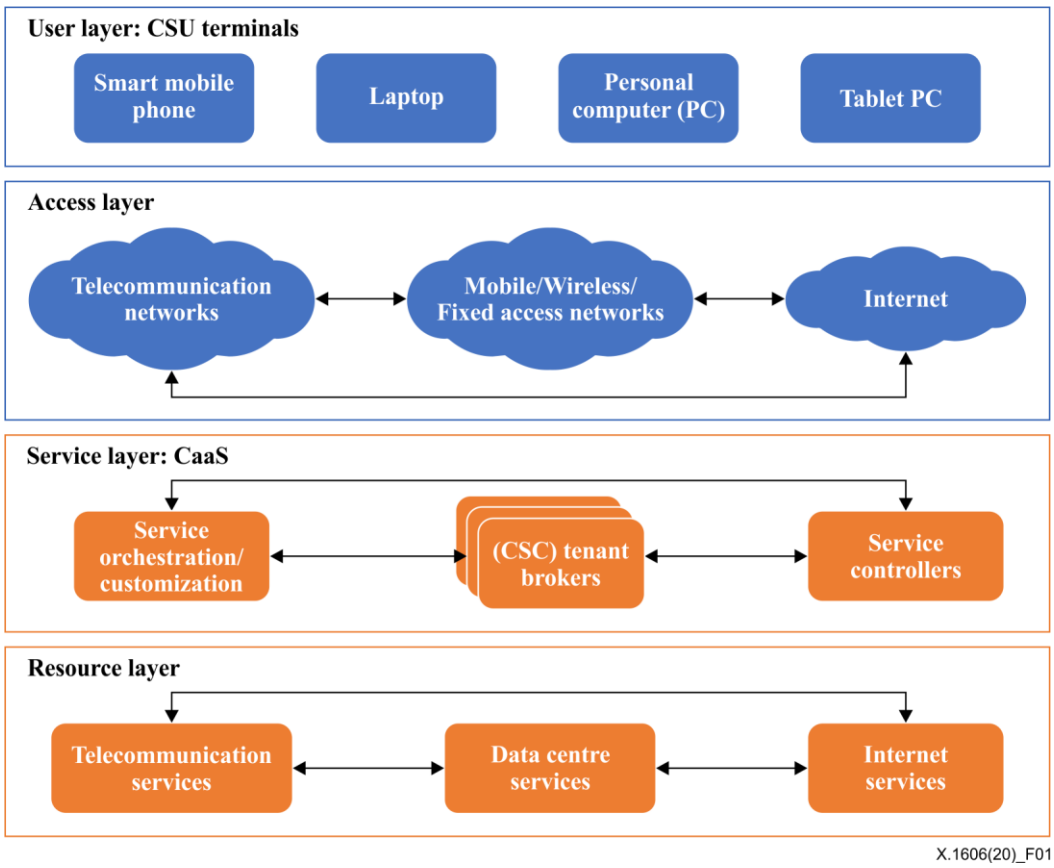

Figure 1 – A general CaaS service model

In the remainder of this Recommendation:

– Clause 7 analyses security threats to CaaS that target one or more of the four layers.

– Clause 8 recommends security requirements for CaaS that address threats to three layers:

- CSU terminal layer;
- CaaS layer;
- service resource layer.

The access layer is not covered here because its security capabilities are not controlled by CaaS, although the security level of the access layer can be evaluated or monitored by CaaS and CSU.

7 Security threats to CaaS

The security threats and challenges to cloud computing identified in [ITU-T X.1601] (also listed in Appendix I) can apply to various CaaS scenarios. Moreover, some specific threats to CaaS are identified in clauses 7.1 to 7.8.

7.1 Identity threats

The core of CaaS is unified communication capabilities, which differ slightly from another SaaS. CaaS integrates and enhances communication capabilities among terminals by leveraging cloud computing. A CaaS supports most mainstream types of terminal or operating system (OS), such as smartphones or personal computers (PCs).

Therefore, under the multi-point to multi-point communication model, CaaS may encounter some special threats if identity abuse occurs.

7.1.1 Identity credential theft

For the convenience of CSUs, many CaaSs adopt an authentication solution, which supports mobile number (i.e., mobile identifier (ID)) authentication or username and password authentication or both. In this case, the default username in the solution can be configured just like the mobile ID. Furthermore, some CaaS support one CSU with one ID accessing the service with multi-terminals concurrently or support synchronizing the communication history among multi-terminals.

The security of mobile number authentication relies heavily on confidence in the authentication, the encryption of the mobile network carrier and the (universal) subscriber identity module (U)SIM card holding the credential(s). There are some vulnerabilities (proved in the field) in mobile networks, especially for the Global System for Mobile Communications Alliance (GSMA) network, which would weaken the trust and might lead identity credential theft (temporarily). For example, some types of subscriber identity module (SIM) cards can be duplicated physically; some dynamic authentication codes transferred by short message service (SMS) in global system for mobile (GSM) communication networks can be intercepted. Intercepted temporary encryption keys can also be abused to hijack the ID temporarily and silently.

Moreover, username and password authentication can give the abuser a chance to make use of this authentication type with other qualified terminals to monitor a CSU (simultaneously). For example, if an abuser can handle a CSU mobile terminal with a (U)SIM card or soft SIM credential, the abuser can obtain the username in the cache and use the reset mechanism to set a new password and keep it cached in the terminal. Then it is possible that the CSU does not realize the password has been reset and ongoing communication content and even its history could both be silently monitored by the abuser.

7.1.2 Identity counterfeit

Once an identity credential of a CSU has been stolen or obtained by an abuser, the identity can be abused to access the service belonging to a CSC that the CSU is associated with. Meanwhile, the abuser can also obtain a social entity endowed with the CSU identity credential or even counterfeit some other social entity or create a new one, which can be shown firstly by the presence function.

Presence is one common CaaS feature, which usually implements the self-portrait of a CSU with a small-sized picture and limited text. Through presence, the CSUs associated with the same CSC can obtain a quick acknowledgement from one CSU. However, the presence of an abused identity can be falsified and be abused for fraudulent activities. For example, an abuser can seize confidential company finance data from an accountant by falsifying a presence as a board member.

Real-time video chat can be a standard CaaS configuration. The scene shown by the abused identity through the video stream can also be falsified to enhance the authenticity of the social entity and the fraudulent activity.

7.2 Account lifecycle management threats

A CSU, CSC or CSP might all have the right to require the deletion of an account on which they have authority. In the overall account lifecycle, when an account is to be retired, it should be agreed in advance what the CSP is supposed to do regarding the communication of content and account information through its CaaS entire service, whether the CSC can keep these data in its logical space or whether the CSU can keep these data in its terminal.

The disposal or the theft of a terminal could also mean that any cached account information should be erased, and any related data deleted.

7.3 Orchestration threat

With the orchestration (see [b-ITU-T Y.3100]) function, a CSC can customize its service processes and service capabilities by itself or through its CSP. For example, a CSC can adjust the process and

the privilege of managing the membership in a chat group and also down- or up-grade the limitation on the scale where a CSU can search a contact.

In terms of customer requirements, a CSP can allow more than two CSCs to share their contacts and even to communicate directly with each other, as well as being able to merge more than one CSC into a bigger one.

Furthermore, to implement a new service feature, a CSP can up- or down-grade the security preconditions on a network to which a CSU has access.

Any orchestration without full consideration of security can affect the isolation of information and services negatively. For example, if the CaaS of a CSC is orchestrated to integrate voice and message services of a GSM network, then it is almost impossible to implement the isolation feature from end to end, because GSM network entities adopted early-age technologies and cannot support any kind of isolation feature. If an unsecure network type is permitted by orchestration to support a more flexible service feature, it can increase the risk level of a CaaS more than just some CSC. For example, if the virtual private network (VPN) access requirement as an isolation method is reconfigured from the mandatory to the optional so as to ensure video chat quality in a CaaS, then the risk of eavesdropping would increase.

7.4 Terminals context threat

The security context of the terminals in a CaaS can be uncertain, especially as the terminals are smartphones or portable devices. If these terminals are personal property, the context could be more complex. These terminals could be used by relatives or visitors of a CSU. The screen of a terminal could be projected to or shared with another screen so that an unknown screen recording is possible. The vulnerabilities of a terminal could be exposed more directly to an attacker in an unsecured network. The communication content through a CaaS could be unencrypted and stored in a terminal. All these cases could lead to data leakage.

If an attacker can control a terminal (remotely or locally), it can abuse the terminal to exploit the vulnerabilities of a CaaS and even its CSU. If many terminals are controlled simultaneously as part of a botnet, the attacker could trigger a distributed denial of service (DDoS) attack also.

7.5 Spam threat and malware distribution

A CSU can be harassed or even phished by a spam attack from other CSUs through a CaaS. Indeed, in most cases, it is hard for a CSU to identify rationally whether to trust the information of a short uniform resource locator (URL) or a quick response (QR) code, which can lead a CSU to access a phishing website or download malware.

7.6 Add-on threat

It is natural for a CaaS to provide some add-ons based on its basic service, such as file sharing, in-built web browser, content management system and even e-business. In most cases, these add-ons are rather lightweight.

The vulnerabilities of these add-ons can open significant threats to the CaaS itself. For example, a click on an unsecure short URL can invoke the web browser extensions, which lack the capability to counter a dangerous web address, so that the probability that the security of the CSU and even the CaaS can be damaged significantly increases.

Some add-ons can guide a CSU to leave its current CaaS and switch to another rogue service. If the CSU is unaware of the switch, it is unable to adjust its trust appropriately and timely, causing a large spectrum of damage (more vulnerabilities exploited, extortion, ransomware, etc.).

7.7 Software development kit threat

A CaaS can provide a software development kit (SDK) to encourage integration by other applications or SaaS. Integration means basically trust to some extent between the CaaS and its SDK user. Therefore, vulnerabilities of the SDK user can increase the threat to the CaaS of attack or abuse.

As a terminal might have several identity credentials for different CSCs, a CaaS SDK user can abuse these credentials without permission to access other CSCs illegally.

7.8 Threats from telecommunication networks vulnerabilities

In addition to Internet access, if a CaaS incorporates other capabilities of the telecommunication network carrier, such as SMS, voice over long-term evolution (VoLTE), circuit-call, multimedia messaging service (MMS) and location, the security of the telecommunication network can have a direct effect on the CaaS.

Any successful abuse of telecommunication network vulnerabilities can lead to data leakage from the CaaS. Similarly, any successful attack on the telecommunication network, especially on the nodes connected with CaaS servers might expand the exposure surface of the CaaS.

Moreover, as modern commercially available terminals can switch access networks and VPNs actively among different providers according to predefined policies with little consideration for the trust and the authenticity of the access network, the CSU can be unaware of the use of an unsecure network environment, which can lead to leakage of confidential information.

8 Security requirements for CaaS

The security requirements for SaaS identified in [ITU-T X.1602] apply to CaaS scenarios. Moreover, this clause establishes some further security requirements to address threats identified in clause 7.

8.1 Identity and access management

8.1.1 Identity management

CaaS should set an upper limit of concurrent terminals sharing the same identity credential. CaaS can verify one terminal with the necessary hardware and service identification as the primary controller, which can authorize access by other terminals on demand.

CaaS can monitor concurrent terminals with the same identity credential and keep all terminals (or at least the primary controller) informed about the latest status of other concurrent terminals. A CSU can use the primary controller or pass more secure authentication (such as bypass authentication) to force a specified terminal to log out, forbid any future access by it and even delete the residual information in it.

CaaS can consider guiding a CSU to the use of different credentials (and at least different passwords) for different CSCs, which can decrease the risk of using one stolen credential to access many CSCs.

8.1.2 Access control

If the concurrency of terminals with one identity credential is a common capability of CaaS, it would be meaningful to allow CaaS to acquire and update the geographic location of terminals so that CaaS can discover any terminal access anomaly. As one terminal can access many networks at the same time, CaaS can consider the possibility to use multi-dimensional information to cross-check the authenticity of the location.

If network security cannot be guaranteed, a VPN can be a good choice to enhance infrastructure security. A CaaS should consider requiring a CSU or CSC to use a mandatory VPN service and forbidding a CSU or CSC to adopt any other VPN service as a hop or a relay to access the mandatory

VPN service. An optional or untrusted VPN could obscure the location of a terminal and can also increase the risk of middle-man attack.

Furthermore, if the risk of an intercepted GSM SMS cannot be accepted by the CSC, CaaS should consider monitoring the type of network accessed by any CSU and then refusing the use of an SMS as an authentication method if the CSU is under a GSM network. Alternatively, CaaS can just exclude the GSM SMS resource for the CSC.

8.1.3 Identity verification

As a CSU can use obscure, inaccurate or even falsified information to make a self-portrait, CaaS should alert all CSUs about whether a social identity in their contacts is verified by some trusted third party. The third party can be a CSC, a CaaS or any other independent authority. The verification can be mandatory or optional, while if it is optional, it can be necessary to alert the CSU that the CSP or the CSC cannot be responsible for the authenticity of the social identities in the CSC.

As the social or business identity of a CSC used to become a customer of a CaaS could be utterly different from the one used in public, it is suggested that CaaS should consider comparing the claimed identity of a CSC in public with the available information to prevent potential public or business fraud. For example, a malicious CSC could pretend to be a charity organization and forge some donation items to abuse the CSU.

8.1.4 Account management

As a CSU can have at least one account under a CSC and a CSC can also have at least one account under a CaaS, CaaS should provide full data access privilege of an account to the CSU or the CSC according to ownership of the data. Furthermore, as one account needs to be cancelled or deleted, CaaS should provide a reliable capability to destroy the account data physically on the terminal side, the service side and the network side in accordance with the terms of the legal authorization by the owner of the data.

8.2 Terminal security

8.2.1 Internal security

CaaS should provide technical measures, such as a security tool or security module embedded in the CSU terminals, to carry on a cyclic or on-demand security check. The security check could evaluate whether the context of a CSU terminal fulfils mandatory security requirements before accessing a CaaS. If a CSU terminal fails to pass the security check, the CaaS could consider refusing to provide services (partly). Meanwhile, the CaaS should guide the CSU to resolve the discovered security risks or could fix the vulnerabilities directly with the authorization of the CSU.

8.2.2 External security

The software used in CSU terminals should be provided by CaaS. CaaS should also provide secure a software distribution platform or sources, which should be official or authorized. CaaS should also declare the verification mechanism so that CSU terminals can use it to verify authenticity and integrity before update. The OS or the software itself in CSU terminals should have a roll-back capability if an update fails.

In most cases, the security update of terminal software is optional. However, if some vulnerability could cause great damage to CaaS, a CSC or even another CSU, and a security update of the terminal software would fix the vulnerability, then CaaS can consider refusing service access temporarily by a CSU terminal before a successful update according to the user agreement.

In most cases, the terminal software distribution of CaaS is public. Nonetheless, in some cases, a CSC might require customized terminal software and demand a limited range of software distribution, for example, only to CSC staff. The distribution should then be private. A bidirectional authentication would be necessary between a CSU and CaaS before a software download or update.

8.3 Service security

8.3.1 Orchestration security

Before an orchestration change is deployed or configured, it is necessary to evaluate whether the change can affect the security boundary, decrease the security level or confuse the trust relationship. If some negative effects are possible, then the security requirements or agreements of a CaaS should be re-negotiated and re-agreed by the CSP, CSC and even CSU.

8.3.2 Countering spam

CaaS should consider supporting a spam-countering function as an optional capability to a CSC. A CSP could also consider permitting CSC to integrate a third-party spam-countering function into its own CaaS. Different service and user agreements among CSPs, CSCs and CSUs could have different constraints on whether to and how to use a spam-countering function.

For example, if all CSUs are employees of a CSC and the corresponding CaaS is exclusively used for the benefit of a CSC, then it is possible that the agreement between the CSP and CSC is enough to utilize a spam-countering function.

Otherwise, if some CSUs are customers of a CSC, then it should be necessary for these CSUs to authorize the CSC (together with the CSP) to assist them to counter spam.

Generally speaking, a spam-countering function should be on the terminal side, cloud side or the combination of both. For alternative technologies used in the function, see [b-ITU-T X.1244] and [b-ITU-T X.1246].

8.4 Security coordination

8.4.1 Add-on and SDK security

CaaS should only allow add-ons that have passed through the security check available on its service. The terminal software should help CaaS to monitor and analyse any add-on anomaly. A white list would help CaaS to limit the capability of an add-on to access an external link or domain name.

If an add-on needs to access customer data to provide the service, a clear authorization by CSU is a precondition. A clear record of access to customer data by an add-on would be meaningful for later audit.

An SDK for CaaS should be able to monitor and analyse application anomalies or SaaS that integrates the SDK. The SDK should encrypt and isolate identity credentials to avoid any potential abuse. For example, application A and application B both integrate the same SDK and exist in the same terminal, but neither of them can access the other's identity credentials.

8.4.2 Infrastructure security

CaaS should be aware of the threats from the infrastructure, for example, as it integrates the service capabilities of telecommunication networks, such as SMS and voice call. CaaS should consider setting a gateway between itself and the telecommunication networks to monitor, counter or filter possible spam and identity fraud spread from telecommunication services. It would be meaningful if CaaS could alert CSUs of the types of communication channels or services in use.

Appendix I

A quick guide to the security threats and challenges listed in Recommendation ITU-T X.1601

(This appendix does not form an integral part of this Recommendation.)

As mentioned in clause 7, the security threats and challenges for cloud computing identified in [ITU-T X.1601] can apply to various CaaS scenarios. This appendix lists all security threats and challenges in [ITU-T X.1601] for quick check. If more details are needed, please see [ITU-T X.1601].

– Security threats for cloud computing
  a) Security threats for CSCs
    1) Data loss and leakage
    2) Insecure service access
    3) Insider threats
  b) Security threats for CSPs
    1) Unauthorized administration access
    2) Insider threats
– Security challenges for cloud computing
  a) Security challenges for CSCs
    1) Ambiguity in responsibility
    2) Loss of trust
    3) Loss of governance
    4) Loss of confidentiality
    5) Service unavailability
    6) CSP lock-in
    7) Misappropriation of intellectual property
    8) Loss of software integrity
  b) Security challenges for CSPs
    1) Ambiguity in responsibility
    2) Shared environment
    3) Inconsistency and conflict of protection mechanisms
    4) Jurisdictional conflict
    5) Evolutionary risks
    6) Bad migration and integration
    7) Business discontinuity
    8) Cloud service partner (CSN) lock-in
    9) Supply chain vulnerability
    10) Software dependencies

c) Security challenges for CSNs
    1) Ambiguity in responsibility
    2) Misappropriation of intellectual property
    3) Loss of software integrity

Appendix II

A mapping of security threats and security requirements

(This appendix does not form an integral part of this Recommendation.)

This appendix relates the threats in clause 7 with the requirements in clause 8 (see Table I.1).

Table I.1 – Mapping of security threats and security challenges in this Recommendation

Threats in clause 7	Corresponding requirements in clause 8
7.1. Identity threats	8.1. Identity and access management
7.1.1. Identity credential theft	8.1.1. Identity management 8.1.2. Access control 8.1.4. Account management
7.1.2. Identity counterfeit	8.1.3. Identity verification 8.1.4. Account management
7.2. Account lifecycle management threats	8.1.4. Account management
7.3. Orchestration threat	8.3.1. Orchestration security
7.4. Terminals context threat	8.2. Terminal security
7.5. Spam threat and malware distribution	8.2. Terminal security 8.3.2. Countering spam
7.6. Add-on threat	8.4.1. Add-on and SDK security
7.7. Software development kit threat	8.4.1. Add-on and SDK security
7.8. Threats from telecommunication network vulnerabilities	8.4.2. Infrastructure security

Bibliography

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.

[b-ITU-T X.1246] Recommendation ITU-T X.1246 (2015), *Technologies involved in countering voice spam in telecommunication organizations*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network.*

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ISO 15531-1] ISO 15531-1:2004, *Industrial automation systems and integration – Industrial manufacturing management data – Part 1: General overview*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020