

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3056

(02/2021)

SERIES Y: GLOBAL INFORMATION
INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS,
NEXT-GENERATION NETWORKS, INTERNET OF
THINGS AND SMART CITIES

Future networks

Framework for bootstrapping of devices and applications for open access to trusted services in distributed ecosystems

Recommendation ITU-T Y.3056

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE

General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899

INTERNET PROTOCOL ASPECTS

General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999

NEXT GENERATION NETWORKS

Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

FUTURE NETWORKS

Y.3000–Y.3499

CLOUD COMPUTING

Y.3500–Y.3599

BIG DATA

Y.3600–Y.3799

QUANTUM KEY DISTRIBUTION NETWORKS

Y.3800–Y.3999

INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES

General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.3056

Framework for bootstrapping of devices and applications for open access to trusted services in distributed ecosystems

Summary

Rapid advancements in communications and associated technologies has led to the emergence of distributed ecosystems with a large number of devices, applications and use cases requiring open access to trusted services. This open access to trusted services in distributed ecosystems can be provisioned by using the inherent security capabilities and mechanisms already present in the devices and the underlying networks. Recommendation ITU-T Y.3056 provides a concept of bootstrapping of devices and applications by network operators who can share the network security capabilities with users and providers of new devices and services. It describes the requirements to be fulfilled by the entities of the ecosystem such that they may benefit from the bootstrapping capabilities. Based on the requirements, a reference model as well as a functional architecture is provided, which together describe the elements, functions and reference points needed for provisioning of the bootstrapping capabilities. Finally, this Recommendation provides the information flows required to enable the bootstrapping capabilities.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3056	2021-02-13	13	11.1002/1000/14594

Keywords

Authentication, authorization, bootstrapping, bootstrap_token, trusted application, trusted device

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2021

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

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	Introduction	3
	6.1 Concept of trusted services.....	3
	6.2 Operator trust and bootstrapping of devices.....	3
	6.3 Role of network operators in enabling trusted services.....	5
7	Requirements	6
	7.1 Pre-conditions.....	6
	7.2 Requirements for the security token.....	7
	7.3 Requirements for the user entity.....	7
	7.4 Requirements for the trusted device entity	7
	7.5 Requirements for the network operator entity	7
	7.6 Requirements for the trusted application entity.....	8
	7.7 Requirements for the ASP entity	8
8	Reference model	8
	8.1 Elements of the trusted device entity.....	9
	8.2 Elements of the network operator entity	9
	8.3 Application element.....	10
	8.4 Security parameters	10
	8.5 Reference points	10
9	Functional architecture	11
	9.1 Functions of authentication element.....	12
	9.2 Functions of authorization element	12
	9.3 Bootstrapping function of the client element	13
	9.4 Token management function	14
	9.5 Session control function	15
	9.6 Specifications of reference points	15
10	Information flows	16
	10.1 Network operator bootstrapping capability exposure.....	16
	10.2 ASP on-boarding flow	17
	10.3 Trust extension flow for user and device	18
	10.4 Bootstrap_token generation flow	19

	Page
10.5 Trusted device and application session flow	21
10.6 Flow for change of network operator	21
11 Security considerations	23
Bibliography.....	24

Recommendation ITU-T Y.3056

Framework for bootstrapping of devices and applications for open access to trusted services in distributed ecosystems

1 Scope

This Recommendation describes the concept, architecture and information flows for bootstrapping of devices and applications by network operators, by providing:

- a bootstrapping concept for entities requiring open access to trusted services in their interactions;
- the requirements imposed on the entities for enabling the bootstrapping capabilities;
- a reference model showing the elements required for bootstrapping;
- a functional architecture diagram showing functions, reference points and security parameters; and
- information flows for the operation of the bootstrapping processes.

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.1124] Recommendation ITU-T X.1124 (2007), *Authentication architecture for mobile end-to-end communication*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 secure element [b-ITU-T X.1158]: A dedicated microprocessor system that contains an operating system, memory, application environment and security protocols intended to be used to store sensitive data and execute sensitive applications.

NOTE – A secure element may reside in a universal subscriber identity module (USIM), a dedicated chip in a phone's motherboard, an external plug in a memory card or as an integrated circuit card.

3.1.2 security degree [ITU-T X.1124]: An identifier (e.g., number) that represents a set of security parameters including at least one authentication mechanism, the crypto algorithms and related parameters to reflect the security requirement of a certain service. It is defined to profile the security requirement of each service.

3.1.3 session key [b-ITU-T X.1113]: The session key is a temporary key used to encrypt data for the current session only. The use of session keys keeps the secret keys even more secret because they are not used directly to encrypt the data. Secret keys are used to derive the session keys using various methods that combine random numbers from either the client or server or both.

3.1.4 trust [b-ITU-T Y.3052]: The measurable belief and/or confidence which represents accumulated value from history and the expecting value for future.

NOTE – Trust is quantitatively and/or qualitatively calculated and measured. Trust is used to evaluate values of entities, value-chains among multiple stakeholders, and human behaviours including decision making.

3.1.5 user [b-ITU-R F.1399]: Any entity external to the network which utilizes connections through the network for communication.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 bootstrapping: A cryptographic process of binding user identity(ies) to the keying material provisioned in the secure element of the user's device, enabling the device to communicate securely with trusted services.

NOTE – Bootstrapping for open access acknowledges the existence and need for one or more identities, which may be associated with any of the bootstrapping for open access actors e.g., user, user's network, user's device, application services provider (ASP) or trusted application.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AKA	Authentication and Key Agreement
API	Application Programming Interface
ASP	Application Services Provider
CIN	Company Identification Number
FQDN	Fully Qualified Domain Name
GBA	Generic Bootstrapping Architecture
GSM	Global System for Mobile communication
HTTP	Hyper Text Transfer Protocol
ICT	Information and Communication Technology
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IPSec	Internet Protocol Security
KYC	Know Your Customer
MAC	Media Access Control
MSISDN	Mobile Subscriber International Services Directory Number
PSK-TLS	Pre-Shared Key Cipher suites for Transport Layer Security
SIM	Subscriber Identification Module
TLS	Transport Layer Security
UID	Universal Identifier or Public Entity Identifier
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module

5 Conventions

In this Recommendation, requirements are classified as follows:

- The keywords "is required to/ are required to" indicate a requirement/requirements, 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, such requirements need not be present to claim conformance; and
- The keywords "optionally" or "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option; it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Introduction

The concept of trusted devices, operator trust and bootstrapping of devices and the role of network operators in enabling trusted services is described below.

6.1 Concept of trusted services

Certain services require additional checks prior to making them available to a beneficiary. A license to drive cars, access to restricted premises, permissions for online banking are a few examples of trusted services each of which require some previous introduction between the intended beneficiary and the provider of the trusted service. Further, these services may have applications which require privacy and security of the information exchanged with the user/device that is using the application. Such services, that require user verification and security of the information, are referred to as trusted services.

Rapid developments in embedded electronics and information and communication technology (ICT) are leading to new and evolving ecosystems of devices and applications that are enabling advanced services by interconnecting physical and virtual things.

These developments require suitable improvements in the ICT infrastructure for identification, authentication and authorization amongst the unrelated and diverse set of entities within the ecosystem including users, service providers, devices, networks and applications. Network operators play an important role in connecting the user's devices to the Internet and with the applications. With some improvements in its ICT infrastructure, the network operator can extend its role to provide the required trust between hitherto unknown entities of the ecosystem. If the ICT layer interfaces and related processes are standardized over a wide range of network technologies, the new standardized infrastructure can be used for an open yet secured access and interactions between devices and applications in distributed ecosystems. This Recommendation provides for the required capabilities and functions to achieve this end.

NOTE – This Recommendation incorporates support for the establishment of trust by the operator for the user and user's device. The reciprocal aspect, in which the user or the user's device establishes the trustworthiness of the network/network operator is also important, especially in the context of the imminent proliferation of private networks, and may be a candidate for further standardization work.

6.2 Operator trust and bootstrapping of devices

The network operator establishes a trust relationship with its subscribers and devices by

- undertaking the verification of every new customer prior to permitting the person access to its services and infrastructure (subscriber verification);

- authenticating the devices through the associated secure element of the devices and the network's security nodes (device authentication).

The network operator creates a measurable degree of trust by verifying its subscribers as per the regulatory or ecosystem norms. As an example, the requirement for verification of subscribers differs when considering prepaid versus post-paid users, or when considering the offer of domestic versus international roaming services. The trust generated by the network operator may create a basis for a differentiated offering of trusted services to a user. For example, a prepaid user that has a lower degree of trustworthiness may be permitted to use non-critical services by an ASP, whereas a post-paid user, verified to a higher degree of trust, may be offered a different class of services.

Once the trust relationship is established between the person and the network operator, the person is referred to as a subscriber as it becomes eligible to use and pay for the network services like calling, messaging, Internet access, etc.

Whilst operator trust ensures identification of users, modern networks have placed a lot of focus on ensuring that the device:

- has a valid and unique identifier that cannot be easily created by an entity other than the manufacturer and can be used for authentication; and
- can be permitted or restricted from connecting to the network i.e., can be authorized or rejected.

The concepts of bootstrapping of devices and that of operator trust provide an important basis for fulfilling the requirements of authentication and authorization when considering the interactions between the users, devices and applications from distributed and diverse ecosystems. However, different network technologies have different schemas and mechanisms for establishing the trust. Network operators may also use different processes for implementing the operator trust even within the same network technology. If a uniform mechanism was provided such that the network operator trust could be used for enabling secure interactions between diverse and distributed ecosystems of devices and applications, it could make it very easy for orderly proliferation of trusted services.

For example, in cellular mobile networks, the authentication between the device and the network is managed by a secure procedure that is executed between the device, the secure element of the subscriber identification module (SIM) and an authorization node in the network. The concept of bootstrapping of devices is meant to extend the authentication and authorization process described above for use by third party applications. To accomplish this, the existing capabilities of the device and networks are extended (e.g., by using different authentication algorithms, or different keys, etc.) to the device-based applications, often by the use of a security token that is generated at the time of enrolling the device for enabling such an extended network authentication.

The security token has a crucial role as it acts like a digital identifier for all of the following:

- the application for which it is generated;
- the device on which it is generated; and
- the network and the network node for which it is generated.

Other than acting as the identifier, the security token also embodies the keying material (key data which is used to protect the security communication of the device and the network) the key length, generation algorithm and lifetime are set according to parameters, such as service type and security degree) required for securing the interactions between the device and the third-party applications.

Transferring of security token(s) between the device and the network is best avoided as it represents a risk of compromise of the token during the process of transfer. As a result, mechanisms exist that allow security tokens to be independently generated by the device and the network. These mechanisms are standardized as authentication and key agreement (AKA) processes.

The bootstrapping of a device may thus be described as a process in which: