

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1451

(05/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Security protocols
(2)

Risk identification to optimize authentication

Recommendation ITU-T X.1451

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.1451

Risk identification to optimize authentication

Summary

Recommendation ITU-T X.1451 specifies a risk identification function in an information and communication technology (ICT) service system as a pre-processor before the authentication function is invoked. It enables the ICT service system to optimize user authentication based on identified risks.

With this specific risk identification function, the ICT service system can make choices on authentication mechanisms adaptively to its users and achieve multiple benefits such as: 1) to improve user experiences; 2) to increase the capacity and reduce the per transaction cost of user authentication; and 3) to reduce the risk of user identity forgery.

For ICT systems, user authentication is a critical security function. Various authentication mechanisms are available, but it may not be clear how to make the best choice from a number of options. Authentication of ICT services should strive to balance multiple functional objectives such as security, user experience, cost and performance.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1451	2020-05-29	17	11.1002/1000/14252

Keywords

Authentication, risk identification.

* 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/>.

© ITU 2020

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.....	1
4 Abbreviations and acronyms	3
5 Conventions	3
6 Introduction.....	3
7 Reference model of an ICT service system with risk identification.....	4
8 Functional components of risk identification subsystem.....	5
8.1 Risk-monitoring module.....	5
8.2 Risk repository module.....	5
8.3 Risk identification engine	7
9 Authentication subsystem.....	10
10 Alternative processing designs for risk identification engine.....	11
Annex A – Non-functional design considerations	13
A.1 Non-functional design criteria	13
A.2 Stability.....	13
A.3 Security	14
A.4 Flexibility	14
A.5 Ease of integration	14
A.6 Manageability	14
A.7 Auditability.....	16
Appendix I – Use case: Risk identification to optimize login authentication.....	17
Appendix II – A risk repository example for mobile payment system	20
Appendix III – A mathematical interpretation of a multi-tier processing design	22
Bibliography.....	23

Recommendation ITU-T X.1451

Risk identification to optimize authentication

1 Scope

This Recommendation specifies a risk identification function in an information and communication technology (ICT) service system as a pre-processor before the authentication function is invoked. It enables the ICT service system to optimize user authentication based on identified risks.

This Recommendation covers the following topics:

- a reference model of an ICT service system where a risk identification function is introduced in between the core service-handling subsystem and the authentication subsystem;
- a detailed explanation of the component modules of this risk identification function, and how risks are identified, and user authentication is optimized;
- alternative processing designs for the risk identification engine.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 level of risk [b-ISO Guide 73]: Magnitude of a risk (3.1.4) or combination of risks, expressed in terms of the combination of consequences and their likelihood.

3.1.2 risk evaluation [b-ISO Guide 73]: Process of comparing the results of risk analysis (3.1.5) with risk criteria (3.1.6) to determine whether the risk (3.1.4) and/or its magnitude is acceptable or tolerable.

NOTE – Risk evaluation assists in the decision about risk treatment (3.1.9).

3.1.3 risk identification [b-ISO Guide 73]: Process of finding, recognizing and describing risks (3.1.4).

NOTE 1 – Risk identification involves the identification of risk sources, events (3.1.2), their causes and their potential consequences (3.1.1).

NOTE 2 – Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 consequence: Outcome of an event (see clause 3.1.2) affecting objectives.

NOTE 1 – An event can lead to a range of consequences.

NOTE 2 – A consequence can be certain or uncertain and in the context of information security is usually negative.

NOTE 3 – Consequences can be expressed qualitatively or quantitatively.

NOTE 4 – Initial consequences can escalate through knock-on effects.

NOTE 5 – Based on the definition given in [b-ISO Guide 73].

3.2.2 event: Occurrence or change of a particular set of circumstances.

NOTE 1 – An event can be one or more occurrences and can have several causes.

NOTE 2 – An event can consist of something not happening.

NOTE 3 – An event can sometimes be referred to as an "incident" or "accident".

NOTE 4 – Based on the definition given in [b-ISO Guide 73].

3.2.3 risk: Effect of uncertainty on objectives.

NOTE 1 – An effect is a deviation from the expected – positive and/or negative.

NOTE 2 – Objectives can have different aspects (such as financial, health and safety, information security, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3 – Risk is often characterized by reference to potential events and consequences, or a combination of these.

NOTE 4 – Information security Risk is often expressed in terms of a combination of the consequences of an information security event and the associated likelihood of occurrence.

NOTE 5 – Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

NOTE 6 – Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

NOTE 7 – Based on the definition given in [b-ISO Guide 73].

3.2.4 risk analysis: Process to comprehend the nature of risk and to determine the level of risk.

NOTE 1 – Based on the definition given in [b-ISO Guide 73].

3.2.5 risk criteria: Terms of reference against which the significance of a risk is evaluated.

NOTE 1 – Risk criteria are based on internal and external context, and are regularly reviewed to ensure continued relevance.

NOTE 2 – Risk criteria can be derived from standards, laws and policies.

NOTE 3 – Based on the definition given in [b-ISO Guide 73].

3.2.6 risk treatment: Process to modify risk.

NOTE 1 – Risk treatment can involve:

- avoiding the risk by deciding not to start or continue with the activity that give rise to the risk;
- seeking an opportunity by deciding to start or continue with an activity likely to create or enhance the risk;
- removing the source of the risk;
- changing the nature and magnitude of likelihood;
- changing the consequences;
- sharing the risk with another party or parties; and
- retaining the risk by choice.

NOTE 2 – Risk treatments that deal with negative consequences are sometimes referred to as risk mitigation, risk elimination, risk prevention, risk reduction, risk repression and risk correction.

NOTE 3 – Risk treatment can create new risks or modify existing risks.

NOTE 4 – Based on the definition given in [b-ISO Guide 73].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
ICT	Information and Communication Technology
ID	Identifier
IP	Internet Protocol
OTP	One-Time Password
PIN	Personal Identification Number
SMS	Short Message Service

5 Conventions

None.

6 Introduction

For many ICT service systems, user authentication is a critical security function. Various authentication mechanisms are available, but it may not be clear how to make the best choice from a number of options. Authentication of ICT services should strive to balance multiple functional objectives such as security, user experience, cost and performance.

Multi-factor authentication is a successful technology in ICT, but should not be regarded as universal for all cases. Example considerations follow.

- User needs to remember a password, bring a hard token, install a soft certificate, check a mobile phone short message service (SMS), look into a camera, etc. The login and authentication process can be complicated and not user friendly.
- For an ICT service system with both a very large number of users and a high access concurrence, simply applying multi-factor authentication to every single user will impose an extremely large burden on both its authentication subsystem and communication network. This will further increase delay in response and impair user experience, as well as imposing a high authentication cost per transaction.
- Although multi-factor authentication ensures fairly good security for the identification of ICT users, it is still not sufficient for applications related directly to monetary resources, such as digital financial services. Forgery or cloning of authentication credentials, Trojans, phishing websites and ever-changing attack techniques of adversaries are great risks to such services and cannot be solved by multi-factor authentication alone.

Considering these challenges, this Recommendation introduces a risk identification function to optimize user authentication.

Traditionally, an authentication subsystem is closely coupled with the core service-handling subsystem and is invoked according to fixed rules when service requests are received. This Recommendation recommends that the core service-handling subsystem and the authentication subsystem be decoupled and a risk identification function (called a "risk identification subsystem") inserted between them. This helps to make authentication-related risk decisions before the authentication subsystem is invoked.

With this specific risk identification function, the ICT service system can adapt choices of authentication mechanisms to its users and achieve the following benefits:

- 1) to improve user experience;
- 2) to increase the capacity and reduce the per transaction cost of authentication; and
- 3) to reduce the risk of user identity forgery.

7 Reference model of an ICT service system with risk identification

A reference model of an ICT service system with risk identification to optimize user authentication is shown as Figure 1.

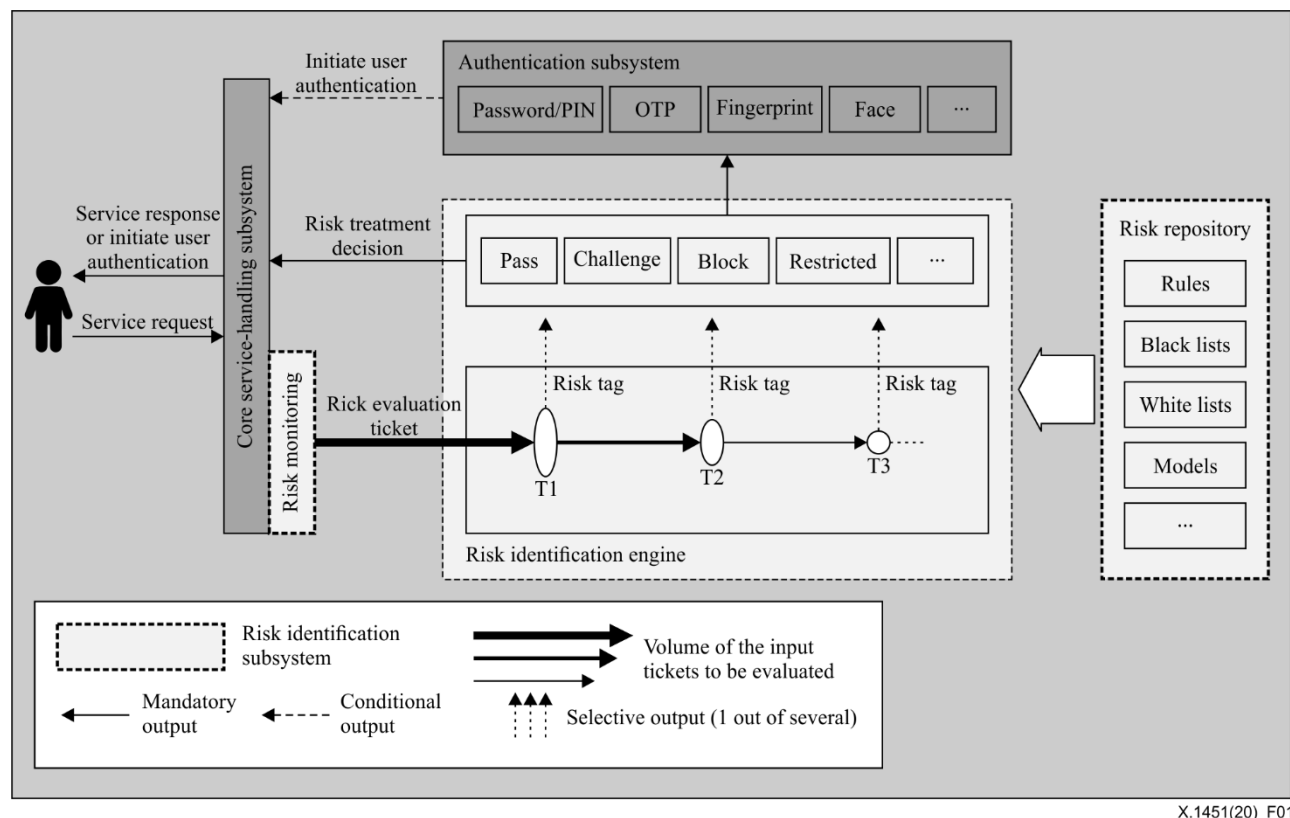


Figure 1 – Reference model of an ICT service system with risk identification to optimize user authentication

In this reference model, the risk identification subsystem is shown as a new function introduced into a traditional ICT service system.

The risk identification subsystem composes the following components, shown in boxes with dashed borders in Figure 1.

- The **risk-monitoring module** resides in the core service-handling subsystem side. It monitors and collects information relevant to risk identification when the core service-handling subsystem receives a service request from the user. The relevant information includes, but is not limited to, information about the user device, user behaviour and user account, and information about the service request itself. All information collected by the risk-monitoring module regarding a given service request should be passed to the risk identification engine in real time.
- The **risk identification engine** is located between the core service-handling and the authentication subsystems. It identifies and evaluates the risk(s) associated with a given service request based on the risk evaluation ticket fed by the risk-monitoring module and the