

Recommendation

ITU-T X.1280 (03/2024)

SERIES X: Data networks, open system communications
and security

Cyberspace security – Identity management (IdM) and
Authentication

Framework for out-of-band server authentication using mobile devices

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	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
Cybersecurity	X.1200-X.1229
Countering spam	X.1230-X.1249
Identity management (IdM) and Authentication	X.1250-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1839
METAVEVERSE AND DIGITAL TWIN SECURITY	X.2000-X.2199
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249

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

Recommendation ITU-T X.1280

Framework for out-of-band server authentication using mobile devices

Summary

In the authentication technology standards, verifier impersonation resistance is considered as a requirement of the highest level of authentication assurance. However, existing authentication technologies focus on user authentication and service providers cannot be verified explicitly.

Recommendation ITU-T X.1280 provides a framework for out-of-band server authentication using mobile devices, which resolves the vulnerability of verifier impersonation and the limitation of user terminal dependency of the existing authenticators. It allows a user to provide user authentication information after verifying the service provider explicitly and independently in the user authentication process on any user terminals.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1280	2024-03-01	17	11.1002/1000/15661

Keywords

Authentication, authenticator, relying party, verification, verifier, verifier impersonation resistance.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

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 2024

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	2
5 Conventions	2
6 Introduction.....	3
7 Framework for out-of-band server authentication	4
7.1 Roles and components	4
7.2 Server authentication information	5
7.3 Authentication model	5
8 Procedures for out-of-band server authentication.....	6
8.1 Out-of-band server authenticator installation and registration.....	6
8.2 Server authentication request	7
8.3 Server authentication information generation and presentation.....	7
8.4 Server authentication	9
8.5 User authentication and service provision.....	10
9 Security threats and security requirements	10
9.1 Security threats	10
9.2 Security requirements	11
Annex A – Extra procedure for out-of-band server authentication	12
A.1 User password automatic renewal	12
Appendix I – Relationship between security requirements and threats	13
Appendix II – Use cases of out-of-band server authentication model.....	14
II.1 Websites and applications	14
II.2 IdPs	14
II.3 Operating systems	15
Appendix III – Relationship to other authentication technologies	17
Bibliography.....	19

Recommendation ITU-T X.1280

Framework for out-of-band server authentication using mobile devices

1 Scope

This Recommendation provides a framework for out-of-band server authentication using mobile devices including the following:

- defines the out-of-band server authentication model and authentication procedure;
- defines criteria and guidelines for generating server authentication information using mobile devices;
- defines security threats and security requirements in the out-of-band server authentication model;
- describes use cases of the out-of-band server authentication model; and
- describes the relationship to other authentication technologies.

This Recommendation does not address issues related to user authentication, regulation, and privacy considerations.

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 authentication [b-ISO/IEC 18014-2]: Provision of assurance of the claimed identity of an entity.

3.1.2 credential service provider (CSP) [b-ITU-T X.1254]: A trusted actor that issues or manages credentials.

3.1.3 relying party (RP) [b-ITU-T X.1254]: Actor that relies on an identity assertion or claim.

3.1.4 verification [b-ISO/IEC 29115]: Process of checking information by comparing the provided information with previously corroborated information.

3.1.5 verifier [b-ISO/IEC 29115]: Actor that corroborates identity information.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 server authentication: Process of verifying the authenticity of the service provider by comparing server authentication information generated by the verifier and a user's out-of-band server authenticator.

3.2.2 server authentication information: Authentication code which is generated using a challenge and response one-time password (OTP) algorithm in the verifier and a user's out-of-band server authenticator.

3.2.3 out-of-band user authentication: Process of verifying the authenticity of a user using another commutation channel which is separate from the communication channel used to sign in or perform a transaction.

3.2.4 out-of-band server authentication: Process of verifying the authenticity of a server using another commutation channel which is separate from the communication channel used to sign in or perform a transaction.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AI	Artificial Intelligence
ATM	Automated Teller Machine
CSP	Credential Service Provider
CTAP	Client To Authenticator Protocol
DNS	Domain Name System
FIDO	Fast Identity Online
ID	Identification
IdP	Identity Provider
IP	Internet Protocol
OAuth	Open Authentication
OTP	One-Time Password
PAM	Pluggable Authentication Modules
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RP	Relying Party
SAML	Security Assertion Markup Language
SMS	Short Message Service
SSL	Secure Socket Layer
QR	Quick Response
U2F	Universal Two Factor

5 Conventions

This Recommendation applies the following verbal forms for the expression of provisions:

- a) "Shall" indicates a requirement,
- b) "Should" indicates a recommendation,

- c) "May" indicates a permission,
- d) "Can" indicates a possibility or a capability.

6 Introduction

In traditional user authentication, only the server authenticates the user and the user is vulnerable to cyber-attacks such as phishing and pharming.

Public key infrastructure (PKI) based server authentication is adequate for the user when using browser-based applications with an address bar. PKI-based authentication is also performed independently of the user authentication process, which makes the user easily overlooked.

This Recommendation provides a framework for out-of-band server authentication using mobile devices, designed to authenticate the server by the user first and help the user to engage with server authentication explicitly in connection with the user authentication process. In user authentication, any user authentication processes can be applied together.

Out-of-band server authentication can be used by browser-based applications and many types of applications and operating systems.

Out-of-band server authentication is performed by verifying the server authentication information by the user and then verifying the user authentication information by the server, thereby providing the verifier impersonation resistance.

With out-of-band server authentication, service providers and users achieve the following benefits:

- 1) User-centric authentication: Instead of asking the user to remember and input their complex user authentication information, the server presents its authentication information so that the user authenticates the server. Users are free from user credential management burdens by changing the user's role from inputting user authentication information to verifying server authentication information. Figure 1 shows user-centric authentication.



Figure 1 – User-centric authentication

- 2) Mutual authentication: The user verifies the server's authenticity with server authentication information generated by the server and the out-of-band server authenticator, respectively. The server verifies the user's authenticity with user authentication information sent after the user confirms two server authentication information matches. Figure 2 shows mutual authentication.