ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

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 |
| METAVERSE 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/.

## 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.

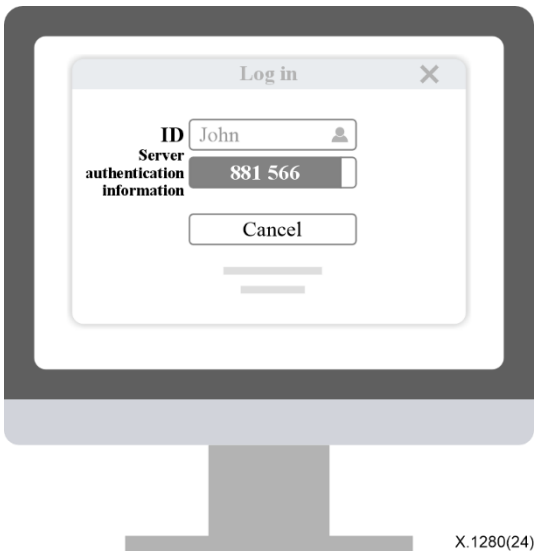


**Figure 1 – User-centric authentication**

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.

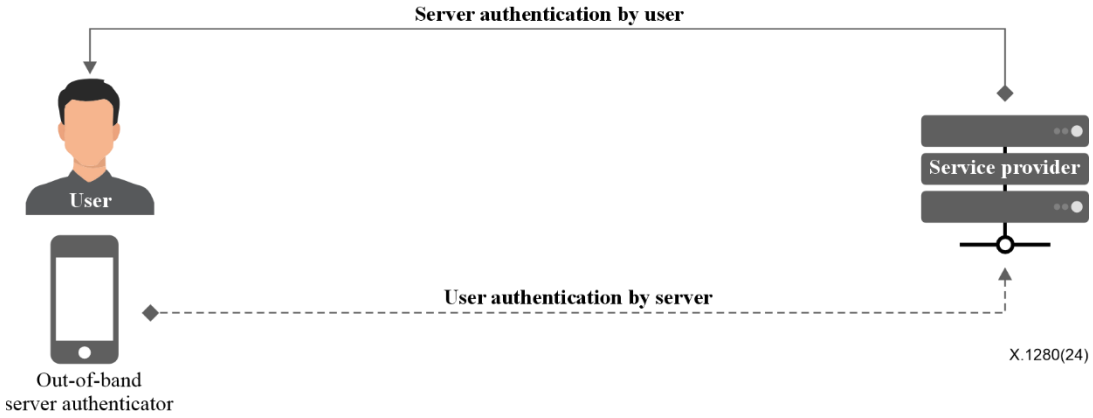


**Figure 2 – Mutual authentication**

3) Unified authentication: Even though more additional user terminals are added, such as computers, smartphones, automated teller machines (ATM) and artificial intelligence (AI) speakers, authentication methods can be unified since the servers present their server authentication information to the user instead of asking the user to input a variety of authentication information. Figure 3 shows unified authentication.

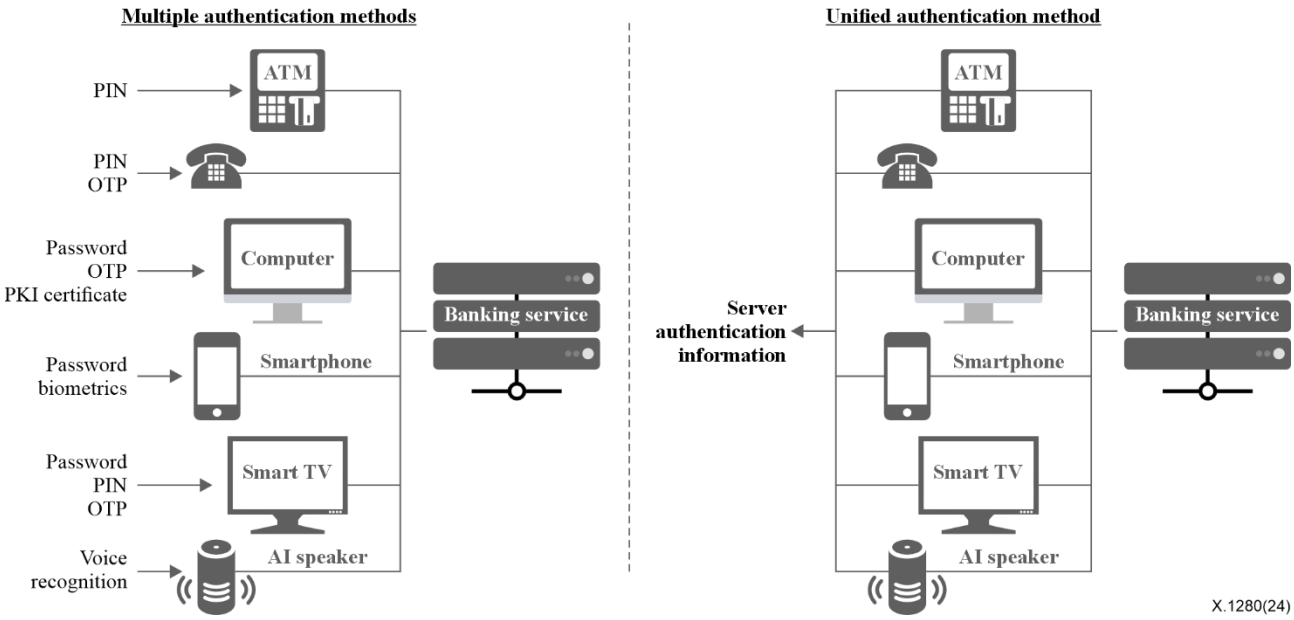


**Figure 3 – Unified authentication (e.g., Banking service)**

## 7 Framework for out-of-band server authentication

The roles and components of the authentication model for the out-of-band server authentication framework, which enables mutual authentication between the user and the server, are defined in this clause. The core flow is verifying the server authentication information by the user first, then verifying the user authentication information by the server.

### 7.1 Roles and components

Table 1 is the list of the roles and components of the out-of-band server authentication framework.

**Table 1 – Roles and components of out-of-band server authentication model**

| Name | Description |
|---|---|
| Verifier | A verifier generates server authentication information in response to the user's request. The information is sent to the relying party to be presented to the user. It sends the offset for generating server authentication information to the out-of-band server authenticator to generate server authentication information to present to the user. |
| Relying party | A relying party presents server authentication information generated and sent by the verifier to the user. |
| User | A user receives services from relying parties and verifiers. |
| User terminal | A user terminal shows server authentication information through applications. Examples of user terminals are computers, smartphones, ATMs and AI speakers. |
| Out-of-band server authenticator | An out-of-band server authenticator generates server authentication information using the offset sent by the verifier. |

## 7.2 Server authentication information

Server authentication information is a multi-digit code used when the user authenticates the server. It shall be generated using the challenge and response one-time password (OTP) once the user requests. Dynamic challenge values and a verification key are used to compute and generate server authentication information. The dynamic challenge values and the verification key are defined in clause 8.

If the server authentication information generated by the server matches the server authentication information generated by the user's out-of-band server authenticator, the server's authenticity is verified.

## 7.3 Authentication model

The main flow of the out-of-band server authentication is that the user authenticates first the server by comparing server authentication information generated by the verifier and the out-of-band server authenticator. Once the user authenticates the server, the authenticator generates user authentication information and sends it to the verifier. The verifier authenticates the user with user authentication information.

Figure 4 illustrates an overview of out-of-band server authentication using mobile devices.

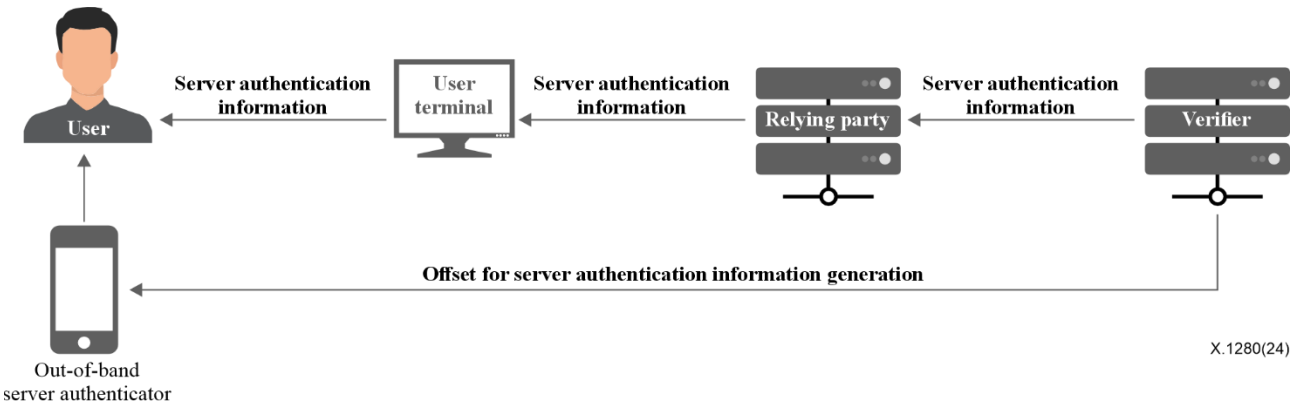


**Figure 4 – Overview of out-of-band server authentication using mobile devices**

In order to initiate the out of band server authentication using mobile devices, it requires a user to type the user ID into the user terminal with a screen. Once the user enters the ID on the user terminal, the relying party shall present server authentication information generated by the verifier to the user first in the user terminal. Then the user compares it with the server authentication information generated by the user's out-of-band server authenticator.

# 8 Procedures for out-of-band server authentication

## 8.1 Out-of-band server authenticator installation and registration

In the out-of-band server authenticator installation and registration step, the user installs the authenticator application on the smartphone and registers it in the verifier.

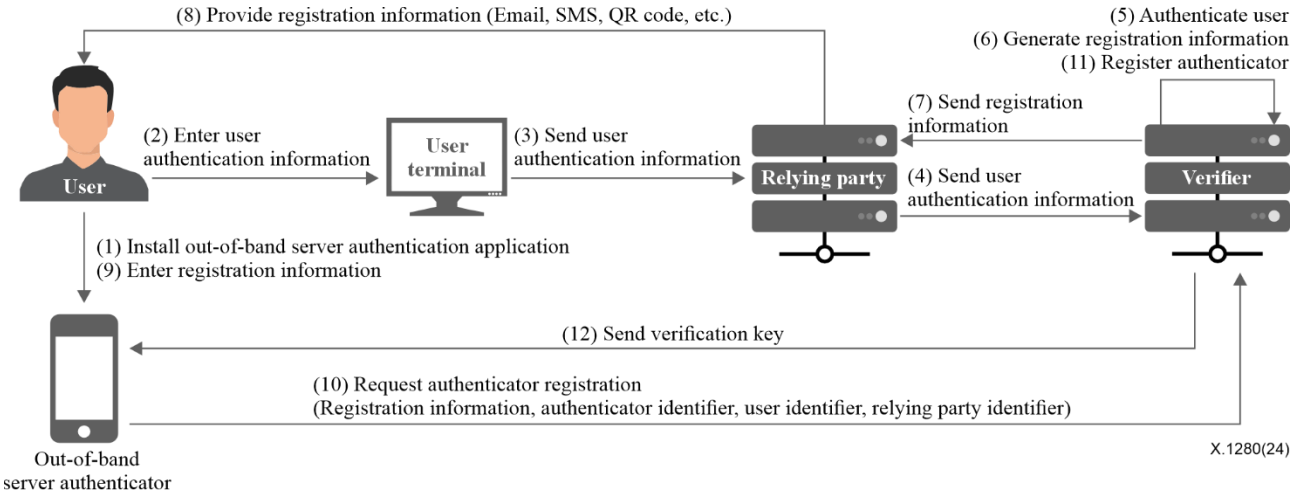


**Figure 5 – Flow of out-of-band server authenticator installation and registration**

Figure 5 identifies the data required in the out-of-band server authenticator installation and registration step and shows the flow. The explanation of the flow is as follows:

(1) The user installs the out-of-band server authenticator application on the smartphone.

(2) The user enters the user authentication information through the user terminal to authenticate as a legitimate user by a reliable method, such as login, e-mail verification, or mobile phone identification, according to the policy of the relying party.

(3) The user authentication information entered in the user terminal is sent to the relying party.

(4) The relying party sends the user authentication information to the verifier.

(5) The verifier authenticates the user.

(6) The verifier generates registration information corresponding to the authenticated user.

(7) The verifier sends the generated registration information, including the user identifier of the relying party and the relying party identifier, to the relying party.

(8) The relying party provides the user with the registration information using trusted methods, such as e-mail, text message, quick response (QR) code, etc.

(9) The user inputs the authenticator registration information into the authenticator installed in the smartphone.

(10) The authenticator sends the registration information, authenticator identifier, user identifier, and relying party identifier to the verifier.

(11) The verifier verifies the registration information and registers the authenticator with the authenticator identifier, user identifier, and relying party identifier.

(12) After registering the authenticator, the verifier sends the corresponding verification key to the authenticator.

The out-of-band server authenticator registration process shall be provided and performed by applying secure socket layer (SSL) protocol using ITU-T X.509 certificates to secure communication between the authenticator and the verifier.

In the case that the out-of-band server authenticator is unable to be used due to loss or damage, the verifier may allow the user to register more than one out-of-band server authenticator as a backup authenticator.

## 8.2 Server authentication request

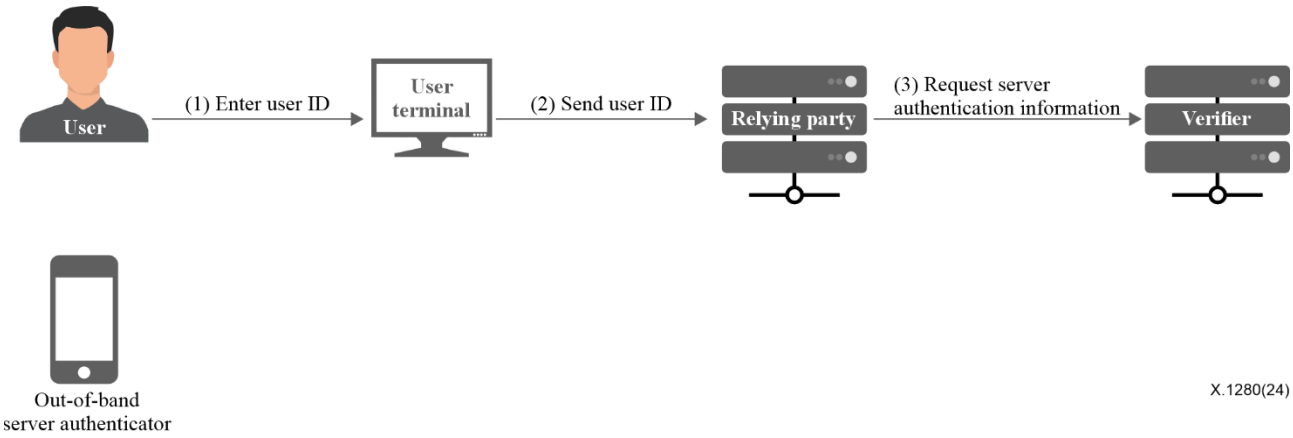


**Figure 6 – Flow of server authentication request**

Figure 6 identifies the data required in the server authentication request step and shows the flow. The explanation of the flow is as follows:

(1) The user in the user terminal connects to the relying party, then enters their ID.

(2) The user ID entered in the user terminal is sent to the relying party.

(3) The relying party requests server authentication information to the verifier.

## 8.3 Server authentication information generation and presentation

In the server authentication information generation and presentation step, the verifier generates server authentication information corresponding to the user ID once it has received the server authentication request from the relying party. Then the verifier sends the server authentication information to the relying party to display on the screen of the user terminal. The verifier also sends the offset to the user's out-of-band server authenticator. The authenticator uses the received offset to generate server authentication information and presents the generated server authentication information.

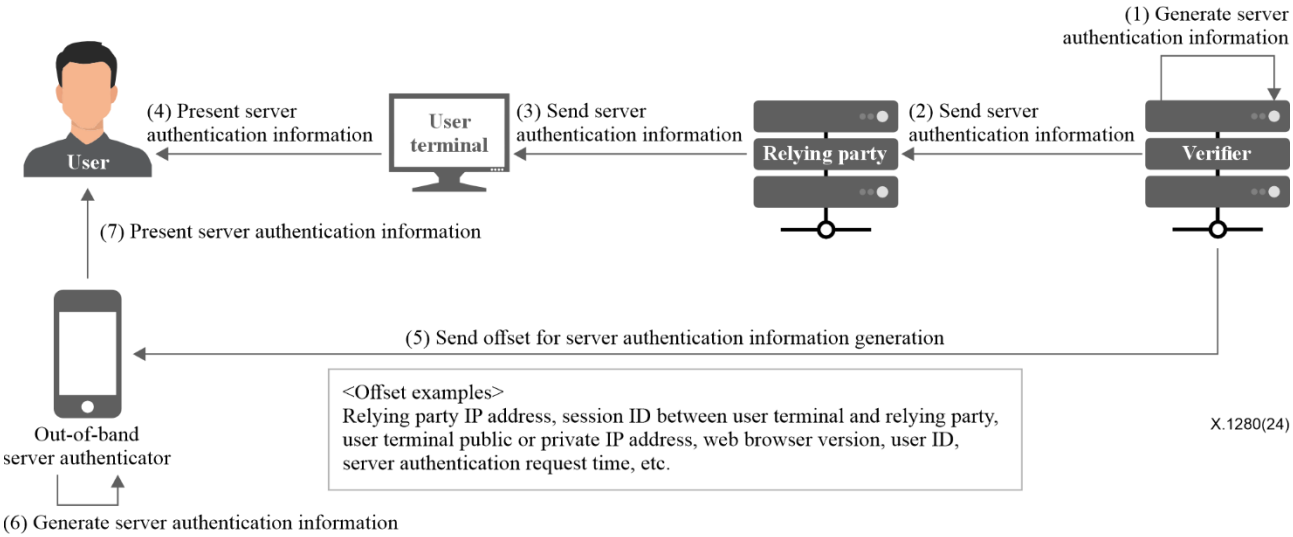


**Figure 7 – Flow of server authentication information generation and presentation**

Figure 7 identifies the data required in the server authentication information generation and presentation step and shows the flow. The explanation of the flow is as follows:

(1) The verifier generates server authentication information once the server authentication request is received, including the user ID and the offset from the relying party. The verifier computes and generates server authentication information with the verification key, which both the verifier and the user's out-of-band authenticator have received and stored during the out-of-band server authenticator installation and registration step, and the offset.

(2) The verifier sends the generated server authentication information to the relying party.

(3) The relying party sends the received server authentication information to the user terminal.

(4) The relying party presents the server authentication information to the user through the user terminal.

(5) The verifier also sends the offset for generating server authentication information to the user's out-of-band server authenticator.

(6) The user's out-of-band server authenticator computes and generates server authentication information with the verification key, which both the verifier and the user's out-of-band authenticator have received and stored during the out-of-band server authenticator installation and registration step and the offset.

(7) The out-of-band server authenticator also presents server authentication information generated by itself to the user.

The offset should include the Internet protocol (IP) address of the relying party server, the session ID between the user terminal and the relying party server, the public IP address of the user terminal, the private IP address of the user terminal, the web browser version of the user terminal, the user ID, and the user's server authentication request time.

Server authentication information should be computed and generated using the verification key and the offset, and then should be converted into a value that is easy for users to read. The value should be at least a 6-digit number or a string. The value should be displayed in the user terminal and out-of-band server authenticator. In addition, server authentication information should have an appropriate validity time according to the type of online services and should visually show the remaining validity time in various forms within the server authentication information display area as illustrated in Figure 8.


**Figure 8 – Example of server authentication information presentation**

Instead of comparing authentication information by the user, the relying party may display a QR code, which includes the server authentication information for the out-of-band server authenticator to read and verify the code. The authenticator then displays understandable information to the user so they can verify whether the server is authentic.

## 8.4 Server authentication

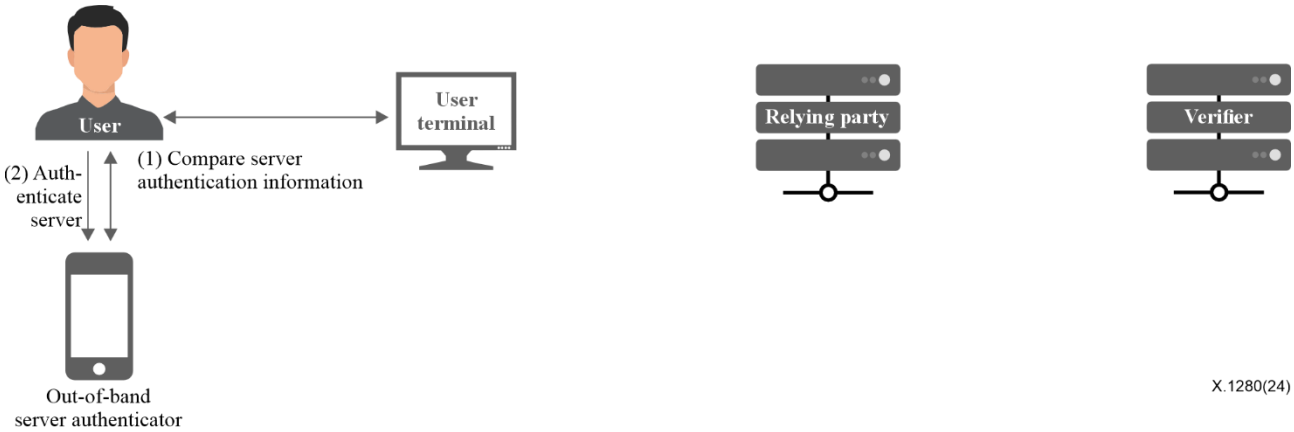


**Figure 9 – Flow of server authentication**

Figure 9 identifies the data required in the server authentication step and shows the flow. The explanation of the flow is as follows:

(1) The user visually compares and verifies server authentication information presented in both the terminal and the out-of-band server authenticator.

(2) The user authenticates the server by selecting approval in the user's out-of-band authenticator.

## 8.5 User authentication and service provision

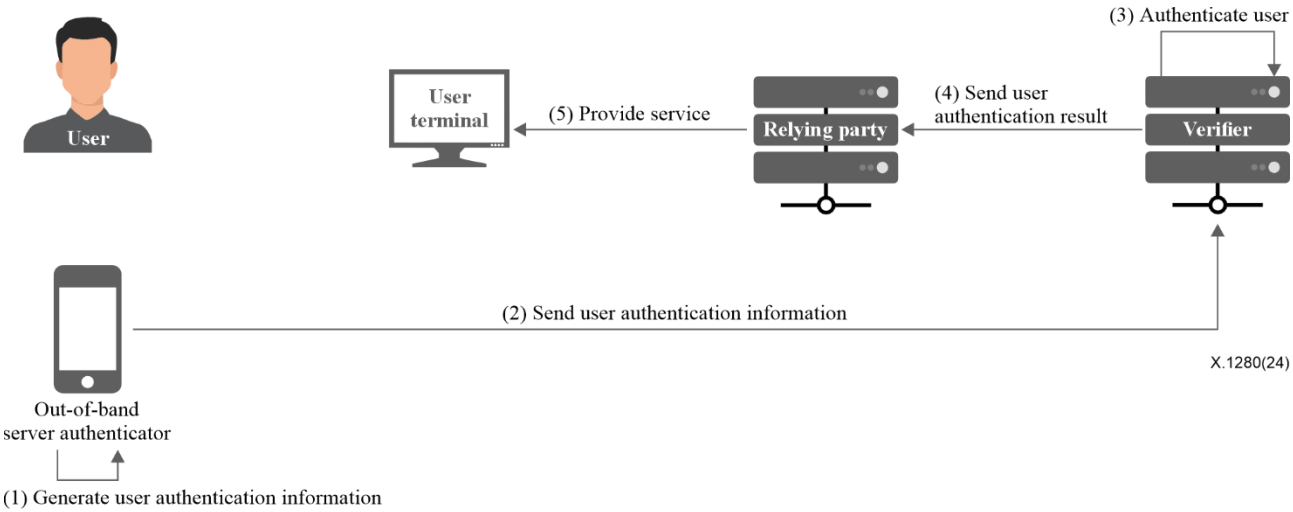


**Figure 10 – Flow of user authentication and service provision**

Figure 10 identifies the data required in the user authentication and service provision step and shows the flow. The explanation of the flow is as follows:

(1) When the user authenticates the server in the user's out-of-band server authenticator, the authenticator generates the user's dynamic user authentication information, such as a one-time password. In order to confirm the legitimate user's use of the authenticator, the user can be identified by using biometric information such as the user's face and fingerprint or personal identification number (PIN) on the smartphone.

(2) The user's out-of-band server authenticator sends the user authentication information to the verifier.

(3) The verifier authenticates the user by verifying the received user authentication information.

(4) The verifier sends the user authentication result to the relying party.

(5) The relying party provides the service according to the user authentication result received from the verifier.

Instead of dynamic user authentication information, strong PKI-based user authentication can be used, such as PKI and fast identity online (FIDO). The required challenge value in PKI-based user authentication can be received together in the server authentication information generation and presentation step, or the received offset can be used as the challenge value.

# 9 Security threats and security requirements

## 9.1 Security threats

In this clause, potential security threats that may arise from the out-of-band server authentication model are identified.

### 9.1.1 Fraudulent online service provider

An attacker makes a user access a fraudulent online service provider and induces the user to enter their password to be stolen instead of using the out-of-band server authenticator.

### 9.1.2 Unable to use out-of-band server authenticator

If a user is unable to use their out-of-band server authenticator due to loss or damage of the authenticator, the user may not be able to access online service since they may forget the current user password or may not be able to use another authentication method.

### 9.1.3 Unauthorized use of out-of-band server authenticator

An attacker may use a user's out-of-band server authenticator, such as by stealing it.

### 9.1.4 Remote attacks on out-of-band server authenticator

An attacker can remotely perform authentication by installing malicious software on the smartphone on which the user's out-of-band server authenticator is installed.

### 9.1.5 False server authentication request

When a user uses an online service that provides out-of-band server authentication, at the time when the user tries server authentication by comparing and verifying the server authentication information, an attacker sends a false server authentication request to the user's out-of-band authenticator by entering the user ID in a different terminal to induce the user to perform wrong authentication.

## 9.2 Security requirements

In this clause, the security requirements are described in response to potential security threats that may arise from the out-of-band server authentication model. The relationship between each security threat and security requirement is described in Appendix I.

### 9.2.1 User password authentication restriction

In order to prevent users who registered an out-of-band server authenticator from a stolen or leaked user password, the user password authentication method may be restricted, and only user authentication through the out-of-band server authenticator may be allowed.

### 9.2.2 Extra methods to release out-of-band server authenticator and reset user password

Extra methods should be provided for releasing the registered out-of-band server authenticator and resetting the user password through separate user authentication, such as identity verification, e-mail verification, and security questions.

### 9.2.3 Additional authentication methods within the out-of-band server authenticator

When authenticating the server through the authenticator, an additional authentication method may be provided to verify that the user is legitimate, such as PIN or biometric authentication by the smartphone on which the out-of-band server authenticator is installed.

### 9.2.4 Simultaneous server authentication request control

After the server authentication information is displayed by the out-of-band server authenticator, new server authentication requests should be blocked or queued until the user completes server authentication.

# Annex A

## Extra procedure for out-of-band server authentication

(This annex forms an integral part of this Recommendation.)

### A.1 User password automatic renewal

In the user password automatic renewal step, after the relying party provides a service to the user through out-of-band server authentication, the online service provider automatically renews the password of the user account. Online service providers can maintain the concept of user passwords to minimize changes to existing data structures and functions, while also strengthening the security of user passwords.

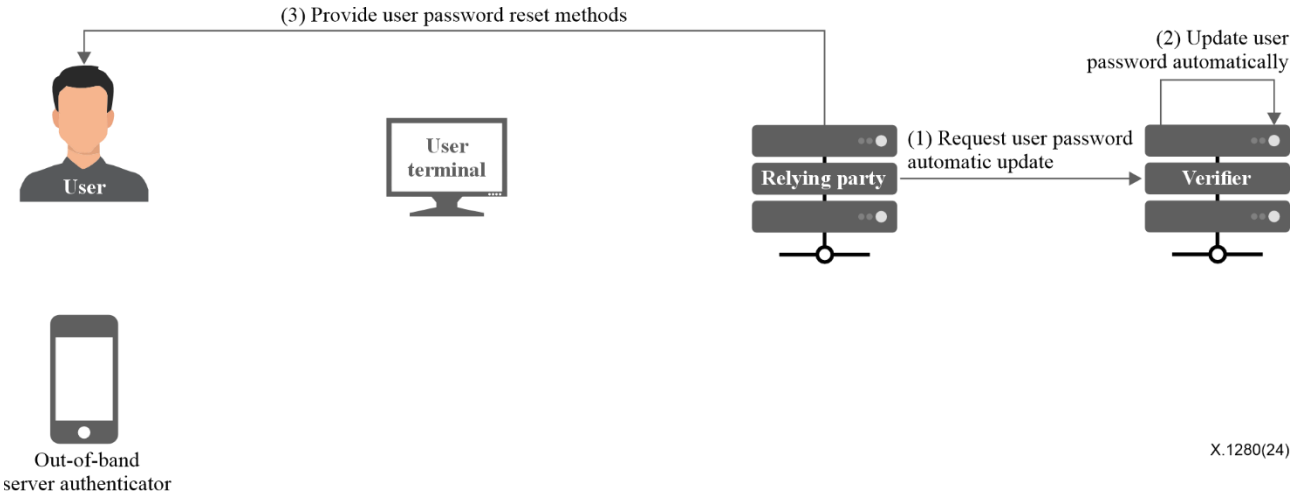


**Figure A.1 – Flow of user password automatic renewal**

Figure A.1 identifies the data required in the user password automatic renewal step and shows the flow. This flow assumes that the verifier performs user password automatic renewal, and it can be performed either by the relying party or the verifier. The explanation of the flow is as follows:

(1) After the relying party provides service to the user after out-of-band server authentication, a user password renewal request for the user is sent to the verifier.

(2) The verifier changes the user password to a randomly generated value with a complex rule.

(3) In case it is impossible to use the out-of-band server authenticator registered by the user due to loss, etc., the relying party provides a method to release the authenticator and reset the user password through separate user authentication so that the user can use the service with the reset user password.

The user can manage their user password without regularly changing it by themselves and remain secure from password leaks.

# Appendix I

## Relationship between security requirements and threats

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

In this appendix, the relationship between potential security threats that may arise from the out-of-band server authentication model and the security requirements are defined in Table I.1.

**Table I.1 – Relationship between security requirements and threats**

| **Security requirements** | **Security threats** | | | | |
|---|---|---|---|---|---|
| | Fraudulent online service | Unable to use out-of-band server authenticator | Unauthorized use of out-of-band server authenticator | Remote attacks on out-of-band server authenticator | False server authentication request |
| User password authentication restriction | o | - | - | - | - |
| Extra authentication methods | - | o | - | - | - |
| Additional user authentication methods | - | - | o | o | - |
| Simultaneous server authentication request control | - | - | - | - | o |

# Appendix II

## Use cases of out-of-band server authentication model

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

### II.1 Websites and applications

Websites, web applications, and various applications that do not use a web browser can solve the limitations of PKI-based server authentication by applying the out-of-band server authentication model.

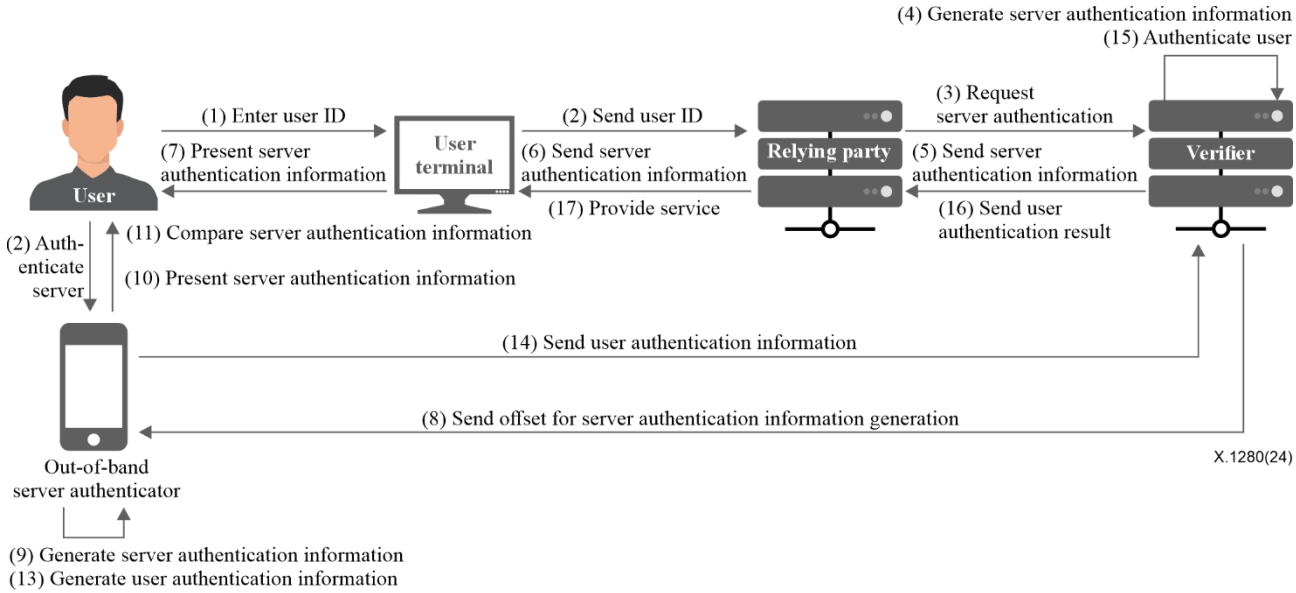


**Figure II.1 – Flow of out-of-band server authentication for websites and applications**

Figure II.1 shows the out-of-band server authentication flow for websites and applications.

Even in the case of corporate websites and web applications using a private domain name system (DNS) that cannot obtain an PKI certificate through a certification authority, and IP address-based applications, and applications that do not use a web browser, the user can perform authentication safely after clearly verifying the online service providers first.

### II.2 IdPs

Identity providers (IdPs) that provide OAuth 2.0 and security assertion markup language (SAML) services can apply the out-of-band server authentication model to secure user account security for all online services connected to them.

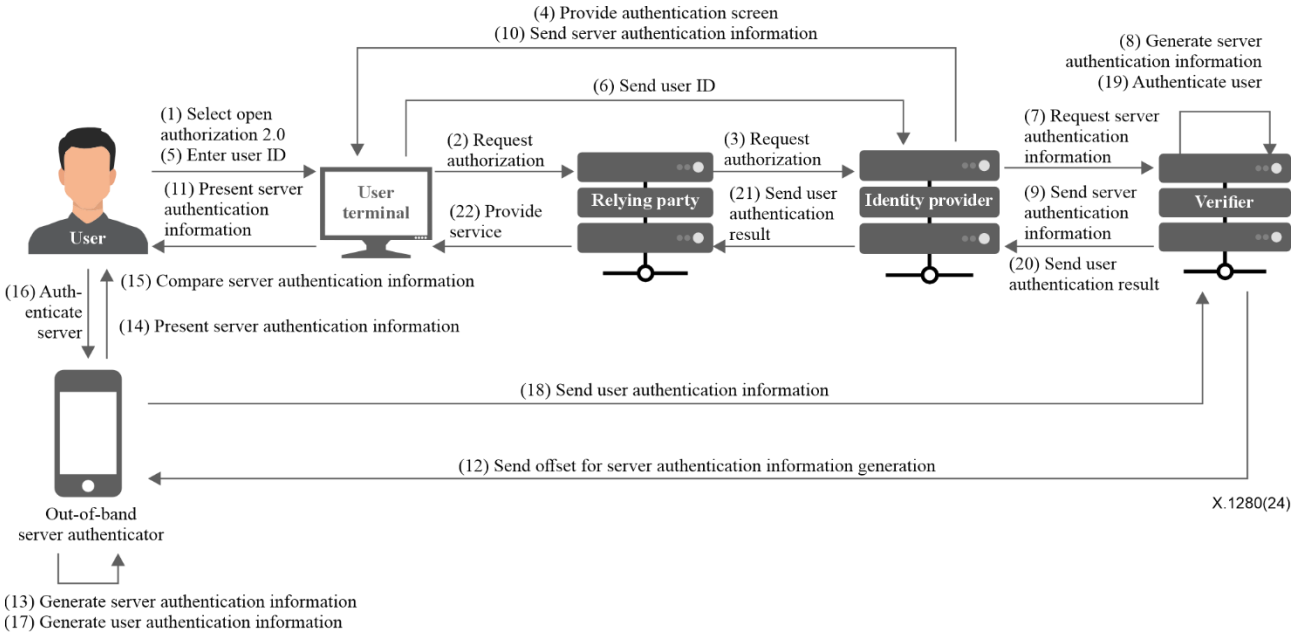


**Figure II.2 – Flow of out-of-band server authentication for IdPs**

Figure II.2 shows the out-of-band server authentication flow for IdPs.

If user authentication information of the ID provider is leaked due to a cyber-attack that impersonated the authentication screen of the IdP, the user accounts of all service providers registered by the user may be at risk. IdPs can be free from phishing and pharming by adding out-of-band server authentication.

## II.3 Operating systems

Windows and Linux-based operating systems can apply the out-of-band server authentication model to strengthen the operating system local account security.

In order to apply the authentication model to the Windows-based operating system, it is necessary to install and configure a third-party credential provider client that can control the operating system's credentials.

In order to apply the authentication model for Linux-based operating systems, it is necessary to install and configure pluggable authentication modules (PAM).

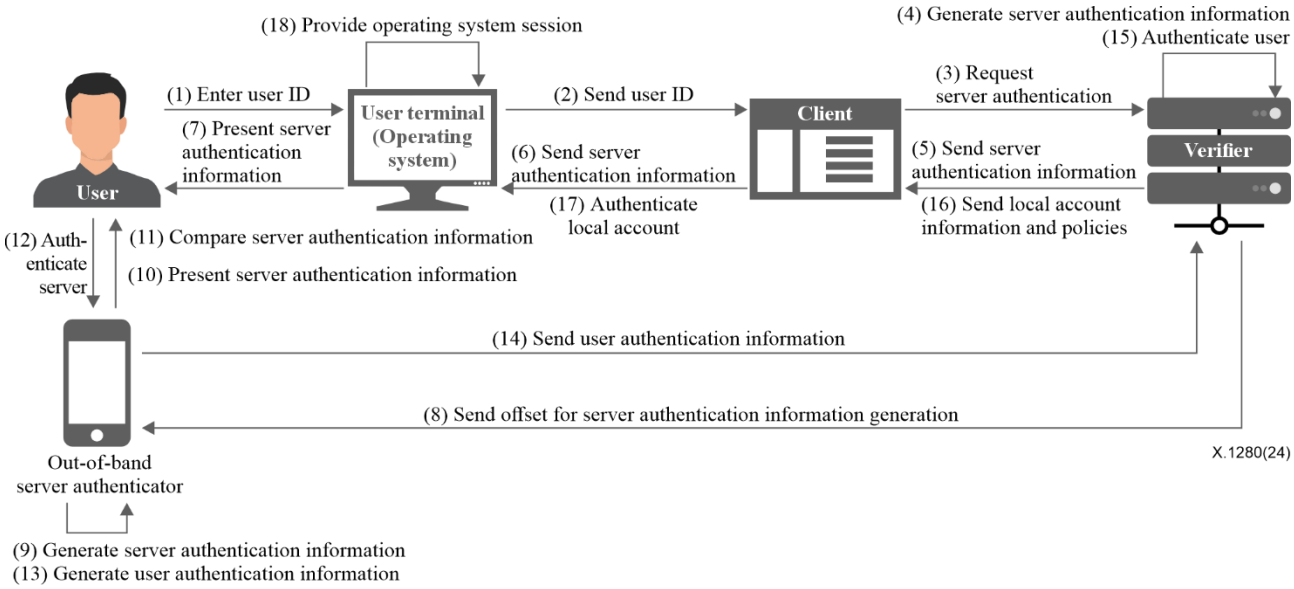


**Figure II.3 – Flow of out-of-band server authentication for operating systems**

Figure II.3 shows the out-of-band server authentication flow for operating systems.

Users can clearly verify that the operating system they are trying to access is correct, and it is possible to prevent incidents caused by writing down access information on a paper or sharing it with other users even though the operating system is running on the cloud.

In addition, if the user password automatic renewal, an additional step in the out-of-band server authentication procedure, is applied, password change policies for the local accounts can be managed more easily and safely.

After entering the user ID, the user can use the operating system after verifying the server authentication information displayed on the operating system login screen and the out-of-band server authenticator. The user does not need to type a user password or use a key file to access operating systems.

In addition, if the user password automatic renewal, an additional step in the out-of-band server authentication procedure, is applied to the client, the operating system account can be managed more easily and safely by automatically changing the password of the operating system local account.

# Appendix III

## Relationship to other authentication technologies

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

Authentication technologies are a fundamental technology that maintain trust between users and online service providers in the digital era. Diverse authentication technologies such as OTP, FIDO, and mobile push authentication have been developed and used widely, considering secure, cost-effective, and convenient authentication. Accordingly, different authentication assurance levels have been classified for new authentication technologies in [b-ITU-T X.1254], [b-ISO/IEC 29115], and [b-NIST SP 800-63-3].

As authentication technologies have been enhanced and standardized, providing verifier impersonation resistance is highly demanded as well as user authenticity. Authentication technologies that comply with the requirement are classified as the highest level.

However, since existing authentication technologies authenticate users only, there are limitations in providing only the user authentication information to the service providers without users verifying them explicitly for verifier impersonation resistance.

Existing user authentication technologies can be mainly divided into in-band authentication that provides authentication information through the primary communication channel between service provider servers and users, and out-of-band authentication that provides authentication information through a separate communication channel.

In-band authentication technologies are verifier impersonation resistant but are not convenient and are not cost-effective. Out-of-band authentication technologies are convenient and cost-effective but are vulnerable to verifier impersonation.

Figure III.1 illustrates authentication information flow for in-band and out-of-band authentication.

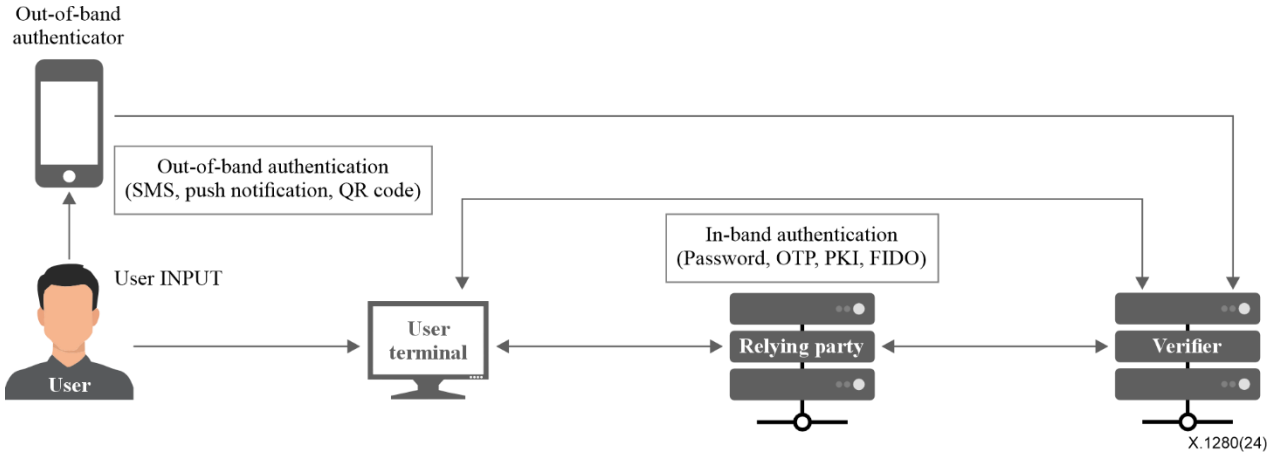


**Figure III.1 – Authentication information flow for in-band and out-of-band authentication**

In-band authentication such as PKI technologies only implicitly provides verifier impersonation resistance since it does not explicitly provide the user with a method to verify the service provider. If a server or an application is changed, it needs to reidentify the user and reissue the certificate on the user terminal. In particular, FIDO is a typical in-band authentication technology because the authenticator communicates with the authentication server via the terminal currently connected to the relying party, even though universal two factor (U2F) and client to authenticator protocol (CTAP) seem like an external authenticator independent of the terminal. Because of that, if two or more terminals are being used at home or at work, the user has to re-register the service in each terminal's

FIDO authenticator. Also, even if using a CTAP authenticator, an external authenticator of FIDO2, it has to be registered or reconnected to each terminal. Therefore, PKI-based in-band authentication technologies have a terminal dependency without verifying a service provider explicitly.

Out-of-band authentication, such as mobile push notification, is an authentication technology that verifies the user's possession of an authenticator, which does not need to reidentify the user and reissue the certificate even though a server or an application is changed. However, if the user is already connected to a fraudulent server without knowing where they connected to, the user cannot resist the verifier impersonation, as illustrated in Figure III.2.

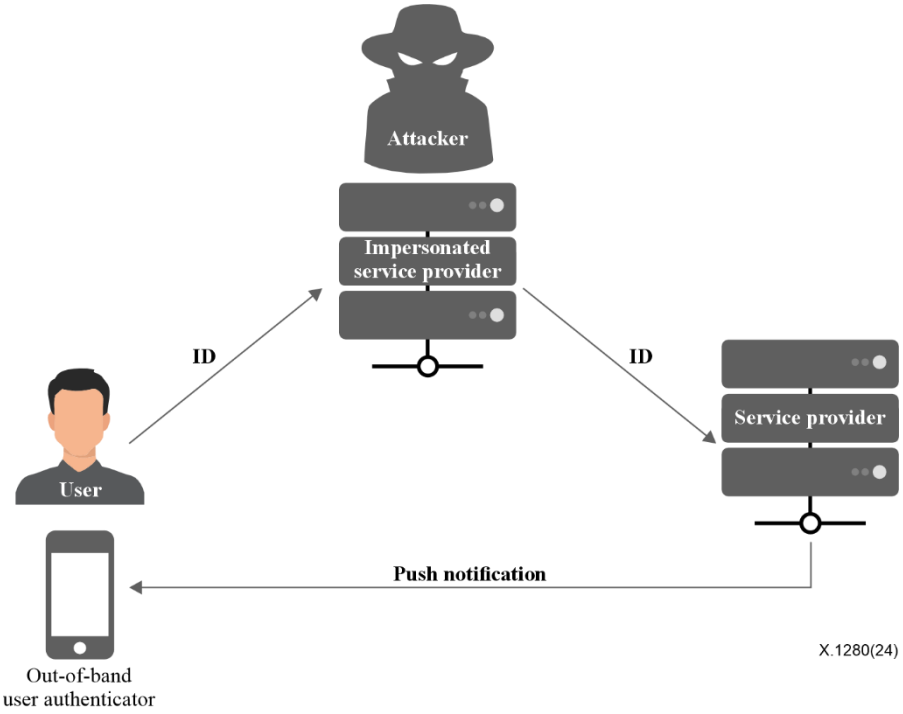


**Figure III.2 – Vulnerability of out-of-band user authentication to impersonated service provider**

Independently with the user authentication technologies, there is a web server authentication technology that the user can use to verify the service provider by checking the ITU-T X.509 certificate known as a padlock symbol on browser, but this is not aligned with the user authentication process so users may find it hard to check the certificate every time, and users who are not familiar with technologies may not even check the certificate. In addition, this is vulnerable to social engineering attacks using similar domain names and is unable to verify online services using a private DNS server, IP address-based online services, and non-browser-based online services.

Therefore, a framework for out-of-band server authentication may be needed that overcomes the vulnerability of verifier impersonation that may happen when using out-of-band user authentication technologies and the limitation of terminal dependency of the authenticator inherited in using PKI-based in-band user authentication technologies.

# Bibliography


[b-ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2020), *Entity authentication assurance framework*.

[b-ITU-T X.1277] Recommendation ITU-T X.1277 (2018), *Universal authentication framework*.

[b-ITU-T X.1278] Recommendation ITU-T X.1278 (2018), *Client to authenticator protocol/Universal 2-factor framework.*

[b-ISO/IEC 29115] ISO/IEC 29115:2013, *Information technology – Security techniques – Entity authentication assurance framework*.

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2021, *Information security – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[b-NIST SP 800-63-3] NIST SP 800-63-3:2017, *Digital Identity Guidelines*.

# 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 |

Published in Switzerland
Geneva, 2024