International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1153

(02/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services – Security protocols

Management framework of a one time password-based authentication service

Recommendation ITU-T X.1153

ITU-T

ITU International Telecommunication Union

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	
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	**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	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
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

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

Recommendation ITU-T X.1153

Management framework of a one time password-based authentication service

Summary

Recommendation ITU-T X.1153 provides a management framework of a one time password (OTP)-based authentication service to support multi-factor authentication. Specifically, this Recommendation includes the general management framework, the centralized management framework, the enhanced centralized framework, and the cross-domain management framework. These frameworks consist of the OTP management models, OTP management operations, and security considerations for providing the OTP authentication service in a secure telecommunication network.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1153	2011-02-13	17

Keywords

Management framework, multi-factor authentication, one time password.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T X.1153

Management framework of a one time password-based authentication service

1 Scope

The one time password (OTP) authentication service supports multi-factor authentication through an OTP token that creates a password for one-time use only. OTP has been developed to cope with fundamental security threats inherent in the traditional static password while requiring each OTP user to have several OTP tokens for the authentication service unless a management framework is provided. This framework enables using the service with only one token.

This Recommendation provides the management framework of a one time password (OTP)-based authentication service to support multi-factor authentication. In addition, it offers an interoperable management framework that allows sharing of a single OTP token among different service providers.

Specifically, this Recommendation provides the following:

– overview of an OTP-based authentication service;

– a general management framework including an OTP management model, OTP management operations, and security considerations in providing the OTP-based authentication service;

– additional features for the interoperable management framework for sharing the OTP token.

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.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*

[ITU-T X.842] Recommendation ITU-T X.842 (2000) | ISO/IEC TR14516:2002, *Information technology – Security techniques – Guidelines for the use and management of trusted third party services.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 identity provider [b-ITU-T X.1252]: An entity that verifies, maintains and manages, and may create and assign identity information of other entities.

3.1.2 tamper detection [b-FIPS PUB 140-2]: A cryptographic module's automatic determination that an attempt has been made to compromise the physical security of the module.

3.1.3 tamper evidence [b-FIPS PUB 140-2]: The external indication that an attempt has been made to compromise the physical security of a cryptographic module. (The evidence of tamper attempt should be observable by an operator subsequent to the attempt.)

3.1.4 tamper response [b-FIPS PUB 140-2]: The automatic action taken by a cryptographic module when tamper detection has occurred (the minimum response action is the zeroization of plaintext keys and CSPs).

3.1.5 trusted third party (TTP) [ITU-T X.842]: An organisation or its agent that provides one or more security services, and is trusted by other entities with respect to activities related to these security services. A TTP is used to offer value-added services to entities wishing to enhance the trust and business confidence in the services that they receive and to facilitate secure communications between business trading partners. TTPs need to offer value with regard to confidentiality, integrity and availability of the services and information involved in the communications between business applications. TTPs should be able to choose the entities to which they will provide services.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 authentication factor: A piece of information used to authenticate or verify a person's identity with regard to appearance or in a procedure for security purposes and with respect to individually granted access rights. Authentication factors consist of ownership factor, knowledge factor, and inherent factor.

3.2.2 authentication framework [based on ITU-T X.811]: A general framework for the provision of authentication service; two-party and (trusted) third-party authentication frameworks.

3.2.3 authorization framework [based on b-IETF RFC 2904]: An architectural framework for understanding the authorization of Internet resources and services; single domain and roaming sequence models.

3.2.4 multi-factor authentication: The combined use of more than one authentication factor. Multi-factor authentication is either two-factor or three-factor. Note, however, that using two types of the same factor is not multi-factor authentication.

3.2.5 one time password [based on b-IETF RFC 2289]: A password that can be used only once as it is changed every time an OTP user logs into the computer system and network. It is secure against the passive attacks allowed by the replaying of captured reusable passwords such as traditional fixed passwords.

3.2.6 OTP authentication system: A system that supports OTP validation for Internet resource access (e.g., login) and other application services requiring authentication. It consists of OTP validation server(s), protocols, facilities, and related-operational system.

3.2.7 OTP service provider: The provider(s) of the OTP validation service offering multi-factor authentication service to other service providers, e.g., Internet service provider or application/contents service provider. A trusted third party would be a good example for OTP service provider to perform OTP validation more efficiently. The OTP service provider does not necessarily have the role of identity provider as defined in [b-ITU-T X.1141].

3.2.8 OTP token: A physical device that generates OTP, wherein a token means that the OTP user possesses and controls a key or password used to authenticate the OTP user's identity. Such physical device embeds the display showing OTP and the numeric keypad optionally.

3.2.9 OTP token identifier: A unique identifier assigned to each OTP token for distinguishing it from other OTP tokens. It may consist of alphanumeric characters.

3.2.10 OTP token vendor: An OTP device manufacturer or vendor dispensing the OTP token to the service provider.

3.2.11 OTP user: A user who carries the OTP token and tries to log into a particular system or use other application services through multi-factor authentication.

3.2.12 OTP validation server: A dedicated server managed by OTP service providers or service providers to validate the OTPs generated by OTP users using their OTP tokens.

3.2.13 service agreement: A mutual agreement regarding the service level among service providers. This agreement includes contracts such as security level, performance level, and billing policy for the provision of the OTP authentication service.

3.2.14 service provider: An Internet service provider and/or an application/contents service provider possessing a dedicated authentication system for verifying subscribers/users. The service provider can be provided with the OTP authentication service directly or through either the identity provider or the OSP.

3.2.15 side-channel attack: Any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms. For example, timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system. Many side-channel attacks require considerable technical knowledge of the internal operation of the system on which the cryptography is implemented.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACSP Application and Contents Service Provider

IdP Identity Provider

ISP Internet Service Provider

OSP OTP Service Provider

OTP One Time Password

PIN Personal Identification Number

PKI Public Key Infrastructure

SA Service Agreement

TTP Trusted Third Party

5 Conventions

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network

operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 OTP-based authentication service

6.1 Introduction

The OTP-based authentication service supports multi-factor authentication through an OTP token that creates the password for one-time use only. OTP-based authentication usually consists of two basic units: an OTP token and a relevant OTP validation server using an identical OTP generation algorithm.

OTP has the following major points:

– Applicability: It can be used to replace the existing password authentication methods that have been most widely used. In other words, it can be used along with various authentication support protocols such as EAP [b-IETF RFC 4793], SAML [b-ITU-T X.1141] and RADIUS [b-IETF RFC 2869] in wired and wireless access networks and with diverse applications.

– Security: OTP improves the security of existing passwords by fundamentally preventing the risk of guessing and reusing a password. OTP-based authentication can be used together with other authentication mechanisms (e.g., PKI, static password) to support multi-factor authentication.

OTP is required to consider the following issues:

– Carrying the OTP token: It is inconvenient for users to carry the OTP token with them at all times. Moreover, the problem of carrying multiple OTP tokens is required to be solved when users use multiple services from various service providers.

– OTP token management: Maintenance is required to be performed to prevent loss and damage of the OTP token. OTP users are required to also be careful to ensure that the OTP token is not used or abused by other persons.

6.2 General features

6.2.1 OTP generation process

In general, the OTP token generates a password through the OTP generation function based on a unique OTP generation key as well as synchronization data.

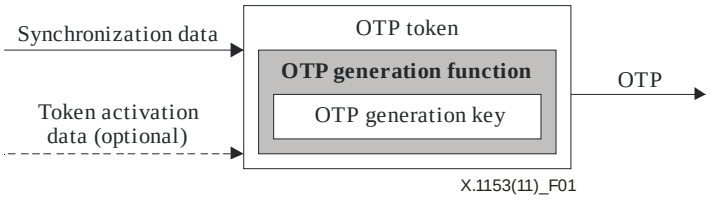


Figure 1 – OTP generation function

In Figure 1, the output of the OTP generation function is an OTP which is the value generated by the OTP generation function and provided to the OTP validation server to verify that the OTP user possesses and controls the OTP token. The OTP token requires the OTP generation key and input data such as synchronization data. In addition, certain tokens may require activation data (e.g., through the input of PIN or biometric) to generate the OTP.

The outer box is the OTP token itself.

The middle-level inner box represents an OTP generation function containing an OTP generation key. The OTP is generated by executing the cryptographic function using the OTP generation key and synchronization data as well as one or more optional token input values (e.g., PIN value):

OTP = OTP Generation Function (OTP generation key, Synchronization data, [Token activation data])

; Synchronization data = {time and/or event counter and/or challenge}, [] optional input

The lower-inner box represents the actual OTP generation key inherent within the OTP token: the OTP generation key is embedded within the token.

The synchronization data includes time, event [b-IETF RFC 4226] counter and/or challenge value. The combination of these inputs may produce OTP types having different attributes as the output of the OTP generation function. The OTP can be divided into four types according to the features of the input synchronization data: challenge-response method wherein the password changes according to a challenge code; time-synchronous method that uses the current time; event-synchronous method wherein the password changes according to the number of OTP generations, and event-time sync method that combines these two methods. The password generated as described above has the feature of being unique to each OTP user and usable only once. With these features of OTP, various considerations are required to be given to the management framework.

The token activation data serves as gating mechanism of the OTP token. In some cases, the function cannot be computed unless token activation data is supplied to activate the OTP token. The activation button and user PIN are good examples of the token activation data that are to access the OTP generation function. Note, however, that user PIN can also be used as synchronization data for adding the security factor to the OTP generation function.

6.2.2 OTP validation process

Figure 2 shows the OTP validation process. First, an OTP user has his/her OTP token registered in the OTP validation server.

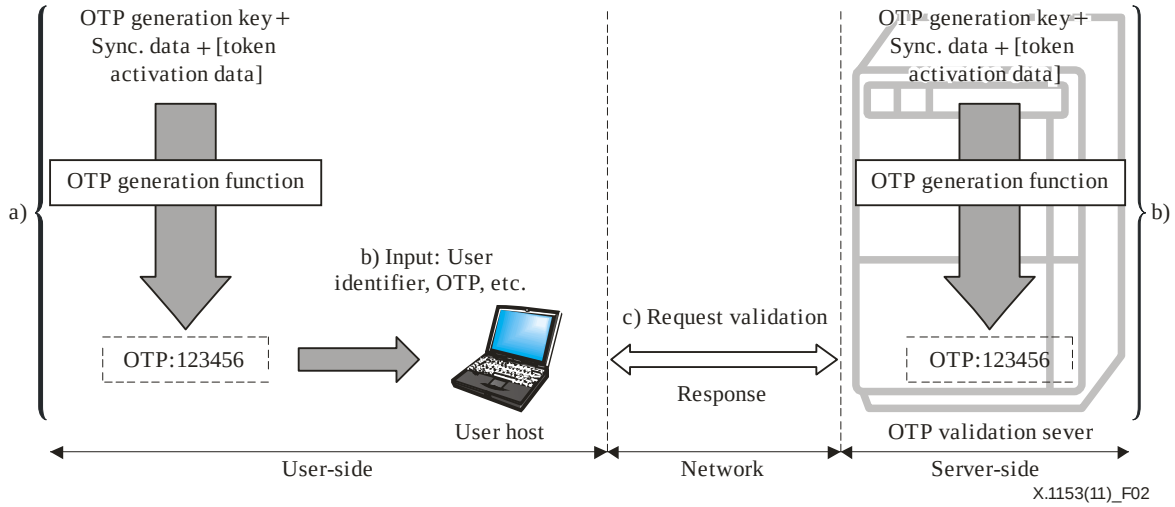


Figure 2 – OTP validation process

a) The OTP user generates an OTP through the OTP generation function (i.e., OTP token) using synchronization data as well as the OTP generation key possessed by the OTP token and OTP validation server in common.

b) It inputs the OTP to the OTP user host for validation. Afterward, the OTP user inputs his/her registered identifier (i.e., ID) with other additional user authenticators (e.g., social security number) requested by the OTP validation server.

c) The OTP user host sends the received OTP to the OTP validation server.

d) The OTP validation server confirms the received user identifier and generates an OTP using the same OTP generation function as the one used in the OTP token, and then confirms the received OTP and passes the result to the user host.

After completing the OTP validation process, the OTP user can get access authorization to the application.

6.2.3 OTP token life cycle

Figure 3 presents the OTP token life cycle organized into six stages: initial, ready, issued, active, suspended, and revoked. If a service provider does not want to interoperate with other service providers, the issued stage and active stage can be merged into one stage block, i.e., the active stage block. The active OTP token is defined as an OTP token in the active stage block; it is supposed to be managed securely by the authenticated OTP user. Operations that transfer to the active OTP token is required to be performed by carefully considering the OTP user's identification.

There are several operations that may affect stage transition. There are also some operations that may not influence stage transition, such as validation (only in case of success), modification, synchronization, and PIN-unlock; hence the "status inquiry" operation, which does not affect stage transition but can be performed in any stage.

These operations are described in clauses 8.2, 9.1.2 and 9.2.2. The following is a description of the stages of the OTP token life cycle:

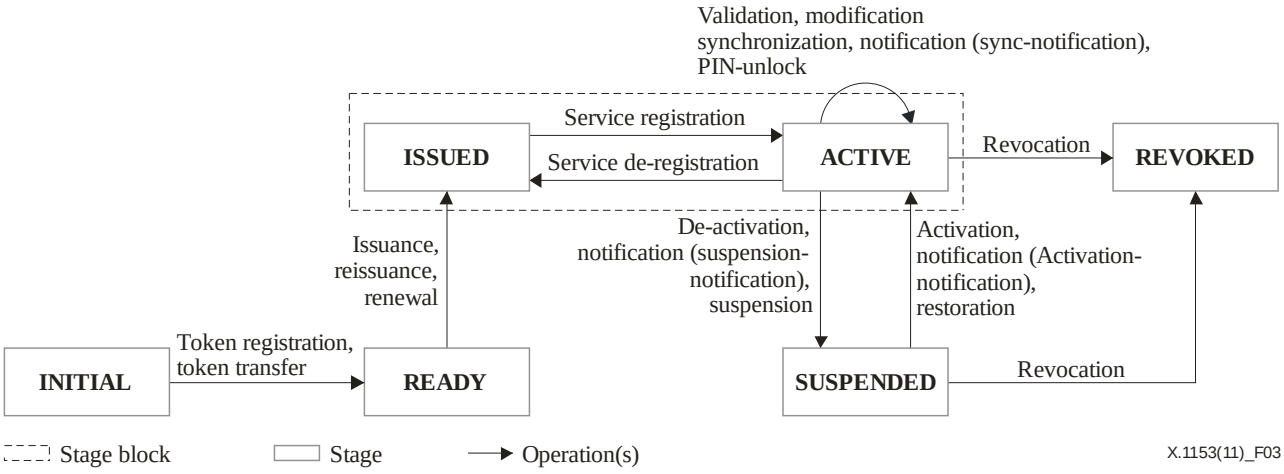


Figure 3 – OTP token life cycle

– **Initial stage**: This stage is the first stage of the OTP token life cycle. Service providers import OTP tokens for distribution to their branch offices in this stage. The initial stage is required to be transited to ready stage when the service provider or OTP token vendor registers token information in the OTP validation server, and the OTP token is ready to be issued and distributed. In particular, the initial stage can be transited to ready stage by the token registration and token transfer operations.

– **Ready stage**: This stage implies that the OTP servers already import the OTP generation keys of each OTP token. Therefore, the OTP token is ready to be validated by OTP servers in this stage. The ready stage is required to be transited to the issued stage when the service provider issues and distributes the OTP token to the OTP user. In particular, the ready stage can be transited to the issued stage through the issuance, reissuance, and renewal operations.

– **Issued stage**: This stage is similar to the active stage, but the validation of an OTP token could be rejected by other service providers that did not issue the OTP token. Therefore, the OTP user who wants to use the OTP issued by another service provider is required to register his/her OTP token to the service provider for further use. The issued stage is required to be transited to active stage to validate and authenticate the OTP user. In particular, the issued stage can be transited to the active stage through the service registration operation.

– **Active stage**: This stage is the only stage wherein the OTP can be validated. Whenever the OTP user transmits an OTP via the Internet to the service provider, the OTP validation server validates such OTP. The active stage can be transited to several stages; it is required to be transited back to the issued stage when the OTP user does not want to use the OTP from the indicated service provider further, but the OTP user is still able to use the OTP from other service providers. The active stage is required to be transited to the suspended stage when the OTP user wants to disable the OTP token because of suspected loss, or the service provider also disables the OTP token when it is suspected to have been subject to misuse by a malicious OTP user. The active stage is required to be transited to the revoked stage when the OTP user wants to revoke the OTP token; the revoked OTP token cannot be used further. When the OTP is validated as correct, this stage will be unchanged. If this OTP is not correct, however, the OTP validation server can count the errors. When the count of the validation failure exceeds the predefined policy, this stage will be transited to the suspended stage. Operations such as modification, synchronization, notification, and suspension also affect the stage transition to the suspended stage. The active stage can be transited back to the issued stage through the service de-registration operation; it can also be transited to the revoked stage through the revocation operation. The PIN-unlock operation can be performed only in this stage, but it does not affect the status transition.

– **Suspended stage**: This stage involves disabling the validation operation. In this stage, service providers are required to always reject the validation request from the OTP user. The suspended stage is required to be transited back to the active stage when the OTP user wants to enable the OTP token following recovery from loss, or the service provider also enables the OTP token when it is believed to be used properly by the OTP user. An OTP token in the suspended stage cannot be transited to the issued stage directly because it is likely to cause a security breach when someone who steals the OTP token can activate the OTP token via service registration without a valid restoration operation. Therefore, an OTP user who requires service de-registration in the suspended stage is required to activate the OTP token first. The suspended stage is required to be transited to the revoked stage when the OTP user wants to revoke the OTP token; the revoked OTP token cannot be used further. The suspended stage can be transited back to the active stage through the notification, activation, and restoration operations and can also be transited to the revoked stage through the revocation operation.

– **Revoked stage**: This stage is irreversible and is the final stage of the OTP token life cycle. None of the operations can change this stage. A revoked OTP token is required to not be reused.

6.3 OTP-based authentication service

6.3.1 Overview of the OTP-based authentication service

The OTP-based authentication service is used for countering the passive attacks which are subject reusable passwords in the existing password authentication methods in telecommunication networks.

Password authentication methods are vulnerable to attacks through password guessing because it consists of a few meaningful characters. Moreover, there is a risk of password replay due to the use of fixed patterns. OTP is secure since it has eliminated such vulnerability by using a password that is changed every time. Furthermore, OTP is more effective because it replaces the password without making major changes to the existing authentication system.

User authentication methods commonly consist of three categories: 1) what you know; knowledge-based authentication methods such as static passwords or personal identification numbers (PIN)s known to users; 2) what you are; biometrics are good examples, and 3) what you have; possession-based authentication methods such as smart cards, cryptographic tokens, or OTP tokens carried by the user.

The OTP-based authentication service is used to support multi-factor authentication for improved security, in conjunction with another authentication method, or even the static password that has traditionally been used in telecommunication networks.

The OTP-based authentication service can be used in a telecommunication network as follows:

– Entity (or user) authentication: as a means of authenticating users or entities that are to receive the agreed upon service by gaining access to Internet resources and services.

– Transaction authentication: as a means of confirming whether the data transmitted via the telecommunication network is true and correct.

The purpose of the OTP-based authentication service is to provide a stricter access control and authentication mechanism for secure communications.

Figure 4 illustrates the probable service flows and relationships of OTP-based authentication from the viewpoint of service providers and enterprise networks, and represents an abstract service view.

A service view is provided according to the management framework and service agreement between the service providers involved. The role of each service provider/network does not necessarily exist separately; a service provider may perform multiple roles independently.

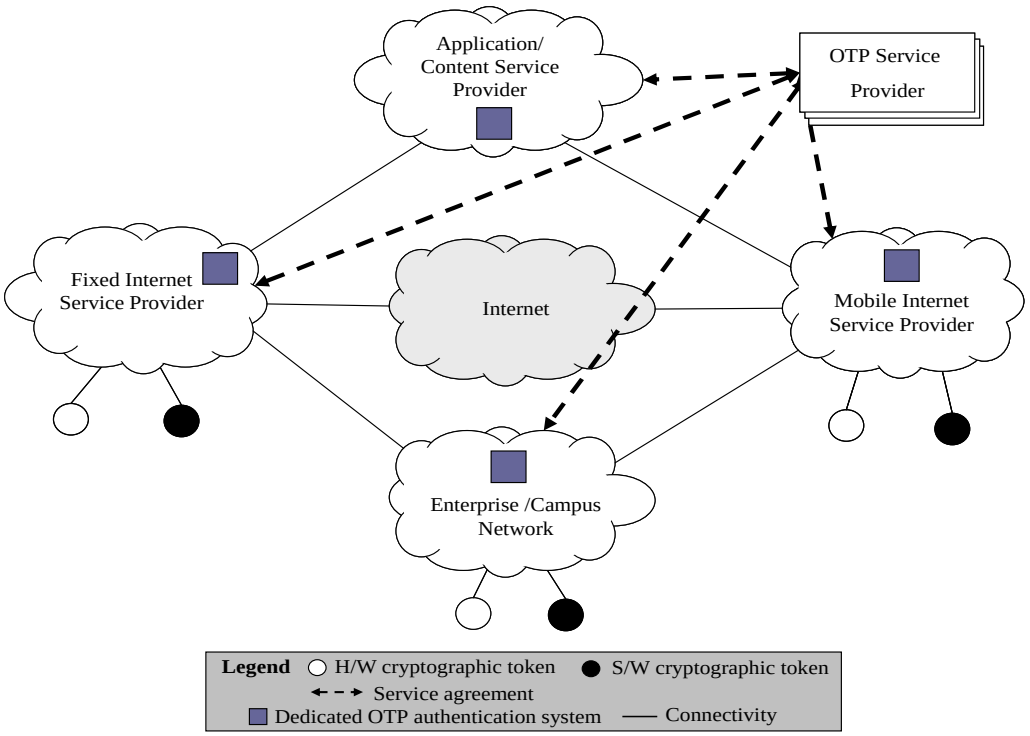


Figure 4 – Overview of the OTP-based authentication service in multiple service domains

6.3.2 Service scenarios of the OTP-based authentication service

The OTP-based authentication service offers various scenarios for service provision. The scenarios vary according to the service agreement between service providers. The deployment model of the service is described in Appendix I. Each scenario refers to the general and common forms of service scenarios that can actually be implemented; it does not list all OTP-based authentication services. For example, a service provider can provide service by using one of the scenarios separately or by creating other service forms according to technical restrictions, security policy or user requirements.

7 OTP management architecture

This clause describes the OTP management architecture that is commonly needed for planning, designing, and constructing the OTP-based authentication service. The OTP management architecture consists of OTP entities, OTP management blocks, OTP management framework, OTP management procedures, and OTP management requirements.

7.1 OTP entities

The entities involved in the OTP management architecture include the OTP user, service provider, OTP token vendor, and OSP (i.e., entity for the dedicated authentication service operating with validation servers).

7.2 OTP management blocks

The OTP-based authentication service is mostly blocked as follows:

– **OTP user token block**: This block is where OTP is transmitted for the purpose of login or service use. The OTP user token block enables a range of authentication token types, authentication methods, operational protocols, and security policy for multi-factor authentication in the enterprise or service provider infrastructure. The OTP authentication token includes hardware or software implementation that combines one or more authentication methods and executes security-critical, client-side authentication operations and secure storage of important data such as the OTP generation key. This block includes

various OTP generation functions such as HOTP [b-IETF RFC 4226]. OTP authentication methods include a mechanism for validating OTP user or authentication support protocols such as SSL, EAP, etc. The operational protocol includes the management described in clauses 8 and 9. Finally, the security policy offers user guidance for multi-factor authentication. This block includes interfaces to interact with protocols in the communication block.

– **OTP validation server block**: This block is where a particular OTP is sent from the OTP user block to be validated. The OTP validation server block consists of the service provider block and OTP authentication block. This block additionally includes the OTP user's identity verification from the service provider. The OTP validation server supports OTP verification and returns the result of verification to the OTP user token block. The operational protocol provides ongoing life cycle management such as validation, issuance, and other operations described in clause 8. OTP validation servers can load validation software from several OTP token vendors, i.e., Domain A and Domain B. For example, Figure 5 shows that both domains are using each other's OTP token vender software and tokens. Policy management is responsible for maintaining reliable operation, which includes operation, business, and security policy. The OTP validation server block is divided into in-house and outsourced architecture.

  • In-house architecture: A service provider implements its own dedicated OTP validation server and has the role of issuer of the OTP token. User identity and OTP-related information (e.g., OTP generation key and serial number) are managed by the service provider.
  • Outsourced architecture: A service provider uses the OTP authentication service from the separated OSP as TTP service provider instead of implementing its own dedicated OTP validation server. In this case, the service provider has the role of issuer, mapping the OTP user's identity and OTP token information. OSP then verifies the OTP validation request including the OTP serial number and OTP transmitted from the service provider.

OTP management blocks are linked through reliable, secure transmission protocols responsible for exchanging OTP authentication data between the OTP user application and the OTP validation server application or another-type OTP validation servers. Authentication protocols support one or more authentication methods, and there are many existing industry standard protocols. The OTP operational protocol exchanges messages regarding the management operations described in clause 8. These protocols are implemented using either existing or new authentication technologies or standard communication protocols.

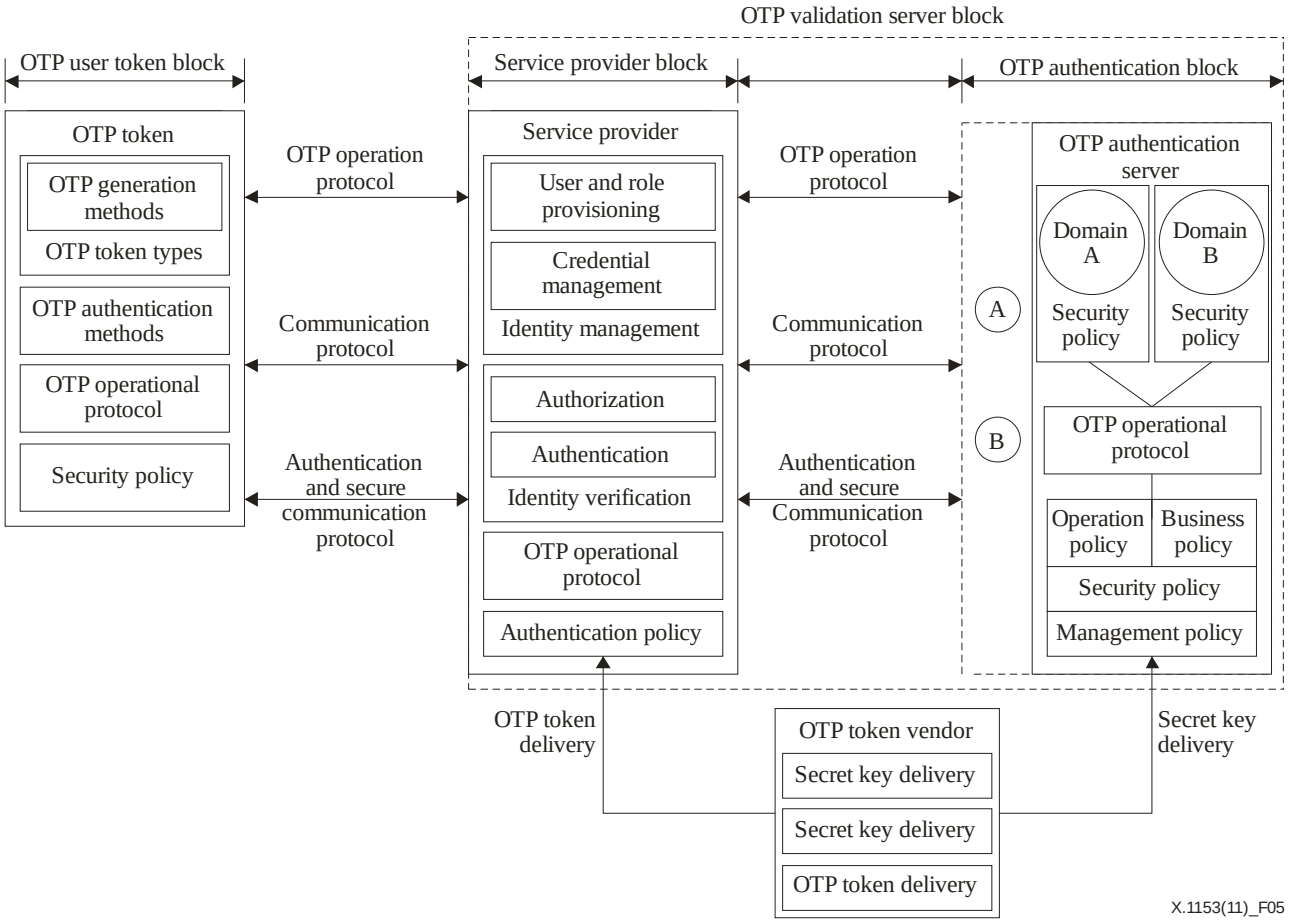


Figure 5 – OTP management architecture

7.3 OTP management framework

The OTP management framework consists of the OTP management models, OTP management operations, and security considerations. OTP management models represent the relationships among the OTP entities. Service providers can selectively choose one of the following four models according to their business model and the service environments:

– **OTP management model for the general management framework**: This model consists of a single OTP service provider (i.e., enterprise) that can offer the OTP authentication service. The service provider is required to manage the OTP validation server(s) internally. Likewise, the OTP user is required to manage multiple OTP tokens to access multiple service providers.

– **OTP management model for the centralized framework**: This model is mainly designed to interoperate with other service providers. OSP manages the centralized OTP validation server(s) to validate the OTPs transmitted from the service providers. In this model, service providers are not required to manage the OTP validation server(s) internally, and cost-effectiveness is relatively high compared to other models. The OTP user is able to access multiple service providers with a single OTP token.

– **OTP management model for the enhanced centralized framework**: This model is designed not only to interoperate with other service providers, but also to enhance the availability of OSP. Nonetheless, the OTP management model for the centralized management framework has the problem of single failure since all validation requests from various service providers are relayed to the single OSP. To address this problem, service providers can selectively manage the duplicated OTP validation server(s) internally. The OTP user is able to access multiple service providers with a single OTP token.

– **OTP management model for the cross-domain framework**: This model is designed to interoperate with other OSPs in other countries or other service domains. The OTP user is able to access multiple OTP services in multiple domains with a single OTP token provided there are service agreements between domains.

Since the OTP management framework is closely related to the security service, several security considerations are required to be inspected before adopting the OTP management model. In Table 1, brief comparisons between the four models are presented.

Table 1 – Comparison of OTP management models

Model	Features	User convenience
For the general management framework	Consists of a single service provider managing the OTP validation server(s) internally.	Multiple OTP tokens for multiple service providers.
For the centralized management framework	Consists of multiple service providers and an OSP managing the OTP validation server(s) centrally.	Single OTP token for multiple service providers (multiple tokens in multiple domains).
For the enhanced centralized management framework	Consists of multiple service providers and an OSP managing the OTP validation server(s) centrally; the service providers can selectively manage the OTP validation server(s) internally.	Single OTP token for multiple service providers (multiple tokens in multiple domains).
For the cross-domain management framework	Consists of multiple service providers and multiple OSPs.	Single OTP token for multiple service providers in multiple domains.

OTP management operations are functions required to implement the specific OTP management model. A total of 18 operations are defined in clauses 8.2, 9.1.2, 9.2.2, and 9.3.2. Table 2 describes the relationships among the management models, operations, and participating entities.

Table 2 – Relationship among management models and operations

Model			Operations	Participating entities
		For the general management framework	Validation	OTP user, service provider{, OSP}[b]
			Issuance	OTP user[a], service provider{, OSP}[b]
			Reissuance	OTP user[a], service provider{, OSP}[b]
			Renewal	OTP user[a], service provider{, OSP}[b]
			Suspension	OTP user, service provider{, OSP}[b]
			Restoration	OTP user, service provider{, OSP}[b]
			Modification	OTP user, service provider{, OSP}[b]
			PIN-unlock	OTP user[a], service provider{, OSP}[b]
			Activation	OTP user, service provider{, OSP}[b]
			De-activation	OTP user, service provider{, OSP}[b]
			Revocation	OTP user[a], service provider{, OSP}[b]
			Token registration	OTP token vender, service provider {and/or OSP}[b]
			Status inquiry	OTP user[a], service provider{, OSP}[b]
	For the centralized management framework		Service registration	OTP user, service provider, OSP
			Service de-registration	OTP user, service provider, OSP
For the enhanced centralized framework and cross-domain framework			Synchronization	Service provider, OSP
			Notification	Service provider, OSP
			Token transfer	{OTP Token Vendor,}[c] service provider, OSP

[a] Operators may perform the operation on behalf of the OTP user.

[b] The OSP is required to participate in performing the operation when the OTP management model for centralized management framework, enhanced centralized framework, or cross-domain framework is adopted.

[c] The OTP token vendor may participate in performing the operation only when the service provider requests it to provide technical support.

7.4 OTP management procedures

The OTP management procedures consist of two phases: set-up and use.

The set-up phase generally consists of the following:

a) The OTP token vendor generates the OTP generation key and token identifier unique to each OTP token.

b) The OTP token vendor delivers the OTP tokens and OTP information for the service provider.

- The OTP information contains the token identifier and OTP generation key as required for the OTP validation server.
- When the interoperable management framework is applied, the service provider securely forwards the OTP information to OSP.

c) The service provider securely distributes the OTP tokens to the OTP user.

- The service provider or the OSP makes a link between the OTP information of the specific OTP token identifier and the user identifier.

In general, the OTP information for the registered OTP user is managed by the corresponding service provider. If the service provider wants to interoperate with other service providers, however, the OTP information is required to be shared with the OSP. Therefore, the OSP can identify the OTP tokens of the OTP user with its token identifier as transmitted by the service provider.

The use phase consists of the following:

a) The OTP user activates the OTP token to generate an OTP.

b) The OTP user transmits the generated OTP and token identifier to the service provider.

The service provider can obtain the token identifier from the pre-registered user identifier.

- When the OTP management model for the centralized management framework is applied, the service provider securely forwards the OTP and the user identifier to the OSP.
- When the OTP management model for the enhanced centralized management framework is applied, the service provider can choose the OTP validation servers to validate the requested OTP. The OTP validation servers are located both within the service provider and in the OSP.
- In particular, if the service provider adopts the SAML [b-ITU-T X.1141]-based ID management framework, the validation of the OTP is required to take place in IdP, not in the service provider. To validate the OTP, the IdP can operate with the OTP validation server(s) located in the IdP within, or send the validation request to the OSP.

c) The OTP validation server located in the service provider or the OSP checks the transmitted OTP.

- The service provider or the OSP can determine the relevant OTP validation server using the token identifier.
- When the interoperable management framework is applied, the OSP replies to the service provider with the validation result.

d) The service provider decides on access authorization for the service or authentication of the OTP user.

7.5 OTP management requirements

7.5.1 General requirements

- The OTP authentication system is required to be interoperable with the identity management system to support multi-factor authentication.
- The OTP authentication system is required to be able to substitute other existing authentication systems easily such as static password, biometrics, etc.
- The OTP authentication system is required to be flexible in various data transmission standards such as TCP/IP, [b-ITU-T X.25], frame relay, [b-IEEE 802.11], etc.
- The OTP authentication system is required to guarantee integrity and confidentiality for credential data.
- The OTP authentication system is required to provide the control service for the availability of the system.
- The OTP authentication system is required to operate according to the relevant policy with information security management system such as [b-ISO/IEC 27001], [b-ITGI-COBIT], etc.
- The OTP authentication system is required to use a common protocol and message format for compatibility.

– The OTP authentication system is required to protect against passive and active Internet attacks: network sniffing, DoS attack, message forgery attack, session hijacking, man-in-the-middle attack, token hijacking and PIN cracking. Considerations of these vulnerabilities are described in clause 8.3.
– The OTP authentication system is required to develop and operate the system according to the secure policies of configuration management.
– The OTP authentication system is required to be duplicated for stable service.
– The OTP authentication system is required to support the backup and recovery of the system for service availability.
– The OTP authentication system is required to be protected by physical access control.

7.5.2 Implementation system-specific requirements

To implement secure OTP service models, there are requirements for the authentication service and for the composition of OTP authentication systems.

– The OTP generation key is required to be stored and managed securely.
– The OTP token is required to be registered, distributed, and destroyed securely.
– Operations triggered to be transited to the active stage block are required to identify the OTP user.
– The OTP token can optionally support access control mechanisms such as PINs.
– The OTP authentication system is required to support modifying the offset by the modification operation automatically or explicitly when the validation is an unintended failure.
– User information for the OTP authentication system is required to be managed securely.
– The OTP authentication system can optionally support various OTP generation methods.
– The OTP authentication system can optionally support OTP tokens of various types from various vendors.
– The specific OTP authentication protocol for OTP validation is required to include the unique identification data for both the OTP user and the OTP token.
– The OTP token is required to use the approved cryptographic algorithm by international standard organizations such as ITU, ISO, IETF, etc.
– The OTP token is recommended to be able to provide tamper detection, tamper evidence, or tamper response functionalities.
– The OTP token is recommended to cope with the side-channel attack.

The security considerations of the OTP authentication system for each type of framework are described in clauses 9.1.3, 9.2.3, and 9.3.3.

8 General management framework

8.1 OTP management model for the general management framework

As shown in Figure 6, the general management framework is an authentication model between the OTP user and a single service provider. This is a simple yet prevalent model. The general service model has only components that are indispensable to the provision of the OTP authentication service.

An OTP user is issued OTP tokens in order to guarantee stronger access control by various service providers. A single service provider is required to build its own OTP validation server to provide the OTP authentication service. The service provider can decide whether to support a single OTP

token through one OTP validation server or build multiple OTP validation servers to support more than two types of OTP tokens.

The general management framework of OTP authentication is dedicated to a single service provider; the OTP validation server can analyse the user's requirements to select an OTP that fits a particular environment. Moreover, its simple composition method allows the authentication system verifying the static password to enhance simply its authentication method by deploying the OTP authentication system, so that the OTP user can be validated through OTP instead of through a static password.

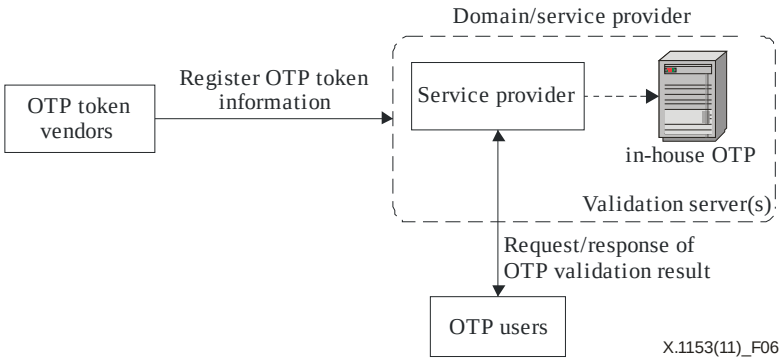


Figure 6 – OTP management model for the general management framework

Since an OTP user cannot use the OTP token issued by a service provider for other services, OTP users who subscribed to more than two service providers experience the inconvenience of carrying multiple OTP tokens. Moreover, every service provider has the burden of deployment, management, and constant maintenance of the OTP validation server.

8.2 OTP management operations for the general management framework

At a high level, the set of operations for the general management framework can be grouped as follows:

– **Validation**: This operation refers to an OTP user's request for validation of OTP to the service provider. The OTP validation server checks the validity of OTP and sends back the results, i.e., whether authentication succeeded or failed; the OTP service provider then transfers the authentication results to the OTP users.

– **Issuance**: This operation involves issuing OTP tokens to OTP users. The OTP user visits the OTP service provider; after his/her identification is checked an OTP token is issued to the OTP user. The activity of OTP token issuance then accompanies service registration as multi-factor authentication.

– **Reissuance**: This operation refers to the reissuance of an OTP token because of loss or damage of the OTP within the expiration date of the OTP token. An OTP user visits the OTP service provider and checks his/her identification. The new OTP token is then reissued to the visiting OTP user, and the issuance of the old OTP token is revoked, accompanying service deregistration for the old OTP token. At this time, the old OTP token can no longer be used for authentication purposes.

– **Renewal**: This operation occurs shortly before the expiration of the OTP token; the OTP user visits the service provider to verify his/her identification, returning the existing OTP token and getting a new OTP token issued by the service provider.

– **Suspension**: This operation refers to the suspension of an OTP token without reissuance/renewal because of the temporary loss of the OTP token. OTP users can urgently request for the suspension of the validation of the OTP generated from their OTP token.

– **Restoration**: If the lost OTP token is returned to the original user, the corresponding OTP token can be restored through appropriate user verification and by recovering the lost OTP token from the OTP token issuer.

– **Modification**: This operation involves adjusting the offset that is closely related to validation information between the OTP token and the OTP validation server. Upon receiving the "modification needed" error message in an OTP authentication transaction, the OTP user enters the ID and OTP on the offset page to complete the OTP offset operation. At the request of the OTP service provider, the OTP validation server renews and saves the validation information for the OTP token (time or event counter), and the OSP transmits the offset result to the OTP user.

– **PIN-unlock**: This operation resets the counts of failed attempts of inputting the hardware PIN. This operation occurs when OTP users request a change in OTP status and the OTP service provider changes the status in response.

– **Activation**: This operation restores the active state from the suspended state and resets the counts of failed attempts to validate the OTP. It initializes an error count when the number of cumulative errors of OTP exceeds a certain number of hits and its use is discontinued. OTP users visit OSP, check their identification, and request for error count initialization. OSP then sends the request for error count initialization to the OTP validation server so that the cumulative OTP error count can be initialized.

– **De-activation**: This operation occurs when the count of validation or modification failures exceeds the predefined value determined by the service providers.

– **Revocation**: This operation entails disposing of the OTP token. When the OTP user does not want to use the OTP token any more, this operation revokes the OTP token.

– **Token registration**: This operation involves the initial registration of information regarding OTP tokens in a batch prior to their issuance to OTP users. OSP registers the token identifier and expiration date plus the OTP generation key in the OTP validation server.

– **Status inquiry**: This operation refers to an OSP check of the OTP-related information of OTP users. Status inquiry operations include the OTP token's management history and status checks (including issue, accident reports, and disposal), OTP token error count checks, and OTP token detailed checks. The OSP can transmit the user identifier to the OTP validation server and check the list of OTP tokens held by the OTP user.

8.3 Security considerations for the general management framework

The following discussion on security considerations of the OTP authentication general management framework assumes that the security requirements have been fully met and that the service is being provided, operated and managed according to the requirements described in clause 7. It should be noted, however, that passive and active attacks can take place on the OTP authentication service itself, as well as on OTP users and the authentication system.

a) Passive attack

OTP authentication request messages transmit sensitive information such as OTP or PIN codes. Attackers can hijack these codes and use them to disguise themselves as OTP users. A typical technique of such attacks is network sniffing. To prevent these attacks, consideration is required to be given to finding ways of securing confidentiality for the sensitive codes included in the OTP authentication request.

b) DoS attack

The attacker may attempt to impede the availability of the OTP authentication system, thereby rendering the authentication system unable to process the validation request of OTPs. Various types of attacks may be attempted, such as restricting normal OTP authentication requests, causing overload to the authentication system itself, and/or imposing overload on the network where the authentication system is connected. These are not necessarily threats to the OTP authentication service itself; once they are detected, however, consideration is required to be given to finding methods of controlling traffic attempting such attacks.

c) Message forgery attack

The attacker can forge or fabricate the contents of the message related to OTP-based authentication. In the validation process shown in Figure 2, the attacker can change the result of "validation failed" to "validation successful" which is transferred from the OTP validation server to the application server; thus causing the acceptance of unauthorized requests. To cope with these attacks, consideration is required to be given to finding ways of supporting integrity for the validation area of authentication.

d) Session hijacking

Even when the OTP user is duly authorized to gain access using OTP, the attacker can hijack the session and deprive the OTP user of access authorization. To counter these attacks, consideration is required to be given to finding ways of providing a separate authentication procedure according to the sensitivity of the application service for the execution of the login process and specific resources in a particular application system.

e) Man-in-the-middle (MITM) attack

By intervening in the communication process between the OTP user and the authentication system, the attacker can receive the OTP user's message, observe or revise the contents of the message, and transmit the revised message to the authentication system. Authentication and confidentiality are suggested as major countermeasures for this attack. As an effective countermeasure for the MITM attack in a general network environment, consideration is required to be given to finding ways of performing mutual authentications or validating the OTP user's message in a cryptographic method between the two communicators.

f) OTP token hijacking and PIN cracking

The attacker may hijack the OTP token carried by the OTP user. By adding a PIN access control function to the OTP token to prevent this attack, malicious use of the hijacked OTP token is restricted. Because the attacker can attempt a brute-force attack to guess the PIN, countermeasures against this attack are required to be considered, such as adding a "lock" function to the OTP token or a "delay" function to the input time of the OTP token after a certain number of failed inputs of the PIN.

9 Interoperable management frameworks

9.1 Centralized management framework

9.1.1 OTP management model for the centralized management framework

As shown in Figure 7, the centralized management framework provides the OTP authentication service to multiple service providers. It consists of realistic scenarios wherein an OTP user wants to access various services in multiple service providers. Unlike the general management framework, the centralized management framework builds an outsourced OTP validation server managed by OSP. The OTP validation server carries out the common OTP authentication service as proxy for multiple service providers.

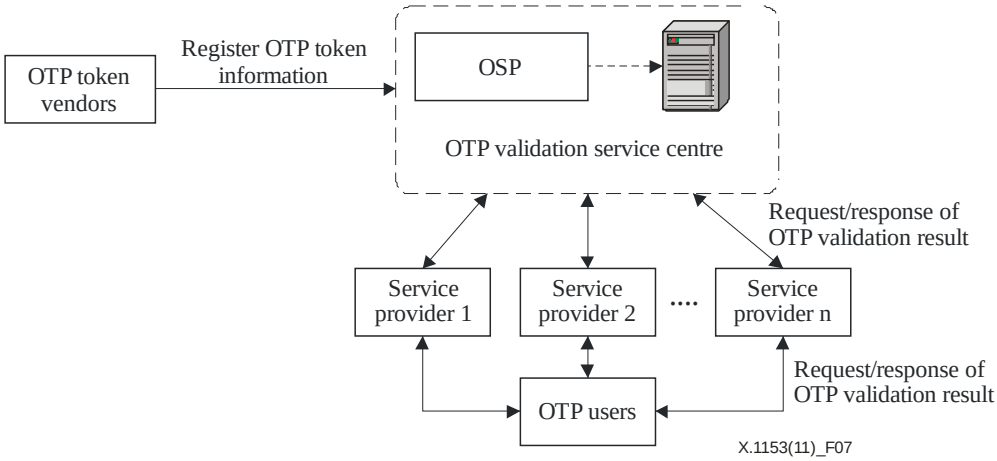


Figure 7 – OTP management model for the centralized management framework

An OTP user is issued an OTP token to be guaranteed more secure service by an issuer. In general, the role of the issuer is assigned to an organization with many branches that are geographically close to OTP users because the OTP token for multi-factor authentication specially needs issuance in person, not by mail. Accordingly, the role of the issuer can be decided by OTP token management, OTP token type, and security policy. Once issued an OTP token, the OTP user can use it for user registration without the need of being issued new OTP tokens to subscribe to the OTP authentication service of other service providers. Service providers process the OTP authentication requested by OTP users by transferring the request to the OSP managing the OTP validation service centre. In other words, service providers can provide the OTP service without building an OTP validation server of their own.

The OTP validation service centre generally includes multiple OTP validation servers to verify the OTP tokens delivered from various OTP token vendors to service providers. Since all authentication operations are centrally managed, the OTP validation service centre is required to be operated as TTP.

The centralized framework has the strong point of being able to provide OTP authentication even if service providers do not build the OTP validation server. As such, service providers can save the costs of building the server by using all OTP tokens of various types supported by the OTP validation service centre. The framework also offers user convenience since all services can be used in common with one OTP token even if users subscribe to multiple service providers.

On the other hand, the framework may have the problem of a single point of failure, i.e., all authentication requests and status checks from service providers must be centrally managed at the OTP validation service centre. Therefore, if any system problem occurs at the OTP validation service centre, all service providers connected to the OTP validation service centre are affected; thus possibly causing large-scale service disruptions.

9.1.2 OTP management operations for the centralized management framework

The centralized framework has the same operations as defined in the general management framework. Two new operations, service registration and de-registration, are additionally defined in the centralized framework. The difference between the general management framework and this framework lies in the fact that service de-registration is made to the other service providers, not to the original OTP token issuer.

– **Service registration**: This operation involves the registration of an OTP token to other service providers. Once an OTP token is issued by a service provider, it can be shared with other service providers by using this operation.

– **Service de-registration**: This operation refers to the de-registration of the OTP token when the OTP user does not want to continue using the OTP from the indicated service provider. However, the OTP user can still use the OTP from other service providers.

9.1.3 Security considerations for the centralized management framework

In the centralized framework environment, security considerations include those described in clause 8.3 for the general management framework. In the interoperable management framework environment, where there is more than one service provider since different management domains share a single OTP validation server, clear definitions are required to be made for the procedure and actors of the issue, registration, renewal, and disposal of tokens according to the security policy at the same level. In case several domains share a single OTP authentication system, consideration is required to be given to counter mechanisms to cope with DoS attacks that may hurt the availability of the authentication system as described in clause 8.3 for security considerations. In this case, an attempt at direct attack by the attacker can be restricted through the dedicated line between the different management domains and the authentication system.

9.2 Enhanced centralized management framework

9.2.1 OTP management model for the enhanced centralized management framework

The biggest problem of the centralized framework is that it is affected by any system problem at the OTP validation service centre as it is centrally managed.

In terms of guaranteeing stability, all facilities at the OTP validation service centre may be duplicated. Nonetheless, the service provider must continue the service if errors occur in the communication area or irreparable damage takes place. Therefore, in-house OTP validation server means are required to be devised for the stable operation of the service in mission critical application domains, including Internet banking or electronic payment, wherein the discontinuation of service may cause critical losses. In terms of the OTP management framework, its in-house architecture finally corresponds to the general management framework. Therefore, service providers wishing to offer only one OTP token service, regardless of the number of service providers accessed by the OTP user, can select the enhanced centralized framework even if they implement an in-house architecture for OTP authentication.

Except for the fact that there are service providers with their own OTP validation server, the model shown in Figure 6 has the same centralized framework. In other words, the model has a scenario wherein an OTP user receives services from multiple service providers and the OTP validation service centre centrally performs the OTP authentication operation as proxy for multiple service providers. Nonetheless, service providers can selectively build an OTP validation server that is identical to that at the OTP validation service centre.

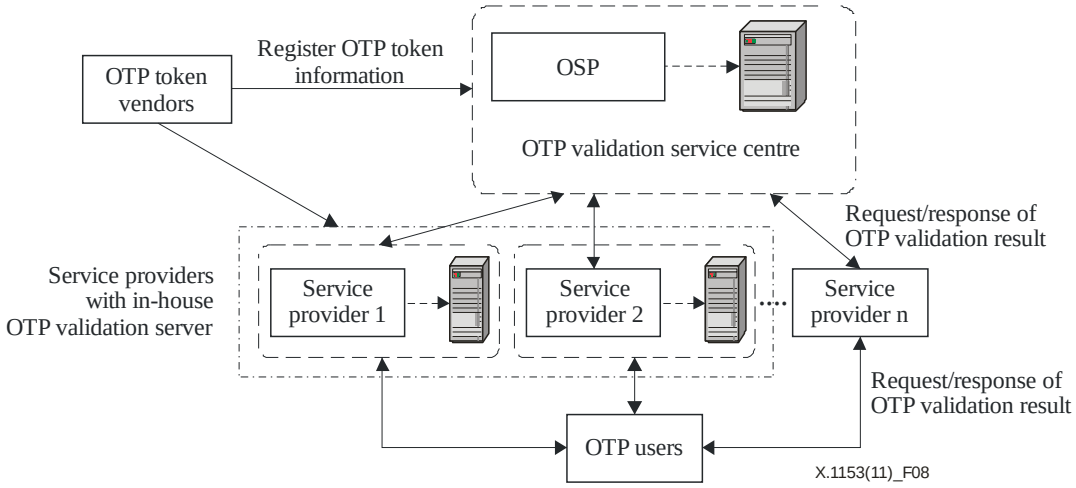


Figure 8 – OTP management model for the enhanced centralized management framework

The in-house OTP validation server can provide the authentication service for its own OTP tokens issued by the service provider. Of course, in case the OTP token issued by another service provider is registered and used, the in-house OTP validation server is limited since it must perform authentication through the OTP validation service centre. Nevertheless, all OTP tokens issued by the service providers themselves are provided with authentication through the in-house OTP validation server. Since the OTP validation server at the OTP validation service centre can be used if any system problem occurs in the in-house OTP validation server, stability increases considerably. A service provider implements the in-house architecture but does not verify the OTP token issued by other service providers for the following reasons:

– First, the service provider of the in-house architecture cannot manage all the user information registered in the other service providers if the number of service providers increases exponentially. User information includes user identifier, token identifier, access authorization, etc.

– Second, as an alternative solution, the service provider of the in-house architecture can forward the OTP validation request to other in-house architecture-based service providers that issue the OTP token without OSP. Likewise, the service provider requires a discovery mechanism to find the appropriate OTP validation location such as directory service and routing table. This solution can be used by the cross-domain framework wherein the number of associated OTP validation servers is relatively small. We can define this framework as the distributed management framework.

– Finally, some organizations, such as the financial section, might not want to share their user information with other parties.

An in-house OTP validation server can be selectively established by service providers that are critically affected by the discontinuation of service. In other words, the in-house OTP validation server has basically all the features of the centralized framework, and service providers with an in-house OTP validation server have the advantage of being able to provide a stable service. The characteristics of this server are identical to those of the centralized framework.

The strong point of the enhanced centralized framework with in-house OTP validation server is that it inherits the strong points of the centralized framework, i.e., all service providers can use one OTP token. Moreover, the framework has the advantage of guaranteeing availability of service even when a system problem occurs at the central OTP validation service centre.

Nonetheless, the service provider establishing the in-house OTP validation server will incur in double cost for the establishment of as well as for the interoperation with the OTP validation service centre. Therefore, since the cost of establishment is relatively higher than for other frameworks, and

operations are very complicated, consideration is required to be given to the exact implementation according to mutually agreed upon algorithms in building the service.

9.2.2 OTP management operations for the enhanced centralized management framework

The enhanced centralized framework with an in-house OTP validation server has the same operations as those of the general management framework described in clause 8. OTP users can perform authentication either through the in-house OTP validation server or through the OTP validation server located at the OTP validation service centre. This composition creates the problem of running counter to the feature of the one time password. Therefore, OTP is required to be validated only once by the service provider or centralized OSP. If authentication is performed by two OTP validation servers, the same OTP can be reused successfully for authentication. To resolve this problem, the in-house OTP validation server and the OTP validation server at the OTP validation service centre is required to synchronize the validation-related information in real time. Therefore, additional new operations of the enhanced centralized framework include server synchronization, backward notification, and transfer regarding the OTP token's information.

– **Synchronization**: The synchronization operation involves the use of transport messages to ensure synchronization of OTP operation-related information between service providers building an in-house OTP validation server and OTP validation server at the OTP validation service centre. Since the OTP validation servers are located at the OTP validation service centre and owned by OTP service providers, the validation information (offset) at the two OTP validation servers is required to be identically maintained whenever OTP users request for OTP authentication and OTP offset.

– **Notification**: If OTP users performed authentication or other operations such as status change using the OTP in an OTP service provider different from the one that issued the OTP, the information is required to be provided to such a service provider to prevent security accidents. This operation includes sync notification, suspension notification, and activation notification.

  • **Activation-notification**: Notification means for error count initialization.

  • **Sync-notification**: Notification means for synchronization.

  • **Suspension-notification**: Notification means for accident reporting.

– **Token transfer**: This operation refers to a process required to join the OTP validation service centre and receive the interoperable authentication service. An OSP operating its own OTP validation server completes a batch registration of all information at the OTP validation service centre, including token identifier, expiration date, issuing service provider, OTP status information (including disposal, accident report, and accident restoration), and OTP generation key of OTP tokens that have already been issued and used prior to the launch of the interoperable authentication service.

9.2.3 Security considerations for the enhanced centralized management framework

In the enhanced centralized framework with in-house OTP validation server, security considerations include those described in clauses 8.3 and 9.1.3 for the other general management frameworks. Because OTP authentication systems with identical operations are managed and maintained in different management domains in the enhanced centralized framework, clear definitions are required to be made for the synchronization operations of the OTP information between OTP validation servers. This operation includes OTP offset and synchronization of OTP validation information. Since identical application services and security policies are presumed in this environment as in the centralized framework, consideration is required to be given to the management methods for verifying identical security.

9.3 Cross-domain management framework

9.3.1 OTP management model for the cross-domain management framework

The cross-domain framework is needed for the interoperability of multiple OSPs. As shown in Figure 7, OTP users using multiple centralized frameworks can receive services from all service providers with one OTP token.

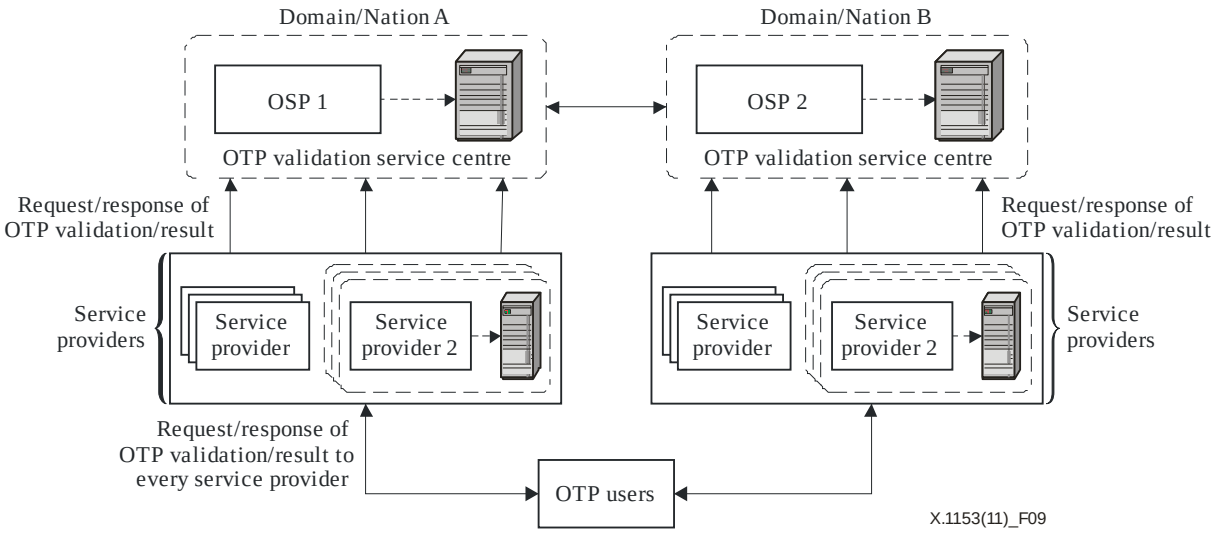


Figure 9 – OTP management model for the cross-domain management framework

The cross-domain framework is applicable without changing the existing authentication system through the interoperation between multiple OSPs that manage the OTP validation service centres undertaking their domains. A service provider can subscribe to the domain where it belongs, the same as the domain where the centralized framework belongs; it only has to use the operations that have been previously supported. Nonetheless, the OTP validation service centre is required to understand the security level of the corresponding domain and subsequently activate interoperation with the other domains if the security level is the same as that of other domains. The service is required to have limited interoperability if the security level is different, including identification proofing method for issuing the OTP between the domains. Policy decisions are important, such as interoperating from the domain with stronger security level to the domain with general security, but not in the opposite case.

The possibility of interoperation between the OTP validation service centres is unlimited and there may be various types of interoperable models according to the service requirements of the relevant domains. Various situations can take place, e.g., wherein the OTP validation service centre in Nation A interoperates with two domains in Nation B and Nation C or wherein the OTP validation service centre in Nation C cannot interoperate with the domain in Nation B but does so with the domains in Nation A and Nation D. In these situations, what matters most is the method of checking in which domain the OTP validation server belongs and performing the authentication of the OTP tokens of OTP users.

The cross-domain framework solves this problem by marking the domain of the OTP validation service centre on the OTP token. In this case, if the OTP user wants to use the OTP token issued by a domain in another service provider's domain, this domain notifies the OTP validation service centre of the issuing domain in the registration process, and the OTP validation service centre allows the registration if the domain has been registered beforehand according to the security level.

9.3.2 OTP management operations for the cross-domain management framework

Before describing the basic operation of the cross-domain framework, suppose interoperable validation service is provided between OTP validation service centre A in domain A and OTP validation service centre B in domain B. Likewise, assume that the OTP user is issued an OTP token from OSP I, which has subscribed to OTP validation service centre A and has registered the use of another service provider to OSP II, which is subscribed to OTP validation service centre B.

The OTP-related operations requested by OTP users to OSP I will not be described here since they are the same as those described in other management frameworks. Among the operations requested by OTP users to OSP II, only those operations requiring additional information transmission between the centres will be described. Compared to existing frameworks, the basic operations of the cross-domain frameworks are extended forms from the flow chart of the general management framework operations. They have fundamentally identical operations but require communication between the centres. The difference is that management operations are processed between centres. Operations commonly include OTP token identifier, vender code, and service provider code to identify the OTP between centres where the OTP token profiles are registered. The following operations are required to be managed: authentication/validation, OTP status management, offset synchronization, and user registration/de-registration. These operations have the same purpose as the operations described in clause 8.2.

These operations have the same procedure for processing a request for management operation from the OTP user. For example, if the remote user of domain A requests for the validation of an OTP to the SP of domain B in Figure 9, the SP forwards to OSP II the corresponding token's OTP, OTP token identifier, authentication centre code, and operational code. The operational code notifies the OTP validation servers of the type of management operation. OSP II checks the authentication centre code and recognizes domain A where the OTP user is registered. The request for validation of OTP is then forwarded to OSP I. Finally, OSP I replies to OSP II with "success" or "failure" as the result of the OTP validation. The OTP user receives the result of the OTP validation from the SP taking over the reply.

9.3.3 Security considerations for the cross-domain management framework

In the cross-domain framework environment, security considerations include those described in the previous clauses for the other frameworks. Additional considerations may include the following:

a) Authority management between the centralized frameworks

The centralized framework environment with in-house OTP validation server uses identical application services and security policies. Note, however, that the cross-domain framework environment may have different application services and security policies; thus, appropriate authority management methods by OTP authentication is required to be considered.

b) Key registration and issue procedure

In the case of the key registration procedure, different registration procedures can be considered depending on the key maintenance and management methods, unlike the previous frameworks. The first method involves saving the key in a particular interoperable management framework only and sharing the token information. The second is to save identical keys in all authentication systems agreed upon between the centres. In this case, consideration is required to be given to finding ways of registering and transmitting the key from the management domain that initially issued the key to the authentication system in the additional management domain. Moreover, even if the OTP token is registered and issued in a centralized framework, identical keys are required to not be saved unless OTP users expressly request that the key registration be saved in other interoperable OTP authentication systems. Consideration is required to be given to the transparent procedure for the above-mentioned key registration and issue.

c) OTP synchronization policy

The synchronization of OTP information between cross-domain OTP authentication systems can vary according to the key registration and issue procedures. If identical keys between centres are saved, synchronization requirements are the same as those for the enhanced centralized framework environment with in-house OTP validation server.

d) OTP authentication policy between centralized frameworks

An attacker may be disguised as the OTP user in a high mission-critical management domain using an OTP hijacked from the management domain of a centralized framework with low mission-critical application services. Therefore, the OTP authentication policy used between cross-domain frameworks is required to consider using different authentication methods.

Appendix I

Service deployment scenarios

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

I.1 Overview of service deployment scenarios

This clause describes the OTP-based authentication service scenarios that can be logically composed apart from the specific requirements for real application services as shown below. The OTP-based authentication service view in clause 6 gives many possibilities of service deployment scenarios. The most important of the nine cases in the following four service areas are described (it will be assumed that the domains want to use OTP for multi-factor authentication in all cases):

(a) Local network access control scenario.

(b) Remote network access control scenario.

(c) Application/contents access control scenario.

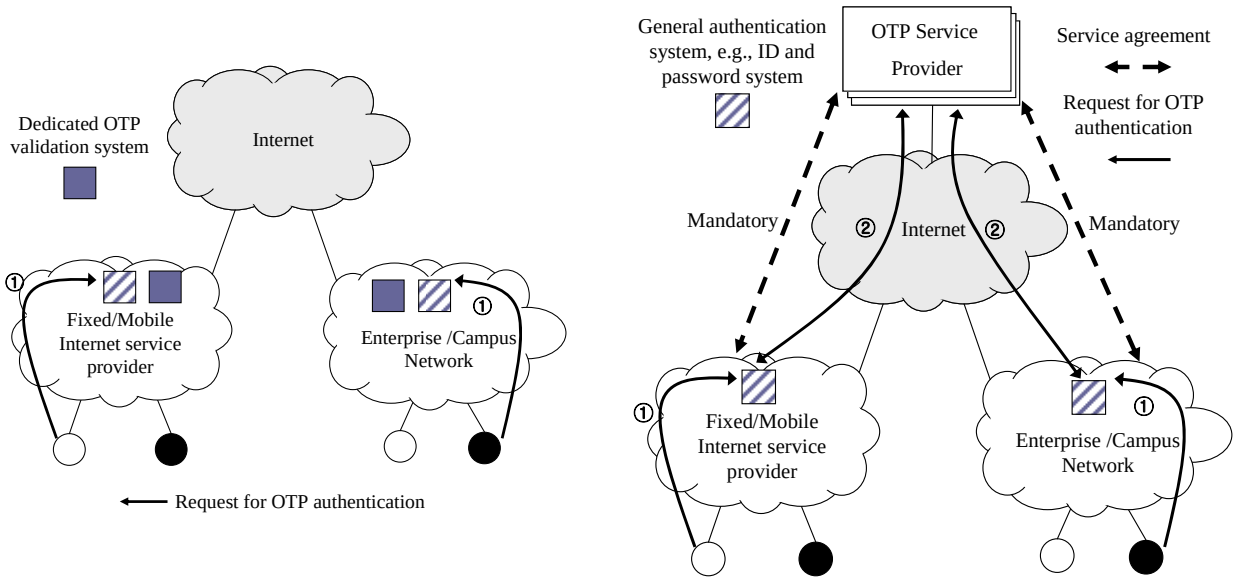
For the expanded use of the traditional ID password to the OTP-based authentication service, hardware-based and software-based OTP tokens can be used as possession-based authentication. Tokens can be provided in various forms including IC card, mobile phone, dedicated token.

I.2 Local network access control scenario

The OTP-based authentication service for local network access control is the simplest scenario. In this scenario, the local network includes fixed/mobile Internet service providers and enterprise/campus networks; users have the following two classifications: subscriber of an Internet service provider and employee of enterprise/campus network. Two types of OTP authentication are possible: two-party and trusted third-party authentication frameworks [ITU-T X.811]. From the OTP authentication process, service providers can implement a procedure wherein the OTP user obtains authorization through the authentication process from a single domain authorization framework: pull sequence, agent sequence, and push sequence [b-IETF RFC 2904]. To use Internet resources, token holders receive verification of user identification as legitimate users from the local network. In general, local network providers determine the authorization for network access from requests from users using registered identity information and passwords through the authentication system they manage on their domains or from outsourced trusted third parties. For example, in wired networks, authentication requests from users are generally forwarded to a corresponding authentication system through the network access server (NAS). With wireless networks using [b-IEEE 802.1x], an authentication request can be sent to the authentication system through authentication protocols such as EAP. In the case of mobile communications networks, they can define their own authentication protocol such as TLS.

An OTP user who has received proper authorization through the authentication process can gain access to his/her office resource and log in to the Internet as well according to the access authorization. Depending on the authentication methods, this scenario is applied not only to the access control of local networks but also to various applications requiring the verification of user identification.

If a trusted third-party service model is applied, however, there is a requirement of charging service fees between OTP service providers and local networks. In this case, OTP authentication service providers generally have a billing management policy. With regard to the local network's use of the OTP authentication verification, service fees can be determined and charged according to the service agreement between the local networks and the OTP service provider.



(a) Dedicated OTP authentication scenario, Scenario (a)-1

(b) TTP-based OTP authentication scenario, Scenario (a)-2

Figure I.1 – Local network access control scenario

- **Scenario (a)-1**

The dedicated OTP authentication scenario describes the management of the OTP validation server in the local network domain independently. In Figure I.1's scenario (a)-1, there is no OTP service provider for the TTP model, and each network domain is required to verify an OTP user's identification and authorization individually. The user's profile may require OTP as additional authenticator for strict access control.

This service flow corresponds to the basic network access control scenario and the two-party authentication model. Under this scenario, the OTP user is required to have the same number of tokens as the domains accessed, since each network domain manages its own OTP validation server and employees/subscribers.

Considering the OTP management framework, scenario (a)-1 corresponds to the OTP management model for the general management framework described in clause 8.

- **Scenario (a)-2**

The TTP-based OTP authentication scenario means that the local network domains outsource the OTP validation server to an outside party. In this service scenario, the local domain and OSP is required to have a service agreement for the authentication service; they have to guarantee secure transport between their authentication systems. Therefore, the local domain does not need to manage the dedicated OTP authentication system; it can implement the single domain authorization framework using the TTP service to assign an OTP user's authorization. Subsequently, OSP can provide strict access control in the local domain, with the OTP user able to access any local domains that make use of the authentication service from the TTP-based OTP SP. In the TTP model, the domain and OSP may need a service agreement to charge authentication service fees.

Considering the OTP management framework, scenario (a)-2 corresponds to the centralized framework addressed in clause 9.1. In the case of scenario (a)-2, each domain needs a service agreement with OSP for OTP authentication. Therefore, users can connect to any domain (i.e., fixed/mobile ISP and enterprise/campus network OSP service providers), although an OTP user possesses only one token. In general, each domain and the OSP can make their link through the token identifier of the OTP token. If ISPs and local domains use each other's OSPs, and the OSPs are interoperable between them, this scenario corresponds to the cross-domain framework described

in clause 9.3. These enhanced framework patterns can be commonly applied to the following scenarios and can be deployed according to the security and service requirement in each domain:

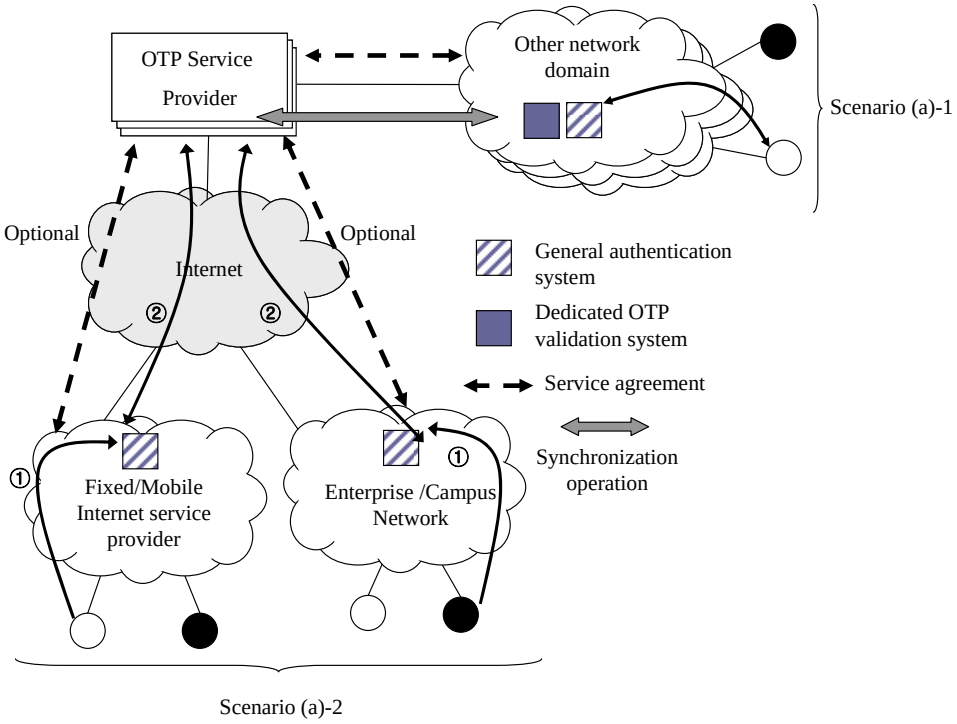


Figure I.2 – Combined local network access control scenario, Scenario (a)-3

- **Scenario (a)-3**

Figure I.2 illustrates the situation in scenarios (a)-1 and (a)-2 combined. The OTP token issued from its own local domain can be used to authenticate in other local domains that have a service agreement with its own OSP regardless of whether the OTP user's local domain possesses a dedicated OTP validation server. Likewise, the OTP user can access any local domain that uses the authentication service from the TTP-based OTP SP.

Considering the OTP management framework, scenario (a)-3 corresponds to the combined model between the centralized management model described in clause 9.1 and the general framework addressed in clause 8.1. The domain in scenario (a)-1 deploys the general management framework but has connection and service agreement to the OSP in scenario (a)-2. Accordingly, this scenario shows the enhanced management framework described in clause 9.2 and requires the operation for offset synchronization between OTP authentication systems.

- **Practical use cases and corresponding framework**

These categories apply to a scenario used in various areas requiring user identification and access authorization in the local networks. Generally, it applies to closed agencies that strictly prohibit outsider access including businesses, hospitals, and military forces as well as ISPs that provide OTP as a premium security service for their own subscribers.

If multi-factor authentication is required for diverse resources in the local networks, this scenario can be implemented by having users enter OTP at the application layer in addition to the traditional authentication process or by integrating other authentication protocols in the form of OTP over X (X includes EAP, Radius, SSL, etc.).

I.3 Remote access control scenario

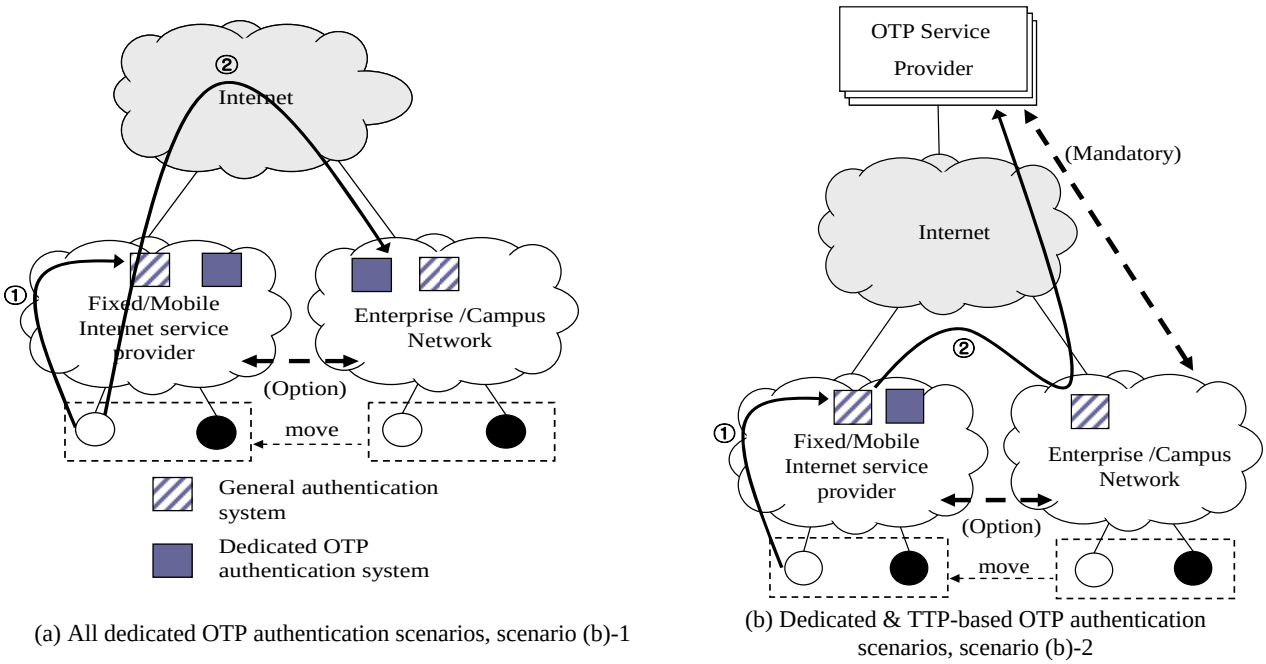
The OTP-based authentication service for remote access control is a scenario wherein subscribers of a specific local network use their own network resources through public networks including the Internet. This scenario applies to cases wherein the scenarios described in the previous clause are expanded to include roaming sequence authorization frameworks [b-IETF RFC 2904].

In this scenario, remote users use the OTP-based authentication service to receive verification and authorization as legitimate users from their registered local network domains. Depending on the agreement between the OTP service provider, SPs, and local network, a variety of scenarios can be suggested as shown in Table I.1. In general, if a service agreement is established between the local networks and SPs, they can exchange user profiles and validation information between OTP authentication systems. If a service agreement does not exist between the two domains, however, they are required to individually go through the authentication process used in each domain. In the remote access control scenario, for example, the application of various VPN policies is possible to protect transported data according to the security requirements of the local domains and user authorization. OTP authentication can then enable stricter access control for the remote user.

If a trusted third-party service model is applied, however, charging service fees between the OTP service provider and local networks is required. In this case, the OTP authentication service provider generally needs to have a billing management policy. Regarding the local network's use of OTP authentication verification, service fees can be determined and charged according to the service agreement between the local networks and the OTP service provider.

Table I.1 – Various scenarios wherein remote access control is applicable

Scenario No.	Local network authentication model	ISP authentication model	Remarks
Scenario (b)-1	2-party service model	2-party service model	– Roaming sequence authorization model. – A service agreement between the local network and ISP is optional. – There may be more than one OTP service provider.
Scenario (b)-2	3-party service model		
Scenario (b)-3	2-party service model	3-party service model	
Scenario (b)-4	3-party service model		



(a) All dedicated OTP authentication scenarios, scenario (b)-1

(b) Dedicated & TTP-based OTP authentication scenarios, scenario (b)-2

Figure I.3 – Remote access control scenario 1

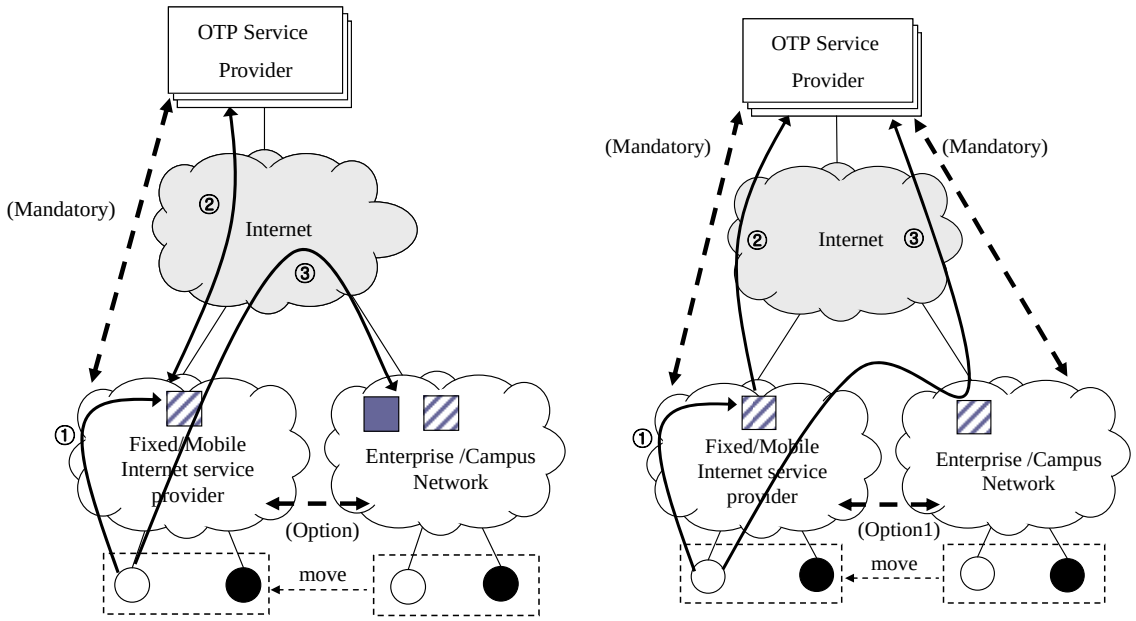
- **Scenarios (b)-1 and (b)-2**

In Figure I.3, scenario (b)-1 illustrates a remote access control situation wherein the local network domain and the ISP use a two-party authentication model. If there is no service agreement between the local network and ISP, an OTP user is required to complete the authentication process not only in the service provider but also in his/her own local domain.

If there is a service agreement between both domains, this scenario takes into account the roaming sequence authorization framework for provisioning valid access. The service provider in this condition forwards an authentication request to the local network, and the OTP user gets remote access in his/her own local domain without additional authentication processes. To enhance user convenience, those domains may use identity federation and provide simplified authentication processes through the pre-sharing of user profiles or by exchanging authentication information.

In Figure I.3, scenario (b)-2 illustrates the case wherein the local network domain uses TTP-based OTP authentication. Likewise, if there is a service agreement between both domains, this scenario takes into account the roaming sequence authorization framework for provisioning valid access.

Considering the OTP management framework, scenario (b)-1 corresponds to the remote access scenario between the OTP management models for the general management framework described in clause 8, whereas scenario (b)-2 corresponds to the remote access scenario between the centralized frameworks addressed in clause 9.1.



(a) TTP-based & Dedicated OTP authentication scenario, Scenario (b)-3

(b) All TTP-based authentication scenarios, Scenario (b)-4

Figure I.4 – Remote access control scenario 2

- **Scenarios (b)-3 and (b)-4**

In Figure I.4, scenario (b)-3 illustrates the case wherein the Internet service provider uses the TTP-based OTP authentication, whereas scenario (b)-4 presents the case wherein the service providers and the local domains all use TTP-based OTP authentication. In the case of scenario (b)-3, if there is a service agreement between the local network and the ISP, they can provide the roaming sequence authorization framework as in scenarios (b)-1 and (b)-2. Otherwise, the OTP user is required to carry out the authentication process in each domain independently.

In the case of scenario (b)-4, if the ISP and the local network domain use the same OTP service provider, and there is a service agreement between them, the OTP user can gain access authorization through only one token in his/her own local domain. In particular, authentication service can be received with other OTP service providers, in which case OTP SPs may need a service agreement for supporting interoperability between them.

Considering the OTP management framework, scenario (b)-3 corresponds to the remote access scenario between ISP, having the OTP management models for the centralized management framework described in clause 9 and the local network deploying the general management framework addressed in clause 8. In the case of scenario (b)-4, the ISP and the local network are getting the OTP authentication service from the same OSP. Accordingly, this scenario corresponds to the centralized management framework in clause 9.

- **Practical use case**

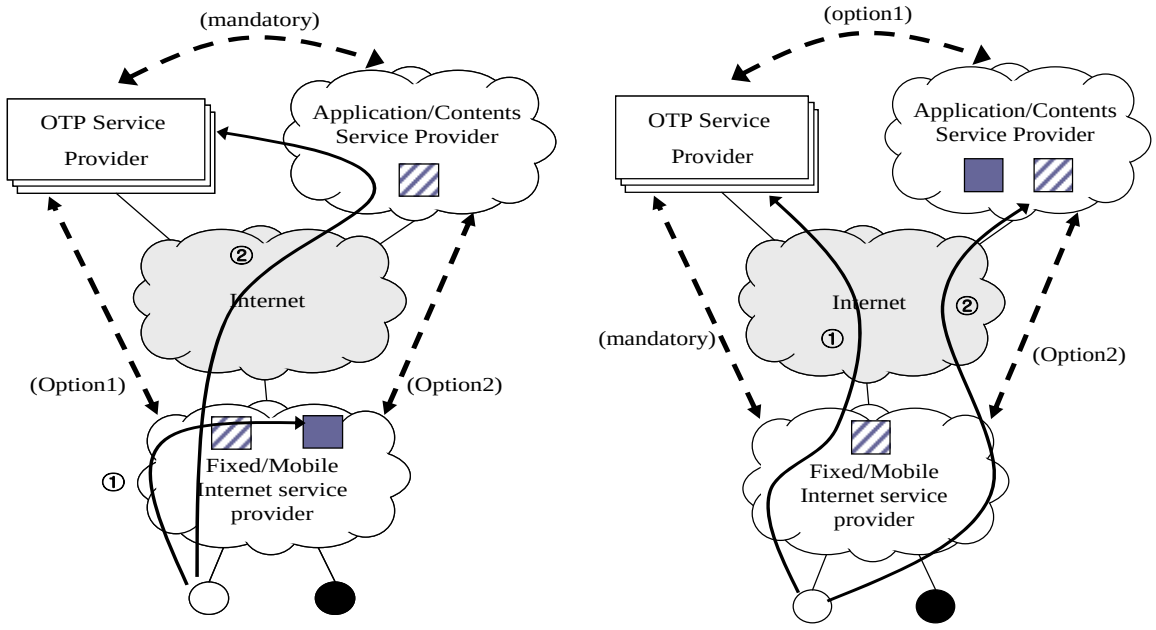
The remote access control scenario has many application cases, including the mobile user's remote access through public networks, branch offices that need to log into local networks (main office), and partners requiring access to resources at the main office. The administrator of the local network domain can establish the OTP-based authentication service when strong remote user authentication is required.

I.4 Application/contents access control scenario

This type of OTP-based authentication for application and content access control is logically identical to the remote access control scenario described in clause I.3, which determines access authorization for the resources that users need to use via service providers. General cases of application/contents access control include the token holder's use of content such as texts, images, and videos through the web. In this case, the application and contents service provider (ACSP) may need to go through separate transaction authentication and exchange of transaction information with financial institutions and credit card companies on purpose to charge a fee for content access.

In the case of the application/contents access control scenario, this clause focuses on two cases in terms of whether an ISP or an ACSP has a service agreement with the OTP service provider, since OSP can offer interoperability from such an ISP or an ACSP.

After going through the authentication process for network access control regardless of OTP authentication, token users log into the application domains they need. If ACSPs require multi-factor authentication for the transmission of sensitive data or access to personal information, however, OTP-based authentication service can be provided through dedicated or other OTP service providers. In particular, these deployment cases have the feature of allowing OTP to realize access control for contents.



(a) Service agreement exists between OSP and ACSP, Scenario (c)-1

(b) No service agreement exists between OSP and ACSP, Scenario (c)-2

Figure I.5 – Application/contents access control scenario

- **Scenarios (c)-1 and (c)-2**

In Figure I.5, scenario (c)-1 illustrates the situation wherein the OTP user can get execution authority for specific contents after verifying user identity and getting access authorization from ISP and ACSP. ACSP can require the OTP user to submit an OTP for stricter execution authority for sensitive content or premium service. Afterward, ACSP can outsource the TTP-based OTP service provider for multi-factor authentication. If the OTP service provider and the ISP have a service agreement for sharing OTP tokens, the OTP user can get access authorization through only one token when using contents services.

In Figure I.5, scenario (c)-2 illustrates the case wherein ACSP uses dedicated OTP authentication. In such case, if ACSP has a service agreement with OSP for sharing an OTP token, the OTP user can get access authorization through only one token when using contents services. In this scenario of Figure I.5, one option represents an agreement in relation to OTP authentication, whereas the other option includes the service agreement for identity sharing such as that for identity federation.

- **Practical use case**

This use case is an OTP security service scenario that is most universally used with various application areas such as financial transactions, e-commerce, web portals, and personal homepage services.

Bibliography

[b-ITU-T X.25] Recommendation ITU-T X.25 (1996), *Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit*.

[b-ITU-T X.1141] Recommendation ITU-T X.1141 (2006), *Security Assertion Markup Language (SAML 2.0)*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-FIPS PUB 140-2] FIPS PUB 140-2 (2001), *Security Requirements for Cryptographic Modules*.

[b-IEEE 802.11] IEEE 802.11-2007, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.

[b-IEEE 802.1x] IEEE 802.1x-2004, *IEEE Standard for Local and Metropolitan Area Networks – Post-Based Network Access Control*.

[b-IETF RFC 2289] IETF RFC 2289 (1998), *A One-Time Password System*.

[b-IETF RFC 2869] IETF RFC 2869 (2000), *RADIUS Extensions*.

[b-IETF RFC 2904] IETF RFC 2904 (2000), *AAA Authorization Framework*.

[b-IETF RFC 4226] IETF RFC 4226 (2005), *HOTP: An HMAC-Based One-Time Password Algorithm*.

[b-IETF RFC 4793] IETF RFC 4793 (2007), *The EAP Protected One-Time Password Protocol (EAP-POTP)*.

[b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*.

[b-ITGI-COBIT] ITGI COBIT (2007), *Control Objectives for Information and related Technology (COBIT v4.1)*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2011