

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



International
Telecommunication
Union

Documents
Document Sharing Hub

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/>.

© ITU 2011

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

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	3
5 Conventions	3
6 OTP-based authentication service	4
6.1 Introduction	4
6.2 General features.....	4
6.3 OTP-based authentication service	8
7 OTP management architecture	9
7.1 OTP entities.....	9
7.2 OTP management blocks.....	9
7.3 OTP management framework.....	11
7.4 OTP management procedures.....	13
7.5 OTP management requirements	14
8 General management framework.....	15
8.1 OTP management model for the general management framework.....	15
8.2 OTP management operations for the general management framework	16
8.3 Security considerations for the general management framework	17
9 Interoperable management frameworks	18
9.1 Centralized management framework.....	18
9.2 Enhanced centralized management framework.....	20
9.3 Cross-domain management framework.....	23
Appendix I – Service deployment scenarios.....	26
I.1 Overview of service deployment scenarios	26
I.2 Local network access control scenario	26
I.3 Remote access control scenario.....	29
I.4 Application/contents access control scenario.....	32
Bibliography.....	34

Downloaded from

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.

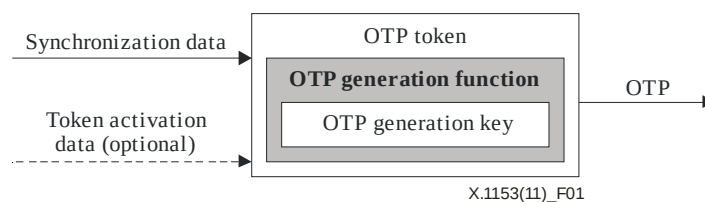


Figure 1 – OTP generation function

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):

$$\text{OTP} = \text{OTP Generation Function (OTP generation key, Synchronization data, [Token activation data])}$$

; 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.

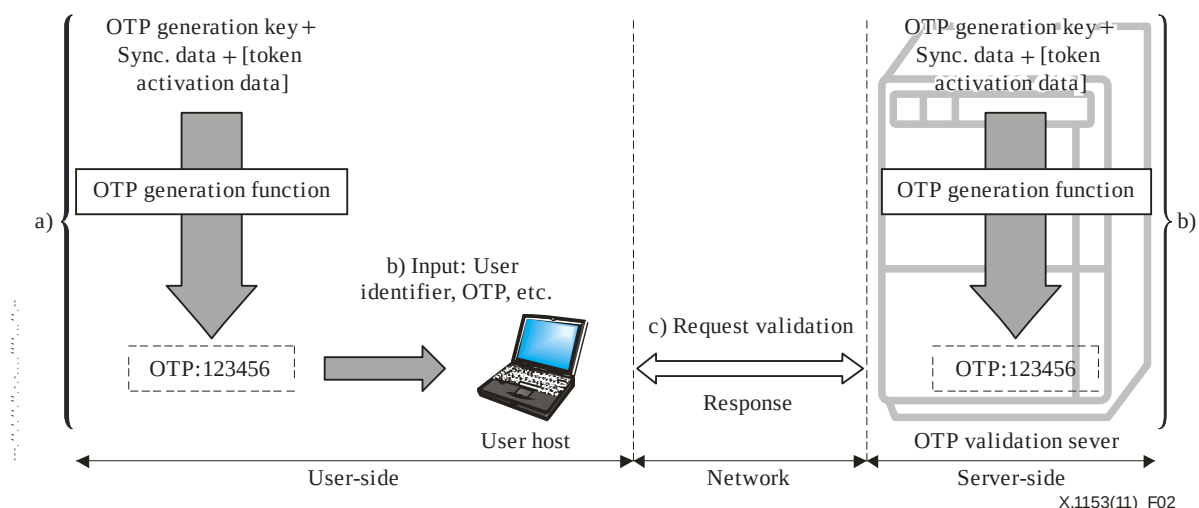


Figure 2 – OTP validation process

- 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:

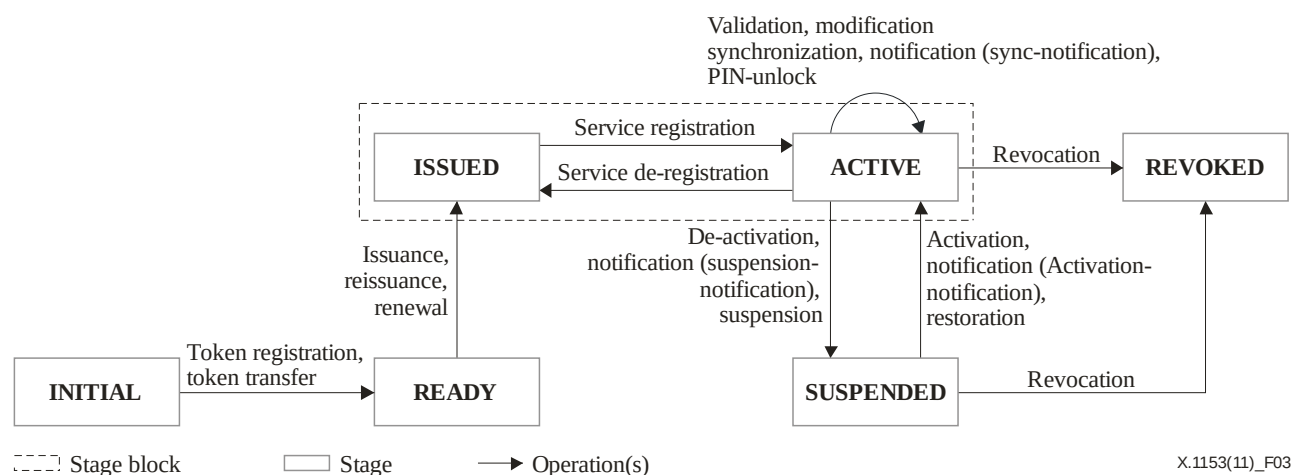


Figure 3 – OTP token life cycle

- **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.