FEITIAN

OTP Server Authentication System V3.0 Brief Introduction

V 1.0

Feitian Technologies Co., Ltd.

Website: www.FTsafe.com

Revision History:

Date	Revision	Description
Mar. 2010	V1.0	Release of the first version

Software Developer's Agreement

All Products of Feitian Technologies Co., Ltd. (Feitian) including, but not limited to, evaluation copies, diskettes, CD-ROMs, hardware and documentation, and all future orders, are subject to the terms of this Agreement. If you do not agree with the terms herein, please return the evaluation package to us, postage and insurance prepaid, within seven days of their receipt, and we will reimburse you the cost of the Product, less freight and reasonable handling charges.

1. Allowable Use – You may merge and link the Software with other programs for the sole purpose of protecting those programs in accordance with the usage described in the Developer's Guide. You may make archival copies of the Software.

2. Prohibited Use – The Software or hardware or any other part of the Product may not be copied, reengineered, disassembled, decompiled, revised, enhanced or otherwise modified, except as specifically allowed in item 1. You may not reverse engineer the Software or any part of the product or attempt to discover the Software's source code. You may not use the magnetic or optical media included with the Product for the purposes of transferring or storing data that was not either an original part of the Product, or a Feitian provided enhancement or upgrade to the Product.

3. Warranty – Feitian warrants that the hardware and Software storage media are substantially free from significant defects of workmanship or materials for a time period of twelve (12) months from the date of delivery of the Product to you.

4. Breach of Warranty – In the event of breach of this warranty, Feitian's sole obligation is to replace or repair, at the discretion of Feitian, any Product free of charge. Any replaced Product becomes the property of Feitian.

Warranty claims must be made in writing to Feitian during the warranty period and within fourteen (14) days after the observation of the defect. All warranty claims must be accompanied by evidence of the defect that is deemed satisfactory by Feitian. Any Products that you return to Feitian, or a Feitian authorized distributor, must be sent with freight and insurance prepaid.

EXCEPT AS STATED ABOVE, THERE IS NO OTHER WARRANTY OR REPRESENTATION OF THE PRODUCT, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

5. Limitation of Feitian's Liability – Feitian's entire liability to you or any other party for any cause whatsoever, whether in contract or in tort, including negligence, shall not exceed the price you paid for the unit of the Product that caused the damages or are the subject of, or indirectly related to the cause of action. In no event shall Feitian be liable for any damages caused by your failure to meet your obligations, nor for any loss of data, profit or savings, or any other consequential and incidental damages, even if Feitian has been advised of the possibility of damages, or for any claim by you based on any third-party claim.

6. Termination – This Agreement shall terminate if you fail to comply with the terms herein. Items 2, 3, 4 and 5 shall survive any termination of this Agreement.

PREFACE

OTP Server Dynamic Password Authentication System V3.0 (or OTP Server Authentication System V3.0 below) is a system which provides a dynamic password authentication and online transaction signature service. Firstly, it helps end-user to identify the genuine application server while helping the application server to authenticate a real end-user. Additionally, it provides digital signatures for online transactions, which helps to create a highly secure communication environment for both end-users and servers.

OTP Server adopts the most advanced technologies and is also based on open-architecture, so that it is not only highly reliable, but also very easy to maintain. It aims to provide various application servers with secure dynamic password authentication services in various flexible authentication schemes to satisfy the needs from different customers.

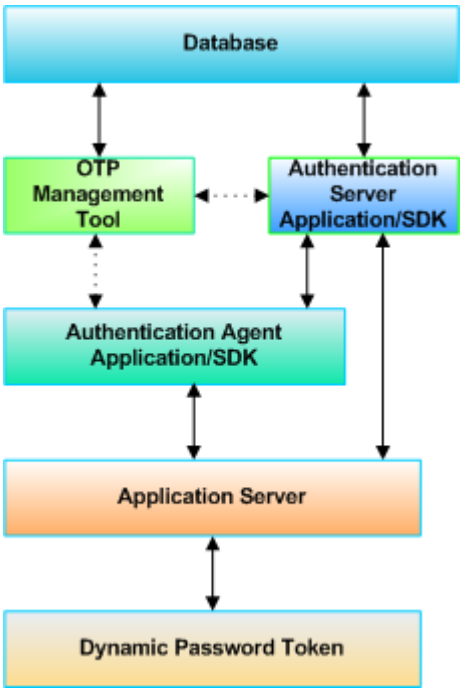
This document provides a brief introduction to the OTP Server Authentication System V3.0.

Contents

Chapter 1. The System

1.1 Abstract

OTP Server Authentication System V3.0 is made up of three main parts: the authentication server, the management tool and the authentication agent, as well as three supplementary parts; the database management system for OTP server, SDK interfaces for customization, and OTP tokens for producing dynamic passwords.



1.2 The Authentication Server

The authentication server is one of the most important parts of the OTP Server Authentication System V3.0, whose main functions includes authenticating dynamic passwords, synchronizing OTP tokens with the system and verifying transaction signatures etc.

The authentication server receives an authentication request from the authentication agent or from a radius server, then verifies the request and sends back the authentication result. In order to fulfill high-performance demands of processing large quantities of data and high levels of concurrent requests in a very reliable way, the authentication server adopts many techniques such as hot standby server and load balancing in its design. Moreover, the authentication server can process requests sent by OTP tokens from other manufacturers through the agent mode or API method, which largely enhances its ability to be integrated into other existing dynamic

password authentication systems.

1.3 The Management Tool

The management tool has an easy-to-use web interface to provide remote management and maintenance of end-users, OTP tokens, authentication servers, authentication agents and log information from the database.

1.4 The Authentication Agent

The authentication agent functions as a bridge between the authentication server and an application server. When an end-user logs in to the application server, the application server will send an authentication request to and receive result from the authentication server through the agent in order to decide whether the end-user is allowed to log in.

To be specific, different application servers will need different authentication agents. If an application server has already integrated the RADIUS protocol for authentication, there is no need for an authentication agent.

1.5 The Database Management System

The database management system is the basis of the OTP Server Authentication System, which contains most data for the system. Customers can choose their own database management system according to their specific needs.

1.6 The SDK Interfaces

In order to satisfy customization demands, SDK interfaces have been introduced, which include interfaces for the authentication server, management tools and an authentication agent in the most popular developing platforms.

Through the SDK interfaces, customers can realize nearly all functions of the OTP Server Authentication System V3.0 in individualized ways.

1.7 The Application System

Strictly speaking, the application system does not belong to the OTP Server Authentication System V3.0. Nevertheless, considering the fact that the main function of the OTP Server Authentication System is to provide authentication services for an application system, it is meaningless to run the OTP Server Authentication System without an application system. The application system is believed to be one part of the OTP Server Authentication

System so that it does not only make a complete system but also maintains close contact with reality.

1.8 The OTP Tokens

The OTP Server Authentication System V3.0 is backwards compatible with all the previous versions of the OTP Server Authentication System. Except for the new OTP c300 token, it supports OTP c100, OTP c200 and OTP c400 tokens.

Chapter 2. **Functions**

2.1 **Authentication Function**

The authentication function is one of the key functions of the OTP Server Authentication System V3.0, comprising both the authentication server and various OTP tokens.

1. OTP c100 Authentication

OTP c100 is an event-based dynamic password token designed by FEITIAN, providing a safe, simple and flexible OTP system for end-users. OTP Server Authentication System V3.0 maintains compatibility with OTP c100 in authenticating requests sent from OTP c100 tokens.

2. OTP c200 Authentication

OTP c200 is a time-based dynamic password token designed by FEITIAN, providing a safe, simple and flexible OTP system for end-users. OTP Server Authentication System V3.0 maintains compatibility with OTP c200 in authenticating requests sent from OTP c200 tokens.

3. OTP c300 Authentication（TOTP）

OTP c300 is a newly designed dynamic password token which is to be introduced together with OTP Server Authentication System V3.0. It can produce the same time-based dynamic passwords as OTP c200 tokens.

4. OTP c300 Authentication（CR-OTP）

Except for time-based dynamic passwords, OTP c300 can also produce challenge-response dynamic passwords, which is a distinctive feature from that of OTP c100 and OTP c200 tokens.

5. OTP c300 Authentication for Application Servers

OTP c300 token, together with OTP Server Authentication System V3.0, can help end-users to identify the real application server whilst helping the application server to authenticate an end-user.

6. OTP c300 Double-Way Authentication

OTP c300 token, together with OTP Server Authentication System V3.0, can easily form a double-way authentication between end-users and the application server (or the authentication server). It is very helpful for end-users to identify fake application servers so that security is maintained.

7. OTP c300 Signatures Authentication

OTP c300 token, together with OTP Server Authentication System V3.0, can digitally-sign critical transactions to provide another level of authentication for end-users. Digital signatures on transactions can effectively prevent crucial data being modified.

8. OTP c400 Authentication

OTP c400 is a dynamic-password- and-PKI-combined token designed by FEITIAN. OTP Server Authentication System V3.0 maintains compatibility with OTP c400 in authenticating requests sent from OTP c400 tokens and management on OTP c400 tokens etc.

2.2 Token Synchronization Function

Techniques based on time and event decides will sometimes lose synchronization with the authentication server. Thus, the synchronization function is necessary to keep them always synchronized.

1. OTP c100 Synchronization

OTP Server Authentication System V3.0 helps OTP c100 tokens to synchronize with the authentication server under the same steps as previous versions, i.e. to provide two continuous dynamic passwords generated by the token.

2. OTP c200 Synchronization

OTP Server Authentication System V3.0 helps OTP c200 tokens to synchronize with the authentication server under the same steps as previous versions, i.e. to provide two continuous dynamic passwords generated by the token.

3. OTP c300 Synchronization

OTP c300 token adds a time factor during the creation of time-based dynamic passwords or challenge-response dynamic passwords. When the time factor is big enough, synchronization with the authentication server will be needed. OTP Server Authentication System V3.0 supports synchronization of OTP c300 with the authentication server.

4. OTP c400 Synchronization

OTP Server Authentication System V3.0 helps OTP c400 tokens to synchronize with the authentication server under the same steps as previous versions, i.e. to provide two continuous dynamic passwords generated by the token.

2.3 Management Function

Management functions are mainly realized using the management tool of OTP Server Authentication System V3.0.

1. Settings of the System

Note: This specific management function is to be introduced into OTP Server Authentication System V3.0.

Setting the system is an important function of the management tool which includes settings of database, authentication methods and end-user source. The premise and basis of proper operations of the system is to correctly setup the system using the management tool.

2. Administrator Group

Management operations such as adding, checking, deleting as well as assigning rights to administrator groups can be performed through “administrator group”. The design of administrator group is to introduce role-based management of the system.

3. User Group

Management operations such as adding, checking, deleting user groups can be performed through “user group”, which is introduced to manage end-users through groups.

4. Administrator

Management operations such as adding, checking, deleting as well as using administrator groups to assign rights to administrators can be performed through “administrator”.

5. User

At “user”, the following management operations can be performed: adding an end-user, importing information of an end-user, assigning a PIN to an end-user, assigning a token to an end-user, checking end-users, deleting an end-user and grouping end-users etc.

6. Token

At “token”, the following management operations can be performed: importing tokens, token synchronization, token locked-up, token testing, deleting tokens, binding/unbinding tokens with end-users and unlocking tokens etc.

7. User-Token

At “user-token”, end-users can be bound with tokens, or later on, unbound or re-bound. Tokens can be tested and synchronized.

8. Authentication Server

Management operations such as adding or deleting authentication servers, as well as creating an authentication agent configuration file can be performed through “authentication server”.

9. Authentication Agent

At “authentication agent”, authentication agents can be added, checked and deleted. Authentication agent configuration files can be exported or edited.

10. User Log

User log is based on end-users. Operations on a particular end-user can be searched and shown in the management tool “user log” page.

11. Administrator Log

“Administrator log” shows operations performed by a particular administrator.

2.4 Application Server Integration

The main purpose of OTP Server Authentication System V3.0 is to provide authentication services for various application servers. That is why it is necessary to integrate the OTP Server Authentication System with application servers.

Normally, there are three integration methods: to use an existing RADIUS protocol of the application server, to install authentication agents on application servers or to use SDK interfaces to realize authentication functions. Please choose from the above three methods according to your own needs.

1. Integration with RADIUS

If the application system is already using RASIUS as an authentication protocol, the first method is the best choice. To integrate with RADIUS, it is not necessary to install any program on the application server, but to alter the settings of the RADIUS server. Normally, some of the most important settings include the IP address, communication port of the authentication server as well as shared key to communicate with the authentication server. The following are a few example application servers that support RADIUS authentication: Windows Server VPN service, WLAN service, Oracle database etc.

2. Integration through Agent

If the application server is a universal system which provides a third-party approved interface for secondary development, and the OTP authentication agent can recognize the authentication protocol of the application server, it is recommended to choose the second method. Installation of OTP authentication agents can save time and energy for developing your own authentication agent. Current popular applications servers that support OTP authentication agents include Windows login, IBM AIX system login, HP-UX system login, Linux system login, FreeBSD system login, Solaris system login, Apache website login, IIS website login, OWA2003 login, OWA2007 login and Citrix Present Server login etc.

3. Integration through SDK Interfaces

SDK interfaces integration is only recommended when the other two methods cannot be applied. However, SDK interfaces integration can bring the highest flexibility for the application server as functions that are not covered in the previous two methods can be realized, e.g. online banking system, online stock market, online gaming systems etc.

Chapter 3. Features

Features of OTP Server Authentication System V3.0 include features of the authentication server, the management tool, the authentication agent, as well as SDK interfaces and the system as a whole.

3.1 Features of the Authentication Server

The authentication server is the core of the whole system.

1. Automatic Synchronization

The authentication server has the added flexible feature to automatically synchronize a token during authentication if the token is found to be out-of-sync.

2. Multiple Token Supports

As for hardware tokens, OTP Server Authentication System V3.0 supports event-based OTP c100, time-based OTP c200, challenge-response OTP c300 and event-based-and-PKI-combined OTP c400 tokens.

OTP Server Authentication System V3.0 also supports mobile phone tokens based on event, time or challenge-response.

Again, OTP Server Authentication System V3.0 supports soft tokens based on event, time or challenge-response.

3. Multiple Authentication Methods

For systems that do not demand high security, it can be set to use a single dynamic password to authenticate an end-user. The advantage of this method is that it is not necessary to remember another fixed password, however security is quite low.

Dynamic passwords can be used together with fixed passwords to log into application servers that do not demand very high security. This method is commonly used to bring secure authentication of current application servers to the next level.

A challenge-response authentication method is normally used in application servers which demand high security and have end-users that are used to using technological products. The disadvantage of this method is that the authentication process involves many steps. However, it brings higher interactivity and security to the application server.

Application servers sometimes use double-way authentication methods against fake application servers. End-users, before proving their personal information, can verify the real application server.

For application servers which want to authenticate critical transactions, transaction signature authentication

methods can be used. This is to verify that those critical transactions are indeed made by the end-user who they claim to be.

4. RADIUS Server Support

According to pre-configured settings, the authentication server can send authentication requests to a designated RADIUS server and collect authentication results to send back to the application server

5. High Performance

The authentication server supports more than ten million concurrent end-users, and a single server can reach concurrent processing rate of 3000 per second.

6. Multiple Algorithms

HOTP algorithm from OATH;

TOTP algorithm from OATH;

OCRA algorithm from OATH;

SM3 algorithm from National Security Standard

7. Prevention of Dictionary Attack

When the authentication server finds that a particular end-user's authentication attempts have failed a certain number of times (can be pre-configured), it will lock that end-user. During locking, the authentication server will refuse authenticating this end-user until he/she has been unlocked. This is an effective prevention for dictionary attacks.

8. Prevention of Denial-of-Service Attack

The authentication server will delay sending a failed authentication result, which effectively prevents denial-of-service attacks.

3.2 The Management Tool

The management tool of OTP Server Authentication System V3.0 provides full management functions on authentications, administrators, end-users, tokens, authentication servers, authentication agents as well as logs.。

1. Remote Management

The web-interfaced management tool of OTP Server Authentication System V3.0 provides customers with an easy tool for locally or remotely managing the system.

2. Management Based on Group

Administrators and end-users can be grouped to facilitate management in the management tool of OTP

Server Authentication System V3.0. Basic functions such as adding, checking, editing and deleting etc. are supported for each group.

3. Role-based Management

OTP Server Authentication System V3.0 supports role-based management. The system administrator can assign different rights to different administrator groups so as to divide management roles.

4. Token Synchronization

OTP c100/200/300/400 tokens can be synchronized in the management tool: input token serial no or the user name which is bound to the token with two continuous dynamic passwords to synchronize.

5. Token Authentication Testing

Authentication on OTP c100/200/300/400 tokens can be tested in the management tool: input token serial no or the user name which is bound to the token with the dynamic password for authentication to test whether the token is working properly.

3.3 The Authentication Agent

OTP Server Authentication System V3.0 provides agents for Windows system login, IBM AIX system login, HP-UX system login, Linux system login, FreeBSD system login, Solaris system login, Apache website login, IIS website login, OWA2003 login, OWA2007 login and Citrix Present Server login etc. Additionally, Windows Server 2003 VPN service, WLAN service, Oracle database can also realize authentication with the authentication server of OTP Server Authentication System V3.0 through RADIUS protocol directly.

3.4 SDK Interfaces

SDK interfaces for the authentication server, the authentication agent and the management tool are provided in the following popular programming languages: C/C++, Java, ASP and PHP and platforms: IBM AIX, HP-UX, Windows, Linux, Solaris and FreeBSD.

3.5 System Features

System features are features of OTP Server Authentication System V3.0 as a whole.

1. Multiple Platforms Support

Platforms as many as IBM AIX, HP-UX, Windows, Linux, SUN Solaris and FreeBSD are all supported.

2. Multiple Database Support

Databases such as DB2, Oracle, SQL Server, Sybase, PostgreSQ and MySQL are supported.

3. Broad Range of Applicability

OTP Server Authentication System V3.0 can be applied to many areas such as finance, insurance, telecommunication, taxation, customs, office, education and entertainment etc.

Additionally, it can be used in many application systems such as telephone banking, telephone stock market, online banking and television shopping etc.

It can be used to provide secure authentication for both internal networks and the internet.

Chapter 4. Key Features Revisited

4.1 Platform Feature

As an authentication platform, OTP Server Authentication System V3.0 has the following features:

(1) Multiple operating system support
(2) Multiple database support with ODBC or other specific interface connection
(3) Full set developing interfaces in various programming languages
(4) Web-interfaced management tool for remote management
(5) Loading balance for multi-authentication services; up to thousands per second concurrent service rate; up to ten million concurrent end-user support
(6) Flexible settings for operation
(7) Supports multiple authentication services with different authentication settings on one computer
(8) Various authentication agents
(9) Central authentication for networks or computer operating systems

4.2 High Security

OTP Server Authentication System V3.0 largely enhanced the security of application servers as:

(1) Dynamic password is a random dynamic one-time password which cannot be re-produced. Thus using dynamic passwords can prevent threats like replay, peep or monitoring.
(2) Fixed password can be used together with dynamic passwords to form two-factor authentication.
(3) Security of OTP c300 token is improved by setting PIN for the token.
(4) Both the challenge code and time-factor from the authentication server have been added into challenge-response dynamic passwords, which largely enhanced the security of the dynamic passwords produced.
(5) Transaction signatures can effectively prevent hackers from modifying sensitive transaction information.
(6) End-users can choose to authenticate an application server, which effectively prevents sensitive personal data from leaking.
(7) Double-way authentication helps both the application server and the end-user against threats

4.3 Low Cost

OTP Server Authentication System V3.0 brings you an incredible low-cost solution：

(1) Self-owned intellectual property rights so no hidden cost
(2) Developed and produced nationally to lower transportation and customs cost and provide timely after-sales service
(3) Double-language GUI design (Chinese and English) with no extra cost
(4) Full configuration and management tool set provided
(5) Advanced pre-sales and after-sales services at reasonable price

4.4 **Ideal Choice**

OTP Server Authentication System V3.0, as a high-security, low-cost platform solution, providing the following benefits to customers:

(1) It is a customer's choice to choose which platform to hold their own application servers.
(2) It is a customer's choice to choose which database for their application servers.
(3) Both installation packages and full set of API interfaces are provided so it is up to the customer to implement their own customized authentication solution.
(4) OTP Server Authentication System V3.0 is equipped with powerful management tools to simplify maintenance work for customers.
(5) OTP Server Authentication System V3.0 brings next-generation security to customers.
(6) OTP Server Authentication System V3.0 can seamlessly integrate with many application servers so that no resources are wasted.

Chapter 5. **Specifications**

Number	Parameter Name	Parameter Value
1	**Concurrent End-user**	10,000,000
2	**Concurrent Processing Rate (Single Service)**	3000 times/second
3	**Authentication Response Time**	<5ms/Second
4	**Data Bandwidth**	<1M
5	**Data Recovery Tolerance**	Clustering Copy
6	**Authentication Method**	Double-way authentication
7	**Protocols**	Radius, LDAP, TCP/UDP, SOAP
8	**Authentication Service Stability**	Up to 1,000,000,000 continuous authentication
9	**Authentication Service accuracy**	Accuracy rate bigger than 99.9999999%
10	**Operating Systems**	IBM AIX, HP-UX, Windows, Linux, Unix
11	**Databases**	Oracle, DB2, Sybase, SQL Server, My SQL
12	**Dynamic password Length**	6-digit or 8-digit
13	**PIN Code**	yes
14	**Authentication Server API Interfaces**	C/C++, Java, Web Service etc.
15	**Authentication Agent API Interfaces**	C/C++, Java, ASP, ASP.NET, PHP etc.

Chapter 6. **Standards**

Supported standards

- ODBC connection for database
- AD/LDAP integration
- HOTP/TOTP/OCRA algorithms for authentication
- National Encryption Standard (SM3)
- Standard RADIUS protocol

Chapter 7. **Certifications**

Number	Certification Name	Issued by
1	**Computer Software Copyright Registration Certificate**	State Intellectual Property Office of P.R.C.
2	**Software Product Registration Certificate**	Science & Technology Committee Of Beijing
3	**Sale License Of Computer Information Security Product**	Department Of Public Security of P.R.C.
4	**Grading Certificate Of Military Information Security Product**	Information Security Testing & Certification Center Of CPLA
5	**FCC Certificate**	FCC Certification Authority
6	**CE Certificate**	CE Certification Authority
7	**OATH Qualification Certificate**	OATH Organization