Revision History:

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec. 2007</td>
<td>V1.0</td>
<td>1\textsuperscript{st} release of the document</td>
</tr>
<tr>
<td>Dec. 2008</td>
<td>V2.0</td>
<td>2\textsuperscript{nd} release of the document</td>
</tr>
<tr>
<td>Mar. 2010</td>
<td>V3.0</td>
<td>3\textsuperscript{rd} release of the document</td>
</tr>
</tbody>
</table>
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.
Contents

Chapter 1. Overview ................................................................. 1

Chapter 2. Architecture .......................................................... 2
  2.1 Environment Layer ......................................................... 2
  2.2 Device Layer ............................................................... 3
  2.3 Application Layer ........................................................ 3
  2.4 Authentication Agent Layer .......................................... 3
  2.5 Authentication Agent Interface Layer ............................. 3
  2.6 Authentication Service Layer ........................................ 3
  2.7 Authentication Service Interface Layer ........................... 4
  2.8 Kernel Layer ............................................................... 4
  2.9 OTP Management Center ............................................ 4

Chapter 3. System Components ............................................... 5
  3.1 Authentication Service/SDK .......................................... 5
  3.2 Database System ........................................................ 6
  3.3 OTP Management Center ............................................ 6
  3.4 Authentication Agent/SDK ........................................... 6
  3.5 Application System .................................................... 6
  3.6 Dynamic Token ........................................................... 6

Chapter 4. System Functions .................................................... 7
  4.1 Authentication ............................................................. 7
  4.2 Token Management ..................................................... 7
  4.3 User Management ........................................................ 7
  4.4 Authentication Service Management ............................. 7
  4.5 Authentication Agent Management ................................ 8
  4.6 Logging Management .................................................. 8
  4.7 PIN Protection ............................................................ 8
  4.8 Dynamic Password (Event Type) ................................... 8
  4.9 Dynamic Password (Time Type) ..................................... 8
  4.10 Dynamic Password (Challenge/Response Type) .............. 9
  4.11 Transaction Signature ................................................. 9
  4.12 Authentication Server ................................................ 9
  4.13 2-way Authentication ................................................ 9

Chapter 5. Features & Advantages ............................................. 10
  5.1 Environment Adaptability .............................................. 10
  5.2 Secure Authentication ................................................ 10
  5.3 Flexible Authentication ............................................... 10
  5.4 Highly Efficient Authentication ..................................... 11
  5.5 Comprehensive Management ....................................... 11
  5.6 Easy Integration ........................................................ 12

Appendix 1: Performance Factors ........................................... 13

Appendix 2: Product Qualification .......................................... 14

Appendix 3: Terms and Abbreviations .................................... 15
Chapter 1. Overview

Most application systems employ an authentication feature to control access. In early stages, the static password was used for authentication. But this kind of password is no longer very secure. It can be thieves with ease.

As a professional information security provider, Feitian Technologies has introduced OTP Server Dynamic Password Authentication System V3.0 for authentication utilizing dynamic passwords. The system consists of a software system and a hardware token. By integrating the authentication system with the application system, users of the application system can be authenticated with dynamic passwords, providing a higher level of security than simple and unsafe static passwords.
Chapter 2. Architecture

With high reliability, availability, and maintainability, the OTP Server Authentication System V3.0 provides an extension capability to existing security functionality and is very cost-effective. The system includes 4 layers: the system environment layer, the system interface layer, the authentication system layer, and the application system layer.

![Diagram of OTP Server Authentication System Architecture]

Figure 1 OTP Server Authentication System Architecture

2.1 Environment Layer

The environment layer mainly includes the operating system, the database system, and the infrastructure services.

1) OTP Server Authentication System V3.0 is a cross-platform system. It can run on Windows, HP-UX, IBM AIX, Linux, Solaris, and FreeBSD platforms.

2) OTP Server Authentication System V3.0 supports a lot of database systems, such as Oracle, DB2, SQL Server, Sybase, and MySQL.

3) OTP Server Authentication System V3.0 supports a set of services as the infrastructure platforms of the OTP Management Center. These services include Jboss, Apache, Tomcat, WebSphere, and WebLogic.

OTP Server Authentication System V3.0 can be used in different environments. In most cases, only minor changes
are required to the environment in which the authentication system is intended to be installed. Thus, the costs of installation and use of the authentication system are reduced.

2.2 Device Layer

The device layer includes the device for user authentication. The device can be the dynamic password tokens, such as OTP c100, c200, c300, c400 hardware tokens, software tokens, cell phone tokens, and SMS tokens.

2.3 Application Layer

The application layer includes the application system which is protected by the OTP Server authentication system. The application system can be of one of the following types in terms of the way in which the OTP Server authentication system is used and the features of the use: the authentication agent application, the authentication agent interface application, the RADIUS application, the authentication server interface application, and the kernel interface application.

2.4 Authentication Agent Layer

The authentication agent layer includes a set of authentication agents for different application systems. Generally, a kind of application system requires an authentication agent. Typically, the authentication agent can be Windows system logon, IBM AIX system logon, HP-UX system logon, Linux system logon, FreeBSD system logon, Solaris system logon, Apache site logon, IIS site logon, OWA 2003 logon, OWA 2007 logon, Citrix Present Server logon etc.

2.5 Authentication Agent Interface Layer

The authentication agent interface layer includes a set of interfaces for connecting the application system and the authentication server. These interfaces support different languages, such as C/C++, Java, PHP, ASP, ASP.NET, and C#. The application system implements authentication using dynamic password via these interfaces, as well as synchronization etc.

2.6 Authentication Service Layer

The authentication service layer includes a set of services for authentication, synchronization etc. These services include the extended RADIUS authentication service and the standard RADIUS authentication service.
2.7 Authentication Service Interface Layer

The authentication service interface layer includes a set of interfaces provided to users for authentication and synchronization etc. When using these interfaces, only the identification is needed to be passed. Other information will be automatically obtained from the database by the interface. The features of the authentication service can be integrated with the application system via these interfaces. The supported languages for the authentication service include C/C++ and Java etc.

2.8 Kernel Layer

The authentication kernel layer includes a set of interfaces provided to users for authentication and synchronization. The application system must pass various parameters when using these interfaces, because they will not obtain the information from the database automatically.

2.9 OTP Management Center

OTP Management Center acts as the coordinator of the authentication system. It runs on the basis of the database system and infrastructure services. The token device, the user, the authentication agent, and the authentication server can be maintained through the Management Center.
Chapter 3. System Components

The OTP Server authentication system provides comprehensive authentication services. The system includes the following components: the authentication service/SDK, the authentication agent/SDK, the database system, OTP Management Center, the application system, and the dynamic token.

![Diagram of System Components]

Figure 1 OTP Server Authentication System Components

3.1 Authentication Service/SDK

The authentication service/SDK provides the function of authenticating with dynamic passwords. It receives authentication requests from the authentication agent or from the application system and authenticates the user by obtaining necessary information from the database. After authentication, it returns a result to the authentication or the application system. Meanwhile, it keeps an authentication log each time an authentication is completed.

The authentication service can be a standard RADIUS authentication service or an extended RADIUS authentication service. Users should choose an appropriate service.

The authentication service SDK provides the functions of the authentication service as different interfaces to users. Users can integrate them with their application systems seamlessly.
3.2 Database System

The database plays an important role in the OTP Server authentication system. Generally, it is a component from a 3rd party. Therefore, a detailed description will not be provided herein.

3.3 OTP Management Center

The Management Center can be used for user management, token management, authentication server management, authentication agent management, and login management. It must be installed and configured properly to enable the whole authentication system to work normally.

3.4 Authentication Agent/SDK

The authentication agent/SDK is the intermediate point between the authentication system and the application system. It receives authentication requests from the application system and forwards them to the authentication server. After authentication, it receives a response from the authentication server and transmits it to the application system.

For the application system having a standard 3rd party authentication interface, the existing authentication agent can be used. For other application systems, the SDK can be used for integration.

3.5 Application System

The application system is the object which is protected by the OTP Server authentication system. The way in which the application system is integrated with the authentication system may vary depending on the features of the application system.

3.6 Dynamic Token

The dynamic token is used to generate a dynamic password each time it is used for authentication by the user. The dynamic token can be a hardware device, a software program, a cell phone token, or an SMS token.
Chapter 4. System Functions

The OTP Server authentication system provides the functions of authentication, token management, user management, authentication server management, authentication agent management, and login management. In addition, some new functions are introduced to Version 3.0 of the authentication system, such as PIN protection, the generation and verification of challenge/response dynamic passwords, the implementation and verification of transaction signatures, the authentication of the authentication server, and the 2-way authentication between the user and the system.

4.1 Authentication

The user can be authenticated by the OTP Server authentication system using necessary information, such as the PIN and dynamic password. For different security strengths, the combination of the account and the dynamic password, or the account, the PIN, and the dynamic password can be used for authentication.

4.2 Token Management

The OTP Server authentication system provides the functions relating to the token, including token import, token deletion, token synchronization, token binding, token registration for loss, registration for loss release, and PIN setting.

4.3 User Management

The OTP Server authentication system provides the functions relating to the user, including user addition, user deletion, user import, user binding to token, token synchronization, and user search.

4.4 Authentication Service Management

The authentication is conducted by the authentication service. There may be several authentication services in a real application system. If they can be configured and managed properly, the OTP Server authentication system can be made more efficient, and load-balancing and redundancy backup can be then further assisted.
4.5 Authentication Agent Management

If the application system does not support the standard RADIUS authentication protocol, the application system should use the authentication agent provided with the OTP Server authentication system with the authentication server for authentication. The configuration of the authentication agent must be added to the database for validation by the authentication server when verifying the validity of an authentication request. For the application system that supports the standard RADIUS authentication protocol, you should add an authentication agent to the database via the Management Center, though it is unnecessary to install the authentication agent in the application system. Otherwise, the authentication server will not serve authentication.

4.6 Logging Management

Both the authentication process and the maintenance process via the Management Center create logs. With the logs, you can view the running status of the system and the operations that have been performed, especially when an exception has occurred. To solve the problem, the logs can be helpful. Additionally, you can search for a log, delete a log, and export a log.

4.7 PIN Protection

The OTP Server authentication system offers full support for the OTP c300 token. Before generating a dynamic password, the OTP c300 token will validate the user by verifying their PIN. Only if the user passes the validation, can they then use the OTP c300 token normally.

4.8 Dynamic Password (Event-based)

The OTP Server authentication system supports generation and verification of event-type dynamic passwords with the OTP c100 token.

4.9 Dynamic Password (Time-based)

The OTP Server authentication system supports generation and verification of time-type dynamic passwords with OTP c200 and OTP c300 tokens.
4.10 Dynamic Password (Challenge/Response)

The OTP Server authentication system supports challenge/response authentication using dynamic password with the OTP c300 token. First, the authentication system generates a challenge code. Then, the OTP c300 token generates a dynamic password based on the challenge code to authenticate itself.

4.11 Transaction Signature

With the OTP c300 token, the OTP Server authentication system can generate a transaction signature and verify it. When conducting a transaction, the user enters the transaction information using the OTP c300 token to generate a signature of the transaction. After that, the transaction information and the signature are transmitted to the authentication server. The authentication server then verifies the correctness of the signature.

By singing the transaction, tampering with the transaction information by an attacker can be prevented effectively. In conjunction with the dynamic password for authentication, security strength can be substantially increased. In particular, transaction information is protected against man-in-the-middle attacks.

4.12 Authentication Server

The OTP Server authentication system also provides the function of authenticating the server in combination with the OTP c300 token. If the user is not sure of the application system they are logging into is correct, they can use the OTP c300 token to generate a challenge code for authenticating the server. Thus, the application system can be authenticated by comparing the response code it has returned with a response code generated by the token based on the challenge code.

4.13 2-way Authentication

To authenticate both the user and the application system, the OTP Server authentication system provides a 2-way authentication feature with the OTP c300 token.
Chapter 5. Features & Advantages

As a professional dynamic password authentication and transaction signature verification platform, the OTP Server authentication system provides features for different environments and application demands.

5.1 Environment Adaptability

1) Comprehensive support for operating systems, including IBM AIX, HP-UX, Windows, Linux, Solaris and FreeBSD;
2) Comprehensive support for database systems, including DB2, Oracle, SQL Server, Sybase, PostgreSQL, MySQL;
3) Can be integrated with any application systems using digital information for authentication.

5.2 Secure Authentication

1) Support for authentication with both dynamic password and PIN;
2) Support for automatic locking after a certain number of authentication failures is reached;
3) Support for timeout invalidity of dynamic password using a time factor;
4) Support for one-time dynamic password avoiding replay attacks;
5) Support for signature verification for a particular transaction preventing tamper to transaction information.

5.3 Flexible Authentication

1) Support for different forms of token, including OTP c100/200/300/400 tokens, cell phone token, and software token;
2) Support for different authentication modes, including time-type or event-type dynamic password authentication, authentication by time-type or event-type dynamic password plus PIN, challenge/response-type dynamic password authentication, authentication by challenge/response-type dynamic password plus PIN, transaction signature authentication, and authentication by transaction signature plus PIN.
3) Support for 2-way authentication, i.e. the application system and the user can authenticate mutually;
4) Support for different token algorithms, including HOTP, TOTP, and OCRA.

5.4 Highly Efficient Authentication

1) Support for authentication for up to 10 million users (or more);

2) Support for load-balancing by a set of authentication servers; support for at least 3000 concurrent requests per second;

3) Support for authentication server cluster.

5.5 Comprehensive Management

1) Support for remote management by providing the Management Center based on web pages;

2) Support for management by groups, e.g. users and authentication agents can be grouped;

3) Support for permission management;

4) Support for configuration management, including configuration of database connection parameters and administrator password;

5) Support for license management, e.g. the licensing information can be imported and viewed;

6) Support for reporting management, providing reports of statistics;

7) Support for logging management, including authentication server logs and management logs;

8) Support for authentication agent management, including addition, deletion, and modification;

9) Support for authentication server management, including addition and modification;

10) Support for token management, including token import, view and binding;

11) Support for user management, including addition and deletion;

12) Support for user group management, including addition and deletion;

13) Support for administrator management, including addition and deletion;

14) Support for authentication test using the dynamic password generated by the token;

15) Support for token synchronization to synchronize tokens in asynchronous status.
5.6 Easy Integration

1) The authentication system can be integrated with the application system via the authentication agent, including Windows system logon, IBM AIX system logon, HP-UX system logon, Linux system logon, FreeBSD system logon, Solaris system logon, Apache site logon, IIS site logon, OWA 2003 logon, OWA 2007 logon, and Citrix Present Server logon;

2) The authentication system can be integrated with the application system via RADIUS protocol, including Windows Server 2003 VPN logon, wireless network logon, and Oracle database logon;

3) The authentication system can be integrated with the application system via SDK interfaces, including the authentication server interface and the authentication agent interface.
## Appendix 1: Performance Factors

<table>
<thead>
<tr>
<th>No.</th>
<th>Technical Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Amount of users supported</td>
<td>More than 10 million</td>
</tr>
<tr>
<td>2</td>
<td>Throughput per authentication server</td>
<td>3000 times/s</td>
</tr>
<tr>
<td>3</td>
<td>Authentication response time</td>
<td>&lt;5ms</td>
</tr>
<tr>
<td>4</td>
<td>Bandwidth used for authentication</td>
<td>&lt;1M</td>
</tr>
<tr>
<td>5</td>
<td>Disaster prevention for authentication data</td>
<td>Backup via cluster</td>
</tr>
<tr>
<td>6</td>
<td>Out-of-band authentication</td>
<td>2-channel authentication</td>
</tr>
<tr>
<td>7</td>
<td>Supported protocols</td>
<td>RADIUS, LDAP, TCP/UDP, and SOAP</td>
</tr>
<tr>
<td>8</td>
<td>Supported operating systems</td>
<td>IBM AIX, HP-UX, Windows, Linux, and Unix</td>
</tr>
<tr>
<td>9</td>
<td>Supported database systems</td>
<td>Oracle, DB2, Sybase, SQL Server, MySQL, PostgreSQL, MSDE, and Access</td>
</tr>
<tr>
<td>10</td>
<td>Supported length of dynamic password</td>
<td>6 digits/8 digits</td>
</tr>
<tr>
<td>11</td>
<td>PIN authentication</td>
<td>Supported</td>
</tr>
<tr>
<td>12</td>
<td>Authentication service interface types</td>
<td>C/C++, Java, Web Service and more</td>
</tr>
<tr>
<td>13</td>
<td>Authentication agent interface types</td>
<td>C/C++, Java, ASP, ASP.NET, PHP and more</td>
</tr>
</tbody>
</table>
## Appendix 2: Product Qualification

<table>
<thead>
<tr>
<th>No.</th>
<th>Certification</th>
<th>Issuer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Computer Software Copyright Registration Certificate</td>
<td>National Copyright Administration of P.R.C.</td>
</tr>
<tr>
<td>2.</td>
<td>Software Product Registration Certificate</td>
<td>Science &amp; Technology Committee of Beijing</td>
</tr>
<tr>
<td>3.</td>
<td>Computer Information Security Product Sales License</td>
<td>Department Of Public Security of P.R.C.</td>
</tr>
<tr>
<td>5.</td>
<td>FCC certificate</td>
<td>FCC certification authority</td>
</tr>
<tr>
<td>6.</td>
<td>CE certificate</td>
<td>CE certification authority</td>
</tr>
<tr>
<td>7.</td>
<td>OATH qualification certificate</td>
<td>OATH organization</td>
</tr>
</tbody>
</table>
## Appendix 3: Terms and Abbreviations

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTP</td>
<td>Dynamic password or one-time password</td>
<td>It is generated using a dedicated hardware device or software program</td>
</tr>
<tr>
<td>HOTP</td>
<td>Event-based dynamic password</td>
<td>OTP c100/c400 tokens can generate HOTPs</td>
</tr>
<tr>
<td>TOTP</td>
<td>Time-based dynamic password</td>
<td>OTP c200/c300 tokens can generate TOTPs</td>
</tr>
<tr>
<td>CR-OTP</td>
<td>Challenge/response dynamic password</td>
<td>OTP c300 tokens can generate CR-OTPs</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service</td>
<td>An authentication protocol</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal identification number</td>
<td>It may be a soft PIN or a device PIN</td>
</tr>
</tbody>
</table>

### File Type

<table>
<thead>
<tr>
<th>File Type</th>
<th>Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>.tnk file</td>
<td>A file used to store token seeds</td>
<td>It must be imported into the OTP Server authentication system</td>
</tr>
<tr>
<td>.lic file</td>
<td>A file used to store license information</td>
<td>It is used when installing the OTP Server authentication system</td>
</tr>
<tr>
<td>.acf file</td>
<td>A file used to store configuration information of authentication agent</td>
<td>It is used when installing the OTP Server authentication system</td>
</tr>
</tbody>
</table>

### C100-related

<p>| Authentication | An event counter used for HOTP authentication by |</p>
<table>
<thead>
<tr>
<th><strong>base</strong></th>
<th>authentication server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication window</strong></td>
<td>The maximum number of retries that can be attempted in a row for authentication by authentication server. The default setting is the authentication base plus 40</td>
</tr>
<tr>
<td><strong>Synchronization window</strong></td>
<td>The maximum number of retries that can be attempted in a row for synchronization by authentication server. The default setting is the authentication base plus 200</td>
</tr>
<tr>
<td><strong>Synchronized status</strong></td>
<td>The status in which authentication is successful using the dynamic password generated by the token</td>
</tr>
<tr>
<td><strong>Asynchronous status</strong></td>
<td>The status in which authentication is unsuccessful using the dynamic password generated by the token but synchronization can be successful</td>
</tr>
<tr>
<td><strong>Ultra-asynchronous status</strong></td>
<td>The status in which synchronization cannot be successful using the dynamic password generated by the token</td>
</tr>
<tr>
<td><strong>Err 1</strong></td>
<td>It indicates that the token has no seed (failed to burn the seed into the token or the seed is lost after burning)</td>
</tr>
<tr>
<td><strong>Err 2</strong></td>
<td>It indicates timeout when pressing the button (over 15 seconds)</td>
</tr>
</tbody>
</table>

### C200-related

<p>| <strong>Authentication time</strong> | The time factor used by authentication server for verifying TOTP, i.e. the sum of current time and the time drift |
| <strong>Authentication window</strong> | The maximum time offset for successive authentication attempts by authentication server. By default, it is the authentication time plus/minus 1 minute |
| <strong>Synchronization window</strong> | The maximum time offset for successive synchronization attempts by authentication server. By default, it is the authentication time plus/minus 10 minutes |
| <strong>Synchronized status</strong> | The status in which authentication can be successful using the dynamic password generated by the token |
| <strong>Asynchronous status</strong> | The status in which authentication cannot be successful using the dynamic password generated by the token but synchronization can be successful |
| <strong>Ultra-asynchronous status</strong> | The status in which synchronization cannot be successful using the dynamic password generated by the token |</p>
<table>
<thead>
<tr>
<th><strong>C300-related</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PIN</strong></td>
<td>It is used by OTP c300 token for authenticating the user.</td>
</tr>
<tr>
<td><strong>Transaction signature</strong></td>
<td>A set of data generated by OTP c300 token using the transaction information provided by the user.</td>
</tr>
<tr>
<td><strong>Verify authentication server</strong></td>
<td>The OTP c300 token can be used to authenticate the authentication server.</td>
</tr>
<tr>
<td><strong>2-way authentication</strong></td>
<td>The OTP c300 token can be used to authenticate both the authentication server and the user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>OTP Server-related</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication server</strong></td>
<td>It receives authentication requests from the user and authenticates the user, and returns an authentication result to the user.</td>
</tr>
<tr>
<td><strong>Authentication agent</strong></td>
<td>It receives authentication requests from an application system and forwards them to authentication server, and then receives the authentication result from the server and transmits the result to the application system.</td>
</tr>
<tr>
<td><strong>Bind token</strong></td>
<td>Associate the token with the user.</td>
</tr>
<tr>
<td><strong>Token seed</strong></td>
<td>A secret key for generating the dynamic password in the token.</td>
</tr>
<tr>
<td><strong>Shared communication key</strong></td>
<td>It is used for encrypting and decrypting communication between authentication agent and authentication server.</td>
</tr>
<tr>
<td><strong>Token ID</strong></td>
<td>The serial number or bar code on the back of the token device.</td>
</tr>
</tbody>
</table>