FEITIAN

OTP Server Authentication System V3.0 Solutions

V3.0

2009-11

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

(1) 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.

(2) 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.

(3) 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.

(4) 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.

(5) 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.

(6) 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.

(7) 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.

(8) 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.

(9) 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

With the development of information technologies, many application servers or systems have been developed to satisfy needs coming from many fields. From online banks and online stock markets to small individual computers, security is always an issue: how to protect security of the application system by correctly identify the users of it.

In early stages, only fixed passwords were used, which has obvious shortcomings such as being hard-to-maintain, low security, low anti-attack ability etc. Dynamic password technology, to some extent, can improve security, convenience and anti-attack ability of a system. However, most systems only use dynamic passwords to simply replace fixed passwords to authenticate an end-user before they log in, which becomes a weak point in security as end-users do not authenticate an authentication system, neither do they sign an online transaction. In this case, hackers can easily adopt techniques such as phishing attacks and man-in-the-middle attacks to cheat end-users of personal sensitive information.

FEITIAN Technologies Co. Ltd, based on its 10-year experience in information security, has developed the OTP Server Authentication System with self-owned intellectual properties. OTP Server Authentication System V3.0 has raised authentication security to the next level by introducing unique authentication techniques of double-way authentication and transaction signing. The following document provides a detailed description on security solutions provided by OTP Server Authentication System V3.0.

Contents

Chapter 1. Fixed Password

Fixed password is password that will not change, i.e. once the password is set, it will always be effective unless it is set again.

Fixed passwords never change, which raise many security issues such as peeping, guessing, dictionary attacks, brute force attacks, monitoring, replaying and Trojan etc. End-users are found to lose critical personal information everyday because of simply losing fixed passwords. Another issue brought about by fixed passwords is password management. Each end-user may have dozens of fixed password to remember for different systems, so that some of them are always forgotten. End-users are always reluctant to change their fixed passwords, although it helps improve security. Moreover, once the password is changed it is still a fixed password, at least for some time. To conclude, fixed passwords have the following distinctive shortcomings:

1.1 High Risk/Low Security

It is easy to set a fixed password to log into a system. Many systems which do not have very high security requirements are still using them. However, fixed passwords have always put end-users and their personal information under high risks.

1.2 Hard to use

In this information age, passwords are used extensively. Many end-users can have up to 15 passwords for registered systems; however users constantly face the following dilemma:

(1) Use one password or a dozen different passwords?

(2) It is always hard to balance between hard and easy-to-remember fixed passwords.

(3) Constantly changing fixed passwords is necessary.

1.3 Low Anti-attack Ability

The threats brought about by fixed passwords are not limited to low security and hard management. Actually, fixed passwords are constantly under attack:

(1) It is easy to guess a short and simple password.

(2) If an end-user chooses to use one fixed password for all login sessions, it is easy but extremely dangerous.

(3) Fixed passwords are always found written on notebooks, notepads and other obvious places.

(4) Even for careful end-users, fixed-passwords can be stolen through peeping, monitoring, replaying, dictionary attack etc.

(5) It is hard to find out that a fixed password is already stolen.

Chapter 2. Dynamic Password

Dynamic passwords are changing passwords, which change randomly and can only be used once, i.e. authentication will fail when a dynamic password is used again. Dynamic passwords offer higher security and greater flexibility than fixed passwords.

2.1 Dynamic Password Theory

Dynamic passwords are also called one-time passwords or changing passwords. It is always changing because of the changing factor used. The changing factor of a dynamic password is actually made of two factors: one is the fixed seed key of the dynamic password token, which uniquely identifies the token and its user; the other is a changing factor, which causes the dynamic password to change. Based on different changing factors, different types of dynamic passwords can be generated, such as time-based dynamic passwords, event-based dynamic passwords and challenge-response passwords.

The authentication process based on dynamic passwords is like this: a dynamic password is generated by the token, and then sent to the authentication server which calculates another dynamic password based on the saved seed key of the token and the changing factor. The two dynamic passwords are compared to decide whether authentication is successful or not: if the two passwords are the same, authentication is successful; otherwise it fails.

A dynamic password has many advantages over a fixed password, such as its dynamic feature, randomness and unpredictability.

2.2 Dynamic Password Calculation

Calculation of a dynamic password, either inside the token itself or at the authentication server side, is basically the same:

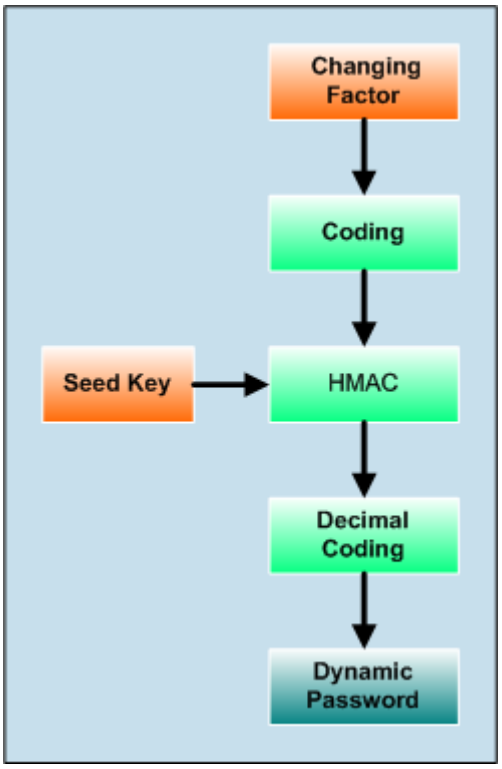

Figure 1 Calculation of a dynamic password

(1) The changing factor is vital in keeping dynamic passwords changing and different from each other: the changing factor of event-based dynamic passwords is event; the changing factor of time-based dynamic passwords is time; the changing factor of challenge-response dynamic passwords is challenge; there are cases where more than one changing factor above has been used as the changing factor of a dynamic password.

(2) The changing factor has to be coded according to a certain rule.

(3) Each token has a unique seed key, so that dynamic passwords generated by one token are always different from other tokens.

(4) A series of numbers is generated by encrypting the seed key and the coded changing factor.

(5) The series of numbers are decimal coded to make a dynamic password.

2.3 Simple Authentication

The following is a demonstration of a simple authentication process which is based on time/event types of dynamic password:

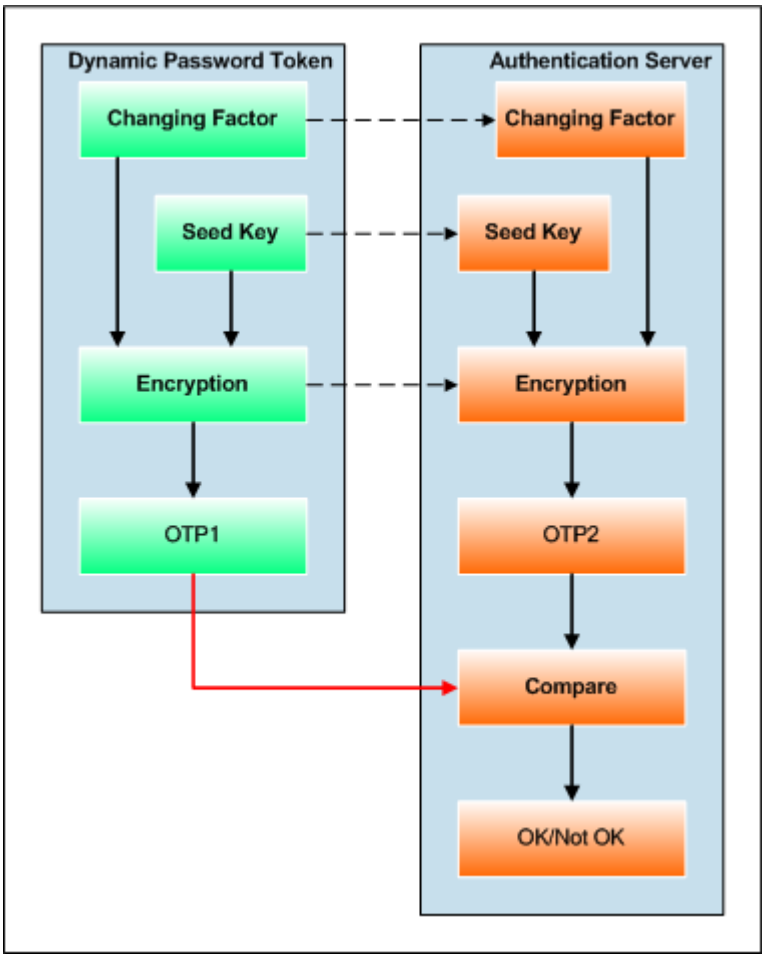

Figure 2 Simple authentication process based on time/event types of dynamic password

(1) The seed key of the token and the changing factor (time or event) is used to generate a dynamic password and sent to the authentication server.

(2) The authentication server uses the saved seed key of the token and the same changing factor (corrected time or event) to generate another dynamic password.

(3) The two dynamic passwords are compared at the side of the authentication server to authenticate the token: if they are same, authentication is successful; otherwise, authentication fails.

Note: the changing factor of the token might not be synchronized with the changing factor at the server side. Several dynamic passwords may need to be used in the authentication process. Authentication will only fail when all dynamic passwords pairs fail to match.

2.4 **Challenge-response Authentication**

The following is a demonstration on the authentication process based on challenge-response types of dynamic password:

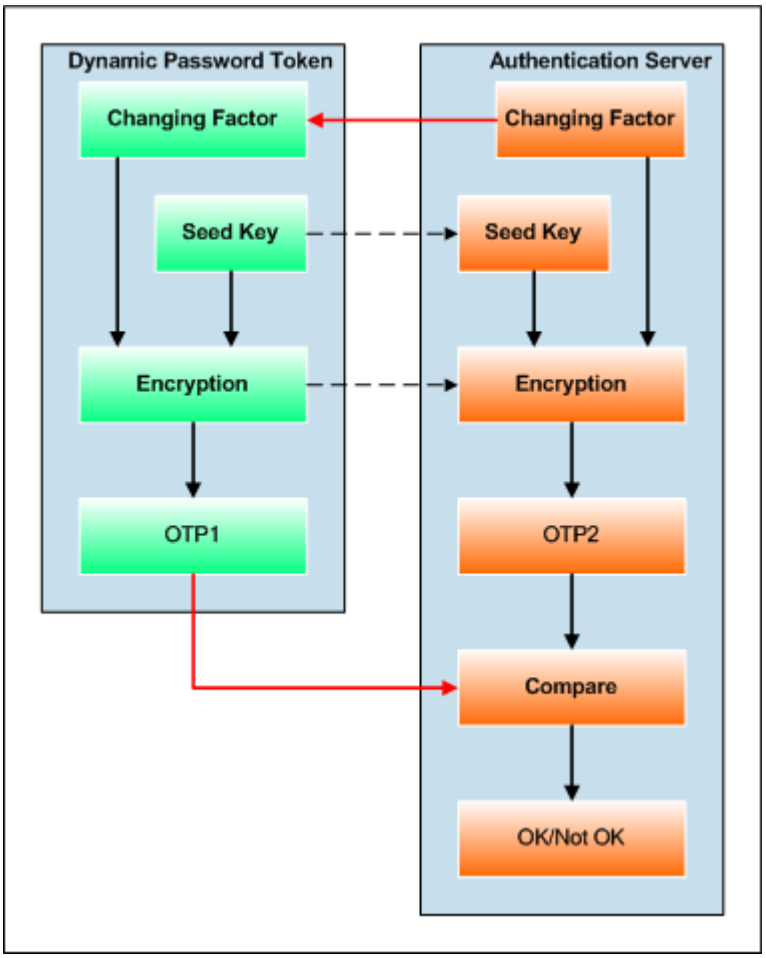

Figure 3 Authentication process based on challenge-response type of dynamic password

(1) A random number is generated at the authentication server and sent to the end-user.

(2) The random number is input into the token as the challenge code, which is used together with the seed key of the token and time component to generate a dynamic password.

(3) The dynamic password is sent to the authentication server.

(4) The authentication server generates another dynamic password based on the saved seed key of the token, the random number and the time component (the latter two forms the changing factor in this case).

(5) See whether the two dynamic passwords are the same: if yes, authentication is successful; otherwise, it fails.

Note: the changing factor of the token might not be synchronized with the changing factor at the server side. Several dynamic passwords may need to be used in the authentication process. Authentication will only fail when all dynamic password pairs fail to match.

2.5 Digital Signature & Verification

A digital signature is introduced to provide security for online transactions. Digital Signing can be used with the OTP c300 token to encrypt (or digitally sign) transaction data, which is sent to the authentication server to verify. Each signing is for one specific transaction and only critical information such as transaction amount, transaction number and time will be signed. So each signature is unique.

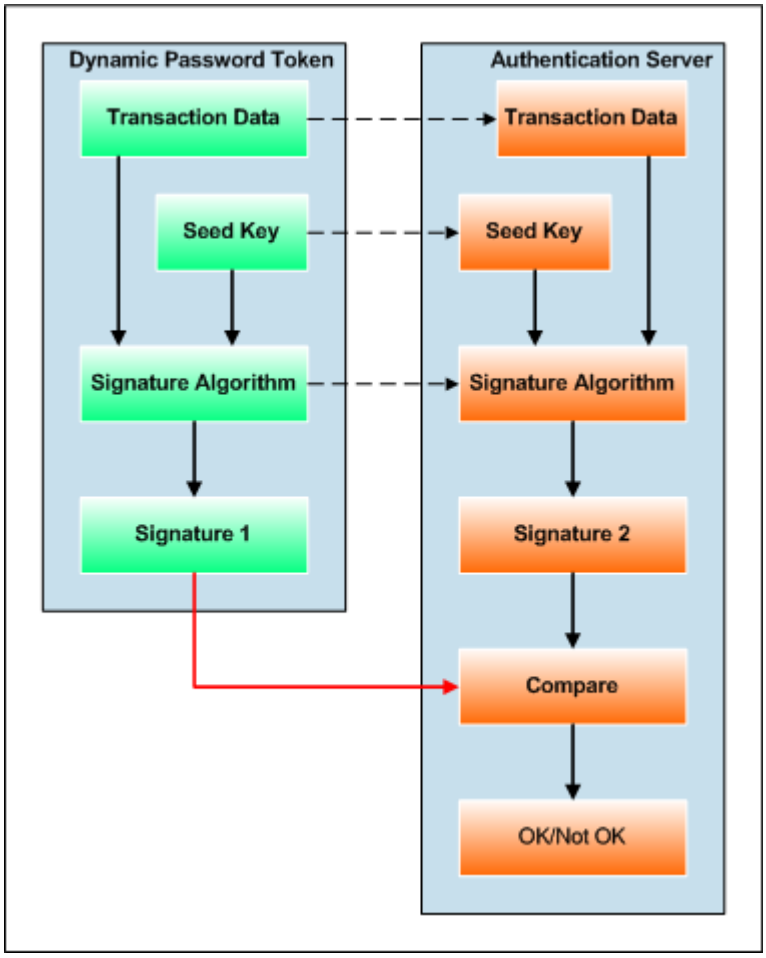

Figure 4 Processes of digital signing and verifying

(1) Token uses seed key and transaction and critical transaction data (such as transaction amount, transaction number and time etc.) to generate a new dynamic password and is send to the authentication server.

(2) The authentication server will also use the saved seed key and the same critical transaction data to generate another dynamic password.

(3) Two dynamic passwords are compared to produce the result of authentication: if they match, authentication is successful, otherwise it fails.

Note: the changing factor of the token might not be synchronized with the changing factor at the server side. Several dynamic passwords may need to be used in the authentication process. Authentication will only fail when all dynamic password pairs fail to match.

2.6 Server Authentication

The aim of server authentication is to prevent fake servers from cheating end-users of their sensitive personal data such as account, password etc. End-user is recommended to proceed with other operations after a successful server authentication.

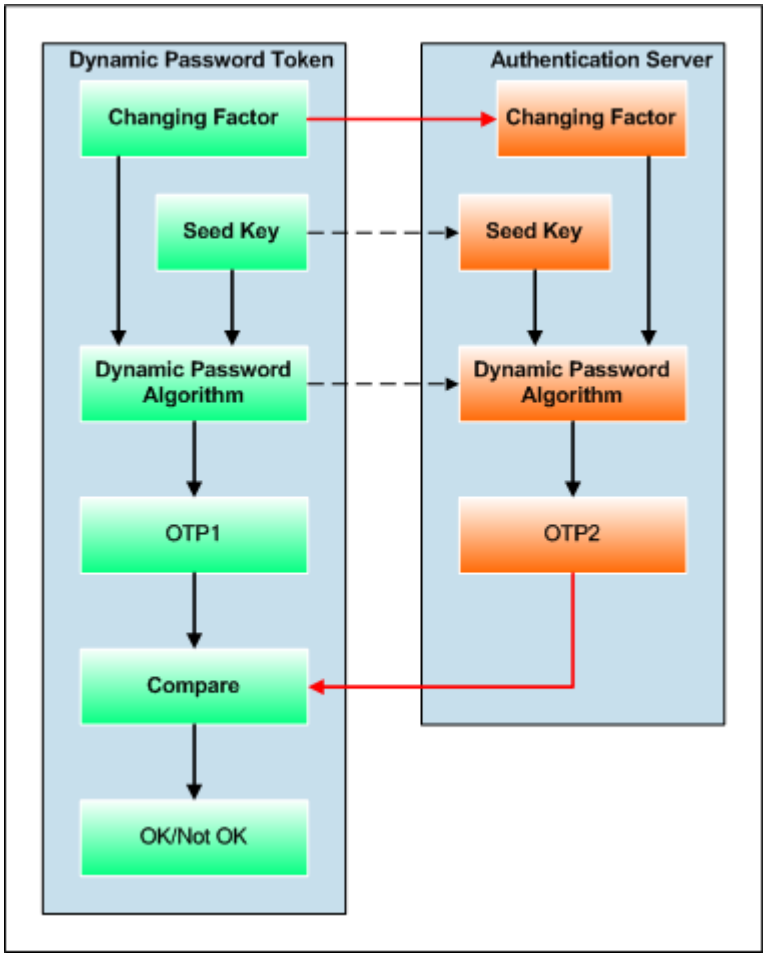

Figure 5 Process of server authentication by end-user

(1) A random number is generated by the token and sent to the authentication server.

(2) The random number will be used as the changing factor by the token, together with the seed key of the token to generate a dynamic password.

(3) The authentication server will use the received random number and the saved seed key of the token to generate another dynamic password and send it back to the end-user.

(4) Two passwords will be compared by the end-user: if they are the same, the server passes the authentication; otherwise it could be a fake server.

2.7 **Characteristics**

As a high-security and flexible authentication technology, dynamic-password authentication has the following main characteristics:

(1) Dynamic

Dynamic passwords change according the changing factor. No two dynamic passwords are the same.

(2) Randomness

Hash algorithm has been implemented in the process of dynamic password generation so that dynamic passwords are unpredictable and hard guess.

(3) One-Time feature (non-reusable feature)

The authentication server keeps a record of the used dynamic passwords so that one dynamic password cannot be authenticated twice.

(4) Anti-attack feature

A dynamic password is a random one-time password so peeping, replaying or dictionary attacks are useless.

(5) Flexibility

Normally, tokens used for generating dynamic password are small offline devices which are easy to carry and use.

Chapter 3. Basic Authentication Solutions

OTP Server Authentication System V3.0 can provide various application-server authentication solutions according to the environment and needs. This chapter focuses on solutions provided by OTP Server Authentication System V3.0 alone, which are called basic authentication solutions.

3.1 Standard RADIUS Solution

Standard RADIUS solution is an authentication solution provided by OTP Server Authentication System V3.0 based on standard RADIUS authentication protocol. No authentication agent needs to be installed. Only the application server needs to be setup to communicate with the authentication server, such as the IP address and communication port of the authentication server, and the shared key and the specific authentication methods used.

Note: Standard RADIUS service needs to be started on the authentication server to use this solution.

3.1.1 Environment

Network devices (most VPN, firewalls, routers or exchange servers), as well as some basic application servers such as a VPN server and Oracle database on Windows 2003 Server, support standard RADIUS protocol. Other application servers, no matter whether they are hardware-based or software-based or combined, can use this solution as far as they support standard RADIUS protocol.

3.1.2 Flowchart

Only settings of the application server need to be changed. E.g. for a VPN service, the authentication process of a standard RADIUS solution uses the following flows:

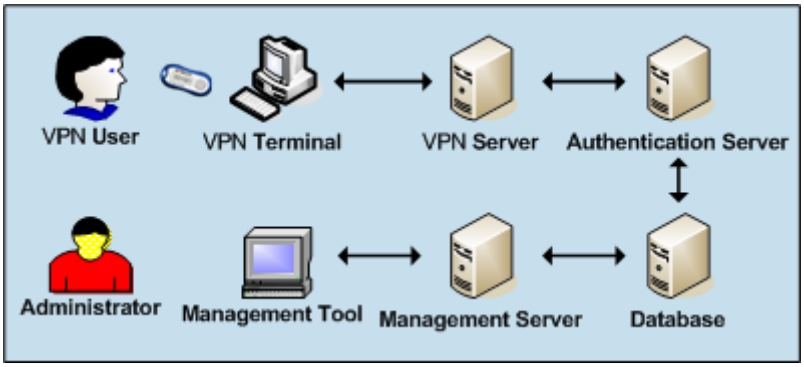

Figure 6 A standard RADIUS solution for a VPN service

When an end-user wants to login, the dynamic password generated by the dynamic password token will be sent to the authentication server through the VPN server based on standard RADIUS protocol. The authentication

server will then return the authentication result to the VPN server, which either grants the VPN terminal rights to log in or refuses a login request.

An administrator uses the management server to manage the authentication server where data for authentication is stored in the database.

Note: the authentication server, the management server and the database can be physically installed on the same machine or on different machines according to different deployment requirements.

3.1.3 Features

The standard RADIUS solution is easy to employ (simply setup communication with the authentication server on the application server) with no installation required for authentication agents.

3.2 Authentication Agent Application Solution

The authentication agent application solution is an authentication solution provided by OTP Server Authentication System V3.0 by using both the authentication agents and the authentication server. Where standard RADIUS protocol is not supported, application server can depend on the authentication agent to work as a bridge to communicate with the authentication server.

Note: extended RADIUS service needs to be started on the authentication server to use this solution.

3.2.1 Environment

Applications such as Windows system login, IIS web service, Apache web service, OWA service, Citrix Present Server as well as other non-Windows system login can use the authentication agent application solution. Authentication requests are sent from the application server to the authentication server through the authentication agent; authentication results are later sent back to the application server through the authentication agent again. As many authentication interfaces exists, different authentication agents are provided.

3.2.2 Flowchart

The following flowchart shows how to authenticate an IIS web service using extended RADIUS authentication service of OTP Server Authentication System V3.0.

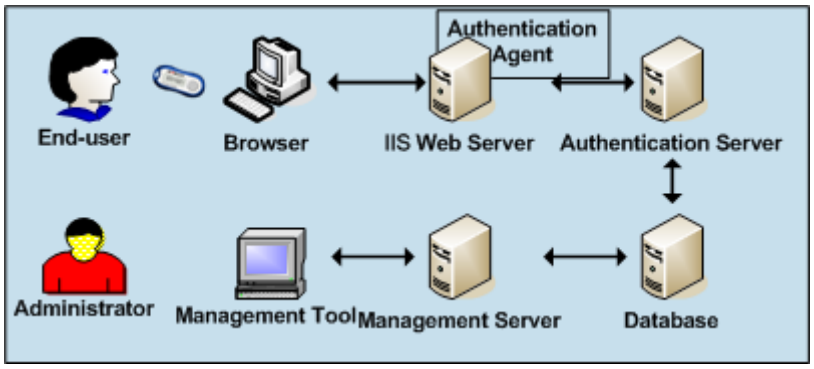

Figure 7 Extended RADIUS authentication service for IIS website

When an end-user logs into an IIS website, a dynamic password needs to be generated by the token and sent to the authentication server through the authentication agent at the IIS web server site. The authentication result will be returned to the authentication agent so that the IIS web server can decide whether to allow the end-user to log in.

An administrator uses the management server to manage the authentication server where data for authentication is stored in the database.

Note: the authentication server, the management server and the database can be physically installed on the same machine or on a different machine according to different deployment requirements.

3.2.3 Features

No development is required to use this solution. Authentication agents can be simply installed at the application server sites to work as a bridge between the application server and the authentication server.

3.3 Authentication Agent SDK Solution

In the case that there are special requirements on the authentication agent, the authentication agent SDK solution can be used. In order to use the authentication agent SDK solution, customers are required to have certain level of development ability and a deeper understanding on authentication processes and theory of the authentication agent relating to OTP Server Authentication System V3.0.

3.3.1 Environment

Self-developed application systems sometimes require flexible authentication solutions or do not have standard authentication interfaces. By using the API interfaces of OTP Server Authentication System V3.0, the authentication agent SDK solution can help customers to develop their application systems with fully-controllable authentication agent interfaces.

3.3.2 Flowchart

For example, an ERP system is protected using the agent SDK solution. The authentication flow is shown in the following figure.

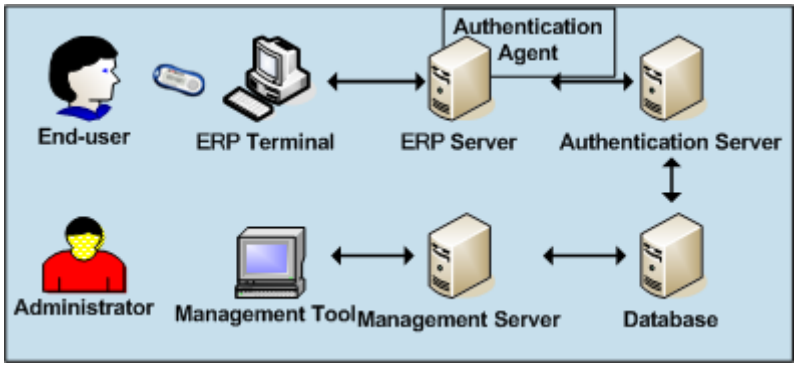

Figure 8 authentication agent SDK solution for an ERP system

When an end-user logs into the ERP system, a dynamic password needs to be generated by the token and sent to the authentication server through the developed authentication agent interfaces at the ERP site. The authentication result will be returned to the agent interface so that the ERP system can decide whether to allow the end-user to log in.

An administrator uses the management server to manage the authentication server where data for authentication is stored in the database.

Note: the authentication server, the management server and the database can be physically installed on the same machine or on a different machine according to different deployment requirements.

3.3.3 Features

An agent SDK solution provides customers the flexibility of choosing customized authentication plans with full functions of OTP Server Authentication System V3.0 for their application servers.

3.4 Authentication Server SDK Solution

When it is required to integrate the authentication server into the application server, the authentication server SDK solution can be used. In order to use the authentication server SDK solution, it is necessary that customers have a certain level of development ability and a deeper understanding on authentication processes and theory of the authentication server relating to OTP Server Authentication System V3.0.

3.4.1 Environment

Sometimes there is a need to develop an application server with simple authentication processes (application server performs full authentication processes without the existence of an authentication server or agent), then

the authentication server SDK can be used to seamlessly integrate full functionality of the authentication server into the application server.

Once integration is done, the current management tool provided in OTP Server Authentication System V3.0 can still be used to manage the database and basic settings through the authentication server interfaces. Additionally, a user-defined management tool can also be developed.

3.4.2 Flowchart

For example, an online banking system is protected using the server SDK solution. The authentication flow is shown in the following figure.

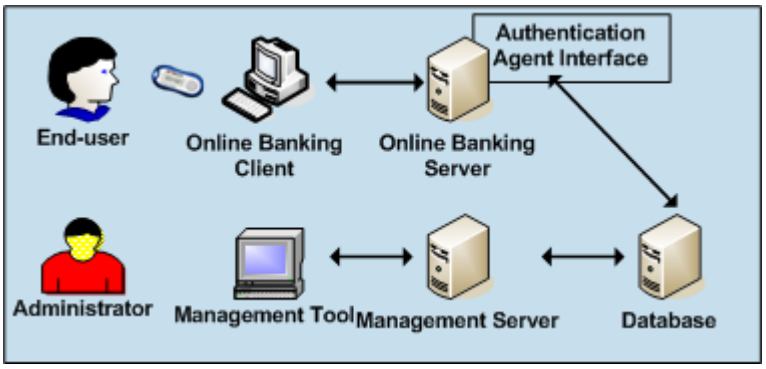

Figure 9 Authentication server SDK solution for an online banking system

When an end-user logs into the online banking system, a dynamic password needs to be generated by the token and sent to the application server through the developed authentication server interface for authentication. The application server then can decide whether to allow the end-user to log in.

An administrator uses the management server provided, to manage the authentication server where data for authentication is stored in the database. However, the user-developed management tool can also be used.

3.4.3 Features

The authentication server SDK solution provides customers with the flexibility of choosing customized authentication plans with the same full functionality of OTP Server Authentication System V3.0 for their application servers.

3.5 Authentication SDK solution

The authentication SDK solution is provided to those who wish not to install the authentication server and the authentication agent provided, but to integrate authentication functions with self-developed management functions.

This solution can bring greater level of flexibility to application servers.

3.5.1 Environment

In most extreme cases, customers may wish the flexibly of integrating authentication functions into the application server without the installation of the authentication server and the authentication agent, whilst implementing their own management tools to manage users, tokens and authentication data. The authentication SDK solution can be used in those cases to seamlessly integrate authentication functions provided by OTP Server Authentication System V3.0 into customized application servers.

3.5.2 Flowchart

The following figure shows a sample authentication flow of the authentication SDK solution used on an online stock market system.

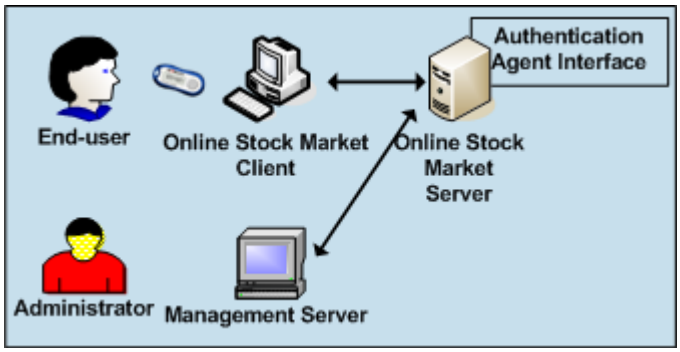

Figure 10 The authentication SDK solution on an online stock market system

When an end-user logs into the online stock market system, a dynamic password needs to be generated by the token and sent to the application server through the self-developed authentication interfaces for authentication. The application server then can decide whether to allow the end-user to log in.

An administrator uses the self-developed management functions to manage authentication data. User, token and authentication data can be stored in s user-defined area of the server.

3.5.3 Features

The authentication SDK solution brings maximum flexibility as well as seamless integration to the application server. However, development work is needed.

Chapter 4. Advanced Authentication Solutions

Advanced authentication solutions are solutions provided by OTP Server Authentication System V3.0 based on OTP c300 tokens, which provides greater security within the authentication process.

4.1 Challenge-response Authentication Solution

Challenge-response authentication is one of the unique features of the OTP c300 token. The challenge-response authentication solution of OTP Server Authentication System V3.0 is based on OTP c300 tokens.

4.1.1 Environment

The OTP c300 Token has many distinctive security features, one of which is to generate challenge-response dynamic passwords. The changing factor of the challenge-response dynamic password generated by the OTP c300 token is comprised of both the challenge seed and a time factor, which largely enhances authentication security. Application servers that have demand for greater authentication security can certainly adopt the challenge-response authentication solution.

4.1.2 Flowchart

A sample flowchart of the challenge-response authentication solution is given below.

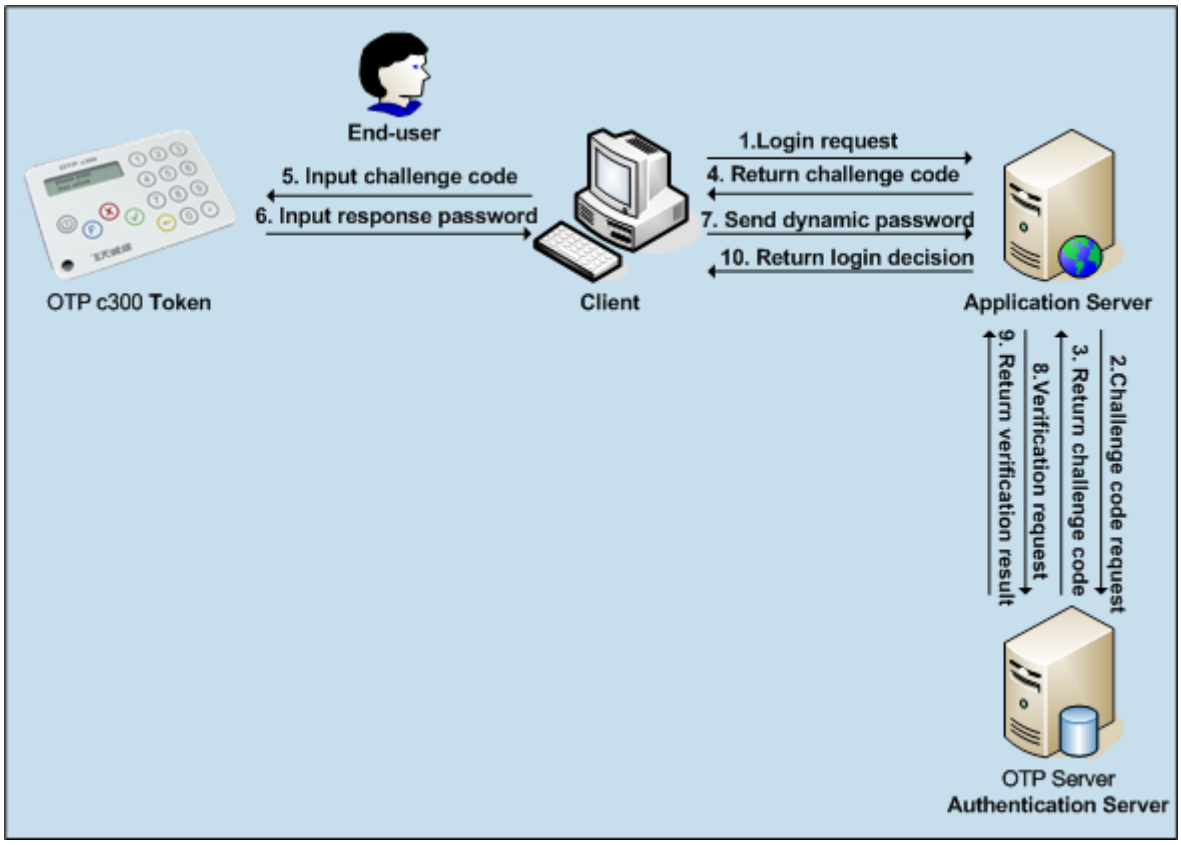

Figure 11 The challenge-response authentication solution

In the above flowchart, challenge code and response code can also be transmitted through other communication channels such as SMS to improve greater security.

4.1.3 Features

Challenge-response dynamic password authentication is a more advanced authentication process than the simple time/event dynamic password authentication. Additionally, generation of the challenge-response dynamic passwords are further protected from unidentified users as a pre-defined PIN is required to be input into the OTP c300 token before a password can be generated.

4.2 Transaction Signature Authentication Solution

Another main feature of the OTP c300 token is digitally signing transactions. Before a transaction is done, critical information is sent to the end-user to confirm who uses the OTP c300 token to digitally sign it in order to authenticate the transaction and their own identity. Only transactions with the correct signature that can be proved to be authorized and unaltered will be processed by the application server.

The advantages brought by digital signatures on transactions include preventing critical transaction information from deliberate modification and ensuring identity verification.

4.2.1 Environment

There are application servers which have requirements for large quantities of online transactions, containing highly sensitive data such as online banking or online stock market information. The transaction signature authentication solution is an ideal solution for these application servers.

4.2.2 Flowchart

From the flowchart below, it is obvious that each critical transaction is protected as the transaction signature requires the identity of the end-user to be verified again by using signatures after the initial login authentication process.

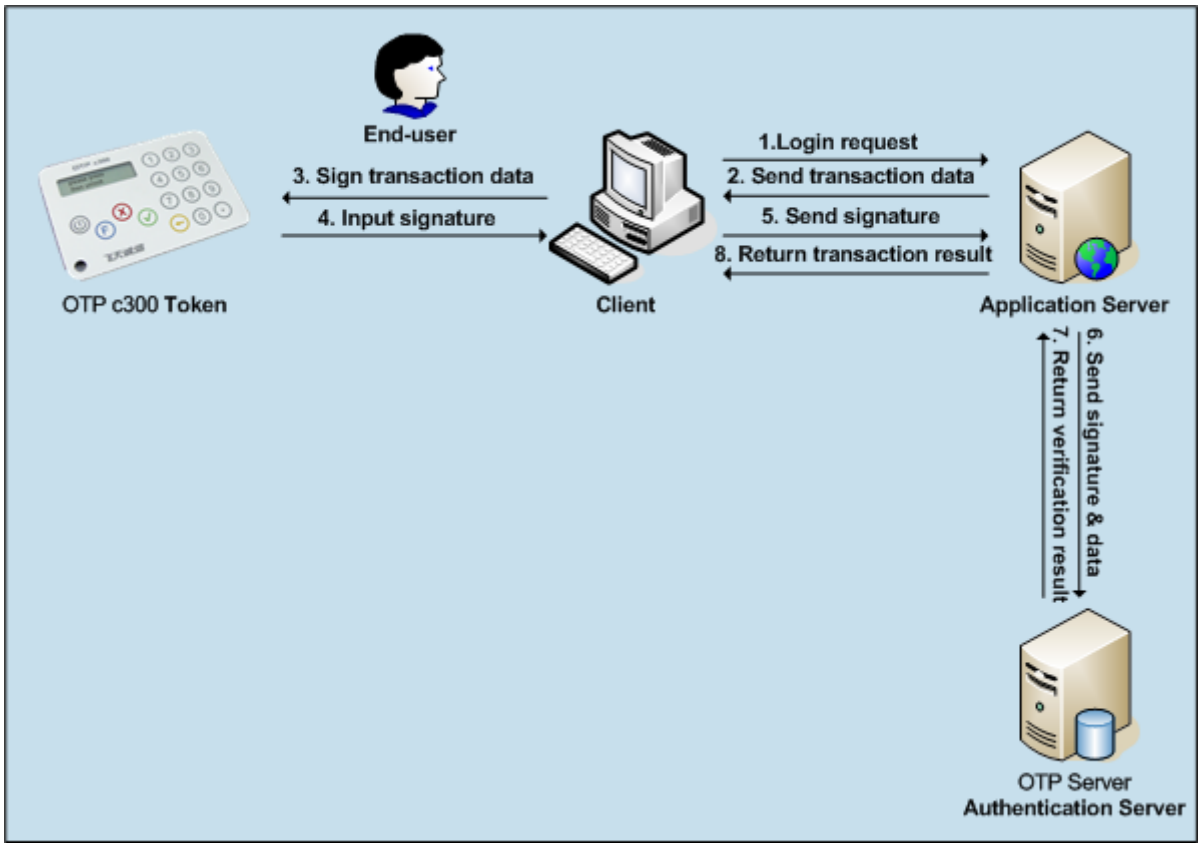

Figure 12 The transaction signature solution

In the above flowchart, it is also easy to introduce challenge-response authentication into the server authentication process in order to bring even greater security levels from the end-user perspective.

4.2.3 Features

Transaction signatures have advantages in transaction protection and end-user identity re-verification. However, application server authentication should also be considered so as to protect end-users from fake servers.

4.3 Double-way Authentication Solution

The OTP c300 token can be used to easily realize double-way authentication: end-user to application server and application server to end-user. Although attacks are mainly aimed at application servers, there are cases that fake application servers are built up to cheat end-users of their personal sensitive data. The ideal solution is to implement double-way authentication during the login process of an application server.

OTP Server Authentication System V3.0, based on the OTP c300 token, provides application servers with a double-way authentication solution to protect both the system and its end-users from online threats. The basic authentication procedure in the double-way authentication solution is that firstly, end-users check the genuineness of an application server before login, and then the identity of the end-user will be verified by the application server. Basic authentication methods (using time/event based dynamic password) or the advanced authentication method (using challenge-response dynamic password) can be used.

4.3.1 Environment

Application servers with large quantities of online transactions on the one hand demand maximum security, in the other hand, have to provide the most secure environment for its end-users. Application servers, which have a broad range of online services, can adopt the double-way authentication solution according to their needs.

4.3.2 Flowchart

The basic authentication procedure of the double-way authentication solution is demonstrated in the flowchart below.

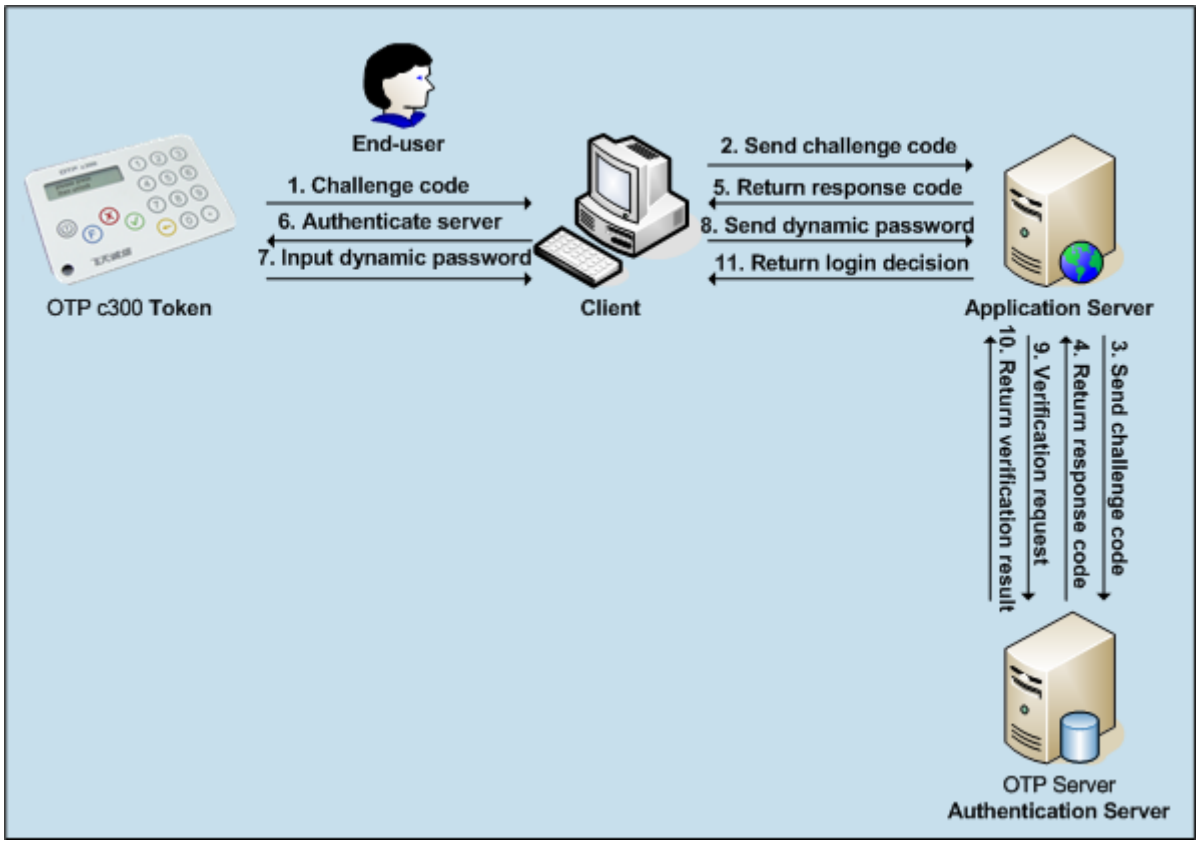

Figure 13 The double-way authentication solution

In the above flowchart, the advanced authentication method (using challenge-response dynamic password) has been adopted. However, it can be easily changed into the basic authentication method (using time/event based dynamic password) without difficulty.

4.3.3. Features

The double-way authentication solution has mainly improved security from the perspective of the end-user. Combined with transaction signature techniques, it can provide a next-level of security in a wider perspective.

Chapter 5. Integrated Authentication Solutions

The integrated authentication solution is a solution that integrates other dynamic password authentication systems (including both hardware and software) into OTP Server Authentication System V3.0 to provide one combined authentication solution. Based on integration approaches, there are three solutions available: the application (server or agent) integration solution, the SDK integration solution, and the relay integration solution.

5.1 Application Integration Solution

To use the application integration solution, dynamic password authentication systems that are integrated need to be based on one open standard such as OATH. Then different dynamic passwords received by the application server or the authentication can be forwarded to corresponding authentication servers to authenticate. There is no interaction between different authentication servers so complexity of design is largely reduced.

5.1.1 Environment

Application servers with an existing dynamic password authentication solution may want to introduce more advanced dynamic password authentication functions or integrate other types of tokens from other dynamic password authentication solutions. As far as these dynamic password authentication solutions are based on the same authentication interface standard, there is no need for development.

OTP Server Authentication System V3.0 is based on OATH.

5.1.2 Flowchart

The authentication flow of the application integration solution is demonstrated in the following figure.

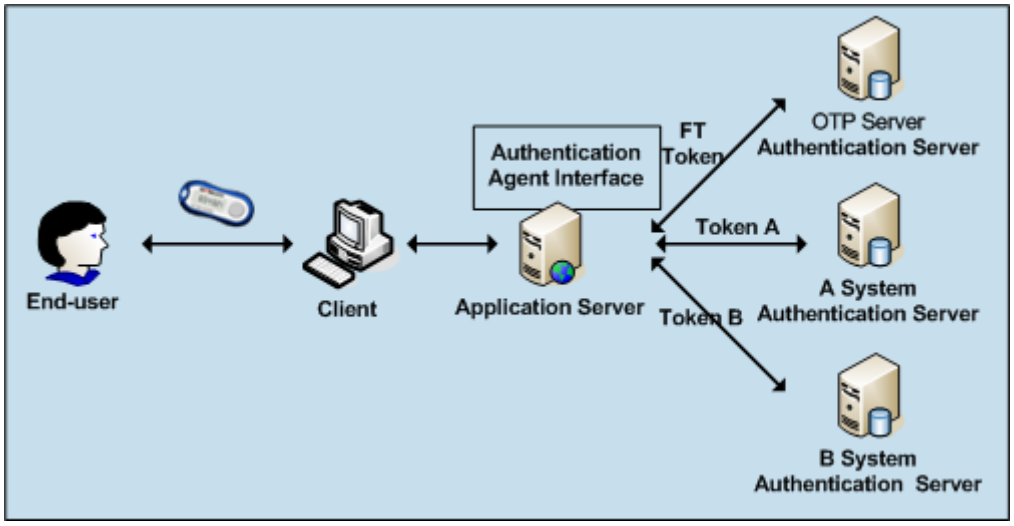

Figure 14 The application integration solution

From the above flowchart, it is obvious that the application server with the integrated agent interface decides which authentication server is used to authenticate a particular dynamic password.

5.1.3 Features

The application integration solution can easily integrate two or more authentication system solutions without any modification on either side. Authentication burden of the application server can be very heavy.

5.2 SDK Integration Solution

The SDK integration solution is to integrate the authentication agent interface into the authentication server of the OTP Server Authentication System so that dynamic passwords generated by tokens of the other system can also be authenticated by the authentication server.

5.2.1 Environment

In the SDK integration solution, it is critical that the authentication agent interfaces are provided by the other dynamic password authentication systems. Application servers, which wish to use one authentication server to authenticate tokens of many manufactures, may consider using the SDK integration solution if the authentication agent interfaces are available.

5.2.2. Flowchart

The authentication flow of the SDK integration solution is demonstrated in the following figure.

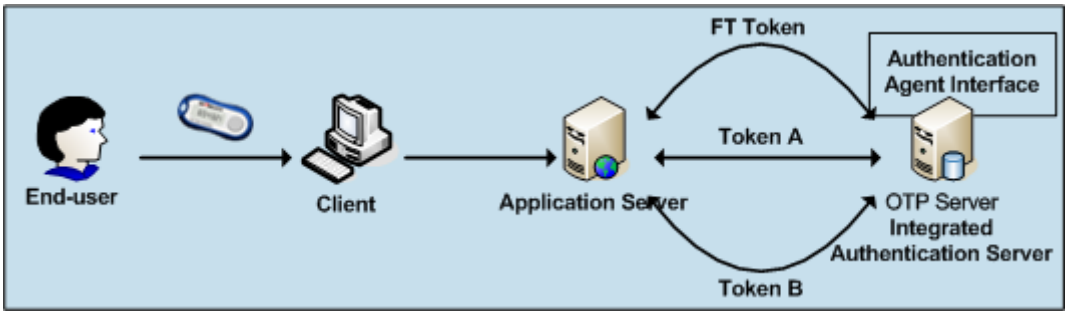

Figure 15 The SDK Integration Solution

Compared to the application integration solution, the authentication burden on the application server is removed.

5.2.2 Features

If agent interfaces are available, the SDK integration solution is an ideal solution for authenticating tokens from more than one manufacturer. A small amount of development work is necessary.

5.3 Relay Integration Solution

In reality, the authentication agent interfaces of dynamic password authentication systems are not always available for development. In such cases, dynamic passwords of tokens from other manufacturers can still be authenticated by the authentication server of the OTP Server Authentication System through relaying the authentication requests to the other authentication servers of other systems

5.3.1 Environment

The relay integration solution is a highly flexible solution for application servers which want to integrate tokens or authentication functions from many dynamic password authentication systems. If the authentication server of the system supports the RADIUS protocol, the authentication request can be relayed by the authentication server of the OTP Server Authentication System directly. Otherwise, the authentication agent interface provided by the system can be used to relay the authentication request.

5.3.2 Flowchart

The authentication flow of the relay integration solution is demonstrated in the following figure.

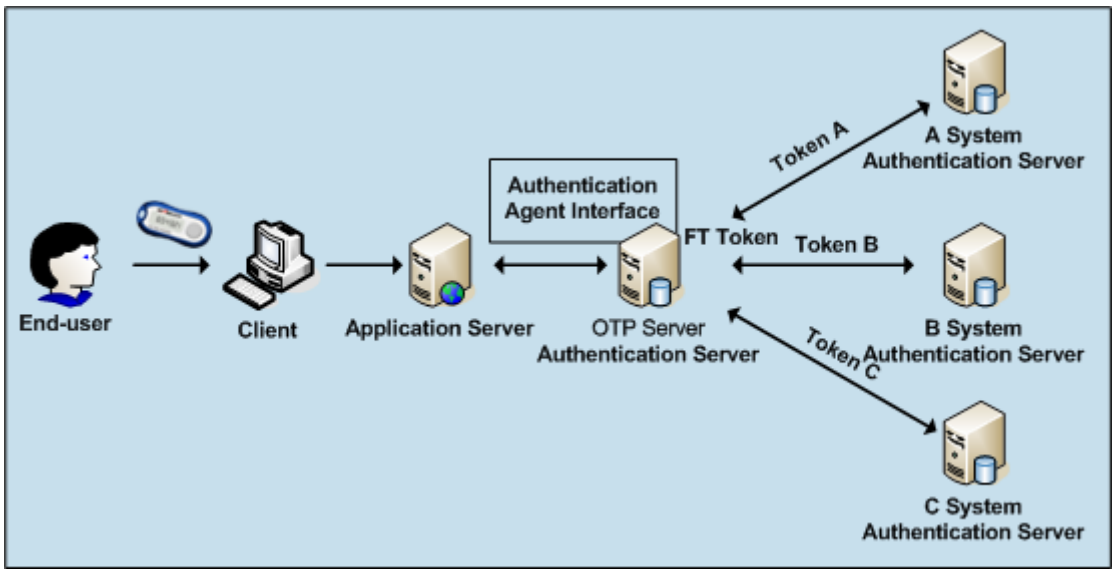

Figure 16 The relay integration solution

It is obvious that burden on the application server is reduced to the smallest while there is no need for open authentication interfaces.

5.3.3 Features

The authentication server of the OTP Server Authentication System will authenticate FEITIAN OTP tokens, whilst authentication request from other tokens will be relayed to the corresponding authentication servers to process. No modification on the other authentication system is necessary.

Chapter 6. Solution Features

Authentication solutions provided by OTP Server Authentication System V3.0 have the following common features:

(1) High Security

In addition to normal security features provided by dynamic passwords such as anti-attacking ability, authentication solutions provided by OTP Server Authentication System V3.0 have introduced other advanced security features such as challenge-response dynamic passwords, double-way authentication and transaction signatures.

(2) Flexibility

Authentication solutions provide by OTP Server Authentication System V3.0 use dynamic password tokens which provide greater flexibility for end-users.

(3) Easy-to-use

End-users can simply press the button of the dynamic password token to generate a dynamic password for login, no software installed, no connection needed.

(4) Economy

Dynamic password authentication solutions are very economical as dynamic password tokens are manufactured and distributed in batches with no hidden management costs.

(5) Wide Applicability

Dynamic password authentication solutions are not limited to be applied to application servers on LAN, WLAN, internet or TV channel..

Chapter 7. **Solution Benefits**

Authentication solutions provided by OTP Server Authentication System V3.0 can bring the following common benefits for a business:

(1) Enhanced security

Security of the application server is largely enhanced by adopting authentication solutions provide by OTP Server Authentication System V3.0 with advanced authentication techniques.

(2) Improved efficiency

Authentication solutions provided by OTP Server Authentication System V3.0 are equipped with advanced management tools to improve management efficiency.

(3) Lower cost

By adopting the authentication solutions of OTP Server Authentication System V3.0, attack-related cost can be largely reduced, as well as management cost.

(4) Higher achievement

By adopting the authentication solutions of OTP Server Authentication System V3.0, businesses can achieve a higher level of authentication, which in turn provides end-users with secure access to application servers almost anywhere at any time.

(5) Lower risk

Authentication solutions of OTP Server Authentication System V3.0 can adopt advanced security techniques such as double-way authentication and transaction signing to lower attack risks of the application server.

(6) Increased competitiveness

Business can increase their competitiveness by adopting the most advanced authentication solution - provided by OTP Server Authentication System V3.0.