FEITIAN

OTP Server Authentication System Authentication Schemes

V1.0

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

As more and more businesses are getting online, Information security is becoming more and more important and authentication security is one of the most important security tasks. Fixed password, as a common way to authenticate an end-user, has obvious shortcomings such as 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 he/she logs in, which becomes a weak point in security as system authentication is not provided to the end-user, and online transactions are not signed. In this case, hackers can easily adopt techniques such as phishing attack and man-in-the-middle attack s to cheat end-users of personal sensitive information.

This document is intended to provide detailed descriptions on the high security authentication schemes that are provided by the OTP Server Authentication System, which adopts the technologies of double-way authentication and transaction signing. The schemes provided by OTP Server Authentication Systems do not only help the application system to authenticate end-users, but also help end-users to authenticate the system, meanwhile supporting digitally signing critical transactions between the two. Thus, end-users are protected from logging into fake systems, receiving man-in-the-middle attacks and losing sensitive data. By adopting the schemes provided by the OTP Server Authentication System, businesses are able to employ higher security systems.

Contents

Chapter 1. Basic Double-way Authentication

1.1 Theory

Double-way Authentication combines two one-way authentications, i.e. firstly, an end-user authenticates an application system, and then the system authenticates the end-user. Identities of both the application system and the end-user are protected through the two one-way authentications. The application system can use two main methods to authenticate an end-user: challenge-response method and time synchronization method.

1.1.1 Authentication by End-users

The reason for an end-user to authenticate an application system before login is to prevent end-users from passing-on important personal data (such as account name, password and dynamic password etc.) by logging into fake systems that attempt to intercept such information. Only when an application system has been successfully authenticated, shall an end-user proceed with authorized operations.

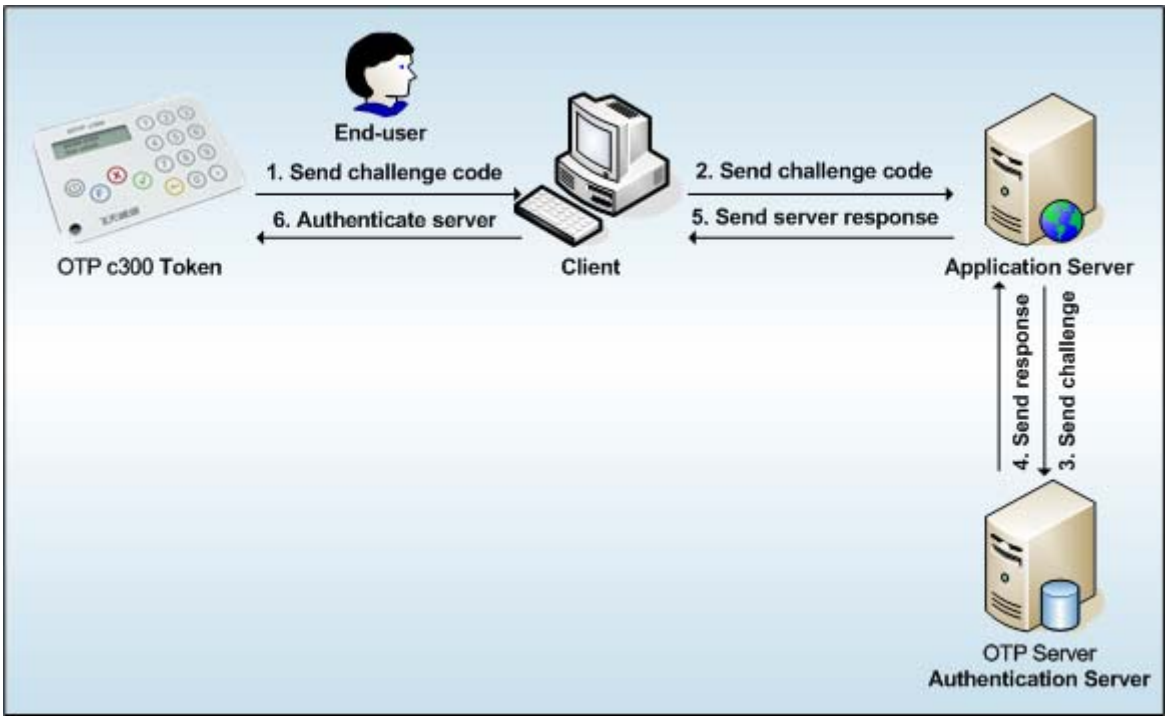

Figure 1 the process of system authentication by end-users

During the authentication process, both the dynamic password token and the authentication server work together: the dynamic password token produces a challenge code and verification code, whilst the authentication server generates a response code, which is transferred back to the end-user through the application server. The end-user compares the response code from the server with the verification code of the token to authenticate the

application system: if they are the same, it is the genuine application system; otherwise it is deemed a fake application system. In the latter case, the end-user should stop the login operation immediately. The following are the steps of the authentication process:

(1) The dynamic password token generates a challenge code, or a dynamic factor to send to the authentication system.

(2) The token uses the challenge code to generate a verification code.

(3) The authentication system uses the challenge code and seed key of the token saved to generate a response code which is sent back to the end-user through the application system.

(4) The end-user compares the verification code with the response code to authenticate the system.

1.1.2 Authentication by application system (Challenge-Response)

A challenge-response dynamic password authentication is successful when the response code generated by the token is the same as the verification code generated by the authentication server, otherwise the authentication fails.

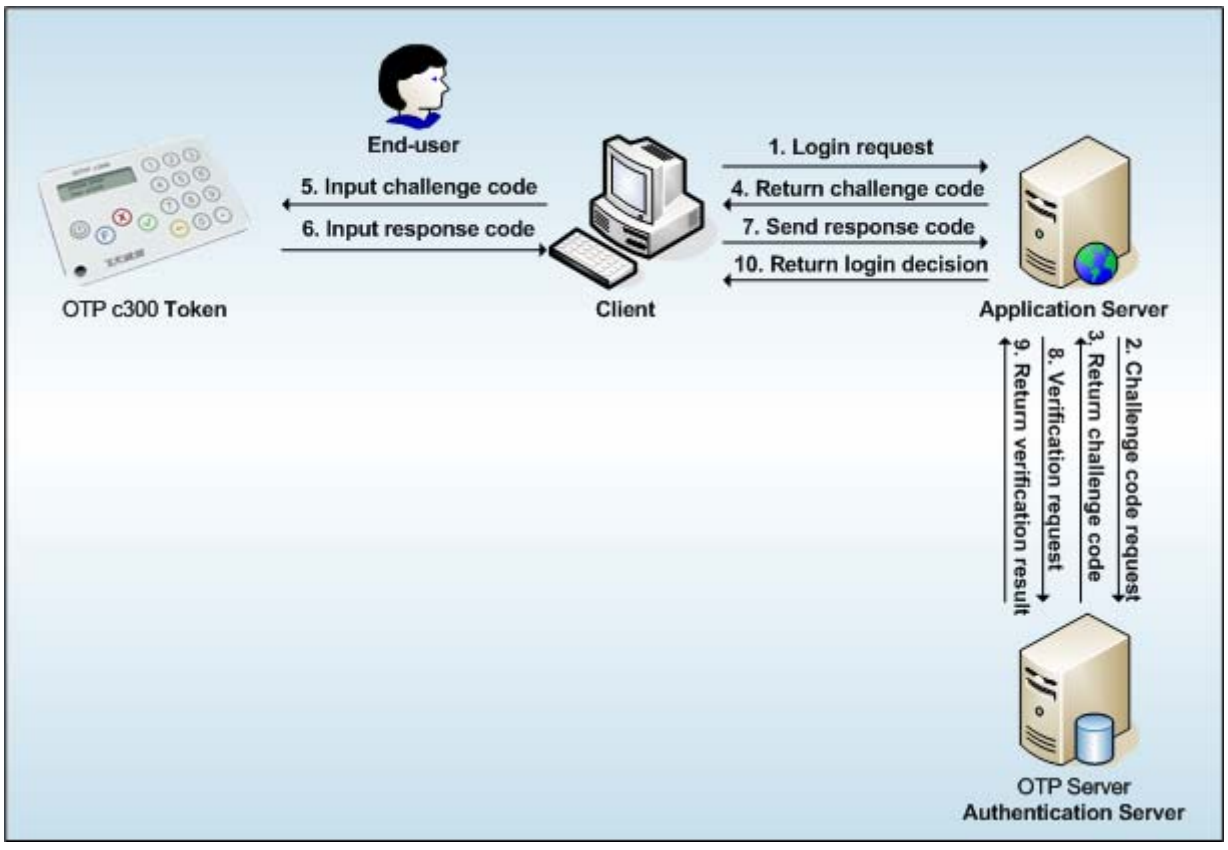

Figure 2 the process of end-user authentication by the system (challenge-response)

During the authentication process, both the dynamic password token and the authentication system work together: the authentication server generates the challenge code and the verification code whilst the token

generates the response code and is sent to the authentication server through the application system. If the verification code is same as the response code of the token, authentication is successful, otherwise it fails and login of the end-user is refused. The following are the steps of the process:

(1) The authentication server generates a challenge code and sends it to the end-user through the application server.

(2) The end-user inputs the challenge code into the token and the token generates a response code.

(3) The end-user sends the response code back to the authentication server.

(4) The authentication server generates a verification code based on the challenge code and seed key of the token saved.

(5) The authentication server compares the response code and the verification code to authenticate the end-user.

Security analysis: Authorized end-users use their own tokens to generate response codes according to the challenge code of the authentication server. Without a token, hackers cannot generate the correct challenge code, thus not allowing them to log into the system.

1.1.3 Authentication by System (Time Synchronization)

A time synchronization dynamic password authentication is successful when the dynamic password generated by the token is the same as the dynamic password generated by the authentication server, otherwise the authentication fails.

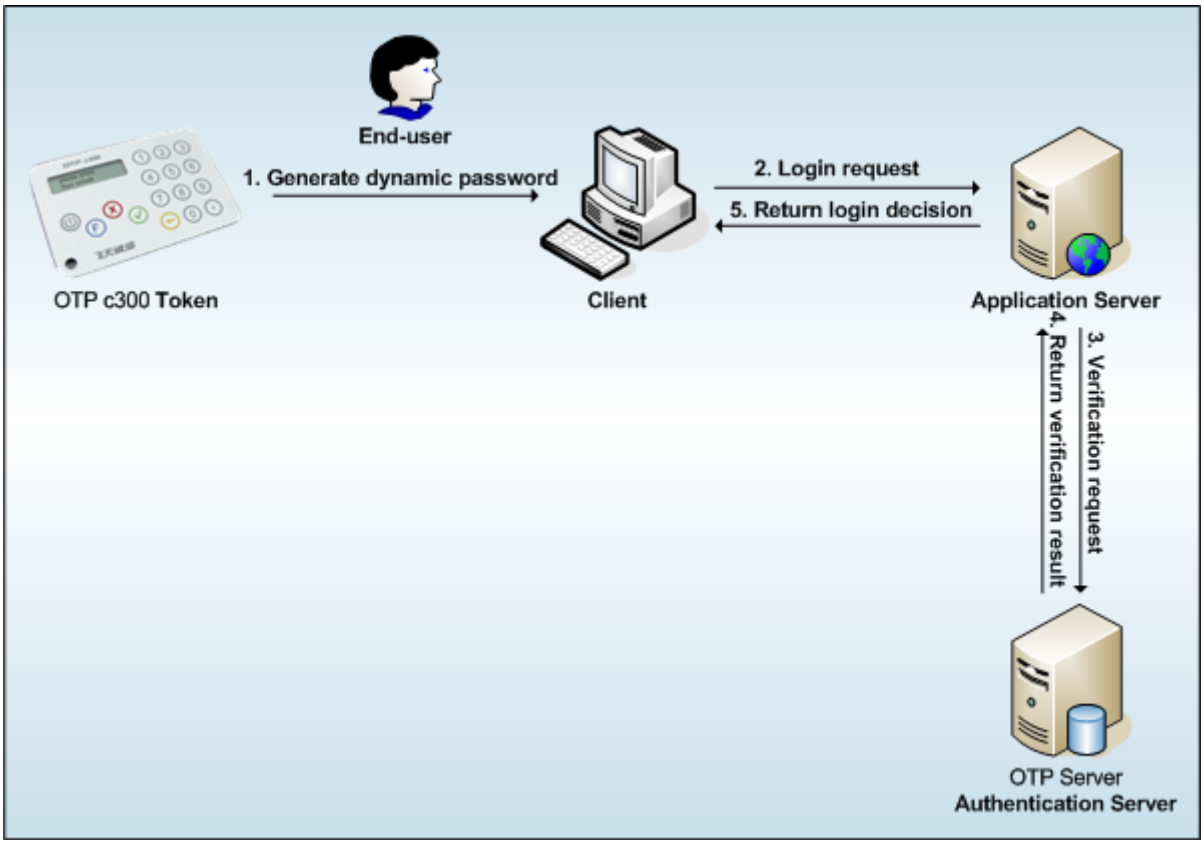

Figure 3 the process of end-user authentication by the system (time synchronization)

During the authentication process, both the token and authentication server work together: the token generates a dynamic password and sends it to the authentication server through the application server, which is verified and compared with the dynamic password generated by the authentication server itself. For a certain moment, since the token has been time synchronized with the authentication server, the two dynamic passwords should match so that it is believed that the end-user is who they claim to be. The authentication server will refuse login of an end-user if the passwords do not match. The following are the steps of the process:

(1) The token generates a dynamic password based on time and sends it to the authentication server through the application server.

(2) The authentication server generates a dynamic password based on the same moment and seed key of the token, and compares the two dynamic passwords to authenticate the end-user.

Security analysis: Authorized end-users use their own token to generate the same dynamic passwords as those generated by the server according to time. Without a token, hackers cannot generate the correct dynamic passwords, thus not allowing them to log into the system..

1.2 Basic Schemes

Based on the above theory, it is clear that two basic double-way authentication schemes are formed as the authentication server can use either the challenge-response method or the time synchronization method to authenticate an end-user. OTP c300 token supports both methods.

The following example is based on the time-synchronization method, which demonstrates the basic double-way authentication process and steps.

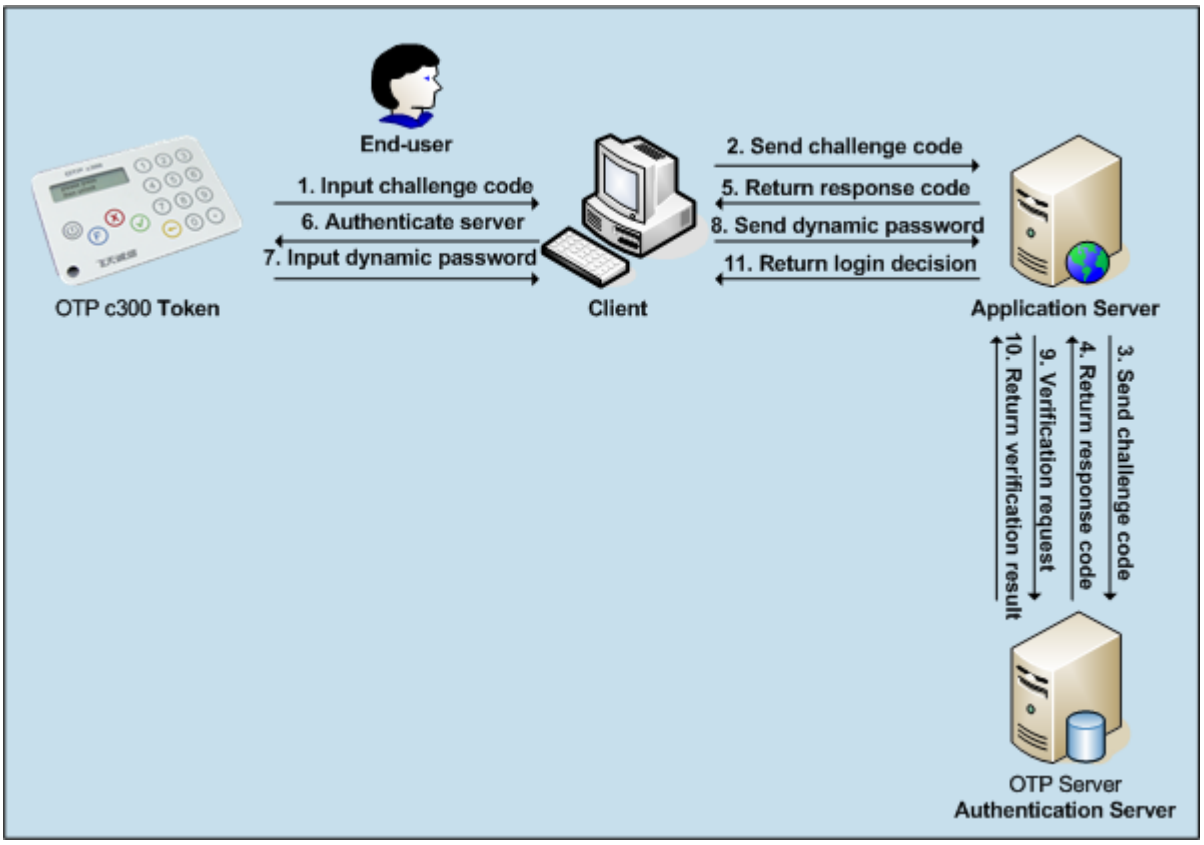

Figure 4 Basic double-way authentication scheme based on time synchronization method

In figure4, step 6 is very important, i.e. the end-user should only proceed with login when the application system is successfully authenticated. Step 10 is another important step, i.e. the application system will only allow the end-user to log in when he/she is successfully authenticated.

Chapter 2. Advanced Double-way Authentication

The basic schemes of double-way authentication have better anti-attack ability against phishing attacks, but not real-time man-in-the-middle attacks. Hackers can still monitor actions on the computer or intercept communications in order to steal the identity of the end-user. Once the identity is stolen, other sensitive information will be under threat.

Advanced double-way authentication combines mobile phone SMS with basic double-way authentication schemes to form an advanced authentication scheme for application systems. Through advanced authentication schemes, not all authentication information is transferred through the internet - but through both internet and SMS. Chances of information interception are largely reduced. It is comparably easier to intercept information on the internet. E.g. it is easy to use Trojan programs to monitor actions on the computer or messages sent through the network. Besides information on the internet, to intercept SMS information at the same time has proved to be very difficult. The hacker is required to have monitoring techniques for both the internet and SMS, as well as monitoring at the same time, which is highly unlikely.

2.1 Theory

Advanced double-way authentication schemes improve the security of basic double-way authentication schemes by adopting a new authentication communication channel. The theory of basic double-way authentication schemes applies to the advanced scheme.

2.1.1 Authentication by End-users

Before an end-user logs in, they should send the challenge code generated by the OTP c300 token to the authentication system through the application system. Then the authentication system will send the response code through SMS to the mobile phone of the end-user. The end-user compares the response code in SMS and the verification code on the token, if they are the same, the application system can be trusted, otherwise, it might be a fake system and the login operation should be immediately stopped.

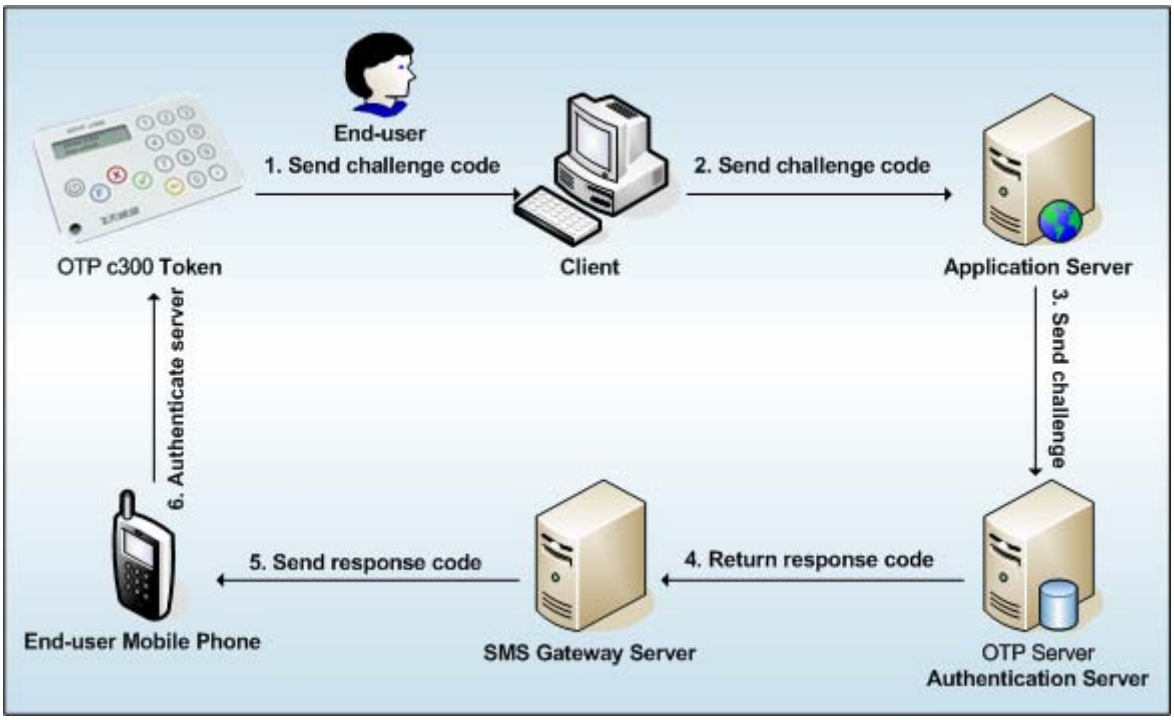

Figure 5 the process of the application system authentication by end-users (Advanced)

From the figure above, if the application system is a fake system, which cannot communicate with the authentication system so as not to generate the correct response code, the end-user is immediately aware.

Security analysis:

(1) Before login, end-users will authenticate the application server to prevent being cheated by fake servers (or phishing systems) of their sensitive information.

(2) Fake systems cannot generate SMS response code for an end-user to log into the real application server.

(3) Sending response codes through SMS not only can prevent response codes from online interception, but also can notify the real end-user that a hacker is trying to attack their account.

2.1.2 Authentication by Application Server (Challenge-Response)

An end-user can proceed with login once the authentication of the application server is successfully carried out. In this case, a login request is sent to the application server by the computer terminal of the end-user. The authentication server then generates a challenge code and sends it back to the end-user through SMS. The end-user inputs the challenge code into the OTP c300 token to generate a response code to send back to the authentication server by replying to the SMS. The response code will be compared with the verification code generated by the server itself. If the comparison is successful (both codes are the same), the application server will notify the end-user to log in. Or, the login request will be refused.

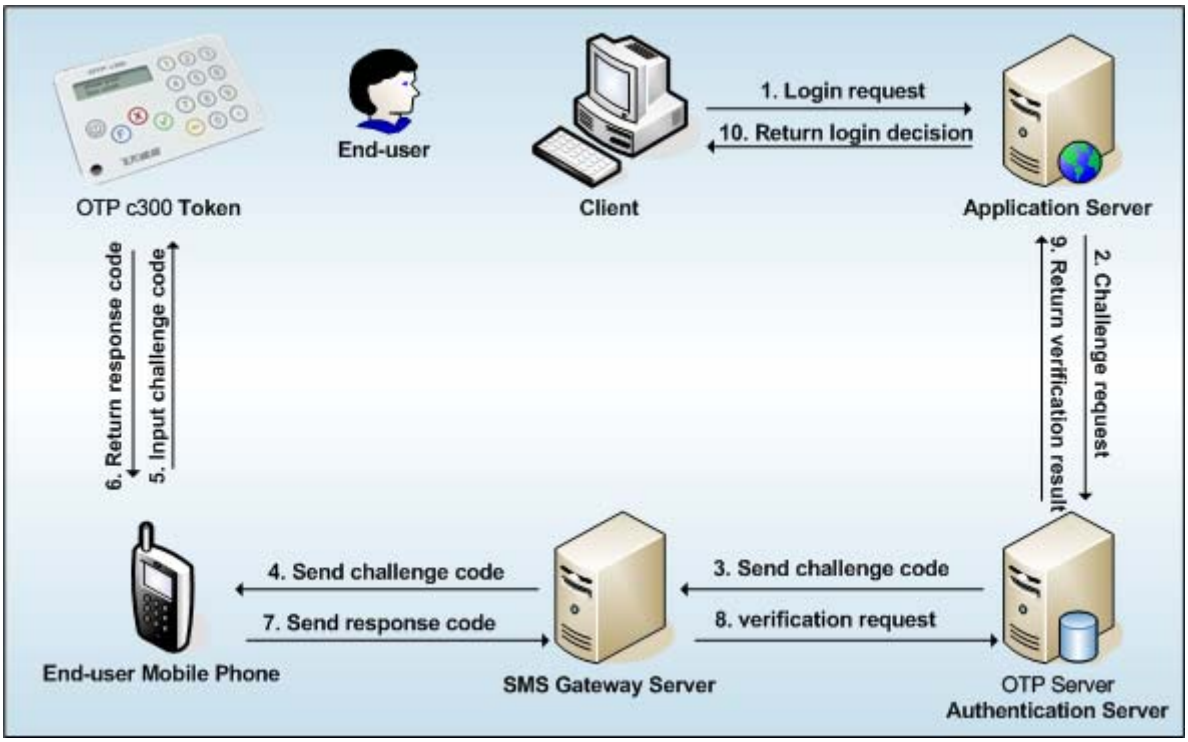

Figure 6 the process of the end-user authentication by the application server (Advanced challenge-response)

Fake servers cannot connect to the authentication server and ask the authentication server to send the challenge code to the end-user through SMS. If the end-user receives an SMS when they were not trying to log in the system, it is obvious that hackers are attempting login as the end-user. Even though as no response code is sent back, the login attempt will be refused. Personal data is protected.

Security analysis:

(1) Real end-users use an OTP token to generate response code to authenticate their own identity. Without a token, it is impossible to generate a correct response code for authentication.

(2) Fake servers cannot send challenge code through SMS to end-users.

(3) SMS communication, in one hand reduces the chance of losing essential information to hackers, and on the other hand, increases the possibility of preventing further attacks from happening as the end-user will receive an SMS whenever a login attempt is made.

2.1.3 Authentication by Application Server (Time Synchronization)

End-users can proceed with login once the authentication of the application server is successfully carried out. In this case, a login request is sent to the application server by the computer terminal of the end-user. The authentication server then generates a dynamic password request and sends it back to the end-user through SMS. The end-user presses the OTP c300 token to generate a dynamic password to sends back to the authentication server by replying to the SMS. The password will be compared with the local dynamic password generated by the server itself. If the comparison is successful (both passwords are the same), the application server will notify the

end-user to log in. Or, the login request will be refused.

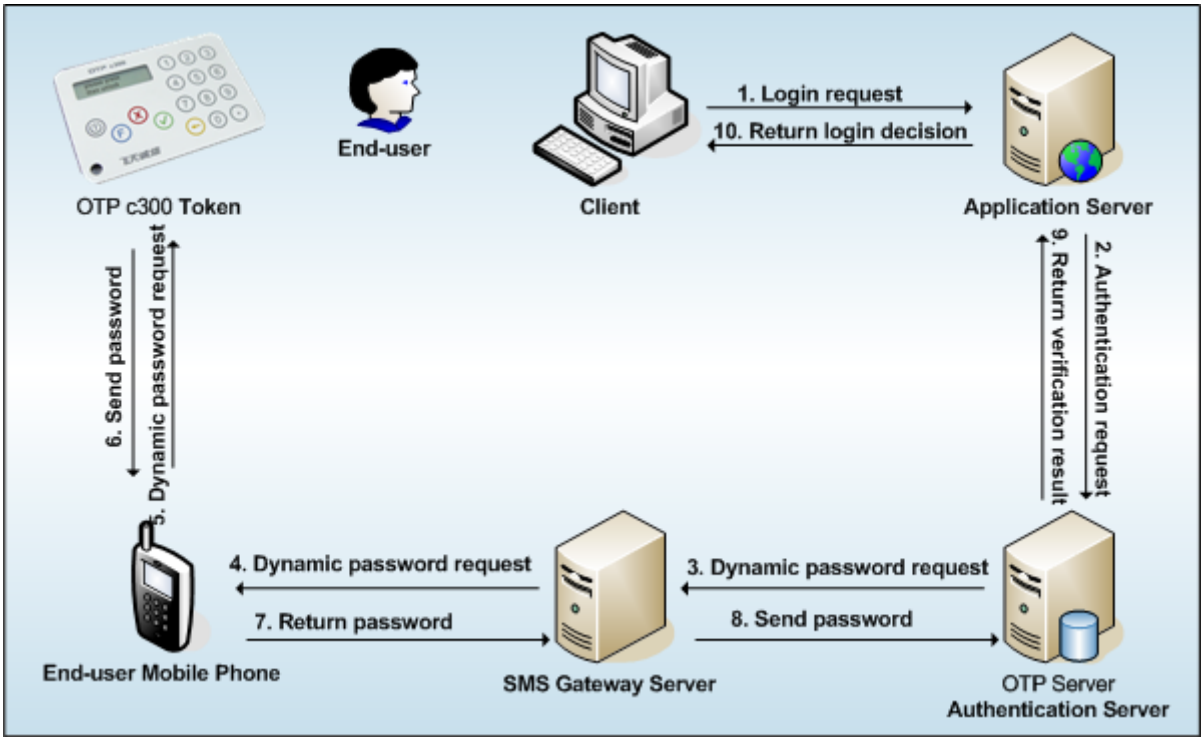

Figure 7 The process of end-user authentication by the application server (Time Synchronization)

The major advantage of the time synchronization authentication method is that it uses fewer operations than the challenge-response authentication method. For systems which require higher flexibility than security, the time synchronization authentication method is a better solution.

Fake servers cannot connect to the authentication server and ask the authentication server to send the dynamic password request to the end-user through SMS. If the end-user receives an SMS when they were not trying to log in the system, it is obvious that hackers are trying to login as the end-user. Even though no dynamic password is sent back, the login attempt will be refused. Personal data is protected.

Security analysis:

(1) Authorized end-users use an OTP token to generate a dynamic password to authenticate their own identity. Without a token, it is impossible to generate correct passwords for authentication.

(2) Fake servers have no way to find out mobile phone numbers of end-users so as to send fake dynamic password request through SMS.

(3) SMS communication, on one hand reduces chance of losing essential information to hackers, and at the same time increases the possibility of preventing further attacks from happening as the end-user will receive SMS whenever a login attempt is made.

2.1.4 Advanced Double-way Authentication Schemes

Based on the above advanced double-way authentication theory, it is obvious that two double-way authentication schemes can be formed, as an application server can choose from two methods to authenticate end-users; the challenge-response method and the time synchronization method. OTP c300 token supports both methods.

The process of advanced double-way authentication is demonstrated by the following figure, where the time synchronization method is used as an example.

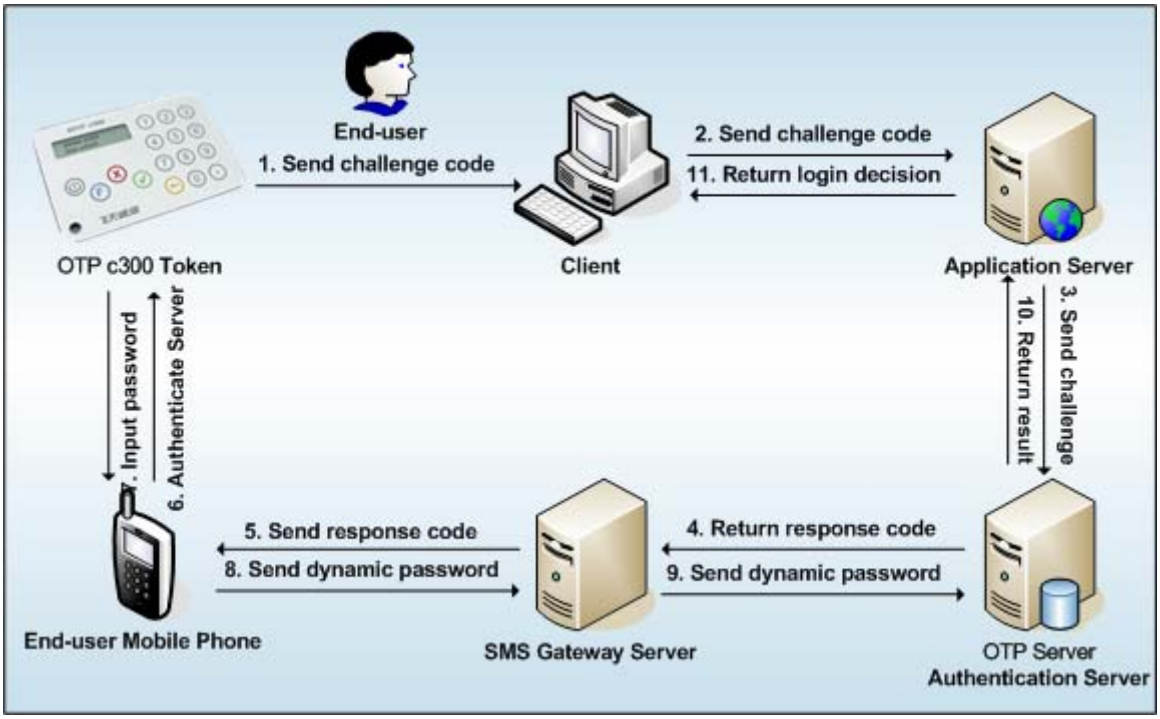

Figure 8 advanced double-way authentication scheme based on time synchronization method

In figure 8, step 6 is very important, i.e. an end-user should only proceed with login when the application system is successfully authenticated. Step 10 is another important step, i.e. the application system will only allow the end-user to log in when they are successfully authenticated.

Chapter 3. Transaction Signature

The aim of signing transactions is to prevent man-in-the-middle attacks, i.e. to prevent hackers from altering transaction data. Transaction signatures ensure that transactions will fail if transaction data is modified.

3.1 Basic Transaction Signature

The basic transaction signature scheme is based on the original authentication steps. No other communication channel or operation steps are needed.

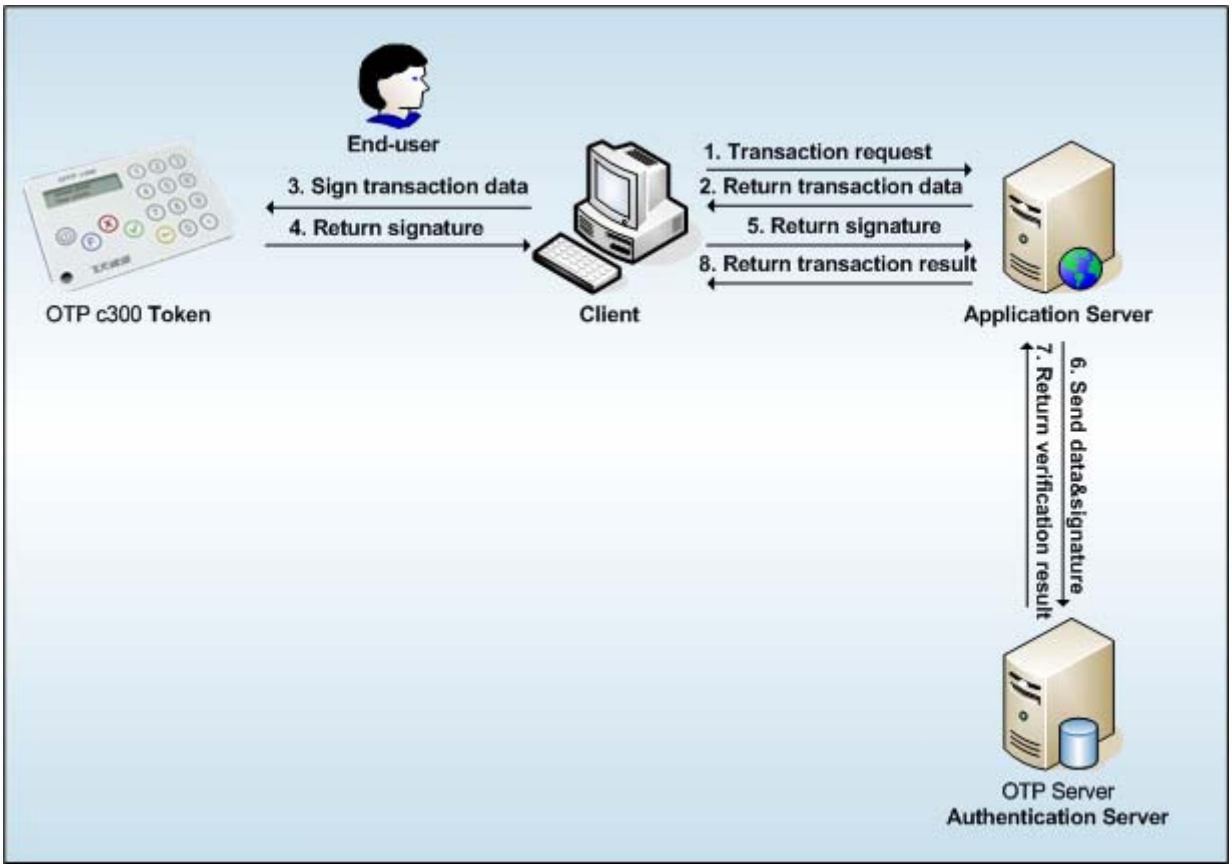

Figure 9 the basic transaction signature scheme

Basically, the transaction signature authentication scheme is done in the following steps. When a transaction request is submitted, the application server will withdraw critical transaction information and send to the end-user to confirm and sign. The end-user uses the OTP c300 token to digitally sign the transaction information and submit the signature together with the confirmation request. The authentication server will verify the signature and return the result to the application server. The application server will decide whether to proceed with the transaction request based on the authentication result of the signature.

Signatures can prevent transactions from being modified. If transaction data is modified during transmission,

signature verification will fail. The application server will stop the transaction immediately.

Security analysis:

(1) Authorized end-users use the OTP token to digitally sign their own transactions. Fake signatures or denials of the transaction are both prevented.

(2) Token-signed signatures cannot be faked easily; transactions without signatures or with fake signatures will not be granted by the application server.

(3) In detail, a hacker (especially in man-in-the-middle attacks) will change transaction data (e.g. transaction amount, destination account etc), which directly causes discrepancy between the transaction request and the transaction data received by the application server. Furthermore, the signed transaction data will not be the same as the fake transaction data. This transaction will just be refused.

Transaction signatures protect both the application system and end-users.

3.2 **Advanced Transaction Signature**

An advanced transaction signature adds another communication channel to the original authentication steps. SMS messaging channel is used to communicate authentication information to prevent online interception.

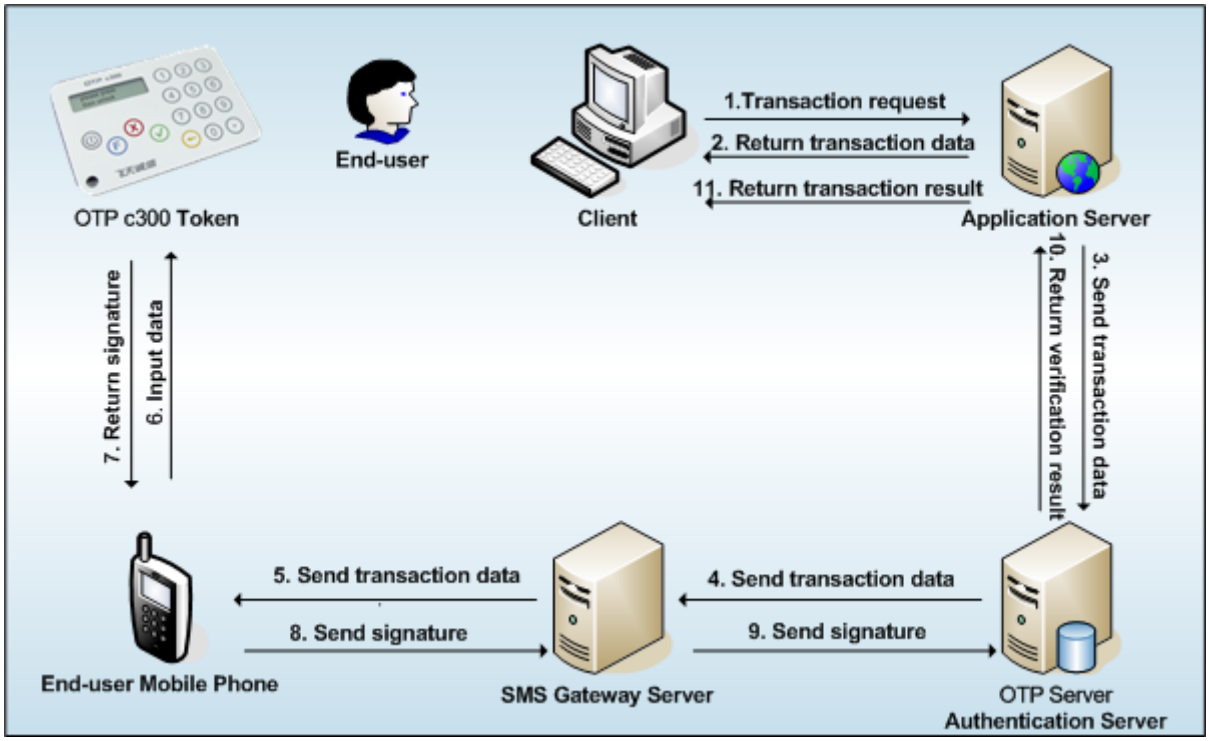

Figure 10 the advanced transaction signature scheme

The advanced transaction signature authentication scheme is done in the following steps. When a transaction

request is submitted, the application server will withdraw critical transaction information and send to the authentication server. Then the authentication server will send the transaction information through SMS to the mobile phone of the end-user, who checks the received transaction information. If the received information is the same as requested, the end-user can use the OTP c300 token to digitally sign the received information and send the signature data back to the authentication server through SMS. Finally, the authentication server verifies the signature, making sure it is not modified during transmission and sends the result to the application server, which proceeds with the transaction.

Signatures can prevent transactions from being modified. If transaction data is modified during transmission, signature verification will fail. The application server will stop the transaction immediately.

Security analysis:

(1) Authorized end-users use the OTP token to digitally sign their own transactions. Fake signatures or denials of the transaction are both prevented.

(2) Token-signed signature cannot be faked easily; transactions without signatures or with fake signatures will not be granted by the authentication server.

(3) In detail, a hacker (especially in man-in-the-middle attacks) will change transaction data (e.g. transaction amount, destination account etc), which directly causes discrepancy between the transaction request and the transaction data received by the authentication server. Furthermore, the signed transaction data will not be the same as the fake transaction data. This transaction will just be refused.

(4) SMS messaging channel can protect end-users in two ways: firstly, critical information is transferred off-line; secondly, the end-user will be notified of any transaction attempt by SMS.

Chapter 4. Scheme Features

Authentication schemes provided by OTP server Authentication System V3.0 does not only overcome the shortcomings of fixed-password systems, but additionally provides a more advanced level of security than a simple dynamic-password system.

4.1 Better than Fixed Password

Compared with fixed-password systems, authentication schemes based on the OTP c300 tokens have used the methods such as dynamic password, challenge-response, time-synchronization, application server authentication by end-users and transaction signatures to largely improve security, anti-attack ability and flexibility of maintenance of the system.

4.2 Better than Simple Dynamic Password

Authentication schemes provided by the OTP Server Authentication System have brought advanced security when compared to simple dynamic password systems by adopting double-way authentication and transaction signatures.

4.3 Simple Phishing Attack Prevention

Phishing attack is formed by building up fake application servers and seducing end-user into providing sensitive personal data. Double-way authentication can effectively prevent simple phishing attacks.

4.4 Real-time Phishing Attack Prevention

Unlike simple phishing attacks, real-time phishing attacks also combine man-in-the-middle attacks, i.e. sensitive data provided by the end-user will be sent to the real application server and result will be sent back to the end-user, which makes the fake server more real. Real-time phishing attacks can only be prevented by adopting advanced double-way authentication methods and advanced transaction signature authentication methods in which critical login data and transaction data is transmitted through SMS.

4.5 Effective Anti-man-in-the-middle Attack

Man-in-the-middle attacks are hard to find and very dangerous, as hackers will monitor all communication between the end-user and the application server and can intercept any wanted information. The transaction signature authentication can effectively prevent man-in-the-middle attack as fake signatures or non-signatures - making transactions stop immediately. Thus, both server and end-users are protected from threats.

4.6 Flexible Schemes

Many methods such as basic double-way authentication, advanced double-way authentication, basic transaction signature authentication and advanced transaction signature authentication are provided by the C300 token. Customized authentication schemes can be easily developed by adopting a simple method or a combination of two or more.

Chapter 5. **Benefits**

Benefits of the schemes provided by OTP Server Authentication System V3.0 and OTP c300 token include:

(1) Improved security

Authentication schemes of OTP Server Authentication System V3.0 can bring improved security for both the end-users and the application server.

(2) Improved efficiency

OTP Server Authentication System V3.0 provides advanced and easy-to-use tools to improve management efficiency.

(3) Lower cost

By adopting authentication schemes of OTP Server Authentication System V3.0, customers are provided with much lower management cost and risk cost is also reduced to the lowest with improved security

(4) Higher performance

OTP Server Authentication System V3.0 provides customers high-performance authentication schemes: end-users are allowed to securely log into the application system from anywhere at any time.

(5) Lower risk

Adopting OTP Server Authentication System V3.0, customers are equipped with low-risk authentication schemes: end-users are protected and happy; businesses are protected from losing revenues.

(6) Higher competitiveness

With the help of OTP Server Authentication System V3.0, businesses gains higher competitiveness with improved trust of end-users and a better image in providing advanced security.