

UNIOTP BUSINESS SOLUTION

VERSION 1.0

SecuTech

www.eSecuTech.com

The data and information contained in this document cannot be altered without the express written permission of SecuTech Solution Inc. No part of this document can be reproduced or transmitted for any purpose whatsoever, either by electronic or mechanical means.

The general terms of trade of SecuTech Solution Inc. apply. Diverging agreements must be made in writing.

Copyright © SecuTech Solution Inc. All rights reserved.

WINDOWS is a registered trademark of Microsoft Corporation.

The WINDOWS-logo is a registered trademark ^(TM) of Microsoft Corporation.

Software License

The software and the enclosed documentation are copyright-protected. By installing the software, you agree to the conditions of the licensing agreement.

Licensing Agreement

SecuTech Solution Inc. (SecuTech for short) gives the buyer the simple, exclusive and non-transferable licensing right to use the software on one individual computer or networked computer system (LAN). Copying and any other form of reproduction of the software in full or in part as well as mixing and linking it with others is prohibited. The buyer is authorized to make one single copy of the software as backup. SecuTech reserves the right to change or improve the software without notice or to replace it with a new development. SecuTech is not obliged to inform the buyer of changes, improvements or new developments or to make these available to him. A legally binding promise of certain qualities is not given. SecuTech is not responsible for damage unless it is the result of deliberate action or negligence on the part of SecuTech or its aids and assistants. SecuTech accepts no responsibility of any kind for indirect, accompanying or subsequent damage.

Contact Information

HTTP: www.eSecuTech.com

E-Mail: Sales@eSecuTech.com

Please Email any comments, suggestions or questions regarding this document or our products to us at: Sales@eSecuTech.com

Version	Date
1.0	2012.4.4

CE Attestation of Conformity



UniOTP is in conformity with the protection requirements of CE Directives 89/336/EEC Amending Directive 92/31/EEC. UniOTP satisfies the limits and verifying methods: EN55022/CISPR 22 Class B, EN55024: 1998.

FCC Standard



This device is in conformance with Part 15 of the FCC Rules and Regulation for Information Technology Equipment.

Operation of this product is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Conformity to ISO 9001:2000



The Quality System of SecuTech Solution Inc., including its implementation, meets the requirements of the standard ISO 9001:2000

ROHS



All UniOTP products are environmental friendly with ROHS certificates.

Table of Contents

ABOUT THIS GUIDE	1
CHAPTER 1: CURRENT SITUATION OF FINANCIAL TRANSACTION	2
1.1 Transaction mode	2
1.2 Transaction security	3
1.3 Common account security risks.....	4
CHAPTER 2: SECURITY ANALYSIS	5
CHAPTER 3: DYNAMIC PASSWORD TECHNOLOGY	6
3.1 Dynamic password overview	6
3.2 Dynamic password characteristics	6
3.3 Static password weak points	8
3.4 Dynamic password usage procedure	8
CHAPTER 4: UNIOTP DYNAMIC PASSWORD AUTHENTICATION	9
4.1 Overview	9
4.2 Solution Description	9
4.3 UniOTP Dynamic password protection for each type of transaction	12
4.4 UniOTP Dynamic password increases user authentication security	12
4.5 UniOTP dynamic password authentication solution analysis	13
4.6 UniOTP Dynamic password authentication benefits analysis	13
CHAPTER 5: ABOUT UNIOTP	14

About this guide

This document is intended for use by management.

UniOTP dynamic password authentication system is a dynamic password authentication product designed by SecuTech Solution Inc. The company is committed to providing superior software protection and authentication experience for the user's personal data and intellectual property.

E-commerce requires that each party cooperates closely in order to provide to the consumer a safer environment and a more comfortable and appropriate consuming platform. It will become one of the most important business models in the future. But, while having brought convenience to people's life, e-commerce also brings several hidden security risks. Attacks are becoming more sophisticated and diverse, and cases where a consumers' profit has been infringed are rapidly increasing. Security is one of the most important obstacles to e-commerce development.

Financial industry refers to those enterprises operating specialized financial products, including banking, insurance, trust, securities industry, leasing industry, mortgage industry etc. With the application of network technology in the financial industry, people can enjoy convenience brought by the computer network, such as online banking and online security trading. But with this convenience, user information security is facing more serious challenges. Various network attack technologies result in economic losses to customers. As the first user information security shield, if authentication is not strong enough, it will cause severe security problem and economic loss.

Authentication is the first step in assuring safety. This safety is directly related to the consumers' personal benefits. Dynamic authentication is a technology that provides a strong authentication method to users and is considered to be a method that can solve today's authentication related problems. The combination of dynamic password with e-commerce greatly raises the security level of electronic transactions, and better protects consumers' benefits.

Enterprise application refers to all kinds of information management systems which is applied by different enterprises, such as E-commerce, Enterprise resource planning (ERP), custom relationship management (CRM), etc. It will greatly improve enterprise management and manufacture efficiency by using enterprise applications to process cumbersome information.

Some of the information maintained by enterprise applications contains confidential information which may involve the core enterprises interests, so security of this information is very important. Enterprise information security can be achieved by building a defence system, including anti-virus, firewall network monitors and etc.

Chapter 1: Current situation of financial transaction

1.1 Transaction mode

1.1.1 OCT (Order confirmation transaction)

When a customer goes to the counter and talks to a teller to do their business directly, customers have to present their ID and bank card to tellers and provide password to complete authentication and do business.

1.1.2 Dedicated terminal

Customers use a dedicated terminal provided by a financial institution (ATM and POS) to process their transactions. Customers need to present credential card (bank card), customer ID and customer password to start independent transactions.

1.1.3 Online transaction

Customers logon to financial institution websites to process business. In online transactions, customers normally provide an account name and password to complete the authentication process. After successfully logging on, customers can process their business online.

1.1.4 Telephone transaction

Customers can process their business through calling the financial institution's hotline. Customers need to provide user credentials and password to complete authentication.

1.2 Transaction security

A variety of transaction modes bring different trading experience to customers along with different security risk.

1.2.1 OCT security

When customers provide their account number and passwords, there is a risk that criminals may peek at their passwords. After stealing the passwords, a criminal can log into customer accounts and perform illegal operations.

1.2.2 Dedicated terminal security

When a user inputs their account number and password, there is a risk that criminals may record their password. Because dedicated terminals are for public use without any special protection, it is easy for criminals to steal a users' identification information.

1.2.3 Online transaction security

There is risk that online transaction user accounts and passwords are stolen by criminals, through listening, installing Trojans on a target computer, network hijack etc.

1.2.4 Telephone transaction security

There is risk that user accounts and passwords are stolen by recording and eavesdropping.

1.3 Common account security risks

1.3.1 Plagiarism leak

Attackers steal customer account information by eye, and fake user customer ID to operate customer accounts illegally. This kind of risk usually occurs when customers do their business in public.

1.3.2 Install Trojans

Attackers install Trojans on a target computer, and steal user accounts and passwords remotely. This security risk usually exists when users perform their business online by PC.

1.3.3 Network sniffing

Attackers extract a user's confidential information through eavesdropping on the data transmission network.

1.3.4 Replay attack

Attackers simulate a user logon, through sending authentication request data packages which was intercepted and recorded via network, to achieve the purpose of operating a user account.

1.3.5 User password guess

If a users password is too simple and uses some special number, such as date of birth, anniversary and name, attackers can obtain users password by using these details easily.

1.3.6 Records leak

If a password is too complicated and users record it on paper, there will be a risk of password leak.

1.3.7 Brute force

Attacker obtain passwords by an enumerating method

1.3.8 Password sharing

To remember various passwords for many different accounts, users usually use the same password. If one password is stolen, criminals can try it on other accounts.

Chapter 2: Security analysis

A general overview of the hidden security risks with e-commerce:

2.1.1 Falsification

Business related information is falsified as it is been transferred over a network.

2.1.2 Information destruction

Due to network devices or software malfunctioning, some data loss can happen.

2.1.3 Identification

A third party who uses weak methods of identification could be used to gain another party's identity and achieve illegal operations.

2.1.4 Information leaking

Information of a transaction between two parties is read by a third party.

UniOTP dynamic authentication system helps solve identification related risks. Below are the common patterns of identification security risks:

- Consumer's account name and password are stolen.
- The attacker installs a trojan horse on a user's computer to steal personal information such as bank account numbers.
- The attacker listens on the network, intercepts user information and gets the bank account number.
- For more convenience, a consumer chooses an easy password such as their birth date, wedding anniversary, name, etc. making the password easy to guess for the attacker.
- The consumer stores password information in a certain place (file or notebook), that might lead to password leaking.
- The attacker uses brute force attack.
- The consumer uses the same password for different accounts, which creates a vulnerability concerning password cracking.

Chapter 3: Dynamic Password Technology

3.1 Dynamic password overview

Dynamic passwords, also called one time passwords, are considered to be one method capable to solve authentication existing security problems. It is widely used for many situations and users such as Banks, Bourse, e-commerce. A Dynamic password generation algorithm, user's private key and dynamic elements constitute the 3 elements used to generate the dynamic password. When you authenticate yourself, besides from your account name and your password, you have to provide the dynamic password to be able to pass the authentication process.

Time based dynamic password generation creates a new unpredictable random password automatically every 60 seconds. This password can only be used once.

Event based dynamic password generates a new unpredictable random password every time you press its button. This password can only be used once.

Challenge response dynamic password uses a challenge code to generate a new unpredictable password. When the user requests authentication, the server will return a challenge code, this challenge code will be used to generate this time's password.

3.2 Dynamic password characteristics

3.2.1 *Dynamic*

Depending on the dynamic factor changes, the password generated by dynamic password token will change. Every password generated is different from each other.

3.2.2 *Valid only one time*

Password generated by the dynamic password token can only be used one time, after that it will become invalid.

3.2.3 *Random*

Passwords are randomly generated, and cannot be predicted based on statistics.

3.2.4 Easy to use

Dynamic password is easy to use, no need for the user to remember the password, he only needs to read the password from the token at authentication time.

3.2.5 Loss report

As the user always keeps the token with him, he can notice the loss of the device immediately and report it as lost to the administrator who will disable the token, reducing risks caused by the loss.

3.2.6 Protection against Trojans/Network interception

As the password is only valid one time, it is a way to protect oneself from peeking, Trojans, network interception.

3.2.7 Protection against brute force attack

The fact that the password is dynamic, and so, that it always changes every time is a good protection against brute force attack. (The attacker has less than 60seconds to crack the password and use it before it becomes invalid or before the user himself uses it)

3.2.8 Economic

One token can be used for more than 3 years, and allow to lower the initial cost.

3.2.9 Computer-independent

The dynamic password Token has a LED display, you do not need to connect it to your computer through the USB port. In this case , it is very safe to use, as there is no connection with the computer as it doesn't have the same security risks as USB based token products and certificate based products (In the case of USB products, there is some risks to get infected by Trojans performing unwanted online transactions).

3.3 Static password weak points

- In Order to make it easier to remember, users often use birth date, phone number, etc. as a password. Hackers can use automated programs to constantly attempt the passwords in order to crack the password.
- If a password is used many times, hackers can calculate the password easily, by identifying the encrypted authentication information transmitted through network by using a interception and reply technique, which will cause unintentional information leak.
- Because most of the current authentication information transmitted through a network is unencrypted, hackers can obtain important information about users through eavesdropping on the network data stream. They identify authentication information and intercept passwords from the network or telephone line.
- Hackers often intercept a user's password by using spies, deception and other methods.

3.4 Dynamic password usage procedure

- 1) User requests connection to the web server
- 2) Web server asks the user to authenticate
- 3) User's computer displays a login interface, asking user to input account name, password and dynamic password.
- 4) User's computer sends user authentication information to the web server
- 5) Web server requests to the Authentication Server to authenticate user's identity.
- 6) Authentication server returns authentication information to the web server.
- 7) Web Server decides if the user can log in or not based on authentication results.

Chapter 4: UniOTP Dynamic Password Authentication

4.1 Overview

UniOTP dynamic password authentication system is a dynamic password product developed by SecuTech Solution Inc. UniOTP dynamic password authentication products can efficiently reduce losses caused by password leaking, and offer a powerful protection for user information and intellectual property. UniOTP dynamic password authentication system can be integrated with many kinds of systems, providing a dynamic password authentication service fitting any users' needs.

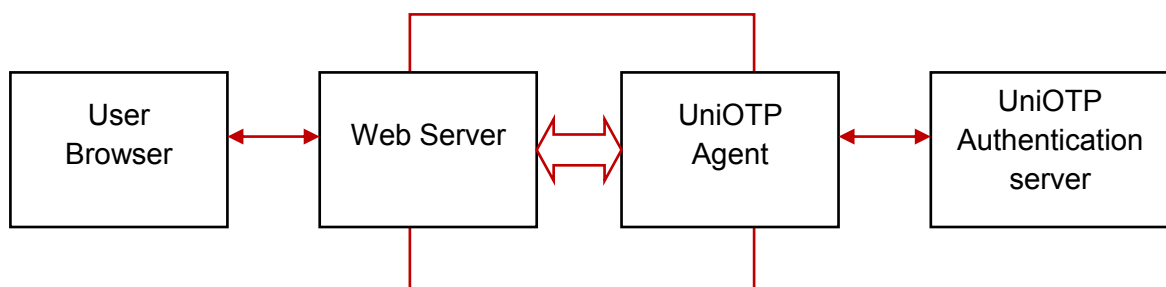
The enterprise server uses Agent SDK to perform the integration with UniOTP dynamic password authentication system and unify user authentication service. UniOTP dynamic password system open architecture and module based tiered structure provides convenience for UniOTP dynamic password system and enterprise server integration. UniOTP dynamic password authentication system robustness, flexibility, high availability and easy maintenance provide the best dynamic password authentication experience to the user.

4.2 Solution Description

E-commerce's web structure mainly uses a server/browser setup. UniOTP dynamic password system provides two integration methods:

4.2.1 First Solution:

Use Agent SDK (or Agent software) to perform integration of Web server and UniOTP dynamic password authentication systems, providing a unified authentication for the consumer. UniOTP's dynamic password system open architecture, high stability and user-friendly interactivity provides the best dynamic password authentication and user experience possible.



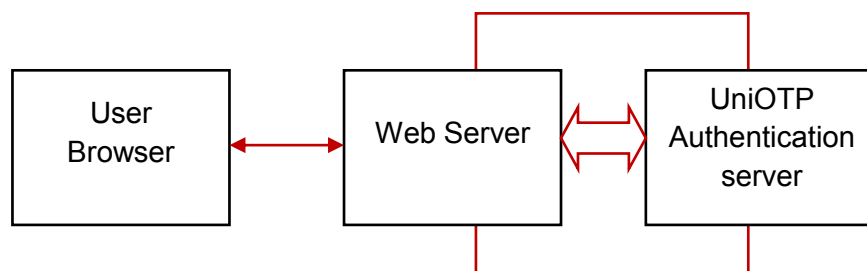
4.2.2 Authentication process:

After having integrated the dynamic password authentication as above, the consumer login process is the following:

- The consumer uses their browser to display the login page
- The consumer fills in their username, password, dynamic password and sends the login request
- The web server authentication module receives the data submitted by the user and uses UniOTP Agent to send this data to the UniOTP authentication server
- UniOTP authentication server processes user authentication information to complete the authentication, and returns authentication results to UniOTP Agent.
- UniOTP Agent returns the authentication results to the Web server authentication module
- The web server decides if the user can login or not depending on the authentication results sent by UniOTP Agent.
- The consumer is able to log in, or receives a log in error message if the authentication failed.

4.2.3 Second solution:

User Server SDK to add dynamic password authentication function to the web server and perform integration of the Web Server System and UniOTP dynamic password authentication system. By using Server SDK integration to perform web application dynamic password authentication, you don't need to rely on a UniOTP authentication server, but, compared to the two precedent methods, this method requires the user to have strong development skills.



4.2.4 Authentication process:

Once you've integrated UniOTP dynamic password authentication according to the picture above, the authentication process is the following:

- The consumer opens the login page in their browser
- The consumer fills in their username, password, dynamic password and sends the login request
- The Web server receives authentication information submitted by the user and calls UniOTP Authentication Module to complete user authentication
- The Web server decides to allow or refuse consumer login depending on authentication results.
- Consumer is allowed to log in, or receives an error message if authentication failed.

4.3 UniOTP Dynamic password protection for each type of transaction

Transaction method	UniOTP protection
OTC transaction	The main security risk of OTC transaction is from plagiarism. The UniOTP dynamic password authentication system uses one time valid password. After the password is used, it is disabled. Therefore UniOTP system can protect user information security effectively.
Dedicated terminal transaction	The one time validity of UniOTP dynamic password provides excellent anti-peek feature. No matter what means exploited by attacker to steal user information from user terminal, the information is no longer valid, therefore UniOTP dynamic password authentication system can eliminate risk from dedicated terminal transaction.
Online transaction	Online transaction is easily attacked. With features of one time validity, randomness and unpredictability, UniOTP dynamic password protects user information from Trojans, network sniffing and replay attacks.
Telephone transaction	The one time validity feature enables UniOTP to eliminate password leakage caused by stealing password via telephone transaction.

4.4 UniOTP Dynamic password increases user authentication security

UniOTP dynamic password is only valid once and cannot be predicted by any statistical means, the attacker cannot deduce what will be the next password from the previous ones, and moreover already used passwords will immediately be disabled after being used once. By using dynamic passwords, you can avoid the potential safety problems which are caused by plagiarism, Trojans, network monitoring and password leaking by the consumers.

4.5 UniOTP dynamic password authentication solution analysis

- UniOTP dynamic password authentication helps financial institutions provide customers with a securer authentication service, and satisfy customers who require higher account security.
- The features of easy integration and maintenance reduce cost effectively.
- Help financial institutions reputation improves with better account protection.
- Secure transaction environments will attract more customers.
- Reduce maintenance cost caused by password theft.
- Easy to use, does not need require any software or connection to a computer by using an interface.
- Reduce users cost effectively. Every UniOTP can be used for 3-5 years.
- Improve account security and reduce customer economic risk.

4.6 UniOTP Dynamic password authentication benefits analysis

- UniOTP Dynamic authentication system helps financial organizations to strengthen its authentication method in order to satisfy consumer security exigencies.
- UniOTP dynamic password authentication system can be integrated simply and maintained easily, thus it will reduce your costs effectively.
- UniOTP dynamic password authentication system will assist E-business service provider to build a more secure platform for consumers and increase credit and reputation of the E-business operator.
- UniOTP Dynamic password authentication protects consumers' information from being stolen, and increases your users' feeling of security.
- One token can be used from 3 to 5 years, reducing initial cost for the consumer.

Chapter 5: About UniOTP

UniOTP dynamic password authentication system is a dynamic password authentication product designed by SecuTech Solution Inc. The company is committed to providing superior software protection and authentication experience for the user's personal data and intellectual property.

Financial sector activities require that each party cooperates closely in order to provide to the consumer a safer commercial environment and a more comfortable and appropriate consuming platform.

Follow us!



[Twitter](#)



[Facebook](#)



[Youtube](#)



[Linked in](#)



About SecuTech

SecuTech Solution Inc. is a company specializing in data protection and strong authentication, providing total customer satisfaction in security systems & services for banks, financial institutions & other industries. Having extensive and in-depth experience within the information security market, SecuTech has drawn upon this experience to utilize today's cutting-edge technologies, enables enterprises, financial institutions, and government to safely adopt the economic benefits of mobile and cloud computing that are effective against increasingly sophisticated cyber attacks.



www.eSecuTech.com SecuTech Solution Inc.

North America

1250 Boulevard René-Lévesque Ouest, #2200,
Montreal, QC, H3B 4W8,
Canada
T: +1 -888-259-5825
F: +1 -888-259-5825 ext.0
E: INFO@eSecuTech.com

China

Level 12, #67 Bei Si Huan
Xi Lu,
Beijing, China, 100080
T: +8610-8288 8834
F: +8610-8288 8834
E: CN@eSecuTech.com

APAC

Suite 5.14, 32 Delhi Rd,
North Ryde,
NSW, 2113, Australia
T: 00612-9888 6185
F: 00612-9888 6185
E: AUS@eSecuTech.com

EMEA

4 Cours Bayard 69002
Lyon, France
T: +33-042-600-2810
F: +33-042-600-2810
M: +33-060-939 6463
E: Europe@eSecuTech.com

©Copyright 2012 SecuTech Solution Inc. All rights reserved. Reproduction in whole or in part without written permission from SecuTech is prohibited. SecuTech UniOTP and the SecuTech logo are trademarks of SecuTech Inc. Windows and all other trademarks are properties of their respective owners. Features and specifications are subject to change without notice.