

UNIOTP USAGE OVERVIEW

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: NETWORK SECURITY RISKS	2
CHAPTER 2: DYNAMIC PASSWORD TECHNOLOGY	3
2.1 Dynamic password overview	3
2.2 Dynamic password characteristics	3
2.3 Static password weak points	5
CHAPTER 3: PRODUCT PARTICULARITIES	6
3.1 Platform particularities	6
3.2 Security Particularities	6
3.3 Other advantages	6
CHAPTER 4: PRODUCT CHARACTERISTICS	7
4.1 Features	7
4.2 Integration methods	7
4.3 Application domains	7
CHAPTER 5: PROTECT WEB APPLICATIONS	8
5.1 Overview	8
5.2 Solution Description	8
CHAPTER 6: ABOUT UNIOTP	11

About this guide

UniOTP authentication system is a strong authentication system that makes use of dynamic passwords. This system is designed to provide user application systems with a securer authentication service and improve the security of user accounts.

UniOTP Authentication server uses a scientific software structure, advanced and mature software technologies that have some advantages such as being highly reliable, easy to implement and easy to maintain. It supports Radius Authentication protocol, providing seamless authentication integration and flexible authentication solutions compatible with any device supporting the Radius Protocol or any system based on the C/S and B/S models, in order to satisfy any user's authentication needs.

Network applications are a kind of software applications published on internet or on the company intranet that are executed in a browser. Network applications are developed using web languages, and displayed using a browser. The reason why network applications are popular is that it is multiplatform and there is no need to install or upgrade periodically. All actions performed by the network application need to use a network (Internet or Intranet), and this is one of the most challenging element concerning network applications security.

Cases where Trojans or other malicious ways are used to retrieve user bank account number, or login username and password to perform unwanted actions, steal user information or property are increasing. Authentication security directly influences user property and personal information safety.

Intranet is widely used in companies, through it, you can perform file management, software sharing, printer sharing, and many other tasks. Any operation that you can perform through the intranet, includes using the company network, manage files, etc all require that you first get authenticated. Intranet is used as the company's internal network; data exchanged on this network needs a very high level of security. Authentication is the first protection to manage intranet user access and plays a vital role for intranet networks security.

Chapter 1: Network Security Risks

Because of the diversity of possible network attacks, there are many security risks affecting network applications. Authentication security is an important element since it is the “door” to access the network application contents. Authentication security's biggest challenge comes from the various ways passwords can leak. The most common methods are the following:

- Account name, login password peeking/listening
- A Trojan has been installed on the computer, and it is being remotely controlled
- The attacker uses network wiretapping, intercepts user packets and extracts login information
- The password is set to a birthday date, wedding anniversary, etc. and is easy to guess for the attacker
- The password is saved or written in a specific place
- The attacker uses a brute force attack
- Using the same password for many accounts with different usages

Due to the static characteristics of the traditional password, it leaves the possibility to implement attacks described above.

Chapter 2: Dynamic Password Technology

2.1 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.

2.2 Dynamic password characteristics

2.2.1 *Dynamic*

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

2.2.2 *Valid only one time*

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

2.2.3 *Random*

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

2.2.4 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.

2.2.5 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.

2.2.6 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.

2.2.7 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)

2.2.8 Economic

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

2.2.9 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).

2.3 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.

Chapter 3: Product Particularities

3.1 Platform particularities

UniOTP Authentication Platform has the following particularities:

- Supports many operating systems
- ODBC database connection and database special connection support a wide range of databases or its combinations.
- Provide a web based management system
- Provides authentication Agent and authentication Server software development kits in many programming languages.
- Support Radius authentication protocol, providing convenience for centralized authentication.
- High reliability and support massive concurrency certification
- Authentication service has extremely flexible settings

3.2 Security Particularities

- Password dynamism provides a protection against peeking, brute force attack and many other sorts of attacks.
- Password generation is made without a pattern, making it unpredictable.
- Each dynamic password is only valid once, after use, it becomes invalid. It can efficiently protect from Trojans, network interception, and other kinds of attacks that operate by stealing the password.
- Dynamic and static passwords can be used together for authentication, providing 2 elements of authentication and in this way, strengthen user information safety.
- The software layer performs user account risk prevention

3.3 Other advantages

- With more security, potential economic loss is reduced
- Provide continual service for the whole process presale, sales, after sales.
- Provide many administration tools and efficiently reduce system maintenance cost for the user
- Provide many kinds of second development samples, making shorter development cycles for the user and further reducing cost.
- Many kinds of directly usable system integration solutions, reducing implementation cost.

Chapter 4: Product Characteristics

4.1 Features

Platforms: Windows, Linux and other operating systems.

Databases: Oracle, SQL Server, MySQL , PostgreSQL

Administration: Provide a Web based information management system and a desktop service management tool.

Conformed to standard: Radius authentication protocol, HOTP/TOTP OATH standard algorithm, ODBC database connection, LDAP User integration

Second development SDK: Provide samples for C/C++/Java/C#/PHP, etc. making simpler authentication agent and authentication server development for the user.

Token type: Time based, event based, challenge/response

4.2 Integration methods

- Supports Radius protocol to perform system seamless integration.
- Performs integration through the agent installation.
- Use the SDK for application post development and integration

4.3 Application domains

- Used in finance, e-commerce, telecommunications, education and entertainment domains.
- Used in computer networks, smart homes, smart security domains
- Used for intranet application systems, company office automation, and company mail systems.
- Used to protect operating system logon and assure other basic software security

Chapter 5: Protect Web Applications

5.1 Overview

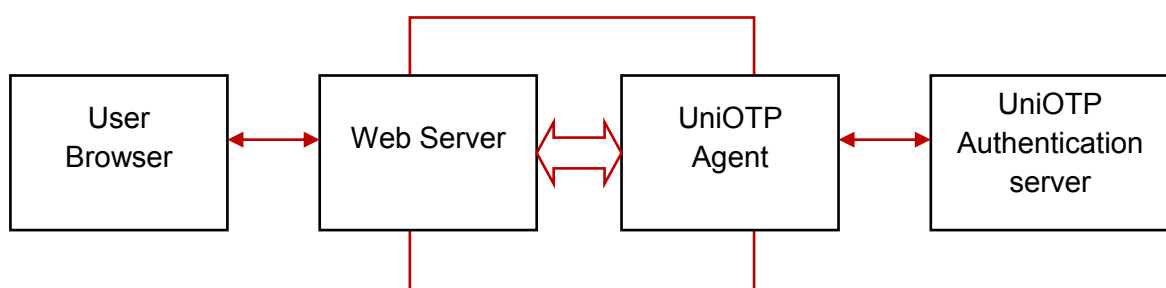
UniOTP dynamic password authentication system is a dynamic password product developed by SecuTech Solution Inc. UniOTP dynamic password authentication products can efficiently reduce losses caused by password leaking, and offer a powerful protection for user information and intellectual property. UniOTP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

5.2 Solution Description

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

5.2.1 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.



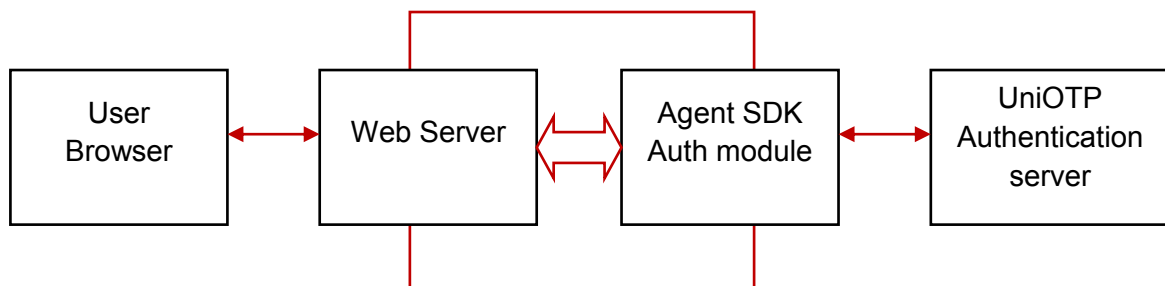
5.2.2 Authentication process:

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

1. The consumer uses their browser to display the login page
2. The consumer fills in their username, password, dynamic password and sends the login request
3. 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
4. UniOTP authentication server processes user authentication information to complete the authentication, and returns authentication results to UniOTP Agent.
5. UniOTP Agent returns the authentication results to the Web server authentication module
6. The web server decides if the user can login or not depending on the authentication results sent by UniOTP Agent.
7. The consumer is able to log in, or receives a login error message if the authentication failed.

5.2.3 Second Solution

Using Agent SDK, you can integrate a module with the UniOTP dynamic password authentication agent function (The web application directly integrates with Web Agent features).

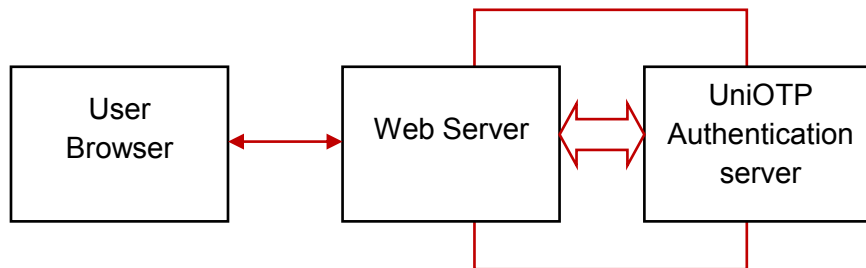


5.2.4 Authentication process

1. User opens the login page in their browser
2. User fills in their information and sends it.
3. Web Application authentication module performs dynamic password authentication and returns authentication results
4. If the authentication succeeds, user is allowed to log in. Otherwise, an error message is shown.

5.2.5 Third 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



5.2.6 Authentication process:

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

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

Chapter 6: 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. The application of an open network makes it more vulnerable to attack. That's why it is needed to have every department to cooperate closely with each other to be able to build a more secure network environment, and be able to have better network services in our lives.

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.

SecuTech 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.