

UNIOTP AUTHENTICATION SYSTEM WHITE PAPER

VERSION 1.1

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	2011.4.20
1.1	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: DYNAMIC PASSWORDS.....	2
1.1 About dynamic password technology	2
1.2 Advantages of dynamic password	3
CHAPTER 2: UNIOTP DYNAMIC PASSWORD AUTHENTICATION SYSTEM.....	5
2.1 System introduction.....	5
2.2 Product composition and features	5
2.3 Platform support.....	7
2.4 Applied Protection System	7
2.5 UniOTP System Structure	8
2.6 LDAP Protocol Support	8
2.7 Core functions of UniOTP Dynamic Password Authentication System	9
2.8 UniOTP dynamic password authentication features	10
APPENDIX	11

About this guide

The UniOTP Technical manual is intended for use by administrators and anyone who wants a clearer understanding of how UniOTP operates. Full descriptions of UniOTP's dynamic password authentication system and advantages of using such a system as well as supported features are also given in this document.

Chapter 1: Dynamic passwords

1.1 About dynamic password technology

Dynamic password technology is an authentication technique which generates dynamic passwords for authentication. The theory is that the encryption key and encryption algorithm are stored both in server and token. The token and server generate dynamic passwords by using the encryption algorithm according to the encryption key which contains a static factor and a dynamic factor dynamically changing with some mechanism to ensure the generated password is different every time. When user authentication is required, users use a password for this authentication generated by using their token, and the authentication server will generate a password by using the same encryption algorithm and password. By comparing these two passwords, the authentication process is realized. According to different dynamic factor changing mechanisms, the dynamic password token can be classified as a time based token which uses time as another dynamic factor, event based token which use frequency of password generation and challenge response based token which uses challenge information sent by the server as a dynamic factor.

1.1.1 Time Based token

Time based tokens use time as a dynamic factor. It usually uses a fixed time interval (usually 60 seconds) to generate a new password. The dynamic factor will change with the time cycle. To avoid authentication failure caused by the out of time synchronization between authentication server and token, there usually is a small allowed time error.

1.1.2 Event based token

Event based tokens use the times of generated dynamic passwords as a dynamic factor. The dynamic factor will change once, as users use the token to generate a new password. The dynamic factor used by the authentication server and password token should be synchronized, but it is difficult to realize the synchronization absolutely, thus the event based authentication also allows the dynamic factor to have some small error.

1.1.3 Challenge response based token

The dynamic factor used by a challenge response based token is generated randomly by the authentication server, and after use it will be disabled. There is no error in event based dynamic factor, therefore challenge response based token can use dynamic factor synchronization.

1.2 Advantages of dynamic password

1.2.1 Dynamic

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

1.2.2 Valid only one time

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

1.2.3 Random

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

1.2.4 Easy to use

Dynamic password technology is easy to use, there is no need for the user to remember a password, they only need to read the password from the token.

1.2.5 Loss report

As the user always keeps the token with them, the loss of a device will be noticed immediately and report it as lost to the administrator who will be able to disable the token, reducing risks caused by the loss.

1.2.6 Protection against Trojans/Network interception

As the newly generated password is only valid once, it protects against peeking, Trojans and network interception.

1.2.7 Protection against brute force attack

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

1.2.8 Economic

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

1.2.9 Computer-independent

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

Chapter 2: UniOTP dynamic password authentication system

UniOTP dynamic password authentication system is a dynamic password authentication technology based authentication platform, designed to provide authentication, confidential information protection and financial security for users.

2.1 System introduction

UniOTP dynamic password authentication system is a strong authentication solution based on dynamic password authentication technology. UniOTP dynamic password authentication systems follow the OATH standard dynamic password generation algorithm. HOTP/TOTP fully supports the Radius authentication protocol and uses ODBC database access method. With the features of high reliability, openness, easy maintenance, easy expansion and high availability, this system can provide protection for various needs.

2.2 Product composition and features

UniOTP dynamic password authentication system product composition:

UniOTP dynamic password authentication system

- Authentication Server
- Information Management System
- Authentication Service Control tool
- Authentication Agent
- Secondary development SDK of agent
- Secondary Authentication Service development SDK
- Password Token
- Documentation

2.2.1 Authentication Server

Authentication server is used to process authentication requests. It fully supports the Radius authentication protocol. To authenticate clients, administrators only need to pack accounts, dynamic passwords and static passwords by their Radius authentication client (supported by application system or using an authentication agent) and submit to authentication server. That authentication system reads information related to that client's account and implements authentication, and then sends the authentication result back to client. If that client use a challenge response based token, the server will start a challenge authentication. Additionally, the authentication server also provides risk warning, logging, and local authentication information synchronization support.

2.2.2 Information Management System

Information management system is a Web information management based tool. As this tool is based on the Web, it can easily use remote management, maintenance, draw statistics and analysis, including token, user and log information etc. this system has strict multiple-level access control to protect the security of user information.

2.2.3 Authentication Service Control Tool

Authentication service control is a desktop application (Windows version), which facilitates administrators to configure and monitor the authentication server.

2.2.4 Authentication Agent

Applications which do not support Radius authentication protocol can be integrated into the UniOTP authentication system by the authentication agent. The Agent plays the role in information transmission between application systems and authentication service, which packs the authentication information submitted by application systems, and decodes the authentication response.

2.2.5 Secondary Development SDK of agent

User use interface functions to implement secondary development, in order to integrate the UniOTP authentication system, which uses the dynamic password authentication function. Currently supported languages are:

C, C++, Java, C#, PHP.

2.2.6 Secondary Authentication Service Development SDK

Secondary authentication service development SDK is used to develop server side dynamic passwords and implement dynamic password authentication. Using this method, the requirement for an authentication server is not necessary, as the application server will work as the authentication server.

2.2.7 Password Token

Password token distributed to end-users

2.2.8 Documentation

Documents about the UniOTP dynamic password authentication system, including help, technical and maintenance documents.

2.3 Platform support

2.3.1 Operating System Support

UniOTP authentication service can work cross platform, on Windows series, Linux and Unix systems, which provides customers, using different platforms, with a unified dynamic password authentication service

2.3.2 Database support

UniOTP authentication service supports multiple databases, including Oracle、SQL Server, PostgreSQL, MySQL etc, which are used for the ODBC database access method. It can cover the differences between different databases, and satisfy customer demands in different environments.

2.3.3 Information Management System Support

UniOTP information management system uses the B/S structure, developed in PHP. Any platform which can run PHP scripts can be used as the server platform for information management systems.

2.4 Applied Protection System

Systems which support the Radius protocol can be integrated into the UniOTP authentication system seamlessly.

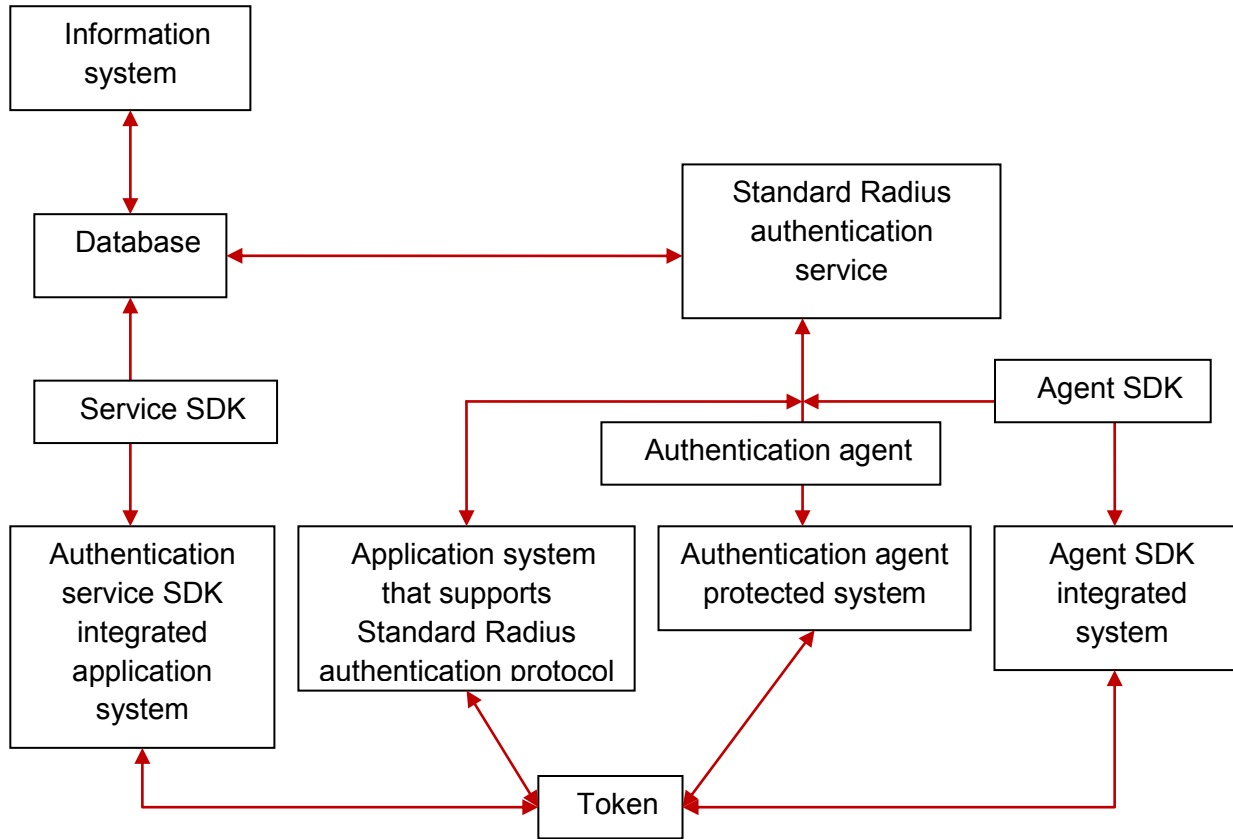
Systems which support some specific third-party authentication can be integrated into UniOTP authentication system by the authentication agent.

Through the authentication agent SDK, it is possible to add an authentication module to integrate into UniOTP authentication system.

Through service SDK, it is possible to add a dynamic authentication service function to your current system.

2.5 UniOTP System Structure

2.5.1 UniOTP authentication system integration structure



2.6 LDAP Protocol Support

UniOTP supports existing users in an application system by the LDAP protocol, and can be integrated into user management production which supports LDAP protocol.

2.7 Core functions of UniOTP Dynamic Password Authentication System

As a dynamic password authentication platform, the core functions of UniOTP dynamic password authentication system is the dynamic password authentication, token and user information management, server configuration (agent configuration) and log management.

2.7.1 Dynamic Password Authentication

UniOTP provides an authentication service verifying dynamic passwords or PIN and sends the authentication result back to authentication requesting clients.

2.7.2 Token Management

Operation includes import, delete, reclaim, distribute and repair (synchronize) token.

2.7.3 User Information Management

Functions include: add, import, delete, information update, loss report, activation and information search.

2.7.4 Server Configuration

Configure the authentication server performance features and optional functions as well as configure and manage agent.

2.7.5 Log Management

Manage log record, classifying queries, backup, export, and view data statistics.

2.7.6 Risk Warning

When information is exposed to a potential risk, user accounts will be locked automatically and a warning email will automatically be sent.

2.8 UniOTP dynamic password authentication features

2.8.1 Cross-platform

UniOTP dynamic password authentication system supports popular operating systems: Windows series, Macs, Linux and Unix etc.

2.8.2 Multiple database support

UniOTP dynamic password authentication system supports popular databases such as: Oracle, SQL Server, MySQL and PostgreSQL etc.

2.8.3 Web Server

Information management systems supported Web servers are IIS and Apache etc.

2.8.4 Multiple Secondary Language Development SDK

Secondary development SDK's included are: C, C++, java, C# and PHP

2.8.5 Variety of potential implementations

Seamless integration with Radius protocol supported system

Integration through authentication agent and SDK agent as well as adding a dynamic password authentication function to existing servers through the authentication SDK

2.8.6 Multiple Standards Support

- OATH event based OTP algorithm HOTP
- OATH time based OTP algorithm TOTP
- Radius authentication protocol
- LDAP protocol

2.8.7 Flexible server configuration

Customers can setup a suitable function by configuring to their requirement to ensure optimal performance.

2.8.8 Customization

- Token customization (colour, style and dynamic password length)
- Authentication service customization
- User interface customization
- System integration customization

APPENDIX

Symbol/Abbreviation	Description
OTP	Dynamic password or one-time password
HOTP	Event-based dynamic password
TOTP	Time-based dynamic password
Radius	Remote Dial-In User Service Protocol
PIN	Personal identification number
LDAP	Lightweight Directory Access Protocol
Event-based Token-related symbols, terminology and abbreviations	
Certification base	Event Dynamic factor used to generate dynamic password by HOTP
Authentication window	the maximum number of password of the password sequence, which is used by server to match the password provided by user in an authentication process
Token synchronization status	Token generate password within the scope of authentication window
Token overflow	Token generated password exceeds the scope of authentication window
Token synchronization	After token overflow, correct token generated password in order to make token generate password within the scope of authentication window
Token synchronization window	The maximum number of password of password sequence, in token synchronization process

Time-based token-related symbols, terminology and abbreviations	
Previous authentication time	The most recent successfully using dynamic password certification time
Certification base	The certification counts cumulation (used to solve the accumulated time error)
Authentication window	the maximum number of password of the password sequence, which is used by server to match the password provided by user in an authentication process
Token synchronization status	Token generated password within the scope of authentication window
Token overflow	Token generate password exceeds the scope of authentication window
Token synchronization	After token overflow, correct token generated password in order to make token generate password within the scope of authentication window
Token synchronization window	The maximum number of password of password sequence, in token synchronization process
Challenge/response-based token-related symbols, terminology and abbreviations	
Certification status	Used to record the response of the authentication server Certification status flag value is “0” or challenge information is out of the valid time of the authentication server will launch a challenge or reject the access request for this authentication request, otherwise the server will implement dynamic password authentication.
Challenge to validity	The valid response time of the challenge information started by server (default by 10 minutes)

File types	
.uinf	Token file
.con	Configuration file
Authentication server	
Authentication service	Used to process server side dynamic password authentication request applications
Authentication proxy	Middle module used to information exchange between application system authentication service
Token binding	When add new users, allocate token to users, and associate token with users
Token serial number	The unique Token ID
Shared secret key	Secret key information used to generate dynamic password
Radius share secret key	Encryption key used for communication between Radius client and server

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.