

# UniOTP Authentication System

## White Paper

**SecuTech Solution Inc.**

**<http://www.esecutech.com>**

Date	Version	Modify
2011-4-20	V1.0	First edition

## Contents

Symbol Convention .....	3
1. Outline.....	4
2. Dynamic password technology.....	5
2.1 About dynamic password technology .....	5
2.2 advantages of dynamic password.....	6
3. UniOTP dynamic password authentication system .....	8
3.1 system introduction .....	8
3.2 product composition and reatures .....	8
3.3 platform support.....	10
3.4 Applied Protection System .....	10
3.5 UniOTP System Structure .....	11
3.6 LDAP Protocol Support.....	11
3.7 Core Function of UniOTP Dynamic Password Authentication System.....	11
3.8 UniOTP dynamic password authentication features .....	12

## Symbol Convention

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 type	
.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

## 1. Outline

As the development of the information technology, information communication 在信 in people’s life becomes more and more important, and brings great convenience and economic benefits. But because more and more people are familiar with computer

technique, many network attack techniques are invented, which extremely threat the information security. As the first network security point, authentication plays critical rule, but the traditional static password authentication which are widely used authentication method is encountering many attacking technology and cannot protect information effectively.

The vulnerability and disadvantage of traditional static password are as follows:

1. With the development of attacking technology, to ensure the security of password in a certain period, passwords become longer and longer, therefore to remember these passwords easily user usually use regular personal information, which increases the danger of passwords.
2. The occasions to use password is increasing, and it becomes a burden to remember so many passwords.
3. If the static password is not modified frequently, the security will reduce gradually over time increase.
4. Static password seems powerless in response to Trojan networking hijacking, spying and other attacks.

The static password disadvantages described above are the main aspects of security risk. Bad User habits, such like using the same password for many accounts and keep password in a place, will cause information leakage. Once user password is cracked, the economic lost will be very serious. In this case, dynamic password shows better performance in anti-attacking aspect, so that in authentication field, it becomes more and more popular.

## **2. Dynamic password technology**

### **2.1 About dynamic password technology**

Dynamic password is an authentication technique which generates dynamic password for authentication. The basic theory is that the encryption key and encryption algorithm are stored both in server and token. The token and server generate dynamic password 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, user use a password for this authentication generated by using his/her token, and meanwhile the authentication server will generate a password by using the same encryption algorithm and password. By comparing two passwords, the authentication process is realized. According to different dynamic factor changing mechanisms, the dynamic password token can be classified into time based token which uses time as dynamic factor, event based token which use frequency of password generation and challenge response based token which use challenge information sent by server as dynamic factor.

### **1. Time Based token**

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

### **2. Event based token**

Event based token uses the times of generated dynamic password as dynamic factor. The dynamic factor will change once, as users use token to generate a new password. Obviously, the dynamic factor in authentication server and password token should be synchronized, but in fact, it is difficult to realize the synchronization absolutely, thus the event based authentication also allows dynamic factor to have error. If the error of dynamic factor in token and authentication server is within the allowed range, it will implement authentication and execute dynamic factor.

### **3. Challenge response based token**

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

## **2.2 advantages of dynamic password**

### **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. Valid only one time**

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

## **3. Random**

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

## **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.

## **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.

## **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.

## **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)

## **8. Economic**

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

## **9. Computer-independent**

The dynamic password Token has a LED display and so, 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 , 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. 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.

#### **3.1 system introduction**

UniOTP dynamic password authentication system is a strong authentication solution based on dynamic password authentication technology. UniOTP dynamic password authentication system following the OATH standard dynamic password generation algorithm - HOTP/TOTP fully supports 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.

#### **3.2 product composition and reatures**

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

|--Document

##### **Authentication Server**

Authentication server is used to process authentication request. It fully supports Radius authentication protocol. Authentication client just needs to pack accounts, dynamic password and static password by Radius authentication client (supported by application system or using authentication agent) and submit to authentication server.



Authentication system reads information related to client accounts and implements authentication, and then sends the authentication result back to client. If clients use challenge response based token, the server will start a challenge authentication. Additionally, authentication server also provides risk warning, logging, and local authentication information synchronization support.

### **Information Management System**

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

### **Authentication Service Control Tool**

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

### **Authentication Agent**

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

### **Secondary Development SDK of agent**

User use interface functions to implement secondary development, in order to integrate into UniOTP authentication system, which realize the dynamic password authentication function. Currently, it supports C、C++、Java、C#、PHP.

### **Secondary Authentication Service Development SDK**

Secondary authentication service development SDK is used to develop server side dynamic password and implements 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.

### **Password Token**

Password token distributed to end-users

## **Document**

Documents about UniOTP dynamic password authentication system, including help document, technical document and maintenance document

## **3.3 platform support**

### **3.3.1 Operating System Support**

UniOTP authentication service can work cross platform, such like Windows series, Linux and Unix system, which provides customers, using different platform, with a unified dynamic password authentication service

### **3.3.2 Database support**

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

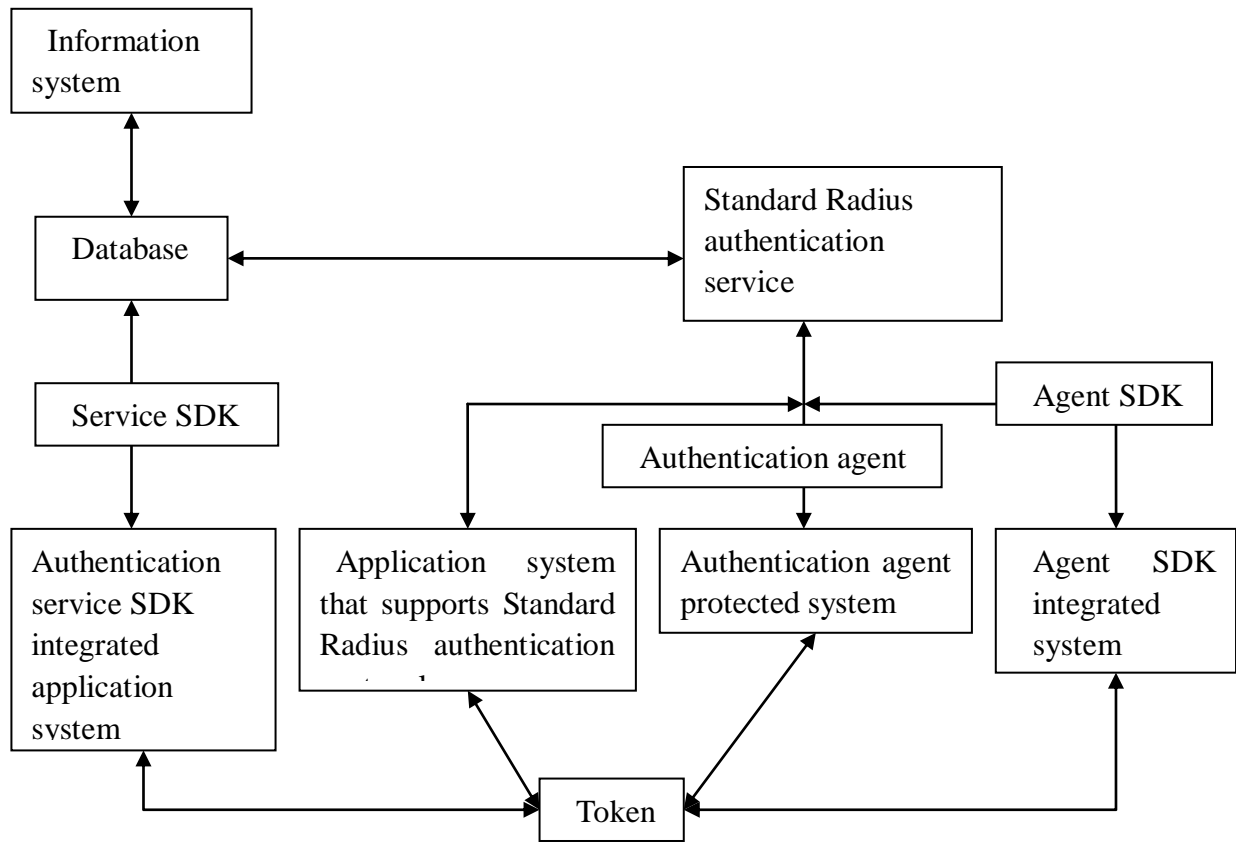
### **3.3.3. Information Management System Support**

UniOTP information management system is using B/S structure, developed in PHP. Any platform which can run PHP scripts can be used as server platform of information management system.

## **3.4 Applied Protection System**

1. Systems which support Radius protocol can be integrated into UniOTP authentication system seamlessly by configuration.
2. Systems which support some specific third-party authentication can be integrated into UniOTP authentication system by authentication agent.
3. Through authentication agent SDK to add authentication module integrate into UniOTP authentication system.
4. Through service SDK add dynamic authentication service function for current system.

### 3.5 UniOTP System Structure



### UniOTP authentication system integration structure

### 3.6 LDAP Protocol Support

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

### 3.7 Core Function of UniOTP Dynamic Password Authentication System

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

### **3.7.1 Dynamic Password Authentication**

It provides authentication service verifying dynamic password and PIN and sends the authentication result back to authentication requesting clients.

### **3.7.2 Token Management**

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

### **3.7.3 User Information Management**

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

### **3.7.4 Server Configuration**

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

### **3.7.5 Log Management**

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

### **3.7.6 Risk Warning**

When information is exposed to potential risk, user account will be locked automatically and send warning email.

## **3.8 UniOTP dynamic password authentication features**

### **1. Cross-platform**

UniOTP dynamic password authentication system supported operating systems are Windows series, Linux and Unix etc.

### **2. Multiple database support**

UniOTP dynamic password authentication system supported databases are Oracle, SQL Server, MySQL and PostgreSQL etc.

### **3. Web Server**

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

4. Multiple Secondary Language Development SDK

C secondary development SDK

C++ secondary development SDK

Java secondary development SDK

C# secondary development SDK

PHP secondary development SDK

5. A variety of implementation

Seamless integration with Radius protocol supported system

Integration through authentication agent

Integration through SDK agent

Add dynamic password authentication function to existing server through authentication SDK

6. Multiple Standards Support

Support OATH event based OTP algorithm HOTP

Support OATH time based OTP algorithm TOTP

Support Radius authentication protocol

Support LDAP protocol

7. Flexible server configuration

Custom can choose suitable function by configuration according to requirement to ensure optimal performance.

8. Customization

Token customization (color, style and dynamic password length)

Authentication service customization

User interface customization

System integration customization