



UniOTP[®] Quick Start

300 | 310 | 500 | 510



SecuTech Solutions PTY LTD.

Phone: +614 03 003 500

Support: eSecuTech.com/support

Email: support@esecutech.com

Website: www.esecutech.com

SDK: esecutech.com/sdk

SDK password: opensesame

UniOTP Family ○

UniOTP 300 and 310



- ✓ HOTP/Event based token
- ✓ Dynamic authentication
- ✓ Cryptographically secure
- ✓ Tamper resistant design

UniOTP 300 and 310



- ✓ HOTP/Event based token
- ✓ Dynamic authentication
- ✓ Cryptographically secure
- ✓ Tamper resistant design

Table of contents

- 00 Product family
- 01 Table of contents
- 02 Product Overview
- 03 Remarks for UniOTP
- 04 SDK Checklist
- 05 Preparation
- 06 Guide to the SDK
- 07 Secure user authentication solution
- 08 Integration
- 09 Effect of UniOTP
- 10 General guide
- 11 Example Windows guide
- 12 Example Windows guide
- 13 OEM Customization
- 14 Frequently asked questions
- 15 Frequently asked questions
- 16 Frequently asked questions

Product Overview

- ✓ UniOTP 300 and 310 are event or OATH HOTP based authenticators. They generate a new one time password when the button is pressed on the token. Each password will only be displayed for 60 seconds.
- ✓ UniOTP 500 and 510 are time or OATH TOTP based authenticator. With an accurate clock inside, they automatically generates and displays a new password every 60 seconds. The hardware device is synchronized with the authentication server.
- ✓ All tokens have globally unique serial numbers on their back, this is required for identifying tokens with their unique serial key.

Remarks for UniOTP

- ✓ The UniOTP requires the installation of a client side agent and authentication server for handling user authentication
- ✓ As all UniOTP's are OATH compliant and certified they are compatible with 3rd party tools, SecuTech is moving towards using such tools, however legacy versions of the management, user and server authentication tools exist, please contact support@esecutech.com.

Checklist

The UniOTP SDK includes

- ✓ The UniOTP token and secret key (sent separately, please contact sales@esecutech.com)
- ✓ Secret key format converter and trouble-shooter
- ✓ UniOTP brochures, datasheets and documentation
- ✓ Server and client programming API and database SQL scripts
- ✓ TinyCore Linux with MultiOTP and Samba4 disk image

Preparation

For Computer

- ✓ Please view the guides before using the UniOTP as it requires a server to integrate with, if a computer has installed a logon agent without a reachable server for authentication, the user will be locked out of their computer. In this event the only option available is use another operating system.
- ✓ On the server computer, please install a server for the UniOTP tokens and connect it to a configured database of your preference. Please ensure that a user management system is also installed and connected to this database before using any logon credentials installation.
- ✓ Please ensure that the correct configurations are made to the router and firewall to allow the UniOTP server to operate and that the connection has been tested.
- ✓ We recommend using MultiOTP or RC Dev's user management and authentication servers and pGina or Samba 4 for user authentication (please note that Samba4 can be used in conjunction with Windows active directory, pGina replaces it).

Guide to the SDK

After obtaining a copy of the UniOTP SDK, please read the Readme file located in the root directory of the UniOTP SDK.

The following is an outline of the folder contents in the UniOTP SDK:

- ✓ Documents: Provides documentation for the UniOTP
- ✓ Client agent library and sample: Provides developers with the API for the client
- ✓ Server authentication library and sample: Provides developers with the API for the server
- ✓ Solutions: Contains usage guides for the UniOTP
- ✓ Token tools: TinyCore disk image and secret key format converter and trouble-shooter

Secure user authentication solution

Using the secure user authentication provided by UniOTP allows administrators to ensure that unwanted access is prevented by providing protection from man in the middle, brute force , Trojan, network sniffing and replay attacks as well as password theft.

Integration

The UniOTP can be integrated with a server using the RADIUS protocol or through a bridge such as a PHP post call, based on your preference. UniOTP is extremely flexible and SecuTech provides API's for seamless integration into existing systems and can be customized for special conditions such as different TOTP recycle times, please contact sales@esecutech.com for more details.

The effect of UniOTP

The UniOTP offers advanced protection from almost all forms of attacks that are used to gain illegal access and has many different possible applications, not just securing access to a VPN or a computer. The ease of use provided by UniOTP where the end user inputs the key from the token when requested means that they do not need to remember any new details or codes , and if the token is lost the codes it generates can be invalidated by the server remotely via user management.

General guide

Installing the UniOTP onto a network is a very quick process and for the standard setup will take approximately 30 minutes to complete. Note that you may choose to use your own tools, however it is still recommended that the guide is reviewed as it best practices, server and inbound/outbound traffic configuration. The majority of the process has already been completed for you with the tools provided in the SDK, but there is no limitation on the amount of customization that an administrator can perform.

As an example, when logging into an operating system integrated with UniOTP, the typical end user's experience through the default installation is the standard credentials login with username and password, and then they are required to input the OTP code from the token. The user name and OTP is sent to the server and validated behind the scenes and is not performed on the local machine, or if no network connectivity is possible the computer itself may have a local authenticator.

Example Windows guide

For Windows Users using MultiOTP and pGina

- ✓ **UniOTP API**
Samples, libraries and manuals for the API's are provided in the SDK for both the server and client and is supported in C, C++, PHP and Java for 32 and 64 bit computers, and in C# for 32 bit.
- ✓ **Management system**
MultiOTP provides a web based user and token management tool.
- ✓ **Secure login credentials agent**
pGina provides integration with the Windows log in screen and configuration and testing tools to connect to the authentication server. The RADIUS plugin should be installed to facilitate this.
- ✓ **Authentication server**
MultiOTP provides both a RADIUS and PHP authentication server, please ensure that the RADIUS protocol port is not blocked on your network (default 1812).

Example Windows guide

For Windows Users using MultiOTP and pGina

- ✓ First install MultiOTP and import UniOTP using the web administration tool via XML formatted secret key files. Next, please synchronize users and tokens as the authentication server relies on users and tokens to be synchronized and configured.
- ✓ Finally install pGina on the client machine and use it's testing tools to confirm that the server is reachable. Typically the router's firewall will block authentication requests on port 1812, please forward this port to your authentication server. Note that the shared key from MultiOTP is default: MySharedSecret.

UniOTP Customization

- ✓ UniOTP products come with a wide range of OEM customization options to suit your business's many needs.
- ✓ Some of these customization options include: LOGO laser engraving, Case Design/Modification options, Custom color options, as well as Custom LOGO service.
- ✓ please contact sales@esecutech.com for more information.

Frequently Asked Questions



What is UniOTP?

UniOTP is SecuTech's OATH one time password user authentication tool designed to maximize security whilst preserving ease of use.



How does UniOTP work?

UniOTP authentication prompts the user for a user name and dynamic one time password, which is then sent to the authentication server for validation. Once validated the user is then granted or denied access to their current operation and can be used in conjunction with an existing authentication system. The one time password is generated with a random number generator chip which the server replicates as well. Once a password has been used it can not be used again.

Frequently Asked Questions



Can I merge UniOTP tokens with my management system?

UniOTP provides support for XML PSKC token file formats which is OATH compliant. Administrators only need to import this token file to their OTP management system to synchronize with UniOTP tokens.



How can I use OTP if I do not have an OTP management system?

SecuTech provides a Linux disk image with management system which can be deployed directly, this system can be found inside the UniOTP SDK. Alternatively, you can use other certified OTP management system, please contact sales@esecutech.com for more information.

Frequently Asked Questions

- ✓ ***How can I use UniOTP if a value within the XML PSKC token file doesn't support my OTP management system?***

Customization services of UniOTP are available, please contact support@esecutech.com for customization values within the XML PSKC token file.

- ✓ ***What should I do if my UniOTP is locked?***

If the user account associated with your UniOTP device is locked, please contact the administrator of your management service to unlock your user account. If you have locked yourself out due to a connection failure please remove the OTP installation directly by using another operating system and accessing the hard drive.

- ✓ ***Who can I contact for more help?***

If you have any questions, please feel free to contact us at esecutech.com/support or support@esecutech.com.

SecuTech Warranty Policy

- ✓ When you buy a product from SecuTech, the product comes with guarantees that cannot be excluded under the Australia consumer law.
- ✓ You are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage.
- ✓ You also are entitled to have the products repaired or replaced if the products fail to be of acceptable quality and the failure does not amount to a major failure.

The relevant guarantees are as follows

- ✓ **Quality** – Products supplied by SecuTech must be of acceptable quality. The test for acceptable quality is whether a reasonable product, fully aware of the state and condition of the products, would find them
 - ✓ *Safe, durable, and free from defects;*
 - ✓ *Acceptable in appearance and finish; and*
 - ✓ *Fit for all the purposes for which goods of what kind are commonly supplied.*This must take into account the nature and price of the products, and any statements on packaging or labeling.

- ✓ **Description** – Products supplied by SecuTech must match the description provided by SecuTech.
- ✓ **Sample** – Products supplied by SecuTech must match any sample shown to you by SecuTech.
- ✓ **Title** – A customer who purchases a product from SecuTech must receive clear title to the product.
- ✓ **Due Care and Skill** – Services provided to you by SecuTech must be provided with due care and skill.
- ✓ **Express warranties** – SecuTech will be legally required to comply with the express warranty that is set out in its items and conditions.
- ✓ **Reasonable time** – Repair services provided by SecuTech must be provided with a reasonable time.

If you think you are entitled to any of the above remedies, please contact SecuTech at sales@eSecuTech.com .

For further information on consumer rights, visit

www.consumerlaw.gov.au and

www.accc.gov.au/consumerguarantees .



APAC

Suite 2.06, 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/F: +33-426002810

M: +33-609396463

E: Europe@eSecuTech.com

China

Level 4, #43 Building,
#8 Dong Bei Wang Xi Lu,
Beijing, 100193

T: +8610-8288 8834

F: +8610-8288 8834

E: CN@eSecuTech.com