

SecureMetric Technology

SecureOTP One Time Password Security

Layered Security Defense for Your System



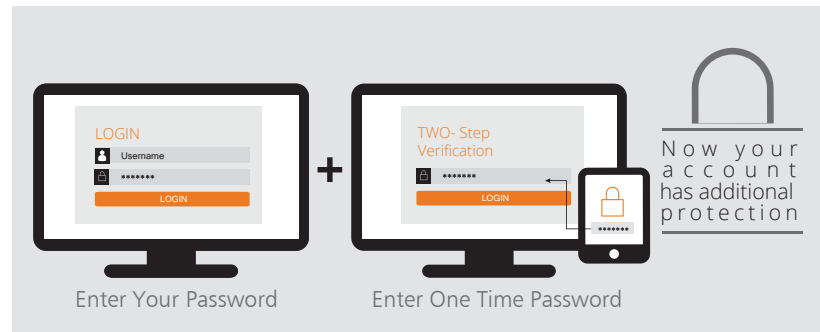
About SecureOTP

SecureOTP is a secure One Time Password (OTP) token that offers strong Dynamic Password with 2 Factor Authentication (2FA). It is based on an advanced microprocessor chip that eliminates the risks presented by static, shared or easily guessed and stolen passwords. No more memorizing or creating compliantly. Simply click the button, and the passwords will be generated automatically.

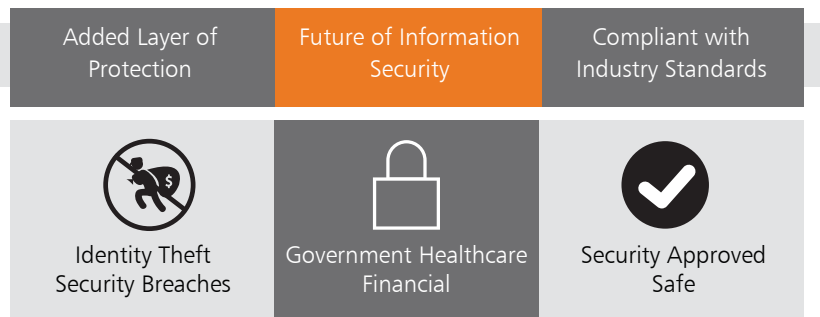
The OTP platform is developed based on OATH (Open Authentication Technique), an industry wide collaboration on OTP standard. It is designed for maximum (SECURITY), yet easy to Deploy and User-Friendly. It can be seamlessly integrated with any other 3rd party Authentication Server that supports OATH standard. As a Non-Connected-security-device, no software or driver installation is needed. It is completely portable to use anytime, anywhere.

SecureOTP is designed to support strong crypto algorithms where the algorithms' computation is done completely on hardware and isolated from the computing environment for better security. SecureOTP is a Tamper Proof token where the data will self destruct once the token is physically broken.

WHAT is 2-Factor Authentication?



WHY use 2-Factor Authentication?



SECUREOTP *Event*

OATH Compliant Event Based OTP Token

The input value will be combined with the initiated secret key inside the token and generate the required One-Time-Password.



SecureOTP Event offers strong 2-Factor Authentication through Event synchronous One Time Password technique or Event based One Time Password. Each time a user presses the token's button, the input value will be combined with the initiated secret key inside the token and generate the required One Time Password. Event based One Time Password will have no expiry time. It is more convenient for users who prefer great user friendliness.

Feature Highlights

- Event-based synchronous
- 8-bit Microprocessor Smart Chip based
- Compliance to OATH event-synchronous algorithm (HOTP)
- 6 digits (can be customized up to 8 digits) LCD screen
- Seamless integration with 3rd party OTP authentication system
- Globally Unique Serial Number
- Onboard OTP generation
- Trendy hard molded plastic (ABS)
- Water Resistance with IP54 certified
- Tamper Proof case
- RoHS compliant
- Zero footprint authentication
- Zero Client Software Installation

SECUREOTP *Time*

OATH Compliant Time Based OTP Token

The One Time Password will change every 30 seconds or 60 seconds.



SecureOTP Time offers One Time Password where the security cryptography is synchronized based on the token's real time clock and the server time. Simply press the button and SecureOTP Time will display a secure One Time Password which is generated based on the current time and the initiated secret key. The One Time Password will change every 30 seconds or 60 seconds. A short validity of the One Time Password prevents someone from "stealing" the password and performing any harmful activities after the valid interval.

Feature Highlights

- Time-based synchronous with 30 seconds or 60 seconds validity
- 8-bit Microprocessor Smart Chip based
- Compliance to OATH time-synchronous algorithm (TOTP)
- 6 digits (can be customized up to 8 digits) LCD screen
- Seamless integration with 3rd party OTP authentication system
- Globally Unique Serial Number
- Onboard OTP generation
- Trendy hard molded plastic (ABS)
- Built in real time clock
- Water Resistance with IP54 certified
- Tamper Proof case
- RoHS compliant
- Zero footprint authentication
- Zero Client Software Installation

SECUREOTP CR

OATH Compliant Challenge - Response OTP Token

Challenge Response is designed to be a 2-way authentication.



SecureOTP CR is built based on OATH Challenge Response Algorithms (OCRA) which enables a real time 2-Factor Authentication that can prevent common threat from Man In The Middle Attacks. Challenge Response is designed to be a 2-way authentication.

The user will key in the correct Challenge phrase, which will then activate the token to generate a Response, i.e. the One Time Password. This technique will prevent token not present mode where the user is always required to hold the token in order to proceed with the authentication process.

Feature Highlights

- 8-bit Microprocessor Smart Chip based
- Trendy hard molded plastic with high contrast LCD screen
- Large Key Pad
- Globally Unique Hardware ID
- Compliance to OATH (OCRA Algorithm)
- Seamless integration with 3rd party OCRA authentication system
- Onboard OTP generation based on random question
- Challenge Response based synchronous
- Support Zero footprint authentication
- Water Resistance with IP54 certified
- Zero Client Software Installation
- Tamper Proof case
- RoHS compliant

SECUREOTP Card

Dynamic Password Cards Provide Strong Authentication

SecureOTP Card provides strong OTP security and greater convenience for you by simply carrying it in your wallet.



The stylish SecureOTP Card from SecureMetric Technology is produced with vibrant customized artwork in a familiar credit card design. The display is a high contrast LCD screen with superb readability designed for maximum brightness in all types of lighting. It comes with an instantaneous refresh rate and the data is able to scroll across the screen providing access to large amounts of information.

SecureOTP Card provides strong OTP security and greater convenience for you by simply carrying it in wallet. In order to access online account, go through normal process and type in the unique numeric password generated by SecureOTP Card.

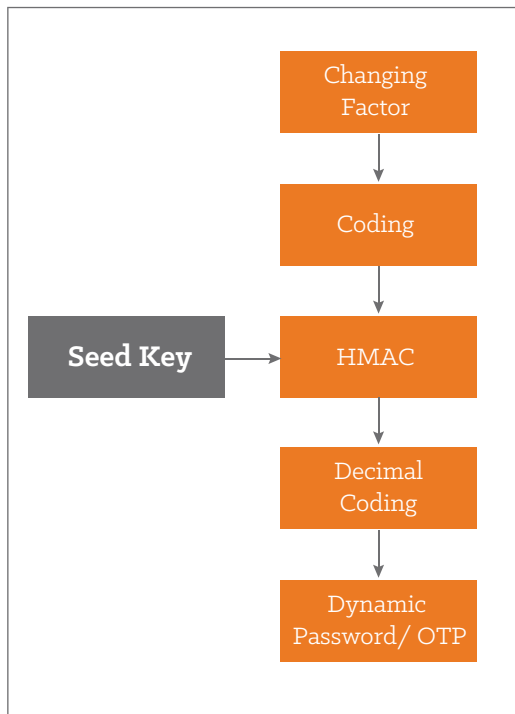
Feature Highlights

- Slim card design able to store in wallet
- Easy to use button triggers response and one time password
- Large and bright numeric display
- Convenient to use
- Enhance trust in online transactions
- No card reader necessary

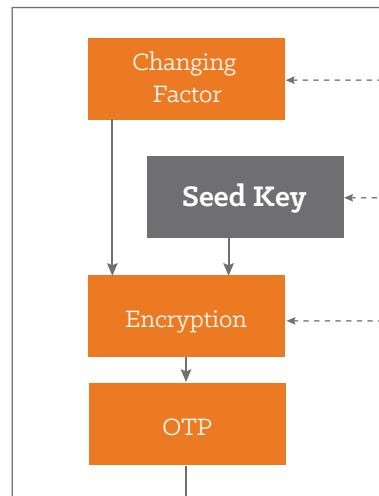
SecureOTP Token

How It Works?

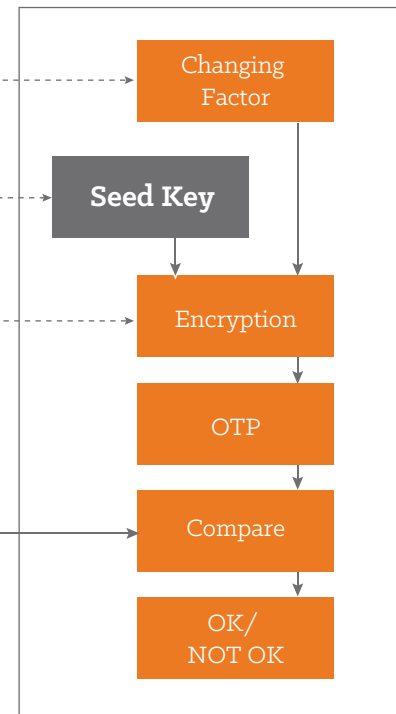
1 Calculation of Dynamic Password



2 Dynamic Password Token



3 Authentication Server



Online Security With

SOMETHING YOU HAVE
SOMETHING YOU KNOW

How OTPs are generated and distributed

- Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time)
- Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order).
- Using a mathematical algorithm where the new password is based on a challenge (e.g. a random number chosen by the authentication server or transaction details) and/or a counter.



Strong Security



Versatile



Cost Effective



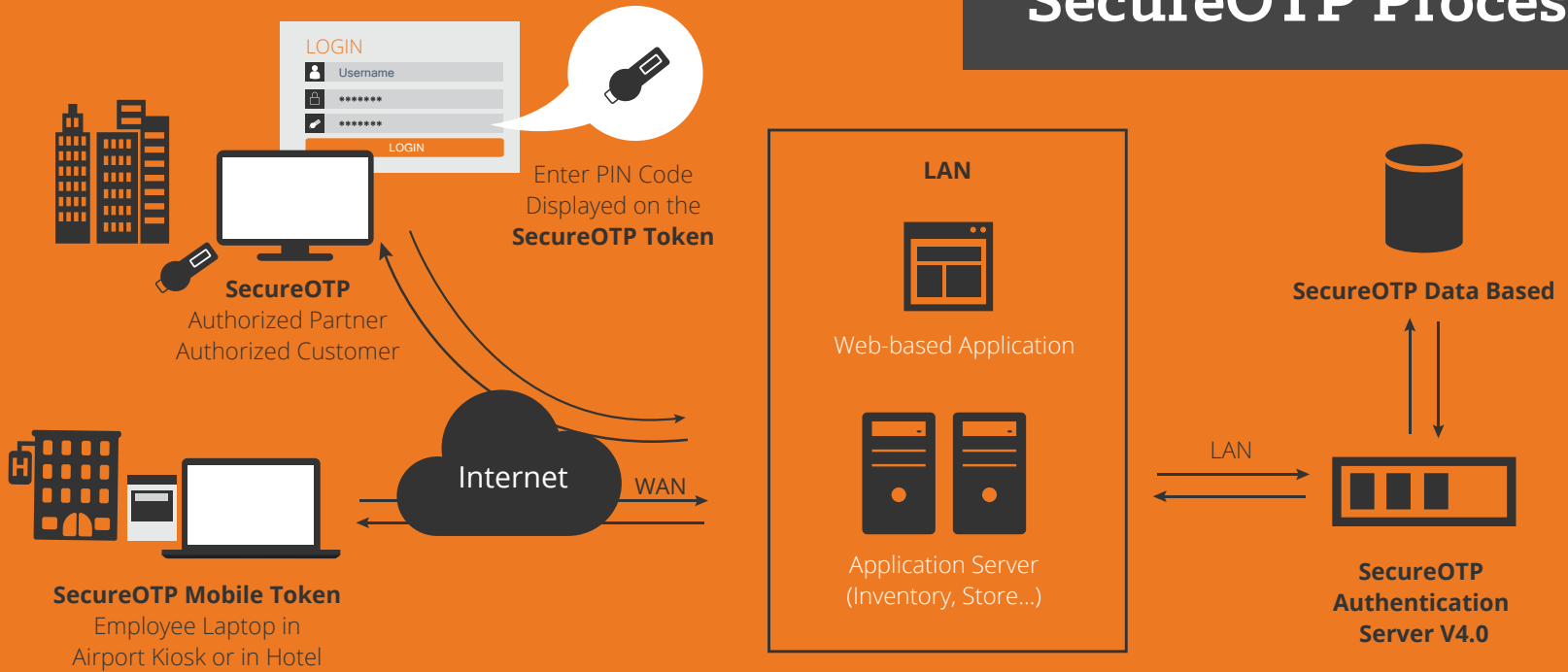
Portable



Easy

ADVANTAGES

SecureOTP Process



CHALLENGE RESPONSE

IS DESIGNED TO BE A
2-WAY AUTHENTICATION

In computer security, challenge-response authentication is a family of protocols in which one party presents a question ("challenge") and another party must provide a valid answer ("response") to be authenticated.



SECUREOTP Authentication Server V4.0

Introduction

With the development of computer technology, network technology and information technology, the system began to develop a variety of applications, from small to personal computer systems, large banks, securities, insurance, electricity, petroleum, petrochemical, health care, taxation, public security, fire, and government departments and other large applications. In order to protect the legitimate interests of the application system, owners and users of these applications generally provide identity authentication to ensure that only legitimate users can access applications.

SecureOTP Authentication Server V4.0 is mainly used to provide authentication services for applications based on dynamic password system to improve the application system authentication security, while improving ease of authentication system, convenience, reduce administrative identity authentication system and maintenance costs.

DATABASE SYSTEM

Basis for SecureOTP Authentication System V4.0 runtime environment. Since the database system is a generic third-party component, so the system is designed to use the various functions it provides, without doing too much attention to other aspects.

USER PORTAL

User portal uses web page form, users can easily operate independently for some token used to reduce the administrator's work stress.

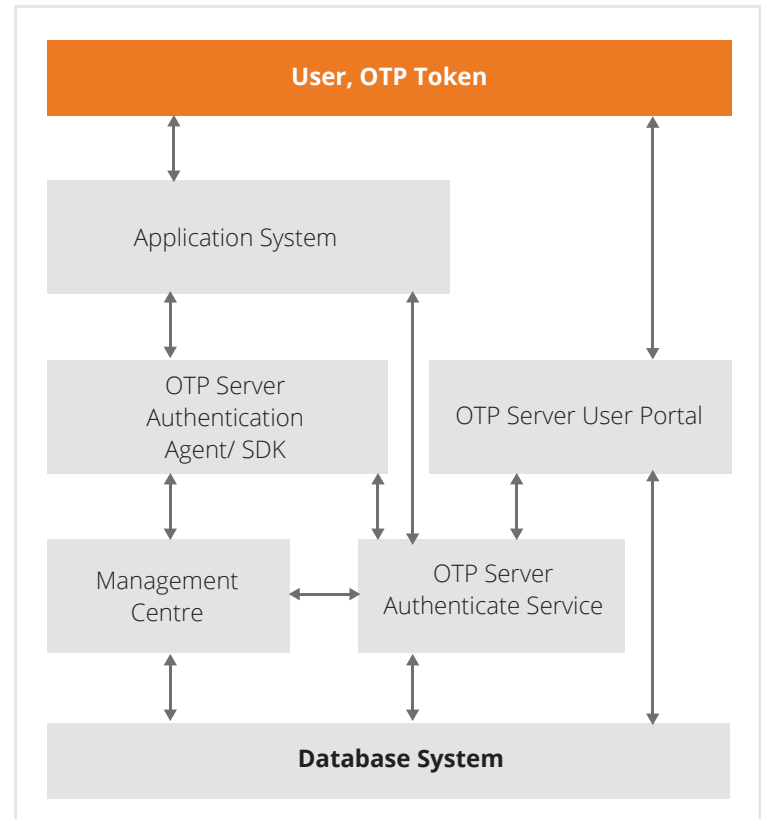
- **Binding Token Replacement Tokens**
- **Unlock Token**
- **Authentication Token**
- **Synchronous Tokens**
- **Report The Loss Token Solution Linked Token**
- **Get An Unlock Code**
- **Modify The Emergency Password**
- **Phone Token Distribute**
- **Modify Static Password and so on**

System Component

SecureOTP Authentication Server V4.0 is a secure authentication system platform that provides a systematic, complete authentication services. The system consists of authentication services / SDK, authentication agent / SDK, database systems, OTP management center, user portals, applications and dynamic tokens.

Authentication Services

Authentication services provider is based on dynamic password and authentication agent services. The authentication server needs the corresponding information from the database directly from agent API or received directly from application systems (such as RADIUS application) entered by user during authentication log in (such as account dynamic password, etc). The authentication server performs the user authentication, and then result is sent back to Agent API or application while the authentication server needs the authentication logs.



OTP Server Authentication System V4.0 Component

SecureOTP Authentication Server V4.0 as a professional Dynamic Password Authentication and Transaction Signature Verification Platform, in order to meet a variety of application environments and the complexity of the application requirements, the system provides a variety of features.



SECUREOTP Authentication Server V4.0

Environmental Adaptability

- Supports a variety of operating systems, including Windows and Linux, which supports 32-bit machines also 64-bit machines.
- Supports a variety of databases, including Oracle, SQL Server, PostgreSQL, MySQL, etc.
- Wide range of applications, can be used for almost anything that can be authenticated by digital information applications.

Integrated Convenience

- Can be authentication agents and application system integration, including Windows system registry, Linux system registry, IIS site login and OWA2007.
- Through RADIUS protocol and application systems integration.
- Via SDK interface and application systems integration. Interfaces include authentication server interface and authentication proxy interface. Language forms, including languages such as C and Java, supported platforms, including Windows and Linux.

PRODUCT SAFETY

- 01 Supports the token seed encryption and integrity checking
- 02 Supports Authentication Agent IP checks
- 03 Supports critical communications data encryption
- 04 Supports database access password encryption
- 05 Management Center Support restricting access to IP

EFFICIENCY

01

Supports ten million users, to meet the massive demand for user authentication.

02

Supports multi authentication server load balancing, support for concurrent requests 3000 times / sec or more.

03

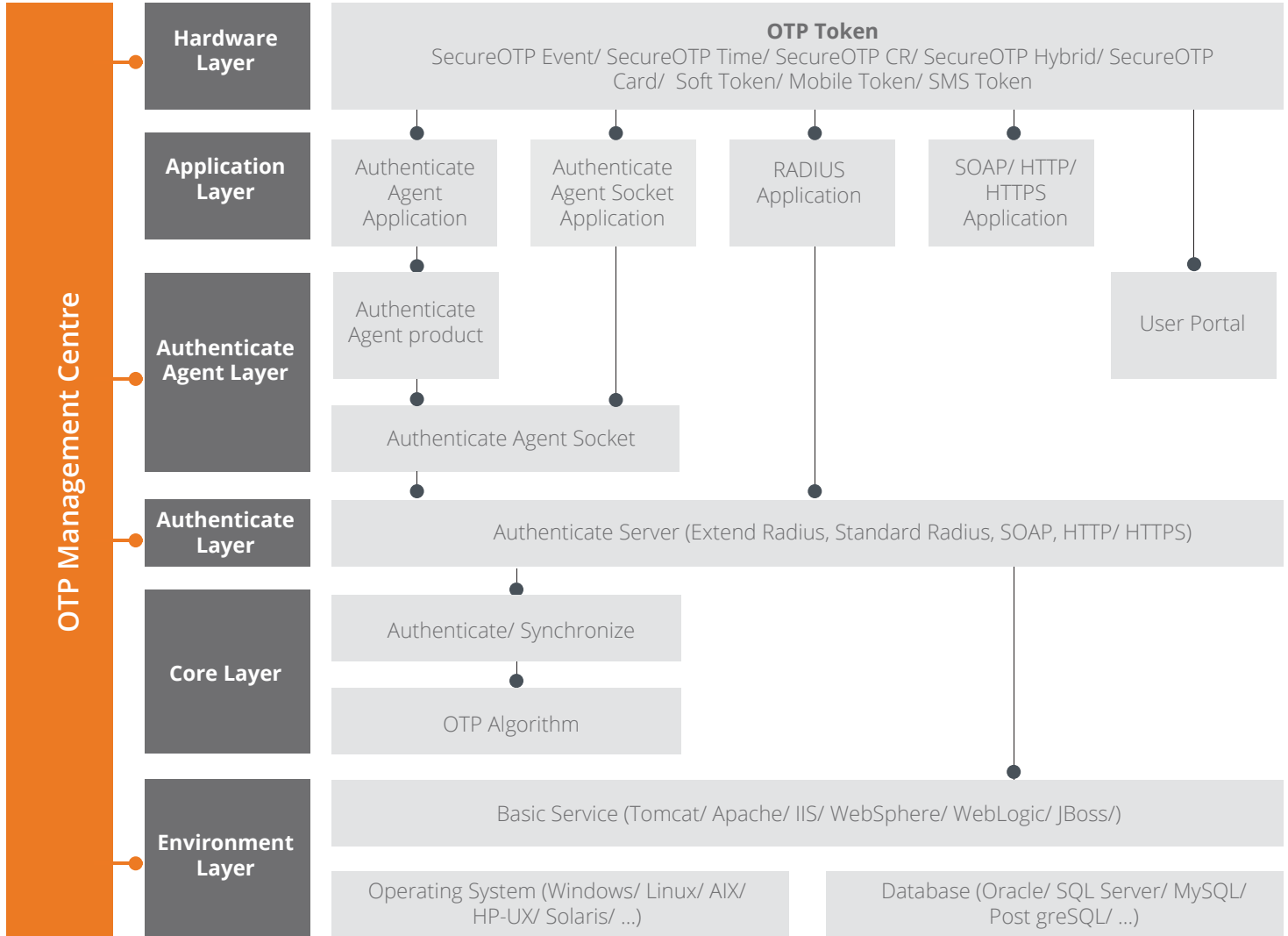
Supports multi authentication server cluster.

The main function of SecureOTP Authentication Server V4.0 is to provide authentication services for applications, according to user needs for security, can provide **Account + Dynamic Password** authentication mode, **Account + Static Password + Dynamic Password** authentication mode.

AUTHENTICATION FLEXIBILITY



- Multiple token types.
- Multiple authentication modes.
- Mutual authentication, ie. applications can authenticate the user, the user can also verify applications.
- Multiple token algorithms, HOTP, TOTP and OCRA algorithm include OATH organization, which also supports SM3 algorithms country dense.
- Forwarding the authentication request.



TECHNICAL SPECIFICATION

Model	SecureOTP Event	SecureOTP Time	SecureOTP CR
Hardware Platform	Secure 8-bit Microprocessor smart chip based		
Hardware Platform	OATH Event based	OATH Time based	OATH OCRA based
	Onboard OTP generation		
	Hard Molded Plastic (ABS)		Hard Molded Plastic (PC)
Token Casing	1 Press Button		Key Pad
	8 Digits LCD Screen		High Contrast LCD Screen
	Water Resistance (IP54 certified)		
	Tamper Proof		
	62mm x 27mm x 10mm dimension		73mm x 50mm x 5mm dimension
	12.3g Weight		21.3g Weight
	RoHS Compliant		
	Memory	Static Random Access Memory	
Power	Standard Lithium Battery		
	14,000 clicks or 3 to 5 years Battery Lifetime		10,000 clicks or 3 years Battery Lifetime
Working Environment	Operating Temperature between 0°C to 50°C		
	Storage Temperature between -20°C to 70°C		
	Humidity Rating of 0 to 100% without condensation		
Unique Identifier	Globally Unique Serial Number		
Middleware	N/A	N/A	N/A
USB Connection	N/A	N/A	N/A



KUALA LUMPUR (HQ)

SecureMetric Technology Sdn. Bhd.
2-2, Incubator 2, Technology Park
Malaysia, Lebuhraya Sg Besi -
Puchong, Bukit Jalil, 57000
Kuala Lumpur, Malaysia
T +603 8996 8225
F +603 8996 7225

HANOI

SecureMetric Technology Co., Ltd
203B, TDL Office Building,
No. 22, Lang Ha Street,
Dong Da District, Hanoi, Vietnam
T +84 4 3776 5410
F +84 4 3776 5416

JAKARTA

PT SecureMetric Technology
Komp. Ruko ITC Roxy Mas,
Block C2, No. 42, Jl. KH.
Hasyim Ashari,
10150 Jakarta, Indonesia
T +62 21 6386 1282
F +62 21 6386 1283

HO CHI MINH CITY

SecureMetric Technology Co., Ltd
L14-08B, 14th floor, Vincom Tower,
72 Le Thanh Ton, Ben Thanh ward,
District 1, Ho Chi Minh City, Vietnam
T +84 8 62 87 85 44
F +84 8 62 68 81 88

SINGAPORE

(Sales Representative Office)
105, Cecil Street, #06-01,
The Octagon,
Singapore 069534
T +65 6827 4451
F +65 6827 9601

MANILA

SecureMetric Technology, Inc.
Office 27, 7F BA Lepanto Building,
8747 Paseo de Roxas, Makati CBD,
Makati City 1226 Philippines
T +63 2 267 6797 +63 2 463 5634
M +63 932 8739046

YANGON

(Sales Representative Office)
3rd Floor, Building (8), Junction Square,
Pyay Road, Kamaryut Township,
Yangon, Myanmar
T +951 2304155
F +951 2304155



EAL



CE FC

www.securemetric.com

sales@securemetric.com