



# SECURETOKEN

## Public Key Infrastructure Security

SecureToken is an advanced secure microprocessor smart chip based USB token that integrates with powerful cryptographic technology designed for strong 2-Factor Authentication (2FA). It can be used to mitigate potential risk of unsafe traditional password based security for digital resources and transactions. SecureToken will make sure only authenticated user can gain access into sensitive data / information / system or authorized any crucial transaction. It enables secure 2FA which combines "What you have (SecureToken)" and "What you know (User PIN)" during the access authentication process.



## Architecture

SecureToken ST2 and ST3 are built based on 8-bit and 32-bit microprocessor smart chip respectively together with card reader in the single USB device platform. As secure smart card technology is still the most secure device platform that prevents hacking and hardware cloning. Thus SecureToken makes the most preferred choice for strong 2FA options.

SecureToken supports many popular onboard security algorithms such as RSA, DES, 3DES, MD5 and SHA-1. Onboard RSA key pair generation together with built-in advanced cryptographic functions with digital signing onboard, making it a powerful plug-in for Public Key Infrastructure (PKI) and Challenge Response Authentication implementation. As the middleware was designed to comply with

PKCS#11 and Microsoft CAPI standards, SecureToken can be seamlessly integrated into many popular applications such as Internet Explorer, Microsoft Outlook, Outlook Express, Mozilla Firefox, and other popular VPNs.

SecureToken's built-in secure and encrypted internal storage offer secure container for user credentials which by default, it can store up to sixteen X.509 v3 digital certificates respectively. By nature, SecureToken supports multiple keys for multiple PKI or smart card applications simultaneously thus cross applications usage of a single SecureToken is possible. Proper authentication with User PIN is required whenever any application trying to access the SecureToken which achieve the essential 2FA's objective.

### Common application fields crucial to have strong authentication are:

- |   |  |
|---|--|
| • Web or Network based Application Security | SSL Secure Web Sign On, Single Sign On, Secure Application Sign On, Secure VPN Sign On, etc. |
| • Public Key Infrastructure Implementation  | Digital Signing, PKI Authentication, Encryption or Decryption                                |
| • Enterprise IT Security                    | Data/File/Drive Encryption, Email Encryption, Workstation or Network Access Security         |



## SECURETOKEN ST2/ST2S

SecureToken ST2 is the most popular and cost effective model which is utilizing 8-bit microprocessor smart chip with 32K (25K usable) internal smart card memory. This model supports up to 1024-bit RSA key pair generation onboard which is the common requirement for most PKI implementation. SecureToken ST2 is designed based on HID driverless architecture but the middleware and token manager tool installer still require a CD-ROM.

Choose SecureToken ST2 if you require extensive customization on the middleware or if you need to include large client software into the Installer.

Choose SecureToken ST2S if you require Windows Smart Card Logon. ST2S come with PC/SC device driver.



## SECURETOKEN ST3

SecureToken ST3 is the latest state of the art Auto-Install model which combines both high speed and high security 32-bit microprocessor with 128K (64K usable) memory smart card based authentication device together with 2MB flash memory for Auto Installer facility for needed middleware and token manager tool. This model eliminates common hassle on implementing USB token where external media such as CD-ROM is still needed for token's middleware and tool installation manually.

SecureToken ST3 is a truly Auto Install model. No manual installation is needed for device driver and middleware.

Choose SecureToken ST3 if you are looking for the best option with maximum speed, security and convenient. Limited middleware customization is possible.



## Advantages of using SecureToken

### Secure

User names and passwords are not longer safe in today's digital world. It can be easily exposed to third party or being hacked by unethical hackers. SecureToken provides secure container for user to keep their security credentials and once it's kept, it will never leave SecureToken without being encrypted. The specialized onboard crypto microprocessors in SecureToken enable far stronger security than software-only solutions. SecureToken is built according to international security standards with rigid requirements to ensure maximum security integrity.

### Versatile

SecureToken can securely hold multiple security credentials, allowing it to support many concurrent PKI applications.

### Cost Effective

SecureToken architecture is based on open standards and it is more cost effective than other hardware security systems like Smart Card or Biometric readers. You can implement Smart Card security without the need to invest on expensive readers. What you need to implement SecureToken is just a USB port.

### Simple

SecureToken can Hot Plug to the USB port of any supported PC and it provides "out of the box" support for Internet Explorer, Microsoft Outlook, Outlook Express, Mozilla Firefox or any software product based on the MS-CAPI or PKCS#11 standards. SecureToken comes with a standard crypto tool kit for partners and OEM customers to ease the integration. SecureToken supports browsers with either Active X or Java Applet interface

### Portable

SecureToken is small enough for you to take it wherever you go. Your digital certificates, passwords, PIN numbers or other personal security information will not be left unattended on your PC.



## Technical Specification

Model	SecureToken ST2S	SecureToken ST2	SecureToken ST3
Hardware Platform	Secure EAL and FIPS Compliant Microprocessor Smart Chip		
Processor	8-bit		32-bit
Card Operating System	SecureCOS		
Software Platform	PC/SC	HID driverless with external media for CSP and Middleware installation	HID driverless with CSP and Middleware Auto Install
Middleware	Comply to PKCS#11 and MS CAPI, hot-pluggable to Internet Explorer, Microsoft Outlook, Outlook Express, Mozilla Firefox and many more.		
Supported Interface	Active X Control or Java Applet		
Memory Size	32k (26K for User) on Smart Chip		128k (64K for User) on Smart Chip 2MB on Flash for Middleware & CSP
Windows Smart Card Logon	YES	NO	NO
Certificate Storage	Up to Five X.509 v3 Digital Certificate		Up to Sixteen X.509 v3 Digital Certificate
On-Board Security Algorithms	RSA, DES, 3DES, SHA-1, Hardware generated 1024-Bit RSA Key Pairs. Optional to support 3rd party algorithms		RSA, DES, 3DES, SHA-1, Hardware generated 2048-Bit RSA Key Pairs. Optional to support 3rd party algorithms
Chip Security Level	Secured and Encrypted Data Storage		
Dimension	59mm x 18mm x 9mm		
Weight	5g		
Power Dissipation	< 250 mW		
Operating Temperature	0 °C to 70 °C (32 F to 156 F)		
Storage Temperature	-40 °C to 85 °C (-40 F to 185 F)		
Humidity Rating	0 to 100% without condensation		
Connector Type	Standard USB 1.1 and support USB 2.0 connection.		
Casing	Hard Molded Plastic, Tamper Proof (Optional), RoHS compliance.		
Memory Data Retention	At least 10 years		
Memory Cell Rewrites	At least 100,000 times		
Standards	CE and FCC		CE, FCC and MyCC Certified
Supported Operating Systems	Win98SE/ME/XP/2000/2003/Vista/Windows7; Optional to Support Linux & MAC OS		

## SecureToken Feature Highlights

- Onboard generation of RSA 1024-bit / 2048-bit key pairs**  
Key pairs generated onboard together with digital signing on hardware to ensure maximum security. It offers secure encrypted storage for X.509 v3 digital certificates.
- Random Number generation performed on hardware**  
Random number generated on hardware for strong challenge response authentication.
- Middleware support PKCS#11 and Microsoft CAPI applications**  
Seamless integration to many popular applications such as Internet Explorer, Microsoft Outlook, Outlook Express, Mozilla Firefox and more. Powerful plug and play connectivity to PKI applications.
- Supports multiple PKI and smart card applications**  
One SecureToken can store multiple key pairs and ready to use on multiple PKI or smart card applications.
- Tamper Prove Casing**  
SecureToken comes with tamper proof hard plastic casing option.
- Compliant and Certified by International Standards**  
FIPS, RoHS, PC/SC compliant, CE and FCC Conformity Certified. Malaysian Common Criteria Evaluation and Certification -EAL-Certified.
- Built-in support for RSA, DES, 3DES, MD5 and SHA-1 algorithms**  
Support various powerful security algorithms with advanced encryption/decryption hardware ready to support.





## Software Development Kit

What you need now is to get a set of SecureToken ST2 or ST3 Software Development Kit which will facilitate all your needs to start integrating SecureToken ST2 or ST3 protection into your software application.

The contents inside the Software Development Kit are listed as below:

- One unit SecureToken ST2 / ST2S DEMO Token
- One unit software/utilities CD-ROM
- Contents inside the CD-ROM:
  - Installation Guide
  - Developer Guide
  - Comprehensive User Manual
  - API Samples for PKCS#11 Interface, Microsoft CryptoAPI
  - Middleware Installation
  - DLLs and Header Files
  - Runtime Installation Package
  - Token Manager for Admin and User
  - User Guide for Online DEMO Token Management System

**SECURETOKEN**  
**ST2/ST2S**  
Software Development Kit



- One unit SecureToken ST3 DEMO Token
- One unit software/utilities CD-ROM
- Contents inside the CD-ROM:
  - Installation Guide
  - Developer Guide
  - Comprehensive User Manual
  - API Samples for Java and Active X
  - API Samples for PKCS#11 Interface, Microsoft CryptoAPI
  - Middleware Installation
  - DLLs and Header Files
  - Runtime Installation Package
  - Token Manager for Admin and User
  - Token Initialization Tool
  - User Guide for Online DEMO Token Management System

**SECURETOKEN**  
**ST3**  
Software Development Kit



**SECURE  
METRIC**  
TECHNOLOGY



**Kuala Lumpur (HQ)**  
**SecureMetric Technology Sdn. Bhd.**  
2-2, Incubator 2, Technology Park Malaysia, Lebuhraya Sg Besi - Puchong,  
Bukit Jalil, 57000 Kuala Lumpur, Malaysia.  
Tel: +603 8996 8225 Fax: +603 8996 7225

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

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

**Ho Chi Minh City**  
**SecureMetric Technology Co., Ltd**  
302 HBT Building  
456-458 Hai Ba Trung Street  
District 1, Ho Chi Minh city, Vietnam  
Tel : +84 8 6291 5258  
Fax: +84 8 6291 5266

**Singapore**  
**(Sales Representative Office)**  
105, Cecil Street, #06-01,  
The Octagon, Singapore 069534  
Tel: +65 6827 4451  
Fax: +65 6827 9601



**EAL**



**CE FC**

