



APAC

Suite 2.06, 32 Delhi Rd, North Ryde, NSW,
2113, Australia
T: +612-9888 6185
F: +612-9888 6185
E: AUS@eSecuTech.com

EMEA

4 Cours Bayard 69002 Lyon,France
57 Lokaertlaan 3080 Tervuren Belgium
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

Email: sales@eSecuTech.com

Web: www.eSecuTech.com

WIKI: www.eSecuTech.com/wiki

Support portal: www.eSecuTech.com/support

SDK software download : (PW: opensesame)

Http://www.eSecuTech.com/downloads

Order: www.eSecuTech.com/store

©Copyright 2018 SecuTech. All rights reserved. Reproduction in whole or in part without written permission from SecuTech is prohibited. SecuTech, UniKey, UniToken, UniOTP, UniMate, UniReader and the SecuTech logo are trademarks of SecuTech. Windows and all other trademarks are properties of their respective owners. Features and specifications are subject to change without notice.

28CSTD/08 2018



SECUTECH

THE KEY TO INFORMATION SECURITY

Our References



Certificates

CE
FCC
ROHS
FIPS 140-2

Partner of

Apple
Autodesk
FreeOTFE
HP
IBM
Intel
Microsoft
Oath
SUN
SIIA
VeriSign

CONTENTS

THE KEY TO INFORMATION SECURITY

3 Company
Introduction

4 Software
Protection
UniKey STD / STD Mini
STD Dual / PRO / PRO Mini
Ultra Dual / Time / Drive

18 Dynamic
Authentication
UniOTP 300/500

20 USB
Authentication
UniMate USB
UniMate Mini
UniMate Drive

26 Cyber Security
and Possible Threats

30 Why SecuTech?

31 Services



Innovation Is a Journey not a Destination

Information Technology is ever more prominent in today's businesses, and as a result malicious entities have not been slow to take advantage of possible vulnerabilities. Thankfully, SecuTech is a global leader in providing hardware based software protection & licensing options, as well as strong authentication for Windows, iOS and Linux based systems, with a wide array of flexibility that tailor to varying business needs. SecuTech's employees persistently pursue the latest information security technology and are able to provide a well-rounded security assessment to quell any malicious threats.

Our solutions enable our customers to adapt to escalating internal and external threats to their sensitive data, and rapidly evolve to address new business requirements and compliance mandates. Our flagship products include:

UniKey®: Software protection and licensing management dongle that is highly customizable and easy to use with a myriad of features: network management and support, RTC (Real Time Clock), partitionable secure flash memory, USB A and C support, depending on your needs. Ensure only users in possession of the physical dongle can access your software.

UniOTP®: OATH based one-time password (OTP) tokens generate a unique secondary password ensuring that only properly authenticated users are granted access. Available in both event- & time-based types, UniOTP® is built to be reliable for continuous use, ideal for remote access solutions.

UniMate®: PKI based two-factor smart card authentication token that manages a broad range of digital certificates, passwords and other credentials that are used in the verification process. Correct password and the UniMate® is required for the authentication process to succeed, considerably minimizing the ability to falsify a user's identity.

Expert Consultancy/Advice: SecuTech's employees pursue the latest information security technology that is driving the development of the industry's cutting edge products, and securing hundreds of customers' valuable data and intellectual property. Access the best software security options for your software, specialist custom solutions, or general overall advice.

Our technology and technical expertise is provided to thousands of customers including: Boeing, Bosch, JVC Kenwood, Siemens, among other various banks and government agencies. Do you want to take advantage of our expertise?

For more information, please visit www.eSecuTech.com



SOFTWARE PROTECTION

As a software creator/vendor, the balance between strong software protection, an effective licensing scheme and a plug-and-play distribution model that doesn't burden the end user with an over-complicated setup process, is integral in maintaining maximized profit margins. By using UniKey®, you're ensuring the protection of your software from piracy & reverse engineering, while having the utilities, samples and documentation to implement a license model that fits your customers and software's use case/specifications.

UniKey® works by ensuring only users in possession of the physical dongle can access your software. Password authentication, multiple protection schemes, software and hardware IDs, remote update service and a driverless format ensures high-level security without sacrificing ease of software distribution. UniKey® is capable of working cross-platform (Windows, iOS and Linux), and is easy to implement with a wide variety of straightforward utilities or direct software integration through API.

Well proven in over 62 countries worldwide, UniKey® offers a solution to software protection, digital rights management and licensing options that support every business' requirements.



UniKey® STD
A standard one-to-one software protection key, ideal for less-budget licensing, where real-time and networking functions are not required.



UniKey® STD Mini
The smallest hardware based protection dongle in the world, protrudes only by 6mm making it virtually invisible. It is perfectly suited for notebooks, embedded devices, medical devices or controls for machineries and equipment.



UniKey® STD Dual
An ideal cost-effective software protection dongle, available for a wide range of platforms utilizing a dual interface: USB A and USB C.



UniKey® PRO
Robust solution for protecting enterprise software designed to operate in a local network infrastructure.



UniKey® PRO Mini
Ideal solution for component licensing when network features are required, it protrudes only by 6mm making it virtually invisible.



UniKey® Ultra Dual
UniKey® Ultra Dual is ideal when network licensing features are required for both USB A and USB C platforms/devices.



UniKey® Time
Containing all features of a UniKey® PRO and a Real Time Clock (RTC), the UniKey® Time is an ideal solution for implementing time-based licensing options in one-to-one or networked environments.



UniKey® Drive
Add an extra layer of security by distributing or storing part of your software on-key in the UniKey® Drive's partitionable flash memory, while providing network licensing features as well. The flash memory comes in 4 resizable partitions: public (plug-and-play), password protected, ROM (data cannot be modified) and hidden (can only be accessed through API).



Software protection has always been an integral part of modern businesses. With SecuTech's wide range of driverless UniKey® dongles this has never been easier to achieve. The UniKey® ensures not to burden the user, while providing exceptional functionality options to the developer to ensure their visions are met.





UniKey® STD/STD MINI

Strong, yet Cost-Effective

Software Protection as well as Local License Solutions



UniKey® STD is the standard, one-to-one, version of the driverless UniKey® dongle. It provides a full set of functions/utilities that enable strong software protection for users and developers alike. It works as a standalone dongle allowing only one end user to use the software at a time. The UniKey® STD is ideal for licensing a large number of components that don’t require network-based licensing and also comes with remote update support.

Unique and Strong Protection for Software

- Strong encryption is employed to secure the transmission between the UniKey® and USB port.
- Each UniKey® dongle features a globally unique Hardware Identification Number (HID), as well as a programmable Software Identification Number (SID).
- Automatically protect your software and IP without modification – UniKey® Enveloper (Windows only for now)
- The UniKey® API allows for customized protection and the ability to directly merge the UniKey® with your source code. API function calls and source code is shared between UniKey® products, so upgrading and downgrading is seamless.






Strong & All-round Protection

UniKey® offers two different protection methods:

- a.The UniKey® Enveloper (Windows Only)
Quickly and easily protect your executable files automatically with the UniKey® Enveloper. Add a protective shield around your desired software that prevents reverse engineering and piracy. This is achieved without the original source code (for compilation) or additional programming.
- b.The UniKey® Application Programming Interface (API)
API protection involves some coding work. However, abundant documentation, samples and libraries are provided in helping to directly integrate the UniKey®’s functionality with your software in a seamless transition to the end user.

Variable & Flexible Licensing

UniKey® STD supports the following licensing models:

	Pay-Per-Use	Charge for the number of times software functionality is used over a period of time.
	Subscription	Charge periodically for software upgrades and new versions.
	Try-Before-You-Buy	Offer limited trial versions, free-of-charge.
	Feature-Based	Enable or disables product features based upon users’ needs and budget.
	Perpetual	Once purchased, the software can be used indefinitely.

Highlight Features

Driverless

UniKey® makes the complicated procedure of deployment as simple as “plug and play”, saving users a lot of time and energy. There is no need to install any software or drivers before using it.

Free Technical Support

SecuTech offers free technical support to our customers worldwide, through our ticket service, email or conference call if necessary. Our technical professionals ensure that the highest level of customer satisfaction and understanding are met. Access our online support ticket system at www.eSecuTech.com/support

Technical Specifications-UniKey® STD / STD MINI	
Security	
Hardware ID	Globally unique, 32-bit
Software ID	User-defined, 32-bit
Protection	Enveloper protection, API protection
Memory	
Capacity	4KB
Memory Date Retention	at least 30 years
Memory Cell Rewriters	at least 1,000,000 times
Max. No. of Features/Applications Enabled Per Key	64
Supported Platforms (end-user)	
Operating Systems Supported ^[1]	Windows98 SE/ME/XP/Vista/7/10, ^[2] Windows Server 2000/2003/2008/2012, Linux(2.4+), Mac OS X(10.4+), Free BSD(5+), ARM 9, MIPS
Supported Platforms (software vendor)	
Development Platforms Supported ^[3]	Microsoft Visual Studio 6.0/2003/2005/2008/2010/2013, Microsoft Access 2002/2003/2007, Borland C++ Builder, Delphi 5/6/7/2006/2007/2009/2010/XE/XE2/XE3
Programming Languages Supported ^[4]	VC++, VB, VC.NET, VB.NET, C, C#, Java, Delphi, Fortran, Access, ActiveX, Arx, BCB, Clarion, dBase, Director, FileMaker, LabView, LabWindows, Matlab, MinGW, NSIS, PowerBuilder, PureBasic, RealBasic, VisualFoxPro, WinDEV
Physical Specifications	
Default Color	Gray
Case Material	Metal and Plastic(UniKey STD) / Plastic (UniKey STD Mini)
Storage Temperature	-10℃ ~ 85℃
Operating Temperature	0℃ ~ 70℃
Humidity Rating (without condensation)	0 ~70%
Min. Operating Voltage	5V
Current Consumption (in mA)	<=150
Dimensions	52.8 x 17 x 7 mm (UniKey STD) / 24.6 x 15 x 7 mm (UniKey STD Mini)
Weight	6.3g (UniKey STD) / 2.4g (UniKey STD Mini)
Certification	
Safety Certification	CE/FCC
Environmental Certification/ Compliance	RoHS
Manufacturer’s Warranty	
Covers Manufacturing & Material Defects	One Year
Customization Service	
Case Color	Yes
Device Naming	Yes
Logo Marking	Yes
Design	Mini case Available

[1] UniKey also supports other operating systems . Please contact SecuTech for details.
[2] including 32 and 64 bits versions.
[3] UniKey also supports other development platforms. Please contact SecuTech for details.
[4] UniKey also supports other programming languages. Please contact SecuTech for details.





UniKey® STD Dual

Dual USB UniKey® Interface for Enhanced Compatibility

Software Protection as well as Local License Solutions

The UniKey® STD Dual shares the same functionality as the UniKey® STD, but with the added advantage of USB Type C interface & support. It provides a full set of functions that deliver strong software protection for developers and users alike. With the STD Dual, seamless connection is now possible for a wide range of devices (PC, Mac, Surface Pro, and others) that utilize USB A or USB C ports. This is your first step to embracing the latest technologies that have transitioned to Type C USB.

Unique and Strong Protection for software

- Strong encryption is employed to secure the transmission between the UniKey and USB port.
- Each UniKey® dongle features a globally unique Hardware Identification Number (HID), as well as a programmable Software Identification Number (SID).
- Automatically protects your software and IP without modification - UniKey® Enveloper (Windows only for now)
- The UniKey® API allows for customized protection and the ability to directly merge the UniKey® with your source code. API function calls and source code is shared between UniKey® products, so upgrading and downgrading is seamless.

Strong and All-round Protection in stand-alone Environment






UniKey® STD Dual is a must have device for protecting software running in a stand-alone environment. It is a new product containing all the features of UniKey® STD with the addition support for USB Type C port devices. We provide console tools to monitor and manage your dongles.

UniKey® offers two different protection methods:

- a. The UniKey® Enveloper (Windows only for now)
Quickly and easily protect your executable files automatically with the UniKey® Enveloper. Add a protective shield around your desired software that prevents reverse engineering and piracy. This is achieved without the original source code (for compilation) or additional programming.
- b. The UniKey® Application Programming Interface (API)
API protection involves some coding work. However, abundant documentation, samples and libraries are provided in helping to directly integrate the UniKey®’s functionality with your software in a seamless transition to the end user.

Variable & Flexible Licensing

UniKey® STD Dual supports the following licensing models:

	Pay-Per-Use	Charge for the number of times software functionality is used over a period of time.
	Subscription	Charge periodically for software upgrades and new versions.
	Try-Before-You-Buy	Offer limited trial versions, free-of-charge.
	Feature-Based	Enable or disables product features based upon users’ needs and budget.
	Perpetual	Once purchased, the software can be used indefinitely.

Highlight Features

Driverless

UniKey® makes the complicated procedure of deployment as simple as “plug and play” , saving users a lot of time and energy. There is no need to install any software or drivers before using it.

Dual USB Compatibility

UniKey® STD Dual supports both USB A and C connectors, for complete compatibility over PC, tablet or hybrid device.

Free Technical Support

SecuTech offers free technical support to our customers worldwide, through our ticket service, email or conference call if necessary. Our technical professionals ensure that the highest level of customer satisfaction and understanding are met. Access our online support ticket system at www.eSecuTech.com/support

Technical Specifications-UniKey® STD Dual	
Security	
Hardware ID	Globally unique, 32-bit
Software ID	User-defined, 32-bit
Protection	Enveloper protection, API protection
Network	No
Memory	
Capacity	4KB
Memory Date Retention	at least 30 years
Memory Cell Rewriters	at least 1,000,000 times
Max. No. of Features/Applications Enabled Per Key	64
Supported Platforms (end-user)	
Operating Systems Supported ^[1]	Windows ME/XP/Vista/7/8/8.1/10, ^[2] Windows Server 2000/2003/2008/2012, ^[2] Linux(2.4+), Mac OS(10.4+), Free BSD(5+), ARM7, ARM9, MIPS, PowerPC, Solaris
Supported Platforms (software vendor)	
Development Platforms Supported ^[3]	Microsoft Visual Studio 6.0/2003/2005/2008/2010/2013/2015, Microsoft Access 2002/2003/2007, Borland C++ Builder, Delphi 5/6/7/10 Seattle/10.1 Berlin/2006/2007/2009/2010/XE/XE2/XE3/XE4/XE5/XE6/XE7/XE8
Programming Languages Supported ^[4]	VC++, VB, VC.NET, VB.NET, C, C#, Java, Delphi, Fortran, Access, ActiveX, Arx, BCB, Clarion, dBase, Director, FileMaker, LabView, LabWindows, Matlab, MinGW, NSIS, PowerBuilder, PureBasic, RealBasic, VisualFoxPro, WinDEV, Lazarus, PHP
Hardware	
Port 1	USB Type A
Port 2	USB Type C
Physical Specifications	
Default Color	Silver
Case Material	Metal
Storage Temperature	-10℃ ~ 85℃
Operating Temperature	0℃ ~ 70℃
Humidity Rating (without condensation)	0 ~70%
Min. Operating Voltage	5V
Current Consumption (in mA)	<=150
Dimensions	40.3x16x7(±0.5)
Weight	8.4g(±0.5)
Certification	
Safety Certification	CE/FCC
Environmental Certification/ Compliance	RoHS
Manufacturer’s Warranty	
Covers Manufacturing & Material Defects	One Year
Customization Service	
Case Color	No
Device Naming	Yes
Logo Marking	Yes

[1] UniKey also supports other operating systems . Please contact SecuTech for details.

[2] including 32 and 64 bits versions.

[3] UniKey also supports other development platforms. Please contact SecuTech for details.

[4] UniKey also supports other programming languages. Please contact SecuTech for details.



UniKey® PRO/PRO MINI

Strong, Flexible Dongle with Comprehensive Licensing Models
Software Protection in a Network Environment

The UniKey® PRO is ideal for protecting software running in a network environment. A single key connected to any machine in the network allows up to 65535 – 1024 concurrent users. SecuTech provides utilities and options to monitor/manage your end users that range from: White/Black listing features, to a real time IP Monitor utility. The UniKey® PRO also contains all features of the UniKey® STD.

Unique and Strong Protection for Software

- Strong encryption is employed to secure the transmission between the UniKey® and USB port.
- Each UniKey® dongle features a globally unique Hardware Identification Number (HID), as well as a programmable Software Identification Number (SID).
- Automatically protect your software and IP without modification - UniKey® Enveloper (Windows only for now)
- The UniKey® API allows for customized protection and the ability to directly merge the UniKey® with your source code. API function calls and source code is shared between UniKey® products, so upgrading and downgrading is seamless.

Strong & All-round Protection

UniKey® offers two different protection methods:

a.The UniKey® Enveloper (Windows only for now)

Quickly and easily protect your executable files automatically with the UniKey® Enveloper. Add a protective shield around your desired software that prevents reverse engineering and piracy. This is achieved without the original source code (for compilation) or additional programming.

b.The UniKey® Application Programming Interface (API)

API protection involves some coding work. However, abundant documentation, samples and libraries are provided in helping to directly integrate the UniKey®’s functionality with your software in a seamless transition to the end user.

Variable & Flexible Licensing

UniKey® PRO supports the following licensing models:

	Pay-Per-Use	Charge for the number of times software functionality is used over a period of time.
	Floating Licensing	Enable concurrent use of your software by one user in a network environment, charging by the number of network seats that use the software simultaneously in network environments.
	Try-Before-You-Buy	Offer limited trial versions, free-of-charge.
	Volume Licensing	Offer volume pricing for multiple single-user copies operating in a network environment.
	Perpetual	Once purchased, the software can be used indefinitely.
	Feature-Based	Enable or disable product features based upon users’ needs and budget.
	Subscription	Charge periodically for software upgrades and new versions.

Highlight Features

Driverless

UniKey® makes the complicated procedure of deployment as simple as “plug and play”, saving users a lot of time and energy. There is no need to install any software or drivers before using it.

Remote Update Support

Remotely update the license of your software on the UniKey® device. This can include the addition/removal of functionalities or extend the validity of the license.

Network Functionality

Multiple networked systems/devices can operate on a single UniKey® device that is attached to the administrating system, with support for: White/Black listing, firewall and subnet crossing, and IP monitoring.

Free Technical Support

SecuTech offers free technical support to our customers worldwide, through our ticket service, email or conference call if necessary. Our technical professionals ensure that the highest level of customer satisfaction and understanding are met.

Access our online support ticket system at www.eSecuTech.com/support

Technical Specifications-UniKey® PRO / PRO MINI

Security	
Hardware ID	Globally unique, 32-bit
Software ID	User-defined, 32-bit
Protection	Enveloper protection, API protection
Memory	
Capacity	4KB
Memory Date Retention	at least 30 years
Memory Cell Rewriters	at least 1,000,000 times
Max. No. of Features/Applications Enabled Per Key	64
Supported Platforms (end-user)	
Operating Systems Supported ^[1]	Windows98 SE/ME/XP/Vista/7/10, ^[2] Windows Server 2000/2003/2008/2012, ^[2] Linux(2.4+), Mac OS X(10.4+), Free BSD(5+), ARM 9, MIPS
Supported Platforms (software vendor)	
Development Platforms Supported ^[3]	Microsoft Visual Studio 6.0/2003/2005/2008/2010/2013, Microsoft Access 2002/2003/2007, Borland C++ Builder, Delphi 5/6/7/2006/2007/2009/2010/XE/XE2/XE3
Programming Languages Supported ^[4]	VC++, VB, VC.NET, VB.NET, C, C#, Java, Delphi, Fortran, Access, ActiveX, Arx, BCB, Clarion, dBase, Director, FileMaker, LabView, LabWindows, Matlab, MinGW, NSIS, PowerBuilder, PureBasic, RealBasic, VisualFoxPro, WinDEV
Physical Specifications	
Default Color	Crimson
Case Material	Metal and Plastic (UniKey PRO) / Plastic (UniKey PRO Mini)
Storage Temperature	-10℃ ~ 85℃
Operating Temperature	0℃ ~ 70℃
Humidity Rating (without condensation)	0 ~70%
Min. Operating Voltage	5V
Current Consumption (in mA)	<=150
Dimensions	52.8 x 17 x 7 mm (UniKey PRO) / 24.6 x 15 x 7 mm (UniKey PRO Mini)
Weight	6.3g (UniKey PRO) / 2.4g (UniKey PRO Mini)
Certification	
Safety Certification	CE/FCC
Environmental Certification/ Compliance	RoHS
Manufacturer’s Warranty	
Covers Manufacturing & Material Defects	One Year
Customization Service	
Case Color	Yes
Device Naming	Yes
Logo Marking	Yes
Design	Mini case Available


[1] UniKey also supports other operating systems . Please contact SecuTech for details.

[2] including 32 and 64 bits versions.

[3] UniKey also supports other development platforms. Please contact SecuTech for details.

[4] UniKey also supports other programming languages. Please contact SecuTech for details.





UniKey® Ultra Dual

Comprehensive Dongle with Dual Interface

Software Protection in a Network Environment with USB C Support

The UniKey® Ultra Dual shares the same functionality as the UniKey® PRO, but with the added advantage of USB Type C interface & support. It provides a full set of functions that deliver strong software protection for developers and users alike. With the Ultra Dual, seamless connection is now possible for a wide range of devices (PC, Mac, Surface Pro, and others) that utilize USB A or USB C ports. This is your first step to embracing the latest technologies that have transitioned to USB C.

Unique and Strong Protection for software

- Strong encryption is employed to secure the transmission between the UniKey® and USB port.
- Each UniKey® dongle features a globally unique Hardware Identification Number (HID), as well as a programmable Software Identification Number (SID).
- Automatically protect your software and IP without modification - UniKey® Enveloper (Windows only for now)
- The UniKey® API allows for customized protection and the ability to directly merge the UniKey® with your source code. API function calls and source code is shared between UniKey® products, so upgrading and downgrading is seamless.

Strong Software Protection in a Network Environment

UniKey® Ultra Dual is available for protecting software running in a network environment. It is a new product containing all the features of UniKey® Pro. A key connected to any machine in the network allows up to 65535 – 1024 concurrent users. We provide console tools to monitor and manage your software’s users, and manage White\Black lists.

UniKey® offers two different protection methods:

a. The UniKey® Enveloper (Windows only for now)








Quickly and easily protect your executable files automatically with the UniKey® Enveloper. Add a protective shield around your desired software that prevents reverse engineering and piracy. This is achieved without the original source code (for compilation) or additional programming.

b.The UniKey® Application Programming Interface (API)

API protection involves some coding work. However, abundant documentation, samples and libraries are provided in helping to directly integrate the UniKey®’s functionality with your software in a seamless transition to the end user.

Variable & Flexible Licensing

UniKey® Ultra Dual supports the following licensing models:

	Pay-Per-Use	Charge for the number of times software functionality is used over a period of time.
	Floating Licensing	Enable concurrent use of your software by one user in a network environment, charging by the number of network seats that use the software simultaneously in network environments.
	Try-Before-You-Buy	Offer limited trial versions, free-of-charge.
	Volume Licensing	Offer volume pricing for multiple single-user copies operating in a network environment.
	Perpetual	Once purchased, the software can be used indefinitely.
	Feature-Based	Enable or disable product features based upon users’ needs and budget.
	Subscription	Charge periodically for software upgrades and new versions.

Highlight Features

Driverless

UniKey® makes the complicated procedure of deployment as simple as “plug and play”, saving users a lot of time and energy. There is no need to install any software or drivers before using it.

Remote Update Support

Remotely update the license of your software on the UniKey® device. This can include the addition/removal of functionalities or extend the validity of the license.

Network Functionality

Multiple networked systems/devices can operate on a single UniKey® device that is attached to the administrating system, with support for: White/Black listing, firewall and subnet crossing, and IP monitoring.

Dual USB Compatibility

UniKey® STD Dual supports both USB A and C connectors, for complete compatibility over PC, tablet or hybrid device.

Free Technical Support

SecuTech offers free technical support to our customers worldwide, through our ticket service, email or conference call if necessary. Our technical professionals ensure that the highest level of customer satisfaction and understanding are met.

Access our online support ticket system at www.eSecuTech.com/support

Technical Specifications-UniKey® Ultra Dual	
Security	
Hardware ID	Globally unique, 32-bit
Software ID	User-defined, 32-bit
Protection	Enveloper protection, API protection
Memory	
Capacity	4KB
Memory Date Retention	at least 30 years
Memory Cell Rewriters	at least 1,000,000 times
Max. No. of Features/Applications Enabled Per Key	64
Supported Platforms (end-user)	
Operating Systems Supported ^[1]	Windows ME/XP/Vista/7/8/8.1/10, ^[2] Windows Server 2000/2003/2008/2012, ^[2] Linux(2.4+), Mac OS(10.4+), Free BSD(5+), ARM7, ARM9, MIPS, PowerPC, Solaris
Supported Platforms (software vendor)	
Development Platforms Supported ^[3]	Microsoft Visual Studio 6.0/2003/2005/2008/2010/2013/2015, Microsoft Access 2002/2003/2007, Borland C++ Builder, Delphi 5/6/7/10 Seattle/10.1 Berlin/2006/2007/2009/2010/XE/XE2/XE3/XE4/XE5/XE6/XE7/XE8
Programming Languages Supported ^[4]	VC++, VB, VC.NET, VB.NET, C, C#, Java, Delphi, Fortran, Access, ActiveX, Arx, BCB, Clarion, dBase, Director, FileMaker, LabView, LabWindows, Matlab, MinGW, NSIS, PowerBuilder, PureBasic, RealBasic, VisualFoxPro, WinDEV, Lazarus, PHP
Physical Specifications	
Default Color	Silver
Case Material	Metal
Storage Temperature	-10℃ ~ 85℃
Operating Temperature	0℃ ~ 70℃
Humidity Rating (without condensation)	0 ~70%
Min. Operating Voltage	5V
Current Consumption (in mA)	<=150
Dimensions LxWxH (in mm)	40.3x16x7(±0.5)
Weight	8.4g
Connection Interface	
Port 1	USB Type A
Port 2	USB Type C
Certification	
Safety Certification	CE/FCC
Environmental Certification/ Compliance	RoHS
Manufacturer’s Warranty	
Covers Manufacturing & Material Defects	One Year
Customization Service	
Case Color	No
Device Naming	Yes
Logo Marking	Yes

[1] UniKey also supports other operating systems . Please contact SecuTech for details.

[3] UniKey also supports other development platforms. Please contact SecuTech for details.

[4] UniKey also supports other programming languages. Please contact SecuTech for details.

[2] including 32 and 64 bits versions.

UniKey® Time

Keep Your Software and Time Protected

Comprehensive Solution with an Independent Real Time Clock

The UniKey® Time hardware key is specifically designed for software vendors who need to control and manage the rental, subscription or maintenance of software. It allows the customers to pay per use, allowing software vendors complete control over sales to end users in a periodical manner. This feature is based on a real time clock located inside the dongle indicating the specific time (hour: minute: second) and date (day/ month/ year). The UniKey® Time also contains all the features of the UniKey® PRO as an added benefit.

Unique and Strong Protection for Software

- Strong encryption is employed to secure the transmission between the UniKey® and USB port.
- Each UniKey® dongle features a globally unique Hardware Identification Number (HID), as well as a programmable Software Identification Number (SID).
- Automatically protect your software and IP without modification - UniKey® Enveloper (Windows only for now)
- UniKey® API allows for customized protection and the ability to directly merge the UniKey® with your source code. API function calls and source code is shared between UniKey® products, so upgrading and downgrading is seamless.









Strong & All-round Protection

UniKey® offers two different protection methods:

- a. The UniKey® Enveloper (Windows Only)
Quickly and easily protect your executable files automatically with the UniKey® Enveloper. Add a protective shield around your desired software that prevents reverse engineering and piracy. This is achieved without the original source code (for compilation) or additional programming.
- b. The UniKey® Application Programming Interface (API)
API protection involves some coding work. However, abundant documentation, samples and libraries are provided in helping to directly integrate the UniKey®'s functionality with your software in a seamless transition to the end user.

Variable & Flexible Licensing

UniKey® Time supports the following licensing models:

	Time-Based	Enable software vendors to charge by the exact amount of time spent using the software.
	Pay-Per-Use	Charge for the number of times software functionality is used over a period of time.
	Floating Licensing	Enable concurrent use of your software by one user in a network environment, charging by the number of network seats that use the software simultaneously in network environments.
	Try-Before-You-Buy	Offer limited trial versions, free-of-charge.
	Volume Licensing	Offer volume pricing for multiple single-user copies operating in a network environment.
	Perpetual	Once purchased, the software can be used indefinitely.
	Feature-Based	Enable or disable product features based upon users' needs and budget.
	Subscription	Charge periodically for software upgrades and new versions.


Highlight Features

- Driverless**
UniKey® makes the complicated procedure of deployment as simple as “plug and play”, saving users a lot of time and energy. There is no need to install any software or drivers before using it.
- Remote Update Support**
Remotely update the license of your software on the UniKey® device. This can include the addition/removal of functionalities or extend the validity of the license.
- Network Functionality**
Multiple networked systems/devices can operate on a single UniKey® device that is attached to the administrating system, with support for: White/Black listing, firewall and subnet crossing, and IP monitoring.
- Real Time Clock (RTC)**
The UniKey® Time utilizes a built-in Real Time Clock that offers users a more reliable overview and control over their subscription based licensing model. Typically, time-based restrictions use a software/user-based clock, which is easily circumvented by malicious users. Luckily, UniKey® Time's RTC is tamper-proof and cannot be falsified. Feel secure that your trials, evaluations, subscriptions and other time-based licensing models are protected.
- Free Technical Support**
SecuTech offers free technical support to our customers worldwide, through our ticket service, email or conference call if necessary. Our technical professionals ensure that the highest level of customer satisfaction and understanding are met. Access our online support ticket system at www.eSecuTech.com/support

Technical Specifications-UniKey® Time	
Security	
Hardware ID	Globally unique, 32-bit
Software ID	User-defined, 32-bit
Protection	Enveloper protection, API protection
Memory	
Capacity	4KB
Memory Date Retention	at least 30 years
Memory Cell Rewriters	at least 1,000,000 times
Max. No. of Features/Applications Enabled Per Key	64
Supported Platforms (end-user)	
Operating Systems Supported ^[1]	Windows98 SE/ME/XP/Vista/7/10, ^[2] Windows Server 2000/2003/2008/2012, ^[2] Linux(2.4+), Mac OS X(10.4+), Free BSD(5+), ARM 9, MIPS
Supported Platforms (software vendor)	
Development Platforms Supported ^[3]	Microsoft Visual Studio 6.0/2003/2005/2008/2010/2013, Microsoft Access 2002/2003/2007, Borland C++ Builder, Delphi 5/6/7/2006/2007/2009/2010/XE/XE2/XE3
Programming Languages Supported ^[4]	VC++, VB, VC.NET, VB.NET, C, C#, Java, Delphi, Fortran, Access, ActiveX, Arx, BCB, Clarion, dBase, Director, FileMaker, LabView, LabWindows, Matlab, MinGW, NSIS, PowerBuilder, PureBasic, RealBasic, VisualFoxPro, WinDEV
Physical Specifications	
Default Color	Blue
Time	On-key clock
Case Material	Metal
Storage Temperature	-10℃ ~ 85℃
Operating Temperature	0℃ ~ 70℃
Humidity Rating (without condensation)	0 ~70%
Min. Operating Voltage	5V
Current Consumption (in mA)	<=150
Dimensions LxWxH (in mm)	52.8x17x7mm (±0.5)
Weight	7.3g
Certification	
Safety Certification	CE/FCC
Environmental Certification/ Compliance	RoHS
Manufacturer's Warranty	
Covers Manufacturing & Material Defects	One Year
On-key Clock Battery Life	Three Years
Customization Service	
Case Color	Yes
Device Naming	Yes
Logo Marking	Yes

[1] UniKey also supports other operating systems . Please contact SecuTech for details.
[2] including 32 and 64 bits versions.
[3] UniKey also supports other development platforms. Please contact SecuTech for details.
[4] UniKey also supports other programming languages. Please contact SecuTech for details.





UniKey® Drive

Greater Piracy Protection when Your Software is Inside the Dongle Driverless Dongle with Partitionable Secured Mass Storage

Built for secure storage, the UniKey® Drive is the first encrypted mass storage dongle with driverless software protection and license management options. UniKey® Drive offers a complete solution for storage of your application’ s software files, drivers, and data over 4 resizable partitions: public, encrypted/password-protected, hidden and read-only storage. In addition to secure mass storage, UniKey® Drive offers all of UniKey® PRO’s software protection functionality and licensing features.

Unique and Strong Protection for Software

- Strong encryption is employed to secure the transmission between the UniKey® and USB port.
- Each UniKey® dongle features a globally unique Hardware Identification Number (HID), as well as a programmable Software Identification Number (SID).
- Automatically protect your software and IP without modification - UniKey® Enveloper (Windows only for now)
- The UniKey® API allows for customized protection and the ability to directly merge the UniKey® with your source code. API function calls and source code is shared between UniKey® products, so upgrading and downgrading is seamless.








Strong & All-round Protection

UniKey®offers two different protection methods:

- a.The UniKey® Enveloper (Windows only for now)
Quickly and easily protect your executable files automatically with the UniKey® Enveloper. Add a protective shield around your desired software that prevents reverse engineering and piracy. This is achieved without the original source code (for compilation) or additional programming.
- b.The UniKey® Application Programming Interface (API)
API protection involves some coding work. However, abundant documentation, samples and libraries are provided in helping to directly integrate the UniKey®’ s functionality with your software in a seamless transition to the end user.

Variable & Flexible Licensing

UniKey® Drive supports the following licensing models:

	Pay-Per-Use	Charge for the number of times software functionality is used over a period of time.
	Floating Licensing	Enable concurrent use of your software by one user in a network environment, charging by the number of network seats that use the software simultaneously in network environments.
	Try-Before-You-Buy	Offer limited trial versions, free-of-charge.
	Volume Licensing	Offer volume pricing for multiple single-user copies operating in a network environment.
	Perpetual	Once purchased, the software can be used indefinitely.
	Feature-Based	Enable or disable product features based upon users’ needs and budget.
	Subscription	Charge periodically for software upgrades and new versions.

Highlight Features

Driverless
UniKey® makes the complicated procedure of deployment as simple as “plug and play”, saving users a lot of time and energy. There is no need to install any software or drivers before using it.

Remote Update Support

Remotely update the license of your software on the UniKey® device.
This can include the addition/removal of functionalities or extend the validity of the license.

Network Functionality

Multiple networked systems/devices can operate on a single UniKey® device that is attached to the administrating system, with support for: White/Black listing, firewall and subnet crossing, and IP monitoring.

Partitionable Flash Memory

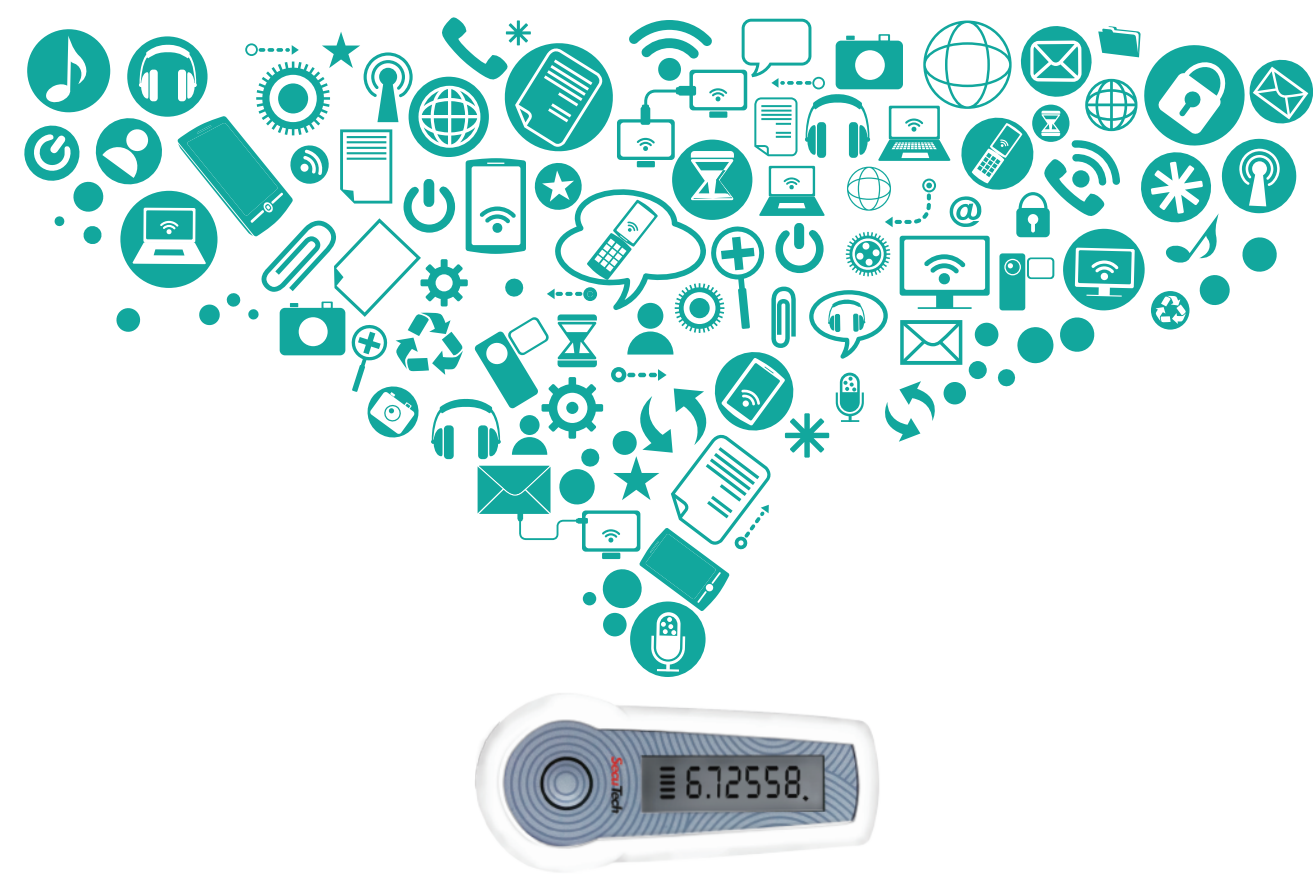
- Public** – can be viewed by the Operating System (OS) as Mass Storage and allows for free manipulation of the data.
Password Protected – data can only be viewed and accessed after the correct password is inputted.
Virtual CD-ROM – data is emulated as a CD-ROM. This allows the users to view/read but cannot modify the contents. This ensures that the security and integrity of the files remains guaranteed.
Hidden Drive – data can only be accessed via the use of API and console. Encrypted partition is invisible to end-users, allowing for safe storage of credentials and other sensitive data.

Free Technical Support

SecuTech offers free technical support to our customers worldwide, through our ticket service, email or conference call if necessary. Our technical professionals ensure that the highest level of customer satisfaction and understanding are met.
Access our online support ticket system at www.eSecuTech.com/support

Technical Specifications-UniKey® Drive	
Security	
Hardware ID	Globally unique, 32-bit
Software ID	User-defined, 32-bit
Secure Communication Channel	128-bit AES encryption
Data Encryption	RSA, AES
Protection	Enveloper protection, API protection
Memory	
Capacity	2G/4G/8G/16G/32G/64G
Memory Date Retention	at least 30 years
Memory Cell Rewriters	at least 1,000,000 times
Max. No. of Features/Applications Enabled Per Key	256
Supported Platforms (end-user)	
Operating Systems Supported ^[1]	Windows98 SE/ME/XP/Vista/7/10, ^[2] Windows Server 2000/2003/2008/2012, ^[2] Linux(2.4+), Mac OS X(10.4+), Free BSD(5+), ARM 9, MIPS
Supported Platforms (software vendor)	
Development Platforms Supported ^[3]	Microsoft Visual Studio 6.0/2003/2005/2008/2010/2013, Microsoft Access 2002/2003/2007, Borland C++ Builder, Delphi 5/6/7/2006/2007/2009/2010/XE/XE2/XE3
Programming Languages Supported ^[4]	VC++, VB, VC.NET, VB.NET, C, C#, Java, Delphi, Fortran, Access, ActiveX, Arx, BCB, Clarion, dBase, Director, FileMaker, LabView, LabWindows, Matlab, MinGW, NSIS, PowerBuilder, PureBasic, RealBasic, VisualFoxPro, WinDEV
Physical Specifications	
Default Color	Black
Case Material	Metal
Storage Temperature	-10℃ ~ 85℃
Operating Temperature	0℃ ~ 70℃
Humidity Rating (without condensation)	0 ~70%
Min. Operating Voltage	5V
Current Consumption (in mA)	<=150
Dimensions LxWxH (in mm)	52.8x17x7mm (Standard size) (±0.5)
Weight	7g
Certification	
Safety Certification	CE/FCC
Environmental Certification/ Compliance	RoHS
Manufacturer’s Warranty	
Covers Manufacturing & Material Defects	One Year
Customization Service	
Case Color	Yes
Device Naming	Yes
Logo Marking	Yes
Capacity	Yes

[1] UniKey also supports other operating systems . Please contact SecuTech for details.
[2] including 32 and 64 bits versions.
[3] UniKey also supports other development platforms. Please contact SecuTech for details.
[4] UniKey also supports other programming languages. Please contact SecuTech for details.



SecuTech UniOTP® Authenticators

Boost Your Business with the Most Reliable and Secure Authentication Solution

Information security is always centered as the premier concern by most organizations, especially at the login/authentication stage. It is difficult to manage employees’ credentials and secure login practices at all times, thankfully, with dynamic one time password authenticators an extra layer of protection is added against brute force attacks or leaked passwords. The UniOTP® range are available in event-based or time-based authenticators, and are OATH standard compliant (i.e. can be used/paired with other OATH based 3rd party servers).

The World’s Most Popular and Convenient Remote User Authentication Solution

The UniOTP® family offers a succinct range of one-time password authenticators that meet your needs whether cost, convenience or security is your priority. UniOTP® authenticators generate secure one-time passwords, ensuring that only properly authenticated users are authorized access to critical applications and sensitive information.

By choosing SecuTech’s UniOTP® as an authentication solution, enterprises can reduce the overhead costs of information security while providing a consistent and easy to use authentication experience for end users, by offering:

- Dynamic Authentication
- Strong Security Guarantee
- Turnkey Solution for end-users
- Tamper-Resistant Design
- Wide Variety of Authenticators

After doing comprehensive research and analysis, SecuTech is ready to provide refined solutions to a wide range of industries:

- UniOTP® E-commerce Solution
- UniOTP® Enterprise Solution
- UniOTP® Financial Institution Solution
- UniOTP® VPN Solution
- UniOTP® Intranet Network Protection Solution
- UniOTP® Web Authentication Solution

Strong Security Guarantee

The passwords are generated by an intricate mechanism which involves a 160-bit encryption key and a 64-bit counter. Each UniOTP device has a unique symmetric key that is combined with a proven algorithm to generate a new one-time password (OTP) at the press of a button or every 60 seconds. The password mechanism helps ensure the security of passwords generated by UniOTP that is nearly impossible for a hacker to replicate or predict.

Turnkey Solution for End-users

A benefit of UniOTP is that it has no footprint, which makes UniOTP quite easy to use. Customers do not have to install any software on the client side. With UniOTP the authentication can be used for network security on PCs, tablet computers and even smart phones.

No matter which type of UniOTP® authenticator you choose, it’s as simple as entering a password, and you can have security with the dynamic password. UniOTP® is presented as a turnkey solution to solve password chaos. It is a big challenge for most people to remember too many complicated passwords. Usually, they will be in a mess and cause troubles as it for end-users. UniOTP® helps the user to save their efforts in remembering their passwords. With UniOTP®, the brain-racking authentication event is reduced to a click and type operation.





A Tamper-Resistant Design

The UniOTP is shielded with a robust casing made of wear-resistant engineering plastics. The hardware device has passed a battery of tests, including electrostatic discharge, immersion, run-over and mechanical shock tests. It is tamper-resistant so that the encryption key and secure data stored in it are far from malicious attacks. In addition, the ergonomic design of the hardware device offers customers a comfortable user experience. The appearance of UniOTP token can also be customized with company artwork to reinforce the issuer’s brand.

A Wide Variety of Authenticators

Each organization’s security requirements may vary greatly from others. Therefore, it is important to find the right authenticator to meet -their individual needs in the terms of total cost of ownership, end-user security needs, product life cycle and other issue. SecuTech offers a series of versatile hardware authenticators as well as on-demand authenticators that provide strong authentication using familiar devices that users already have.

Features

-  Highly reliable and durable
-  tamper-Resistant ABS engineering plastic case
-  Easy integration
-  Compliant with OATH Standard
- Unique token serial number
- Wide variety of authenticators
 - SecuTech provides different types of OTP product, including time-based, event-based and challenge / response-based authenticators, to meet customers’ requirements.
- Scratch resistance screen cover
- Portable design, convenient to take anywhere
- OEM service – fit customers’ needs
 - Logo customization
 - Appearance customization

Technical Specifications	
UniOTP	300/500
Dimensions, L*W*H (mm)	59*26*10
Weight (g)	14
Materials	Engineering Plastic
Water Resistance	Daily
Battery Lifetime	3 to 5 years
Display	Liquid Crystal (LCD)
Operating Temperature	-10℃ – 50℃
Warranty	1 to 5 years
Product Safety Standards	CE, RoHS

By using UniOTP you can stay ahead of attackers and protect yourself from the dangers that plague the information industry in a way that is consistent, reliable and proven to work. Your customers, clients and partners will know that you have taken the best possible measures to ensure the safety of your intellectual property, securing both your products and their interests. UniOTP automatically uses strong authorization and layered security as well as one time passwords that change every 60 seconds to prevent unauthorized access making it the easiest, most secure and user friendly OTP solution available today.

It is not an option to wait for something to happen, think secure, get UniOTP.

SecuTech UniMate® PKI Two Factor Authenticators

In the digital age of today, an increasingly substantial amount of organizational and personal information is being migrated and accessed online. Technology has undoubtedly brought convenience, and to a large extent, altered how we handle information. The increasing dependence on technology has changed the face of global processes down to our personal digital identities. This resulted in safe keeping measures of information becoming more difficult to keep up with, and malicious entities have not been slow to take advantage of possible vulnerabilities.

SecuTech is at the forefront of information security, and by employing their third flagship product: UniMate® - as a strong authentication solution, you can rest easy knowing your digital credentials and information stays secure.





UniMate USB / UniMate Mini
FIPS 140-2 Level 2 certified PKI Token for PCs.





UniMate Drive
UniMate Drive is split into two partitions: a normal partition (read and write) and a Virtual CD-ROM (read-only) partition.


UniMate® Features


- 

FIPS 140-2 Certified
UniMate is FIPS 140-2 certified, passing strict technical requirements for use by enterprises, governments and even military. FIPS 140-2 validation involves cryptographic modules that have been tested and validated under the Cryptographic Module Validation Program as meeting requirements for FIPS PUB 140-2.
- 

All-in-one Smart Card
UniMate USB is based on 32-bit smart card technology. Smart card technology offers the most sophisticated and secure form of authentication to your PKI infrastructure, with all encryption and decryption processes taking place on-board the device.
- 

Virtual CD-ROM
The Virtual CD-ROM partition is a read-only partition on the device formatted with your data. All programs and files stored in the Virtual CD-ROM partition can only be read, ensuring unchanged transfer of data and consistent distribution of software.
- 







Multiple PKI System Support
UniMate supports multiple international standards and PKI systems including RSA for USA/Europe, ECC for DSTU and ECC/SM for China, with future support for more.
- 

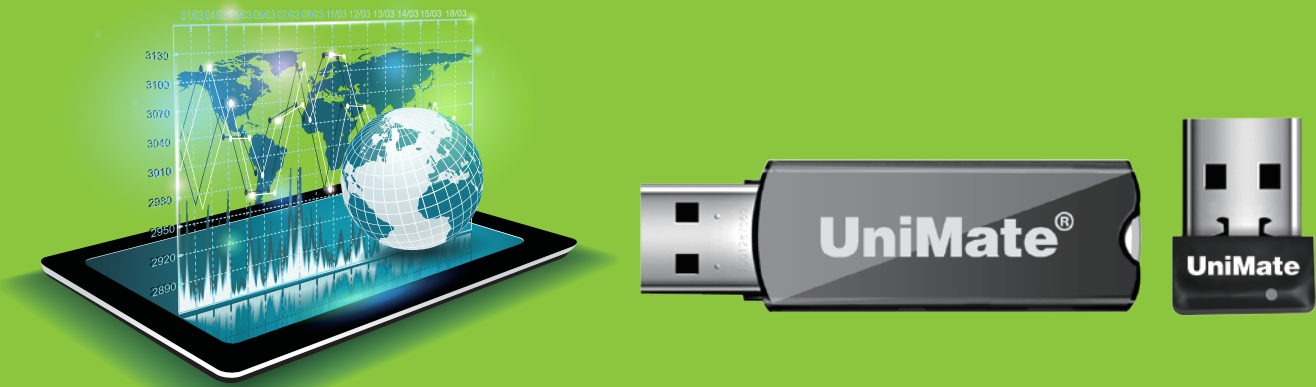
Rich Middleware
UniMate is designed to be compatible with several security standards including PKCS#11, MS-CAPI, miniDriver, and FIDO, collective standards for security products in the industry. UniMate APIs enables trouble free integration with MS-CAPI and PKS#11 compliant software.
- 

On-demand Partition
UniMate Drive features a flash memory that can be resized in order to suit the users' needs.

Highly Configurable

OEM customization is available to customize UniMate for your business needs. Customization options include logo laser engraving, custom case design, custom color options, as well as custom HID/naming services etc.

	Logo Customization	Brand your UniMate with your company or branding logo on-device, branding UniMate with your corporate identify.
	Case Options	Choose metal casing with your own color, logo and a unique serial number.
	Color Options	Choose from a variety of colors from the color palette to customise your case.
	Device Naming Service	Get company specific branding according to your corporate identity and improve the recognition of your product with the Device Naming Service.
	CSP Naming Service	Cryptographic Service Provider (CSP) names can be set per UniMate device to improve the recognition of your product.
	Encryption algorithm customization	Customized encryption algorithms can be supported by UniMate to meet various specifications or standards.



UniMate® USB / Mini

Cost Effective PKI USB Two Factor Authenticator
FIPS 140-2 (Level 2) Certified PKI Token

Two-Factor Authentication

As opposed to single-factor authentication, where only a password is required to verify the user’s credentials, two-factor authentication requires two separate modes of validation: “something you know” – the password, & “something you have” – the UniMate® device. Both password and the UniMate® device are needed to successfully complete the login process. UniMate® features the ability to generate encryption keys and store: passwords, digital certificates and personal credentials within the token.

High-Performance Smart Card Based Device

The UniMate® USB/Mini device is optimized with a 32-bit smart card to generate RSA encryption key pairs quickly onboard the token, enabling sophisticated security with minimal hassle and effort.

Multi-Level Permission Management

UniMate® utilizes three levels of token permission management: administrator, user and guest. Administrator holds the highest permission level, and guest holding the lowest. Any operation on the token requires explicit permissions, ensuring the security of the device is maintained to users with the appropriate permission level.

Virtual CD-ROM Partition

UniMate® has a built-in CD-ROM partition which allows users to view/read but not modify stored contents, and hence maintained the integrity of files.

Features	UniMate USB/Mini
CCID	✓
Secure Mass Storage	
On-Demand Partition	
Smart Card	✓
Onboard Encryption	✓
PKCS#11 Supported	✓
MS-CAPI Supported	✓
X.509 Certificate Supported	✓
Globally Unique Hardware ID	✓
Customized UniMate Name	✓
3-Level Permission Management	✓
Customization Service	✓
Secure Memory	✓

Technical Specifications - UniMate® USB/Mini	
Hardware	
Onboard Capacity	> 64 KB
Dimensions	UniMate USB: 52.8mm x 17mm x 7mm UniMate Mini: 24.6mm x 15mm x 7mm
Weight	UniMate USB: 6.4g UniMate USB Mini: 2.3g
Case Material	Tamper-Resistant Metal (UniMate USB) / Plastic (UniMate USB Mini)
Color (Factory Default)	Grey
Operating Temperature	0°C to 70°C
Storage Temperature	-10°C to 85°C
Humidity Rate	0-70% without condensation
Min.Operating Voltage	5 V
Current Consumption	150mA
Device Interface	USB 2.0
USB Protocol	CCID (Chip Card Interface Device)
Hardware Algorithms	
PKI Middleware	PKCS#11, MS-CAPI, FIDO
Onboard Encryption Algorithms	2048-bit RSA, 1024-bit RSA, 128-bit AES, 192-bit AES, 64-bit DES, 64-bit TDES
Onboard Hashing	160-bit SHA-1, 160-bit HMAC_SHA, 128-bit MD5, 128-bit HMAC-MD5
Performance Index	
Time For Digital Signing via USB	<0.5s
RSA 1024-bit Key Generation Time	< 3s
RSA 1024-bit Sign Time	< 300ms
RSA 2048-bit Key Generation Time	< 12s
RSA 2048-bit Sign Time	< 500ms
Certifications	
Computer Security	FIPS 140-2
Manufactory	CE/FCC (FCC Declaration of Conformity) RoHS (Restriction of Hazardous Substances Directive)
Device Identification	
Hardware ID	Globally-unique
Hardware Encryption Algorithms	AES (ECB 128-bit, 192-bit, 256-bit), AES (CBC 128-bit, 192-bit, 256-bit) DES (ECB), DES (CBC), RSA (1024-bit, 2048-bit), 3DES (ECB), 3DES (CBC)
Hardware Hashing Algorithms	MD5,SHA-1
PKI Support	PKCS#11, MS-CAPI, X.509v3
Memory Cell Rewrites	At least 100,000
Memory Data Retention	At least 10 years
Operating Systems	Windows 98 SE , Windows 2000, Windows ME, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008. Windows 7, Windows 8, Windows 10, Linux (2.2+), FreeBSD (5.x, 6.x, 7.x, 8.x, 9.x), Mac OS X (10.4, 10.5, 10.6), (32-bit and 64-bit all above)
Warranty	
Manufacturing & Material Defects	1 year



UniMate® Drive

PKI USB Two Factor Authentication Token with Partitionable Mass Storage

The UniMate® Drive consists of two partitions: a normal partition (read/write) and Virtual CD-ROM partition (read only).

Two-Factor Authentication

As opposed to single-factor authentication, where only a password is required to verify the user’s credentials, two-factor authentication requires two separate modes of validation: “something you know” – the password, & “something you have” – the UniMate® device. Both password and the UniMate® device are needed to successfully complete the login process. UniMate® features the ability to generate encryption keys, and store passwords, digital certificates and personal credentials within the token.

High-Performance USB Attached SCSI Protocol (UASP)

The UniMate® device is optimized with the latest USB 3.0 compatible transfer hardware and protocol, to quickly transfer data between devices, while also enabling sophisticated security with minimal hassle and effort.

Multi-Level Permission Management

UniMate® utilizes three levels of token permission management: administrator, user and guest. Administrator holds the highest permission level, and guest holding the lowest. Any operation on the token requires explicit permissions, ensuring the security of the device is maintained to users with the appropriate permission level.

Secure File System

The UniMate® device also provides users with a secure file system, which allows users to store credentials and other important information on the token’s internal memory (separate from Mass Storage).

On-demand Partition

The available flash memory can be resized and comes in two partitions:

Public: Simple “plug-and-play” token that can be viewed and modified by the OS and user.

Virtual CD-Rom: Data is viewed and stored as a CD-ROM, allowing users to view and read, but not modify any stored content. The integrity of the data is always guaranteed to be intact.

Features	UniMate® Drive
CCID	
Secure Mass Storage	✓
On-Demand Partition	✓
Smart Card	
Onboard Encryption	✓
PKCS#11 Supported	✓
MS-CAPI Supported	✓
X.509 Certificate Supported	✓
Globally Unique Hardware ID	✓
Customized UniMate Name	✓
3-Level Permission Management	✓
Customization Service	✓
Secure Memory	✓

Technical Specifications - UniMate® Drive	
Hardware	
Onboard Capacity	> 64 KB
Flash Memory	2GB, 4GB, 8GB, 16GB, 32GB
Dimensions	52.8mm x 17mm x 7mm
Weight	7.2g
Case Material	Tamper-Resistant Metal
Color (Factory Default)	Black
Operating Temperature	0°C to 70°C
Storage Temperature	-10°C to 85°C
Humidity Rate	0-70% without condensation
Min.Operating Voltage	5 V
Current Consumption	150mA
Device Interface	USB 2.0
USB Protocol	USB Attached SCSI Protocol (UASP)
Hardware Algorithms	
PKI Middleware	PKCS#11, MS-CAPI, FIDO
Onboard Encryption Algorithms	2048-bit RSA, 1024-bit RSA, 128-bit AES, 192-bit AES, 64-bit DES, 64-bit TDES
Onboard Hashing	160-bit SHA-1, 160-bit HMAC_SHA, 128-bit MD5, 128-bit HMAC-MD5
Performance Index	
Time For Digital Signing via USB	<0.5s
RSA 1024-bit Key Generation Time	< 3s
RSA 1024-bit Sign Time	< 300ms
RSA 2048-bit Key Generation Time	< 12s
RSA 2048-bit Sign Time	< 500ms
Certifications	
Manufactory	CE/FCC, RoHS
Device Identification	
Hardware ID	Globally-unique
Hardware Encryption Algorithms	AES (ECB 128-bit, 192-bit, 256-bit), AES (CBC 128-bit, 192-bit, 256-bit) DES (ECB), DES (CBC), RSA (1024-bit, 2048-bit), 3DES (ECB), 3DES (CBC)
Hardware Hashing Algorithms	MD5,SHA-1
PKI Support	PKCS#11, MS-CAPI, X.509v3
Memory Cell Rewrites	At least 100,000
Memory Data Retention	At least 10 years
Operating Systems	Windows 98 SE , Windows 2000, Windows ME, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008. Windows 7, Windows 8, Windows 10, Linux (2.2+), FreeBSD (5.x, 6.x, 7.x, 8.x, 9.x), Mac OS X (10.4, 10.5, 10.6), (32-bit and 64-bit all above)
Warranty	
Manufacturing & Material Defects	1 year

Cyber Security and Possible Threats

It is important to consider possible cybersecurity threats to prevent any data breaches or attacks, since it is cheaper and easier to prevent a data breach, than recover from one. Cyber-attacks are more frequent, sophisticated, and attack at a broader scope than ever before. In this section we will cover some of the current issues, threats and vulnerabilities that businesses face, the potential losses due to cyberattacks, and finally, some preventive measures.

Current Issues

- Distributed Denial of Service (DDoS)** – One of the most common and hardest to prevent, a DDoS attack is designed to freeze the online operations of a business/service for a certain amount of time. There is no permanent damage sustained, however potential impressions can be ruined.
- Credential-harvesting malware** – A threat to businesses and individuals alike, by tunneling and stealing login credentials. Due to increased use of internet banking, shared accounts and smart phone apps, this threat is widespread and difficult to manage.
- Router scanning/Packet Sniffing** – Hackers specialized in exploiting router vulnerabilities to gather credentials, login details and other data that can be used in conjunction with other malicious attacks in an attempt to penetrate your system.
- Phishing** – Users are tricked allowing malicious content directly into their system. Usually involves manipulative cold emails persuading recipient to check the included attachment. Specifically targeted phishing attacks, through multiple mediums and social media, fraudulent entities masquerading as partner contacts are also quite common.
- Ransomware** – Once a hacker has access to your system, through a mixture of phishing, malware or virus attempts, they encrypt your data for extortion purposes. Ransomware can have a cheap start up and pays well. Paying the ransom doesn't always restore your data.
- Malicious use of leaked tools** – Pirated or open-source tools can be subject to modification and code injection. This is an effective way for hackers to penetrate a secure system and apply additional malware or ransomware.
- Cloud Computing** – Having access to your data at all times and all over the world is a great feature, however, data can be compromised via a 3rd party breach (Dropbox 2012, TeamViewer 2016).
- General education/office policy** – It is just as important to let your employees know of the security requirements and guidelines, as it is to set them up. Often accidental breaches occur due to employee neglect and privilege miss-management.

In a telephone survey conducted in the UK*, it was discovered that “virtually all UK businesses covered by the survey are exposed to cyber security risks”. However, the silver lining being that most businesses are aware of the importance of cyber security and take steps to prevent any possible breaches or attacks. The reporting of breaches (and its severity) is still infrequent though.

Business awareness and attitudes are changing; and employers are willing to seek information, advice or guidance in preventing breaches. When seeking expert information conflicting advice and information overload starts to play a major factor in cyber security aversion. Large business managers are more likely to understand and sift through conflicting advice, while middle business and lower managers are usually overwhelmed and take information at face value.

Also, large businesses have the resources & expertise to hire external consulting services or engage in specialized training. They are also more likely to have a cyber security policy in place (and a recovery plan).

Average cost of all breaches identified in the last 12 months

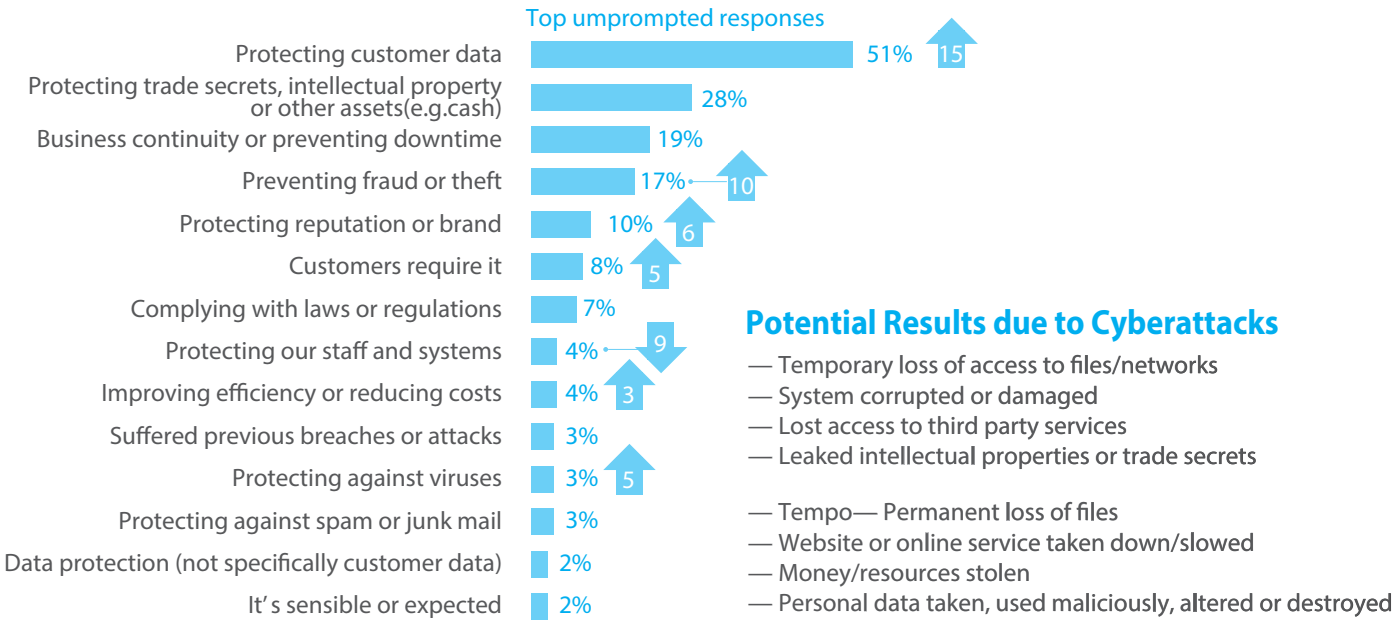
(Cyber Security Breaches Survey 2017*)

	All businesses	Micro/small	Medium	Large
	All Breaches			
Mean cost	1,570	1,380	3,070	19,600
Median cost	0	0	0	1,470
Base	737	413	218	106
	Breaches with an outcome			
Mean cost	2,330	2,070	5,950	13200
Median cost	300	300	1,000	8,230
Base	321	167	102	52

Main Reasons for investing in cyber security, among businesses who invest

(Cyber Security Breaches Survey 2017*)

Q.What are the main reasons that your organisation invests in cyber security?



Actions to Mitigate Cyber Security Incidents

There are many ways to prevent cyberattacks. Always configure, review and update current systems and applications, use an antivirus & firewall, backup regularly, have a well thought out office policy, employ user restrictions on unverified users and use multi factor authentication solutions to mitigate damage sustained by a cyber-breach. It is much cheaper to prepare and prevent cyberattacks before they occur compared to dealing with the fallout after. Cyber security is an important part of SecuTech and will gladly share its knowledge, expertise and flagship products in preparation/prevention of any cyberattacks. **Most importantly, there is no such thing as a perfect and unbreachable system and hence, SecuTech can help you make this breaching process so onerous that attackers will give up before any damage is done.** For more information, visit www.esecutech.com.

*Cyber Security Breaches Survey 2017 is a collaborated work of R. Klahr, J.N. Shah, P. Sheriffs, T. Rossington and G. Pestell from the Ipsos MORI Social Research Institute, and M. Button, V. Wang of the Institute for Criminal Justice Studies, University of Portsmouth. The original publication is accessible via <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017>.

Expert Cybersecurity Consulting Services

SecuTech’s comprehensive solutions focus on the protection of software and intellectual property, license management, and strong authentication solutions available across multiple platforms. Our expert technicians are quick to adapt to new internal and external threats, and rapidly evolve to address new business requirements and compliance mandates. We will work closely with your: CEOs, Software Engineers and Students willing to learn, and are careful to maintain a clear and straightforward line of discourse. SecuTech will recommend the correct implementation of our flagship solutions, or coordinate a new/custom solution instead to make sure your project is successful.

Software Licensing Professional Services

As a software producer, appropriate protection and choice of licensing model is critical to ensure the software’s sustainability and satisfy market requirements. A suitable licensing model will help your business target a wider range of customers with different styles of usage and cost requirements where appropriate. SecuTech can help you assess the best options for your software, developing an effective protection scheme, license management, and distribution model to achieve a clean end user experience.

Expert Multi Factor Authentication Solutions

Two Factor Authentication (TFA) is readily proven to be a deterrent, and to minimize the impact of a possible data breach. SecuTech provides both One Time Password (OTP) & Public Key Infrastructure (PKI) tokens, server configuration options and anything else needed to secure your authentication process.

Vulnerability Management

SecuTech can help you identify possible vulnerability points that may threaten your software’s efficiency/effectiveness, and convey possible improvements.

How We Can Help?

All requirements and setups are different, if your business requires a custom solution – we can help. SecuTech can provide expert consultancy services and even manage/operate new projects with the help of our experienced team of technicians and years of experience in the IT sector.

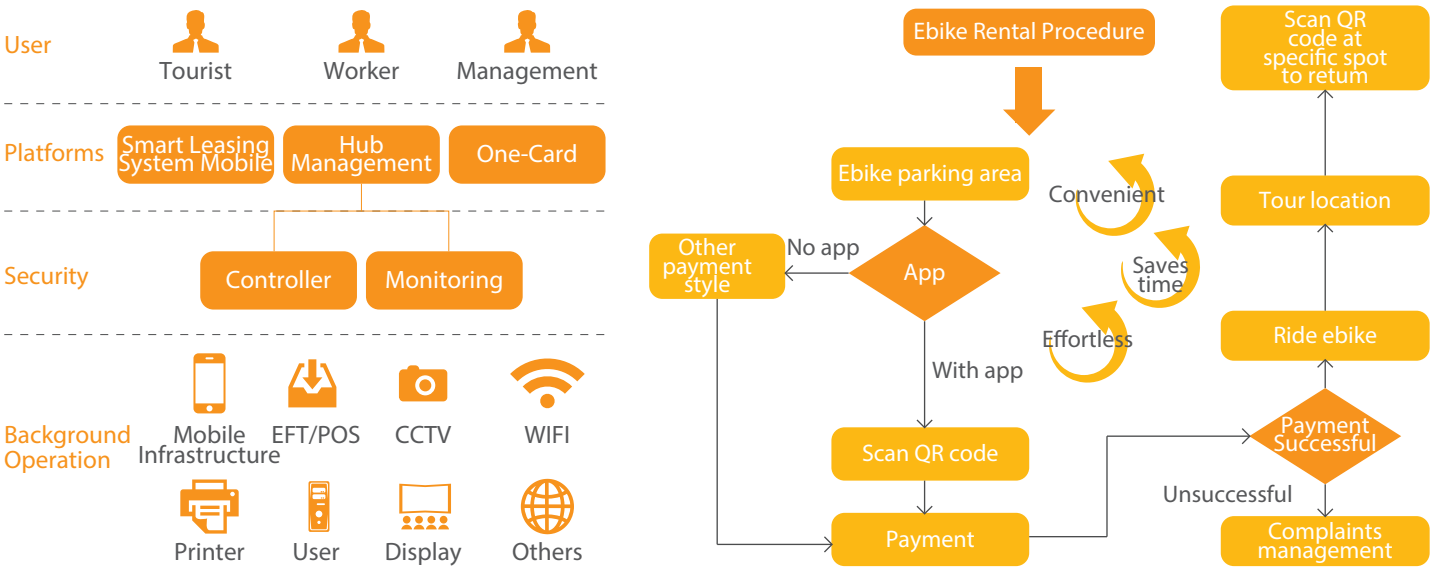
Do you want to take advantage of our expertise?
For more information visit www.eSecuTech.com

Scan and Pay customized solution

While SecuTech Solutions specializes in cyber security hardware, we have also spearheaded custom technologically advanced projects. Scan and Pay was developed to add convenience and security to tourist Smart Bike and Electric Car rental spots. Scan and Pay offers the benefits of 24 hour self-checkout from the convenience of their phone. By merging a free smart phone app and an integrated QR system, it doesn’t burden the end user with the hassle of having to handle cash, or operator interaction. They are free to enjoy the pristine scenery at their own pace and schedule.

Utilising mobile apps such as WeChat (a popular social media and payment app developed by Tencent), users can rent, pay, track and get support directly through the app. SecuTech is able to integrate your scan and pay service with other compatible apps.

The rental process is simple: the user (or tourist) arrives at the smart bike or E-Car rental location, uses the WeChat app or scan the QR code to make a booking & payment, the vehicle is unlocked, a booking confirmation is sent to the user, the user is now free to use the vehicle, and finally scan the QR code when returning the vehicle to confirm its return status. GPS and other support features are present on the bike/E-Car, so tampering with the vehicle is rare.



Sample Scan and Pay System Framework

The vehicle is loaded with an on board terminal that displays: the vehicle location, various navigation options and support information. Hand held ticketing systems are also available for modular maintenance checking, information withdrawal and general optimization. The other benefits are seamless integration with an integrated marketing app that can report and monitor various information; e.g. income generation per scenic view analysis.

SecuTech faced great challenges when designing the overall system structure, ensuring that flexibility and ease of use is paramount to both tourists and employees. Security was also a great concern as the bikes/E-Cars would potentially get stolen, vandalized or not maintained properly; therefore an effective protection layer was also required. The protection layer consists of a dispatch center and a monitoring system.

Overall the combination of having a secured mobile based payment system, with the technological benefits of implementing smart security options and operational monitoring, succeeded in bringing a safe and convenient self-checkout system to an already crowded city in China. Tourists are already seeing the benefits of a stress-free sightseeing experience. SecuTech is known worldwide for high quality products, reliability and meeting client’s expectations.



Electric Car self-checkout controller platform with QR scan



WeChat mobile app with QR scan and payment authentication




Smart Dinosaur Kid Rides implemented in various huge malls throughout China




SecuTech China partner in smart rides

SECURITY




Strong Authentication

Authentication is typically a signing-in process where a person proves his/her identity with the correct credentials. This process is used to ensure that a user is who they claim to be. Strong authentication is achieved through the use of a second factor or credential to be presented at the login process.



Reliable PKI Implementation

The PKI keys and digital certificates are securely generated, stored and used on the security devices by SecuTech – the sensitive and precious private keys never leave the device and will never be exposed to the insecure PC environment.




State-of-the-Art Cryptography

SecuTech follows industry's best practices and only uses well-established and thoroughly tested cryptographic algorithms. The passwords and credentials stored on our keys are encrypted onboard the key with various encryption algorithms.


On-board Key Generation

On-board key generation enables RSA keys to be generated and stored in the hardware device, instead of being stored or loaded onto the PC. This ensures maximum protection via the encryption ciphers. Therefore, the keys can never be compromised through methods such as Cold Boot attacks or other exploits.




Multi-level Security Management

SecuTech's products are designed with multi-level security and permission management. Logging on to any permission level needs a certain PIN, and any operation requires the corresponding permission level. The PIN has to be verified before it can be modified. Only permitted administrators hold the PIN, which is confidential to the end user.




VPN Security

VPNs are generally considered to have strong protection for data communications. Secure VPNs provide both network authentication and encryption. SecuTech's security products support multiple VPN authentication methods which enables seamless integration with VPN systems. In this way, strong authentication for remote access is achieved easily.




CONVENIENCE




Driverless

SecuTech brought driverless technology to the information security industry, and developed the most advanced driverless security product families. This driverless feature requires no driver installation so it saves users the trouble of dealing with "dongle not found" problems and makes everything easy and fast. In general, it helps reduce 90% of software post-sales work and provides more cost-effective deployment for end users.




Cross Platform

All SecuTech's products work on most popular OSes, including Windows, Linux, MacOS, FreeBSD, and embedded systems etc., both 32-bits and 64-bits systems. As such, software licensing is easily implementable across most platforms, supported by a range of programming languages with samples included in the SDK.




CONSIDERATION

SecuTech provides customers with a wide range of options for customization, such as laser-etched branding, customized case, hardware naming service, and software (API) customization (for more information about product customization, please refer to the OEM service.)



Quality

Quality is something SecuTech will never sacrifice. Our products are designed and built to last. The facts speak for themselves; SecuTech consistently has a lower average annual failure rate than the industry average. We back this with high-quality after-sales services and we even offer an industry-beating reliability refund guarantee on selected hardware devices for peace of mind.



THE ENVIRONMENT

Technology improved the way we live, work and play. But there's one place where technology should have no impact, the environment. Through responsible use, reuse and recycling, people can protect and preserve the environment together. All products by SecuTech are environmental friendly and we also provide recycling service for customers.




DEVICE CUSTOMIZATION SERVICE

The laser-etching technology enables a customer's specific logo to be marked on the device's case, making it look outstanding as well as improving the recognition of your company and products.




DEVICE NAMING SERVICE

With the Device Naming Service, a customer's specific brand will show as the name of the specific device. It not only contributes to increasing brand awareness but enhances the image of the company.



DEVICE COLOR CUSTOMIZATION SERVICE

Color and style are usually used to improve the image of a company. Different industries or companies may have their own color preferences. SecuTech provides multiple case color options. With a cute and distinctive appearance, the resulting product and company branding will impress customers greatly.



FREE SUPPORT TICKETS SERVICE

By purchasing any product of SecuTech, customers can submit support tickets for free. With the ticket number, customers can log on to the support portal to get help from our diligent and experienced support staff. This number also helps track the support history of each customer.



CAPACITY CUSTOMIZATION SERVICE

SecuTech's products can provide storage capacity for storing secure data. This capacity may vary with different product and is completely customizable.



APIS CUSTOMIZATION SERVICE

API (Application Programming Interface) is a set of tools for building software applications. A good API makes it easier to develop a program by providing all the required building blocks. A programmer then puts the blocks together. SecuTech not only provides robust APIs, but can also customize APIs according to various functionality requirements for customers. This guarantees high performance and operating environments' consistency.

