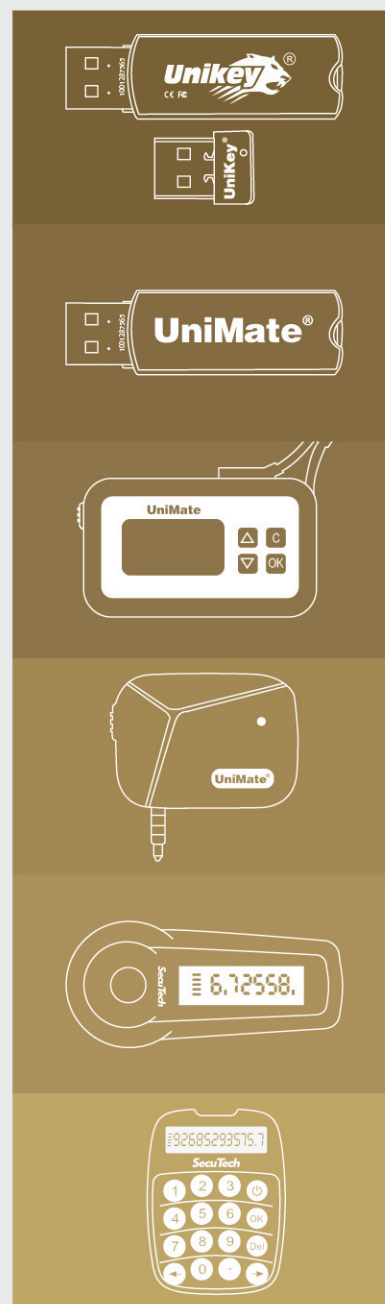




SECUTECH

THE KEY TO INFORMATION SECURITY



Our References

Yale University

DataStitch

SIEMENS

KENWOOD
COMMUNICATIONS

KIDS

FUJIFILM

BOSCH

BOEING

THE INSTITUTE OF
ORIENTAL PHILOSOPHY
UK

goldsmith CAD CAM

PSBank
PHILIPPINE SAVINGS BANK



Certificates

CE

FCC

ROHS

FIPS 140-2

Partner of

Apple

Autodesk

FreeOTFE

HP

IBM

Intel

Microsoft

Oath

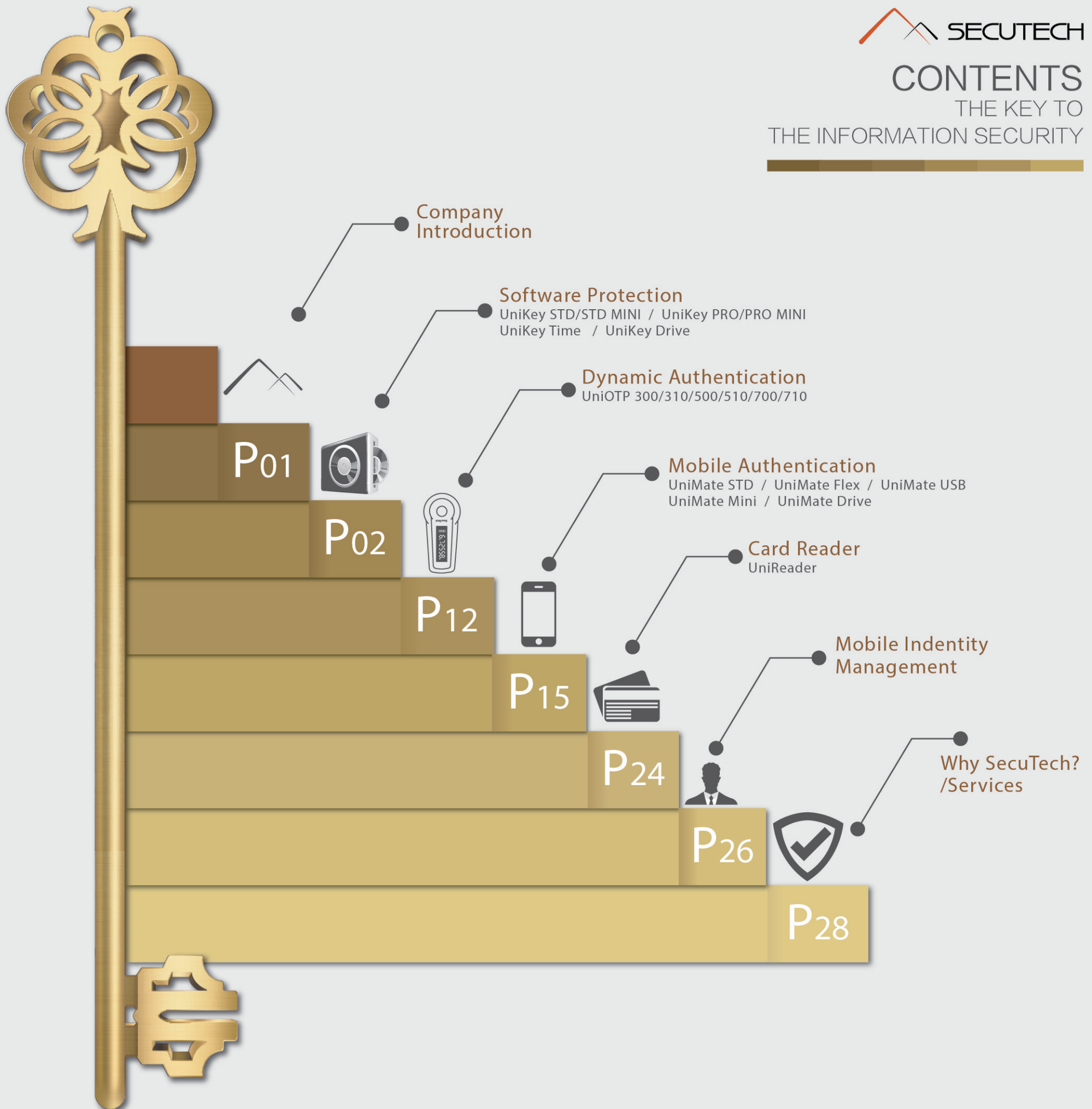
SUN

SIIA

VeriSign

CONTENTS

THE KEY TO
THE INFORMATION SECURITY





SecuTech is a leader in the creation and support of information security technology. When companies like Boeing, Kenwood, Rolls and Royce, and Siemens think of information security and digital rights management, they think of SecuTech. SecuTech leverages its new technology and diverse technical expertise to provide advanced custom solutions worldwide.

SecuTech's UniKey Software Rights Management products are the first Driverless Hardware key choice of software developers and publishers to protect intellectual property, increase revenue, and reduce losses from software piracy. UniToken provides enhanced security for accessing confidential information and for moving a private certificate between computers. It provides two-factor (password and physical possession of a token) authentication for confidential data. UniOTP is an open, flexible authentication solution that supports any form of authentication, including Windows Logon, Active Directory authenticating, cloud computing, and mobile authentication. UniMate TRRS and USB DUAL-Enabled two-factor authentication token enables customers to manage a broad range of authentication credentials, including one time password, digital certificates and static passwords, it's easy to works on iPhone, iPad , Android, PC and Mac, and it is the first security token available for both PC, smart phones and other mobile devices which can work seamlessly between devices.

SecuTech is a company specializing in data protection and strong authentication, providing total customer satisfaction in security systems & services for banks, financial institutions & other industries. Having extensive and in-depth experience within the information security market, SecuTech has drawn upon this experience to utilize today's cutting-edge technologies, enables enterprises, financial institutions, and government to safely adopt the economic benefits of mobile and cloud computing that are effective against increasingly sophisticated cyber attacks.

For more information, please visit www.eSecuTech.com

Do you want to take advantage of our expertise?



Software Protection

As a software vendor, you can maximize profit margins significantly on how well you protect and license the software to meet the needs of the market and your business. Helping your sales teams to meet their revenue targets by using a well constructed licensing implementation and to give your customers the tools they need to operate within the terms of their license agreements by limiting unauthorized and inadvertent over deployment whilst offering a clean customer experience is not simple.

With a team of professionals responsible for the design, implementation and management of some of the world's most complex enterprise licensing systems, our product's life time limited warranty, and the company's 24/7 service, you will find SecuTech's hands-on approach to be deeply focused on your customers, your business and your needs.

UniKey works cross-platform (Windows, Linux, and Mac) and offers a solution for software protection and digital rights management that is well proven in over 62 countries. It is available in a variety of models to support every business need.



UniKey STD

SecuTech's most cost-effective software protection key, ideal for less-budget licensing, where real time and networking features 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 machinery and equipment.



UniKey PRO

Robust solution for protecting enterprise software designed for operating in a networked infrastructure.



UniKey PRO MINI

Ideal solution for component licensing when networking features are required, it protrudes only by 6mm making it virtually invisible.



UniKey Time

Combining the features of the Net key and the Time key, the UniKey Time is an ideal solution for implementing time-based licensing in networked environments.



UniKey Drive

Ideal for distributing your software on-key, stored in flash memory. Use the UniKey Drive dongle when you want to license a large number of components or require metered licensing.

Software protection has always been an integral part of a modern business; and 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.



LOWEST
PRICE
PROMISE



UniKey® STD/STD MINI

Strong, yet, Cost-Effective Solution for Software Protection
Software Protection as well as Local License Solutions

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

Unique and Strong Protection for Software

- Secure communication between dongle and USB port, employing strong encryption.
- Each UniKey® dongle features a globally unique Hardware Identification Number (HID), as well as a customizable Software Identification Number (SID).
- Best-in-class tools for automatic protection (Enveloper, without source modification).
- UniKey® API enables to customize your protection and embed calls to your protection keys throughout your application's sourcecode.

Strong & All-round Protection

UniKey® offers two different protection methods:

a. The UniKey® Enveloper

UniKey® Enveloper is the fastest way to protect your executable files. It adds a protective shield around executable files and DLLs.






UniKey® Enveloper is an automatic software protection solution. You do not need the original source code or additional programming.

b. The UniKey® Application Programming Interface (API)

API protection involves some coding work, but we provide abundant documentation & samples to perform different functions in various programming languages. With the help of UniKey® API, you can easily achieve strong software protection and produce sophisticated software protection schemes.

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 much time and energy. There is no need to install any software or drivers before using it.

Free Technical Support

Serving customers in over 62 countries and providing solutions to thousands of governments, companies, resellers, individual developers and institutions worldwide, SecuTech offers excellent Free Technical Support for our industry. Our technical professionals work closely with UniKey® customers to ensure the highest level of customer satisfaction and understanding of our products.

Online Support Ticket System: 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, ^[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, Fortean, 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°C ~ 85°C
Operating Temperature	0°C ~ 70°C
Humidity Rating (without condensation)	0 ~70%
Min. Operating Voltage	5V
Current Consumption (in mA)	<=150
Dimensions LxWxH (in mm)	52.8x17x7mm(±0.5) (UniKey STD) / 24.6x15x7mm(±0.5) (UniKey STD MINI)
Weight (in grams)	9g (STD)/3g (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® PRO/PRO MINI

**UniKey® PRO is Flexible, Powerful and Easy with A Variety of Licensing Models!
Strong Software Protection in a Network Environment**

UniKey® PRO is the most advanced system available for protecting software running in a network environment. A single key connected to any machine in the network allows up to 65,535 concurrent users. UniKey® PRO comes with a many options to monitor and manage your software's users, they range from: White/Black lists to a real time IP Monitor. The UniKey® PRO also contains the features of UniKey® STD.

Unique and Strong Protection for Software

- Secure communication between dongle and USB port, employing strong encryption.
- Each UniKey® dongle features a globally unique Hardware Identification Number (HID), as well as a customizable Software Identification Number (SID).
- Best-in-class tools for automatic protection (Enveloper, without source modification).
- UniKey® API enables to customize your protection and embed calls to your protection keys throughout your application's source code.

Strong & All-round Protection

UniKey® offers two different protection methods:

a. The UniKey® Enveloper

UniKey® Enveloper is the fastest way to protect your executable files. It adds a protective shield around executable files and DLLs.








UniKey® Enveloper is an automatic software protection solution. You do not need the original source code or additional programming.

b. The UniKey® Application Programming Interface (API)

API protection involves some coding work, but we provide abundant documentation & samples to perform different functions in various programming languages. With the help of UniKey® API, you can easily achieve strong software protection and produce sophisticated software protection schemes.

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

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 period of the license.

Network Functionality

Supports network functionality, allowing a controlled number networked clients to operate on a single UniKey device attached to the network off the device's privileges, with support for black- and white-listing, elected licensing schemes, common firewalls and subnet crossing.

Free Technical Support

Our technical professionals work closely with UniKey® customers to ensure the highest level of customer satisfaction and understanding of our products. Serving customers in over 62 countries and providing solutions to thousands of governments, companies, resellers, individual developers and institutions worldwide, SecuTech offers excellent Free Technical Support for our industry.

Online Support Ticket System : www.eSecuTech.com/support/

Technical Specifications-UniKey® PRO / PRO MINI

Security	
Hardware ID	Globally unique, 32-bit
Software ID	User-defined, 32-bit
Protection	Envelope 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, Fortean, 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°C ~ 85°C
Operating Temperature	0°C ~ 70°C
Humidity Rating (without condensation)	0 ~70%
Min. Operating Voltage	5V
Current Consumption (in mA)	<=150
Dimensions LxWxH (in mm)	52.8x17x7mm(±0.5) (UniKey PRO) / 24.6x15x7mm(±0.5) (UniKey PRO MINI)
Weight (in grams)	9g(PRO) / 3g (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® Time

UniKey® Time Takes Care of Your Software Every Minute!

A Comprehensive Dongle with a Real Time Clock Inside for Renting and Leasing Software

UniKey® Time hardware key is specially 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 compete and timely control of sales to end users in a periodical manner. This function is based on a real time clock deposited in the dongle indicating the specific time (hour: minute: second) and date (day/month/year). The UniKey® Time also contains the features of UniKey® PRO

Unique and Strong Protection for Software

- Secure communication between dongle and USB port, employing strong encryption.
- Each UniKey® dongle features a globally unique Hardware Identification Number (HID), as well as a customizable Software Identification Number (SID).
- Best-in-class tools for automatic protection (Enveloper, without source modification).
- UniKey® API enables to customize your protection and embed calls to your protection keys throughout your application's source code.

Strong & All-round Protection

UniKey® offers two different protection methods:

a. The UniKey® Enveloper

UniKey® Enveloper is the fastest way to protect your executable files. It adds a protective shield around executable files and DLLs.









UniKey® Enveloper is an automatic software protection solution. You do not need the original source code or additional programming.

b. The UniKey® Application Programming Interface (API)

API protection involves some coding work, but we provide abundant documentation & samples to perform different functions in various programming languages. With the help of UniKey® API, you can easily achieve strong software protection and produce sophisticated software protection schemes.

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

Network Functionality

Supports network functionality, allowing a controlled number networked clients to operate on a single UniKey device attached to the network off the device's privileges, with support for black/white-listing, elected licensing schemes, common firewalls and subnet crossing.

Driverless

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

Real Time Clock

UniKey® Time utilizes a real-time clock in every dongle. As a result, a more flexible real-time functionality control and protection can be implemented with UniKey® Time. Since the real time clock inside UniKey® Time is independent of the host computer's clock, the timing with UniKey Time is more secure and accurate than its competitors. Software vendors can set the current time to the real time clock inside UniKey and check the software expiration time.

Free Technical Support

Our technical professionals work closely with UniKey® customers to ensure the highest level of customer satisfaction and understanding of our products. Serving customers in over 62 countries and providing solutions to thousands of governments, companies, resellers, individual developers and institutions worldwide, SecuTech offers excellent Free Technical Support for our industry.

Online Support Ticket System : 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, Fortean, 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°C ~ 85°C
Operating Temperature	0°C ~ 70°C
Humidity Rating (without condensation)	0 ~ 70%
Min. Operating Voltage	5V
Current Consumption (in mA)	<=150
Dimensions LxWxH (in mm)	52.8x17x7mm (±0.5)
Weight (in grams)	9g
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

**The 1st Driverless Dongle with Secure Mass Storage
Greater Piracy Protection with Secure Flash Memory**

UniKey® Drive, an innovative USB device that allows software vendors to protect, license & deliver their software applications, drivers and data to end-users using a single USB key. As the first driverless dongle with secure mass storage, UniKey® Drive empowers software vendors with the flexibility to choose the level of protection/licensing options and the ability to deliver fully licensed and protected software. The UniKey Drive contains all the features of UniKey PRO, with the added Mass Storage Flash Memory.

Unique and Strong Protection for Software

- Secure communication between dongle and USB port, employing strong encryption.
- Each UniKey® dongle features a globally unique Hardware Identification Number (HID), as well as a customizable Software Identification Number (SID).
- Best-in-class tools for automatic protection (Envelope, without source modification).
- UniKey® API enables to customize your protection and embed calls to your protection keys throughout your application's source code.

Strong & All-round Protection

UniKey® offers two different protection methods:

a. The UniKey® Envelope

UniKey® Envelope is the fastest way to protect your executable files. It adds a protective shield around executable files and DLLs.

UniKey® Envelope is an automatic software protection solution. You do not need the original source code or additional programming.

b. The UniKey® Application Programming Interface (API)

API protection involves some coding work, but we provide abundant documentation & samples to perform different functions in various programming languages. With the help of UniKey® API, you can easily achieve strong software protection and produce sophisticated software protection schemes.

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

Smart-card Technology

UniKey Drive is based on smartcard technology, which is used to protect software by storing & executing programs, algorithms and data on the device in isolation from the user's machine. This significantly improves the security and protection of data.

Available Partitions

Hidden Drive can be viewed by the Operating System (OS) as Mass Storage & allows for free manipulation of the data by the OS.

Password Protected Partition can be viewed by the Operating System (OS) as Mass Storage & allows for free manipulation of the data by the OS.

Virtual CD-ROM Partition is emulated as a CD-ROM. This allows users to view/read but not modify them, therefore the security and integrity of the files within this partition is guaranteed.

Hidden Drive is a partition that will not appear in the OS directory, therefore can only be accessed by the use of API. Since the encrypted partition is invisible to end-users this allows for safe storage of credentials and other similar sensitive data.

Free Technical Support

Our technical professionals work closely with UniKey® customers to ensure the highest level of customer satisfaction and understanding of our products. Serving customers in over 62 countries and providing solutions to thousands of governments, companies, resellers, individual developers and institutions worldwide, SecuTech offers excellent Free Technical Support for our industry.

Online Support Ticket System : www.eSecuTech.com/support/

Technical Specifications-UniKey® Drive

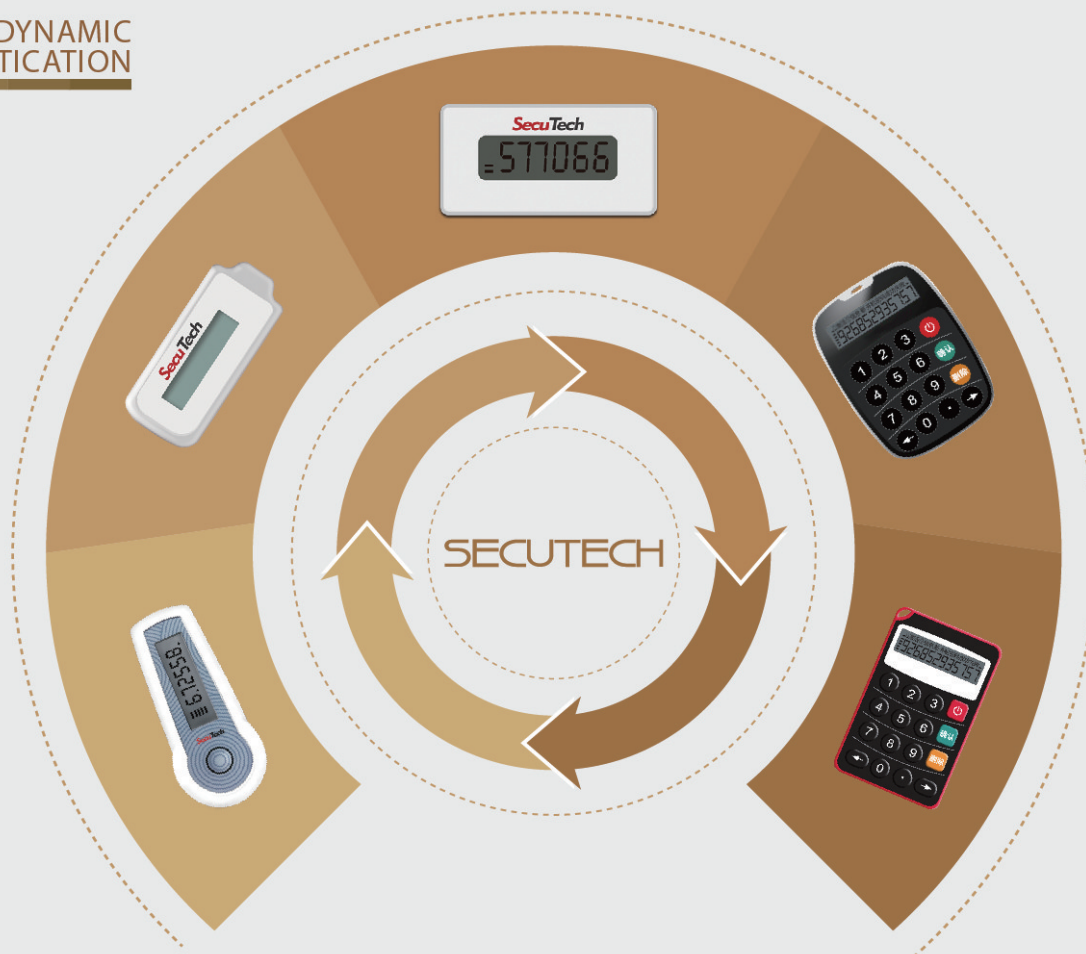
Security	
Hardware ID	Globally unique, 32-bit
Software ID	User-defined, 32-bit
Secure Communication Channel	128-bit AES encryption
Data Encryption	RSA, AES
Protection	Enveloper protection, API protection
Memory	
Capacity	2G/4G/8G/16G/32G/64G
Memory Data Retention	at least 30 years
Memory Cell Rewriters	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, Fortean, 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°C ~ 85°C
Operating Temperature	0°C ~ 70°C
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 (in grams)	9g
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 centred as the premier concern by most organizations, especially those which need high volume data transaction through a network, such as government, military, corporations, financial institutions, hospitals and private businesses. As multi-factor authentication requires multiple means of identification at login it is therefore widely recognized as the most secure method for authenticating access to data and applications. To help organizations increase their data security and reduce their IT costs, SecuTech promotes the highly secure multi-factor authentication solution UniOTP which complies with the OATH standard and is ideal for remote access solutions.

The world's most popular and convenient remote user authentication solution

UniOTP's wide range of two-factor strong authentication solutions ensure that only authorized individuals can access your organization's sensitive information-enabling more efficient business, protecting your data, lowering IT costs and boosting user productivity. UniOTP helps enterprises protect secure data, enable new business models to provide secure access to employees, customers and partners, and bring confidence to everyday transactions anywhere.

UniOTP one-time solution can be used in wide range of industries and very easy to deploy. After doing comprehensive research and analysis, SecuTech is ready to provide sophisticated solutions to different users, including:

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

By choosing SecuTech UniOTP as an authentication solution, enterprises can reduce the overhead costs of distributing replacement tokens and drive down the overall cost of security while providing a consistent and easy to use authentication experience for end users. SecuTech offers the broadest range of authenticators provided and SecuTech can meet the priority of users in cost, convenience and security. UniOTP authenticators help you protect essential data and can guarantee the identities of persons, devices and applications which exchange that information. With UniOTP's authentication solutions, you can strengthen VPN security for remote access, protect data on laptops and desktop computers, enhance network access security and perform secure password management with:

- | | |
|-----------------------------------|----------------------------|
| —Dynamic Authentication | —Strong Security Guarantee |
| —Turnkey Solution for End-users | —A Tamper-Resistant Design |
| —A Wide Variety of Authenticators | |

Dynamic Authentication

The traditional password is static, which is less secure and more vulnerable to a replay attack. For an enterprise depending on broad distribution of tokens to protect access to information and applications, token reliability is a major concern. UniOTP® offers enterprises leading levels of strong authentication by generating various passwords endlessly to eliminate password exposure and meet security requirements. The dynamic passwords are generated by a series of efficient algorithms compliant with OATH standard, and will be invalid after the time/event limit.

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

Dimensions (LxWxH)

UniOTP300/500	59x26x10 (mm)
UniOTP310	45x19.4x7 (mm)
UniOTP510	46.4x24x8.6 (mm)
UniOTP700	72x46.5x3.2 (mm)
UniOTP710	69x52x3.5 (mm)

Weight

UniOTP300/500	14g
UniOTP310	8g
UniOTP510	10.5g
UniOTP700	39.3g
UniOTP710	13.3g
Materials	Engineering Plastic
Water Resistance	Daily
Battery Lifetime	3 or 5 years
Display	Liquid Crystal (LCD)
Server Support	UniOTP Authentication System V1.0
Operating Temperature	-10 0C - 50 0C
Warranty	1-5 years Warranty
Product Safety Standards	CE, RoHS



UniOTP 300

UniOTP 300 is an event-based authenticator. It generates a new one-time-password when the button on the device is pressed. Each password will be displayed on the LCD screen for 60 seconds and has an inbuilt antidrift mechanism that prevents a new password from being generated for 60 seconds.



UniOTP 310

UniOTP 310 is also an event-based authenticator. Its features are identical to the UniOTP 300 however it has a sleek case and does not have the antidrift mechanism which may be required for certain systems.



UniOTP 500

UniOTP 500 is a time-based authenticator. With an accurate clock inside, it automatically generates and displays a new password every 60 seconds. The hardware device must be synchronized with a remote authentication server prior to use. The 60 second cycle can be changed to suite different systems.



UniOTP 510

UniOTP 510 is also a time-based authenticator. Its features are identical to the UniOTP 500 however it has a sleek case with no buttons.



UniOTP 700

UniOTP 700 is a challenge/response (OCRA)-based authenticator which uses the added security of PIN protection and challenge response. Compared to the regular one-time password, the UniOTP 700 is activated with a verification code generated by the server, after the users inputs their user name and static password, it will then generate a one-time, dynamic password.



UniOTP 710

UniOTP 710 is also a challenge/response (OCRA) based authenticator with identical features to the UniOTP 700, however it is a much thinner OCRA device which can fit into a wallet comfortably.

DYNAMIC AUTHENTICATION

SecuTech offers the industry's broadest range of authenticators to meet your needs whether cost, convenience or security is your priority. UniOTP authenticators generate highly secure one-time passwords ensuring that only properly authenticated users are authorized to have access to critical applications and data. UniOTP authenticators comply with OATH standards and are ideal for remote access solutions. UniOTP authenticators are available in both: event-based and time and challenge response versions, they never expire and do not require battery replacement.

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.



MOBILE AUTHENTICATION

NEXT-GENERATION AUDIO-BASED TWO-FACTOR AUTHENTICATION

Traditional USB Tokens provide a scalable two factor authentication security solution for desktops, VPNs, WLANs and Web portals to enhance enterprise security, but it can not be used for mobile devices. UniMate, the first dual enabled two factor authentication token providing customers with more flexibility and choice for both PC and mobile devices.

SecuTech UniMate TRRS and USB DUAL-Enabled two-factor authentication token enables customers to manage a broad range of authentication credentials, including one time password, digital certificates and static passwords, it's easy to works on iPhone, iPad, Android, PC and Mac, and it is the first security token available for both PC, smart phones and other mobile devices which can work seamlessly between devices.



UniMate STD

Innovative certificate-based authenticators provide secure access to the internet for both mobile and PC platforms which require strong authentication. UniMate is the most economic solution with high security.



UniMate Flex

Focus on mobile banking security. The 2-factor interactive authenticator with LCD display is specially designed to secure your mobile banking account. All transaction details, including bank account, payee's name and transfer amount will be displayed on the UniMate Flex screen. To make a successful transaction, you must press the confirm button. All these procedures guarantee the safety of mobile banking, and eliminate the risk of your transaction being intercepted by criminals.



UniMate USB

FIPS 140-2 Level 2 Certified PKI Token for PCs and mobiles.



UniMate Mini

Cost-effective and Portable FIPS 140-2 Level 2 Certified PKI Token for PCs and mobiles.



UniMate Drive

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



UniMate® STD Datasheet

FIPS 140-2 Level 2 Certified PKI Token for PCs and Mobiles

Highlights



FIPS Certified

UniMate is FIPS 140-2 certified, passing strict technical requirements for use by enterprises, governments and even the military. FIPS 140-1 and 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 140-1 and FIPS PUB 140-2.



All-in-one Smart Card

UniMate 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.



Smart Phone Compatible

Different from traditional USB tokens, UniMate is the first to bring smart card PKI authentication to smart Phone devices. With the help of UniMate PKCS#11 libraries and support for iOS and Android, users can perform strong authentication on their mobile devices.



Rich Middleware

UniMate STD 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 enable trouble free integration with MS-CAPI and PKCS#11 compliant software.

Highly Configurable

OEM customization is available to customize UniMate to your business needs.

Customization options include logo laser engraving, custom case design, custom color options, as well as custom HID/naming service, and more.

Features

- Chip Card Interface Device (CCID) USB protocol
- Durable and reliable
- Tamper evident ABS engineering plastic case
- Easily fits onto your key-rings
- Full compatibility with Android, iOS
- PKI application support including:
 - CSP/PKCS#11 support
 - X.509v3 standard certificate format
 - Multiple key storage
- Sophisticated SDK enables further app development and integration
- Intelligent power management system
- Rechargeable battery
- OEM service tailored to customers' needs
 - Encryption algorithm customization
 - Logo customization
 - Appearance customization
 - Gold-plated plug
- FIPS 140-2 certified
- On-board 2 MB auto-run drive
- Optional functionality including:
 - NFC capability
 - Binding to a specific SIM card, mobile device and app

	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.

Technical Specifications-UniMate® STD

Hardware

Audio Jack Port	Globally unique, 32-bit
USB Interface	USB Type A
Hardware ID	64 bits, globally unique
Weight	12 g
Internal Memory	> 16 KB
Dimensions	42.5x31.8x11.1 (mm)
Smart Card	High performance smart card. Supports RSA, 3DES, SHA, AES, GOST/DSTU and more.
USB Communication	CCID
Power Supply	Lithium-ion rechargeable battery
Middleware	PKCS#11/Mini-Driver/MS-CAPI Audio Authentication/API X.509 Digital Certification
Supported Platforms	Mobile OS: iOS, Android, Symbian, Window Phone
Supported Operating Systems	Windows, Linux, Mac OS X
Auto Run	2MB Virtual CD-ROM Partition

Performance Index

Time For Digital Signing via Audio	<2 s
Time For Digital Signing via USB	<0.5s

Battery

Capacity	180 mAh
Expected Lifetime	3 years
Minimum Recharge Cycles	500
Type	Lithium-ion Rechargeable Battery

Certifications

Computer Security	FIPS 140-2
Manufacturing	CE/FCC (FCC Declaration of Conformity) RoHS (Restriction of Hazardous Substances Directive)

Device Identification

Hardware ID	64-bit globally-unique
-------------	------------------------

Features

Hardware Encryption Algorithms	AES/DE/RSA/3DES
Hardware Hashing Algorithms	MD5/SHA-1

Memory

Capacity	16 KB
Memory Cell Rewrites	100,000
Memory Data Retention	30 years

Performance Index

Digital Signing (via TRRS)	< 2 seconds
Digital Signing (via USB)	< 0.5 seconds

Physical

Case Material	Tamper-resistant ABS Plastic
Color (Factory Default)	Black
Device Interface	USB Type A, 3.5mm TRRS
Humidity Rating (Without Condensation)	0 - 70%
Minimum Operating Voltage	4.7 V
Operating Temperature	10 °C ~ 40 °C
Storage Temperature	-10 °C ~ 70 °C
USB Protocol	CCID (Chip Card Interface Device)

Platforms

Mobile Operating Systems	iOS/Android/Symbian/Windows Phone
Operating Systems	Windows/Mac OS X/Linux

Warranty

Manufacturing & Material Defects	1 year
----------------------------------	--------



UniMate® Flex Datasheet

FIPS 140-2 Level 2 Certified PKI Token for PCs and Mobiles

Highlights



FIPS Certificated

UniMate is FIPS 140-2 certified, passing strict technical requirements for use by enterprises, governments and even the military. FIPS 140-1 and 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 140-1 and FIPS PUB 140-2.



All-in-one Smart Card

UniMate 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.



Smart Phone Compatible

Different from traditional USB tokens, UniMate is the first to bring smart card PKI authentication for smart Phone devices. With the help of UniMate PKCS#11 libraries and support for iOS and Android, users can perform strong authentication on their mobile devices.



Visual Confirmation

UniMate Flex uses an in-built 128x64 pixel LCD screen to display the data to be digitally signed. The hashing, signing and displaying processes are all performed on-device, ensuring the entire process is secure.



International Language Support

UniMate Flex offers support for numerous international languages including English, Japanese, Chinese, Russian, Spanish and Portuguese.



Rich Middleware

UniMate STD 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 PKCS#11 compliant software.

Highly Configurable

OEM customization is available to Customize UniMate to your business' needs. Customization options include logo laser engraving, custom case design, custom color options, as well as custom HID/naming service, and more.

	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 Customize 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.

Features

- Scratch resistance screen cover
- Chip Card Interface Device (CCID) USB protocol
- Durable and reliable
- Tamper evident ABS engineering plastic case
- Easily fits onto your key-rings
- Full compatibility with Android, iOS
- PKI application support including:
 - CSP/PKCS#11 support
 - X.509v3 standard certificate format
 - Multiple key storage
- Sophisticated SDK enables further app development and integration
- Intelligent power management system
- Rechargeable battery
- OEM service tailored to customers' needs
 - Encryption algorithm customization
 - Logo customization
 - Appearance customization
 - Gold-plated plug
- FIPS 140-2 certified
- On-board 2 MB auto-run drive
- Optional functionality including:
 - NFC capability
 - Binding to a specific SIM card, mobile device and app

Technical Specifications-UniMate® Flex**Hardware**

Audio Jack Port	3.5mm TRRS
USB Interface	USB Type A
Hardware ID	64 bits, globally unique
Weight	23 grams
Internal Memory	> 16 KB
Dimensions	65x36x11.4(mm)
Smart Card	High performance smart card, supports RSA, 3DES, SHA, AES, GOST/DSTU etc
Control Buttons	4 buttons: prev/next page buttons/confirmation button/cancel button
LCD Display	Monocolor display/128x64 points/supports sleep screen customization
USB Communication	CCID
Power Supply	Lithium-ion rechargeable battery
Middleware	PKCS#11 Minidriver MS-CAPI Audio Authentication API X.509 Digital Certification
Supported Platforms	Mobile OS: iOS, Android, Symbian, Window Phone PC: Windows, linux, Mac OS X
Auto Run	2MB Virtual CD-ROM Partition
Performance Index	
Time For Digital Signing via Audio	<2 s
Time For Digital Signing via USB	<0.5s

FIPS



UniMate® USB Datasheet/Mini Datasheet

FIPS 140-2 Level 2 Certified PKI Token for PCs and Mobiles/

Cost-Effective and Portable FIPS 140-2 Level 2 Certified PKI Token for PCs and Mobiles



FIPS Certified

UniMate is FIPS 140-2 certified, passing strict technical requirements for use by enterprises, governments and even the military. FIPS 140-1 and 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 140-1 and FIPS PUB 140-2.



All-in-one Smart Card

UniMate 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 STD 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 PKCS#11 compliant software.

Highly Configurable

OEM customization is available to customize UniMate to your business needs.

Customization options include logo laser engraving, custom case design, custom color options, as well as custom HID/naming service, and more.

	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

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

Capacity

Onboard capacity	> 64 KB
Flash memory	2GB, 4GB, 8GB, 16GB, 32GB
Dimensions	52.8 x 17 x 7 mm(UniMate USB)/24.6 x 15 x 7 mm(UniMate Mini)
Weight	6.3 g

Temperature

Operating	0°C to 70°C
Storage	-10°C to 85°C
Humidity Rate	0-70% without condensation
Min.Operating Voltage	5 V

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
----------------------------------	-------

Certifications

Computer Security	FIPS 140-2
Manufactory	CE/FCC (FCC Declaration of Conformity) RoHS (Restriction of Hazardous Substances Directive)

Device Identification

Hardware ID	32-bit globally-unique
-------------	------------------------

Features

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

Memory Cell Rewrites	At least 100,000
Memory Data Retention	At least 10 years

Performance Index

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

Physical

Case Material	Tamper-Resistant Metal
Color (Factory Default)	Grey
Current Consumption	50 mA
Device Interface	USB 2.0
Humidity Rating (without condensation)	0 - 70%
Minimum Operating Voltage	5 V
Operating Temperature	0 °C ~ 70 °C
Storage Temperature	-10 °C ~ 85 °C
USB Protocol	CCID (Chip Card Interface Device)

Platforms

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	One year
----------------------------------	----------

PKI



UniMate® Drive Datasheet

Selective Mass Storage

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

Two-Factor Authentication

As opposed to single-factor authentication, where often a password is only needed to authenticate, two-factor authentication requires two factors: "Something You Know" and "Something You Have". Both the correct password ("Something You Know") with the correct UniMate device ("Something You Have") is needed to successfully complete the authentication process. UniMate features the ability to generate encryption keys and store passwords, digital certificates and personal credentials within the key.

High-Performance Smart Card Based Device

Although RSA encryption is computationally intensive, the device is optimized with an on-board smart card to generate RSA encryption key pairs quickly, enabling sophisticated security with minimal hassle and effort.

Multi-Level Permission Management

UniMate utilizes three levels of token permission management: Administrator, User and Guest, where Administrator holds the highest permission level to 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 permissions.

Secure File System

In addition to secure authentication, UniMate also provides users with a secure file system. The file system operates using a multi-level protection method to protect digital credentials. UniMate implements three separate levels of permissions: Administrator, User and Guest. Any operation on the UniMate device requires explicit permission, where operations on the device are granted to users with the necessary permissions.

Mass Storage

The two partitions on the device are the normal partition and Virtual CD-ROM partition.

Technical Specifications-UniMate Drive

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	✓

Normal Drive

The normal partition functions as ordinary flash memory that can be used to store files and other data, with capacity up to 32GB and is customizable on a customer's requests.

Virtual CD-ROM

After formatting the partition with your data, the Virtual CD-ROM partition appears as a CD-ROM disc upon connecting the UniMate Drive. Much in the same way as CD or DVD, the contents of the virtual CD-ROM can only be read but not modified. All files stored in the Virtual CD-ROM partition are protected against unauthorized deletion or modification, guaranteeing the integrity of data.

Customization Service

OEM customization is available to customize UniMate to your business' needs.

Customization options include logo laser engraving, custom case design, custom color options, as well as custom HID/naming service, and more.

Technical Specifications-UniMate® Drive

Capacity	
Onboard capacity	> 64 KB
Flash memory	2GB, 4GB, 8GB, 16GB, 32GB
Dimensions	57 × 16 × 8 mm
Weight	9 grams
Temperature	
Operating	0°C to 70°C
Storage	-10°C to 85°C
Humidity Rate	0-70% without condensation
Min. Operating Voltage	5 V
Humidity	USB 2.0 high speed
Operating Systems Supported	Windows 2000, XP, 2003, Vista, 7, 8, 10, Server 2008 2012 and Linux (both 32-bit and 64-bit)
Hardware Algorithms	
Data	AES Cipher-Block chain model
Encryption Keys	256-bit Hardware
PKI	PKCS#11, MS-CAPI
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



UniReader® (TRRS IC)

Pay with your card easily and securely on your mobile device with UniMate Reader's compact point-of-sale card reader.

Enabling smart phone e-commerce, UniReader provides mobile card reader hardware solutions to app developers and financial businesses relying on smart phone devices (iPhone, Android, and more). The UniReader family includes magnetic strip & integrated chip certified devices with TRRS & USB connectors.

Features



Innovative hybrid interface design supports both mobile and PC platforms

- Audio jack port for iPhone, iPad, iPod, Android phones and tablets
- USB port for PC with driverless, plug-and-play technology



Convenient payment

- Pay with your iPhone, iPad, or Android phone anytime, anywhere
- Install the mobile app and be ready to pay in minutes



Secure transactions

- UniMate Reader provides encrypted, end-to-end security



Sensitive data stored in the device



Data Stored •

Hybrid Interface •

Secure Transaction •

Convenient Payment •

New Solution To Pay By Card •

- The most cost-effective mobile POS solution
- Portable design, convenient to take anywhere
- Tamper-evident ABS engineering plastic case
- Sophisticated SDK enables greater app development and ease of integration
- Intelligent power management system
- Rechargeable battery
- OEM service – tailored to customers' needs
 - Logo customization
 - Appearance customization
 - Gold-plated plug
- Optional functionality
 - NFC available
 - Binding to a specific SIM card, mobile device and app
 - CPU card support
 - Certificate-based authentication

Hardware

Dimensions L×W×H (in mm)	43.5x42x10.4
Weight (in grams)	15g
Operating Temperature	0°C to 50°C, 15 to 85% humidity, non-condensing
Humidity	15 to 90% humidity

EMV Card Reader

Smart Card Interface Standard	ISO7816
Type of Card Contact	Friction contact
Software Interface Standard	EMV
Rail and Cover Life	1,000,000 Passes Minimum.

Mobile Identity Management

Mobile devices are playing an increasingly integrated role in our lives on account of the rapid popularity of smart phone devices. As a consequence, with the increasing capabilities and complexity of mobile devices and the gradually growing incorporation of sensitive information on them, the added convenience brought by mobile devices also bring new security risks.

This could not be truer for mobile banking. Users performing transactions and banking tasks on mobile devices risk theft of bank account details via a host of methods. Other sources of personally identifiable information can be stolen from mobiles phones and used in illicit activity. According to the 2011 Mobile Threat Report by Lookout, a highly-regarded mobile security company, “attackers are deploying a variety of increasingly sophisticated techniques to take control of the phone, personal data, and money” and malware writers are recurrently “using new distribution techniques”. Mobile malware is on the rise and no platform is unsusceptible, affecting Android, Symbian, Blackberry, iPhone and users of other platforms; evidently, more secure methods for performing tasks such as online banking safely are necessary.

On top of secure verification of online transactions, hardware-based multi-factor authentication on the mobile platform is achievable thanks to SecuTech’s innovative USB to TRRS adapter. The adapter leverages the TRRS audio interface on mobile platforms for use with USB interface authenticators, converting the signal between the two interfaces and bridging the gap between authentication solutions on different platforms. Mobile devices possess the capacity for multi-factor authentication, allowing sensitive use of mobile devices by organizations whilst ensuring critical data is tightly secured with robust authentication measures.

SecuTech offers UniMate STD and Flex, two multi-factor authentication devices designed primarily for use with mobile banking, whereby the addition of a physical device to the transaction process significantly increases the difficulty of bank account theft. UniMate Reader was designed by Secutech for secure mobile point-of-sale, capable to be used with TRRS interfaces and enabling the secure use of cards for transactions anywhere. In bringing strong authentication to the mobile platform, UniMate STD and Flex enables two-factor USB authenticators to be used with mobile devices, with ease of implementation and exceptionally minimal migration cost.

Mobile Banking Verification

Designed specifically for banking on the mobile platform, requiring interaction with the physical device to successfully complete the transaction process. Safeguards bank account credentials from theft, where technologies employed enable secure confirmation of transactions and provide compatibility with all platforms supporting USB and TRRS interfaces.

UniMate STD

UniMate Flex



Strong Authentication

Authentication is typically a signing-on process where a person proves his or her identity with certain proof. The process is used to ensure that a user is who they claim to be. Strong authentication is achieved through the use of more reliable identification evidence, required by the login/access 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 the industry's best practices and only uses well-established and thoroughly tested cryptographic algorithms. The passwords and credentials stored on security products are encrypted onboard 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**

The security product from SecuTech is designed for 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. The administrator holds the PIN, which is confidential to the end user.

**VPN Security**

VPNs are generally considered to have very 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

CONSIDERATION

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

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 the products by SecuTech are environmental friendly and we also provide the service recycling service for customers.

Driverless

SecuTech Solution Inc. 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**

UniKey software protection works for almost all popular OSes, including Windows, Linux, Mac OS X, FreeBSD and embedded systems, both 32 and 64 bits. UniKey provides a universal software protection solution on various platforms and makes software licensing easy. UniKey supports a range of programming languages with samples included in the SDK.

**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.





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 its 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.



OUR SERVICES

color

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 place a 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

According to different needs of customers, our security products also provide a certain amount of room for storing secure data. This capacity may vary with different products and is completely customizable.

API

APIS CUSTOMIZATION SERVICE

An 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 building blocks. A programmer then puts the blocks together. SecuTech not only provides good, robust APIs but will also customize the APIs according to various functionality requirements for customers. This guarantees high performance and operating enviroment consistency.



APAC

Suite 2.06, 32 Delhi Rd, North Ryde, NSW,
2113, Australia
T: 00612-9888 6185
F: 00612-9888 6185
E: AUS@eSecuTech.com

EMEA

4 Cours Bayard 69002 Lyon, France
T/F: +33-426002810
M: +33-609396463
E: Europe@eSecuTech.com

China

Level 4, #43 Building, #8 Dong Bei Wang Xi Lu,
Beijing, 100193
T: +8610-8288 8834
F: +8610-8288 8834
E: CN@eSecuTech.com

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