



6528B

Application Note

**Secure Your Embedded Devices
using AT90SC/SO and VaultIC**







Table of Contents

1	<i>Introduction</i>	5
1.1	High-tech Goods Counterfeiting	5
1.2	Digital Content Copy	5
1.3	Identity Theft	6
1.4	INSIDE's Secure Microcontroller Families	6
2	<i>Secure Your Hardware – Anti-cloning Solutions</i>	8
2.1	Prevent the Cloning of Your High-tech Goods	8
3	<i>Secure Your Digital Content – DRM and Software Copy Protection</i>	11
3.1	Digital Rights Management	11
3.2	On-the-fly Encryption	12
3.3	Software Protection	13
4	<i>Secure Your Privacy – Multi-factor User Authentication Solutions</i>	14
4.1	USB tokens common features	14
4.2	Implement a high-end USB token	17
5	<i>The New VaultIC Family</i>	19
5.1	Flexibility, Rapid Development/Integration for Embedded Products	19
6	<i>Conclusion</i>	21
	<i>Definitions and Acronyms</i>	23
	<i>Reference List</i>	25
	<i>Revision History</i>	26



1. Introduction

High-tech goods counterfeiting, multimedia content copying, and identity theft are all major concerns today. The proven cryptographic protocols implemented in INSIDE Secure®'s tamper-resistant microcontrollers offer a powerful turnkey solution to fight these threats. This paper presents examples of efficient and cost effective IP protection applications utilizing secure chips in various embedded systems.



Note


In the rest of the document, "INSIDE" means "INSIDE Secure".

1.1 High-tech Goods Counterfeiting

According to the 2005 report ([R1]) by accounting firm KPMG® International, fake high-tech goods (cell phones, computers, printer cartridges, etc.) account for about \$100 billion in sales lost to counterfeiters each year. This means that around 10 percent of all high-tech goods sold each year worldwide are fakes! Therefore, 10 percent of all high-tech sales are lost to the Intellectual Property (IP) owners. Besides financial considerations, counterfeiting presents noticeable collateral risks for the consumers – no guarantee that faulty goods will be replaced and fake goods may even injure the customer due to improper testing, poor quality of consumables, etc. Counterfeit goods can also severely degrade the public image of companies by deteriorating customer satisfaction not to mention that fake automotive or aeronautic spares present a real concern for public health and safety. Some renowned companies have been targeted by international criminal organizations, which have sold thousands of counterfeit-branded products in several countries. Generally speaking, famous brand-name products are more exposed to counterfeiting because they are seen as "must have" goods and therefore are easier to sell on the counterfeit market. Many accessories and peripherals (for mobile phones, personal digital assistants, portable MP3 and video players) are the target of criminals that use increasingly sophisticated manufacturing means and industrial production techniques. Any high-tech product, whatever the market (mass marketed items such as music players or even industrial equipment, machines, etc.) is vulnerable to counterfeiters who aim at making money, taking advantage of the public image of famous brands by cloning equipment/parts and selling similar products at a much lower price. Another strategy may only be cost reduction. Some companies may prefer cloning expensive equipment (e.g. network equipment) they have already purchased for their own use, thus stealing IP, rather than buying new certified products.

1.2 Digital Content Copy

Intellectual and artistic property (music, movies and software) piracy is also a real problem for the electronics industry. Even if the full cost of illegal multimedia content duplication cannot be quantified, the availability of multiple perfect copies of copyrighted materials is seen by most of the media industry as a threat to its viability and profitability. Digital media publishers have business models based around charging a fee for each copy or performance of the multimedia product. As a consequence, Digital Rights Management (DRM) was designed as a means to allow them to control any duplication and dissemination of the content. However, hackers are actively trying to crack the DRM systems. The famous Content Scrambling System (CSS) algorithm used for DVD copy protection was revealed three years after its creation to be easily susceptible to a brute force attack ([R3]). Many other recent copy protection systems have already failed. For example, the hacker of the CSS system has also hacked a famous music store system, allowing the removal of the copy protection from the purchased music files ([R4]).



Governments are now backing the fight against counterfeiting. Among these initiatives are the US Strategy Targeting Organized Piracy ([R5]), the European Association for the Protection of Encrypted Works and Services ([R6]), and the UK Foundation for Art and Creation Technology ([R7]).

1.3 Identity Theft

Another burning issue is the identity theft of web applications. According to 2010 Identity Fraud Survey Report by Javelin Strategy and Research ([R8]), the amount lost to fraud over a one-year period for online applications (banking, shopping, etc.) is estimated at \$54.4 billion in 2005 in the U.S. alone. User credentials are mainly stolen through offline means (stolen wallet, theft of paper mail, misappropriation by friends). Online attacks are relatively rare (11.6%), but according to a Gartner Survey ([R9]), phishing⁽⁴⁾ attacks are growing exponentially. In reaction to the growing threat, the US Federal Financial Institution Examination Council (FFIEC) has established a guidance ruling for user online authentication to banking services. As reported in a 2005 news ([R10]), US banks will have to comply with these rules by the end of 2006 and deploy two-factor authentication solutions (explained below) whenever needed. Microsoft® also believes that passwords are no longer reliable and enforce new strong authentication means in its Windows VISTA™ operating system. With strong authentication, each party involved in the transaction process can be confident of the other party's identity. This enables trusted e-commerce and transactions, secure logon, protection against phishing, pharming⁽³⁾ and more.

1.4 INSIDE's Secure Microcontroller Families


This paper will show how to prevent the threats mentioned with the use of INSIDE's secure microcontrollers. The high-level examples presented herein only show principle methods. Detailed references will be given for full technical explanations and implementation recommendations. Moreover, the solutions exposed herein may be patented. The proven technology used in INSIDE secure microcontrollers is already widespread and used in national ID/health cards, e-passports, bank cards (storing user Personal Identification Number, account numbers, authentication keys among others), pay-TV access control and cell phone SIM cards (allowing the storage of subscribers' unique ID, PIN code, and authentication to the network), where cloning must definitely be prevented. More than one billion of such microcontrollers have been already sold by INSIDE and successfully implemented in many secure systems. INSIDE's secure products will advantageously replace complex and expensive proprietary anti-tampering protection system. Their advantages include low cost, ease of integration, higher security, proven technology.

1.4.1 Versatility

Three secure microcontroller families are available: AT90SC, AT90SO and VaultIC. The AT90SC and AT90SO are "open" solutions where the implementer can develop their own on-chip application using available INSIDE software libraries. Beyond this, the VaultIC family chips feature comprehensive embedded firmware that provides standard, public domain-proven cryptographic algorithms. This is deemed safer than using proprietary algorithms, since their strengths or weaknesses are well studied by the scientific community. The VaultIC will be further described later in this paper.

1.4.2 Tampering Resistance

AT90SC & AT90SO microcontrollers are designed to keep contents secure and avoid leaking information during code execution. While on regular CPUs, measuring current consumption, radio emissions and other side channels attacks may give precious information on the processed data or allow the manipulation of the data. INSIDE's secure microcontrollers' security



features include voltage, frequency and temperature detectors, illegal code execution prevention, tampering monitors and protection against side channel attacks and probing. The chips can detect tampering attempts and destroy sensitive data on such events, thus avoiding data confidentiality being compromised. These features make cryptographic computations secure in comparison with regular microcontrollers whose memories can be easily duplicated. It is much safer to delegate cryptographic operations and storage of secret data (keys, identifiers, etc.) to an INSIDE secure microcontroller.

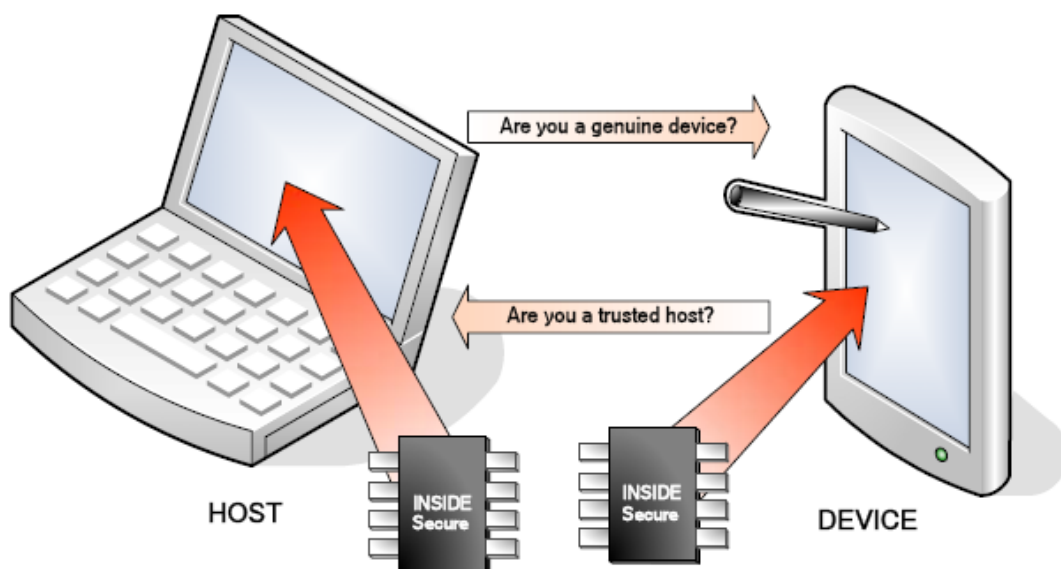
1.4.3 Success Stories

INSIDE secure microcontrollers already have successfully been integrated into embedded systems using various form factors. Applications include franking machines, tachographs, set-top boxes, network routers, etc.

2. Secure Your Hardware – Anti-cloning Solutions

INSIDE secure microcontrollers are perfectly designed to secure embedded systems. For example, the VaultIC family is especially good at preventing the connection of an unauthorized/fake sub-system to a wider system of interconnected devices (refer to [Figure 2-1](#)). This applies to scenarios as simple as a mobile phone authenticating its battery (ensuring the battery is genuine), or a little more complex such as a server authenticating a network device. When an unauthorized/counterfeit part is detected by the system, the overall functionality can be limited or even denied depending on the manufacturer's policy. Anti-cloning protection does not need not to be 100% efficient as the research presented in the June 2006 RSA® Conference by Cryptographic Research ([\[R11\]](#)) explains. The implemented protections must make cloning unprofitable to hackers: "[...therefore] using hardware tamper-resistant microcontrollers forces attackers to be invasive, or use very complex and expensive equipment."

Figure 2-1. Authentication



2.1 Prevent the Cloning of Your High-tech Goods

Anticlone is safely implemented through one-way or mutual strong authentication⁽⁷⁾. Various authentication protocols exist (refer to [\[R12\]](#), [\[R13\]](#)), but the principle method is the following:

1. The authenticator sends a challenge (e.g. a random number) to the equipment that must be authenticated ("the claimant").
2. The claimant computes a digital signature of the combination of this challenge with an optional identifier, using a private or secret key. The requested signature is then returned to the authenticator.
3. The authenticator checks the signature using either the same secret key or the public key associated to the claimant's private key and decides whether the claimant is authorized or not based on the signature verification result.

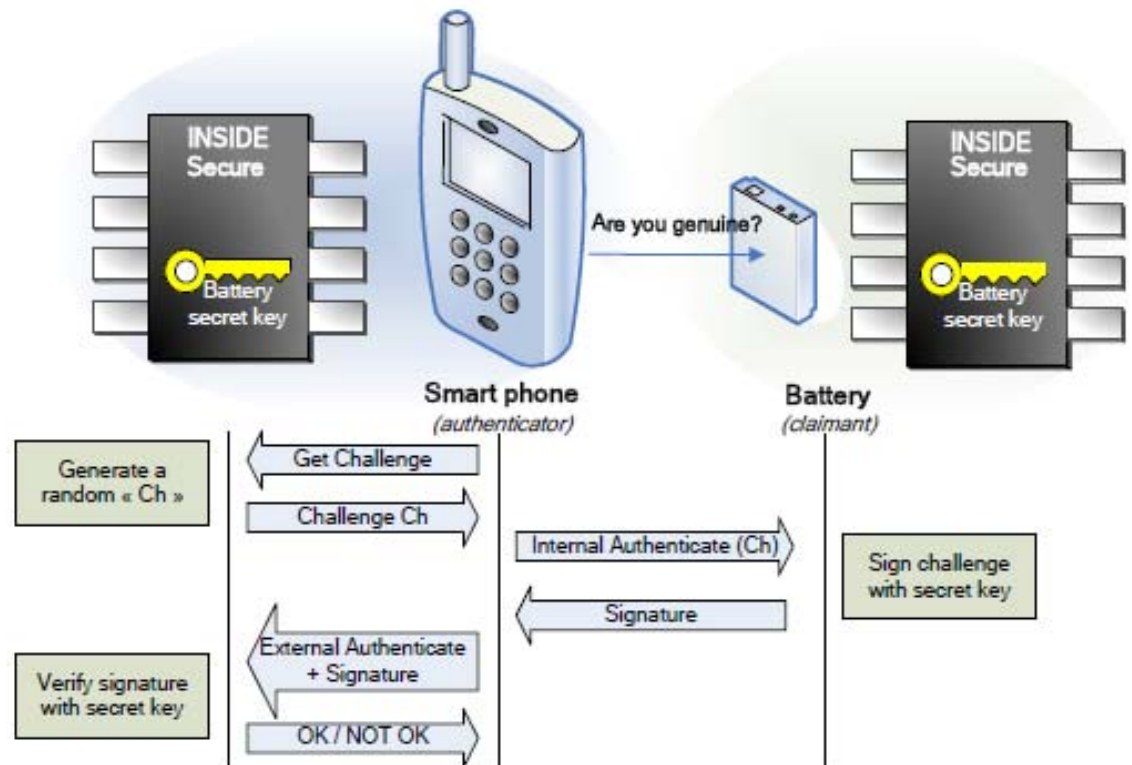
Let us illustrate this process with the example of a cell phone (the authenticator) authenticating a battery (the claimant). This example (refer to [Figure 2-2](#)) is based on the ISO/IEC 9798 standard ([\[R12\]](#)). This application can be implemented using two VaultIC chips – one in the phone and

one in the battery. The battery-side VaultIC chip contains a secret key (loaded during battery manufacturing) that can never be extracted and is utilized to compute signatures. Consequently, the VaultIC must be cloned in order to make counterfeit batteries which is practically impossible.

The phone's VaultIC contains the same secret key, either loaded during phone manufacturing, or remotely updated through an encrypted communication channel.

The battery does not need a microcontroller other than the VaultIC – the phone can be connected directly to the battery's secure microcontroller through the battery contacts.


Figure 2-2. Cell phone battery anti-cloning system example



A more detailed description of the scenario is shown below:

1. The phone sends a challenge (random number) to the battery.
 - The phone sends a "Get Challenge" command to its VaultIC. The VaultIC sends back the requested challenge.
 - The phone sends an "Internal Authenticate" command to the battery's VaultIC with the generated challenge. The battery's VaultIC then computes a signature of this challenge using the secret key.
2. The phone receives the battery's computed signature and forwards it to its own VaultIC for verification:
 - The phone sends an "External Authenticate" command, with the battery's signature, to its VaultIC.
 - The phone's VaultIC returns the validation.

The same technique can be applied to printers authenticating cartridges, a video game console authenticating a joystick, a PC (or remote web site) authenticating a portable MP3 player, a



server authenticating a network device, etc. Depending on the customer's infrastructure, symmetric key systems (DES) may be preferred to public key systems (RSA™). As a general rule, the host must be carefully designed so that the peripheral authentication process cannot be bypassed.

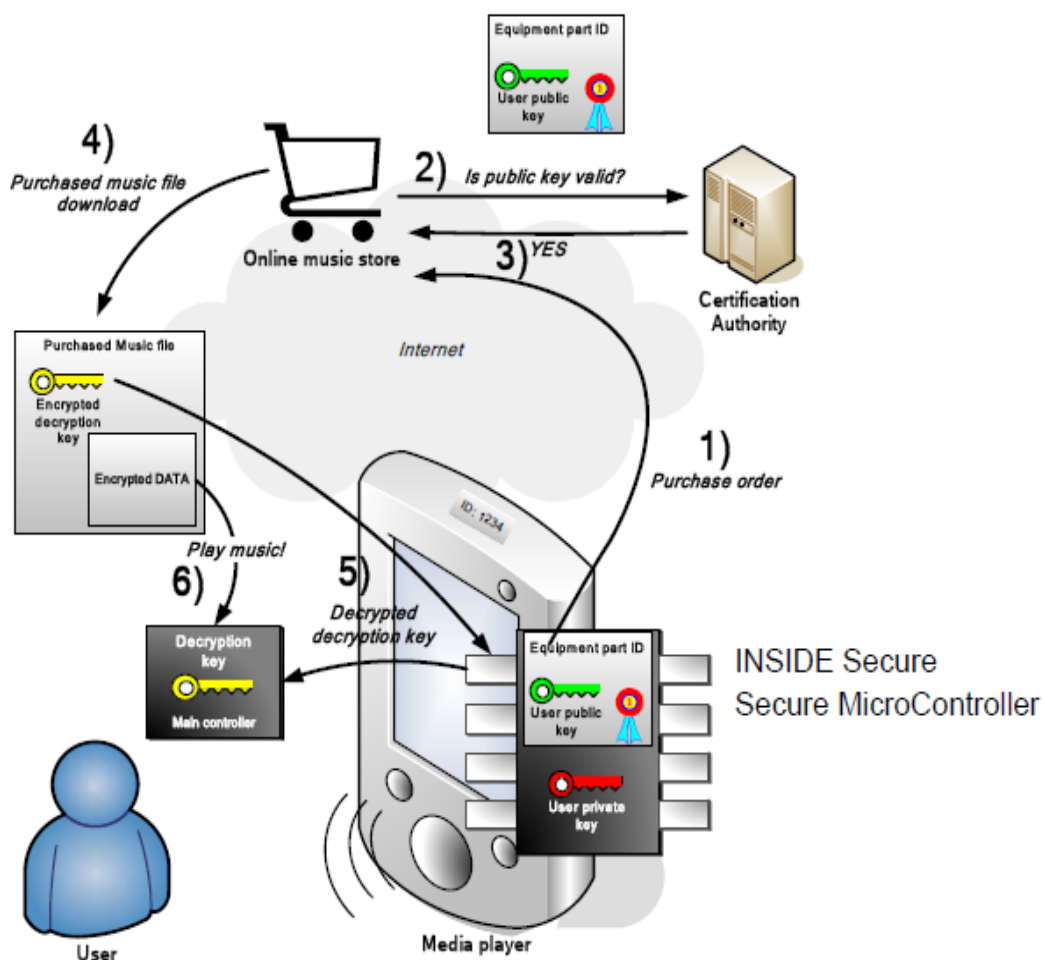
3. Secure Your Digital Content – DRM and Software Copy Protection

INSIDE secure microcontrollers will help when protecting multimedia data. They are designed for key and certificate management used in DRM, and software protection areas. DRM systems that do not run on tamper-resistant hardware cannot, theoretically, be secure since digital content can be copied at a hardware level.

3.1 Digital Rights Management

As an example (refer to Figure 3-1), let us see how to bind a music file to a single music player by using an VaultIC microcontroller. The ultimate goal of DRM is to prevent access to a digital cleartext music file that could be copied infinitely without any degradation in sound quality.

Figure 3-1. Secure media player



1. Provisioning⁽⁵⁾ : in a preliminary personalization phase, the manufacturer makes the equipment generate a specific key pair.
 - The manufacturing equipment sends a “Generate Key Pair” command to the VaultIC. The generated “user private key” remains internally stored in a file on the VaultIC and can never be extracted. The associated “user public key” is read from the equipment and certified (i.e. signed with a “certification authority” private key).

The certificate is stored back in the VaultIC. This makes it impossible to have valid public keys generated by something else other than a VaultIC personalized for this purpose. Moreover, this certificate binds the generated public key to the equipment identifier.

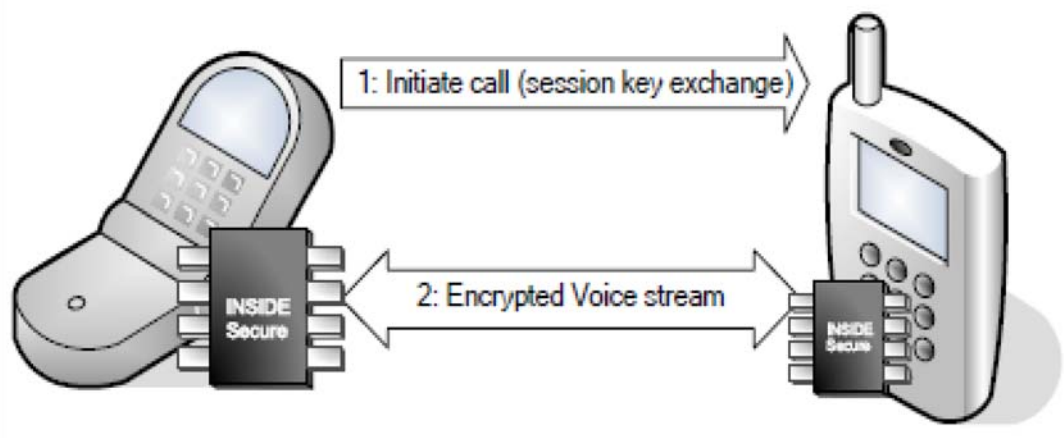
2. The customer sends a purchase order (refer to step 1) in [Figure 3-1](#)) together with its equipment part ID and public key certificate. The media player sends the command:
 - “Read Record” to fetch the certificate from the VaultIC file system.
3. The music provider checks the “user public key” validity (steps 2 and 3). Verifying the public key is necessary otherwise anyone could create their own public key pair, send it to the music store and then decrypt music files outside of DRM-enabled products.
4. The music provider encrypts the purchased music file with a random, single-usage “encryption key” that is in turn encrypted with the customer’s “user public key” (as a consequence, no one else can decrypt this decryption key).
5. The customer downloads the encrypted music file into their media player (step 4). To play it, the player’s main controller sends the following command:
 - “Decrypt Data”, where the provided data is the encrypted “decryption key”. The “decryption key” is decrypted thanks to the customer’s “user private key”.
6. The decrypted “decryption key” is sent back to the main controller (step 5). The main controller can now decrypt the music data and play it (step 6).


As a general design rule, the transmission of the decrypted keys between the secure microcontroller and the main controller must be secured either logically, by encrypting the communications, or physically (offering tamper protection), or both. However, storing cryptographic keys into a controller that is not designed to be secure is dangerous.

3.2 On-the-fly Encryption

INSIDE secure microcontrollers feature on-the-fly encryption/decryption functions that can be applied to data streams with a reasonable baud rate, for example, encrypted voice communications. On-the-fly encryption requires the use of a symmetric cipher algorithm (3DES, AES, etc.), because public key algorithms are too slow. In such applications, a symmetric session key is exchanged using a public key cryptographic protocol (refer to step 1) in [Figure 3-2](#)). For the sake of simplicity, this step is not detailed here. Some of the possible protocols include Kerberos, Authenticated Key Exchange Protocol, Diffie-Hellman, El-Gamal, and more.

Figure 3-2. Encrypted voice communication





Once the phones have established a communication channel with symmetric session keys:

1. Load the encryption/decryption key into the VaultIC:
 - Each phone sends a “Manage Security Environment” command containing the session key to its VaultIC.
2. Then voice stream can be ciphered/deciphered for as long as the communication lasts (step 2):
 - For an outgoing voice stream, the VaultIC will instantly encrypt the digitized voice stream with the “Encrypt data” command.
 - For an incoming voice stream, the VaultIC will instantly decrypt the digitized voice stream with the “Decrypt data” command.

3.3 Software Protection

Software copy protection is securely achieved by putting vital sensitive functions into a secure microcontroller integrated in a USB dongle. If the dongle cannot be cloned, the software is use-less. The software design needs to be resistant to reverse engineering so the dongle is always mandatory to the software functioning.

4. Secure Your Privacy – Multi-factor User Authentication Solutions

The methods to authenticate humans are generally classified into three cases: physical attribute (e.g. fingerprint, retinal pattern, facial scan, etc.), security device (e.g. ID card, security token, software token or cell phone), and something the user knows (e.g. a password/passphrase or a personal identification number).

To fight against identity theft, the multi-factor authentication is a stronger alternative to the classical login/password authentication (called weak authentication). It combines two or more authentication methods (often a password combined with a security token). Two-factor systems greatly reduce the likelihood of fraud by requiring the presence of a physical device used together with a password. If the physical device is lost or the password is compromised, security is still intact. The reader can refer to NIST's ([R14]) for further details.

Multi-factor authentication requires a strong authentication. Anticlone is safely implemented through one-way or mutual strong authentication. Various authentication protocols exist ([R12], [R13]), but the principle method is the following: method to complement the password authentication and this strong authentication method requires storing secret data. Pure software multi-factor solutions are thus not reliable. If sensitive data is stored in files on a hard disk, even if those files are encrypted, the files can be stolen, cloned and subjected to various kinds of attacks (e.g. brute force or dictionary attack⁽¹⁾ on passwords). Therefore secure microcontrollers-based hardware tokens are a must. Placing secrets outside the computer avoids risking exposure to malicious software, security breaches in web browsers, files stealing, etc.

Numerous companies are now providing authentication solutions based on USB tokens. Tokens connected through USB are a convenient solution since they require no additional hardware. INSIDE's turnkey USB secure microcontroller solutions can help providers focus on their security model and their application without losing too much time on tamper protection and other complex hardware security concerns.

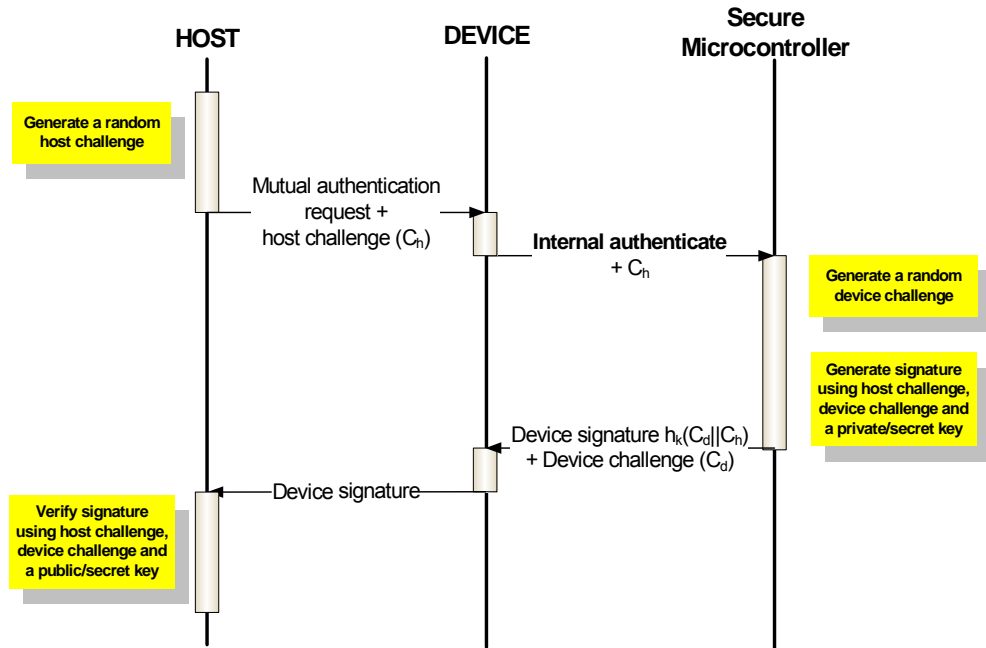
4.1 USB tokens common features

The USB tokens (refer to Figure 4-2) are generally able to:

- Perform challenge response authentication

This challenge response protocol is considered a strong authentication method. As shown in Figure 4-1, hk is a digital signature operation (such as DES, RSA, elliptic curve (ECC) signature, etc.). The "||" operator is the "concatenation" operator. Figure 4-1 shows how a device can require assistance from a secure microcontroller to identify itself to the host. Note that the usage of "challenges" (random numbers, in fact) prevents obvious replay attacks. In such a protocol, the claimant entity (in this case, the device) can produce a correct signature only if it knows the right secret/private key. If many devices share the same key, identifiers can also be involved in the authentication process to distinguish between devices.

Figure 4-1. Challenge-response unilateral authentication



- Perform one-time password generation

One-time password (OTP) is another strong authentication method that has the advantage of being usable over simple media such as phones (the OTP is dialed). This method does not require complex computations as with challenge-response authentication.

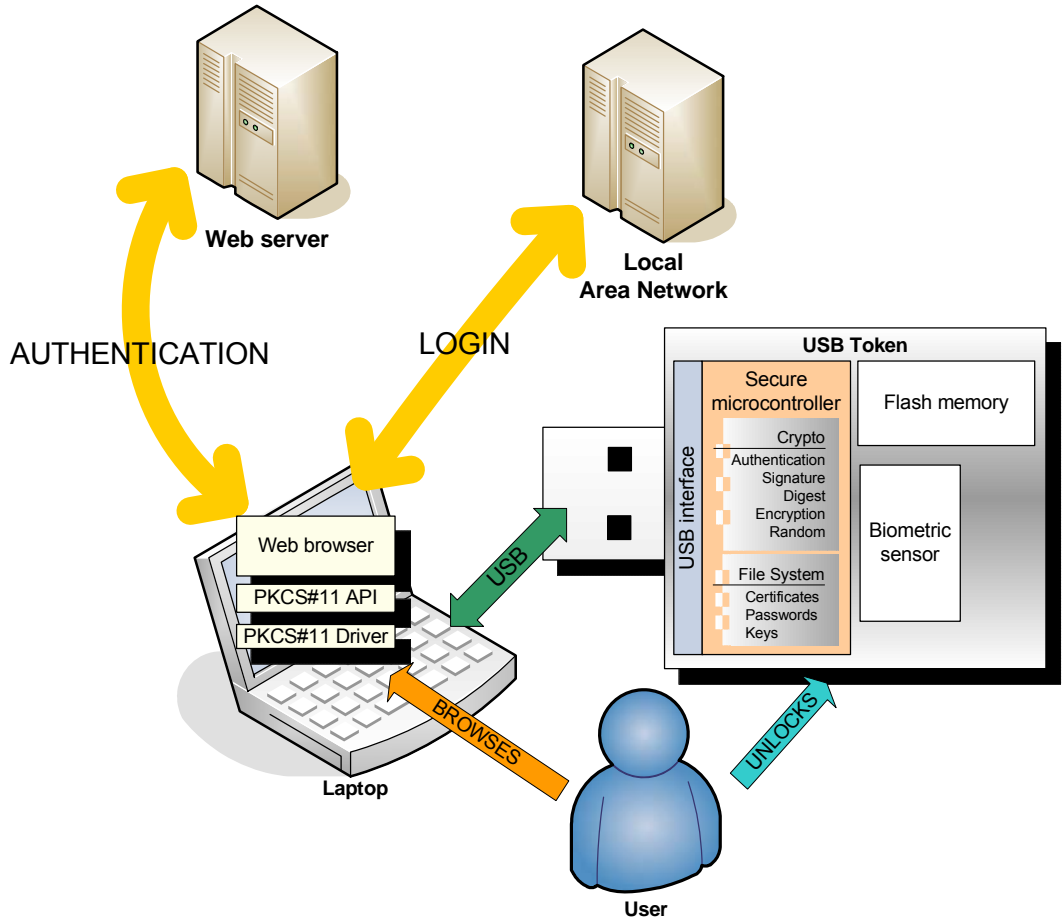
The principle method of one-time passwords is as follows ([R15] for further details). Let us assume we have a client and a server. In a preliminary provisioning step, a list of passwords is generated on the client side using a client’s secret passphrase and a seed⁽⁶⁾ from the server (it is computationally infeasible to guess password N+1 from password N, but on the server side, verifying that password N+1 is correct is straightforward knowing password N). Then, during normal usage, the user identifies himself to the “authenticator” and provides the next password in the list. Since a new password is used on each authentication attempt, and this password cannot be re-used, there is no risk of it being compromised. Besides RFC 1760, many other OTP implementations exist but standardization is pending to enable interoperability between various authentication systems ([R16] , [R17]).

- Perform token holder authentication

This feature is used to unlock the token and protect against loss or theft. This authentication can be done using a simple password, or through biometric authentication, and is necessary to prevent token access when lost or stolen. Note that biometric authentication methods must never be used in place of a password for online submission (if stolen, your identity is compromised forever) but they prove useful for offline usage (e.g. unlock hardware) because:

- They have no risk of being forgotten
- There is no need to write it down somewhere
- They are impossible to counterfeit (whereas bad passwords can be guessed)

Figure 4-2. Hardware token common features



Besides the multi-factor authentication, the following secondary features are often used in such tokens:

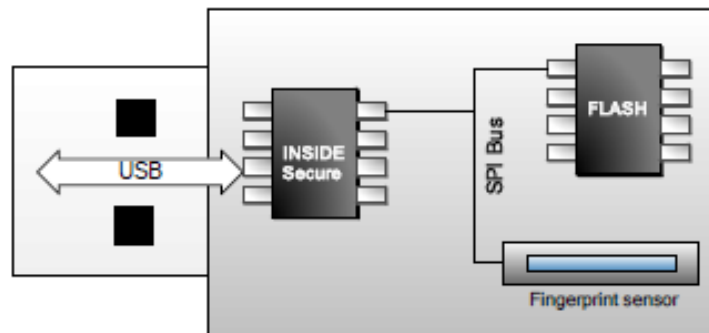
- Single sign-on. Single sign-on enables users to enter, once, a master login/password on the USB token and then gain access to a personal database of login/password entries associated to web site URLs. This enables a seamless user login on various web sites during browsing.
- Certificate storage. USB tokens can store user certificates for authentication and private keys for document signature. Storing private keys on a protected hardware token prevents anyone other than the legitimate user signing documents.
- Token sharing. Currently, most web applications require their own hardware token (one for each bank, one for the online book store, etc.). The multiplication of tokens currently deters their utilization. So token sharing is an attempt to put multiple authentication applications into a single token.
- PKCS #11 API (RSA™) or MS-CAPI (Microsoft®). These are standardized PC computer software libraries that offer high-level cryptographic services (digital signature, key generation and storage, encryption/decryption, etc.) that are mostly used by web browsers but are available to virtually any application. The cryptographic services can be implemented as pure software or rely on a hardware

token through a dedicated driver. INSIDE secure microcontrollers perfectly fit as PKCS11 ([R18]) or MS-CAPI ([R19]) compliant hardware tokens.

4.2 Implement a high-end USB token

The following example shows how to use an INSIDE secure microcontroller to rapidly develop simple, yet very secure, hardware tokens for multi-factor authentication solutions. As a comprehensive example, we are going to show how to interface an INSIDE USB secure microcontroller with Atmel fingerprint sensors ([R20]) and Atmel Flash memory mass storage through an SPI bus (subsets of this comprehensive solution can be even more easily implemented). Refer to Figure 4-3 below.


Figure 4-3. OTP-enabled, mass storage biometric USB token



4.2.1 Scenario #1

The user wants to log into their favorite e-banking web site which requires a one-time password.

1. The user connects their USB token to the PC.
2. The user provides a password/fingerprint to their USB token to prove they are a legitimate user. In the case of a password lock and depending on the system, the password may be entered on the USB token device, if it has an entry device, or typed on the PC and transmitted to the token. Direct entry is the preferred method because when entered on a PC, keyboard loggers or USB spies may intercept the user's secret data. A fingerprint must always be captured directly on to the USB token. In the case of a password lock, the following sequence of commands must be sent to the secure microcontroller:
 - Select the authentication application (Select command)
 - Request a random number (Get Challenge command)
 - Combine the password with the challenge (using a mathematical function called “hash”) and submit the combination (Submit Password command). If successful, access to the secure microcontroller cryptographic features and user personal data is then unlocked. PC applications (e.g. web browser) can then request cryptographic operations through the PKCS#11 API.
3. The user types the URL of the online banking web site into the web browser and enters its identifier on the user identification screen.
4. The web browser application now calls the PKCS#11 API to retrieve an OTP using the C_Sign function. In turn, the PKCS#11 driver sends a “GetOTP(n)” command to the USB token which will return the nth OTP, since the user has unlocked their token. This



password is then transmitted to the web site. A user two-factor strong authentication has been performed.

4.2.2 Scenario #2:

The user signs an important document stored on a Flash mass storage device.

1. As in scenario #1, the user connects the token and unlocks it through the relevant holder authentication method.
2. Special commands now allow the PC to access the Flash memory, decrypted on-the-fly by the secure microcontroller, which holds the encryption keys. The user gets the document onto their PC.
3. Upon the user's request, the document is signed by the token using the "Generate Signature" command.

5. The New VaultIC Family

The VaultIC is a new microcontroller family based on the technology implemented on the AT98SC and AT90SO series. Its embedded firmware provides a turnkey solution for the applications explained above and many more! The VaultIC family provides a generic solution to the security threats stated in this paper. The VaultIC family is an alternative to Trusted Platform Modules (TPM) for the embedded market ([R21]). VaultIC family members offer more-flexible interfaces than TPMs with a lower pin count. The key management can also be freely customized and is not as stringent as on TPMs.



Note

The AT98SC Serie is the previous generation of Security Modules.

5.1 Flexibility, Rapid Development/Integration for Embedded Products

Currently, the VaultIC family members feature:

- Various communication interfaces including SPI (Serial Protocol Interface), TWI (Two Wire Interface) and USB (Universal Serial Bus)
- Low pin count (Reset, Vcc, GND, and communication interface specific pins) so integration into an existing board is simple. VaultIC chips are available in small packages (SOIC8, QFN20, QFN44...) to fit into the most size-constrained devices.
- Low power consumption, in order to extend battery life in portable devices and low-power systems. VaultIC devices consume less than 100 μ A in standby mode, and only 5 to 15 mA during CPU⁽²⁾-intensive operations depending on the required action.
- Embedded firmware that provides advanced functions:
 - Secure dynamic file system: a fully user-defined nonvolatile storage of sensitive or secret data. Parts of the file system can be password-protected. It also stores the configuration of the cryptoalgorithms.
 - Identity-based authentication (up to 8 users) with advanced access conditions including administration mode (to manage other users authentication data) and FIPS-approved mode (to use FIPS-approved algorithms).
 - Secure communication channel (using Global Platform v2.2 SCP02 and SCP03) for downloading sensitive data in the VaultIC file system.
 - Secure key transport with wrapping and unwrapping mechanisms
 - Command set to perform cryptographic operations using keys and data from the file system including: Authentication, Digital signature generation/verification, Encryption/decryption, One-Time Password generation, Message Digest, Random, On-chip public key pair generation.
 - Cryptographic algorithms: RSA PKCS#1 v2.1 [R23], EC-DSA FIPS-186 [R24], ISO9797 MAC using 3DES [R25], Raw RSA X.509, ANSI X9.62 ECDSA [R26], NIST SP 800-38B AES CMAC [R27], FIPS 198 HMAC[R28]....
 - Cryptographic protocols: ISO9798 [R12] secret-key unilateral or mutual authentication, FIPS196 [R13] public key based unilateral or mutual authentication and Microsoft Card Minidriver [R29].
 - X.509 certificate verification.

- Robust communication protocols stacked over the physical communication interfaces.
- Certified FIPS 140-2 Security Level 3 (with draft NIST SP800-131 recommendations for 2011) and FIPS 140-2 Security Level 4 for physical protection.
- An evaluation kit (ATVAULTIC-STKxx) with samples, board, documentations and software components for a first handle of VaultIC.

Figure 5-1. VaultIC Starter Kit



What's in the Starter Kit?

- VaultIC Samples with one dedicated test socket
- One generic USB to SPI/I2C adaptor or USB Dongles
- One USB Cable
- One CD-ROM

What's in the CD-ROM?

- Support documentation set (Getting Started, Applications Notes...)
- Demonstrations to get an insight into the VaultIC features
- *VaultIC Manager* Tool to personalize the VaultIC file system
- Hardware independant cryptographic API (with source code)



Caution

The VaultIC Starter kit, samples or documentation require a Non Disclosure Agreement signed with Inside Secure and an Export License due to cryptographic modules. For more information, please contact your local INSIDE Secure sales office or e-security@insidefr.com.



Note

VaultIC Family is detailed on the INSIDE Secure's website [\[R22\]](#).



6. Conclusion

High-tech goods counterfeiting, multimedia content copying and identity theft have an increasing cost to industry and consumers. Besides the few examples presented herein, AT90SC and AT90SO series microcontrollers can successfully protect a broad range of applications against these threats among others. Typically, the extra cost of a security chip remains negligible compared to the derived benefits. With their embedded firmware, VaultIC microcontrollers allow an even easier implementation of secured embedded systems.





Definitions and Acronyms

1. **Brute force attack, dictionary attack:** hacking techniques that consist in trying commonly used passwords (dictionary attack) or every character combination (brute force) to guess a password.
2. **CPU:** Central Processing Unit
3. **Pharming:** advanced technique consisting of the creation of fake web sites (e.g. banking) that perfectly mimic the real ones. Users are seamlessly directed to these fake sites, and enter their login and password that are recorded by hackers! Seamless redirection can be achieved through false URLs (that surprisingly look like the right one) sent by e-mail, or by Internet Domain Name Servers hacking (DNS cache poisoning) that will erroneously translate good URLs to the hackers IP address.
4. **Phishing:** technique consisting in stealing user credentials (login/password) through fake e-mails
5. **Provisioning:** activity consisting in loading/generating user credentials, cryptographic keys, identifiers into equipment.
6. **Seed:** (pseudo-)random number
7. **Strong authentication:** exchange of messages during which a claimant proves its identity to a verifier by demonstrating its knowledge of a secret but without revealing it.



Reference List

- [R1] KPMG Report - Managing the Risks of Counterfeiting in the Information Technology Industry, 2005
http://www.agmaglobal.org/press_events/press_docs/Counterfeit_WhitePaper_Final.pdf
- [R2] Article "Flood of Fakes: Counterfeits inundate high-tech market", Dean Takahashi (Mercury News), Feb 2006
- [R3] DeCSS article
<http://www.wikipedia.org/wiki/DeCSS>
- [R4] News from November 2003
http://news.cnet.com/2100-1027_3-5111426.html
- [R5] United States Patents and Trademarks Office
<http://www.uspto.gov/main/profiles/stopfakes.htm>
- [R6] European Association for the Protection of Encrypted Works and Services
<http://www.aepoc.org>
- [R7] Foundation for Art and Creative Technology
<http://www.fact.co.uk>
- [R8] 2010 Identity Fraud Survey Report, Javelin Strategy and Research, 2010
https://www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveyConsumer.pdf
- [R9] Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce, 2005 Press Releases
http://www.gartner.com/press_releases/asset_129754_11.html
- [R10] US banks given authentication deadline, Oct 2005
<http://www.finextra.com/fullstory.asp?id=14389>
- [R11] Attack of the Clones: Building Clone-Resistant Products, RSA 2006
<http://www.cryptography.com/public/pdf/Clone-Resistance2006.pdf>
- [R12] ISO/IEC 9798-2, "Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms", International Organization for Standardization, Geneva, Switzerland, 2008 (third edition).
- [R13] Entity authentication using public key cryptography, 1997 February 18
<http://www.itl.nist.gov/fipspubs/fip196.htm>
- [R14] Electronic Authentication Guideline, NIST Special Publication 800-63
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
- [R15] The S/KEY One-Time Password System, February 1995
<http://tools.ietf.org/html/rfc1760>
- [R16] OATH - IETF HMAC OTP Draft 4 - Initiative for Open Authentication
http://www.openauthentication.org/pdfs/HMAC_OTP_DRAFT_4.pdf
- [R17] RSA-OTP PKCS #11 v2.20 Amendment 1: PKCS #11 mechanisms for One-Time Password Tokens
<ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20a1.pdf>
- [R18] PKCS #11 v2.20 : Cryptographic Token Interface Standard
<ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf>
- [R19] The Cryptography API, or How to Keep a Secret, Robert Coleridge (MSDN Technology Group), August 19, 1996
http://msdn.microsoft.com/library/default.asp?url=/library/enus/dncapi/html/msdn_cryptapi.asp
- [R20] AT77C105A- FingerChip sensor datasheet
<http://www.alldatasheet.com/datasheet-pdf/pdf/115275/ATMEL/AT77C105A.html>

- [R21]** Trusted Platforms for Homeland Security, Atmel, 2004
http://www.Atmel.com/dyn/resources/prod_documents/doc5062.pdf
- [R22]** INSIDE Secure VaultIC Family
<http://www.insidesecondure.com/eng/Products/Secure-Solutions/VaultIC>
- [R23]** PKCS #1: RSA Cryptography Standard
<ftp://ftp.rsasecondure.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf>
- [R24]** FIPS-PUB 186, Digital Signature Standard, 1994
<http://www.itl.nist.gov/fipspubs/fip186.htm>
- [R25]** ISO/IEC 9797, "Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm", International Organization for Standardization, Geneva, Switzerland, 1994 (second edition).
- [R26]** ANSI X9.62. Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)©. 1998.
- [R27]** NIST SP 800-38B - Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication - May 2005
- [R28]** FIPS PUB 198. The Keyed-Hash Message Authentication Code (HMAC). March 2002.
- [R29]** Microsoft® - Smart Card Minidriver Specification for Windows® Base Cryptographic Service Provider (Base CSP) and Smart Card Key Storage Provider (KSP) Version 5.07 - Sept 2007

Revision History

Document Details

Title: Secure Your Embedded Devices using AT90SC/SO and VaultIC Families

Literature Number: 6528B

Date: 04Feb11

- **Revision B :**
 - Adapt AT98SC features to VaultIC features
 - Adapt for Inside Secure Template
- **Revision A :**
 - First Release



Headquarters

INSIDE Secure

41, Parc Club du Golf
13586 Aix-en-Provence Cedex 3
France
Tel: +33 (0)4-42-39-63-00
Fax: +33 (0)4-42-39-63-19

Product Contact

Web Site

www.insidesecond.com

Technical Support

e-security@insidefr.com

Sales Contact

sales_web@insidefr.com

Disclaimer: All products are sold subject to INSIDE Secure Terms & Conditions of Sale and the provisions of any agreements made between INSIDE Secure and the Customer. In ordering a product covered by this document the Customer agrees to be bound by those Terms & Conditions and agreements and nothing contained in this document constitutes or forms part of a contract (with the exception of the contents of this Notice). A copy of INSIDE Secure Terms & Conditions of Sale is available on request. Export of any INSIDE Secure product outside of the EU may require an export Licence.

The information in this document is provided in connection with INSIDE Secure products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of INSIDE Secure products. **EXCEPT AS SET FORTH IN INSIDE SECURE'S TERMS AND CONDITIONS OF SALE, INSIDE SECURE OR ITS SUPPLIERS OR LICENSORS ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL INSIDE SECURE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, EXEMPLARY, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF REVENUE, BUSINESS INTERRUPTION, LOSS OF GOODWILL, OR LOSS OF INFORMATION OR DATA) NOTWITHSTANDING THE THEORY OF LIABILITY UNDER WHICH SAID DAMAGES ARE SOUGHT, INCLUDING BUT NOT LIMITED TO CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCTS LIABILITY, STRICT LIABILITY, STATUTORY LIABILITY OR OTHERWISE, EVEN IF INSIDE SECURE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.**

INSIDE Secure makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. INSIDE Secure does not make any commitment to update the information contained herein. INSIDE Secure advises its customers to obtain the latest version of device data sheets to verify, before placing orders, that the information being relied upon by the customer is current. INSIDE Secure products are not intended, authorized, or warranted for use as critical components in life support devices, systems or applications, unless a specific written agreement pertaining to such intended use is executed between the manufacturer and INSIDE Secure. Life support devices, systems or applications are devices, systems or applications that (a) are intended for surgical implant to the body or (b) support or sustain life, and which defect or failure to perform can be reasonably expected to result in an injury to the user.

A critical component is any component of a life support device, system or application which failure to perform can be reasonably expected to cause the failure of the life support device, system or application, or to affect its safety or effectiveness.

The security of any system in which the product is used will depend on the system's security as a whole. Where security or cryptography features are mentioned in this document this refers to features which are intended to increase the security of the product under normal use and in normal circumstances.

© INSIDE Secure 2011. All Rights Reserved. INSIDE Secure®, INSIDE Secure logo and combinations thereof, and others are registered trademarks or trade-names of INSIDE Secure or its subsidiaries. Other terms and product names may be trademarks of others.