Secure Your Embedded Devices

Secure Microcontrollers

Application Note

1. Introduction

High-tech goods counterfeiting, multimedia content copying, and identity theft are all major concerns today. The proven cryptographic protocols implemented in Atmel'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.

1.1. High-tech Goods Counterfeiting

According to the 2005 report [KMPG05] 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.

Examples of the counterfeiting of high-tech goods are given in [MERC]. 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

Rev. 6528A–17 May 06

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 (*refer to [WPD-DE]*). 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 (*refer to [CNN]*).

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

1.3. Identity Theft

Another burning issue is the identity theft of web applications. According to [JAV06], 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 [GAR05], phishing (1) 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 [FINE], 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 will enforce new strong authentication means in its new 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 (2) and more.

1. Phishing: technique consisting in stealing user credentials (login/password) through fake e-mails
2. 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.

1.4. Atmel's Secure Microcontroller Family

This paper will show how to prevent the threats mentioned with the use of Atmel'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 Atmel 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 [1] of such microcontrollers have been already sold by Atmel and successfully implemented in many secure systems.

Atmel'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.

Versatility

Three secure microcontroller families are available: AT90SC, AT91SC and AT98SC. The AT90SC and AT91SC are "open" solutions where the implementer can develop their own on-chip application using available Atmel software libraries. Beyond this, the AT98SC 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 AT98SC will be further described later in this paper.

Tampering Resistance

AT9xSC 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. Atmel'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 Atmel secure microcontroller.

Success Stories

Atmel 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.

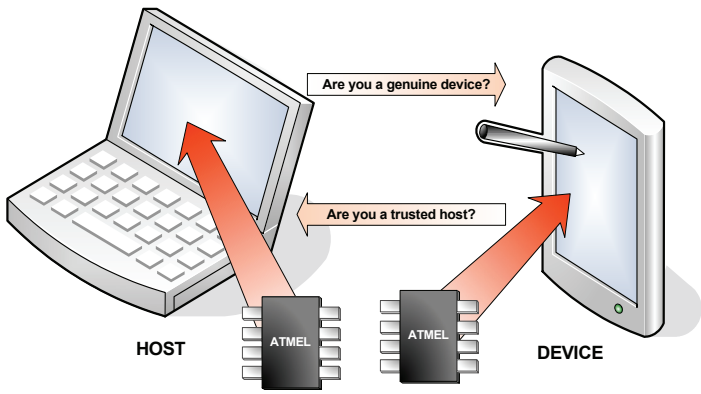
1. The billionth was sold in March 2006

2. Secure Your Hardware – Anti-cloning Solutions

Atmel secure microcontrollers are perfectly designed to secure embedded systems. For example, the AT98SC 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 [CRI06] 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

Anticloning is safely implemented through one-way or mutual strong authentication [1]. Various authentication protocols exist (*refer to [ISO9798], [FIPS196]*), 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.

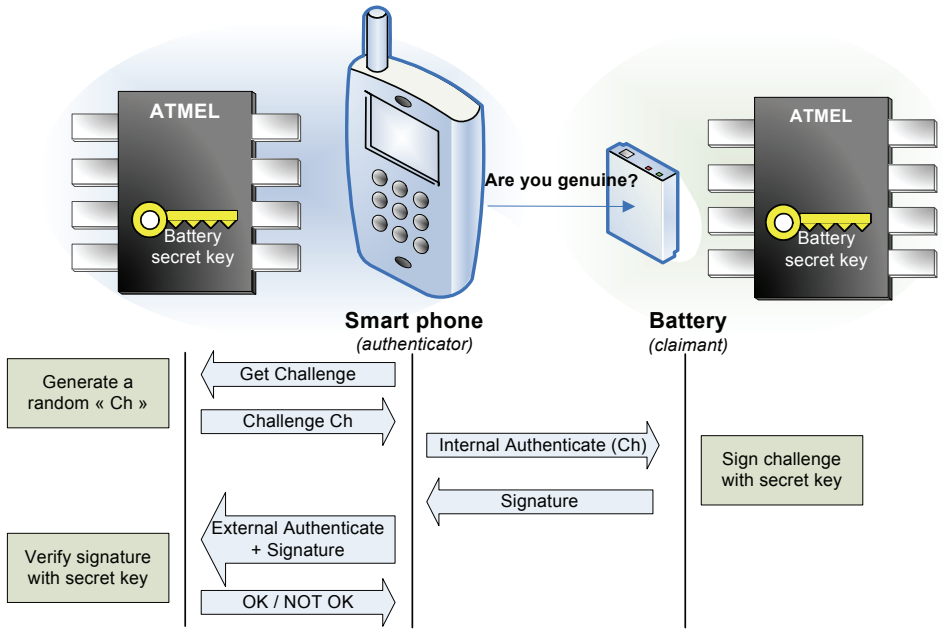
Let us illustrate this process with the example of a cell phone (the authenticator) authenticating a battery (the claimant). This example (*refer to Figure 2-2*) is based on the ISO/IEC 9798 standard [ISO9798]. This application can be implemented using two AT98SC chips – one in the phone and one in the battery. The battery-side AT98SC chip contains a secret key (loaded during battery manufacturing) that can never be extracted and is utilized to compute signatures. Consequently, the AT98SC must be cloned in order to make counterfeit batteries which is practically impossible.

1. 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.

The phone's AT98SC 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 AT98SC – 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 AT98SC. The AT98SC sends back the requested challenge.
   - The phone sends an "Internal Authenticate" command to the battery's AT98SC with the generated challenge. The battery's AT98SC 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 AT98SC for verification:
   - The phone sends an "External Authenticate" command, with the battery's signature, to its AT98SC.
   - The phone's AT98SC 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.

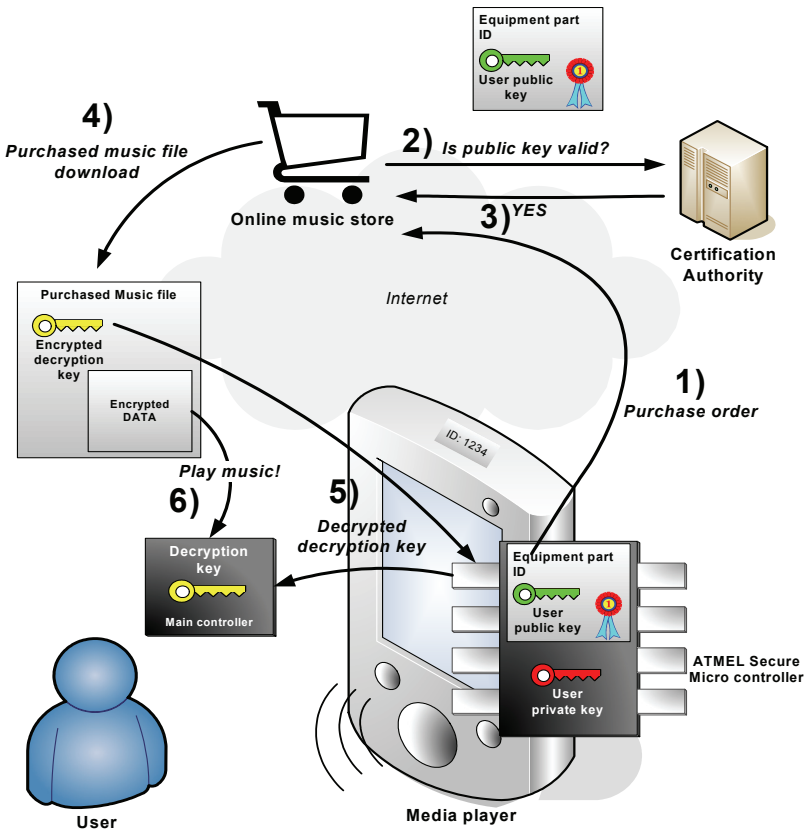
3. Secure Your Digital Content – DRM and Software Copy Protection

Atmel 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 AT98SC microcontroller. The ultimate goal of DRM is to prevent access to a digital clear-text music file that could be copied infinitely without any degradation in sound quality.

Figure 3-1. Secure media player



1. Provisioning [1]: 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 AT98SC. The generated “user private key” remains internally stored in a file on the AT98SC 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 AT98SC. This makes it impossible to have valid public keys generated by something else other than an AT98SC personalized for this purpose. Moreover, this certificate binds the generated public key to the equipment identifier.

1. Provisioning: activity consisting in loading/generating user credentials, cryptographic keys, identifiers into equipment.

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 AT98SC 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*).

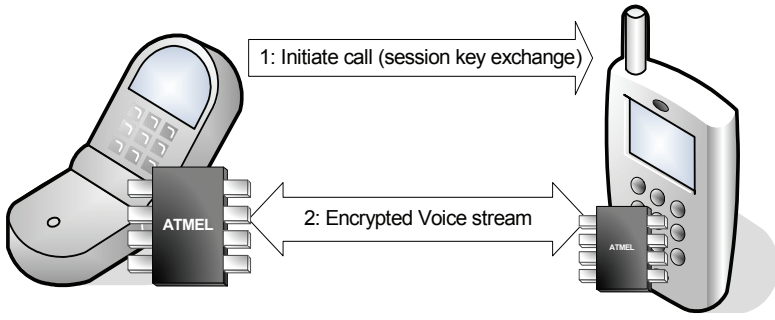
As a general design rule, the transmission of the decrypted keys between the secure microcontroller and the main controller must be secured either logically, by encrypting the communications, or physically (offering tamper protection), or both. However, storing cryptographic keys into a controller that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

3.2. On-the-fly Encryption

Atmel 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 AT98SC:
   – Each phone sends a "Manage Security Environment" command containing the session key to its AT98SC.

2. Then voice stream can be ciphered/deciphered for as long as the communication lasts (*step 2*):
   - For an outgoing voice stream, the AT98SC will instantly encrypt the digitized voice stream with the “Encrypt data” command.
   - For an incoming voice stream, the AT98SC 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 useless. 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 [SP800-63] for further details.

Multi-factor authentication requires a strong authentication. Anticloning is safely implemented through one-way or mutual strong authentication. Various authentication protocols exist (refer to [ISO9798], [FIPS196]), 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. Atmel's turnkey USB secure microcontroller solutions can help providers focus on their security model and their application without loosing too much time on tamper protection and other complex hardware security concerns.

4.1. USB tokens common features

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

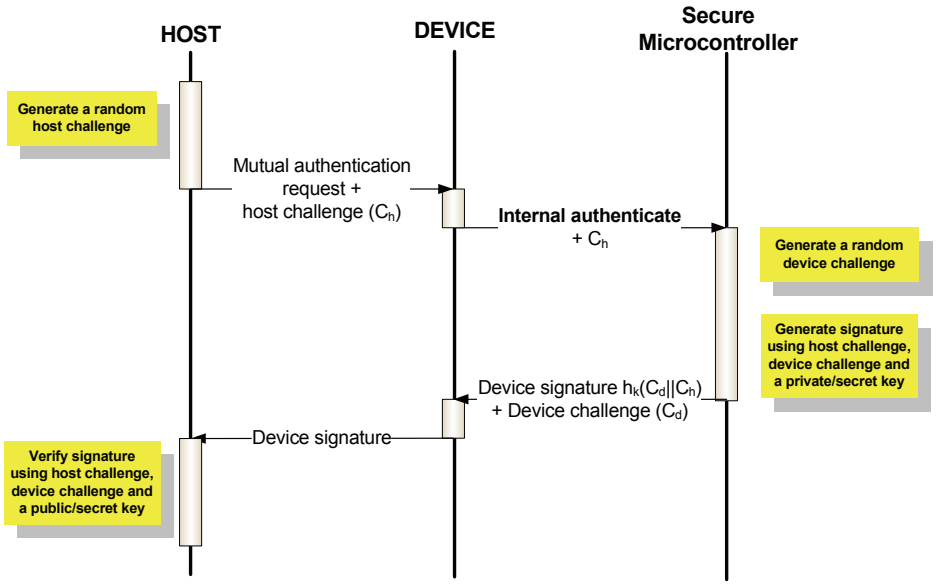
- Perform **challenge response authentication**

  This challenge response protocol is considered a strong authentication method. As shown in Figure 4-1, h_k is a digital signature operation (such as DES, RSA, elliptic curve (ECC) signature, etc.). The "||" operator is the "concatenation" operator. Figure 4-1shows 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.

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.

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.

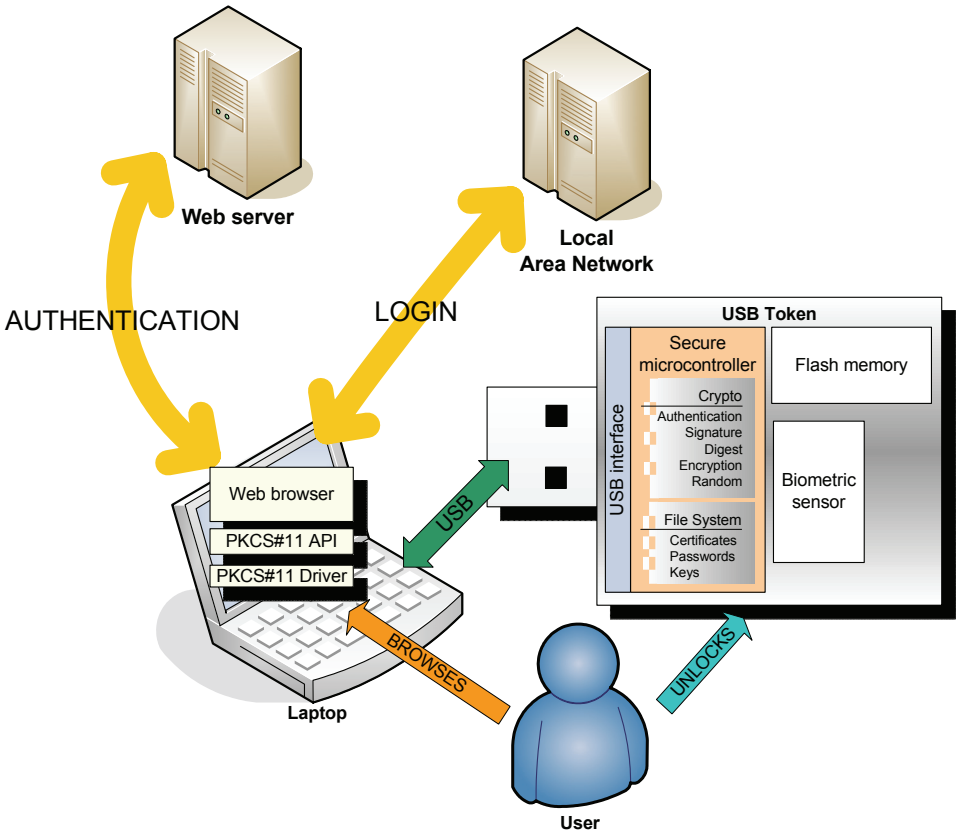
  The principle method of one-time passwords is as follows (*please refer to [RFC 1760] for further details*). Let us assume we have a client and a server. In a preliminary provisioning step, a list of passwords is generated on the client side using a client's secret passphrase and a seed [1] from the 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 (*refer to [OATH], [RSA-OTP]*).

- 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)

1. seed: (pseudo-)random number

Figure 4-2. Hardware token common features



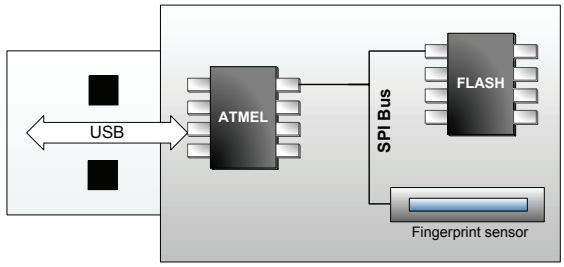
Besides the multi-factor authentication, the following secondary features are often used in such tokens:

- **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. Atmel secure microcontrollers perfectly fit as [PKCS11] or [MS-CAPI] compliant hardware tokens.

4.2. Implement a high-end USB token

The following example shows how to use an Atmel 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 Atmel USB secure microcontroller with Atmel fingerprint sensors (*refer to [ATM-FIN]*) 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



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.

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 AT98SC Family

The AT98SC is a new microcontroller family based on the technology implemented on the AT90SC and AT91SC series. Its embedded firmware provides a turnkey solution for the applications explained above and many more! The AT98SC family provides a generic solution to the security threats stated in this paper.

The AT98SC family is an alternative to Trusted Platform Modules (TPM) for the embedded market (*refer to [ATM-TPM]*). AT98SC 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.

5.1. Flexibility. Rapid Development/Integration for Embedded Products

Currently, the AT98SC family members feature (*refer to [ATM-AT98] for further details*):

- **Various communication interfaces** including SPI (Serial Protocol 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. AT98SC chips are available in small packages (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. AT98SC devices consume less than 100 µA in standby mode, and only 5 to 15 mA during CPU [1]-intensive operations depending on the required action.
- **Embedded firmware** that provides advanced functions:
  - Secure 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.
  - Administration mode to manage chip internals, security features, cryptographic configuration and file system contents. It allows downloading data into the AT98SC file system using an encrypted channel with session keys.
  - Command set to perform cryptographic operations using keys and data from the file system including: authentication, digital signature, encryption/decryption, hash, random, public key pair generation.
  - Cryptographic algorithms: RSA PKCS#1 v2.1 [PKCS1], EC-DSA [FIPS186], [ISO9797] MAC using 3DES.
  - Cryptographic protocols: [ISO9798] secret-key unilateral or mutual authentication and [FIPS196] public key based unilateral or mutual authentication.
  - Robust communication protocol stacked over the physical communication interfaces.
- **An evaluation kit** (AT98SC-EV1)

Please refer to the AT98SC family roadmap [2] for a detailed schedule of new features such as:

- X.509 certificate verification/generation
- HOTP algorithm (*refer to [OATH]*)
- TWI (Two-Wire interface), UART(Universal Asynchronous Receiver Transmitter)
- SOIC-8 package or similar

1. CPU: Central Processing Unit
2. Contact your local Atmel sales office.

5.2. Customize Your Security?

Currently, it is not possible to load user code on the AT98SC devices. For that reason, the Python® programming language support is planned. A virtual machine-based Python execution environment will allow a full customization of the AT98SC operation. Customers will be able to easily develop their own set of applications embedded in the AT98SC chips using a high-level language without bothering with low-level hardware considerations.

The Python language is already successfully used within the industry (Philips®, NASA, Lucasfilms Ltd, AstraZeneca® International, Nokia®, etc.) and offers a low-cost solution because it is license-free. The Python language is also used in portable devices, the most famous example being the Nokia Series 60 Smartphone embedding a full Python interpreter (*see [NOKIA]*). Moreover, free yet efficient development tools are already available (based on IBM®'s Eclipse™ IDE). Python is appreciated for its fast learning curve, fast application development, maintainability, and readability of source code (*See [PYTH-ST]*).

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, AT9xSC 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, AT98SC microcontrollers allow an even easier implementation of secured embedded systems.

7. References

[**AEPOC**] European Association for the Protection of Encrypted Works and Services, Web: http://www.aepoc.org

[**ATM-AT98**] AT98SC008CT Description, Atmel, Web: http://www.Atmel.com/dyn/products/product_card.asp?part_id=3882

[**ATM-FIN**] AT77C105A- FingerChip sensor description, Atmel, Web: http://www.Atmel.com/dyn/products/product_card.asp?part_id=3609

[**ATM-TPM**] Trusted Platforms for Homeland Security, Web: http://www.Atmel.com/dyn/resources/prod_documents/doc5062.pdf

[**CNN**] Web: http://www.cnn.com/2003/TECH/internet/11/27/itunes.code.ap

[**CRI06**]Attack of the Clones: Building Clone-Resistant Products, RSA 2006, Web: http://www.cryptography.com/resources/whitepapers/Clone-Resistance2006.pdf

[**FACT**] Foundation for Art and Creative Technology, Web: http://www.fact.co.uk

[**FINE**] US banks given authentication deadline, Oct 2005, Web: http://www.finextra.com/fullstory.asp?id=14389

[**FIPS186**] FIPS-PUB 186, Digital Signature Standard, 1994, Web: http://www.itl.nist.gov/fipspubs/fip186.htm

[**FIPS196**] Entity authentication using public key cryptography, 1997 February 18, Web: http://www.itl.nist.gov/fipspubs/fip196.htm

[**GAR05**] Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce, 2005 Press Releases, Web: http://www.gartner.com/press_releases/asset_129754_11.html

[**ISO9797**] 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).

[**ISO9798**] ISO/IEC 9798-2, “Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms”, International Organization for Standardization, Geneva, Switzerland,1994 (first edition).

[**JAV06**] 2006 Identity Fraud Survey Report, Javelin Strategy and Research, January 2006.

[**KPMG05**] KPMG Report - Managing the Risks of Counterfeiting in the Information Technology Industry, 2005

[**MERC**] Counterfeits inundating high-tech market, D. Takahashi (Mercury News), Web: http://www.siliconvalley.com/mld/siliconvalley/13774284.htm

[**MS-CAPI**] The Cryptography API, or How to Keep a Secret, Robert Coleridge (MSDN Technology Group), August 19, 1996, Web: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncapi/html/msdn_cryptapi.asp

[**NOKIA**] Python TM for series 60, Web: http://www.forum.nokia.com/python

[**OATH**] IETF HMAC OTP Draft 4 - Initiative for Open AuTHentication, Web: http://www.openauthentication.org/pdfs/HMAC_OTP_DRAFT_4.pdf

[**PKCS1**] PKCS #1: RSA Cryptography Standard, Web: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf

[**PKCS11**] PKCS #11 v2.20 : Cryptographic Token Interface Standard, Web: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf

[**PYTH-ST**] Python Success Stories, Web: http://www.python.org/about/success

[**RFC 1760**] The S/KEY One-Time Password System February 1995,
Web: http://rfc.net/rfc1760.html

[**RSA-OTP**] PKCS #11 v2.20 Amendment 1: PKCS #11 mechanisms for One-Time Password Tokens, Web: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20a1.pdf

[**SP800-63**] Electronic Authentication Guideline, NIST Special Publication 800-63,
Web: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

[**USPTO**] United States Patents and Trademarks Office,
Web: http://www.uspto.gov/main/profiles/stopfakes.htm

[**WPD-DE**] DeCSS article, Web: http://www.wikipedia.org/wiki/DeCSS

Atmel Corporation

2325 Orchard Parkway
San Jose, CA 95131, USA
Tel: 1(408) 441-0311
Fax: 1(408) 487-2600

Regional Headquarters

Europe
Atmel Sarl
Route des Arsenaux 41
Case Postale 80
CH-1705 Fribourg
Switzerland
Tel: (41) 26-426-5555
Fax: (41) 26-426-5500

Asia
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimshatsui
East Kowloon
Hong Kong
Tel: (852) 2721-9778
Fax: (852) 2722-1369

Japan
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
Tel: (81) 3-3523-3551
Fax: (81) 3-3523-7581

Atmel Operations

Memory
2325 Orchard Parkway
San Jose, CA 95131, USA
Tel: 1(408) 441-0311
Fax: 1(408) 436-4314

Microcontrollers
2325 Orchard Parkway
San Jose, CA 95131, USA
Tel: 1(408) 441-0311
Fax: 1(408) 436-4314

La Chantrerie
BP 70602
44306 Nantes Cedex 3, France
Tel: (33) 2-40-18-18-18
Fax: (33) 2-40-18-19-60

ASIC/ASSP/Smart Cards
Zone Industrielle
13106 Rousset Cedex, France
Tel: (33) 4-42-53-60-00
Fax: (33) 4-42-53-60-01

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906, USA
Tel: 1(719) 576-3300
Fax: 1(719) 540-1759

Scottish Enterprise Technology Park
Maxwell Building
East Kilbride G75 0QR, Scotland
Tel: (44) 1355-803-000
Fax: (44) 1355-242-743

RF/Automotive
Theresienstrasse 2
Postfach 3535
74025 Heilbronn, Germany
Tel: (49) 71-31-67-0
Fax: (49) 71-31-67-2340

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906, USA
Tel: 1(719) 576-3300
Fax: 1(719) 540-1759

Biometrics/Imaging/Hi-Rel MPU/
High Speed Converters/RF Datacom
Avenue de Rochepleine
BP 123
38521 Saint-Egreve Cedex, France
Tel: (33) 4-76-58-30-00
Fax: (33) 4-76-58-34-80

Literature Requests
www.atmel.com/literature