# CryptoAuthentication™ Product Uses

## Abstract

Companies are continuously searching for ways to protect property using various implementations of security; however the cost of implementation can drive companies away from effective hardware solutions to less secure software solutions. With the introduction of the AT88SA10HS/102S devices, affordable hardware security is now in reach and can provide exceptional protection for:

- Confidential file protection
- Embedded software anti-cloning
- Development system anti-cloning
- Media transmission encryption
- USB security dongles
- Securing wireless or other radio transmission nodes
- Authentication for data over power lines
- Physical access control
- Electronic lockers
- Hardware user authentication
- Consumable product authentication
- Battery authentication.

## 1. Overview

This document provides an introduction to the Atmel AT88SA10HS/102S CryptoAuthentication devices. These exceptional devices enable solutions to countless problems across many industries. The use cases outlined in this document will provide a brief description of possible applications for the AT88SA10HS/102S devices and how they can be implemented.

## 2. AT88SA10HS/102S Introduction

To understand the operations and applications explained later in this document you will first need to have a basic understanding of the AT88SA10HS/102S devices and how they work. The AT88SA10HS and AT88SA102S were developed to work together. The AT88SA102S is designed to be embedded in the product that is protected or authenticated (client) and the AT88SA10HS device is designed to be placed in the validating system (host). The AT88SA102S client device can be used with or without the host side device. When the AT88SA102S is used without the host side AT88SA10HS chip the host microcontroller must store secret information in order to perform the validation of the client. Having the secret information stored in the embedded source code presents a security risk as the secrets may be ascertained with little effort. For the strongest security the AT88SA10HS host device should be used; this keeps the customer's secret keys protected securely in hardware away from hackers attempting to reverse engineer the host embedded code.

**CryptoAuthentication Product Uses**

**AT88SA10HS AT88SA102S**

**Application Note**

8663B–SMEM–3/09

The AT88SA10HS/102S devices uses a cutting edge SHA-256 engine embedded in hardware as the heart of their security architectures. In the most basic operation the device is sent a challenge to which it will respond with a unique response that only it can produce. Since challenge and response pairs are nearly infinite for each device, each device can be used indefinitely without fear of repeating the same challenge-response pair. The response generated by the device is created by hashing the input challenge with a secret key stored in protected memory thus a particular device will always respond exactly the same to a given challenge. A product using the AT88SA10HS/102S can be configured so that the entire product line uses the same key or so that each device has a unique key. The response that a particular device will produce can only be reproduced by something that knows the key that is stored in the device.

## 3. Secure Key Exchange

In addition, the AT88SA102S device can be used for secure key exchange. If the device is used in conjunction with a symmetric encryption algorithm such as AES or DES an end-to-end encrypted transmission can be created. In the case of symmetric encryption the weakest link is securely transferring the keys to encrypt and decrypt the data at each end. The AT88SA102S can facilitate this by using the unique response produced by the device as a key to the symmetric encryption algorithm. This is done be sending a random challenge to a system that contains the key stored in the AT88SA102S and then encrypting the message with the system response. The message and the random challenge are then sent to the client device where the challenge is feed into AT88SA102S and the response from the CryptoAuthentication chip is used as a key to decrypt the message.

## 4. Key Diversification

Key diversification is highly recommended when using the CryptoAuthentication device. The device is designed with an embedded 265bit key that is never exposed. This 256 bit key is always used during the MAC hashing operation of the SHA-256 engine, however, additional bits can be incorporated into the result as well. CryptoAuthentication also provides a 62 bit customer secret that can be burned into fuses in the device once, and after which can never be read. In addition to the 62 bit secret an additional 23 bits of incremental blow fuses can be used as needed by the customer.

All of these methods as well as the incorporation of the devices unique serial number can be used in the key diversification schema. When these values are added into the MAC the response then becomes an output of all of the values. This makes a strong diversification configuration for the CryptoAuthentication device. When using diversified keys a source of compromise can be isolated easier and a remedy implemented much more rapidly. The incremental burn fuses provided by the AT88SA102S can also be used to provide a consumable usage tracking or to limit device usage cycles.

## 5. Programming Services

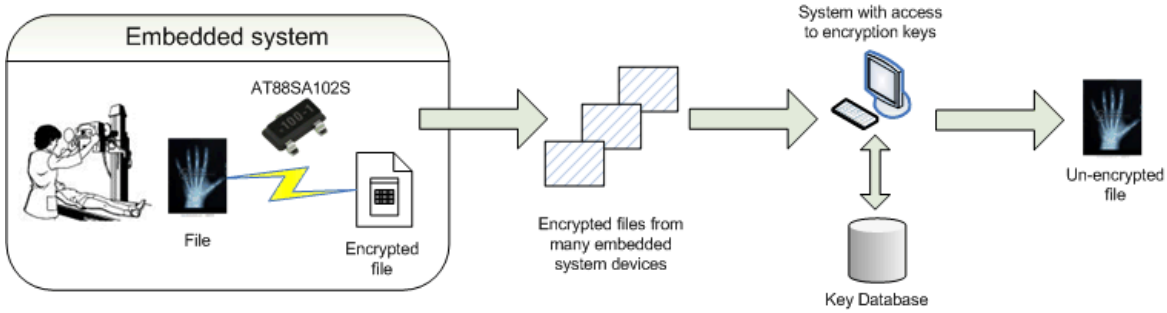
To enable a greater scale of control of secrets when diversified keys are utilized, Atmel offers a secure programming service. This programming service provides several key components which implement an end to end management and secret insertion for production devices programmed during manufacturing at Atmel facilities. The service provides for secure transport of customer secrets directly to the manufacturing facility and delivering their secrets to their devices. This service enables customers to minimize the risk of secret compromise by limiting exposure of the secrets to key personnel, maintaining confidentiality, providing accountability for units programmed, and by verifying that the devices are locked down properly.

**Note:** For additional security information read the “CryptoAuthentication High Level Security Design” which gives a detailed explanation of the security offered by the CryptoAuthentication family of devices.

## 6. Confidential File Protection

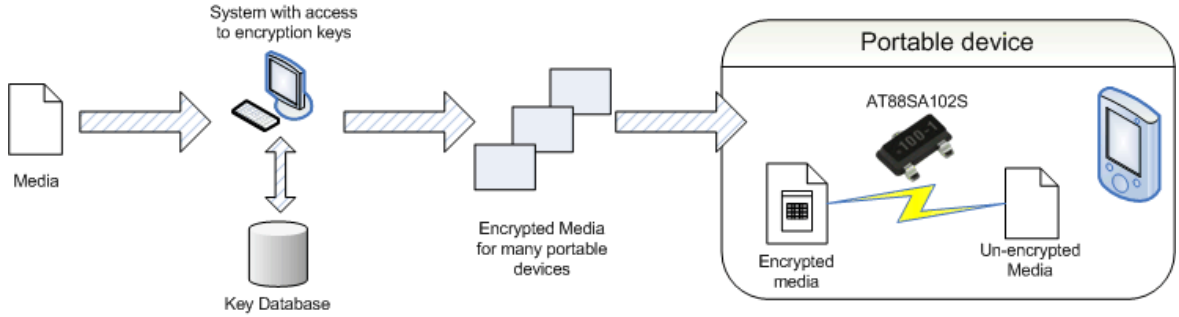
The AT88SA102S provides an affordable solution that secures documents while in transit. Securing confidential files is accomplished by using a symmetric encryption algorithm for communication as explained in the introduction. The individual embedded system devices create a random number and feed it into the AT88SA102S as a challenge. They then used the response from the AT88SA102S to encrypt the confidential file. The file and the random challenge can then be transmitted over any public medium. To complete the communication the system consuming the file needs to have knowledge of the keys stored in the AT88SA102S device that was used to encrypt the file. The consuming system takes the random challenge it received with the file and feeds it through a SHA-256 algorithm along with the device secret key. The system then uses the response from the SHA-256 algorithm as the key to decrypt the file. Embedded systems creating confidential files can all have the same keys or can be configured to have unique keys. Figure 1 shows a configuration where files are produced by embedded systems, the files in transit could be multiple files from the same embedded system or files from many embedded systems.

*Figure 1. Protecting Files*




The AT88SA102S also enables media destined for portable devices to be protected and unusable to any other application that may intercept the file while in transit. This is also done using a symmetric encryption algorithm as shown in Figure 1. However the system with knowledge of the keys produces the encrypted file and random input and transmits them to the portable device. The portable device then takes the random challenge it received with the media and feeds it into AT88SA102S and uses the response as the key to decrypt the media. Figure 2 shows this configuration. The files in transit could be multiple files destined for the same portable device or files to many portable devices.

*Figure 2. Encrypting Media*

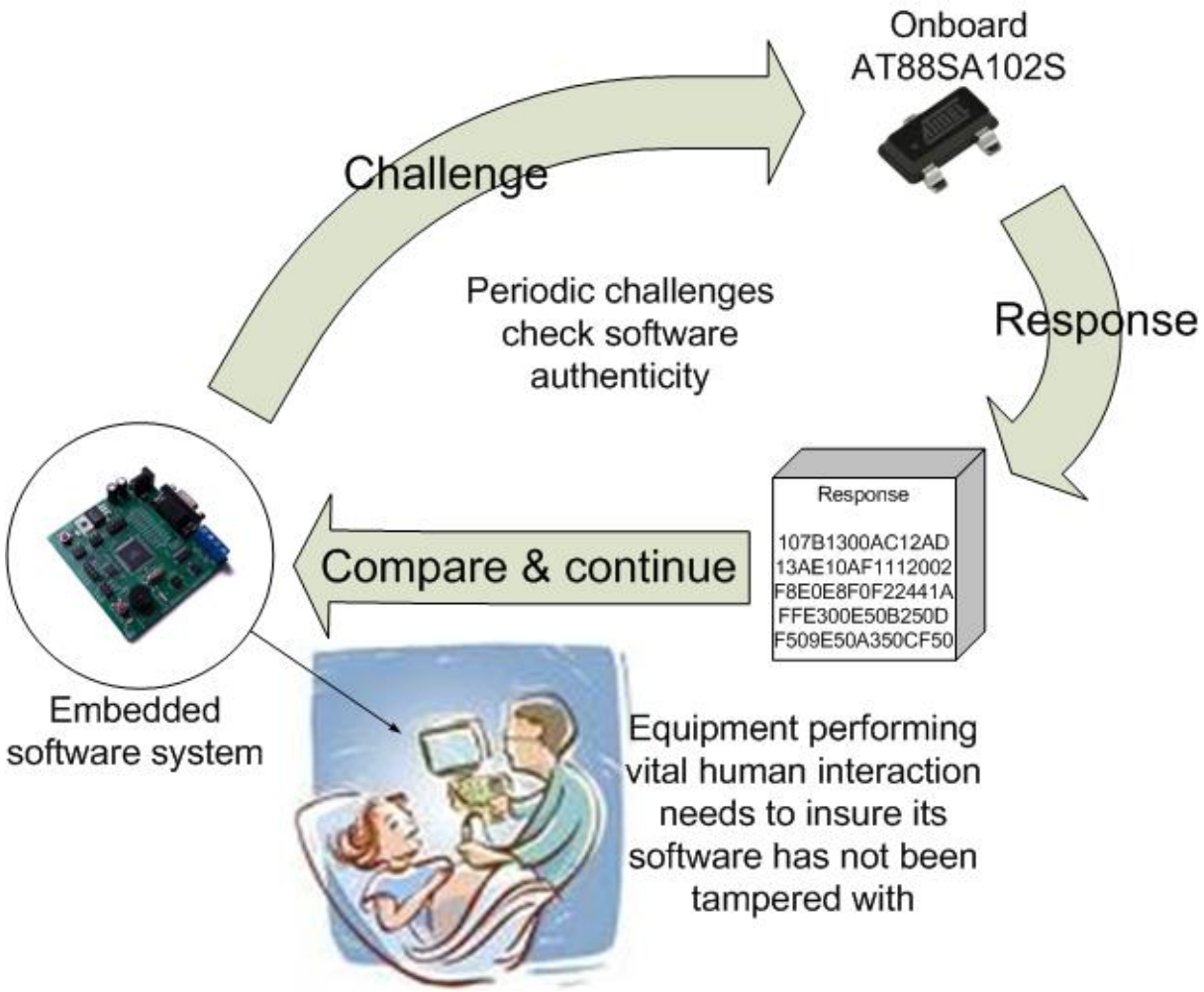


## 7. Embedded Software Anti-cloning

Software used to power embedded systems (host) is often copied, edited or changed by counterfeiters. Companies looking for an inexpensive way to protect their host embedded software from competitors and counterfeiters can now use the AT88SA102S as an onboard CryptoAuthentication device.

To configure embedded software for anti-cloning protection the AT88SA102S is integrated into the host. At random intervals a challenge is sent to the CryptoAuthentication device. The response from the CryptoAuthentication is then compared to the expected response. By providing a large number of challenges and placing those in unique areas, the source code can be relatively well protected. This makes it extremely difficult for anyone to reverse engineer the source code. This added difficulty will make it more cost effective for competitors and cloners to develop an entirely new system rather than modify your existing source code. The basic operation of this security model is displayed in Figure 3.

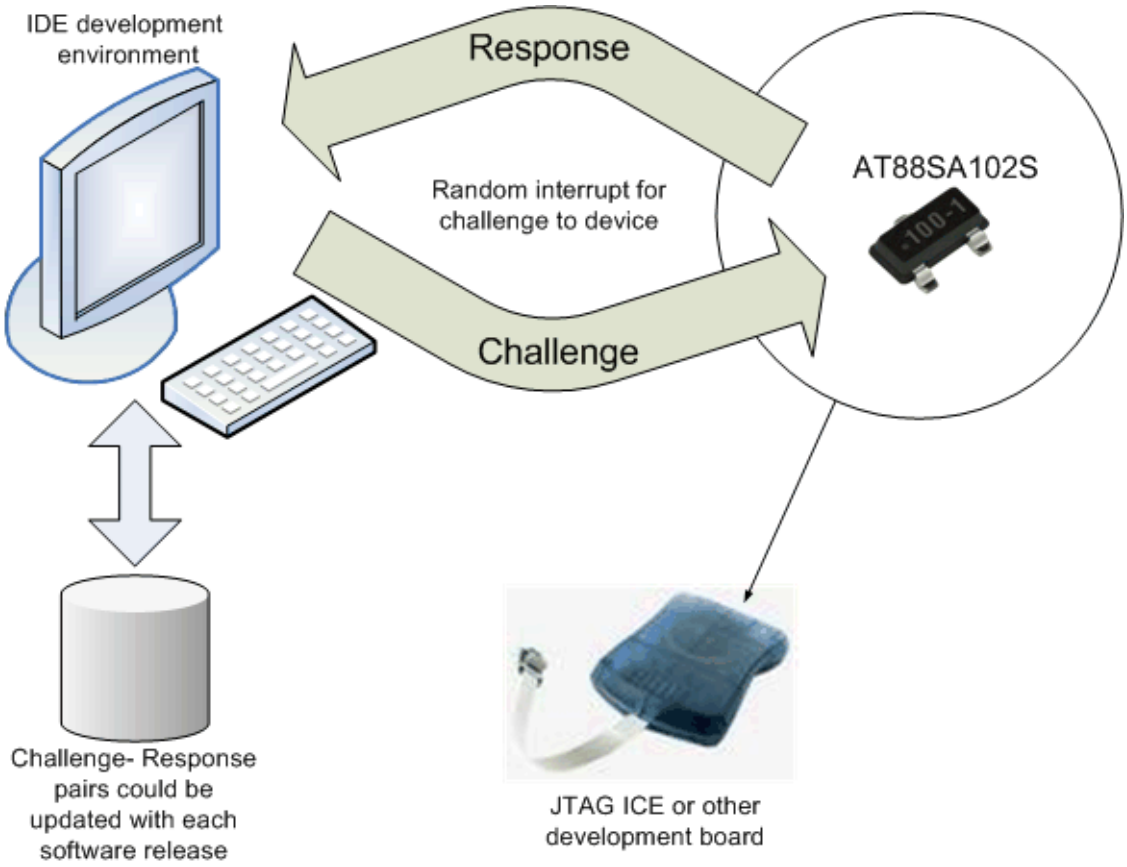
*Figure 3. Embedded Source Protection*



## 8. Development System Anti-cloning

The AT88SC102S provides an exceptional method of preventing third parties from creating clones of evaluation and development boards. To implement anti-cloning each evaluation or development board should be embedded with its own AT88SC102S CryptoAuthentication device. The Integrated Development Environment (IDE) would then be programmed to challenge the board prior to allowing the developer access to it. Counterfeiters will not be able to replicate every possible occurrence of challenge and response that can be handled by a board containing a legitimate CryptoAuthentication device, thereby thwarting common cloning attempts. In this model it would be beneficial to use hard coded challenge and response pairs instead of integrating the algorithm and keys into the application code where they would be vulnerable to attack. Providing a periodic method of renewing challenge-responses would increase security by removing any existing compromise as each incremental application upgrade could replace the list of challenge-response pairs. Figure 4 shows a graphical representation of the operation of this security model.

*Figure 4. Evaluation Board Authentication*

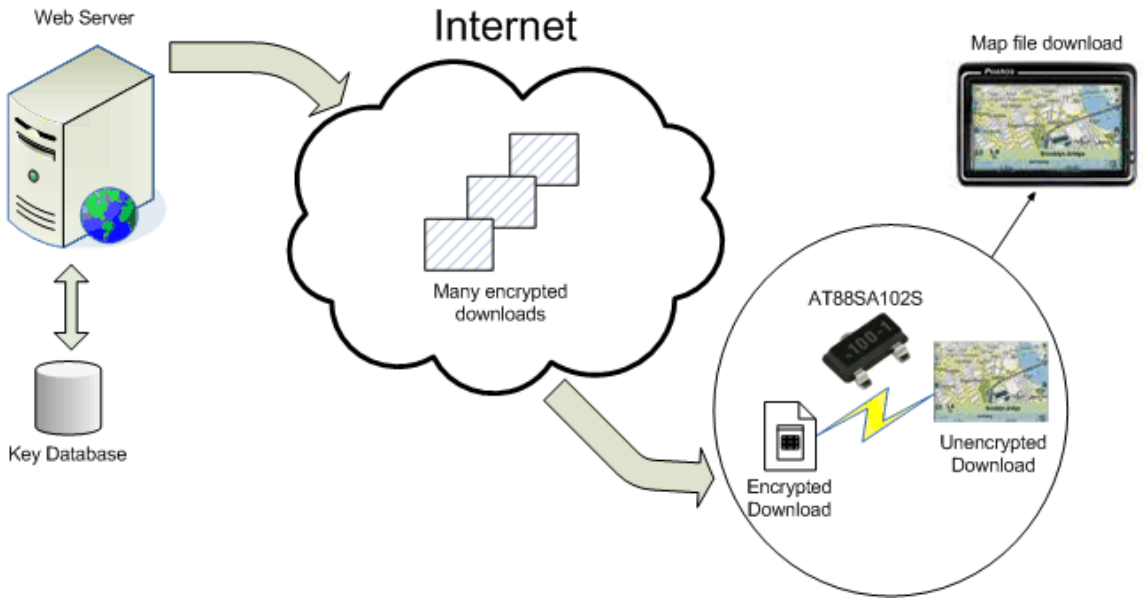



Companies need to identify authentic boards prior to rendering technical support. An interface could be implemented that would enable the user to enter any string of text that would in turn be feed to the CryptoAuthentication device on the development board and the response displayed to user. The help desk operator could verify the system by providing the user a custom string and asking them for the generated response. The call center operator would then be able to verify the authenticity of the development board prior to rendering service to the customer.

## 9. Media Transmission Encryption

Downloading files from internet sites has become common practice and in many cases the only way to get select software applications, upgraded features, extensions, or plug-ins. The AT88SA102S offers a solution to protect against theft of download content. The AT88SA102S CryptoAuthentication is attached to the downloading system, either embedded in hardware or as a temporary attachable device. The keys protected within the device can be used to ensure that only the purchaser or authorized consuming system will have the ability to decrypt and use the download. The download is encrypted and a challenge is sent along with the download. If the installer does not get the correct response from the CryptoAuthentication the download will be useless. Figure 5 is a graphical representation of protecting downloads using the AT88SA102S device.

*Figure 5. Encrypted Downloads*

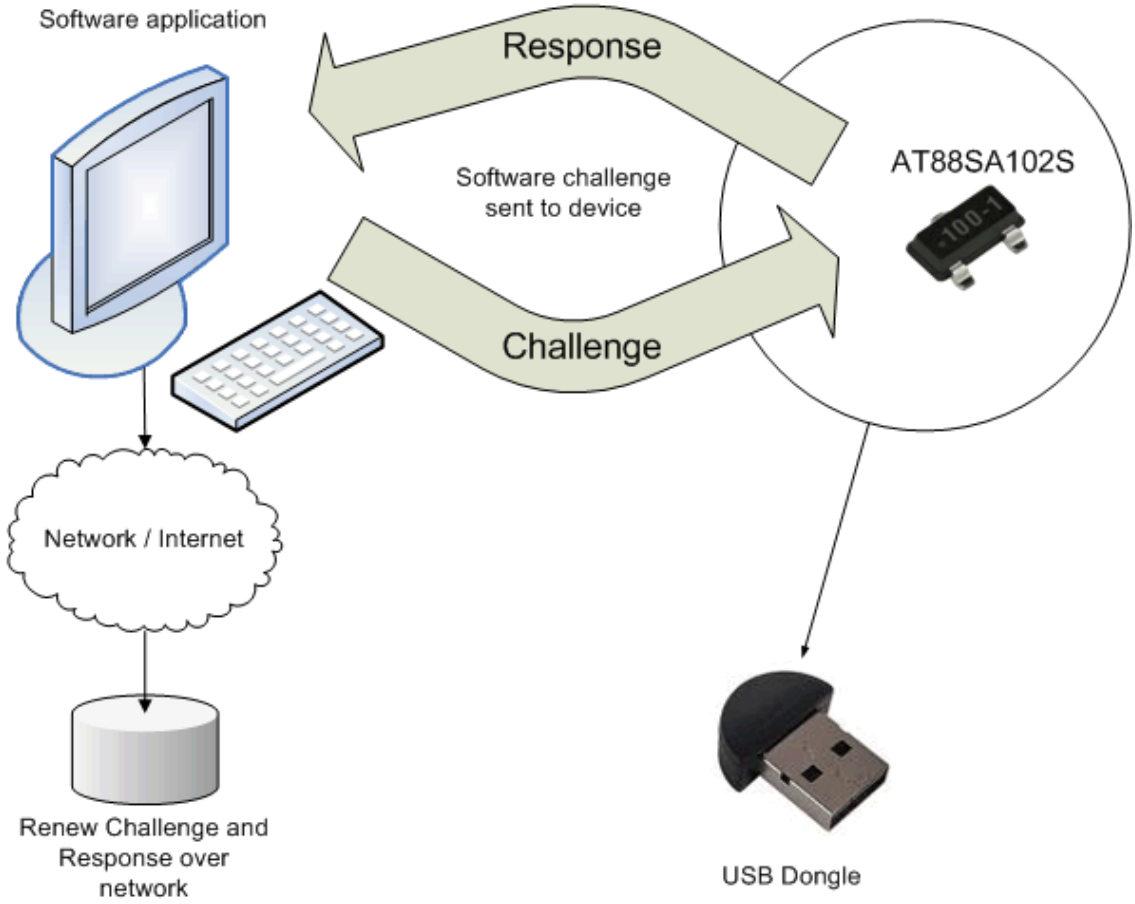



Often the downloader needs to verify that the download has not been tampered with during transit. This can also be done using the CryptoAuthentication device. The sending system needs to use the CryptoAuthentication to make a hash of the download and send the hash along with the download. The download user can then recreate the hash in the same manor that it was by the sending system. If the two hashes match the downloader has verified that the download has not been changed since it left the sending system.

## 10. USB Security Dongles

The AT88SA102S can enable security for a web application using an individualized USB dongle. This would provide web shopping, banking, and private member sites the ability to restrict user logon and usage to one individual and ensure that the user's device is physically present before allowing them access to resources. This is extremely secure because unique challenges could be generated by the remote web application for each use. Since each challenge is unique and no challenges are stored on the user's machine, replay attacks would be impossible. Figure 6 shows how the AT88SA102S would be used in a USB dongle to secure web or software applications.

*Figure 6. Prevent Unlicensed Software*

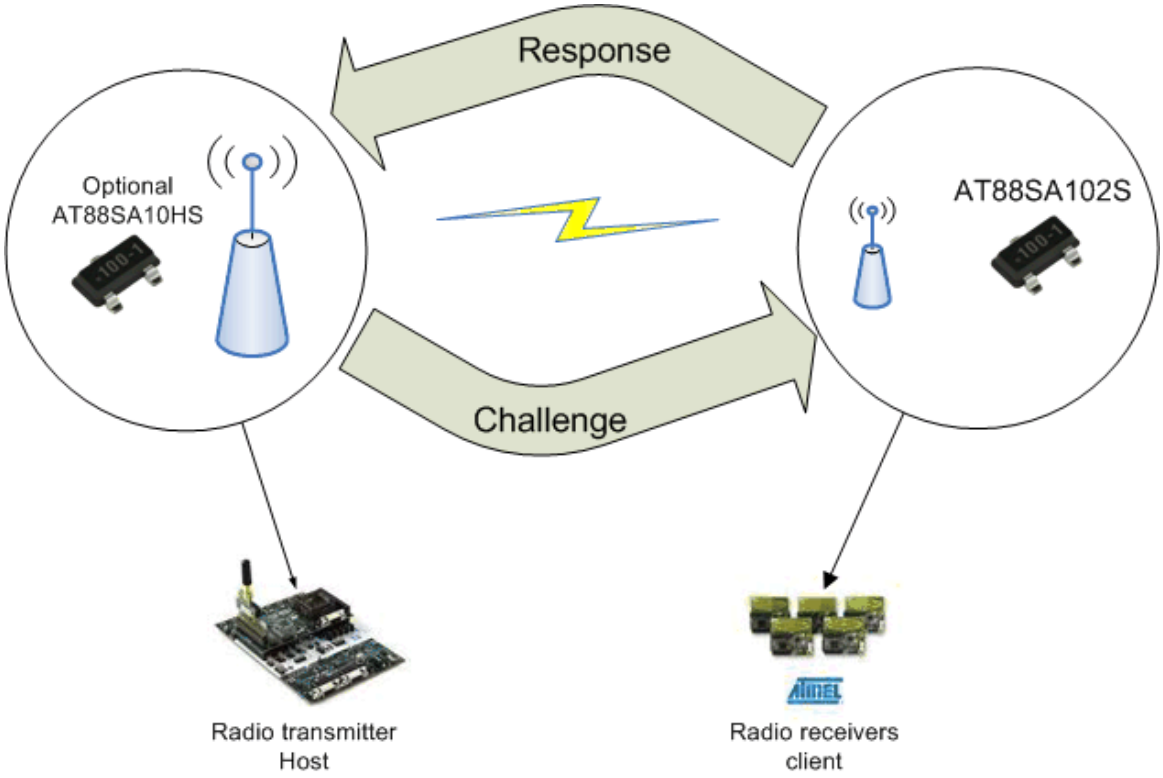



Protecting PC software applications from pirating is an ongoing struggle for any company producing software products. The AT88SA102S also enables an affordable and secure dongle solution for software. A single AT88SA102S CryptoAuthentication on a USB dongle can be used by an application to verify that the user is present and that only one user can use the software. This can be implemented by coding the challenge and responses into the software application and periodically sending a challenge to the attached device during the applications operation. The correct response from the CryptoAuthentication verifies that the user's hardware device is present. Since the AT88SA102S holds the key securely in hardware, the effort level required to circumvent the hardware security will outweigh the benefit received.

## 11. Securing Wireless or Other Radio Transmission Nodes

Radio transmission devices have to verify each node prior to allowing access to the network. The AT88SA102S is a great option for offering a low cost verification method. By installing AT88SA102S CryptoAuthentication devices in the radio nodes (client), the transmitting node (host) can verify that it is communicating with valid network nodes before transmitting important commands or information. Additional security can be achieved by adding an AT88SA10HS device in the host, so that the customer secrets would not have to be kept in the microprocessor code where developers and subcontractors may have access to them. Figure 7 shows a configuration that utilizes the AT88SA10HS/102S in a radio node network.

*Figure 7. Wireless Node Authentication*



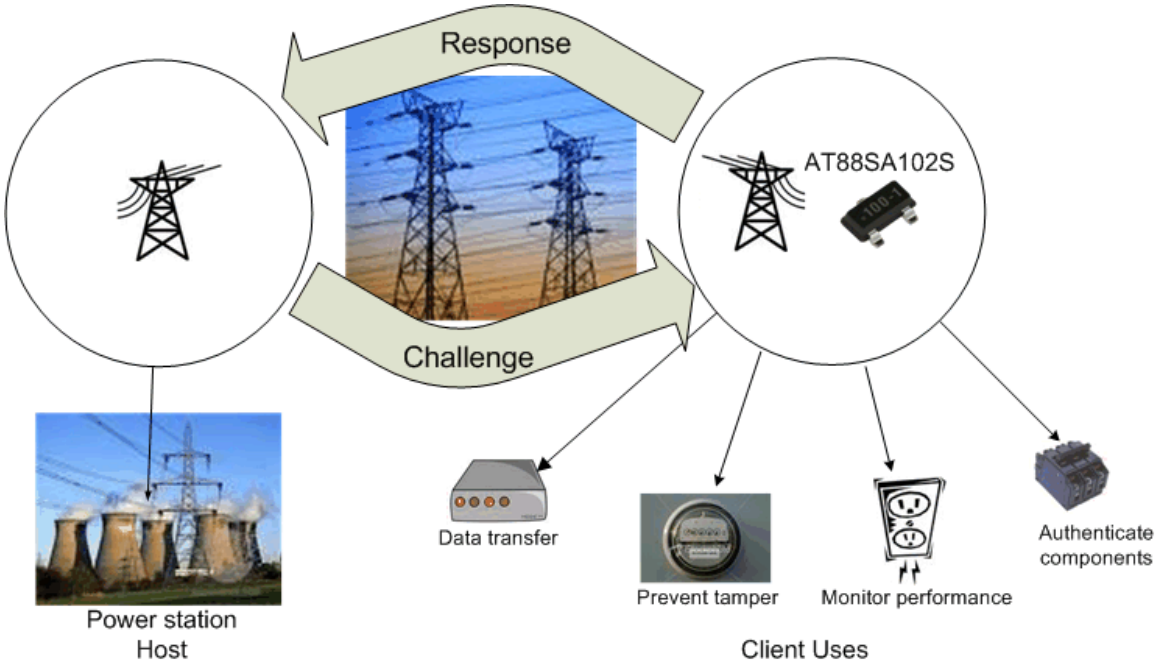

Wireless networks may need to transmit encrypted data between each node in order to prevent “man in the middle” and eavesdropping attacks. The AT88SA102S CryptoAuthentication can be used to facilitate encrypted communications between wireless nodes. To accomplish this would require placing AT88SA102S devices both sending and receiving nodes This would be done by sending a random challenge to the AT88SA102S device in the transmitting node and using the response as a symmetric encryption key to encrypt the transmitted data prior to transmitting. The transmitting node would send the random challenge along with the encrypted data packet. In the receiving node an AT88SA102S device with the same key would send the random challenge to its device and use the response generated by the device as a decryption key.

The AT88SA102S device could also be used to authenticate the transmission as the packet could be hashed and the hash sent along with the transmission. The receiving node would then hash the packet and verify that the hash created was the same as the transmitted hash, which would verify the authenticity of the transmission.

## 12. Authentication for Data over Power Lines

Recent advances in transmitting data over power lines provide possibilities for brand new industries. However the implementation of such systems also creates new questions about who can access transmitted information, and who is sending the communication. The devices on both ends of the communication need to be authenticated and validated. The low cost implementations using the AT88SA102S, such as shown in Figure 8, make it possible to authenticate many devices across the power grid expanding the capabilities of this new technology.

*Figure 8. Power grid Authentication*

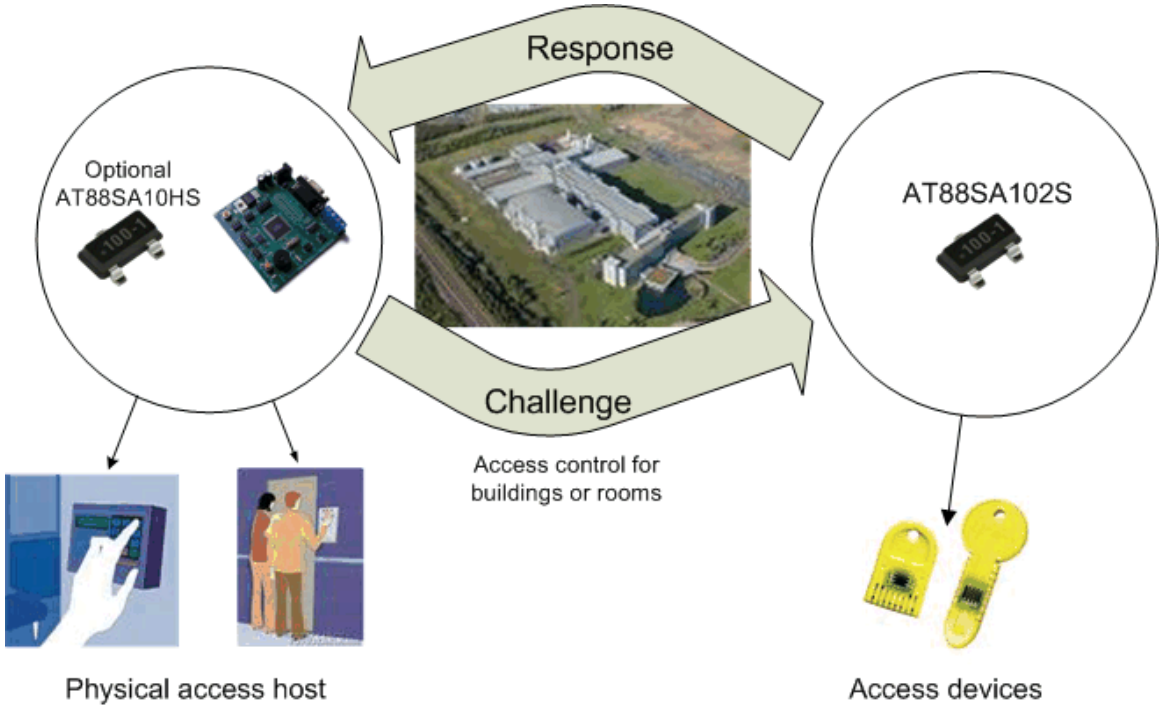



The AT88SA102S can be used to enable encrypted communications between nodes on an electrical power grid. This would be done in the same way that was explained in the section titled “Securing wireless or other radio transmission nodes”.

## 13. Physical Access Control

There are many products on the market that can be used for controlling access to buildings or campuses. Controlling physical access to authorized persons only can present many challenges when various persons or groups need to access specific resources while others need global or unit access. The AT88SA102S CryptoAuthentication device provides a great low cost solution that only uses a single communication wire to implement. The CryptoAuthentication devices can be personalized so that no two devices will ever be the same anywhere in the world. For an added level of security the AT88SA10HS device which shares the same single communication wire can be optionally used in the host to secure the host side keys. This configuration is displayed in Figure 9.

*Figure 9. Building Security*

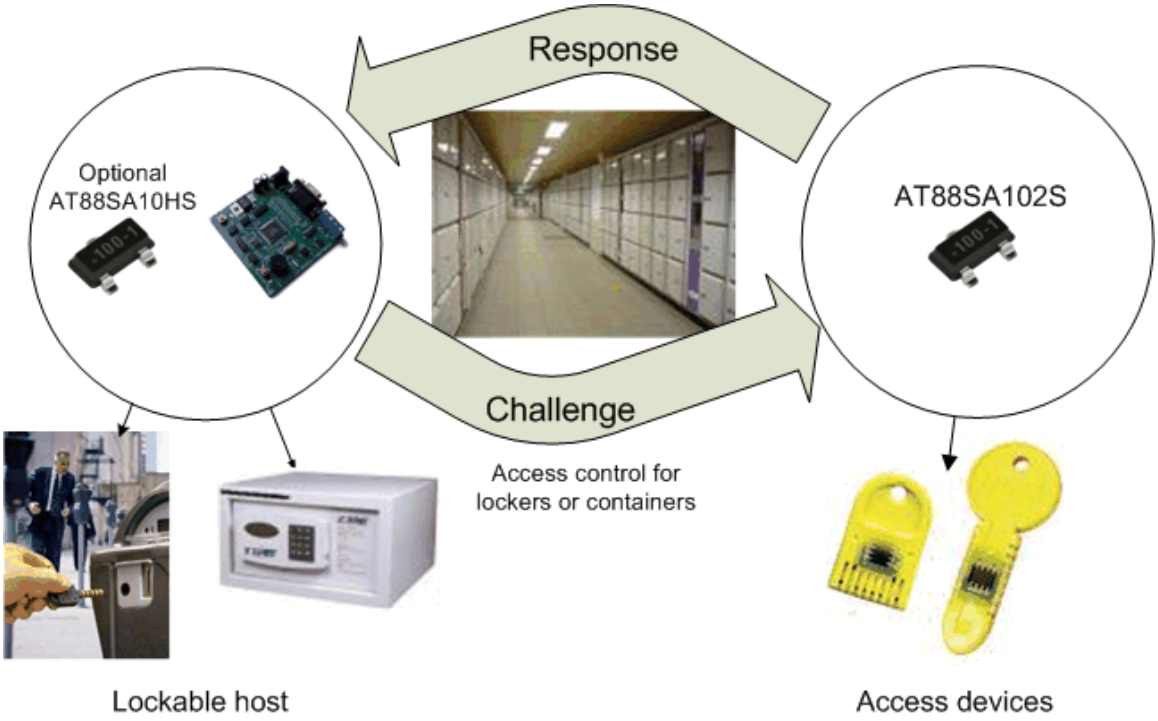



The AT88SA102S can be used to create an elaborate facility access control scheme. Unlike tumbler locks, CryptoAuthentication can be used to provide unlimited key combinations. The CryptoAuthentication device provides 62 bits of fuses that are one time programmable by the customer. The customer will use these fuse bits to customize access devices to their facility. This ensures that each customer will never have an overlap with other suppliers. The authentication process also uses that unique serial number in each chip to verify that no two users will be exactly the same. Additionally the CryptoAuthentication provides 23 sequential blow fuses that can be used to determine access configurations, monitor usage, or control use cycles. With the nearly infinite availability of keying configurations each user will have a unique configuration which could be used to track or monitor access on a personalized or a resource level for a campus.

## 14. Electronic Lockers

The cost of securing electronic lockers, safes and other small compartments multiply quickly when the number of individual units is large. Solutions using the AT88SA102S CryptoAuthentication device now make securing many individual units or areas with many zones very affordable. The optional addition of the AT88SA10HS device can be used on the host side to make the lock both very secure and very inexpensive. Figure 10 displays the AT88SA10HS/102S devices being used to secure electronic locking applications.

*Figure 10. Storage Lockers*

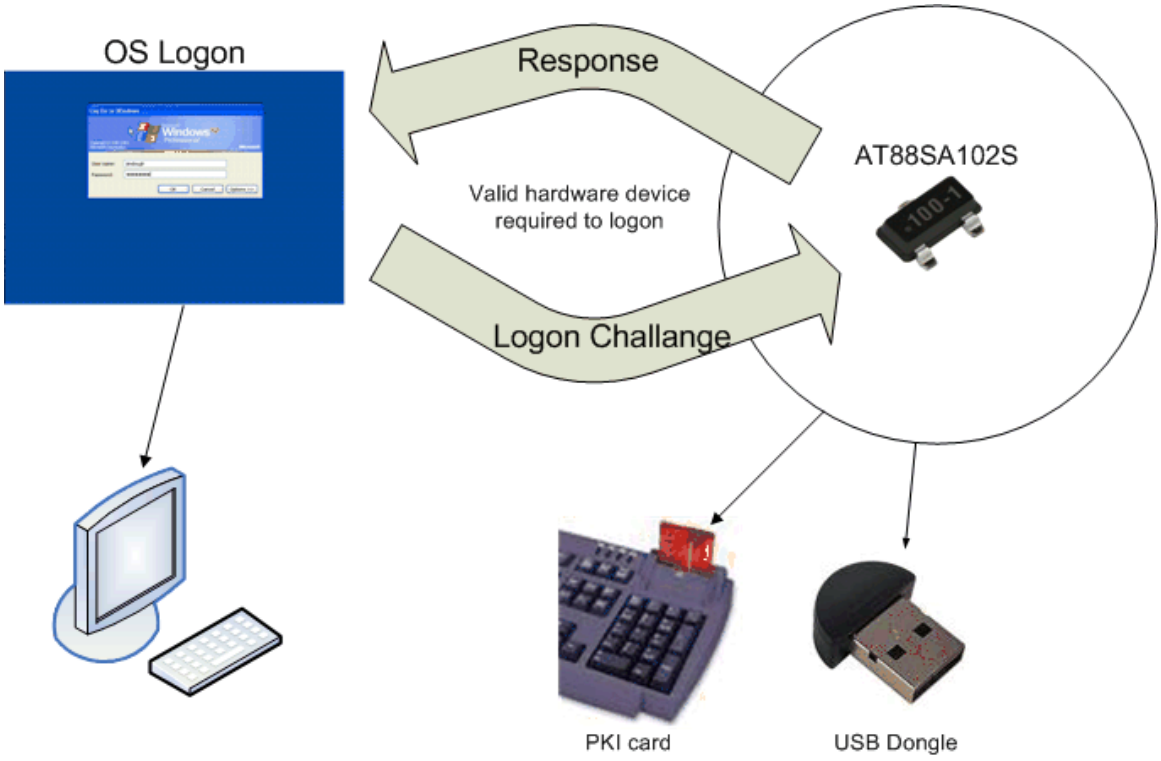



The customizable aspect of the AT88SA102S uses unique serial numbers in each device along with 62 bit customer implemented secrets and a 265 bit secret key. This enables each locker produced to have a unique worldwide keying combination, eliminating any possible overlap or key combination reuse as often occurs in tumbler lock solutions. Master lock keys could also be produced for a set of units or product line. The incrementally burnable keys could be used to implement a per use payment structure or to render keys unusable after a preset number of usages.

## 15. Hardware User Authentication

Users log on to many systems each day, in many cases using unique passwords. Users may be tempted to manage their passwords by writing them down, while convenient for the user this is one of the leading causes of security compromise. The AT88SA102S offers an additional level of security for hardware “two factor logon” at a low per user cost. Configuring the system to communicate with the AT88SA102S prior to allowing user access provides increased security over password authentication alone. The implementation of a hardware user authentication is displayed in Figure 11.

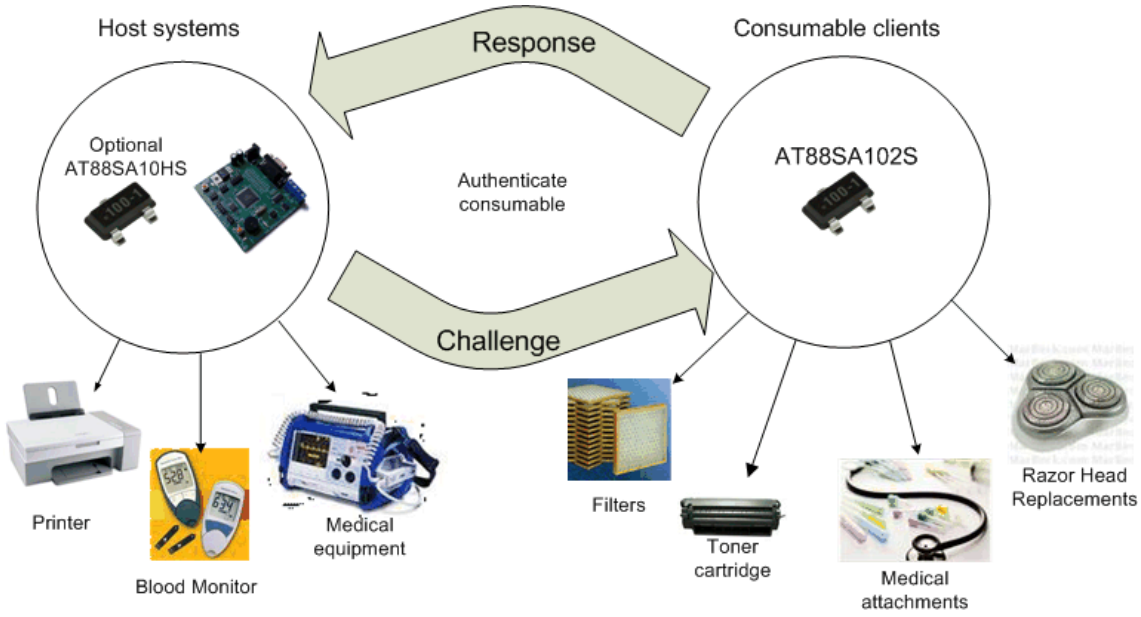
*Figure 11. Two Factor Logon*



## 16. Consumable Product Authentication

By embedding the AT88SA102S into the consumable (client) and sending a challenge from the system (host) companies can guarantee that only authentic consumables are used in their systems. Figure 12 shows an example of using the AT88SA102S to validate consumables.

*Figure 12. Consumable Authentication*



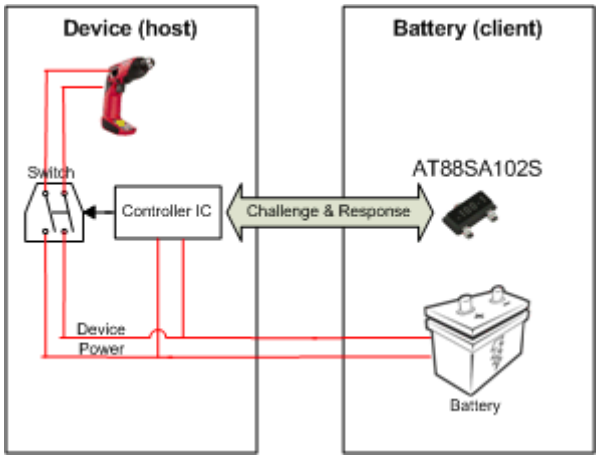

Secure personalization of each consumable must be implemented using the 62 bits of secret fuses. Using the secret fuses to implement a key diversification scheme is recommended in order to limit the adverse effect if one of the keys is compromised by failed control processes or corporate espionage. When using a diversified key the source of compromise can be isolated and a remedy implemented much more rapidly. The incremental burn fuses provided by the AT88SA102S can also be used to provide a consumable usage tracking or to limit device usage cycles.

An additional level of security can be added to the system by using the AT88SA10HS in the host. The AT88SA10HS maintains the secret keys in hardware instead of embedding them into the host microprocessor code. This makes the keys irretrievable for hackers attempting to circumvent the system.

## 17. Battery Authentication

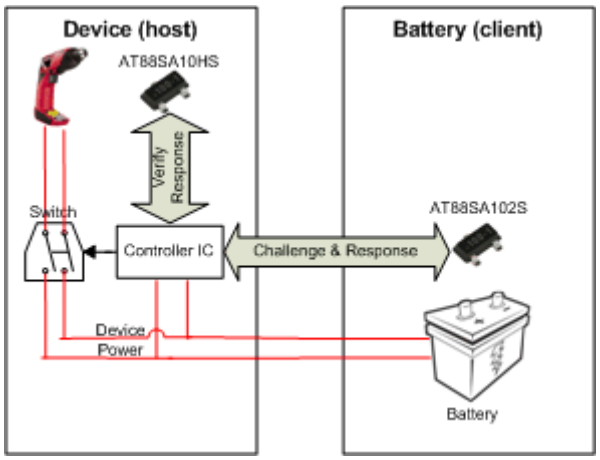
The AT88SA102S chip can be used in battery powered embedded systems to authenticate the battery (client) that connects to the portable embedded system (host). The AT88SA102S is installed in the battery; on startup the host communicates to the client by sending a challenge; the client responds with a unique response. The AT88SA102S is also capable of configuration where one host can use multiple replacement batteries or battery models. Figure 13 displays the configuration of the AT88SA102S device for battery authentication.

*Figure 13. Battery Protection*




An additional level of security can be added to the system by using the AT88SA10HS in the host. The AT88SA10HS maintains the secret keys in hardware instead of embedding them into the host microprocessor code. This makes the keys irretrievable for hackers attempting to circumvent the system. The addition of the AT88SA10HS is displayed in Figure 14.

*Figure 14. Battery Protection with Host Device*




## 18. Summary

The multipurpose functionality of the CryptoAuthentication devices makes them an exceptional tool for enabling hardware security. Nearly any application that requires authentication or individual identification of nodes can use this device as part of its security solution architecture. If your security requirements vary from those listed in this document or you are not sure that the CryptoAuthentication devices fit your specific application, please contact your local Atmel representative. Chances are we have a product that will fit your need.

## Appendix A. Glossary

**Embedded system that performs validation or authentication (host)**

A special-purpose computer system designed to perform one or a few dedicated functions, often with real-time computing constraints. It is usually embedded as part of a complete device including hardware and mechanical parts.

**Product being protected or authenticated (client)**

A special purpose embedded system that performs limited functionality and is usually does not perform any actions on its own but is entirely dependent on the host system.

**Symmetric encryption algorithm**

An encryption algorithm where the same key is used for both the encryption and decryption of data. The key must be kept secret, and is shared by both the message sender and recipient.

**Data Encryption Standard (DES)**

A method for encrypting information that was selected by NBS as an official Federal Information Processing Standard (FIPS) for the United States in 1976. DES is currently recommended for end of life by NIST[1]

**Advanced Encryption Standard (AES)**

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.[1]

**Joint Test Action Group IEEE 1149.1 (JTAG)**

Standard group formed in 1985 to develop a testability framework. A working group now under the Computer Society of the IEEE's Test Technology Technical Committee (TTTC). Has taken the TM and ETM-Bus specifications of the Department of Defense as a basis for the new set of draft IEEE standards numbered 1149.x.[2]

**In Circuit Emulator (ICE)**

The in-circuit emulator (ICE) is commonly adopted as a microprocessor debugging technique. In this paper, a parameterized embedded in-circuit emulator and its retargetable debugging software are proposed. The parameterized embedded in-circuit emulator can be integrated into different style processors such as microcontroller, microprocessor, and DSP processor. The GUI interface debugging software can help user to debug easily. As a result of it, the duration of microprocessor debugging design procedure time is reduced.

**Integrated Development Environment (IDE)**

Software program which allows the use of different individual tools from one single development platform.[2]

**Programming Services**

A system operated by Atmel to provide a secure method to insert customer's secrets into devices as a part of the device manufacturing process.

[1] National Institute of Standards and Technology, Nov 26, 2001. http://csrc.nist.gov

[2] IEEE Standards Organization, May 12, 2009. http://standards.ieee.org

## Supporting Documents

CryptoAuthentication High Level Security Design

## Appendix B. Revision History

| Doc. Rev. | Date | Comments |
|---|---|---|
| 8663B | 03/2009 | Initial document release |

## Headquarters


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


## International


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

***Atmel Europe***
Le Krebs
8, Rue Jean-Pierre Timbaud
BP 309
78054 Saint-Quentin-en-
Yvelines Cedex
France
Tel: (33) 1-30-60-70-00
Fax: (33) 1-30-60-71-11

***Atmel 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


## Product Contact

***Web Site***
www.atmel.com

***Technical Support***
securemem@atmel.com

***Sales Contact***
www.atmel.com/contacts

***Literature Requests***
www.atmel.com/literature




**8663B–SMEM–3/09**