Using a Cryptographic IC for Key Management and Logistical Support

Atmel White Paper

Author:
Christopher Gorog, PMP, Applications Manager

Abstract

System architects and designers often find themselves faced with unique challenges of managing communication, authentication, and other security needs across multiple systems, components within a system, or varying system models. In later stages of the same product cycle, production engineers need the ability to manage multiple subcontractors, supply chains, product compatibilities, and/or licensing requirements across their various product lines.

Turnkey cryptographic ICs can provide a central mechanism to implement all these capabilities. It provides the architectural, development, and production groups with a centralized management tool integrated into each system that facilitates overall product management. This article will benefit both high level architects looking to improve new products as well as system designers tasked with solving one or more of these issues in a timely and cost-effective way.

Table of Contents

Introduction

In this document, we will explore a solution to two major industry problems. The first problem is the management of security needs within embedded system products. These security needs start with verifying the internal integrity of individual products, but they do not end there. Most products today interact on a scale that is larger than their own attached components. They communicate with peripherals, other embedded systems, and outside data sources. With the interconnection of systems comes the security need for verifying attached peripherals, authenticating remote sources, and protecting or verifying data communications. The first solution will explore how an onboard cryptographic IC in each embedded system can provide solutions for individual and multi-system security needs.

The second area that will be addressed is the logistical needs for overall management of product lines and manufacturing processes. The logistical support problems addressed by this document fall into two general areas: production or manufacturing support, and product licensing support. The solution outlined will give manufacturers the ability to control how and where their products are used, which geographic areas they are supplied to, and/or who is licensed or authorized to use them. Companies that use multiple subcontractors in their manufacturing environment can achieve control over access to secrets and the numbers of products being produced, and restrict the markets in which their products are used.

This document will explore how the same cryptographic IC recommended for the first security solution for embedded systems can also enable the product owner to maintain control over the production, licensing, and use of their products.

Managing security for embedded devices

Security of embedded devices in the simplest description comes down to using complex math equations (algorithms) to prove who the participants of the digital conversation are (authentication), provide confidentiality of the communication between the participants (encryption), and ensure that communication has not be intercepted in transit and changed (integrity). To ensure that algorithms are strong enough to provide protection from the most advanced attacker, strong algorithm equations have been created and standardized by government and technical organizations. These standard algorithms are used in many places, and are the same for each system that uses them. In order to enable two or more systems to be unique and to allow communication only between their trusted end systems, the algorithms are designed with a unique changeable piece. The cryptographic term used to describe the changeable portion of an algorithm is a "key".

Cryptographic keys, much like the keys to your car or house, have to be protected and kept safely away from anyone you do not want to have access to your property. In the case of your house, you are protecting furniture and personal items you call your own property. In the case of a digital system, the key protects your sensitive personal files. These are the small pieces of data that define who you are. Compromising these items may allow someone to steal your personal identity and use that to commit fraud.

Management of the keys in digital systems is a very important aspect of today’s technological age. Many product lines have been hacked simply by someone discovering the key that is used in every model in the product line. In many cases, the theft of large amounts of information and large redevelopment costs could have been avoided had the system architects implemented robust key management and cryptographic protection in their product designs.

Successful key management requires a secure method of storing, exchanging, and renewing keys. In addition, systems need to be able to cryptographically verify that the keys have the same value as expected, without exposing the value of the key itself. When communicating from a system to a peripheral or between multiple systems, the same cryptographic operations performed in each system or peripheral need to produce the same result. To implement stronger levels of security, the systems should also have a method to change key values often and/or have a method to derive keys from secrets that are never accessible. The key management model should encompass the entire product line, incorporating methods of managing multiple product models.

Strength of cryptographic IC storage

Why use a cryptographic IC in the first place? Is it not possible to do the same cryptographic operations in software? The problem with software implementations is that they are written in software, and the software program has to be saved in the system. This exposes the keys and secrets in some form in unsecured memory.

Protection from this vulnerability is the central strength of the cryptographic IC. Secured memory locations are accessible only after the configured access prerequisites are met, while some other memory locations are never accessible. The memory locations are encrypted and protected by layers of physical security all beneath an active metal shielding.

Hardware cryptographic ICs provide all the features needed for a high-security key management implementation within a system, as well as between multiple systems or between systems and peripherals. Unlike software-only security implementations, the secrets inside a cryptographic IC used for key management are not accessible to the system processes. Thus, the secrets are as secure as possible.

Types of storage

The cryptographic IC memory storage enables a variety of use cases, as well as varying levels of protection. A read-only memory resource makes it possible to store manufacturer or model information. The owner of this data may not care if it is read, but does not want it to be altered. A read/write memory resource is only valuable in a cryptographic or secrets management scheme if there are restrictions on who is able to write to the memory resource. It is valuable for the cryptographic IC to provide previously set up security controls for these types of memories, limiting who has access and how they can use the memory resource. The most valuable type of memory resource in a cryptographic IC is the memory resource configured as non-readable and non-writeable. These memory contents are known only to restricted persons and/or systems, and are used to authenticate the IC as well as to verify the contents of other types of memories.

Secret memory configuration

As mentioned earlier, keys to cryptographic algorithms are very sensitive. Keeping them away from unauthorized access is the center of any key management strategy. To meet this requirement in the most robust fashion, these keys should always be stored in non-readable/non-writeable memory and never stored in unprotected memory. The cryptographic IC is designed specifically to protect these types of high value secrets.

System security needs vary, and an adept cryptographic IC should provide the capability to support multiple uses in a single IC. Flexible IC configuration options offer developers the ability to implement the following memory configurations:

1. Limited use or single use secrets
2. Secrets linked together in parent/child relationships
3. One secret authenticated prior to the read/write or encrypted read/write of another secret
4. Multiple secrets combined into a rolling authentication
5. Password storage and verification
6. Incremental counters
7. One-time programmable memory blocks
8. Individual programmable OTP bits for consumption logging

In some configurations, it is valuable to have cryptographic keys that are never written down or saved in any way. Imagine instead that each key is recreated every time it is needed for use. This configuration could utilize non-readable memory in the cryptographic IC. It would create the keys for each use by starting with a random input and using the cryptographic IC to combine the random input with the secret in unreadable memory. The cryptographic IC output would in turn be used as a temporary session key, which would only be valid for a short amount of time. This would be valuable when many nodes need to utilize the same key and need to change keys often. If each node or system contained the same cryptographic IC, they could seamlessly change keys on a network while exchanging only encrypted values that look random to any viewer.

Key management strategies using a cryptographic IC

Cryptographic ICs provide a secure method to store secrets. The data stored in the secure memory depends on the implementation, and may vary according to system needs. Choosing an IC that provides versatile configuration options is important for strong overall product key management. A versatile key management IC will have the ability to store multiple secrets, configure some as internal secrets, store some as read only, and store some with restricted read/write access.

Integrating product line management

Cryptographic ICs contain and protect the owner's secrets within the product. These secrets need to be programmed into the cryptographic IC for use by the end product. Programming the IC with custom secrets effectively matches the products functionality and/or intellectual property (IP) directly to the physical cryptographic IC. Each product is required to have a physical cryptographic IC within it in order to operate. Thus, subcontract manufacturers can only produce the number of products for which they have been provided physical cryptographic ICs.

Using such a process, product owners have the capability to control who is approved to make their products, and how many they can make. They can allocate allowed product model types, allowed feature sets, and/or limit usage intervals.

An example of a possible logistics support model could be implemented using four sections or zones of memory in the cryptographic IC. The first section/zone would contain a secret programmed by the product owner and not accessible to any licensee or subcontract manufacturer. The second section/zone would contain a secret programmed uniquely for each licensee or subcontract manufacturer, which would be kept confidential between that manufacturer and the product owner. The third section/zone would contain readable manufacturer identification information, and the forth section/zone would contain model information about the product itself.

To authenticate a valid product, product owner, licensee, and/or subcontract manufacturer, cryptographic operations can be performed on each secret separately or cumulatively. Data items for supported models, geographic areas authorized for operation, supply organization tracking, allowed usage dates, or time in the supply system could all be added into the product's cryptographic IC memory locations. Systems can verify that each data component has not been tampered with and that it matches the product owner's desired use cases. If any of the information does not match the desired product usage requirements, systems can assume that they are counterfeit or have been tampered with and restrict their usage. Advanced models can update systems in the field to blacklist the serial numbers of items that have been compromised or produced by subcontractors that are no longer in good standing with the product owner.

Cryptographic ICs can be used to place user restrictions on the product, peripheral, or subcomponent. They can restrict use of a component to only a single user or system. They can be configured to match local settings on first use to prevent multiple systems from using the same component. Products that are network connected can implement component registration, collect data, and track usage and/or user trends. Product owners and OEMs can now achieve ultimate control over how their products are used in the field.

Product control and licensing

Cryptographic ICs provide the ability to authenticate and verify beyond a shadow of a doubt that the item or information received is what it is expected to be. This capability provides an exceptional product management tool. When each product is developed around the cryptographic IC, companies and organizations have a scalable management tool to manage all products in the field as if they were a single system. Whether the need is to have the products communicating and acting like a large system or simply to keep track of them as they pass through supply chains, the cryptographic IC can become the product manager's best friend.

The business model of licensing designs or peripheral interfaces for use by other manufacturers and designers has become commonplace in today's global market environment. Companies rarely manufacture every piece of the systems they market. Often, system designers or standards organizations do not manufacturer any concrete products whatsoever. Instead, they license designs, IP, and/or knowledge of protocols for communicating to other manufacturers so that other companies can profit from expanding markets which they themselves could not satisfy.

The challenges in licensing and manufacturing products include how to verify that both trusted and un-trusted parties are utilizing IP and restricted interfaces in accordance with the product owner's licensing requirements. Enforcing the use of a cryptographic IC in each product gives the product owner a method of managing how many products are manufactured, where each product is supplied, timeframes for product supply and usage, and price or market controls. As a result, product owners can control manufacturing flow and track the efficiency of product licensee or manufacturing subcontractors.

Cryptographic IC manufacturers like Atmel have designed their ICs with customers' logistical needs in mind. They offer methods of secure programming such that the product owner's secrets are inserted in an encrypted format. This ensures that the OEM secrets are known only to the OEMs themselves.

Conclusion

This document explored a solution to two major industry problems that uses a simple, cost-effective cryptographic IC added to each system. The strong protection offered by a cryptographic IC can provide centralized security for a system, and can also provide a tool for controlling the logistics of manufacturing processes or product licensing.

Whether you are a member of an architecture, design, manufacturing, or product support team, your next step should be to contact your local Atmel sales office to learn more about the Atmel solutions that enable your company to take positive control of product management throughout the entire product life cycle.

References

1. Guidelines for Smart Grid Cyber Security, NISTIR 7628, August 2010, USA National Institute of Standards and Technology (NIST), Web http://csrc.nist.gov/publications/PubsNISTIRs.html
2. CryptoAuthentication Product Uses, March 2009, Atmel Corporation
3. ATSHA204 Datasheet, February, 2011, Atmel Corporation

About Atmel Corporation

Atmel is a leader in microcontroller and touch solutions. Headquartered in San Jose, CA, Atmel (NASDAQ: ATML) has 40 local sales offices worldwide. Atmel is a worldwide leader in the design and manufacture of microcontrollers, capacitive touch solutions, advanced logic, mixed-signal, nonvolatile memory and radio frequency components. With wafer fabrication locations in Colorado Springs, CO, and third party foundries, Atmel is able to provide the electronics industry with complete system solutions focused on consumer, industrial, security, communications, computing and automotive markets. In addition, the company has test and assembly facilities in the Philippines and subcontractors, employing approximately 5,100 employees worldwide.

Further information can be obtained from the Atmel website at www.atmel.com.

Contact: Christopher Gorog, PMP, Applications Manager, Colorado Springs, Colorado, USA
Tel: (+1) (719) 540-1451
email: Christopher.Gorog@atmel.com

Atmel Corporation
2325 Orchard Parkway
San Jose, CA 95131
USA
Tel: (+1)(408) 441-0311
Fax: (+1)(408) 487-2600
www.atmel.com

Atmel Asia Limited
Unit 01-5 & 16, 19F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
HONG KONG
Tel: (+852) 2245-6100
Fax: (+852) 2722-1369

Atmel Munich GmbH
Business Campus
Parkring 4
D-85748 Garching b. Munich
GERMANY
Tel: (+49) 89-31970-0
Fax: (+49) 89-3194621

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

Disclaimer: The information in this document is provided in connection with Atmel 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 Atmel products. EXCEPT AS SET FORTH IN THE ATMEL TERMS AND CONDITIONS OF SALES LOCATED ON THE ATMEL WEBSITE, ATMEL ASSUMES 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, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS AND PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Atmel 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 products descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.