Injecting Trust to Protect Revenue and Reputation

A Key Injection System for Anti-cloning, Conditional Access and DRM Schemes

A Certicom Technical Overview
October 2005

certicom™

Introduction

Electronic keys uniquely identify, protect and authenticate devices used in conditional access and digital rights management (DRM) schemes such as DTCP (Digital Transmission Content Protection), HDCP (High-bandwidth Digital Content Protection), CPRM (Content Protection for Recordable Media) and others. In these cases, if a device is cloned, content owners lose the ability to control access to files and streaming media; service providers lose the ability to charge for services and device vendors lose the trust of their customers.

In cases such as medical devices and industrial sensors, it is essential that only authorized components are used in the system or network in order to protect the brand or integrity of the solution. Cloned devices not only represent a substantial revenue loss for companies that make their money on replacement parts, but also represent a significant risk to their brand.

Embedding keying material at time of manufacture can help solve several device life-cycle problems. The keying material can come in a variety of formats (from data encrypted on a CD to signatures on digital certificates) but the need to protect it is the same as it forms the basis for the security of the system. In fact, if keys are leaked, the security of the entire system can be compromised for many years, and there is a potential of losing millions of dollars in revenue.

This paper discusses how traditional methods for transferring keying material to manufactures can be compromised. This is referred to as key leakage and can lead to cloned products that erode revenues and in the case of replacement parts, a company's reputation. This paper also discusses how a cryptographically 'wrapped' key-injection system gives control of keying material back to the device vendor and ensures an efficient and secure distribution of data material that does not impact the manufacturing process.

Before looking at the specifics of key injection and Certicom's solution, the following use cases will show how widespread and varied the security problems can be within the manufacturing process.

certicom™

The Need to Inject Keys Securely

Cloning of devices and replacement parts negatively affects the entire supply chain from the device manufacturer to the content provider and service providers. In other cases, potential fines can be levied against organizations that are found to have leaked keys, intentionally or not. This section shows several problems that can be solved with a trusted key injection platform.

Outsourced manufacturing

As consumers continue to demand devices that are cheaper and manufactured faster, vendors are forced to outsource more of their manufacturing process. Although some would point to this trend as continuous improvement and globalization, outsourcing presents its own unique challenges to device vendors such as the splitting of a manufacturing run.

For example, a third-party manufacturer could produce the contracted quantity of devices plus an additional amount. In this scenario, the device vendor receives the contracted quantity but the rest of the devices are sold on the black market. These cloned devices represent significant revenue lost to the device vendor.

In the case of silicon vendors, the issue is preventing key injection mistakes. For example, if the same key is inserted into more than 1 chip by mistake, when the OEM assembles the system and tries to bind the key to the device serial number, the manufacturing process gets interrupted when the same key appears more than once. This would result in a brand and quality control hit on the silicon vendor.

In both cases, the vendor needs a mechanism to meter and track the number of devices produced and the keys inserted by the third-party manufacturer. Otherwise there is no way to determine how many cloned devices have been manufactured and are being sold in the market or if there is a quality issue with the chip. Device and silicon vendors need to stop an illegitimate production run by controlling the amount of keying material the manufacturer receives or quickly eliminate any quality issues on the run.

Subscription services

Consumer products, especially those associated with service providers, are well-known targets of illegitimate businesses.

Devices, such as mobile handsets, set-top boxes and satellite radios, are exposed to risks from fraud and theft of service. As these devices become platforms for additional value-added services, security threats create a liability for service providers where the potential loss of revenue could be significant.

With the advent of digital rights management (DRM), security is the center of attention. The security of the entire system begins with ensuring the unique identifiers for each device are protected from the time the device is manufactured and throughout its lifetime.

The common requirement among these devices, especially ones subsidized by service providers, is the need for secure boot, a service lockdown mechanism, remote provisioning and service activation. These requirements begin with unique keying material being injected securely into the device.

Brand protection and the business of replacement parts

Device vendors that invest significant money and time on innovation are also affected by the cloning of replacement parts.

In the technology arena, the replacement parts often contain information, such as machine configuration data or critical parameter data, which allows a device to operate correctly. For example, replacement medical parts used to monitor a patient or administer a treatment, could update the treatment machine with new safety parameters.

These replacement parts or devices contain functionality resulting from innovative and expensive research and development. While very few malicious manufacturers are capable of re-creating this critical information, many of them could reproduce or copy the replacement part. This cloning erodes a vendor's investment and could negatively affect its reputation and brand should the cloned part interfere with the quality and operation of the device.

Similar to the problem described above, a common business model for selling expensive machines is to initially sell the complete machine or system at a price that is not beneficial to the seller, and reclaim foregone profits by supplying parts for the ongoing operation of the initial sale.

Therefore, anything the original manufacturer can do to legally reduce the number of parts manufactured by other parties is important. To do this, original manufacturers need to find ways to raise the initial or ongoing cost of producing the replacement parts.

These anti-cloning techniques rely on cryptography and trusted computing concepts that are beyond the scope of this paper. However, in both cases the solution rests on securely injecting unique keying material into the replacement part, otherwise original manufacturers may face erosion of revenues from cloned devices as described in the first use case.

Industrial sensors

The cloning of devices has become a significant problem, especially for industrial sensor manufacturers. These devices are typically difficult to design but inexpensive to build. Cloning operations avoid the costs associated with innovation by focusing solely on material duplication. They harvest the benefits of the innovation by producing components in the same form as the original manufacturer and unfairly competing with the original manufacturer's product.

Producers of industrial sensors are also concerned with protecting their brand as quite often their devices are part of mission critical processes. Any cloning of their devices would represent a financial loss and could negatively affect their reputation and brands.

Similar to the use cases above, this issue can be solved by securely injecting keys into the device so that only legitimate sensors can be added to the network. At the same time these keys need to be tracked and reported on to ensure "extra" devices are not sold on the black market.

Vendors can rely on security technologies to make themselves a less attractive target to illicit organizations that try to hijack business by stealing and reproducing manufacturer's innovative technology.

The Role of Key Injection

Key injection is a critical component of anti-cloning, DRM and conditional access systems. Unique keying material is embedded into a device to create a unique identifier that links a particular device to services, replacement parts and billing systems. This unique identifier also protects customers and end users against the tedious procedures required to register devices.

Since the manufacturer is the only one to have access to keying material, only the manufacturer can create new devices and replacement parts.

The security gap in legacy key-injection systems

Traditionally, a vendor that is concerned about securing the key injection stage at a manufacturing site has little choice but to implicitly trust that a third-party manufacturer is operating in a manner that gives due consideration to the vendor's device and system security. And, although the keying material itself is secure, often the channel for transport and delivery of the keying material to the third-party manufacturer is not. This security gap leads to an increased risk of cloned devices and replacement parts often sold on the grey market.

Typically, a vendor uses one of two delivery methods to send unique keying information to a third-party manufacturer.

Bulk encryption method

Keying information is bulk encrypted and sent to the manufacturer, where, upon arrival, all of the keying material is decrypted at once, and the manufacturer is then trusted not to compromise the bulk of information. Although this method of sending bulk keying material is efficient and doesn't slow down the manufacturing process, the vendor loses control of the keys because there is no metering or reporting mechanism. A vendor has no way of knowing whether keys not used in the legitimate manufacturing process were destroyed or used to manufacture clones.

Online method

Another transport method used—one that restricts access to keying information—is an online client-server mechanism. With this mechanism, a client at the manufacturer's facility is connected to a network and makes requests for keying information on a per-device basis, to a server under the control of the vendor.

Although more secure than the bulk encryption method, there are a number of problems with the online process. The primary concern is that an off-site server that uses a public shared packet-switched network cannot guarantee a minimal service level or response time to the manufacturing line. And secondly, most manufacturing facilities will not begin a production run without all of the necessary materials on hand, including data materials. Delays in supplying keying material can result in down-time on the manufacturing line which is a considerable expense.

When device vendors outsource manufacturing to third-party vendors who are often geographically dispersed and near impossible to monitor, they need a mechanism to not only secure transport but also monitor the manufacturing process. They need a system to allow them to 1) report on identities and number of units manufactured and 2) restrict access to keying information without impacting the manufacturing process.

Innovative and Secure Key Transport/Injection System

Backed by 20-years of experience in cryptography, Certicom developed Certicom KeyInject™, a trusted key injection platform that enables device vendors to track production outsourced to contract manufacturers, and greatly minimize the risk of device cloning. Certicom KeyInject controls access to keying information, metering the use of this information and generating reports on key usage. This system solves the problems inherent in both the bulk encryption and online method.

By using Certicom KeyInject, vendors can restrict access to the keying data and ensure that the information is secure right up until the instant the device is programmed. The system consists of a controller module and an appliance module connected by two-way communication channels.

In addition to securing the transport of the keying material, Certicom KeyInject produces a usage report that identifies the keying material used and the number of units manufactured. Manufacturers must submit each session's usage information before being granted access to additional keying material. This reporting mechanism provides times and a date stamp. So, although the keying material is sent in bulk, vendors control access by asking for information on usage and then issuing credits, called metering, quickly over the Internet. Vendors retain control over the keying information without having a negative impact on the manufacturing process.

By gaining access to usage information, vendors not only control distribution of keying material, they can use this information to better understand the manufacturing process. Should they be suspicious of the legitimacy of the process, they can stop or restrict a manufacturer's ability to key devices through the metering system.

An added benefit of the usage report is that vendors can also better understand manufacturing capacity, which could be useful for scheduling or sourcing future projects.

certicom™

Certicom KeyInject

The core of KeyInject's security is in the Hardware Security Module (HSM), a FIPS 140-Validated cryptographic PCI card. The most sensitive program code for KeyInject runs within the security boundary of the HSM which protects the cryptographic identity of the KeyInject server, maintains the KeyInject meter, and enforces the KeyInject reporting policy. This level of security is accomplished by storing data values directly on the HSM, which can only be accessed by the HSM's internal secure state machine. Any attempts to retrieve, or otherwise compromise, these highly secured KeyInject data elements will cause the HSM to erase all of its internal memory.

The key components in Certicom KeyInject include:

- Certicom KeyInject Controller – Trusted key management and reporting system for the device vendor, typically located at head office
- Certicom KeyInject Appliance – Trusted key injection and metering appliance installed at the third-party manufacturer site
- Key Source – Custom key generation or loading of third-party keys that may be acquired from a licensing authority such as Digital Content Protection, LLP
- Customization Services – Interface to third-party manufacturing line equipment

The key features of Certicom KeyInject include:

- Supports any number of manufacturing sites
- Provides a single point of access to control, manage and get information about keys distributed to multiple sites
- Provides access to key usage information when needed or in near real-time
- Easy to use and easily configurable (HTML-based) user interface, so it can be quickly tailored to a silicon vendor or OEM's needs
- The key material can be changed or altered to support different modes of key transport
- Supports on-device key generation
- Connects to any key source, or Certicom can provide the key source
- Key material can be changed or altered to support multiple product models on a given manufacturing run

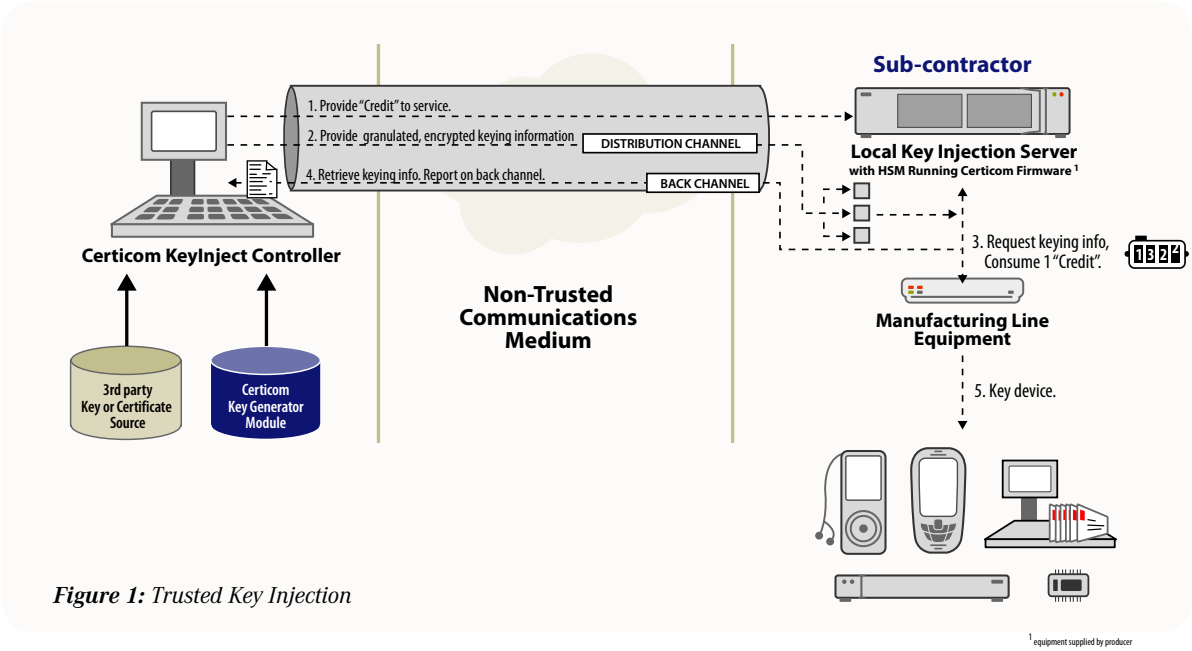

Figure 1: *Trusted Key Injection*

The KeyInject process

- KeyInject Appliances are built and shipped to customers for registration (assigned cryptographic identities) which occurs using a secure protocol that communicates directly with the controller. KeyInject Appliances are then sent to manufacturing facilities.
- Certicom KeyInject creates a secure pipe between the device vendor and the contract manufacturer.
- The device vendor creates device keys and bulk encrypts them for transmission to the manufacturer.
- Bulk encrypted data is stored on-site in the KeyInject Appliance and decrypted for the manufacturer as needed.
- Appliances are operated independently of the KeyInject Controller, but they require information from the controller to update configuration and increase their credit pool, which is the metered number of decryptions.
- The HSM is used to protect decryption keys on-site and force usage reports.
- The KeyInject Appliance must be periodically loaded with more keys. To get the additional keys, it sends its encrypted key report (Encrypted Back Channel Log) to the KeyInject Controller and if the report is valid, the KeyInject Controller releases more credits to the Appliance. Each record contains a sequenced serial number that is assigned by the HSM before the record is cryptographically protected. If a manufacturer alters or prevents the record from being sent back to the controller, the controller will know.

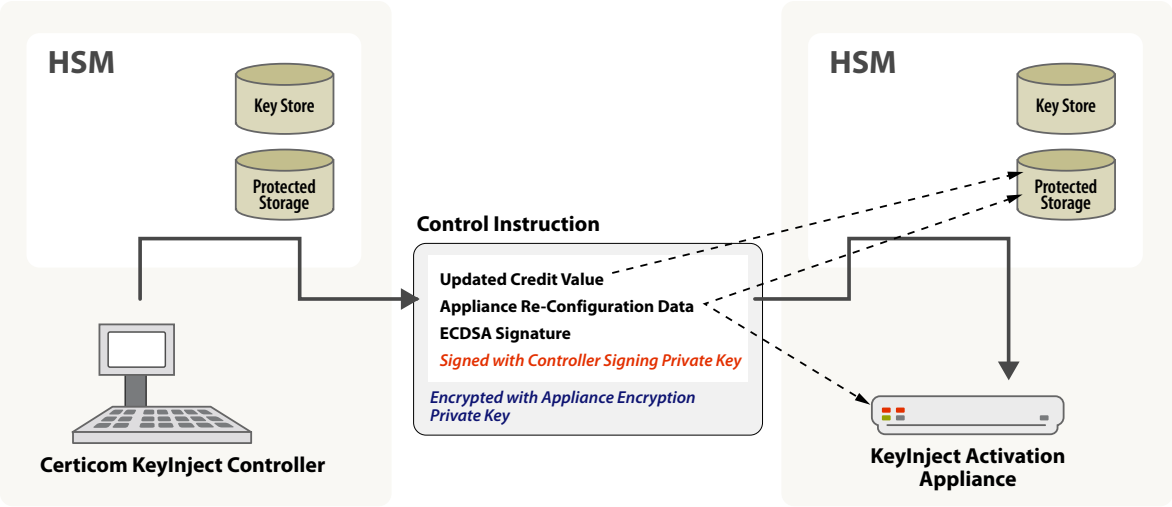

Figure 2: *Control Instruction*

Certicom's Advantage: Understanding the Manufacturing Process

For a key injection system to be truly effective, it must be flexible enough to support a vendor's unique needs during the manufacturing process. KeyInject offers that flexibility. For many years Certicom has worked with device vendors. Certicom understands the embedded and device industry, their technologies, processes, challenges and security risks. Certicom has identified that the majority of device vendors use one of three modes to assign a cryptographic identity to a device, known as provisioning a device. Two of these methods are based on injecting keys into a device; the third method consists of the device generating its own key.

While the methods are effective in assigning key identifiers, there are security risks associated with each. Certicom KeyInject can be configured to match the system's key scheme and address the security problem associated with each mode.

1) **Addressable key:** A serial number on the device is associated with a unique key which is stored on a database maintained by the device vendor. These keys are typically generated through a third-party conditional access or DRM scheme. With Certicom KeyInject this information is metered and reported so that the device vendor maintains control, and can determine which device is linked to which key.

2) **Sequential key:** Under this scheme, manufacturers allocate keys, which are usually provided by a third-party, to devices in sequencial order, which if not controlled could result in the same key being used twice. Certicom KeyInject prevents duplication by metering and reporting on key usage and distribution. This prevents key duplication: once used, a key can never be injected into a second device.

3) **Digital signature generation:** This scheme allows a device to create its own keys. A public key is bound to the device through a digital signature. Certicom KeyInject provides the metering and reporting that confirms the number of devices made and their cryptographic identity, data which proves it is an authorized device.

Mode of Operation

As with each key scheme discussed above, Certicom KeyInject has been designed to support several deployment options or modes. The modes, known as network and file, accommodate the available systems of the third-party manufacturer, and seamlessly fit into the manufacturing process.

1. Network mode: For those companies with a reliable network, Certicom KeyInject can be configured in Network Mode. This mode allows the Certicom KeyInject Controller to actively go out to a network to monitor, replenish and gather reports from the Certicom KeyInject Appliance. Under this mode of operation, Certicom KeyInject establishes a secure SSL pipe between the Controller and Appliance to transmit secure messages. The SSL pipe is mutually authenticated with elliptic curve cryptography (ECC) -based certificates on either end of the connection.

2. File Mode: For companies located in areas with unreliable networks, Certicom KeyInject can be installed in File Mode, an offline deployment method. Keying material sent by CD, DVD or other offline method is cryptographically protected from transport through to injection.

Both modes of operation use the same messaging structure to securely store, forward, process and maintain KeyInject-related data and keys. All messages use ECC, AES, and SHA-2 cipher suites to implement the Certicom KeyInject protocols.

Conclusion

In today's competitive environment, the challenges and risks faced by device vendors can be overwhelming. They need to balance the cost of innovation against the realities and demands of the marketplace. Certicom KeyInject can help meet those demands by giving vendors a cost effective factory provisioning system that protects against the ever growing device cloning threat from third-party contract manufacturers. Certicom KeyInject specializes in controlling and reporting the volume of keyed devices, at manufacture time, to protect a company's investment from black market device threats with a focus on complementing conditional access and DRM systems.

certicom™

About Certicom

Certicom protects the value of your content, software and devices with government-approved security. Adopted by the National Security Agency (NSA) for classified and sensitive but unclassified government communications, Elliptic Curve Cryptography (ECC) provides the most security per bit of any known public-key scheme. As the undisputed leader in ECC, Certicom security offerings are currently licensed to more than 300 customers including General Dynamics, Motorola, Oracle, Research In Motion and Unisys. Founded in 1985, Certicom's corporate offices are in Mississauga, ON, Canada with worldwide sales headquarters in Reston, VA and offices in the US, Canada and Europe. Visit www.certicom.com

Contact Certicom

Corporate Headquarters

5520 Explorer Drive, 4th Floor
Mississauga, Ontario
L4W 5L1
Tel: +1-905-507-4220
Fax: +1-905-507-4230
E-mail: info@certicom.com

Sales Offices

Worldwide Sales Headquarters
1800 Alexander Bell Dr., Suite 400
Reston, Virginia 20190
Tel: 703-234-2357
Fax: 703-234-2356
E-mail: sales@certicom.com

Ottawa
84 Hines Road, Suite 210
Ottawa, Ontario
K2K 3G3
Tel: 613-254-9270
Fax: 613-254-9275

U.S. Western Regional Office
393 Vintage Park Drive, Suite 260
Foster City, CA 94404
Tel: 650-655-3950
Fax: 650-655-3951
E-mail: sales@certicom.com

Europe
Golden Cross House
8 Duncannon Street
London WC2N 4JF UK
Tel: +44 20 7484 5025
Fax: +44 (0)870 7606778

Engelska Huset
Trappv 9
13242 Saltsjo-Boo
SWEDEN
Tel: +46 8 747 17 41
Mobile: +46 70 712 41 61
Fax: +46 708 74 41 61

www.certicom.com