Meeting Government Security Requirements Today and Tomorrow

An Overview of the Certicom Security Architecture for Government

December 2004

certicom™

Introduction

Government IT spending in 2004 is $46B, and is expected to … reach $56.5B by 2009

– (Datamonitor PLC, 2004)

The government market has always been a lucrative market for technology companies. As government communications become more and more networked, the range of devices to access this network has grown, and with it, the need for security. Many of these devices require security and the government will be spending a lot of money to satisfy these requirements.

Federal Information Processing Standard (FIPS) 140-2 has become the de facto security standard within the government—not only in the United States, but in other countries as well. Other industries such as healthcare and finance have also adopted FIPS 140-2 because of the high degree of security it specifies. Under the US Federal Government's Crypto Modernization Program, requirements such as Elliptic Curve Cryptography are also making headway in the government space and will have greater impact in the future.

However, the road to FIPS Validation is long, complex and expensive, and the FIPS standards themselves require constant monitoring to ensure compliance. Vendors looking to capitalize on sales to the government need a solution that will simplify the process of getting to market for them and offer the flexibility to meet future requirements.

Through an examination of current government security requirements, including the FIPS 140-2 Validation process and its challenges, this paper will show that the Certicom Security Architecture for Government provides government suppliers with a competitive advantage today, and offers a bridge to future success.

certicom™

Government Security Requirements

Like any other organization, government agencies would like to be able to use commercial off-the-shelf (COTS) products. In order to use these products, however, they must meet stringent security requirements that have been set out by organizations such as the Department of Defense, National Institute of Standards for Technology (NIST) and the National Security Agency (NSA). By far the most important directives revolve around the FIPS 140-2 standard. The Department of Defense refers to this standard in a number of directives it created for the communication of sensitive data. In fact, FIPS 140-2 is becoming the de facto standard for government security requirements.

Departments and agencies that deal in mission-critical national security information must use products that meet a further criteria—NSA-approved product. At a recent Internet Engineering Task Force on security[1], the NSA presented their requirements—one of the key stipulations was the use of Elliptic Curve Cryptography (ECC)-based algorithms.

To capture a piece of this evolving market, or even maintain current positions, vendors who traditionally have not required a high level of security expertise have no choice but to expand their understanding of these standards and cryptography. The products developed must meet the continually advancing specifications.

The following directives refer specifically to FIPS 140-2 requirements for security-related products purchased by the government:

- **Department of Commerce Directive 16-02** (December 1992)
- **National Information Assurance Acquisition Policy (NSTISSP) No. 11** (June 2002)
- **Department of Defense directive 8500** (October 2002)
- **Department of Defense directive 8500.1/8500.2** (October 2002/February 2003)
- **NIST Special Publication 800-23**
- **Department of Defense directive 8100** (April 2004)

A number of European and financial standards also refer to FIPS 140-2.

FIPS and the importance of FIPS 140-2

In the US, requirements for government security are regulated by FIPS publications, which are developed by NIST for use government-wide. NIST develops FIPS publications when there are compelling federal government requirements for security and interoperability and there are no acceptable industry standards or solutions.

By far, the most important is FIPS 140-2, which describes US federal government cryptography requirements that software and hardware products must meet for sensitive but unclassified use. FIPS 140-2 refers to the validation of the complete module that applications must call on to perform the cryptographic functions. More detail is provided below. Other FIPS, such as FIPS 186-2, which describes the use of the Elliptic Curve Digital Signature Algorithm (ECDSA), and FIPS 197, which specifies the Advanced Encryption Standard (AES) refer to specific implementations of algorithms, which can be included inside the FIPS 140-2 Validated module.

FIPS 140-2 Validation on products that implement cryptography is quickly becoming mandatory to sell to the government market. In 2002, The Federal Information Security Management Act (FISMA) removed the provision that allowed agencies to issue waivers for the purchase non-FIPS

[1] IETF, Security Area Advisory Group meeting, November 11, 2004.

approved products. Without FIPS 140-2 validation, vendors will be prevented from selling their products to government customers.

Because of the high level of security ensured by FIPS, other countries such as the United Kingdom and Canada and other industries such as financial and healthcare are also starting to adopt FIPS standards, and particularly FIPS 140-2, for their security requirements.

A look at FIPS Validation

For most vendors, there are two forms of FIPS validation. The first validates only the encryption techniques used by a particular algorithm such as those referred to in FIPS 186-2 or FIPS 197. This includes symmetric encryption algorithms such as AES, DES, 3DES and RSA; hash algorithms such as SHA-1 and digital signatures such as DSA and ECDSA. In this case FIPS identifies how these are defined, and how they must be implemented to achieve validation. The Cryptographic Algorithm Validation Program (CAVP), operated by NIST, handles these validations.

The second, higher level, and more important validation is FIPS 140-2. This standard specifies eleven security areas that must be met by a "cryptographic module" used inside a security system that protects information. A cryptographic module can be hardware, firmware or software that carries out cryptographic functions like encryption, authentication techniques or random number generation. A cryptographic module performs the security services for a particular product. FIPS 140-2 also provides four increasing, qualitative levels of security, from 1 to 4 (1 being the lowest) for these eleven areas and then assigns a single overall rating. For more information on these levels, please refer to Certicom's application note: Certicom Security for Government Suppliers, available at http://www.certicom.com/fips.

To receive FIPS 140-2 validation, a cryptographic module must:

- **Have a well-defined crypto boundary so that all sensitive security information remains within the cryptographic core of the product**

- **Use at least one FIPS-approved algorithm with correct implementation and an intact crypto boundary**

The process for validating either an algorithm or a FIPS 140-2 cryptographic module is outlined in Figure 1. The FIPS module must be validated through the Cryptographic Module Validation

Program (CMVP), also operated by NIST. At least one algorithm within a module must be validated by the CAVP prior to entering the FIPS 140-2 Validation process through the CMVP. All of the tests under CMVP are handled by one of nine CMT labs that are accredited under the National Voluntary Laboratory Accreditation Program (NVLAP).

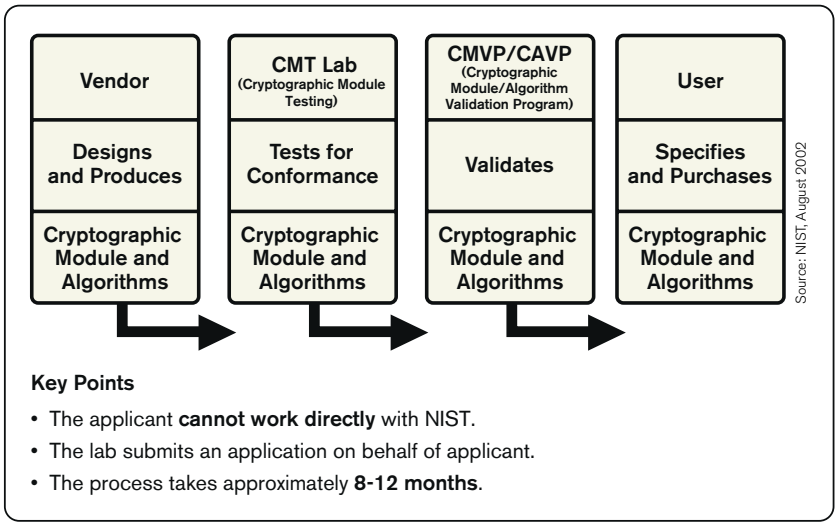

Figure 1: *The FIPS 140-2 Validation Process*

Market Entry Barriers and Issues

While the government market is attractive and lucrative, the FIPS validation process represents a significant barrier to entry.

In the first place, the validation process itself takes 8-12 months and can require multiple developers to complete. Secondly, the cost of validating a cryptographic module is quite high. In addition to development expenses, the cost to submit a module for validation ranges between $50,000 and $100,000.

Once a product is validated, you will require in-house security expertise to monitor the constantly evolving FIPS standards, and make any changes required to maintain validation. For example, the FIPS 140-2 standard is updated every 5 years. New algorithms are constantly being added to improve the standard and make it more robust.

Validation is platform specific: individual validation certificate numbers are required for each platform. Moreover, any changes or additions to a validated product require revalidation, incurring additional costs.

Finally, building to the FIPS 140-2 standard is complex. According to NIST, 48% of cryptographic modules submitted by new applicants and 20% of returning applicant modules contain security flaws. A full 30% of algorithms tested by NIST do not conform to the FIPS standard[2]. This implies that you can spend time and money developing a solution that requires FIPS validation for the government market, submit it to a testing process that can take up to a year, and afterwards learn that your solution is flawed and cannot be FIPS validated without further improvements.

The other option is to incorporate a pre-validated cryptographic module within your product. This allows you to bypass the validation process costs and time, yet still claim FIPS 140-2 Inside. The following considerations will ensure you make the right choice:

Extensible architecture: A platform that offers a common API to write to makes it easier to change out cryptographic software providers and support other protocols with minimal code re-writes.

Update flexibility: Using a pre-validated module allows you to make changes to your product or solution and maintain FIPS validation by re-using the same module for security. As the standard evolves, the vendor is the one who monitors and makes the changes to the module, so all you have to do is switch it out to maintain validation.

Platform flexibility: If you need the flexibility of having FIPS 140-2 Validation for multiple operating system platforms, the ideal security level for the pre-validated module is FIPS 140-2 security level 1. At FIPS 140-2 security level 2, you become restricted to the platforms that are approved according to Common Criteria.

Wired vs. wireless use: There are modules that exist that have been optimized for constrained environments. Using one of these ensures that you will avoid issues with footprint and bandwidth requirements.

Given the barriers and the benefits, the question is raised: how can you as a government supplier find a reliable FIPS implementation that will enable you to get to market quickly with the least amount of risk?

The answer is the *Certicom Security Architecture for Government*. This solution enables device manufacturers and independent software vendors to reach the government market with solutions that offer built-in security that meets stringent government security standards, without impacting time-to market, product margins or product lifecycle costs.

[2] NIST survey of accredited FIPS laboratories.

The Evolution of Cryptography in Government and the Benefits of ECC

Before going into detail on the Certicom Security Architecture for Government, it is important to take a look at the evolution of cryptography within the government because it provides a view into the importance of some of the supported algorithms.

The security industry is slow to adopt new technologies, mainly because every component of a security system needs to be tested and validated by standards and the industry to ensure that it can last the test of time.

In the last few years, there has been a shift away from one encryption standard, DES—to another—AES. DES and its successor 3DES have been used as the de facto encryption method for the past 20 years but now they are proving to be too weak for today's technology. Since NIST selected AES as the replacement for DES in 2000, AES has also made inroads into the financial community and large enterprises.

Currently, NIST is mandating that AES be matched in strength by public key algorithms. At recommended key sizes for government applications however, traditional public key systems such as RSA cannot provide the performance required because the required key size is too large.

CRYPTOGRAPHIC STRENGTH	KEY SIZE RATIO	HASH ALGORITHM	ELLIPTIC CURVE ASYMMETRIC ALGORITHMS	RSA/DSA/DH ASYMMETRIC ALGORITHMS	EXPECTED LIFETIME EXPIRY
56 bits	DES	–	–	–	expired
80 bits	3DES (2 key)	SHA-1	160 bits	1024 bits	2010
112 bits	3DES (3 key)	SHA-224	224 bits	2048 bits	2030
128 bits *	AES-128	SHA-256	256 bits	3072 bits	2031+
192 bits	AES-192	SHA-384	384 bits	7680 bits	2031+
256 bits *	AES-256	SHA-512	512 bits	15360 bits	2031+

guidelines for public key sizes for AES – supplied by NIST
* 128 bit is commercial strength and 256 bit is for classified information

Figure 2: *Public Key Size Comparisons for AES*

The main advantage of Elliptic Curve Cryptography, or ECC, is key size. ECC keys scale linearly with AES, so the equivalent key sizes are smaller and more suited to environments where performance, battery life, memory, and/or bandwidth are issues.

There are many signs that ECC stands to experience the same type of adoption rates as DES and AES. In October 2003, the NSA purchased extensive licensing rights to Certicom's ECC-based intellectual property, paving the way for ECC to become a crucial technology for protecting national security information.

In fact the NSA has declared that "the next generation cryptography to protect US Government information will use elliptic curve cryptography,"[3] and NSA-approved products must use ECC. ECMQV itself is specified in Special Publication 800-56. Although they are not binding the same way a FIPS publication is, documentation in a Special Publication is a key step on the road to being incorporated into a FIPS.

In addition, ECDSA, which is in wide use in the postal and financial industries because of its ability to enable thousands of transactions to be signed every minute, has just been awarded FIPS Validated status. This means that vendors who use an ECDSA implementation with a certificate number can rest assured that that implementation has been verified by a third party.

[3] IETF Security Area Advisory Group presentation, Nov 2004

The Certicom Security Architecture for Government

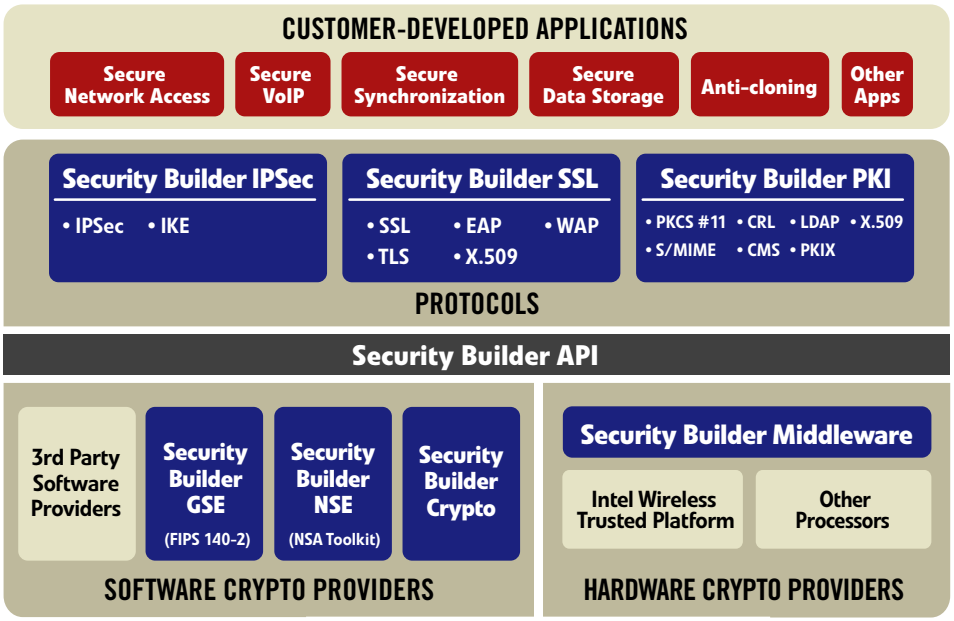

Figure 3

The *Certicom Security Architecture for Government* enables companies to quickly and cost-effectively access the government market with a platform that can be used to develop solutions which meet government security standards, including FIPS 140-2 and ECC.

It includes:

- **software cryptographic providers**
  - **Security Builder® GSE™** *FIPS 140-2 Validated cryptographic toolkit*
  - **Security Builder® NSE™** *cryptographic toolkit for national security information*
  - **Security Builder® Crypto™** *cross-platform cryptographic toolkit*
- **a modular set of security protocol toolkits**
  - **Security Builder® IPSec™** *client-side virtual private network toolkit*
  - **Security Builder® PKI™** *digital certificate management toolkit*
  - **Security Builder® SSL™** *complete Secure Sockets Layer security protocol toolkit*
- **a hardware abstraction layer that has been optimized for a specific chipset**
  - **Security Builder® Middleware™**

All components of the Certicom Security Architecture for Government are unified by a single common API, Security Builder® API™, that sits between the protocols and cryptographic providers, and enables developers to quickly migrate their applications to whichever cryptographic module is required.

certicom™

The Components of Certicom Security Architecture for Government

Security Builder API

The foundation of the Certicom Security Architecture is the Security Builder API. It provides the means by which applications access various Certicom-supported cryptographic providers. The API enables the seamless addition of defined cryptographic support from different cryptographic providers to an application. A cryptographic provider could be a software toolkit, such as Security Builder GSE, or a piece of hardware. Security Builder API abstracts away the differences among cryptographic providers without requiring code changes. This means that as a developer, you can easily migrate your application to a different cryptographic provider without having to recode your entire application. As requirements change in the government market, this provides an easy bridge to meet future requirements.

Software Cryptographic Providers

Security Builder GSE

Security Builder GSE is a FIPS 140-2 Validated cryptographic module that is available for leading client and server side platforms, enabling end-to-end security. Validated platforms include: AIX, HP-UX, Palm, Red Hat Linux, Sun Solaris, Windows 98, Windows CE and Windows 2003[4].

Using Security Builder GSE as the software cryptographic provider within the Certicom Security Architecture for Government allows vendors to run Security Builder SSL, Security Builder PKI and Security Builder IPSec in FIPS approved mode of operation.This expands the possible applications where a FIPS module can be easily incorporated. In fact, any protocol that uses a FIPS Approved Algorithm Implementation can run in FIPS Approved mode when using a FIPS 140-2 cryptographic module such as Security Builder GSE as its core cryptographic provider. This means as new protocols are introduced, the Certicom Security Architecture will be able to support them, as long as they use FIPS Approved Algorithm Implementations.

Security Builder NSE

Security Builder NSE enables organizations to quickly build applications that meet the field-of-use guidelines set out by the National Security Agency (NSA) to protect mission-critical national security information. The Security Builder NSE toolkit covers the technology that was part of the 26 patents licensed by the NSA from Certicom plus optimized implementations. It also includes support for ECC-based algorithms such as ECDSA, ECMQV and EC support for S/MIME, TLS and IKE.

[4] Windows 98/Windows CE certificate # 316, Palm Certificate #351, all other platforms pending. For more information, visit: http://csrc.nist.gov/cryptval/140PreVal.pdf.

certicom™

Security Builder Crypto

Security Builder Crypto offers highly efficient implementations of the most widely used cryptographic operations. It is available on more than 30 different platforms and provides a complete suite of cryptographic algorithms for developers to easily integrate encryption, digital signatures, and other security mechanisms into applications.

Hardware Abstraction Layer

Security Builder Middleware

Security Builder Middleware is a hardware abstraction layer that links Security Builder API, and thereby all security services, to a specific hardware cryptographic provider. It wraps the cryptographic features given by the hardware cryptographic provider in a series of registration functions. Applications call one or more registration functions in Security Builder Middleware to link in the cryptographic features from the cryptographic provider.

Protocol Toolkits

CSA also provides toolkits for higher level protocols. These protocols can operate in FIPS approved mode of operation when Security Builder GSE is used as the software cryptographic provider.

Security Builder IPSec

Security Builder IPSec, a client-side virtual private network toolkit, enables developers to easily embed standards-based network access onto constrained devices. With the smallest code size and widest support for all industry-leading VPN gateways, Security Builder IPSec provides efficient security and enables better performance than is normally achievable with traditional IPSec implementations.

Security Builder PKI

Security Builder PKI is a comprehensive digital certificate management toolkit capable of adding robust PKI security to applications. It supports CMS for the development of S/MIME applications, interoperates with third-party PKIs and CAs, and complies with the following industry-standards: IETF-PKIX, PKCS, ANSI, and ISO. PKCS #11, included in Security Builder PKI, provides hardware security module support for the entire Certicom Security Architecture.

Security Builder SSL

Security Builder SSL is a complete Secure Sockets Layer protocol toolkit for enabling secure and efficient SSL/TLS transmission of data. The toolkit provides security support for public and symmetric key algorithms including ECC and supports the following protocols: SSL 2.0, SSL 3.0, TLS 1.0, WAP 2.0, EAP-TLS, EAP-TTLS, EAP-PEAP.

certicom™

Certicom Professional Services

In addition to providing the tools you need to add comprehensive security to your mobile platforms, Certicom also shares the benefits of nearly 20 years experience in designing security for constrained environments through Certicom Professional Services. In addition to offering general information security and cryptographic services, Certicom Professional Services provides a range of offerings specifically tailored to the requirements of government suppliers, including: FIPS 140-2 platform development and porting, custom security solutions and ECC/MQV consulting. Certicom Professional Services help developers achieve the optimal balance among features, performance and investment.

The Value of the Certicom Security Architecture for Government

The Certicom Security Architecture for Government provides device manufacturers and independent software vendors a number of advantages:

Comprehensive security platform that meets stringent government requirements

The *Certicom Security Architecture for Government* is a robust, feature-rich solution that allows you to meet both client and server-side security requirements needed to access the government market. It includes all the tools to embed FIPS 140-2 Validated cryptography, as well as meet NSA field-of-use guidelines—and specifically requirements for ECC—for mission critical information.

Flexibility and portability

The *Certicom Security Architecture for Government* is available on more than 10 FIPS Validated platforms and can be quickly ported to new platforms thanks to its modular approach. Through standards based PKCS #11 support, The Certicom Security Architecture for Government also supports a wide range of hardware cryptographic providers, including Eracom protectOrange and SafeNet Luna cards. The common API among toolkits also allows you to easily switch cryptographic providers.

Lower total cost of development and improved time-to-market

Certicom handles the expensive and time-intensive FIPS 140-2 Validation process for you and provides updates and upgrades to customers as government requirements change. We monitor the standards to ensure compliance so you can focus on your core competencies. Certicom is committed to updating all FIPS Validations when new features and functionality are added to Security Builder GSE.

Optimized for size and performance

With all applications sharing a common security code base, the Certicom Security Architecture for Government helps ensure the smallest possible security footprint. The client-side implementation of Security Builder GSE is optimized for embedded platforms and requires less than 150 KB, ensuring that you can conserve valuable space and still deliver strong security without impacting network or user experience. Where memory space is not as constrained, the Certicom Security Architecture for Government can be optimized for faster performance.

Bridge to ECC: the choice for government cryptography

Partner with the company that has the most experience implementing ECC, the algorithm that is quickly becoming the choice for government cryptographic requirements. In October 2003, The National Security Agency (NSA) purchased extensive licensing rights to Certicom's ECC-based intellectual property, for the purpose of protecting mission-critical national security information. The US Government views ECMQV as a major component of key management. Certicom was also awarded Certificate #1 for the first FIPS-validated implementation of ECDSA.

Using the Certicom Security Architecture for Government

The following section describes some scenarios where the *Certicom Security Architecture for Government* can be used.

Secure key storage using hardware security modules

FIPS 140-2 enumerates four distinct levels of security, each incrementally more rigorous than the one preceding it. From Level 2 upward, FIPS 140-2 requires security solutions to have a physical component: i.e. to protect elements such as transaction-signing keys in a tamper-resistant hardware module. In any situation where the trusted keys used to sign transactions, files or documents are required to be protected in hardware security modules (HSMs).

Security Builder PKI, a digital certificate management toolkit, supports PKCS #11/Cryptoki to accommodate hardware-based security. By writing to the Security Builder API within the Certicom Security Architecture for Government, developers can expose PKCS #11 for use with other protocols such as SSL and IPSec.

Digital Passports

By the end of 2005, new U.S. passports will include a microprocessor chip that will be readable without contact with a reader through an RF connection. Driven by mandates from its member governments, ICAO (International Civil Aviation Organization) has issued a set of security standards by which the data in this chip can be verified and protected by the use of digital signatures.

The Certicom Security Architecture for Government provides compact code for these digital signature algorithms, including ECDSA, and a programming architecture to make use of them. Writing applications to Security Builder API within the Certicom Security Architecture simplifies the development of secure applications and ensures that the cryptographic operations are properly executed and compactly written.

Federal ID Smartcards

Homeland Security Presidential Directive 12, issued August 12, 2004, mandates the implementation of a secure ID standard that provides the direction for the next iteration of government employee ID cards. These cards will be issued with digital certificates validated by a digital signature. The ID card will generate a signature in response to a challenge to enable an authorized employee to:

- **gain physical access to government facilities**
- **log in to government computing networks**
- **sign transactions within government databases**

Within the Certicom Security Architecture for Government, the Security Builder PKI toolkit includes all the optimized cryptography to generate and validate these signatures within the constrained environment.

In addition to fast and easy implementation of the Federal ID standards, Security Builder NSE offers elliptic curve algorithms recommended by NSA directives. This includes elliptic curve MQV, a key-agreement scheme referenced in NIST Special Publication 800-56 that can make use of the private key stored on the ID card to enable secure communications.

certicom™

Conclusion

The *Certicom Security Architecture for Government* provides real competitive advantages to government suppliers—from reduced time-to-market and costs to increased flexibility and the opportunity to offer products that meet stringent government security requirements on a number of platforms. It provides an end-to-end offering for solutions which require FIPS 140-2 Validation on both the client and the server-side.

Customers such as Bluefire Security, LRW Digital and Synchrologic have already benefited from implementing Certicom technology into their applications.

By choosing the *Certicom Security Architecture for Government*, you can ensure that your products will meet government security requirements now and well into the future.

About Certicom

Certicom Corp. (TSX:CIC) is the authority for strong, efficient cryptography required by software vendors and device manufacturers to embed security in their products. Adopted by the US Government's National Security Agency (NSA), Certicom technologies for Elliptic Curve Cryptography (ECC) provide the most security per bit of any known public key scheme, making it ideal for constrained environments.

certicom™

Certicom White Papers

To read other Certicom white papers, visit www.certicom.com/whitepapers.

The Inside Story

Many Happy Returns: The ROI of Embedded Security

Wireless Security Inside Out (authored by Texas Instruments and Certicom)

Welcome to the Real World: Embedded Security in Action

Sum Total: Determining the True Cost of Security

The Elliptic Curve Cryptosystem for Smart Cards

Elliptic Curve DSA (ECDSA): An Enhanced DSA

Formal Security Proofs for a Signature Scheme with Partial Message Recovery

Postal Revenue Collection in the Digital Age

An Elliptic Curve Cryptography Primer

ECC in Action: Real World Applications of Elliptic Curve Cryptography

Using ECC for Enhanced Embedded Security: Financial Advantages of ECC over RSA or Diffie-Hellman

Good Things Come in Small Packages: Certicom Security Architecture for Mobility

certicom™

Contact Certicom

Corporate Headquarters

5520 Explorer Drive
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
Herndon, Virginia 20190
Tel: 703-234-2357
Fax: 703-234-2356
E-mail: sales@certicom.com

Canada

5520 Explorer Drive
Mississauga, Ontario
L4W 5L1
Tel: 905-507-4220
Fax: 905-507-4230
E-mail: info@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

1810 Gateway Drive, Suite 220
San Mateo, 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

www.certicom.com