CERTICOM WHITEPAPER SERIES

Making the Grade

MEETING GOVERNMENT SECURITY REQUIREMENTS — SUITE B

December 2010

certicom™

certicom™

Table of Contents

Introduction **3**

Part I: Setting the Terms **5**

Why ECC? 5

ECC and the NSA 6

Part II: Keys and Signatures **7**

Bits and pieces 7

Digital Signatures 8

Part III: ECC Applied **9**

Wireless Communications 9

Voice Over IP 9

Smart Cards 10

Machine Readable Travel Documents 11

Air Traffic Control 12

The Commercial Relevance of Suite B **12**

Final Thoughts **13**

About Certicom **13**

Additional Certicom White Papers **14**

certicom™

Introduction

From a security standpoint, the expectations of public-sector technology buyers are both stringent and clear, spelled out in the terms of rigorous standards such as FIPS, the United States Federal Information Processing Standard.

The challenging part for vendors is formulating the right response to those expectations—'right' meaning one that both complements their existing technology solutions and at the same time satisfies government requirements to the letter.

This white paper concentrates on a particular case in point: the selection, by the US National Security Agency (NSA), of elliptic curve cryptography (ECC) to protect classified and unclassified information. The class of cryptographic algorithms discussed is:

- **Suite B:** cryptographic algorithms for protecting classified and sensitive but unclassified information. The list of Suite B algorithms was announced by the NSA at the RSA 2005 conference and later updated as follows:

	Algorithm	Unclassified	Classified
Encryption	AES	128-bit key	256-bit key
Signatures	ECDSA	256-bit curve*	384-bit curve**
Key Exchange	ECDH or ECMQV	256-bit curve	384-bit curve
Hash	SHA	SHA-256	SHA-384

*The 256-bit curve is the NIST curve with a 256-bit prime modulus
**The 384-bit curve is the NIST curve with a 384-bit prime modulus

The protocols included in Suite B are Elliptic Curve Diffie-Hellman (ECDH) for key transport and agreement; the Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signatures; the Advanced Encryption Standard (AES) for symmetric encryption; and the Secure Hashing Algorithm (SHA). All support the NSA's strategic approach to achieving what it terms 'information assurance', encompassing confidentiality, integrity, availability, authenticity and non-repudiation. It is important to note that the RSA algorithm is not included in Suite B.[1]

Important!

This paper presumes a basic knowledge among readers of symmetric and asymmetric (i.e. public key) cryptography, and particularly of ECC. For further information on these subjects, we refer you to our other white papers, specifically: *ECC in Action* and *An Elliptic Curve Cryptography Primer.*

Go to www.certicom.com/whitepapers

Another excellent resource is our FAQ: *The National Security Agency's ECC License Agreement with Certicom Corp.*

[1] See the NSA Suite B web site at www.nsa.gov/ia/programs/suiteb_cryptography/

Vendors who want to sell into government must therefore have a firm grasp on ECC-based algorithms: what they are, how they work, and why they are important. That is the object of this paper: to equip technology vendors with a working knowledge of ECC, its protocols and their applications, enabling developers to integrate ECC into products destined for government-sector use.

It is also important at this stage to point out that Suite B is not just for government use. As with other technologies in the past, the US Government has led the way in what it considers adequate for secure communications. Many corporations also have sensitive intellectual property online and/or electronically process sensitive information. Suite B algorithms are also appropriate in these types of situations.

It is a clear indication that the state of cryptanalysis has advanced to where traditional commercial practice is inadequate for highly sensitive commercial information. For commercial companies to maintain their competitive edge, they, too, should be thinking about using Suite B cipher suites.

certicom™

Part I: Setting the Terms

The NSA licensed patents related to ECC from Certicom Corp. in 2003 to secure classified information; they announced Suite B requirements in 2005. Generally speaking, we believe, what appealed to the NSA about ECC was its strong security, efficiency and scalability over conventional public-key cryptography algorithms. We believe these benefits of ECC were very important to the NSA as it chooses its security for use over several decades in its crypto hardware. It is important to note, at this point, that the NSA only licensed some of Certicom's patents and that Certicom has many more patents and ECC toolkits that are also useful for implementing Suite B algorithms efficiently.

The technologies included under the NSA's ECC licensing agreement include those designed for:

- federal, state or local government agencies to protect classified or mission-critical national security information or information under 10 USC 2315; and
- foreign government agencies: a) to protect classified or mission-critical national security information where interoperability with US entities is a possibility; or b) to protect classified or mission-critical national security information that originated with the US federal, state or local government.

These are broad categories, and the significance of that breadth is that a great many vendors—selling to clients both within the US and outside of it—will have to build ECC into the security components of their offerings[2]. The NSA also licensed several patents that covered mathematical techniques that are crucial to the security of ECC-based protocols. One of these techniques provides resistance to the very dangerous 'small subgroup attacks'. The other uses 'public key validation' to ensure resistance to a variety of attacks including the 'invalid-curve attacks'.

Why ECC?

The selection of ECC on the public-key crypto side of things is tied in with the designation of AES, the Advanced Encryption Standard, as the ideal algorithm for symmetric-key cryptography within the US Federal Government. (AES received this status from NIST, the National Institute for Standards in Technology, under FIPS 197.)

AES is excellent for symmetric cryptography: it's fast, it's strong and it's scalable. In any security system that employs both symmetric and public-key cryptography, the public-key algorithm has to match these qualities of AES. Of all the algorithms available today, only ECC has shown itself to be up to the task.

[2] It should be mentioned that the NSA and other government agencies may also require the use of certain classified algorithms as well.

Capable of providing 128-bit security with a small key size, ECC scales perfectly with AES—and, in fact, provides a superior alternative in the public-key domain. It has shown itself to be an excellent solution for exchanging keys in a public-key system, and for creating digital signatures.

Other options such as RSA and DSA/DH do not match ECC's ability to scale linearly with AES. For instance, ECC requires a key size of just 256 bits to match 128-bit AES security; RSA, on the other hand, must generate a sizable 3072-bit public key. NESSIE—the New European Schemes for Signatures, Integrity and Encryption—recommends an RSA key size of 6000 bits to match the strength of AES 128. Such a key would obviously be unsupportable for many computer systems, particularly those involving constrained devices. Again, this is probably one of the key reasons that the RSA algorithm is not included in Suite B.

ECC and the NSA

The NSA's use of ECC in Suite B pertains to elliptic curves over **GF(p)**, where **p** is a prime number greater than 2^{255}. This refers to the finite field over which the elliptic curve is defined.

There are two kinds of finite fields that are widely standardized: binary fields and, as the NSA has chosen, prime fields. They are both equally secure. Prime fields lend themselves to faster implementations on platforms with fast integer multiplication, such as Pentium computers. Binary fields are extremely efficient when implemented in silicon.

The NSA's Suite B use of ECC applies to all of the following functions:

- Key agreement
- Key transport
- Digital signatures

For key agreement and key transport, ECDH is the designated protocol; for digital signatures, ECDSA has been approved. Here we come to the heart of our paper—a closer examination of how these work.

certicom™

Part II: Keys and Signatures

Key establishment involves the use of cryptographic algorithms to generate and exchange keying material. When they are sound, these functions are performed so that third parties eavesdropping on an information exchange cannot acquire the keys—deliberately or inadvertently.

Specifically, key establishment is the process for establishing a shared secret key via either a key agreement or key transport scheme. In a key agreement scheme, all parties contribute information that allows the others involved in the exchange to derive shared keying material. In key transport, one party determines the keying material, which is then encrypted and transported to the intended receivers.[2]

The American National Standards Institute (ANSI) and NIST are each in the process of producing standards and recommendations for key establishment. NIST Special Publications 800-56 and 800-57 outline approaches, respectively, for key establishment and key management. Today, security products intended for government use require FIPS 140-2 validated modules with an approved key establishment method.

Bits and pieces

Key establishment involves the use of primitives—cryptographic building blocks that facilitate the implementation of more complicated schemes. NIST demands that all key-establishment schemes incorporate a primitive based on either the Diffie-Hellman (DH) algorithm.

Choosing an algorithm creates other, related decision points. There are two ways to compute DH in accordance with ANSI: using a discrete-log cryptosystem (DLC) over a finite field (ANSI X9.42); or using ECC (ANSI X9.63).

Yet one must be careful: these choices are not equivalent. Using a DLC over a finite field, for example, requires extremely large keys to match the strength of AES—as large as 15,000 bits to measure up to 256-bit AES. And 15,000 bits is hardly economic in terms of processing resources. This further demonstrates why the NSA's Suite B algorithms include only the ECC versions not the DLC versions.

Elliptic Curve Diffie-Hellman (ECDH) is faster than Diffie-Hellman over a finite field, offering the performance and security advantages of ECC.

[2] Public-key encryption schemes can be transformed into key-transport schemes using an approved key-wrapping method recommended in NIST SP 800-56. An example is S/MIME, where public-key encryption is combined with key wrapping to achieve the effect of key transport. This permits the efficient encryption of large emails to multiple recipients.

Digital Signatures

Digital signatures are special bitstrings that are generated using a specific message or piece of information and a user's private key.

While digital signatures can only be generated uniquely—by an individual user with his or her private key—anyone who has a copy of the originator's public key can verify that the signature is authentic: that the message in question originated where it purports to have originated, and that it has not been interfered with in transmission. In these ways, digital signatures can be used to ensure integrity and non-repudiation: to prove that a particular piece of information has not been tampered with, and that a specific transaction or information exchange did indeed occur.

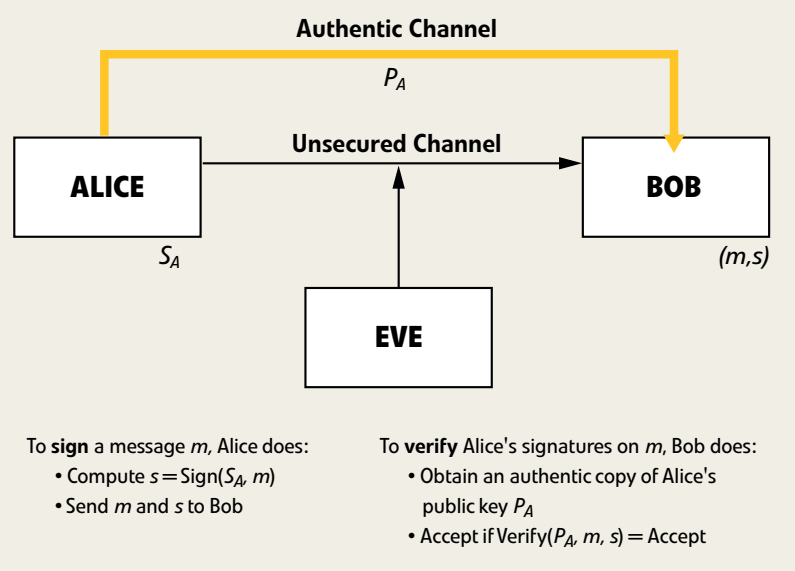

Figure 1: *Digital Signatures*

ECDSA, the Elliptic Curve Digital Signature Algorithm, was standardized through ANSI (X9.62) in 1999, and also standardized in IEEE in 1363-2000. Secure and flexible, it can be calculated using elliptic curves over prime or binary fields. It has also been recommended for US Federal Government use under FIPS 186-2. (See Figure 2 for a comparison of the speed of ECDSA and RSA operations at similar strengths.)

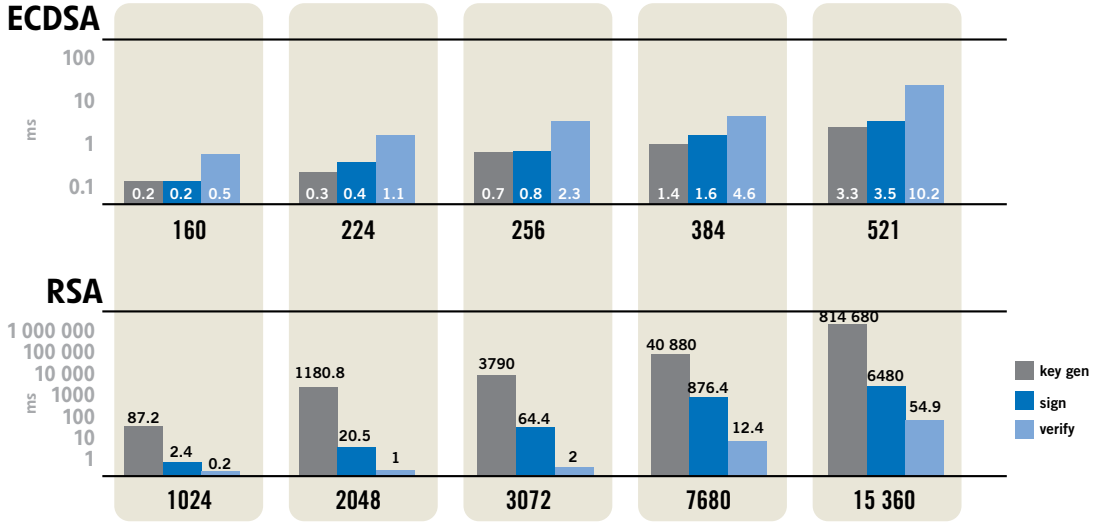

Figure 2: *Comparing the speed of ECDSA and RSA operations at similar strengths.*[3]

Part III: ECC Applied

There is an almost limitless variety of possible applications for ECC in the government context—applications in which key agreement, key transport and digital signing play crucial roles.

Wireless Communications

ECC is particularly well suited to handling key agreement for wireless communications in situations where security is at a premium and resources are at a minimum—for example, enabling secure broadband connectivity at temporary military camps where it is impractical to install a hardwire infrastructure.

In such settings, base stations and their corresponding clients typically consist of compact, constrained devices. Power conservation is a concern—and to accommodate true roaming capabilities, quick handoffs between base stations are necessary. At the same time, those connections have to be secure.

Voice Over IP

ECC has applications for government users outside of field scenarios, of course. Voice over IP is one example. There are cost advantages—and operational flexibilities—to be gained through the use of VoIP in place of traditional circuit-switched telephone lines. But since VoIP traffic moves through packet-switched networks, it raises a whole set of security concerns not associated with conventional phone services. VPNs have been looked to as a solution, but secure VPN connections are cryptographic, requiring asymmetric authentication and key establishment methods in the initial phases of each connection. For VoIP this presents a challenge, due to the number of connections that might be established in the course of just a single call.

[3] The performance was measured on: Intel Pentium 4 with a 3GHz Processor.

ECC allows communicating parties to authenticate to one another and establish session keys quickly—greatly reducing time, bandwidth demands, and processor time demands.

Smart Cards

There is a great deal of public-sector interest in the adoption of multipurpose Personal Identity Verification (PIV) smart cards. Federal ID Smartcards Homeland Security Presidential Directive 12 mandates the implementation of a secure ID standard providing direction for the next iteration of government employee ID cards. These cards will be issued with digital certificates validated by a digital signature. Validation of the signature will permit authorized employees to:

- gain physical access to government facilities;
- log in to government computing networks; and
- sign transactions within government databases.

Conceivably, a PIV card containing a user's public and private key pairs would enable individuals to sign documents and forms electronically—even emails—providing irrefutable confirmation that a message originated with a given sender.

If a conventional algorithm is used—RSA being the most obvious example but not an algorithm recommended by the NSA—then the card itself must add on an RSA co-processor to support the associated performance demands. ECDSA, on the other hand, can be computed using just the CPU. And if an ECC co-processor is built in, it will typically accelerate the signing function considerably over the RSA alternative.

Several interrelated specifications for PIV cards were released in the winter of 2005. FIPS 201 specifies aspects of existing administrative procedures and technical specifications that are expected to change with implementation and use of the standard. NIST Special Publication 800-73, Integrated Circuit Card for Personal Identity Verification specifies the interface and data elements of PIV cards themselves. NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification, specifies technical acquisition and formatting requirements for biometric data, while NIST Special Publication 800-78, Recommendations for Cryptographic Algorithms and Key Sizes specifies acceptable cryptographic algorithms and key sizes for the PIV system.

ECC is indicated as an acceptable cryptographic algorithm for authentication, digital signing and key management under NIST 800-78—ECDSA in the first two instances, and ECDH or ECMQV in the latter. (The key-size advantages of ECC are clear in the specification itself: whereas an RSA key of 1024, 2048, or 3072 bits is called for to meet card-authentication requirements, the equivalent ECC key range is 163 to 283 bits.[4])

[4] *NIST Special Publication 800-78, First Public Draft,* Cryptographic Algorithms and Key Sizes for Personal Identity Verification

Machine Readable Travel Documents

Digital signatures can also be used to secure Machine Readable Travel Documents—in various ways. In the near future, for example, new US electronic passports will include a microprocessor chip that will be readable without contact with a reader through an RF connection. The ICAO (International Civil Aviation Organization) has outlined a set of security standards by which the data in this chip can be verified and protected by the use of digital signatures, and ECDSA conforms to those standards.

Even without a built-in chip, electronic passport security can be strengthened using ECDSA through the inclusion of a digital signature printed in barcode format. The signature would confirm authoritatively that the electronic passport is legitimate and linked directly to the bearer. Any discrepancy would be a sign of possible fraud.

Obviously, the amount of space available for this bar code is minimal. A compact and scalable algorithm like ECDSA creates a two-dimensional barcode that fits nicely, containing anywhere from 20 to 40 bytes of information. By comparison, an equivalent RSA signature would generate a barcode of 128 bytes—and overwrite other regions on the electronic passport.

This same principle is being applied today to postage marks as a fraud-prevention measure: printed barcodes on letter mail and parcels verify that the postage applied by a particular postage meter is valid and authentic.

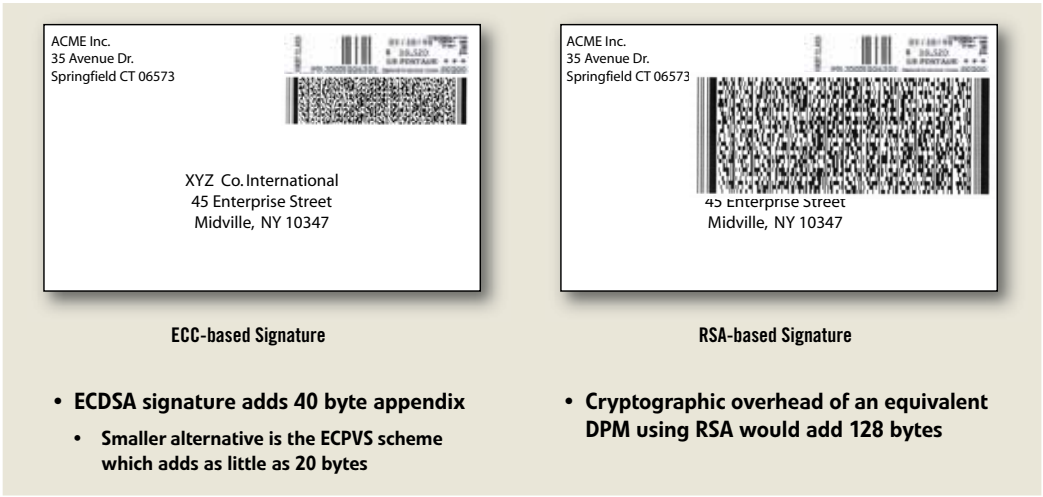

Figure 4: *ECC: ROI for Digital Postage Marks*

Electronic visas may also follow this same development and would benefit from the standards being developed today. ECDSA could even be used to sign digital photographs in such a way that the photograph can be proven to be unaltered. For forensic purposes, this could be invaluable: a photograph or recording could be admitted as evidence in a hearing with the assurance that it has not been tampered with or modified in any way.

Similarly, but on a less sensitive scale, applying a digital signature to a movie or sports ticket, or a subway or bus access card would make any copy or altered version easily detectable—and invalid.

Air Traffic Control

Machine Readable Travel Document security is essential to ensuring public safety, particularly where air travel is concerned. So too, of course, is securing the information exchanges between aircraft and control towers. Any interference with or corruption of data transmitted between planes in the air and controllers on the ground could have devastating and tragic consequences.

The ICAO and the US Federal Aviation Administration are intent upon mitigating the risk of such events through development of the Aeronautical Telecommunications Network (ATN): a next-generation data-link network. Using ECDSA to sign communications and confirm their authenticity, the ATN provides a reliable, trusted and bandwidth-constrained connection between controllers and aircraft.

The Commercial Relevance of Suite B

In addition to its influence on government procurement, Suite B is relevant to other industries because it highlights the fact that the typical commercial practice of using either 1024-bit or 2048-bit RSA or Diffie-Hellman with AES-128 leaves systems with a security weakness.

In the coming years, cryptographic mismatches such as these will come under increasing scrutiny by financial regulators and Sarbanes Oxley and HIPAA compliance auditors, among others. As such, Suite B will indirectly establish the level of due care a commercial company must use when protecting sensitive information such as financial data or health records.

Suite B's market impact will extend even further as corporate CxOs come to realize that their intellectual property is currently protected by weaker algorithms than what the government has specified for their sensitive information. As all the recent news about lost and stolen corporate information shows, no company wants private data concerning its employees or customers, pre-public release financial data, or product IP to be made public. Executives will be quick to point out that their information is easily the equivalent of SBU. As a result, companies with significant intellectual property, such as semiconductor manufacturers, pharmaceutical companies, and high technology product manufacturers, will require their cryptographic solutions implement at least Suite B algorithms.

Final Thoughts

Ultimately, the importance of Suite B comes down to compliance: compliance with standards for security; compliance with expectations of performance. Understanding the development choices available within agencies' frameworks of requirements is essential; applying them inventively is the key to competitive advantage. ECDH for key agreement and ECDSA for digital signatures both afford significant advantages in terms of security, compactness, scalability and future-readiness. And where technologies relating to national security are concerned—under NSA's Suite B—these protocols are indispensable.

About Certicom

Certicom, a wholly owned subsidiary of Research In Motion Limited (RIM) (Nasdaq: RIMM; TSX: RIM), manages and protects the value of content, applications and devices with government-approved security. Adopted by the National Security Agency (NSA) for government communications, Elliptic Curve Cryptography (ECC) provides the most security per bit of any known public-key scheme. As the global leader in ECC, Certicom's security offerings are currently licensed to hundreds of multinational technology companies, including IBM, General Dynamics, Motorola and Oracle. Founded in 1985, Certicom's corporate office is located in Mississauga, Ontario, Canada with worldwide sales offices in USA and Asia. Visit www.certicom.com.

USA
3600 Glen Canyon Rd., Suite 1
Scotts Valley, CA 95066
USA
Tel: 1.831.438.4100
Fax: 1.831.438.4111
Sales: 1.800.561.6100
sales@certicom.com

Corporate Headquarters
5520 Explorer Drive, 4th Floor
Mississauga, ON L4W 5L1
Canada
Tel: 1.905.507.4220
Toll Free: 1.800.561.6100
(NA only)
info@certicom.com

Japan
Research In Motion Japan Ltd.
Nippon Brunswick, Building 7F
5-27-7 Sendagaya,Shibuya-ku,
Tokyo 151-0051, Japan
Tel: 03 6367 3567
sales@certicom.com

certicom™

Additional Certicom White Papers

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

Sum Total: Determining the True Cost of Security
Sourcing Security: Five Arguments in Favour of Commercial Security Solutions

Government

Making the Grade: Meeting Government Security Requirements (Suite B)
Meeting Government Security Requirements: The Difference Between Selling to the Government and Not
FAQ: The National Security Agency's ECC License Agreement with Certicom Corp.

Mobility

The Inside Story
Many Happy Returns: The ROI of Embedded Security
Welcome to the Real World: Embedded Security in Action

Sensor Networks

Securing Sensor Networks

DRM & Conditional Access

Injecting Trust to Protect Revenue and Reputation: A Key Injection System for Anti-Cloning, Conditional Access and DRM Schemes
Achieving DRM Robustness: Securing the Device from the Silicon Up to the Application(PDF)

Enterprise Software

Using Digital Signatures to cut down on Bank Fraud Loss

ECC

An Elliptic Curve Cryptography Primer
ECC in Action: Real World Applications of Elliptic Curve Cryptography
Using ECC for Enhanced Embedded Security (PDF)