

FAQ: The National Security Agency's ECC License Agreement with Certicom Corp.

This FAQ is composed of 4 general sections

1. [About the Agreement](#) p. 1
2. [Questions beyond the NSA agreement – “Suite B”](#) p. 5
3. [Questions about Certicom](#) p. 10
4. [Implementation Questions](#) p. 13

ABOUT THE AGREEMENT BETWEEN CERTICOM AND THE NSA

1. What is the NSA agreement?

The US Government's National Security Agency (NSA) purchased licensing rights to Certicom Intellectual Property around Elliptic Curve Cryptography (ECC) protocols. This agreement gives the NSA a non-exclusive, worldwide license, with the right to grant sublicenses, to 26 US patents and applications, and corresponding foreign rights, in a limited field of use. Outside the field of use, Certicom retains all rights to the technology.

2. What patents did they license?

The NSA licensed Certicom protocol patents, security patents and implementation patents. The NSA licensed patents on Elliptic Curve technology related to some of the Suite B algorithms.

3. Why did the NSA license these patents?

We believe there are two main reasons the NSA was interested in these patents. First, ECC is the public key technology that offers the most security per bit. As computing power increases, it becomes easier to break all cryptosystems so cryptographic keys must increase as well. The block cipher, Advanced Encryption Standard (AES), has a scalable key size and ECC scales linearly with AES over time. The RSA (Rivest, Shamir and Adelman) public key protocol does not scale; its key sizes grow exponentially and quickly become too big to be computationally efficient. For example, per the National Institution of Standards and Technologies' (NIST) guidance, AES with a 256-bit key requires a 512-bit ECC key size or a 15,360-bit RSA key size.

Secondly the NSA was interested in the authenticated key agreement protocol, ECMQV, invented by Certicom. ECMQV is an extremely efficient key agreement protocol that inherently provides many security services that are essential to high security, high assurance communications. Today, most people use Diffie-Hellman (DH) key agreement which suffers from the man-in-the-middle attack where as ECMQV does not.

4. Why 26 patents and not Certicom's entire patent portfolio of over 300 patents and patents pending?

The NSA licensed 26 patents because those were the ones that covered the patents around ECMQV for the specific field of use in which they were interested. Since the NSA does not directly implement this technology, they did not license any implementation patents with the exception of one – Point Compression.

Over the years Certicom has discovered many efficient ways of implementing ECC in both hardware and software/firmware. These implementation patents were not licensed by the NSA. In addition, Certicom has patents covering other ECC based schemes such as ECC digital signatures with message recovery and many security patents unrelated to ECC. There was no need to license these patents for the uses that the NSA had envisioned.

5. Did the NSA license only US Patents?

No. The corresponding foreign rights including six Canadian Patents and five European Patents are licensed by the NSA.

6. How do the NSA and Certicom define the Field of Use?

Directly from our agreement with the NSA:

“**Field of Use**” means the technology and methods necessary to implement in either an NSA Approved Product or a product for national security compliant with FIPS 140-2 or its successors the Licensed Patents and Patent Applications with elliptic curves over $GF(p)$ where p is a prime number greater than 2^{255} .

7. What is an “NSA Approved Product?”

Directly from our agreement with the NSA:

“**NSA Approved Product**” means a product that is approved by the NSA for use by either:

1. US Government agencies for protecting classified information, mission critical national security information or for protecting information under 10 USC 2315;
2. State and Local Government agencies for protecting classified information, mission critical national security information or for protecting information under 10 USC 2315; or
3. Foreign Government agencies for protecting classified information or mission critical national security information where interoperability with US entities using an NSA approved product is a possibility or the aforementioned information originated in the US Federal, State or Local Government.

8. What sublicensing rights does the NSA have?

The NSA has the right to grant sublicenses to the 26 licensed patents in the limited field of use defined above.

9. What does the NSA intend to do with the right to sublicense?

We believe the NSA is interested in the proliferation of the technology. To that end, the NSA is granting a royalty free sublicense to manufactures who implement this technology into their products to address the Government's needs. Note that Certicom can grant the exact same rights if the manufacture wishes to obtain the license from the original patent holders. Certicom retains ownership of all 26 patents.

10. What does it mean to have NSA approval?

It means that the product has been evaluated and approved for use by the NSA. The NSA has their own evaluation team in place to validate security implementations primarily for department of defense applications.

11. What does it mean to have FIPS 140-2 approval?

NIST has a well established process to evaluate products that contain cryptography. A company selling products to the US or Canadian Governments for the protection of sensitive but unclassified information must have their products validated through the FIPS 140-2 accredited laboratory.

12. What kind of product can I license this technology for?

As stated in our contract with the NSA, you can license this technology for products that fit the field of use definition "...either an NSA Approved Product or a product for national security compliant with FIPS 140-2 or its successors..."

13. What is excluded from an NSA sublicense?

The field is restricted to $GF(p)$ where p is a prime number greater than 2^{255} .

If you wish to use smaller field size or the binary field $GF(2^m)$ in your products, then these products would be excluded from the sublicense.

Finally, NSA did not license implementation patents with the exception of one – Point Compression. Certicom has a tremendous portfolio of implementation patents for security, performance and efficiency in both hardware and software. Implementers should talk to Certicom about its products and other intellectual property before embarking on a long development cycle.

14. Will this have any affect on foreign equipment manufactures?

Provided foreign equipment manufactures comply with the field of use restrictions, they will be granted a license to the technology from the NSA or Certicom.

15. Will this have any affect on foreign governments?

Foreign governments will be able to take advantage of this license as well. The US Government wishes to communicate with its allies in a highly secure fashion. This technology will be targeted to that end.

16. Why the $GF(p)$ field size?

$GF(p)$ was chosen because it has been well studied over the last 20 years. For national security applications, the NSA would like to see key sizes of at least 256 bits which is why they specify that p is a prime number greater than 2^{255} .

17. Why did the NSA not license the binary field $GF(2^m)$?

The binary field has been well studied over the last 20 years as well and is perfectly secure; however we believe the NSA wanted to limit the implementation choices. The NSA's stated goal is to foster interoperability amongst secure communications equipment used across various government organizations. By limiting the implementation choices, this interoperability is easier to achieve.

18. Did the NSA license any implementation patents?

Yes. The NSA licensed one very popular implementation patent called Point Compression. This is a mathematical technique used to reduce key sizes in transit by 50%. There are a number of other implementation patents that could be used in the field of use for security, performance and efficiency in both hardware and software but these would have to be licensed separately from Certicom.

19. What commercial terms do I get from the NSA?

You get the right to use the 26 patents within the field of use defined above. Currently, the NSA and Certicom offer these rights under a royalty free license.

20. What ownership or technology rights did the NSA pay for?

The NSA does not own any of the 26 patents but has sub-licensing rights to the patents over their lifetime. The NSA has a non-exclusive, worldwide license, with the right to grant sublicenses, to 26 US patents and applications, and corresponding foreign rights, in a limited field of use defined above. Outside the field of use, Certicom will retain all rights to the technology.

21. Can I get the NSA sublicense from Certicom?

Yes. Certicom offers the same royalty free license rights within the field of use for the 26 patents as the NSA.

22. As a manufacturer wanting to build products for the defined field of use, do I need to license anything from Certicom outside the NSA license?

No. A manufacturer can implement the ECC protocols by themselves; however Certicom brings a lot to the table in terms of toolkits that can dramatically shorten both the development and evaluation cycles. Many manufacturers have already taken advantage of our proven implementations. Certicom has a number of ECC implementation patents that brings value in terms of performance and efficiencies.

QUESTIONS BEYOND THE NSA AGREEMENT – “SUITE B”

23. What is Suite B?

The NSA announced Suite B at the RSA Conference February 2005. Suite B has two different levels of security, one for classified information and one for sensitive but unclassified information. The algorithms are as follows:

Purpose	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

24. Does the NSA license cover Suite B algorithms?

Yes, the ECC portions of Suite B algorithms are covered by the license agreement within the field of use.

25. Why has the NSA defined a Suite B?

We believe Suite B was defined to take advantage of the cryptographic strength of ECC, and to narrow the choices in crypto algorithms. One of the goals is to facilitate sharing of information securely between government organizations which can only be accomplished by setting clear cryptographic standards for systems.

We believe another of the goals is to address the issue of homogeneous cryptographic strengths for symmetric and asymmetric algorithms. For example AES at 128 bits should be paired with ECC at 256 bits and SHA at 256 bits in order to have the whole system at one cryptographic level. Today there are no such rules, and as a result, there are widespread poor cryptographic practices such as using RSA 1024 to exchange keys for AES 128.

26. Is this the first time the NSA has come out with a full cryptographic suite?

Yes. This is the first time the NSA has attempted to address all aspects of cryptography to yield consistent cryptographic strength of equipment that will be fielded under crypto modernization initiatives. All algorithms are publicly available, have been well studied by mathematicians and cryptographers, have withstood the test of time, and are widely used today to secure many applications and devices.

27. What is crypto modernization?

Certain crypto standards, such as Data Encryption Standard (DES), have been in use for the last 20 years or more. These algorithms are now starting to show their age. With crypto modernization, the NSA has researched and defined algorithms that will last for the next 20 to 50 years.

The NSA has stated that there are approximately 1.3 million units of high grade cryptographic equipment that will have to be replaced over the next 10 years. In addition, the US Government would like to buy commercial off the shelf (COTS) products that utilize Suite B.

28. Why does the NSA like ECC?

ECC is the only proven public key technology that scales in a practical way over time. As computing power increases, it becomes easier to break all cryptosystems so cryptographic keys must increase in size to maintain their strength. The NIST chart below demonstrates this clearly. As you can see, in order to match the AES key strength at 256 bits, you would need to use RSA keys of size 15360 bits. Keys at this size are unusable. With ECC you can use a key size of 512 bits to offer equivalent security.

Cryptographic Strength	Symmetric Algorithm	Hash Algorithm	Elliptic Curve Asymmetric Algorithms	RSA/DSA/DH Asymmetric Algorithms
128 bits	AES-128	SHA-256	256 bits	3072 bits
192 bits	AES-192	SHA-384	384 bits	7680 bits
256 bits	AES-256	SHA-512	512 bits	15360 bits

29. Why has the US Government endorsed ECC for both classified and sensitive but unclassified?

We believe the NSA is trying to promote the notion of sharing information securely between Government departments at all levels of communication for Homeland Security. This was a key point in the presentation by Mr. Daniel G. Wolf, the National Security Agency's Director of Information Assurance, at the 14th Annual RSA Conference in 2005. Setting clearly defined cryptographic standards & protocols are crucial for interoperability and making the sharing of information securely a reality.

30. Is the US alone in selecting ECC?

No. The NESSIE project (New European Schemes for Signatures, Integrity and Encryption) (2000-2003) did extensive evaluation on crypto algorithms. For more information, visit: <https://www.cosic.esat.kuleuven.ac.be/nessie/> They recommend ECDSA as a signature scheme and published a chart of key size recommendations that proposes even larger keys than the one above for RSA algorithms.

In addition, in 2001, the Government of Japan formed the CRYPTREC Evaluation Committee which is composed of eminent Japanese cryptographers. They have aggressively evaluated various cryptographic techniques to recommend the optimum cryptographic techniques necessary for the security of future e-Government systems. They recommend a number of ECC-based protocols including ECDSA and ECDH. <http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html>

31. What cryptographic technology has the US Government been using and why are they changing it?

The US Government has used a variety of cryptographic technologies over time. By specifying Suite B, the Government is standardizing on ECC which offers significantly better performance and strength-per-bit over legacy public key systems, such as RSA. By standardizing on ECC, the Government expects to be able to more readily purchase COTS equipment and that interoperability among different products will be improved.

The US Government points to NIST to recommend and validate cryptographic algorithms through FIPS 140-2. NIST Special Publications 800-56 and 800-57 outline approaches, respectively, for key establishment and key management. They include ECDH, ECMQV and ECDSA.

32. What impact does Suite B have on equipment vendors to the Federal Government?

Equipment vendors will have to upgrade their equipment to include Suite B algorithms. There is no hard deadline but it is a formal initiative under the Government's crypto modernization efforts.

33. What is the timeframe where my products will have to support Suite B?

There is no established timeframe yet. Please talk to the NSA about their crypto modernization efforts.

34. Who is affected by the NSA initiative and what do they have to do?

All suppliers to the Government are encouraged to upgrade their equipment to include Suite B in secure communications.

35. What exactly is the NSA asking government agencies to do?

Today the NSA is working through its crypto modernization efforts – that is setting the standards for future communications within the Government and with its allies. NSA understands that this will take time and no hard deadlines have been set to date.

36. Why is RSA not allowed in Suite B?

We believe RSA is not used in Suite B primarily because RSA keys do not scale with technology over time. As AES key sizes grow, RSA keys become too big to be used practically. ECC does not suffer from this problem. Given that this equipment is in the field for many years, the decision was made to use one public key technology that could last for decades.

37. What does this mean for users of RSA?

Users of RSA will have to add ECC to address the government market. We expect that protocol and application standards will be updated to add Suite B requirements. Many standards-based protocols already support ECC so the Suite B definition should not be onerous in many circumstances.

38. Why not continue to use RSA?

You can continue to use RSA. However, in the future, the Government will require the use of Suite B which is ECC-based for public key. A timeframe has not been established yet.

39. Is ECC found in standards?

Yes. ECC is found in many standards. Here is a brief list.

Group	Standards
IEEE	• 1363-2000 • 1363a • 1363.2
CEN	• TC331 WG3 (DPM)
NESSIE	• ECDSA • "PSEC"
SECG	• SEC1 • SEC2
ANSI X9F	• X9.24 Key management • X9.37 Check Image Exchange • X9.57 Cert management • X9.59 Payment • X9.62 ECDSA • X9.63 Key establishment • X9.68 Compressed certificates • X9.73 CMS • X9.84 Biometrics • X9.90 IRD • X9.92 ECPVS • X9.95 Time stamps • X9.96 XML CMS
FIPS	• FIPS 186-2 Signatures (ECDSA) • SP 800-56 Key establishment • SP 800-57 Key Management
FAA Security	• Next generation ATN • Secure ACARS
ISO	• 14888 • 15946 • 9796 • 18033 • ...
IETF	• PKIX • SMIME • IPSec (IKE) • TLS
CE 1394	• Consumer Electronics DTCP
OMA	• WTLS • WPKI • WMLScript • ...

40. Is ECC found in widely used IETF protocols IPsec and TLS?

There are draft standards available. However they must be updated to reflect Suite B. NSA is keenly interested in industry participation to help facilitate this effort.

41. Why should I move to ECC?

You should move to ECC for a number of reasons. First, it's a must to sell products to the US Government. Second, ECC is extremely efficient and offers significant improvements over RSA, especially in the long run.

42. How is ECC different from RSA?

The underlying math is different but the public key protocols are similar. You need a key agreement scheme and a digital signature scheme similar to RSA. The efficiencies provided by ECC mean that you will get more transactions per second from your servers using this cryptosystem.

43. Is there a big cost in adding ECC?

No. There is a perception that ECC is costly. The underlying mathematics is complex but that has nothing to do with implementation costs. As a public key technology, ECC is extremely efficient in code size and performance, much more so than RSA. Certicom has done ECC implementations in less than 4 kbytes of code. In addition, ECC can be implemented on 8-bit processors without the need for a crypto coprocessor thereby reducing your cost of goods. If your application calls for high performance (i.e., hardware implementation), ECC acceleration in hardware is less expensive than implementing AES. Certicom has many examples to prove it.

44. Is ECC truly better than RSA?

Yes. As we saw earlier you can get the equivalent security strength from RSA but at the cost of much higher key sizes. This means more CPU power, more bandwidth and more power consumption are required with RSA.

45. Can I use a FIPS 140-2 suite of algorithms?

Suite B includes FIPS algorithms but also adds ECC, RSA and DES. ECDSA has not been added to the FIPS 140-2 suite and ECDH and ECMQV are coming soon. Over time these will be aligned. The important distinction is that Suite B defines key sizes that also must be used.

46. Why can't SHA-1 be used?

SHA-1 was designed for approximately 80 bits of security. Recent cryptographic attacks against SHA-1 have led to a growing consensus that new products and applications should use one of the newer SHA-2 hashes. Suite B starts with SHA-2 at 256 bits.

47. How does Suite B apply to foreign Governments and manufacturers?

The US Government wishes to communicate with its allies in a highly secure fashion. Suite B is a requirement for interoperable secure communications. Suite B is an open set of algorithms that provides a high level of security for the application. There is nothing stopping foreign Governments from selecting their own standards, however, interoperability with the US will require the implementation of Suite B.

48. Can I influence the evolution of this technology?

Yes. As noted above there are a number of industry related standards initiatives that you could get involved in.

People are encouraged to join SECG (Standards for Efficient Cryptography Group) at www.SECC.org. This is an industry consortium, founded in 1998 to develop commercial standards that facilitate the adoption of efficient cryptography and interoperability across a wide range of computing platforms. SECG members include leading technology companies and key industry players in the information security industry.

QUESTIONS ABOUT CERTICOM

49. What does Certicom bring to the party?

Certicom has been in business for 20 years researching and developing strong, efficient cryptography. We realized in the early years, if ECC was strong then it would be significantly better than anything else out there. Over the years Certicom filed patents to protect its technology around ECC and started building developer toolkits for the OEM/ISV community. Certicom brings proven secure highly optimized implementations to the party!

50. Why was Certicom selected by the NSA?

The NSA selected Certicom because it holds a significant intellectual property position around ECC-based public key cryptography. The NSA felt that if they wanted to standardize on ECC for the US Government then they had to license concept patents from Certicom.

51. Do I have to license any further intellectual property from Certicom with regard to the NSA sublicense?

Not necessarily. An equipment manufacturer could implement the ECC protocols in Suite B within the field of use without licensing anything further from Certicom. However, Certicom does have extensive hardware and software implementation patents that an OEM/ISV could take advantage of. In addition, Certicom offers developer toolkits that meet the specifications of Suite B. Certicom believes it has the most efficient implementations and many OEMs/ISVs have taken advantage of these. OEMs/ISVs should at least look at Certicom before embarking on a long development cycle.

In addition, if the OEM/ISV wants access to a larger market than they should consider talking to Certicom. You will have to take a license from Certicom if you intend to sell your product outside the field of use.

52. Can I get the NSA license through Certicom?

Yes. Certicom retains ownership of the patents and will license them under the same terms as the NSA.

53. If a customer licenses Certicom's Security Builder Crypto or Security Builder GSE, are they free and clear of any intellectual property infringement?

Yes. Certicom indemnifies its customers for the use of our patents in our libraries.

54. Is all of the intellectual property required for Suite B contained in Security Builder Crypto and Security Builder GSE?

Yes. Anyone using Security Builder Crypto or Security Builder GSE has all they need to build products for Government marketplace.

55. Is it cheaper to take an Intellectual Property license or Security Builder Crypto / Security Builder GSE license from Certicom?

It is normally cheaper to take a patent license from Certicom because we are not delivering any software or providing support.

56. Is Certicom going to build a Suite B toolkit for OEMs/ISVs?

Yes. In fact Security Builder Crypto can be used today for Suite B. Certicom is working closely with the NSA to provide a Suite B specific toolkit with the added levels of code assurance.

57. What about patents that have not issued? If I license the intellectual property and/or toolkit am I entitled to those patents as well?

When licensing a toolkit you are entitled to all intellectual property, pending and issued, that is embedded in those products.

58. Does Certicom have any fundamental ECC patents?

We believe we have some of the very best implementation and security patents around ECC. That doesn't mean that you can't implement ECC without Certicom. It simply means that we believe we have patents on the best ways of implementing ECC.

59. How do I take advantage of the NSA license agreement and be confident that I do not infringe any of Certicom's implementation patents?

The quickest way to be sure is to talk to us first about our patents outside of the NSA licensed patents and let us explain what we can do to help you. Another approach is to review all our issued patents that are publicly available. You can find a high-level overview at www.certicom.com/ip. They are not listed here because the list is quite long and requires extensive explanations.

60. Why would I license from Certicom?

First, OEMs want an implementation that's proven to work and is secure. Certicom has 20 years of experience in this field and can get you to market fast with a product that meets Suite B requirements. Certicom's implementations take advantage of every innovation we discovered over the years, not just the 26 patents licensed by the NSA. The use of Certicom's toolkits can greatly shorten both development and government product evaluation timeframes, allowing you to reach the market as fast as possible.

Second, the NSA field of use is limited both in terms of the addressable market and technology. From a technology standpoint OEMs/ISVs are limited to specific key sizes for $GF(p)$, not $GF(2^m)$. A relationship with Certicom opens the door on all fronts.

61. How do we license from Certicom?

Certicom licenses patents, products and most often a blend of both. There are two basic components to our licensing; OEM/ISV License and the Production License. The OEM/ISV License is a "right to build" license, and the Production License is a "right to ship" license.

62. Is Certicom's royalty rate reasonable?

Certicom wants to see the technology deployed on a wide scale and is motivated to do so. We have over 300 customers who believe our royalty rate is reasonable.

63. Will ECC be ubiquitous?

Absolutely! We've been behind this technology for almost 20 years and we've seen other schemes come and go. ECC provides the strongest security per bit of any known scheme and it readily scales to meet future security needs. Commercially, if you consider health records and intellectual property at least the equivalent of the Government's sensitive, but unclassified rating, then ECC is simply the best public key cryptosystem to protect this type of data.

64. Does Certicom have a monopoly on ECC?

No. Certicom does not own ECC, nor does it have a monopoly. ECC is available in the public form and has been specified by many standards. Certicom does have the largest patent portfolio covering this area of cryptography with protocol, security and implementation patents.

65. Does Certicom plan to go after Intellectual Property infringers?

Certicom has an obligation to its share holders to protect its intellectual property. If we believe Certicom's intellectual property is clearly being used without license we will notify the company. Certicom licenses its patents on reasonable and non-discriminatory terms.

66. Can I use open source code that might be available to implement ECC?

Yes provided it does not infringe Certicom's patents. The OEM/ISV should contact Certicom first and ask if the open source implementation in question does infringe Certicom intellectual property. Certicom will look at the open source implementation and let you know of any issues. In addition to intellectual property concerns, there may be more efficient or stronger implementations available from Certicom than can be found with open source.

IMPLEMENTATION QUESTIONS

67. What are the reasons for using Certicom versus a home grown solution?

Certicom has been implementing this technology for years. Certicom has the most efficient implementations in software, firmware and hardware; it has ported to over 30 platforms and has worked with over 300 partners to deliver world class solutions. Certicom can deliver a proven solution without risk.

A company that uses home grown solutions based on open source must carefully vet these implementations to ensure they are working properly. Extra development cycles must be spent validating your implementation of AES and ECC. Extra development cycles must be spent in building properly functioning random number generators. Extra development cycles must be spent in proving to NIST or the NSA that your implementations are correct. WEP is an example where known, good open source crypto algorithms were used in an inappropriate manner. Significant R&D resources were spent on correcting these problems. All these factors lead to increased time and risk in your product development cycle.

68. Does Certicom have tools that can get me to market fast?

Certicom has over 300 partners from silicon to end-to-end systems. Our tools have been quoted as being the best in the world for rapid time to market. These are proven, secure tools that allow you to quickly add security to devices and applications.

69. If we decide to do our own implementation will Certicom support us?

Yes. Certicom can help you with this. Just ask.

70. What companies use Certicom to deliver ECC?

You can find a list of our customers that have implemented Certicom technology at www.certicom.com/customers.

71. Can I use open source to implement Suite B?

If you want to use open source to implement Suite B then you should check with Certicom. There may be patents that open source infringes outside those licensed by the NSA, for example implementation patents, as well as security holes or inefficient implementations in that software. Certicom can tell you.

72. If we use a chip like the Freescale PowerQUICC that already has ECC in it, do we still have to take a license from Certicom?

It depends on the capability of the existing chip. Assuming the user stays within the NSA field of use then it is possible to simply license the chip. Again there is room for optimizations if you use Certicom Intellectual Property.

Let's look at the Freescale PowerQUICC communications processors as an example.

Freescale's PowerQICC II and III chip families are very popular in the industry. They have an RSA/ECC hardware multiplier that can be used to accelerate public key operations. The module can be programmed to perform RSA and Diffie-Hellman up to 2048-bits and ECC, $GF(2^m)$ and $GF(p)$, with programmable field size up to 511-bits.

Freescale does provide high level security support for well established protocols including IPSec, IKE, iSCSI, SRTP, SSL 3.1/TLS 1.0 and 802.11i. Today these protocols all use RSA for public key.

If you wanted to implement Suite B for example, you could use the Freescale PowerQUICC II or III chipsets but there is currently no higher level ECC firmware support for those devices beyond some very basic functions. In other words there is no firmware for ECDSA signatures, or ECMQV key agreement. This functionality could be written by the user or could take a highly optimized implementation from Certicom.

73. What are the benefits of licensing from Certicom?

The primary reasons are to get a proven implementation without security risks, faster NSA approvals, no risk of patent infringement, and a wider field of use.

74. Why can I get faster NSA or FIPS validation working with Certicom?

Simply because Certicom has already been through it several times. We have extensive relationships with the certification bodies and NIST. We are constantly providing code updates and reviews on multiple operating systems for our customers. Certicom has a security module that has already received FIPS 140-2 validation on several platforms. The NSA has also reviewed Certicom implementations for ECC and know that they are proven and secure.

75. Will companies now have to use Certicom toolkits?

No. OEMs/ISVs do not have to use Certicom. They can grow their own solution or outsource the development with the associated risks

76. Where do I get ECDSA Certificates?

ECDSA certificates are not as widely available as RSA-based certificates but there are solutions available in the market. You can get commercial ECDSA certificates from some of the traditional PKI vendors. The other approach that is increasingly being used by OEMs/ISVs is to use Certicom tools to create certificates that are built into your products.

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.

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

Europe

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

Ottawa

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

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

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

www.certicom.com