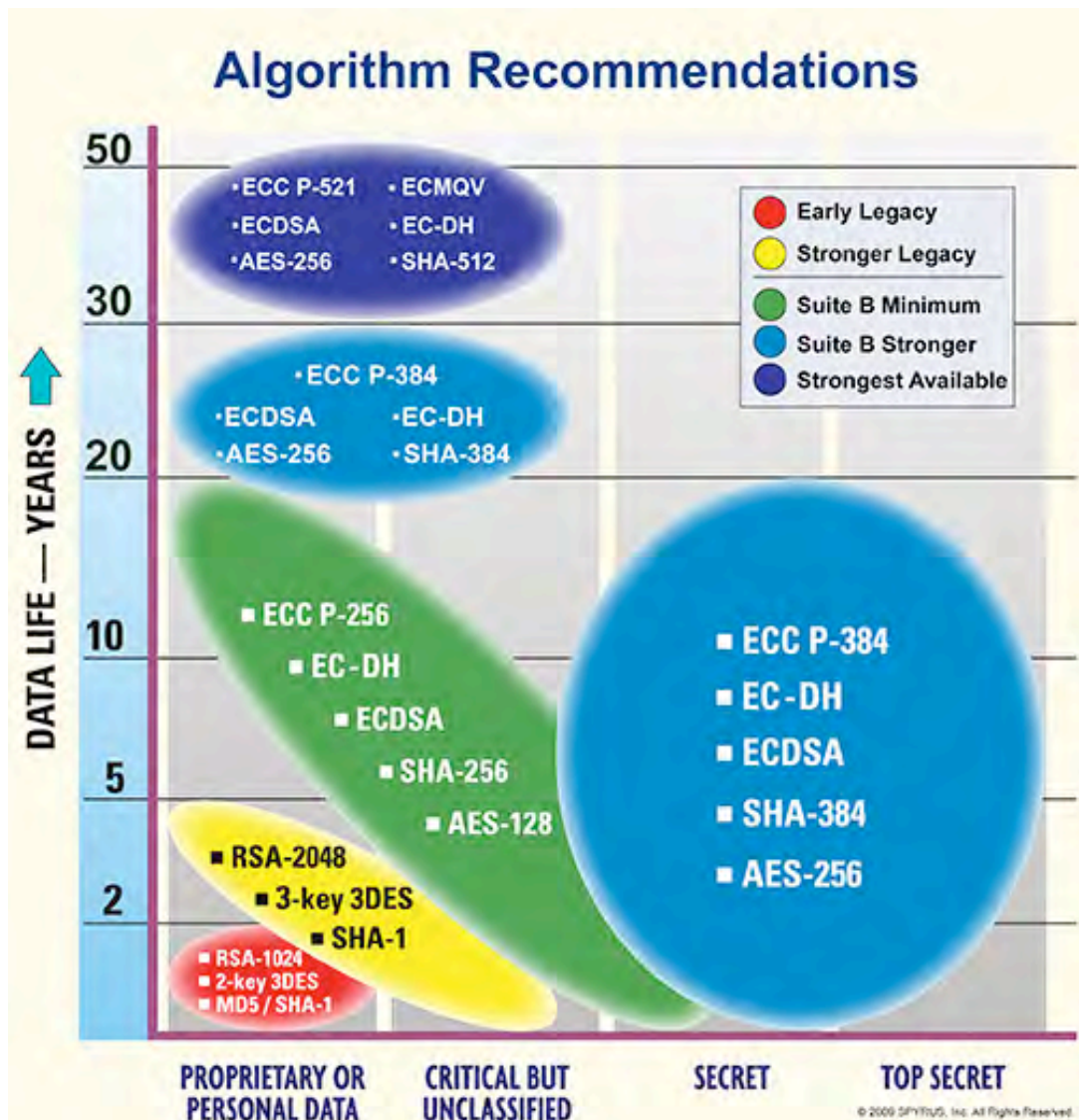




Crypto Modernization

Public key cryptography has become ubiquitous. As time passes, however, longer keys and stronger algorithms become essential for long-term information assurance. SPYRUS solves this critical problem with our support for the U.S. Government Suite B standard for cryptographic algorithms.

The new cryptographic algorithms are significantly faster, more compact, and secure enough to protect valuable and even classified data for the foreseeable future. SPYRUS recommends that users migrate away from the decades-old legacy RSA, triple-DES, and MD5/SHA-1 algorithms to the newer, stronger, faster, and more compact Suite B algorithms, including elliptic curve cryptography (ECC), AES, and SHA-2. SPYRUS was the first company to support these algorithms across its entire product line.



Suite B: Meeting Tomorrow's Threats, Today

Information Security for the Future

The war on terror has highlighted the need for our federal, state and local government agencies to communicate quickly and securely with one another and with our international allies. The information exchanged can have different levels of sensitivity: Some information may be classified, some unclassified but sensitive, and some information intended for public dissemination must first be validated as authentic.

To address these and other issues, the U.S. Government has initiated a cryptographic modernization program. Classified Suite A algorithms are required for U.S. Government internal use. Unclassified Suite B algorithms can be used to protect unclassified and classified data; to facilitate information sharing across federal, state, and local governments; and with our allies and multinational coalition partners.

The Suite B Algorithms: ECC, AES, and SHA-2

If information must be kept secret for 50 years, you cannot wait 49 years before encrypting it with a stronger algorithm. You must take into account the likely future capabilities of your adversaries and use appropriate-strength cryptography now.

The U.S. Department of Defense (DoD) understands that although sensitive data must be protected for decades, there is also a current need to share information securely with other agencies. The National Security Agency (NSA) has taken unprecedented steps to enable secure information sharing at both domestic and international levels.

In June 2003, the NSA announced that for particular applications, NSA-approved implementations of the Advanced Encryption Standard AES-128 algorithm could be used to protect classified information up to the Secret level, and AES-192 and AES-256 could be used to protect Top Secret data. In October 2003, the NSA licensed 26 key patents in the field of elliptic curve cryptography from Certicom, Inc., for national-security-related applications, involving key sizes over 255 bits and FIPS 140-2 certification, among other requirements. At the 2005 RSA Conference, the NSA announced that the unclassified Suite B algorithms can be authorized for multinational and domestic information sharing of Secret and Top Secret data with P-384 ECC keys, using the EC Diffie-Hellman key establishment scheme, the ECDSA digital signature algorithm, SHA-384, and AES-256. For FOUO, SBU, LEO, and similar unclassified but sensitive data, P-256 ECC keys, SHA-256, and AES-128 are required. A minimum of P-256, SHA-256, and AES-128 is also recommended for most commercial applications, although very long-term data storage may benefit from the stronger key lengths.

SPYRUS Receives First ECC License

SPYRUS received the first patent license for elliptic curve cryptography issued by the National Security Agency (NSA) under the terms of the NSA Field of Use patent license. The license covers 26 individual U.S., Canadian, and European patents and patent applications, and applies to all uses and users of the SPYRUS family of products.

The Field of Use includes elliptic curve cryptography in the prime field $GF(p)$, using 256-bit or longer keys in implementations that are FIPS 140-2 compliant, among other requirements. Typical applications involve federal, state, and local governments, and include interoperability with foreign governments.

SPYRUS is the first company under this license to incorporate this patented technology in all products, including the LYNKS[®] Series II Hardware Security Module (HSM); the Rosetta[®] Series II smart card and USB security devices; En-Sign[™] Software; Security In A Box[®], the Signal Identity Manager[™], and the Hydra Privacy Card[®] Series II (Hydra PC[™]).

Barring unforeseen developments in quantum computing or molecular cryptography, SPYRUS believes that elliptic curve cryptography with P-521 keys, using the ECMQV or EC-DH key establishment scheme and ECDSA digital signatures, together with AES-256 and SHA-512, can ensure commercial data security for at least the next 50 years.

SPYRUS Announces Suite B Support

U.S. DoD crypto equipment supports two different suites of cryptographic algorithms. Suite A algorithms are used for classified applications, and are classified themselves. Suite B algorithms are unclassified algorithms that are strong enough for both classified and unclassified applications and can also be released to our allies, coalition partners, Homeland Defense, and the mission-critical infrastructure.

The following components are required for Suite B:

- ECC P-384 keys for Classified data, and P-256 for Critical But Unclassified data
- The EC Diffie-Hellman key establishment scheme
- The ECDSA digital signature algorithm
- AES-256 & SHA-384 for Classified data, and AES-128 and SHA-256 for Critical But Unclassified applications

SPYRUS goes beyond Suite B by offering the highest-strength P-521 ECC key and SHA-512 hash algorithm for use with extremely sensitive applications, including secure key backup and restore. We support the full range of SHA-224/256/384/512 and AES-128/192/256 algorithms.

SPYRUS products support all seven of the schemes in NIST SP 800-56A, using on-token key derivation functions in all cases.

ECC Performance Advantages

From both size and performance standpoints for equivalent security and information assurance, elliptic curve cryptography is the best choice.

- ▲ ECC operations are much faster than their RSA equivalents. The time required for an RSA algorithm decryption or signature operation increases with the cube of the key size. To increase the security from a key length from 1024 to 15,360 bits takes $15^3 = 3,375$ times as long. The time required for an ECC key agreement operation also increases with the cube of the key size, but to go from the equivalent 163-bit to a 521-bit ECC key requires only 32 times as long.
- ▲ If long-term, high-strength security is the most important factor, the benefits of ECC are even more pronounced. For greatest security, private key operations must be confined to hardware tokens, including smart cards and hardware security modules (HSMs). These devices are limited in available RAM and computational power. Generating an 8,192-bit or 15,360-bit RSA key on such devices is completely impractical. Generating a P-521 key on a LYNKS HSM or Rosetta Series II smart card, on the other hand, requires only a few seconds, and the P-384 and P-256 operations are even faster.

ECMQV Support

One of the most meaningful patents in the NSA patent license is the ECMQV (Menezes-Qu-Vanstone) key establishment scheme, which has been standardized in ANSI X9.63 and further refined in NIST SP 800-56A, *Recommendations for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*.

Both Full ECMQV (for real-time sessions) and One-Pass ECMQV (for store and forward applications) will be supported in all SPYRUS products. In addition, the five EC Diffie-Hellman key establishment schemes specified by NIST SP 800-56A will be supported.

SPYRUS Support for Suite B ... And More

Since 2004, SPYRUS has implemented an extensive cryptographic modernization program of its entire product line to meet the requirements of new FIPS standards, including ECC. SPYRUS products meet and even exceed the algorithmic requirements for Suite B support. For example:

- ▲ SPYRUS products support high-strength ECC P-521 keys and SHA-512 for use with extremely sensitive applications, including secure key backup and restore. P-521 keys are equivalent to a 15,360-bit RSA key in strength, but the ECC operations are much faster than RSA.
- ▲ All seven of the ECMQV and EC Diffie-Hellman key establishment schemes required by SP 800-56A are supported for all three key strengths.

SPYRUS Support for the Global Information Grid and Commercial Markets

A key initiative of the crypto modernization program is securing multinational information sharing with our allies and coalition partners throughout the world. Equally important is the need for algorithms that are compact, efficient, and can be secure for at least 50 years. Protecting the privacy and authenticity of personal information such as medical history, adoption records, sealed court records, witness protection information, and census records all require the strongest cryptographic algorithms available, because the protection must last for the lifetime of the individual.

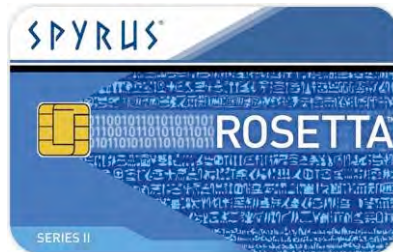
SPYRUS anticipates that the Suite B standard will be broadly accepted for interoperability within government and commercial organizations worldwide. These algorithms will provide the basis for information assurance and set the standard for both unclassified and selected classified information for years to come.

The entire SPYRUS product line meets or exceeds the Suite B standard, including the Rosetta Series II USB and smart card security devices, the LYNKS Series II HSM (in PCMCIA and USB versions), the Hydra Privacy Card Series II (Hydra PC™) USB Encryption Devices, En-Sign Security Device Management software, Security In A Box, and Signal Identity Manager.

See the SPYRUS product information at www.spyrus.com for the exciting details of these and other hardware and software products.



Rosetta Series II USB



Rosetta Series II Smart Card



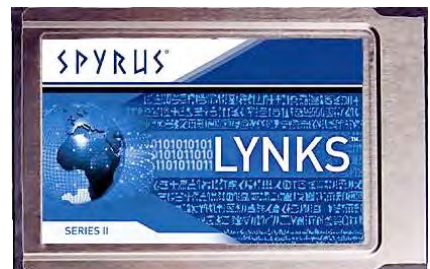
PAR 2 Smart Card Reader



Hydra Privacy Card Series II



LYNKS Series II HSM (USB)



LYNKS Series II HSM (PCMCIA)

©2006–2010 SPYRUS, Inc. All rights reserved. SPYRUS, the SPYRUS logos, Security to the Edge, Suite B On Board, LYNKS, Rosetta, Signal Identity Manager, Security In A Box, Hydra Privacy Card, and Hydra PC are either registered trademarks or trademarks of SPYRUS in the United States and/or other countries. All other trademarks are the property of their respective owners. Individual SPYRUS products may embody technology protected by one or more of the following patents or patent applications: U.S. Pat. Nos. 6,003,135; 6,088,802; 5,761,305; 5,889,865; 5,896,455; 5,933,504; 5,999,626; 6,122,736; 6,141,420; 6,336,188; 6,487,661; 6,563,928; 6,618,483; 6,981,149; U.S. Pat. Appl. Ser. Nos. 09/434,247; 09/558,256; 09/942,492; 10/185,735; Can. Pat. Appl. Ser. Nos. 2176972; 2176866; 2202566; 2174261; 2155038; 2174260; E.P. Pat. Appl. Ser. No. 96201322.3; 97106114.8; 96105920.1; 95926348.4; 96105921.9

Document number 402-000000-06