Crypto FAQ
CryptoBytes
RSA Algorithm
PKCS
Advanced Encryption Standard
Tech Notes
Staff & Associates
Standards
Bulletins
Challenges

RSA Laboratories Submits New AES Mode to NIST

June 18, 2002

RSA Laboratories has collaborated with Hifn and MacFergus to design a new authenticated enc Counter with CBC MAC, or simply CCM. CCM provides both authentication and encryption. CC construction, building on traditional mechanisms. RSA Laboratories has submitted CCM to the N Institute of Standards and Technology (NIST) for consideration as a standard mode for use with Advanced Encryption Standard (AES). All of the submissions are available at the NIST Propose page.

CCM was designed initially for use with packet-oriented security protocols. As such it includes p authenticate the packet header and the payload, while encrypting only the payload. However, C be used for encrypting files, messages and other data. CCM uses a single cryptographic key to authentication and encryption.

Traditionally, two different cryptographic algorithms are used for authentication and encryption, its own key. For example, authentication might be provided by HMAC-MD5 and encryption by T Since completely different mechanisms are used, there is no synergy between them. CCM uses cipher to provide authentication and encryption. It was designed with AES in mind.

NIST has received a number of other submissions of authenticated encryption modes. Details o submissions are available on the NIST Proposed Modes web page. The biggest difference betw and these other submission is patent status. CCM is intended to be unencumbered by patents, authors of CCM have not, and will not, apply for patents on CCM.

CCM has the following properties:

Small implementation size. CCM uses only the encryption operation of the underlying blc CCM does not use decryption operations. As a result, CCM implementations are smaller alternatives.

Packet header authentication. CCM was designed for the packet environment. It can aut arbitrary packet header, then authenticate and encrypt the packet payload.

Single key. CCM uses a single key for all cryptographic operations. As a result, CCM implementations only compute one key schedule. AES-CCM is slightly faster than the str application of AES-CBC-MAC for authentication and AES-CTR for encryption since only schedule is needed.

Packet overhead. CCM increases the packet size by adding an initialization vector and a check value. This is the same overhead associated with other authenticated encryption n

Cryptographic confidence. CCM has a mathematical proof. The proof shows that CCM p level of confidentiality and integrity comparable to other authenticated encryption modes.

At least one implementation of CCM is freely available. Doug Whiting, one of the CCM co-autho first CCM implementation. His code makes use of the open source AES implementation from Br and it is available here.

United States: 1-877-RSA-4900 or 781 515 5000, Europe, Middle East, Africa: +44 (0)1344 781000,
Asia/Pacific: + 61 2 9463 8400, Japan: +81 3 5222 5200