CCM Use Requirements Specification

The Counter with CBC-MAC (CCM) mode is designed to use the Advanced Encryption Standard (AES) block cipher, or any other block ciphers with a block size of 128 bits or more, to provide authentication and encryption using a single block cipher key that is established beforehand. Thus, CCM requires a well-designed key management structure. CCM is intended for use in a packet environment; the plaintext input includes a header, which is authenticated but not encrypted, and a payload, which is authenticated and encrypted. CCM operates on the whole packets; it does not support partial processing or stream processing. A packet must be an integral number of octets. Each packet must be assigned a unique value, called a nonce. The size of the nonce determines the maximum number of packets that can be authenticated and encrypted with a single block cipher key. The total number of octets protected with a single block cipher key is limited to 2^64 octets.

CCM processing expands the packet size by appending an encrypted authentication tag. Successful verification of the authentication tag provides assurance that the packet originated from a source with access to the block cipher key. Consequently, successful verification of the authentication tag also provides assurance that the packet was not altered after the generation of the authentication tag. Failed verification of the authentication tag is designed to reveal intentional, unauthorized modifications of the packet, as well as accidental modifications.

CCM protects the packet payload from disclosure. A breach of confidentiality is as unlikely as guessing the block cipher key.

CCM allows pre-computation of the key stream if the nonce value is known, allowing half of the computational load to be pre-processed. This property can be used to improve the efficiency of an implementation.

CCM uses only the encryption function of the block cipher. This property can be used to minimize the size of an implementation.