6.11 Additional AES Mechanisms

	Functions						
Mechanism	**Encrypt & Decrypt**	**Sign & Verify**	**SR & VR[1]**	**Digest**	**Gen. Key/ Key Pair**	**Wrap & Unwrap**	**Derive**
CKM_AES_GCM	✓						
CKM_AES_CCM	✓						
GKM_AES_GMAC		✓					

6.11.1 Definitions

Mechanisms:

CKM_AES_GCM
CKM_AES_CCM
CKM_AES_GMAC

6.11.2 AES-GMAC

AES-GMAC, denoted **CKM_AES_GMAC**, is a mechanism for single- and multiple-part signatures and verification. It is described in NIST Special Publication 800-38D [GMAC]. GMAC is a special case of GCM that authenticates only the Additional Authenticated Data (AAD) part of the GCM mechanism parameter. When GMAC is used with C_Sign or C_Verify, pData points to the AAD. GMAC does not use plaintext or ciphertext.

The signature produced by GMAC, also referred to as a Tag, is 16 bytes long.

Its single mechanism parameter is a 12 byte initialization vector (IV).

Constraints on key types and the length of data are summarized in the following table:

Table 1, AES-GMAC: Key And Data Length

Function	**Key type**	**Data length**	**Signature length**
C_Sign	AES	<2^64	16 bytes
C_Verify	AES	<2^64	16 bytes

For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK_MECHANISM_INFO** structure specify the supported range of AES key sizes, in bytes.