Algorithm Dependency Cheat Sheet

This document is intended to describe the algorithms which have prerequisite and covered with the current FIPS140 validation.

Algorithm		Prerequisite
DSA		SHA RNG or DRBG 800-90
DRBG 800-90	Hash DRBG	SHA (sizes must match)
	HMAC DRBG	HMAC (sizes must match)
	CTR DRBG	TDES using CTR mode AES using CTR mode
	Dual EC DRBG	ECDSA with Key Pair Implemented SHA (sizes must match)
DSA-2		SHA RNG or DRBG
ECDSA-2		SHA RNG or DRBG
RSA		SHA RNG or DRBG
HMAC		SHA
CCM		AES
ECDSA		SHA RNG or DRBG
CMAC		AES TDES
KAS FFC		DSA SHA RNG or DRBG CCM or CMAC or HMAC
KAS ECC		ECDSA SHA RNG or DRBG CCM or CMAC or HMAC
Galois Counter Mode (GCM) 800-38 D		AES / RNG or DRBG
XTS 800-38E		AES (with mode of operation using forward cipher function) AES (with mode of operation using forward and inverse cipher function)