Application Notes

nShield Support for Cryptographic Algorithms

01 July 2024

Table of Contents

1. Introduction

This topic details the implemented restrictions imposed in various firmware modes.

Security World mode designation	new-world "mode" parameter	Description
Unrestricted		The unrestricted Security World mode protects keys with FIPS approved cryptography, but it is not designed to be fully compliant with all the requirements and restrictions of a particular certification standard. This mode can be used by customers who want their keys securely managed within the FIPS level 3 boundary, but don’t need full compliance with the certification approved modes of operation. ℹ For Solo XC, Solo+ and Edge, the unrestricted mode is compliant with FIPS 140-2 Level 2.
FIPS 140 Level 3	`fips-140-level-3`	This is the FIPS 140 level 3 approved mode of operation. Customers needing FIPS 140 Level 3 compliance can use this mode on an HSM with a FIPS validated fw version.
Common Criteria CMTS	`common-criteria-cmts`	The Common Criteria approved mode of operation for Protection Profile EN 419 221-5 Cryptographic Module for Trust Services. Customers needing Common Criteria (CC) compliance can use this mode on an HSM with a CC validated fw version.

2. Features and Restrictions

Introductory Notes

- This topic covers all sorts of module features, not just algorithm/mechanisms
- For the most part a blank table cell means "no restriction"; there are a few exceptions to this, for example, flag settings for particular modes
- The information is low-level and may need interpreting to answer high-level questions
- This topic does not cover higher level APIs like PKCS#11 or JCE

The details are correct as of July 2023, except that there are a couple of gaps for very new functionality Feature/Mode Matrix.

3. Configuration

<table>
<tr><th>Feature</th><th>Unrestricted</th><th>FIPS 140 Level 3</th><th>Common Criteria CMTS</th></tr>
<tr><td>InitModeFlags</td><td colspan="2">UseFIPSApprovedInternalMechanisms</td><td>UseFIPSApprovedInternalMechanisms
AuditLogging</td></tr>
<tr><td>NSOPermsModeFlags</td><td>AlwaysUseStrongPrimes</td><td>FIPSLevel3Enforcedv2
AlwaysUseStrongPrimes
StrictSP80056Ar3</td><td>CommonCriteriaCMTSRestrictions
AlwaysUseStrongPrimes</td></tr>
<tr><td>Public NSOPerms</td><td>ReadFile
FormatToken
GenerateLogToken
LoadLogicalToken
WriteShare
ChangeSharePIN
GetRTC</td><td>LoadLogicalToken
WriteShare
ChangeSharePIN
GetRTC</td><td>ReadFile
FormatToken
GenerateLogToken
LoadLogicalToken
WriteShare
ChangeSharePIN
GetRTC</td></tr>
</table>

4. Functionality

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
Cmd_Import		No private key import Public key import requires FIPS auth	No private key import
ExportAsPlain		Forbidden for private keys	
Key generation		Requires FIPS auth	
Key generation		Pairwise check always on	
Impath			Forbidden
Minimum impath groups	DHPrime3072	DHPrimeMODP3072	n/a
Default module attributes	ModuleAttribTag_Challenge ModuleAttribTag_ESN ModuleAttribTag_KML ModuleAttribTag_KLF2 ModuleAttribTag_KNSO ModuleAttribTag_KMList ModuleAttribTag_KLF3 (nShield 5 & later)		
SignModuleState with KLF		Forbidden	
Audit logging			Mandatory
AlwaysUseStrongPrimes		Mandatory	

5. Asymmetric Algorithms/Mechanisms

5.1. Diffie-Hellman Key Agreement

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
DHPrivate key generation (KeyType_DHPrivate)		Forbidden	
DHPrivate default size	1024/160	2048/224	1024/160
DHPrivate key agreement (Mech_DHKeyExchange)		Forbidden (including DLIES)	
DHExPrivate key generation (KeyType_DHExPrivate)			
DHExPrivate domain parameters		Restricted as per SP800-56Ar3	
DHExPrivate key generation minimum size		2048/224 minimum if |p|=3072, |q|>=256.	
DHExPrivate default size	2048/256		
DHExPrivate key agreement minimum size		2048	
DHExPrivate key agreement (Mech_DHExKeyExchange)		Forbidden with Cmd_Decrypt (Permitted with KDF)	
ElGamal encryption/decryption (Mech_ElGamal)		Forbidden	

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
IEEE DLIES with ANSI X9.63 KDF and 3DES CBC encryption (Mech_DLIESe3DEShSHA1)		Forbidden	
IEEE DLIES with ANSI X9.63 KDF and AES CBC encryption (Mech_DLIESeAEShSHA1		Forbidden	
IEEE DLIES with ANSI X9.63 KDF and AES CBC encryption (Mech_DLIESeAEShSHA1DHEx)			

When a DHEx key is loaded into the module, the domain parameters are validated. If the domain parameters do not match those found in SP800-56Ar3, the validation time is significantly longer. Entrust recommends that you always use SP800-56Ar3 domain parameters.

5.2. DSA Signature

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
DSA key generation (KeyType_DSA)			
DSA key generation sizes		FIPS 186-4 sizes only; 2048 minimum	
DSA signature key sizes		FIPS 186-4 sizes only; 2048/224 minimum	
DSA signature hashes		RIPEMD160 & SHA-1 forbidden	
Legacy DSA domain generation (KeyType_DSAComm)		Forbidden	

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
Legacy DSA domain generation (KeyType_DSACommVariableSeed)			
FIPS 186-4 DSA domain generation (KeyType_DSACommFIPS186_3)			
DSA SHA-1 signature (Mech_DSA)		Forbidden	
DSA SHA-2 signature (Mech_DSAhSHA224, Mech_DSAhSHA256, Mech_DSAhSHA384, Mech_DSAhSHA512)			
DSA RIPMED160 signature (Mech_DSAhRIPMED160)		Forbidden	

5.3. RSA Signature/Encryption

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
RSA key generation (KeyType_RSAPrivate)	Strong primes always on (see note below)		
RSA key generation public modulus size		2048 minimum; multiple of 2	
RSA key generation rules (<1024)	FIPS 186-4 B.3.6	Forbidden	FIPS 186-4 B.3.6
RSA key generation rules (>=1024)	FIPS 186-4 B.3.6		
RSA key generation/import public exponent		16-256 bits	
RSA signature key sizes		2048 minimum	

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
RSA signature hashes		RIPEMD160 & SHA-1 forbidden	
RSA raw encryption/decryption (any RSA mech with bignum plaintext)		Forbidden with Mech_RSApPKCS1 (pPKCS11), permitted otherwise	
RSA PKCS#1 encryption/decryption (Mech_RSApPKCS1, Mech_RSApPKCS1pPKCS11 with bytes plaintext)		Forbidden	
RSA raw sign/verify (any RSA mech with bignum plaintext)		Forbidden with Mech_RSApPKCS1 (pPKCS11), permitted otherwise	
RSA PKCS#1 any-hash signature (Mech_RSApPKCS1, Mech_RSApPKCS1pPKCS11 with bytes/hash plaintext)		Forbidden	
RSA PKCS#1 SHA-1 signature (Mech_RSApPKCS1, Mech_RSApPKCS1pPKCS11 with bytes/hash plaintext)		Forbidden	
RSA PKCS#1 SHA-2 signature (Mech_RSAhSHA224pPKCS1, Mech_RSAhSHA256PKCS1, Mech_RSAhSHA384pPKCS1, Mech_RSAhSHA512pPKCS1 with bytes/hash plaintext)			

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
RSA PKCS#1 SHA-3 signature (Mech_RSAhSHA3b224pPKCS1, Mech_RSAhSHA3b256PKCS1, Mech_RSAhSHA3b384pPKCS1, Mech_RSAhSHA3b512pPKCS1 with bytes/hash plaintext)			
RSA PSS SHA-1 signature (Mech_RSAhSHA1pPSS with bytes/hash plaintext)		Forbidden	
RSA PSS SHA-2 signature (Mech_RSAhSHA224pPSS, Mech_RSAhSHA256pPSS, Mech_RSAhSHA384pPSS, Mech_RSAhSHA512pPSS with bytes/hash plaintext)			
RSA PSS SHA-3 signature (Mech_RSAhSHA3b224pPSS, Mech_RSAhSHA3b256pPSS, Mech_RSAhSHA3b384pPSS, Mech_RSAhSHA3b512pPSS with bytes/hash plaintext)			
RSA PSS RIPEMD160 signature (Mech_RSAhRIPMED160pPSS with bytes/hash plaintext)		Forbidden	

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
RSA SHA-1 OAEP encryption (Mech_RSApOAEP with bytes plaintext)			
RSA SHA-2 OAEP encryption (Mech_RSApOAEPhSHA224, Mech_RSApOAEPhSHA256, Mech_RSApOAEPhSHA384, Mech_RSApOAEPhSHA512 with bytes plaintext)			
RSA SHA-3 OAEP encryption (Mech_RSApOAEPhSHA3b224, Mech_RSApOAEPhSHA3b256, Mech_RSApOAEPhSHA3b384, Mech_RSApOAEPhSHA3b512 with bytes plaintext)			

5.4. Elliptic Curve Key Agreement

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
ECC enablement	EllipticCurve feature (enabled by default from firmware V13.5 onwards)		
ECC domain parameters		224 minimum; SECP256k1 forbidden; non-named curves forbidden	
ECDH key agreement (Mech_ECDHKeyExchange)		Forbidden with Cmd_Decrypt (Permitted with Cmd_DeriveKey)	

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
ECDHC key agreement (Mech_ECDHCKeyExchange)		Forbidden with Cmd_Decrypt (Permitted with Cmd_DeriveKey)	
ECDH key generation (KeyType_ECDHPrivate, KeyType_ECPrivate)			
ECDHLax key generation (KeyType_ECDHLaxPrivate)		Forbidden	
ECDHLax key agreement (Mech_ECDHLaxKeyExchange)		Forbidden	

5.5. Elliptic Curve Signature

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
ECC enablement	EllipticCurve feature enabled by default from V13.5 onwards		
ECC domain parameters		224 minimum; SECP256k1 forbidden; non-named curves forbidden	
ECDSA key generation (KeyType_ECDSAPrivate, KeyType_ECPrivate)			
ECDSA signature RNG		Never uses unvalidated RNG	
ECDSA signature hash		RIPEMD160 & SHA-1 forbidden	
ECDSA verify hash		RIPEMD160 forbidden	
ECDSA SHA-1 sign (Mech_ECDSA)		Forbidden	
ECDSA SHA-1 verify (Mech_ECDSA)			

<table>
<tr><th>Feature</th><th>Unrestricted</th><th>FIPS 140 Level 3</th><th>Common Criteria CMTS</th></tr>
<tr><td>ECDSA RIPMED160 sign/verify (Mech_ECDSAhRIPEMD160)</td><td></td><td>Forbidden</td><td></td></tr>
<tr><td>ECDSA SHA-2 sign/verify (Mech_ECDSAhSHA224, Mech_ECDSAhSHA256, Mech_ECDSAhSHA384, Mech_ECDSAhSHA512)</td><td></td><td></td><td></td></tr>
<tr><td>ECDSA SHA-3 sign/verify (Mech_ECDSAhSHA3b224, Mech_ECDSAhSHA3b256, Mech_ECDSAhSHA3b384, Mech_ECDSAhSHA3b512)</td><td></td><td></td><td></td></tr>
<tr><td>ECDSA sign/verify GBCS mode (Mech_ECDSAhSHA256kGBCS)</td><td colspan="2">Forbidden</td><td></td></tr>
</table>

5.6. X25519/Curve25519 Signature/Encryption

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
Ed25519 key generation (KeyType_Ed25519Private)		Forbidden	
Pure Ed25519 sign/verify (Mech_Ed25519)		Forbidden	
Prehashed Ed25519 sign/verify (Mech_Ed25519ph)		Forbidden	

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
Prehashed Ed25519 sign/verify with context (Mech_Ed25519phctx)		Forbidden	
X25519 key generation (KeyType_X25519Private)		Forbidden	
X25519 key agreement (Mech_X25519KeyExchange)		Forbidden	

5.7. Ed448 Signature

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
Ed448 key generation (KeyType_Ed448Private)		Forbidden	
Pure Ed448 sign/verify (Mech_Ed448)		Forbidden	
Pure Ed448 sign/verify with context (Mech_Ed448ctx)		Forbidden	
Prehashed Ed448 sign/verify (Mech_Ed448ph)		Forbidden	
Prehashed Ed448 sign/verify with context (Mech_Ed448phctx)		Forbidden	

5.8. KCDSA Signature

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
KCDSA enablement	KISAAlgorithms feature required		
KCDSA key generation (KeyType_KCDSAPrivate)		Forbidden	

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
KCDSA signature (Mech_KCDSAHASH160, Mech_KCDSASHA1, Mech_KCDSASHA224, Mech_KCDSASHA256, Mech_KCDSARIPMED160)		Forbidden	
KCDSA domain generation (KeyType_KCDSACommon)		Forbidden	

6. Symmetric Mechanisms/Algorithms

6.1. ARIA

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
ARIA key generation (KeyType_ARIA)		Forbidden	
ARIA CBC no padding (Mech_ARIAmCBCpNONE)		Forbidden	
ARIA ECB no padding (Mech_ARIAmECBpNONE)		Forbidden	

6.2. Camellia

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
Camellia key generation (KeyType_Camellia)		Forbidden	
Camellia CBC no padding (Mech_CamelliamCBCpNONE)		Forbidden	
Camellia ECB no padding (Mech_CamelliamECBpNONE)		Forbidden	

6.3. CAST256

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
CAST256 key generation (KeyType_CAST256)		Forbidden	

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
CAST256 CBC PKCS#5 padding (Mech_CAST256mCBCi128pPKCS5)		Forbidden	
CAST256 ECB PKCS#5 padding (Mech_CAST256mECBpPKCS5)		Forbidden	
CAST256 CBC no padding (Mech_CAST256mCBCpNONE)		Forbidden	
CAST256 ECB no padding (Mech_CAST256mECBpNONE)		Forbidden	
CAST256 CBC-MAC PKCS#5 padding (Mech_CAST256mCBCMACi0pPKCS5)		Forbidden	

6.4. DES

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
Single-DES key generation (KeyType_DES)		Forbidden	
Single-DES CBC PKCS#5 padding (Mech_DESmCBCi64pPKCS5)		Forbidden	
Single-DES CBC no padding (Mech_DESmCBCpNONE))		Forbidden	

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
Single-DES ECC PKCS#5 padding (Mech_DESmEBCpPKCS5)		Forbidden	
Single-DES ECB no padding (Mech_DESmECBpNONE)		Forbidden	
Single-DES CBC-MAC PKCS#5 padding (Mech_DESmCBCMACi0pPKCS5)		Forbidden	
Single-DES CBC-MAC no padding (Mech_DESmCBCMACpNONE)		Forbidden	
2-key triple-DES key generation (KeyType_DES2)		Forbidden	
2-key triple-DES PKCS#5 padding (Mech_DES2mCBCi64pPKCS5)		Forbidden	
2-key triple-DES CBC no padding (Mech_DES2mCBCpNONE)		Forbidden	
2-key triple-DES ECC PKCS#5 padding (Mech_DES2mEBCpPKCS5)		Forbidden	
2-key triple-DESS ECB no padding (Mech_DES2mECBpNONE)		Forbidden	
2-key triple-DES CBC-MAC PKCS#5 padding (Mech_DES2mCBCMACi0pPKCS5)		Forbidden	

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
2-key triple-DES CBC-MAC no padding (Mech_DES2mCBCMACpNONE)		Forbidden	
3-key triple-DES key generation (KeyType_DES3)		Forbidden	
3-key triple-DES PKCS#5 padding (Mech_DES3mCBCi64pPKCS5)		Decrypt only	
3-key triple-DES CBC no padding (Mech_DES3mCBCpNONE)		Decrypt only	
3-key triple-DES ECC PKCS#5 padding (Mech_DES3mEBCpPKCS5)		Decrypt only	
3-key triple-DESS ECB no padding (Mech_DES3mECBpNONE)		Decrypt only	
3-key triple-DES CBC-MAC PKCS#5 padding (Mech_DES3mCBCMACi0pPKCS5)		Forbidden	
3-key triple-DES CBC-MAC no padding (Mech_DES3mCBCMACpNONE)		Forbidden	

6.5. AES (aka Rijndael)

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
AES key generation (KeyType_Rijndael)			

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
AES CBC PKCS#5 padding (Mech_RijndaelmCBCi128pPKCS5)			
AES ECB PKCS#5 padding (Mech_RijndaelmECBpPKCS5)			
AES CBC no padding (Mech_RijndaelmCBCpNONE)			
AES ECB no padding (Mech_RijndaelmECBpNONE)			
AES GCM (Mech_RijndaelmGCM) with module-generated IV			
AES GCM (Mech_RijndaelmGCM) with user-supplied IV		Forbidden	
AES GCM (Mech_AESmGCM)			
AES KWP (Mech_AESKeyWrapPadded)			
AES CMAC with PKCS#5 padding (Mech_RijndaelmCMAC)			
AES CBC-MAC with PKCS#5 padding (Mech_RijndaelmCBCMACi0pPKCS5)		Forbidden	
AES CBC-MAC with no padding (RijndaelmCBCMACi0pNONE)		Forbidden	

6.6. RC4

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
RC4 key generation (KeyType_ArcFour)		Forbidden	
RC4 encrypt/decrypt (Mech_ArcFourpNONE)		Forbidden	

6.7. SEED

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
SEED key generation (KeyType_SEED)		Forbidden	
SEED CBC PKCS#5 padding (Mech_SEEDmCBCi128pPKCS5)			
SEED ECBPKCS#5 padding (Mech_SEEDmECBpPKCS5)			
SEED CBC no padding (Mech_SEEDmCBCpNONE)			
SEED ECB no padding (Mech_SEEDmECBpNONE)			
SEED CBC-MAC PKCS#5 padding (Mech_SEEDmCBCMACi0pPKCS5)			

6.8. HMAC

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
HMAC SHA-1/2/3 key generation (KeyType_HMACSHA1, KeyType_HMACSHA224, KeyType_HMACSHA256, KeyType_HMACSHA384, KeyType_HMACSHA512, KeyType_HMACSHA3b224, KeyType_HMACSHA3b256, KeyType_HMACSHA3b384, KeyType_HMACSHA3b512)		Minimum 14 bytes (112 bits)	
HMAC SHA-1/2/3 sign/verify (Mech_HMACSHA1, Mech_HMACSHA224, Mech_HMACSHA256, Mech_HMACSHA384, Mech_HMACSHA512, Mech_HMACSHA3b224, Mech_HMACSHA3b256, Mech_HMACSHA3b384, Mech_HMACSHA3b512)			
HMAC MD5 key generation (KeyType_HMACMD5)		Forbidden	
HMACMD5 sign/verify (Mech_HMACMD5)		Forbidden	
HMAC RIPEMD160 key generation		Forbidden	
HMACRIPEMD160 sign/verify (Mech_HMACRIPEMD160)		Forbidden	

7. DeriveKey Mechanisms

7.1. Key Wrapping (see also IES variants)

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
EncryptMarshalled (DeriveMech_EncryptMarshalled, DeriveMech_DecryptMarshalled)		AESKeyWrapPadded & RSApPKCS1OAEPhSHA512 only	
AESKW non-default ICV		Forbidden (wrap & unwrap)	
Raw encryption (DeriveMech_RawEncrypt, DeriveMech_Decrypt) permitted mechanisms		AESKeyWrapPadded, RijndaelmGCM, AESmGCM, OAEP with NIST hashes	
Padded raw encryption (DeriveMech_RawEncryptZeroPad, DeriveMech_RawDecryptZeroPad)		Forbidden	
PKCS#8 wrap (DeriveMech_PKCS8Encrypt, DeriveMech_PKCS8Decrypt, DeriveMech_PKCS8DecryptEx) permitted mechanisms		AESKeyWrapPadded, RijndaelmGCM, AESmGCM, OAEP with NIST hashes	
AES Key Wrap (DeriveMech_AESKeyWrap, DeriveMech_AEKeyUnwrap) (see also Mech_AESKeyWrapPadded)			

7.2. Key Derivation

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
MAC on a key (DeriveMech_RawSign)		KeyType_Random output only	
NIST SP800-56Cr1 KDF (DeriveMech_ConcatenationKDF) with SHA1 or SHA-2			
NIST SP800-56Cr1 KDF (DeriveMech_ConcatenationKDF) with RIPEMD160 hash		Forbidden	
ANSI X9.63 KDF (DeriveMech_ConcatenationKDF)		Forbidden	
Either ConcatenationKDF with RSA key agreement (DeriveMech_ConcatenationKDF)		Forbidden	
Either ConcatenationKDF with ECDHC key agreement (DeriveMech_ConcatenationKDF)			
Either ConcatenationKDF with ECDH key agreement (DeriveMech_ConcatenationKDF) with h=1			
Either ConcatenationKDF with ECDH (DeriveMech_ConcatenationKDF) with h>1		Forbidden	
SP800-108 KDF with AES-CMAC (DeriveMech_NISTKDFmCTRpRijndaelCMACr32)			

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
SP800-108 KDF with AES-CMAC or HMAC SHA-256, HMAC SHA-384 or HMAC-384 (DeriveMech_NISTKDFmCTRr8)			
DES split/join XOR (DeriveMech_DESsplitXOR, DeriveMech_DESjoinXOR, DeriveMech_DESjoinXORsetParity, DeriveMech_DES2splitXOR, DeriveMech_DES2joinXOR, DeriveMech_DES2joinXORsetParity, DeriveMech_DES3splitXOR, DeriveMech_DES3joinXOR, DeriveMech_DES3joinXORsetParity)		Forbidden	
Random split/join XOR (DeriveMech_RandsplitXOR, DeriveMech_RandjoinXOR)			
AES split/join XOR (DeriveMech_AESsplitXOR, DeriveMech_AESjoinXOR)			
Key concatenation (DeriveMech_ConcatenateBytes)			
Public from private (DeriveMech_PublicFromPrivate)			

7.3. Key Agreement

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
ECCMQV with ANSI X9.63 KDF (DeriveMech_ECCMQV)		Forbidden	
ECCMQV with SP800-56Ar3 KDF (DeriveMech_ECCMQVdNISTCKDF)			
ECDH key agreement (DeriveMech_ECDHKA)		Forbidden	
DH key agreement (DeriveMech_DHKA)		Forbidden	
X25519 key agreement (DeriveMech_X25519KA)		Forbidden	

7.4. IES Variants

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
ECIES (DeriveMech_ECIESKeyWrap, DeriveMech_ECIESKeyUnwrap) with ECDH/ECDHC and ANSI X9.63 KDF		Forbidden	
X25519 ECIES (DeriveMech_ECIESKeyWrap, DeriveMech_ECIESKeyUnwrap)		Forbidden	

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
RSA key wrap of symmetric key (DeriveMech_RSAKeyWrap, DeriveMech_RSAKeyUnwrap) with OAEP and AES-KWP			
RSA key wrap of asymmetric key (DeriveMech_RSAKeyWrap, DeriveMech_RSAKeyUnwrap) with OAEP, AES-KWP and PKCS#8			

7.5. Rainbow

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
ARQC verification (DeriveMech_CompositeARQCVerify)		Forbidden	
Watchword sign/verify (DeriveMech_CompositeWatchWordVerify, DeriveMech_CompositeWatchWordSign)		Forbidden	

7.6. HyperLedger

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
HyperLedger client key derivation (DeriveMech_HyperledgerClient)		Forbidden	

7.7. MILENAGE

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
MILENAGEOP key generation		Forbidden	
MILENAGESubscriber key generation		Forbidden	
MILENAGERC key generation		Forbidden	
MILENAGEOPC key derivation		Forbidden	
MILENAGEAV key derivation (f1…f5)		Forbidden	
MILENAGEResync (f1s/f5s)		Forbidden	
MILENAGEGenAUTS (for testing)		Forbidden	

7.8. TUAK

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
TUAKSubscriber key generation		Forbidden	
TUAKTOP key generation		Forbidden	
TUAKf1 key derivation		Forbidden	
TUAKf1s key derivation		Forbidden	
TUAKf2345 key derivation		Forbidden	
TUAKf5s key derivation		Forbidden	

7.9. Hashing

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
SHA-1 (Mech_SHA1Hash)			
SHA-2 (Mech_SHA224Hash, Mech_SHA256Hash, Mech_SHA384Hash, Mech_SHA512Hash)			
SHA-3 (Mech_SHA3b224Hash, Mech_SHA3b256Hash, Mech_SHA3b384Hash, Mech_SHA3b512Hash)			
HAS160 (Mech_HAS160Hash)		Forbidden	
RIPEMD160 (Mech_RIPEMDS160Hash)		Forbidden	
Tiger (Mech_TigerHash)		Forbidden	

7.10. Internal Security Mechanisms

Feature	Unrestricted	FIPS 140 Level 3	Common Criteria CMTS
3DES internal security mechanisms (Mech_3DESwSHA1, Mech_3DESwCRC32)	Forbidden		
V2 Blobcrypt (AES, RSA & DH ISMs)	Forbidden		
V3 Blobcrypt (AES & RSA ISMs)	Mandatory		
Share key KDF	Mandatory	NISTKDFmCTRpRijndaelCMACr32	