Application Notes

nShield Security World Ciphersuites

04 December 2024

Table of Contents

1. Releases

Attribute	DLf1024s160mDES3	DLf1024s160mRijndael	DLf3072s256mRijndael	DLf3072s256mAEScSP800131Ar1	ECp521mAES
Introduced	Original	Old	v11.50	v12.50	Forthcoming
FIPS Firmware Versions	n/a			v12.72, v13.2, v13.4	forthcoming

2. Cryptographic Properties

Attribute	DLf1024s160mDES3	DLf1024s160mRijndael	DLf3072s256mRijndael	DLf3072s256mAEScSP800131Ar1	ECp521mAES
Overall Strength	80 bit		128 bit		
Internal Cryptography	Proprietary			FIPS-140 approved	
Internal Signatures	DSA-1024		DSA-3072		ECDSA-P521
Working Key Blobs	DES3-CBC Proprietary MAC	Proprietary KDF AES-256-CBC HMAC-SHA1		SP800-108 KDF AES-256-CBC HMAC-SHA256	
Key Recovery	RSA-1024 PKCS#1v1.5 DES3-CBC Proprietary MAC	RSA-SVE-1024 Proprietary KDF AES-CBC-256 HMAC-SHA512	RSA-SVE-3072 Proprietary KDF AES-CBC-256 HMAC-SHA512	RSA-OAEP-3072 SHA-256 SP800-108 KDF AES-CBC-256 HMAC-SHA512	ECDH-P521 SP800-56Ar2 KDF AES-CBC-CTR HMAC-SHA256
Passphrase Recovery	RSA-1024 PKCS#1v1.5		RSA-OAEP-3702 SHA-256		ECDH-P521 SP800-56Ar2 KDF AES-CBC-CTR HMAC-SHA256

3. nCore Configuration

Attribute	DLf1024s160mDES3	DLf1024s160mRijndael	DLf3072s256mRijndael	DLf3072s256mAEScSP800131Ar1	ECp521mAES
FIPS Mode Bits	FIPS140Level3			FIPSLevel3Enforcedv2 + StrictSP80056Ar3	
KML Type	DSAp1024s160		DSAp3072s256		NISTp521hSHA1
Key Hash	SHA1				
KMWK	DES3 0101...			AES-256 0000...	
HKMWK	1d572201be533ebc89f30fdd8f3fac6ca3395bf0			c2be99fe1c77f1b75d48e2fd2df8dffc0c969bcb	

4. FIPS Mode Restrictions

Attribute	DLf1024s160mDES3	DLf1024s160mRijndael	DLf3072s256mRijndael	DLf3072s256mAEScSP800131Ar1	ECp521mAES
Single-DES	Forbidden				
DES3 Encryption	Permitted			Forbidden	
DES3 Decryption	Permitted				
DES3 MAC	Permitted			Forbidden	
RSA Public Modulus	≥1024 bits			≥2048 bits	
RSA Public Exponemt	16-256 bits				
DSA Public Modulus	≥1024 bits			≥2048 bits	
DSA Group Order	≥160 bits			≥224 bits	
DSA Signature Generation	Permitted				Forbidden
DH Public Modulus	≥1024 bits			≥2048 bits	
DH Group Order	≥160 bits			≥224 bits	

Attribute	DLf1024s160mDES3	DLf1024s160mRijndael	DLf3072s256mRijndael	DLf3072s256mAEScSP800131Ar1	ECp521mAES
DH Without Group Order	Permitted			Forbidden	
ElGamal	Forbidden				
ECC Group Order	≥160 bits			≥224 bits	
Non-Cofactor ECDH	Permitted			Forbidden	
ECIES with XOR encryption	Forbidden				
ECIES with KDF2	Forbidden				
KDF2 in CKDF	Permitted			Forbidden	
SHA1 Signature	Permitted			Forbidden	
Non-default ICV with AES-KW	Permitted			Forbidden	
Non-default ICV with AES-GCM	Permitted			Forbidden	

Attribute	DLf1024s160mDES3	DLf1024s160mRijndael	DLf3072s256mRijndael	DLf3072s256mAEScSP800131Ar1	ECp521mAES
Non-approved hashes with KDFs	Permitted			Forbidden	
Unauthenticated key wrapping	Permitted			Forbidden	
Private key plaintext import	Forbidden				
Private key plaintext export	Forbidden				
Public key plaintext export	Authentication required				
KCDSA, SEED, ARIA	Forbidden				