3. Approved Algorithms

Approved algorithms are: -	**Minimum Key Size (bits)**	**Note/Comments**
Symmetric Key		
AES	128	FIPS 197; Where a choice exists, AES should be selected.
3DES/Triple DES	112/168	3-Key 3DES is recommended. Use of 2-key 3DES may continue but migration to 3-key during the next upgrade or during periodic key rotations is encouraged.
RC4	128	
RC5	128	
IDEA	128	Sunset – Use is restricted for backward compatibility reasons only.
CAST	128	Sunset – Use is restricted for backward compatibility reasons only.
Asymmetric Key	**Minimum Key Size (bits)**	**Note/Comments**
RSA	1024 (sunset) 2048 (New implementations)	➢ All new CA implementations must use a 2048 minimum key size ➢ Certificates issued from a legacy CA can continue to have a 1024 minimum key size.
DSA	1024-bit finite field/160-bit subgroup	
DH	1024	As specified in ANSI X9.42
ECDSA	160/256	As specified in ANSI X9.62 with NIST recommended curves
ECDH	160/256	As specified in ANSI X9.63

Symmetric Key **Hash**	**Minimum Key Size (bits)** **Output** (bits)	**Note/Comments** **Notes**
MD5	128	Sunset (only for backward compatibility) Link to MDS EOL
SHA-1/256/384/512	160/256/384/512	If a choice exists, SHA-256 or larger is preferred. SHA-1 as a sole hash mechanism may be sunset in the near future.

Use of any other cryptographic algorithm is prohibited.