

TDES Guidance

November 14, 2002

FIPS 46-3 approves the use of two FIPS-approved cryptographic algorithms: DES and Triple DES (TDES). DES uses a single key to perform a cryptographic operation; TDES uses three keys, one for each of three DES operations. TDES produces the same output as DES if all three keys are identical (one key TDES); TDES can also be implemented using two identical keys and a third that is different (two key TDES), or with three distinctly different keys (three key TDES). FIPS 46-3 approves TDES as the symmetric encryption algorithm of choice over DES, with DES permitted for legacy systems only. Note that another approved cryptographic algorithm is specified in FIPS 197, the Advanced Encryption Standard. FIPS 46-3 is scheduled for review in 2004 and will be revised to become FIPS 46-4. When FIPS 46-4 is signed after a public review, NIST expects that DES and one key TDES will no longer be approved for protecting new data. At that time, algorithm validation certificates of DES and one key TDES implementations that were issued prior to the signing of FIPS 46-4 by the Cryptographic Module Validation Program will expire. Algorithm validation certificates for TDES implementations with multiple keying options will remain valid for the two key and three key options. When TDES is used for protecting new data, NIST strongly recommends the use of three key TDES, as greater protection is provided for the data than is provided by two key TDES. However, NIST anticipates that the use of two key TDES will be allowed for a period of time, tentatively until 2015.