FIPS 140-2 Validation Document

June 30, 2016
Version 3.0

Introduction

The purpose of this document is to provide Cryptographic Module Validation Program (CMVP) and Cryptographic Algorithm Validation Program (CAVP) information including the NIST pages containing manufacturers and dates. This information will validate the encryption algorithms used and certificates in Xerox products.

Additional information regarding these programs can be found here:

NIST CMVP home page
http://csrc.nist.gov/groups/STM/cmvp/index.html
AES algorithm list
http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html
Triple DES algorithm list
http://csrc.nist.gov/groups/STM/cavp/documents/des/tripledesval.html
HMAC algorithm list
http://csrc.nist.gov/groups/STM/cavp/documents/mac/hmacval.html
RNG algorithm list
http://csrc.nist.gov/groups/STM/cavp/documents/rng/rngval.html
Secure Hash algorithm list
http://csrc.nist.gov/groups/STM/cavp/documents/shs/shaval.htm
RSA algorithm list
http://csrc.nist.gov/groups/STM/cavp/documents/dss/rsanewval.html
DRBG algorithm list
http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgnewval.html

Module and Algorithm Certificate Table

Product	Cryptographic Module	FIPS approved Algorithms
WorkCentre 3655, 5845/5855/5865/5875/5890, 5945/5955, 6655, 7220/7225, 7830/7835/7845/7855, 7890 with 2016 Xerox® ConnectKey® Technology WorkCentre 3655i, 5865i/5875i/5890i, 5945i/5955i, 7220i/7225i, 7830i/7835i/7845i/7855i, 7890i	OpenSSL #1747 Mocana #1614	**AES (CBC)** OpenSSL Certificate #1884 Mocana Certificate #1505 **Triple-DES (CBC)** OpenSSL Certificate #1223 Mocana Certificate #1006 **RSA** OpenSSL Certificate #960 Mocana Certificate #738 **SHA-256** OpenSSL Certificate #1655 Mocana Certificate #1333 **HMAC** OpenSSL Certificate #1126 Mocana Certificate #885 **DRBG** OpenSSL Certificate #157 Mocana Certificate #64
ColorQube 8700/8900, 9301/9302/9303 with Xerox® ConnectKey® 1.5 Technology WorkCentre 3655, 5845/5855/5865/5875/5890, 5945/5955, 6655, 7220/7225, 7830/7835/7845/7855, 7890 with Xerox® ConnectKey® 1.5 Technology	OpenSSL #1051 Mocana #1276	**AES (CBC)** OpenSSL Certificate #1821 Mocana Certificate #1131 **Triple-DES (CBC)** OpenSSL Certificate #1174 Mocana Certificate #826 **RSA** OpenSSL Certificate #914 Mocana Certificate #538 **SHA-256** OpenSSL Certificate #1599 Mocana Certificate #1055 **HMAC** Mocana Certificate #644
WorkCentre 7120/7125 WorkCentre 7425/7428/7435 WorkCentre 5325/5330/5335	RSA Bsafe #828	AES Certificate #490 DSA Certificate #199 ECDSA Certificate #47 HMAC Certificate #244 RNG Certificate #270 RSA Certificate #203 SHS Certificate #560 Triple-DES Certificate #501

Product	Cryptographic Module	FIPS approved Algorithms
WorkCentre 7525/7530/7535/7545/7556 ColorQube 9301/9302/9303 WorkCentre 5735/5740/5745/5755/5765/5775/5790	Mocana #1273	AES Certificate #1131 AES Certificate #1132 AES Certificate #1133 AES Certificate #1134 Triple-DES Certificate #826 SHS Certificate #1055 HMAC Certificate #644 RNG Certificate #629
	Datacryptor #1276	AES Certificate #1131 AES Certificate #1132 AES Certificate #1133 AES Certificate #1134 Triple-DES Certificate #826 SHS Certificate #1055 HMAC Certificate #644 RSA Certificate #538 DSA Certificate #369 ECDSA Certificate #134 RNG Certificate #629
	OpenSSL #1051	Triple-DES Certificate #627 AES Certificate #695 DSA Certificate #264 SHS Certificate #723 HMAC Certificate #373 RSA Certificate #323 RNG Certificate #407
WorkCentre 5632/5638/5665/5675/5687/5690 WorkCentre 5135/5150		AES Certificate #1471 TDES Certificate #990 AES Certificate #1472 SHS Certificate #1331 RSA Certificate #719

Table 1