Bulletin

National Guidance for Use of Rights Management Services (RMS)

OVERVIEW

Microsoft's **Rights Management Services** (RMS) is a security tool embedded in Exchange and Windows server products, that provides the ability to protect sensitive but unclassified information during transmission. RMS has been in production use in VA since approximately 2007. According to Microsoft, (https://technet.microsoft.com/en-us/library/hh831364%28v=ws.11%29.aspx), RMS is compliant, and has been validated, with Federal Information Processing Standard (FIPS) 140-2 for cryptographic modules.

GUIDANCE

VA Handbook 6500, SC-13, Cryptographic Protection -- OI&T requires that the information system implements cryptographic uses and type of cryptography required for each use in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, and standards:

(a) When cryptography is required and employed within information systems, OI&T must comply with applicable Federal laws, policies, regulations, standards, and guidance, including FIPS 140-2 (or its successor) validated encryption which requires the system to perform all cryptographic operations (including key generation) using FIPS 140-2 (or its successor) validated cryptographic modules operating in approved modes of operation.

(b) VA sensitive information must be encrypted during transmission and at rest when outside of VA-owned or managed facilities (e.g., medical centers, CBOCs, regional offices, etc.).

Since RMS is FIPS 140-2 compliant and validated, which complies with VA's requirement for cryptography, RMS can be used to protect VA sensitive information internally and externally.

POINT OF CONTACT

Prince K. Lamptey
630-667-6572   Prince.Lamptey@va.gov

Office of Information Security
Field Security Service