

## Media Encryption Security Features Checklist

### Core Security Functionality

Hard Drive Encryption  
 Saved Files  
 Temporary Files  
 Page Files  
 Deleted Files  
 Secure File Deletion  
 Registry or Operating System  
 Boot Files  
 Unused Sectors  
 Hidden Partitions  
 Hibernation Mode  
 Logout / Lockout  
 Non-Magnetic Drives  
 Removable Drives  
 Data Recovery by  
 Administrator

### Conformance to Protocol Standards

Password Management /  
 Recovery (Admin)  
 PKI Authentication  
 Multifactor Authentication  
 Revocation of Access

### PKI Standards

X.509 Certificates  
 LDAP Repository  
 Certificate Revocation  
 Cryptographic Algorithms

### Cryptographic Standards

#### *Encryption Algorithms*

Advanced Encryption  
 Standard (AES)  
 Triple- Data Encryption  
 Standard (3DES)

#### *Key Establishment Algorithms*

Rivest, Shamir, Adleman  
 (RSA)  
 Other algorithms based on  
 exponentiation of finite fields  
 Key Exchange Algorithm  
 (KEA)  
 Elliptic Curve algorithms

#### *Digital Signature Algorithms*

RSA  
 Digital Signature Algorithm  
 (DSA)  
 Other algorithms based on  
 exponentiation of finite fields  
 Elliptic Curve Digital  
 Signature Algorithm (ECDSA)

#### *Hashing Algorithms*

SHA-1  
 SHA-224  
 SHA-256  
 SHA-384  
 SHA-512

### Assurance Standards

FIPS 140-1  
 FIPS 140-2

### Cryptographic Algorithm Validation Program

Cryptographic module  
 validated

### Configurability

Changeable Default Values  
 Multiple Users  
 Different User Access Rights  
 Transaction Logging  
 Log Integrity  
 Log Centralization  
 Security Alerts

### Usability

Configuration by Users  
 Authentication by Users  
 Interruptions during Initial  
 Encryption Process  
 Computer use during Initial  
 Encryption Process  
 Software /Hardware  
 Compatibility  
 Maintenance by  
 Administrators  
 Administrator Recovery  
 Third Party Recovery

### Manageability

Central Management  
 Remote Management  
 Unattended Reboot  
 Authentication of  
 Management Traffic  
 Encryption of Management  
 Traffic

### Scalability

Degree of Scalability