



S T A T E O F M A R Y L A N D  
DEPARTMENT OF INFORMATION TECHNOLOGY

## **Encryption Standard**

Agencies must ensure that encryption is utilized to protect any nonpublic information when it is stored or transmitted through any environment. IT Systems employing encryption must comply with all applicable Federal Information Processing Standards (FIPS) publications and guidelines for encryption (Reference <http://csrc.nist.gov/publications/fips/> for guidance).

To help accomplish this each agency using encryption must establish at a minimum the following:

- Secure cryptographic keys;
- Use of Public Key Cryptography methods approved by the State CIT;
- All cryptographic keys must have a designated, unique owner.

Key change intervals shall be established by each agency, but must be no longer than the following:

- Master keys must be changed once per year, if the product allows;
- Key encrypting keys (e.g., asymmetric or symmetric) must be changed at a minimum of every six (6) months;
- Link encrypting keys must be changed every six (6) months.

Keys must be distributed in a secure manner ensuring that the entire key is not exposed while in transit to any one individual at any one time.

Default cryptographic keys may not be utilized. Exceptions are for emergency recovery, system calibration or vendor certification purposes. In such cases, a documented process describing the storage, maintenance, use and destruction of these keys must be in place.

### **Public Key Technology (Asymmetric)**

All public key management systems, Certificate Authorities (CAs), key distribution systems, key recovery systems, and cross-certification processes must be approved by the

State CIT. Every public key and certificate must have an associated scope of use, which must be checked by any user or server that accepts or relies upon the certificate.

The process for issuing digital certificates must:

- Establish the identity of the subject;
- Establish that the subject is the holder of the associated private keys;