Requirements and Testing Procedures		Guidance
3.6 Cryptographic keys used to protect stored account data are secured.		
Defined Approach Requirements **3.6.1** Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms. **Customized Approach Objective** Processes that protect cryptographic keys used to protect stored account data against disclosure and misuse are defined and implemented. **Applicability Notes** This requirement applies to keys used to encrypt stored account data and to key-encrypting keys used to protect data-encrypting keys. The requirement to protect keys used to protect stored account data from disclosure and misuse applies to both data-encrypting keys and key-encrypting keys. Because one key-encrypting key may grant access to many data-encrypting keys, the key-encrypting keys require strong protection measures.	**Defined Approach Testing Procedures** **3.6.1** Examine documented key-management policies and procedures to verify that processes to protect cryptographic keys used to protect stored account data against disclosure and misuse are defined to include all elements specified in this requirement.	**Purpose** Cryptographic keys must be strongly protected because those who obtain access will be able to decrypt data. **Good Practice** Having a centralized key management system based on industry standards is recommended for managing cryptographic keys. **Further Information** The entity's key management procedures will benefit through alignment with industry requirements, Sources for information on cryptographic key management life cycles include: • *ISO 11568-1 Banking — Key management (retail) — Part 1*: Principles (specifically Chapter 10 and the referenced Parts 2 & 4) • *NIST SP 800-57 Part 1 Revision 5— Recommendation for Key Management, Part 1: General*.