Requirements and Testing Procedures		Guidance
3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Use of strong cryptographic keys significantly increases the level of security of encrypted account data. **Further Information** See the sources referenced at "Cryptographic Key Generation in *Appendix G*.
3.7.1 Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	**3.7.1.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define generation of strong cryptographic keys.	
	3.7.1.b Observe the method for generating keys to verify that strong keys are generated.	
Customized Approach Objective		
Strong cryptographic keys are generated.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Secure distribution or conveyance of secret or private cryptographic keys means that keys are distributed only to authorized custodians, as identified in Requirement 3.6.1.2, and are never distributed insecurely.
3.7.2 Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	**3.7.2.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define secure distribution of cryptographic keys.	
	3.7.2.b Observe the method for distributing keys to verify that keys are distributed securely.	
Customized Approach Objective		
Cryptographic keys are secured during distribution.		