Requirements and Testing Procedures		Guidance
4.2 PAN is protected with strong cryptography during transmission.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Sensitive information must be encrypted during transmission over public networks because it is easy and common for a malicious individual to intercept and/or divert data while in transit. **Good Practice** The network and data-flow diagrams defined in Requirement 1 are useful resources for identifying all connection points where account data is transmitted or received over open, public networks. While not required, it is considered a good practice for entities to also encrypt PAN over their internal networks, and for entities to establish any new network implementations with encrypted communications. PAN transmissions can be protected by encrypting the data before it is transmitted, or by encrypting the session over which the data is transmitted, or both. While it is not required that strong cryptography be applied at both the data level and the session level, it is strongly recommended. If encrypted at the data level, the cryptographic keys used for protecting the data can be managed in accordance with Requirements 3.6 and 3.7. If the data is encrypted at the session level, designated key custodians should be assigned responsibility for managing transmission keys and certificates. *(continued on next page)*
4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. *This bullet is a best practice until its effective date; refer to applicability notes below for details.* • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.	**4.2.1.a** Examine documented policies and procedures and interview personnel to verify processes are defined to include all elements specified in this requirement. **4.2.1.b** Examine system configurations to verify that strong cryptography and security protocols are implemented in accordance with all elements specified in this requirement. **4.2.1.c** Examine cardholder data transmissions to verify that all PAN is encrypted with strong cryptography when it is transmitted over open, public networks. **4.2.1.d** Examine system configurations to verify that keys and/or certificates that cannot be verified as trusted are rejected.	
Customized Approach Objective		
Cleartext PAN cannot be read or intercepted from any transmissions over open, public networks.		