Requirements and Testing Procedures		Guidance
3.5 Primary account number (PAN) is secured wherever it is stored.		
Defined Approach Requirements **3.5.1** PAN is rendered unreadable anywhere it is stored by using any of the following approaches: • One-way hashes based on strong cryptography of the entire PAN. • Truncation (hashing cannot be used to replace the truncated segment of PAN). – If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN. • Index tokens. • Strong cryptography with associated key-management processes and procedures. **Customized Approach Objective** Cleartext PAN cannot be read from storage media. **Applicability Notes** It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs) must all be protected. This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN.	**Defined Approach Testing Procedures** **3.5.1.a** Examine documentation about the system used to render PAN unreadable, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the methods specified in this requirement. **3.5.1.b** Examine data repositories and audit logs, including payment application logs, to verify the PAN is rendered unreadable using any of the methods specified in this requirement. **3.5.1.c** If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	**Purpose** The removal of cleartext stored PAN is a defense in depth control designed to protect the data if an unauthorized individual gains access to stored data by taking advantage of a vulnerability or misconfiguration of an entity's primary access control. Secondary independent control systems (for example governing access to, and use of, cryptography and decryption keys) prevent the failure of a primary access control system leading to a breach of confidentiality of stored PAN. If hashing is used to remove stored cleartext PAN, by correlating hashed and truncated versions of a given PAN, a malicious individual can easily derive the original PAN value. Controls that prevent the correlation of this data will help ensure that the original PAN remains unreadable. **Further Information** For information about truncation formats and truncation in general, see PCI SSC's FAQs on the topic. Sources for information about index tokens include: • PCI SSC's Tokenization Product Security Guidelines (*https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf*) • *ANSI X9.119-2-2017: Retail Financial Services - Requirements For Protection Of Sensitive Payment Card Data - Part 2: Implementing Post-Authorization Tokenization Systems*