PCI DSS v4.0 变更系列之五

——第二大类要求点

要求点变更的说明之第二大类：保护账户数据

要求3：保护所存储的账户数据

该章节主要求中重申了对于非永久存储位置的账户数据应进行妥善的控制，使用完成后应立即删除。如变为永久存储，应按要求进行加密保护。

要求3.3.2增加了对授权完成前的敏感认证数据存储的强加密保护。

要求3.4.2限制远程访问时对卡号的拷贝与移动，要求通过技术手段进行限制。

要求3.5.1.1增加了对哈希算法中用到的密钥的安全管理要求。

要求3.7.9涉及共享密钥时对密钥的指导。

请注意：标准3.3.1-3.3.2和3.5.1.1禁止使用定制化验证方法（customized approach）

v4.0要求点的英文原文	对应的v3.2.1要求	与v3.2.1的变化/新要求说明
3.1 Processes and mechanisms for protecting stored account data are defined and understood.		
3.1.1 All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	3.7	在原3.7要求的基础上，增加了策略和流程需要保持更新的要求。
3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	新要求	记录、分配及理解执行要求3的管理活动所对应的角色及职责。
3.2 Storage of account data is kept to a minimum.		
3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Limiting data storage amount and retention	3.1	对原3.1的要求进行了强化，强调了对所有存储的持卡人数据位置的覆盖。 此处也增加了新的要求点，要求维护授权完成前的敏感认证数据的存储情况。

time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.		
3.3 Sensitive authentication data (SAD) is not stored after authorization.		
3.3.1 SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.		
3.3.1.1 The full contents of any track are not retained upon completion of the authorization process.	3.2.1	对原 3.2.1 的要求重新进行了描述。
3.3.1.2 The card verification code is not retained upon completion of the authorization process.	3.2.2	对原 3.2.2 的要求重新进行了描述。
3.3.1.3 The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.	3.2.3	对原 3.2.3 的要求重新进行了描述。
3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	新要求	要求敏感认证数据在完成授权前进行强加密存储保护。
3.3.3 ***Additional requirement for issuers and companies that support issuing services and store sensitive authentication data:*** Any storage of sensitive authentication data is: • Limited to that which is needed for a legitimate issuing business need and is secured. • Encrypted using strong cryptography. *This bullet is a best practice until its effective*	3.2.a 3.2.b	在原 3.2.a-3.2.b 要求的基础上，把对涉及发卡业务的机构对敏感认证数据的存储要求独立为一个要求点。 要求存储的敏感认证数据最小化，并进行强加密存储保护。

date; refer to Applicability Notes below for details.		
3.4 Access to displays of full PAN and ability to copy PAN is restricted.		
3.4.1 PAN is masked when displayed (the BIN and last four digits **are the maximum number** of digits to be displayed), such that only personnel with a legitimate business need can see **more than** the BIN and last four digits of the PAN.	3.3	将原3.3要求的至多前6后4的显示要求，调整为至多显示卡BIN和后4，更适用于当前卡号位置的实际情况。
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.	12.3.10	该要求参照了原12.3.10的要求，明确提出除了有明确的业务需要的情况外，实施技术手段限制卡号的拷贝与移动。
3.5 Primary account number (PAN) is secured wherever it is stored.		
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.	3.4	把原3.4要求中提及的“index tokens and pads”中的“pads“进行了移除，其它的内容保持不变。
3.5.1.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.	新要求	在使用哈希进行存储保护时，要求使用带密钥的哈希，并将密钥进行密钥管理（参见要求3.6-3.7）。

3.5.1.2 If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media **OR** • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.	新要求	对使用磁盘/分区级别的数据加密卡号的情况，限定于可移动电子介质。如用于非可移动电子介质，应参考 3.5.1 进行额外的强加密保护。
3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.	3.4.1	在原 3.4.1 的要求上，增加了对用于访问磁盘/分区中解密后数据的认证因素（如密码、密钥等）进行安全的存储。
3.6 Cryptographic keys used to protect stored account data are secured.		
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.	3.5	对原 3.5 的要求重新进行了描述。
3.6.1.1 ***Additional requirement for service providers only:*** A documented description of the cryptographic architecture is maintained that includes: • Details of all algorithms, protocols, and keys used for the protection of stored	3.5.1	在原 3.5.1 加密架构文档的基础上，增加了防止同一密钥同时在生产和测试环境使用的要求。

account data, including key strength and expiry date. • Preventing the use of the same cryptographic keys in production and test environments. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Description of the key usage for each key. • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.		
3.6.1.2 Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device. • As at least two full-length key components or key shares, in accordance with an industry-accepted method.	3.5.3	对原 3.5.3 的要求重新进行了描述。
3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	3.5.2	对原 3.5.2 的要求重新进行了描述。
3.6.1.4 Cryptographic keys are stored in the fewest possible locations.	3.5.4	对原 3.5.4 的要求重新进行了描述。
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.		
3.7.1 Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	3.6.1	对原 3.6.1 的要求重新进行了描述。

3.7.2 Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	3.6.2	对原 3.6.2 的要求重新进行了描述。
3.7.3 Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	3.6.3	对原 3.6.3 的要求重新进行了描述。
3.7.4 Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: • A defined cryptoperiod for each key type in use. • A process for key changes at the end of the defined cryptoperiod.	3.6.4	对原 3.6.4 的要求重新进行了描述。
3.7.5 Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.	3.6.5	对原 3.6.5 的要求重新进行了描述。
3.7.6 Where manual cleartext cryptographic key- management operations are performed by personnel, key-management policies and procedures are implemented include	3.6.6	对原 3.6.6 的要求重新进行了描述。

managing these operations using split knowledge and dual control.		
3.7.7 Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.	3.6.7	对原 3.6.7 的要求重新进行了描述。
3.7.8 Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	3.6.8	对原 3.6.8 的要求重新进行了描述。
3.7.9 *Additional requirement for service providers only:* Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider’s customers.	新要求	针对服务供应商分享密钥给客户用于账户数据的存储与传输时，要求记录并发布相应的指导文档，指导密钥的传输、存储及密钥的更新。

要求 4：在开放的公共网络上传输过程中使用强效加密保护持卡人数据

要求 4 针对主账号的传输保护，进一步澄清了机构的内网与涉卡范围的持卡人数据有数据传输时，将使得这个内网需要进行 PCI DSS 要求的审核。同时也澄清了主账号的传输可以在数据层面，也可以在会话层面，并推荐两个层面均实施保护。

v4.0 要求点的英文原文	对应的 v3.2.1 要求	与 v3.2.1 的变化/新要求说明
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.		
4.1.1 All security policies and operational procedures that are identified in Requirement 4 are: • Documented. • Kept up to date. • In use.	4.3	在原 4.3 要求的基础上，增加了策略和流程需要保持更新的要求。

• Known to all affected parties.		
4.1.2 Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.	新要求	记录、分配及理解执行要求 4 的管理活动所对应的角色及职责。
4.2 PAN is protected with strong cryptography during transmission.		
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.	4.1	在原 4.1 要求的基础上，增加了适用于保护主账号传输的证书的要求，要求证书处于有效状态，不应处于过期或调销状态。 在支持安全的协议和配置方面，强化了不允许回退到不安全版本、算法及实现的情况。
4.2.1.1 An inventory of the entity’s trusted keys and certificates used to protect PAN during transmission is maintained.	新要求	要求对用于主账号传输保护的密钥和证书进行维护。
4.2.1.2 Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	4.1.1	对原 4.1.1 的要求重新进行了描述。
4.2.2 PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.	4.2	对原 4.2 的要求重新进行了描述。