WHITE PAPER

Complying with the Payment Card Industry Data Security Standard

For retailers, financial institutions, payment processors, and a range of other organizations that store or access payment card information, and the service providers that enable their businesses, compliance with the Payment Card Industry Data Security Standard (PCI DSS) is a critical mandate. This paper looks in detail at many of the vital requirements PCI DSS sets out for securing sensitive cardholder data, and it reveals how specific SafeNet Identity and Data Protection solutions from Gemalto can help address these requirements.

Since Visa first rolled out its Cardholder Information Security Program (CISP) in 2001, organizations that manage cardholder data have been given detailed guidelines for securing their infrastructure and ultimately the payment data they manage. While these guidelines aren't new, organizations' technological environments and the threats that have to be combatted have changed dramatically in recent years. Further, the industry's guidelines continue to evolve, with the most recent release of PCI DSS, version 3.2, taking effect in July, 2018.

The following section provides a brief introduction to relevant SafeNet solutions. The paper then looks at several specific requirements from the latest version of PCI DSS, and illustrates how Gemalto can help address these mandates.

Introduction to SafeNet Solutions

While the PCI DSS features rules on everything from changing employee passwords regularly to deploying firewalls, many rules focus on the security of stored cardholder data and the systems used to manage it. Gemalto can help address many of the critical challenges of addressing these PCI DSS standards. Further, SafeNet solutions help organizations take a comprehensive, data-centric approach to security that not only helps address near-term compliance objectives but ensures the security of sensitive assets in the long term. SafeNet solutions are efficient, flexible, and adaptable, enabling businesses to address dynamic security threats and evolving business objectives.

Gemalto provides the best technologies, expertise and services available for securing a complete infrastructure: network, users, data, software, at the core and at the edge. From the physical and virtual datacenter to cloud-enabled environments, Gemalto helps organizations remain secure, compliant, and in control. Following is a brief introduction to several of the most relevant SafeNet offerings:

Transaction Protection and Key Management

- SafeNet Hardware Security Modules (HSMs). SafeNet HSMs provide reliable protection for transactions, identities, and applications by securing cryptographic keys and provisioning encryption, decryption, authentication, and digital signing services. PCI DSS-regulated organizations can use SafeNet HSMs to do code signing of the hardware payment device in point-to-point encryption implementations and software used in payment applications to comply with the Payment Application Data Security Standard (PA-DSS). SafeNet HSMs offer a cost-effective PKI solution for the production of PCI-certified payment terminals, and incorporate features developed through extensive operational experience, implementing best practices in hardware, software, and operations that make the deployment of secure HSMs as easy as possible. Offering dedicated hardware key management to protect sensitive cryptographic keys from attack, SafeNet HSMs ensure the integrity and protection of encryption keys used to seed PCI-POI devices and sign firmware updates throughout the key lifecycle.
- SafeNet KeySecure. SafeNet KeySecure can centrally, efficiently, and securely manage cryptographic keys and policies—across the key management lifecycle, throughout the enterprise, and within virtualized data centers and public cloud environments.

Data Encryption Solutions

- SafeNet ProtectApp. SafeNet ProtectApp offers robust encryption of data at the application layer, including the industry's most widely used Web application servers and enterprise applications. The solution is deployed in combination with SafeNet KeySecure for centralized key and policy management.
- SafeNet ProtectDB. SafeNet ProtectDB delivers transparent column level encryption of sensitive data stored in databases, both in the data center and the cloud. The solution is deployed in combination with SafeNet KeySecure for centralized key and policy management.
- SafeNet ProtectFile. SafeNet ProtectFile provides transparent file encryption on servers' on-premises, in the cloud or in virtualized environments. The solution is deployed in combination with SafeNet KeySecure for centralized key and policy management.
- SafeNet ProtectV. SafeNet ProtectV provides full disk encryption of virtual machines so you can securely run even your most sensitive workloads or any highly regulated data in the cloud. Whether using Amazon Web Services, Microsoft Azure, IBM SoftLayer Cloud, or VMware, SafeNet ProtectV ensures cloud-enabled security. The solution is deployed in combination with SafeNet KeySecure to enable enterprises to maintain complete ownership and control of their encryption keys and keep high-value assets isolated and safeguarded from the cloud service provider, tenants in shared environments, and any other unauthorized party.
- SafeNet Tokenization. SafeNet Tokenization protects sensitive data by replacing it with a unique token that is securely stored, processed and can be transmitted across the organization. The solution is deployed in combination with SafeNet KeySecure to provide a single, centralized interface for logging, auditing, and reporting access to protected data, keys, and tokens.
- SafeNet High Speed Encryptors. SafeNet High Speed Encryptors (HSE) provide proven high-assurance Layer 2 network security for your sensitive data, real-time video and voice, as it moves across virtual and physical networks, between data centers, to the last mile, and up to the cloud and back again.
  SafeNet HSE are certified FIPS 140-2 L3, Common Criteria, NATO, UC APL, CAPS. The solutions ensure maximum network performance, near-zero overhead, microsecond latency with "set and forget" management and low total cost of ownership. High-assurance vulnerability protection ensures true end-to-end, authenticated encryption and state-of-the-art client side key management.

Authentication and Access Control

- SafeNet Authentication Solutions. Offering the broadest range of authentication methods and form factors, SafeNet authentication solutions allows customers to address numerous use cases, assurance levels, and threat vectors with unified, centrally managed policies—managed from one authentication back end delivered in the cloud or on-premises. Supported authentication methods include context-based authentication combined with step-up capabilities, OOB, one-time password (OTP), and X.509 certificate-based solutions. All authentication methods are available in numerous form factors, including smart card, USB token, software, mobile app, and hardware tokens.

Professional Services

New internal polices and regulatory compliance mandates evolve each day, including PCI DSS. The challenge is to stay ahead and to put a system in place that satisfies the existing regulations and future proofs your solutions for tomorrow. Gemalto Professional Services can help your organization develop a plan that incorporates both internal policies and external requirements, as well as develop a blueprint framework that you can leverage to meet PCI DSS and other regulatory requirements.

Regulations	How Gemalto Addresses
Requirement 2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.	Designed to protect key material from other tenants on the appliance—meaning different functions can leverage the same appliance without fear of losing keys to other tenants—SafeNet Network HSM can be separated into one-hundred cryptographically isolated partitions, with each partition acting as if it was an independent HSM. This provides a tremendous amount of scalability and flexibility, as a single HSM can act as the root of trust that protects the cryptographic key lifecycle of twenty dependent applications. SafeNet encryption solutions from Gemalto enable multi-tenancy and separation of duties to ensure that only authorized users can access the secure data. As the PCI Security Standards Council's virtualization guidelines state, "VMs that are not active (dormant or no longer used) could still house sensitive data such as authentication credentials, encryption keys, or critical configuration information. Inactive VMs containing payment card data can become unknown, unsecured data stores, which are often only rediscovered in the event of a data breach."1 In virtualized or cloud-enabled environments, it can be difficult to securely and permanently delete cardholder data. In these environments, virtual machine image snapshots are created and automated operations routinely backup or move virtual workloads to other host systems. This proliferation of images can ultimately pose a significant exposure. Virtual machines, whether in the cloud, virtualized or on-premises data centers can be susceptible to an array of threats, including unauthorized copying, administrators exploiting super user privileges, and more. Gemalto provides appliances (hardware and virtual security appliances) that ensure dedicated security. SafeNet ProtectV enables organizations to encrypt entire virtual machines, and secure them against such threats. Security teams can logically separate the virtual images that hold sensitive data from other images in the environment, and so guard against inadvertent data commingling—even in multi-tenant cloud environments. In addition, the solution enables organizations to implement granular access controls that mitigate the threat of potential hackers who might breach cloud hypervisors, and from the cloud super-users who administer the virtual environment. With SafeNet ProtectV, organizations can delete a key and all the associated data in partitions, operating systems, and swap partitions will be rendered unreadable. In addition, SafeNet ProtectV offers comprehensive capabilities for ensuring the secure storage and removal of cardholder data: All data is encrypted, even in snapshots and backups > All copies and snapshots of virtual machine instances are tracked > It is impossible to instantiate without authorized access > Audit trail of actions pertaining to all copies of data Administrators can revoke privileges, keys, and access in case of a breach In addition, with SafeNet KeySecure or SafeNet Virtual KeySecure, organizations can centrally manage encryption keys used to protect sensitive data in virtualized and cloud environments. By retaining central control over keys, security teams can enforce policies for isolating server instances in virtualized and cloud environments. 1 PCI Security Standards Council, "Information Supplement: PCI DSS Virtualization Guidelines", Version: 2.0, Virtualization Special Interest Group, https://www.pcisecuritystandards.org /documents/Virtualization_InfoSupp_v2.pdf
Requirement 2.2.3 Implement additional security features for any required services, protocols, or daemons that are consider to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	Operating at Layer 2 of the network stack, SafeNet High Speed Encryptors (HSE) encrypt all data that traverses an open network. All the appliances use strong cryptography and are certified FIPS 140-2 L3 and Common Criteria.

Requirement 2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	If remote administrative access isn't encrypted, highly sensitive information, including administrators' IDs and passwords can be exposed. This is particularly critical when it comes to administrators accessing critical encryption and key management platforms. SafeNet solutions have been architected to eliminate these security gaps. For example, all remote administrative access to the SafeNet KeySecure server web-based management interface is secured using TLS. TLS (transport layer security). Gemalto appliances' non-console administrative access is encrypted to prevent unauthorized access. In addition, SafeNet HSMs can protect TLS server keys and certificated used by products with web-based management, and SafeNet Authentication solutions can be used to provide even greater levels of security for non-console administrative access.
Requirement 2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data.	SafeNet solutions enable clear and secure distinction between different clients even in multi-tenant, shared environments.
Requirement 3 Protect stored cardholder data	Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Gemalto delivers a variety of encryption solutions that support standard, robust algorithms to ensure the security of sensitive data. These solutions can encrypt cardholder data in files, folders, applications, databases in both traditional and cloud or virtualized environments. Additionally, Gemalto offers solutions that can apply transparent encryption to lock down stored cardholder data as follows: > Sensitive data stored in files and folder can be secured with SafeNet ProtectFile > Sensitive data stored at the column level in databases can be secured with SafeNet ProtectDB > Sensitive data can be secured as it is generated or first processed by an application with SafeNet ProtectApp These solutions are all deployed in tandem with SafeNet KeySecure for centralized and secure key and policy management. Gemalto also offers a tokenization solution that complements these encryption capabilities. This format preserving tokenization technology converts the PAN (primary account number) to a token in the same format, allowing associated applications to operate seamlessly. As a result, tokenization is transparent to end-user operations, while keeping encrypted information secure in one central location. As a result, organizations can effectively and efficiently reduce the scope of their PCI DSS audits. The solution replaces sensitive data in databases and applications with token values, resulting in fewer servers to audit.
Requirement 3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: > One-way hashes based on strong cryptography, (hash must be of the entire PAN) > Truncation (hashing cannot be used to replace the truncated segment of PAN) > Index tokens and pads (pads must be securely stored) > Strong cryptography with associated key-management processes and procedures.	Gemalto's data-centric approach to data security means that once data is encrypted at the primary site, it is automatically secured when replicated to disaster recovery sites and archives. SafeNet KeySecure manages keys for a variety of encryption products including databases, file servers, tokenization, applications and self-encrypting drives, tape archives, Storage Area Networks, virtual workloads, and a growing list of vendors supporting the OASIS KMIP standard. Without access to the keys, the data is unreadable regardless of where it is stored. SafeNet ProtectV, a full disk encryption solution for virtual machines, specifically addresses logical access, and the use of SafeNet KeySecure addresses the non-association of keys and user accounts necessary to ensure strong key management, secure processes and outlined procedures. Gemalto's portfolio of encryption solutions enable standards-based encryption and support strong encryption algorithms, including 3DES and AES. In addition, by supporting encryption of unstructured files, columns in databases, applications, and more, these solutions enable organizations to granularly protect PCI DSS-regulated records and files, and ensure they remain encrypted even as they are saved to external storage media, USB drives, and other devices. SafeNet Tokenization also supports requirement 3.4, rendering PAN unreadable by replacing it with token values.

Requirement 3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse	SafeNet KeySecure from Gemalto is the industry's leading platform for the centralized management and security of encryption keys supporting a broad encryption ecosystem—encompassing Gemalto and third-party products—for the protection of sensitive data in databases, file servers and storage, virtual workloads, and applications across traditional and virtualized datacenters and public cloud environments. Only Gemalto delivers enterprise key management in flexible deployment options spanning FIPS 140-2 Level 3 or 2 validated hardware appliances and hardened virtual appliances supporting a hardware root of trust using SafeNet Network Hardware Security Modules (HSM) or through a service such as the Amazon CloudHSM.
Requirement 3.5.1 3.5.1 Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date Description of the key usage for each key Inventory of any HSMs and other SCDs used for key management Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	SafeNet Data Protection solutions detailed logging and reporting capabilities enable service providers to maintain and manage their cryptographic architecture and ensure compliance with PCI DSS and other regulatory requirements.
Requirement 3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	SafeNet KeySecure centralizes the storage and management of keys on a single, dedicated security appliance—where all keys are stored encrypted and integrity-checked within the platform, and are never available in plaintext to anyone. Access to keys may be restricted to designated key owners or groups of SafeNet KeySecure users. More granular levels of permissions may also be granted via SafeNet KeySecure's centralized policy management capabilities.
Requirement 3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data 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 (such as a host 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	With SafeNet KeySecure, keys are encrypted using a multi-layered hierarchy of key encryption keys. The SafeNet KeySecure k460 appliance features an HSM that adheres to the FIPS 140-2 Level 3 standard, which supports U.S. government requirements for ensuring that key management is tamper resistant. In addition, SafeNet Hardware Security Modules (HSM) integrate with several database encryption partners in order to store the encryption keys in a hardware based appliance.
Requirement 3.5.4 Store cryptographic keys in the fewest possible locations.	SafeNet KeySecure centralizes the storage and management of encryption keys on a single appliance (or more typically an integrated cluster of dedicated security appliances) —where all keys are stored encrypted and integrity checked within the platform. Further, SafeNet KeySecure can function as a central key manager for multiple encryption platforms, including those from Gemalto, as well as a number of third parties.

Requirement 3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: > 3.6.1 Generation of strong cryptographic keys > 3.6.2 Secure cryptographic key distribution > 3.6.3 Secure cryptographic key storage > 3.6.4 Cryptographic key changes for keys that have reached the end of their crypto period (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57). > 3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. > 3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. > 3.6.7 Prevention of unauthorized substitution of cryptographic keys. > 3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	SafeNet KeySecure delivers granular authorization controls for roles and permissions for key management, creation, and administration. In addition, these robust appliances support separation of duties for privileged users; for example, enabling organizations to set up policies so that no single administrator can make a critical configuration changes without additional approvals from other administrators. This enables enforcement of data access based on user privileges, job responsibilities, and data location, securing against rogue admins, and ensuring compliance. In the case of a service provider, it enables the provider to ensure their customers that only the customer has access to the keys, and therefore the data too. The SafeNet KeySecure appliance features the SafeNet PCIe HSM, a FIPS 140-2 Level 3 compliant module that supports U.S. government requirements for ensuring that key management is tamper resistant. Following are some additional details around how SafeNet KeySecure addresses specific requirements: 3.6.1—Using SafeNet KeySecure administration tools, either via CLI or admin GUI, administrators can generate strong keys using the hardware-based random number generation capabilities provided by the cryptographic accelerators on the SafeNet KeySecure device. The steps and procedures involved can easily be included in any security policy procedures. 3.6.2— SafeNet KeySecure provides full lifecycle key support and automated operations. The solution simplifies the management of encryption keys across the entire lifecycle including secure key generation, storage and backup, key distribution and key deactivation and deletion. For endpoint applications requiring key distribution, encryption keys can be securely delivered and distributed from the key manager to the local application with SafeNet Data Protection Solutions from Gemalto. 3.6.3—Keys are always stored securely on the SafeNet KeySecure platform. Encryption keys themselves are encrypted using a multi-layered hierarchy of key encryption keys. With the SafeNet KeySecure appliance, encryption keys are stored in a tamper-resistant hardware security module (HSM). 3.6.4— SafeNet KeySecure centrally manages the cryptographic keys and policies—across the key management lifecycle, throughout the enterprise, and within virtualized data centers and public cloud environments. SafeNet KeySecure provides a key rotation mechanism that allows customers to efficiently rotate keys according to security policy. 3.6.5—Keys are always stored on the SafeNet KeySecure device in an encrypted form. SafeNet KeySecure centralized management includes detailed logging and audit tracking of all key state changes, administrator access and policy changes. Audit trails are securely stored and signed for non-repudiation. 3.6.6—Split knowledge for key creation and deletion/access is supported through SafeNet KeySecure's 20+ administrative access control lists (ACLs). Security teams can require that two administrators must approve certain types of actions—i.e. key creation, etc. Additionally, split knowledge control of keys is often employed in situations in which raw key bits are stored, exposed, or accessed in the clear. SafeNet KeySecure provides a more secure key storage mechanism in that the raw key bits may never be stored, exposed, or accessed in the clear. With the SafeNet KeySecure solution, authorized users of encryption keys have access to cryptographic operations, but not access to the raw key bits. Cryptographic operations are performed only with keys to which an authorized SafeNet KeySecure user has access. Finally, there are ways to require that information must be shared across multiple SafeNet KeySecure administrators before key-specific administrative operations are performed. Administrators can also enforce policies that require multiple authentication levels to be met before cryptographic operations are performed with pecific encryption keys.

Requirement 4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: > Only trusted keys and certificates are accepted. > The protocol in use only supports secure versions or configurations. > The encryption strength is appropriate for the encryption methodology in use.	Gemalto offers high-assurance network encryption devices, including Ethernet and fibre channel encryptors that enable organizations to secure cardholder data submitted across a range of networks. Operating at Layer 2 of the network stack, SafeNet High Speed Encryptors (HSE) from Gemalto encrypt all data that traverses an open network. The appliances use strong cryptography and are certified FIPS 140-2 L3, Common Criteria, NATO and UC APL. By using Gemalto's SafeNet encryption and tokenization solutions, organizations can leverage robust security mechanisms that render data unreadable early in the data processing lifecycle, and ensure that data remains inaccessible to unauthorized users, even as it is transmitted across networks.
Requirement 6 Develop and maintain secure systems and applications 6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: > In accordance with PCI DSS (for example, secure authentication and logging) > Based on industry standards and/or best practices. > Incorporating information security throughout the software-development life cycle	Without assurance of an application's integrity, and without knowing who published an application, it's difficult for end users to know how much to trust software. Digital signatures help maintain the electronic integrity and authenticity of code by associating it with an application vendor's unique signature. A certificate is a set of data that completely identifies an entity, and is issued by a certification authority (CA). The data set includes the entity's public cryptographic key. To obtain a certificate from a CA, an application provider must meet the criteria for a commercial publishing certificate. It is recommended that applicants generate and store their private key using a dedicated hardware solution, such as an HSM. The HSM protects the identity, whether it is a server, virtualization server, or the user. SafeNet HSMs from Gemalto take this level of security one step further by storing the signing material in a hardware device, thus ensuring the authenticity and integrity of a code file.
Requirement 7 Restrict access to cardholder data by business need to know 7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	With Gemalto's SafeNet solutions, organizations can establish granular controls over who can access cardholder data. For example, by encrypting at the application level with SafeNet ProtectApp, your security teams can ensure that unauthorized users, even those with administrative permissions for an underlying server, cannot access sensitive data in the application.
Requirement 8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	Gemalto's SafeNet Strong Authentication Solutions ensures that each individual user is assigned a unique credential.
Requirement 8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	SafeNet Authentication solutions provide operational role segregation and delegated management ensuring that each user or privileged user can access resources only according to their role designation.
Requirement 8.1.3-8.1.8 8.1.3 Immediately revoke access for any terminated users. 8.1.4 Remove/disable inactive user accounts at least every 90 days. 8.1.5 Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: Enabled only during the time period needed and disabled when not in use. Monitored when in use. 8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts. 8.1.7 Set lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. 8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Gemalto's Authentication solutions offers a complete set of provisioning rules and policy engines that cover all functionalities listed under requirements 8.1.3 through 8.1.8, for example: Authentication is controlled by the real-time application of rules that are automatically applied to users based on their group membership. Changes to user access permissions initiate the provisioning / de-provisioning process without any admin intervention All of Gemalto's SafeNet authentication solutions provide an extensive log and report mechanism which gives an up to date picture of all authentication and management events.

Requirement 8.2 > 8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: > Something you know, such as a password or passphrase > Something you have, such as a token device or smart card > Something you are, such as a biometric.	Offering the broadest range of authentication methods and form factors, Gemalto allows customers to address numerous use cases, assurance levels, and threat vectors with unified, centrally managed policies—managed from one authentication back end delivered in the cloud or on premise. Supported authentication methods include context-based authentication combined with step-up capabilities, OOB, one-time password (OTP) and X.509 certificate-based solutions. All authentication methods are available in numerous form factors, including smart card, USB token, software, mobile app, and hardware tokens.
Requirement 8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Passwords are encrypted via SSL when authentication to the SafeNet KeySecure or other SafeNet appliance is performed. Within the platform, passwords are hashed so that they can never be inadvertently exposed.
Requirement 8.2.3 Passwords/phrases must meet the following: > Require a minimum length of at least seven characters. > Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above. 8.2.4 Change user passwords/passphrases at least every 90 days. 8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used. 8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	SafeNet Authentication solutions offers a complete set of provisioning rules and policy engines that cover all functionalities listed under requirements 8.2.3 through 8.2.6 via the use of a unique policy engine that allows centralized control of PIN length and complexity. Moreover policies can be defined for SafeNet Data Protection solutions to ensure that password/phrase requirements are met.
Requirement 8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	Gemalto provides the broadest range of strong authentication methods and form factors covering numerous use cases, assurance levels, and threat vectors, such as remote network access. Supported authentication methods include context-based authentication combined with step-up capabilities, OOB, one-time password (OTP) and X.509 certificate-based solutions. All authentication methods are available in numerous form factors, including smart card, USB token, software, mobile app, and hardware tokens.
Requirement 8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: > All user access to, user queries of, and user actions on databases are through programmatic methods. > Only database administrators have the ability to directly access or query databases. > Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	Gemalto provides a number of solutions for securing cardholder data residing in databases throughout its lifecycle. SafeNet ProtectDB encrypts data at the database column level. Only authorized users or applications can successfully access sensitive data in the columns that have been encrypted within the database. SafeNet ProtectFile encrypts database files and backups. Granular access policies can be applied based on users and groups, file types, and processes for increased control over high-value data. SafeNet ProtectApp can perform a range of cryptographic operations, including encryption, decryption, digital signing and verification, secure hash algorithms (SHA), and hash-based message authentication code (HMAC) for fields containing credit card numbers. Once application data is encrypted, only authorized users and processes will be able to view and use the data – even if it has been backed up, replicated or stolen. SafeNet Tokenization from Gemalto, deployed in tandem with SafeNet KeySecure, secures sensitive card holder data that has been tokenized by controlling access to data across the data center.

Requirement 9 Restrict physical access to cardholder data	Gemalto offers effective capabilities for addressing these access requirements. Gemalto smart cards can be integrated with various building access technologies in order to function as both an employee's physical and digital ID. The same smart card that is used for network and computer security can be personalized and printed with ID pictures to function as an employee's ID badge. Fitted with a magnetic stripe or RF proximity technology, the card can also be used for door access systems. Smart ID badges can be issued using the same technology that issues standard ID badges today; existing badge printers would simply need to be upgraded to accept the smart card chip.
Requirement 9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed	SafeNet KeySecure enables secure, geographically distributed management of keys in files and folders, disk and tape media, to ensure centralized key management throughout the data lifecycle. Once the encryption keys are destroyed, the data cannot be accessed in clear text.
Requirement 10 Track and monitor all access to network resources and cardholder data Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.	Gemalto's SafeNet encryption and key management products provide a NIST SP 800-88r1 approved sanitization method known as Cryptographic Erase in which the keys that are used to encrypt the data are sanitized and the encrypted data is left intact. Appliances such as SafeNet KeySecure provide a central repository for all cryptographic activity data, which significantly streamlines auditing and logging efforts. SafeNet KeySecure maintains an extensive set of centralized log files that can be used to track administrator and user activities. Log files are time stamped and include specific administrator or user identification information. Log files are digitally signed to prevent tampering.
Requirement 10.2 Implement automated audit trails for all system components to reconstruct the following events: > 10.2.1 All individual accesses to cardholder data > 10.2.2 All actions taken by any individual with root or administrative privileges > 10.2.3 Access to all audit trails > 10.2.4 Invalid logical access attempts > 10.2 5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges > 10.2.6 Initialization, stopping, or pausing of the audit logs > 10.2.7 Creation and deletion of system-level objects	With Gemalto encryption offerings such as SafeNet ProtectFile, SafeNet ProtectDB, SafeNet ProtectV and SafeNet ProtectApp, organizations can gain an effective means for securing access to cardholder data, and for establishing detailed auditing and logging of access to this encrypted data. By leveraging a central key management platform like SafeNet KeySecure, organizations can effectively and efficiently comply with PCI DSS rules for auditing and logging. Centralized management includes detailed logging and audit tracking of all key state changes, administrator access and policy changes. Audit trails are securely stored and signed for non-repudiation. All of Gemalto's SafeNet authentication solutions provide an extensive log and report mechanism which gives an up-to- date picture of all authentication and management events.
Requirement 10.5 Secure audit trails so they cannot be altered. > 10.5.1 Limit viewing of audit trails to those with a job-related need. > 10.5.2 Protect audit trail files from unauthorized modifications. > 10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter. > 10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. > 10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Log files are digitally signed to prevent tampering with SafeNet KeySecure and encryption solutions. Plus, as part of the flexible set of log configuration options, SafeNet KeySecure enables log files to be automatically rotated to a backup or archiving log server. As a result, an audit trail can be effectively maintained to meet audit history and legal regulations.

Requirement A.1 Shared hosting providers must protect the cardholder data environment A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment. A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only. A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	For organizations such as service providers that deliver shared cloud-computing services to clients, multi-tenancy and separation of duties are cornerstones of Gemalto's identity and data protection solutions. The ability to ensure that only authorized entities have access to their data, even on shared infrastructure is vital to all shared environments, and particularly to multi-tenant cloud-enabled environments. SafeNet ProtectV is a high-availability encryption solution that encrypts data within instances, virtual machines and storage volumes and uses strong key management capabilities to ensure each enterprise customer maintains complete ownership and control of its data and encryption keys. In addition, role-based encryption polices, together with segregated key management, ensure separation of duties between cloud service provider system administrators and the organization's IT administrators, or between different units in the organization's own virtual environment. With SafeNet ProtectV, data is safeguarded and completely isolated from the cloud service provider, tenants in shared environments, or any other unauthorized party. Through SafeNet ProtectV's centralized management console, enterprises can audit and obtain compliance reporting on users accessing secured data.

About Gemalto's SafeNet Identity and Data Protection Solutions

Gemalto's portfolio of SafeNet Identity and Data Protection solutions enables enterprises, financial institutions and governments to protect data, digital identities, payments and transactions–from the edge to the core. Our solutions take a data-centric approach to security with innovative encryption methods, best-in-class crypto management, and strong authentication and identity management to help customers protect what matters, where it matters.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free