Get Ready for PCI DSS

What is PCI DSS?
The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card providers. This standard was created to increase controls around cardholder data to reduce credit card fraud.

What data is protected?
Cardholder data and sensitive authentication data are defined as follows:
- Account Data
- Cardholder Data includes: Sensitive Authentication Data includes:
  - Primary Account Number (PAN)
  - Cardholder Name
  - Expiration Date
  - Service Code
  - Full track data (magnetic-stripe data or equivalent on a chip)
  - CAV2/CVC2/CVV2/CID
  - PINs/PIN blocks

When will it take effect?
The requirements introduced in PCI DSS 3.1 will be considered best practices until January 31, 2018. Starting February 2, 2018, PCI DSS 3.2 will take effect as new requirements.

What happens if you don’t comply?
- Big fines
- Losses of revenues and customers
- Damage to reputation and trust

What’s new in PCI DSS 3.2?
8.3 Requires multi-factor authentication for any personnel with administrative access into the cardholder data environment, even from within the company’s own network.

Who must comply
- Financial Institutions
  - Banks, insurance companies, lending agencies, brokerages.
- Merchants
  - Restaurants, retailers, transportation, entertainment. Any business with point of sale terminals that process credit cards.
- Service Providers
  - Transaction processors, payment gateways, call centers, etc.

Gemalto IAM solutions for PCI DSS
- SafeNet Authentication Service (SAS)—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, Out-of-Band (OOB), one-time password (OTP), and X.509 certificate-based solutions. All authentication methods are available in numerous form factors, including smart cards, USB tokens, software, mobile apps, and hardware tokens.
- SafeNet Trusted Access (STA)—is an intuitive cloud access management service that makes it easy to manage cloud access with cloud single sign-on and scenario-based access policies. By combining the convenience of single sign-on with granular access policies, organizations can tighten access controls, and reduce password fatigue.
- Certificate-Based Authentication (PKI)—Gemalto’s comprehensive public key infrastructure (PKI) authentication solutions provide military-grade security. Supporting a wide portfolio of IDPrime smart cards and USB eTokens, Gemalto’s authentication management solutions ensure the proper security controls are in place to verify the identity of users and enable advanced security applications such as authentication, digital signing and encrypted email on any PC, desktop or mobile device.

| PCI requirements directly addressed with Gemalto 2FA solutions |
|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| 7               | 7.1.2           | 8.11            | 8.1.2           | 8.1.3-8.1.8     | 8.2             | 8.2.3           | 8.3             | 9               | 10               |
| Access Management | ✔               |                 |                 |                 |                 |                 |                 |                 | ✔               |
| Privileged access |                 | ✔               |                 |                 |                 |                 |                 |                 |                 |
| Context-based    |                 |                 | ✔               | ✔               | ✔               | ✔               | ✔               | ✔               | ✔               |
| OTP Push         | ✔               | ✔               | ✔               |                 | ✔               | ✔               |                 |                 |                 |
| PKI (cert-based) | ✔               | ✔               | ✔               | ✔               | ✔               | ✔               |                 |                 |                 |
| Converged Badge  | ✔               | ✔               | ✔               | ✔               | ✔               | ✔               |                 |                 |                 |
| OOB             |                 | ✔               | ✔               | ✔               |                 |                 |                 |                 |                 |
| OTP HW          | ✔               | ✔               | ✔               | ✔               | ✔               | ✔               |                 |                 |                 |
Gemalto IAM solutions for PCI DSS

Requirement 7.1.2
Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

Solution:
SafeNet credential management solutions give IT administrators the ability to assign permissions per group, so users only have access to the data they need. This limits unnecessary multiple instances of personal data held within the organization. The more critical and private the data, the more security needed to access.

Requirement 8.1.1
Assign all users a unique ID before allowing them to access system components or cardholder data.

Solution:
Gemalto’s SafeNet Strong Authentication Solutions ensure that each individual user is assigned a unique credential. Unique ID is fulfilled by SafeNet Authentication Service using one-time password and context authentication or Gemalto’s PKI solutions with certificate-based authentication.

Requirement 8.1.2
Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.

Solution:
SafeNet Authentication solutions (SafeNet Authentication Service and PKI) 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

1.3 Immediately revoke access for any terminated users.
1.4 Remove/disable inactive user accounts at least every 90 days.
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.
1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.
1.7 Set lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate.

Solution:
Gemalto’s Authentication solutions offer 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
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.

Solution:
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 cards, USB tokens, software, mobile apps, and hardware tokens.

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.

Solution:
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.

Solution:
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 cards, USB tokens, software, mobile apps, and hardware tokens.

Requirement 9
Restrict physical access to cardholder data.

Solution:
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 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 portfolio of SafeNet authentication solutions gives organizations navigating PCI DSS the tools they need to solve these challenges according to the shape of their operations and their IT architecture.

For more information visit Gemalto PCI DSS compliance.