cpl.thalesgroup.com

THALES
Building a future we can all trust

Get Ready for PCI DSS 4.0 with Thales OneWelcome Identity Platform

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard that provides a baseline of technical and operational requirements designated to protect payment data and reduce credit card fraud.

What data is protected?

PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD). Cardholder data and sensitive authentication data are considered account data and are defined as follows:

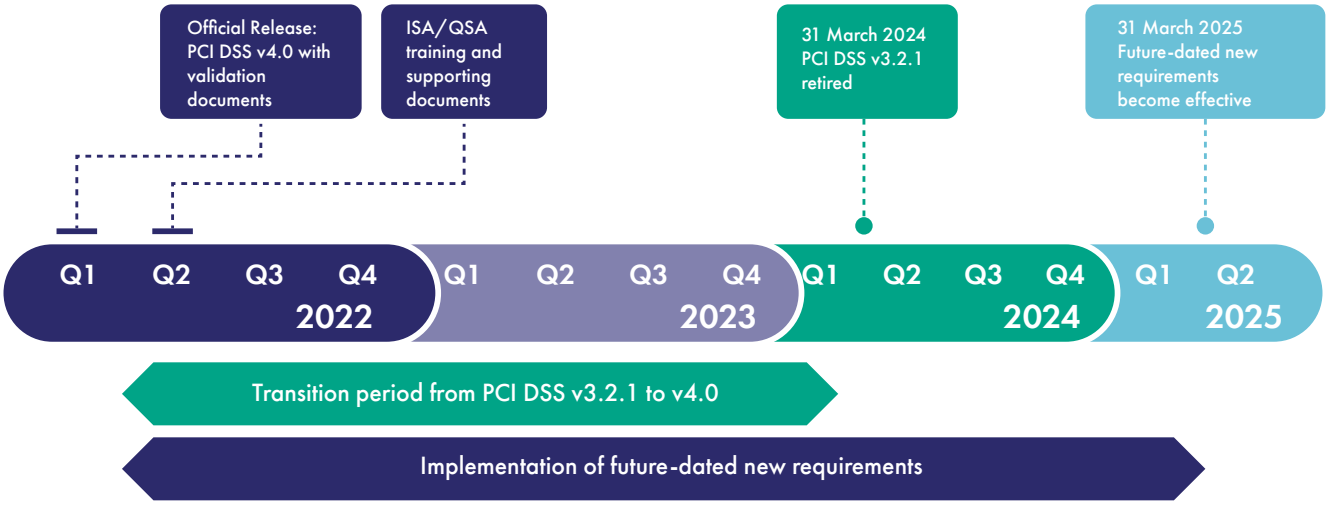
Account Data	
Cardholder Data includes	**Sensitive Authentication Data includes**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

What is new in PCI DSS 4.0?

The new version of the standard was released on March 31, 2022. Changes from the previous version 3.2.1 include:

- Expansion of Requirement 8 to implement multi-factor authentication (MFA) for all access into the cardholder data environment.
- Updated firewall terminology to network security controls to support a broader range of technologies used to meet the security objectives traditionally met by firewalls.
- Increased flexibility for organizations to demonstrate how they are using different methods to achieve security objectives.
- Addition of targeted risk analyses to allow entities the flexibility to define how frequently they perform certain activities, as best suited for their business needs and risk exposure.

Details about the updates can be found in the PCI DSS v4.0 Summary of Changes document on the PCI SSC website.



When will PCI DSS 4.0 take effect?

PCI DSS v3.2.1 will remain active for two years after v4.0 is published. This provides organizations time to become familiar with the new version, and plan for and implement the changes needed. The implementation timeline is shown in the image below.

What happens if you don't comply?

- Big fines
- Losses of revenues and customers
- Damage to reputation and trust

Who must comply?

Financial Institutions

Banks, insurance companies, lending agencies, brokerages.

Merchants

Restaurants, retailers, transportation, entertaiment. Any business with point of sale terminals that process credit cards.

Service Providers

Transaction processers, payment gateways, cell centers, etc.

PCI DSS 4.0 requirements addressed with the OneWelcome Identity Platform

ARTICLE	7	8.2	8.3	8.4	8.5	8.6	9	10
Access Management	√						√	√
OTP		√	√	√	√	√		
FIDO		√	√	√	√	√		
PKI-based		√	√	√	√	√		
Certificate-based		√	√	√	√	√		
Contextual Access		√	√	√	√	√		

How the OneWelcome Identity Platform helps you comply with PCI DSS 4.0 requirements

Requirement 7.2

7.2.1 Access requirements are established according to job functions following least-privilege and need-to-know principles.

7.2.2 Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.

Solution:

The OneWelcome Identity Platform enables you to centrally manage unique user identities, risk-based authentication policies, and add/revoke access to systems in your Cardholder Data Environment (CDE). OneWelcome offers powerful and expansive modern authentication capabilities that meet the needs of diverse users and user types.

Requirement 8.2

8.2.1 All actions by all users are attributable to an individual

8.2.2 All actions performed by users with generic, system, or shared IDs are attributable to an individual person.

8.2.4 Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization

8.2.5 Access for terminated users is immediately revoked.

8.2.6 Inactive user accounts are removed or disabled within 90 days of inactivity.

Solution:

The OneWelcome Identity Platform ensures that each individual user is assigned a unique credential. The solution offers a complete set of provisioning rules and policy engines that cover all functionalities listed under the above requirements. The OneWelcome authentication solution provides an extensive log and report mechanism which gives an up-to-date picture of all authentication and management events.

Requirements 8.3, 8.4, and 8.5

8.3.1 An account cannot be accessed except with a combination of user identity and an authentication factor.

8.3.3 Unauthorized individuals cannot gain system access by impersonating the identity of an authorized user.

8.3.4 An authentication factor cannot be guessed in a brute force, online attack.

8.3.11 An authentication factor cannot be used by anyone other than the user to which it is assigned

8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.

8.4.2 MFA is implemented for all access into the CDE.

8.4.3 MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE.

8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse

Solution:

Offering the broadest range of authentication methods and form factors, OneWelcome 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, one-time password (OTP), X.509 certificate-based solutions, and FIDO security keys.

Requirement 9

Restrict physical access to cardholder data

Solution:

OneWelcome offers effective capabilities for addressing these access requirements. Smart cards can be integrated with various building access technologies to function as both an employee's physical and digital ID.

Requirement 10

Processes and mechanisms for logging and monitoring all access to system components and cardholder data are in place and enforced

Solution:

The OneWelcome Identity Platform provides a full audit trail of access events as well as automated log export and seamless integrations with SIEM systems to ensure continuous monitoring and compliance.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

For more information, visit Thales PCI DSS Auditing and Compliance page.