Welcome to PCI compliance. *Simplified!*

You're probably already wondering what PCI compliance is and how Crypteron can help. Don't worry, we're here to help you navigate this complex topic. No time to lose, so let's get started

What is Crypteron?

Crypteron is the world leading data security platform for enterprises building cloud applications. Crypteron consists of the cloud (or on-premise) service as well as the SDK packages that integrates everything together. With Crypteron, you can be PCI compliant without the usual complexity, cost and mistakes. Crypteron handles the data encryption and key management requirements for PCI compliance so your business can focus on features that delight your end customers.

Testimonials

> *"We all love that it's a turn-key solution that maintains our strict security and PCI compliance requirements"*
>
> – William Ward, CIO, GivePay Commerce

> *"Crypteron is the best product for our data security needs"*
>
> – Samuel Butler, CTO, FSoft/Swoosh Finance

> *"Crypteron is awesome. You guys ranked 1st in our internal vendor bake-off covering the top 20 vendors. It was powerful yet so simple that even our junior developers were immediately productive."*
>
> – EVP, Top US Bank *
>
> * private due to bank policies

Key features

✓ Fastest Integration: The typical Crypteron integration takes 15 minutes from no data security to completely done. Why spend 12 or more months with complex solutions from other vendors?

✓ Automatic Management: Encryption keys are automatically managed by the Crypteron cloud and agent libraries. Keys are themselves encrypted and stored separately from the rest of your infrastructure - just as demanded by PCI DSS. You can always use the Crypteron Dashboard to manage advanced use cases.

✓ Regulatory Compliance: Crypteron enables compliance for your application with standards like PCI-DSS, GDPR, HIPAA, FISMA and more. One solution covers multiple compliance standards. Who doesn't like that?

✓ Built for performance: Crypteron's advanced security keeps latencies under 1 millisecond and throughput above 4 GB/sec by utilizing hardware-based AES-NI acceleration and detailed optimizations. As the rest of your application scales in size, so does the data security components powered by Crypteron's agent libraries.

✓ Any Cloud, Any Database: Whether you're dealing with SQL Server, MySQL, object stores, message queues, a big data analytics cluster, streaming data – Crypteron covers everything with one solution instead of managing multiple incompatible security systems. And this capability works in any cloud or non-cloud (e.g. bare-metal server closet) scenario.

✓ Unbreakable military grade AES 256 encryption: Crypteron uses authenticated AES 256-bit in GCM mode that's so robust that even the National Security Agency (NSA) recommends it for protecting of military classified information.

What is PCI?

PCI stands for Payment Card Industry. The Payment Card Industry Security Standards Council (PCI SSC) is a group of card companies (like VISA, MasterCard etc.) who felt market adoption would improve if businesses had one security standard to meet rather than separate security standards coming from each card company. The Payment Card Industry Data Security Standard (PCI DSS) is that one security standards designed to ensure that any business, that accepts, processes, stores or transmits credit card information does so in a secure manner. Note that PCI DSS is a globally applicable standard.

What is the scope of PCI-DSS?

PCI compliance covers people, processes and technologies when handling cardholder data (e.g. card account number, cardholder name etc.) and/or sensitive authentication data (e.g. CVC or PIN). As you can imagine, this is very broad but thankfully the most important pieces are focused in few key areas.

So, what should I focus on?

If your business has payments or e-commerce components to it, obviously your compliance efforts will mostly revolve around the servers doing that work. Server hosting (i.e. facilities operating your server machines) must be PCI compliant but that's the easiest part. Many cloud providers and hosting companies offering PCI compliant hosting. The biggest challenge is that the server software built by your business and running on such servers must also be PCI compliant. ***Your server software*** is ***THE*** most important and complex piece - and that's exactly where Crypteron's data security platform comes into the picture.

Crypteron's patented data security and key management platform enables your server application to be PCI compliant in minutes instead of the usual months and years. In fact, Crypteron exceeds PCI DSS so not only is your data is truly protected through best practices but also you get simultaneous compliance with other standards like GDPR, HIPAA, FISMA etc.

What does the compliance process look like?

Here is a checklist that can help you navigate

1. **Scope things out**: Have a rough idea of what pieces of your business may touch any credit card data (e.g. your transaction completing server or call center processes if accepting phone orders) and which ones never (e.g. your marketing website)
2. **Get a general feel**: Read the 12 high level requirement list in the next section to get a general feel for things. If you are familiar with PCI DSS, you can quickly visually scan the "Detailed PCI DSS Requirements and Security Assessment Procedures" section in the official PCI DSS specification to get a deeper idea but we think it's unnecessary and overwhelming to read and digest every word at this stage.
3. **Pick vendors**: Don't be overwhelmed as nobody satisfies the requirements without outside help. Pick vendors to address complex parts for you so you can focus on your core business. Crypteron will be a chief vendor considering it addresses the most critical piece i.e. data security of your server application but keep in minds other vendors who can help too. For example, you may want to host with a PCI compliant hosting company instead of hiring and training staff in-house to replicating that.
4. **Build solution**: With the general architecture in mind and vendors in place, continue building out the rest of your application and business
5. **Test for compliance**: Before processing real card data, you will need to demonstrate PCI compliance. Entities handling fewer transactions can perform a Self-Assessment Questionnaire (SAQ) and then claim PCI compliance. Larger entities will need to perform an independent audit by a PCI Qualified Security Assessor (QSA) as well as perform quarterly vulnerability scans using Approved Scanning Vendors (ASV) to satisfy requirement 11.2.2

Top level requirements

There are 12 top-level requirements designed to protect sensitive data. They are as follows:

1. Install and maintain a firewall
2. Avoid vendor default security parameters <= CRYPTERON
3. Encrypt stored data <= CRYPTERON
4. Encrypt transmitted data
5. Protect against malware and viruses

6. Build and maintain systems with security in mind
7. Restrict cardholder data on a need-to-know basis
8. Authenticate users
9. Limit physical access
10. Track and monitor all access to sensitive resources and data
11. Regularly scan and fix vulnerabilities
12. Establish an IT security policy and educate staff about it

As you can guess, achieving PCI compliance is a joint effort between you and vendors helping you be compliant. Let's examine how Crypteron can simplify the most complex parts for you.

How Crypteron solves PCI compliance

Let's have a look at relevant sub-category within each relevant top-level category. Note that there can be overlap between the various requirements as well as the controls/solutions.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Out of scope for this document as Crypteron is not a firewall solution. Please consult your firewall vendor.

Requirement 2: Do not use vendor-supplied defaults for passwords and security parameters

Requirement	Crypteron Solution
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	Crypteron has no default security parameters. All security parameters (AppSecrets) are fully randomized for each application.
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.	Crypteron ensures that the key management functionality is separated from the application runtime functionality.
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data.	Unlike most storage encryption approaches (e.g. disk encryption), Crypteron's encryption platform ensures that cardholder data is separately encrypted even in shared hosting environments.

Requirement 3: Protect stored cardholder data

Requirement	Crypteron Solution
3.3 Mask PAN when displayed	Crypteron supports masking and does so right at the data security layer, not the UI/presentation layer. If done at the UI layer, the scope of PCI compliance becomes significantly larger since the UI is often on the client device and not in the datacenter.
3.4 Render primary account number unreadable anywhere it is stored	Crypteron brings complete data-at-rest encryption and is fully independent of the underlying security of the storage medium or policy. Even logging, backups or admin access of the databases will not leak sensitive data.

	Crypteron also avoids complications from requirement 3.4.1 by encrypting the data fields directly instead of relying on disk encryption
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:	Crypteron protects the data encryption keys by encrypting them with key encryption keys, which are encrypted by master keys. Access to the key encryption keys and master keys is highly restricted and those keys never leave the service.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data	Crypteron follows NIST guidelines to take care of the key management difficulties so you don't have to.
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	Crypteron's platform and documentation provides a unified, well understood approach on how cardholder data is protected.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement	Crypteron Solution
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks	Crypteron agents use multiple layers of encryption when working with the Crypteron service. Sensitive data never leaves the Crypteron SDK/agents but data encryption keys and security ACLs are secured by multi-layered encryption (defense-in-depth). There is a hardened TLS outer layer and an AES 256-bit encrypted inner layer (fully independent of the outer TLS 'pipe')

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Out of scope for this document as Crypteron is not an antivirus solution. Please consult your antivirus vendor.

Requirement 6: Develop and maintain secure systems and applications

Requirement	Crypteron Solution
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely	Crypteron decouples data security and key management from the rest of your application, thereby promoting secure development practices.
6.4 Follow change control processes and procedures for all changes to system components.	Crypteron allows for separate development, test and production environments. Your code and designs stay the same, only the AppSecret (a glorified API key) is swapped out in the right environment. This control ensures that developers cannot accidentally access production data.

6.5 Address common coding vulnerabilities in software-development processes	Crypteron follows cryptographic best practices. Crypteron's CipherDB SDK makes the application resilient to SQL injection.

Requirement 7: Restrict access to cardholder data by business need to know

Requirement	Crypteron Solution
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	Crypteron allows for separate development, test and production environments. Your code and designs stay the same, only the AppSecret (a glorified API key) is swapped out in the right environment. This control ensures that developers or testing staff cannot accidentally access production data.
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	By encryption all sensitive data, "deny all" is the default unless specifically decrypted for a need-to-know purpose.
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	Crypteron's platform and documentation provides a unified, well understood approach on how cardholder data is protected.

Requirement 8: Identify and authenticate access to system components

Crypteron isn't a user authentication solution but can help as shown below. You will want to consult your user authentication vendor for broader compliance within this category.

Requirement	Crypteron Solution
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted	Crypteron separates access to database infrastructure from access to data. This means database administrators can go their job by modifying the database infrastructure without being able to decrypt the sensitive data itself. This can dramatically reduce compliance scope when using cloud databases.

Requirement 9: Restrict physical access to cardholder data

Out of scope for this document. Please consult your datacenter vendor or corporate facilities/security staff.

Requirement 10: Track and monitor all access to network resources and cardholder data

Out of scope for this document. Please consult with your operating system, user authentication and network equipment vendors.

Requirement 11: Regularly test security systems and processes.

Out of scope for this document. Please consult with your security testing vendor.

Requirement 12: Maintain a policy that addresses information security for all personnel.

Out of scope for this document. Please consult with your HR or legal teams.

What's the next step?

You made it this far – congratulations! As you can see, PCI compliance is a complex topic and requires coordinated work between you and several of your security and infrastructure vendors. However, the core part is protection of card data and Crypteron has you covered very well there.

Get started for free today at crypteron.com or contact us at sales@crypteron.com.