PCI DSS & other security requirements

Very often customers ask questions connected with security. In this article we would like to summarize key requirements connected with Payment Card Industry Data Security Standards (PCI DSS). There are other rules that we and our partners need to follow (like GDPR for example) but it will be the topic for another article.

The most important question that needs to be answered before going into details of PCI DSS requirements is - **Am I actually processing payment card data?**

Key PCI DSS requirements mentioned below apply only in case that the partner has access to card number (PAN - Primary Account Number), expiry data or other related card data. If the partner does not touch them, if the partner cannot see those numbers there is only one requirement - a simple Self Assessment Questionnaire (SAQ) needs to be fulfilled to confirm that the partner is compliant with PCI DSS requirements.

It is very important that you choose the correct way of integration with the card issuing platform. If you use our mobile SDKs or white label products, usually you will not have access to card data and will be able to approve your project just after fulfilling SAQ mentioned above. So please consider this way of integration to avoid additional costs and risks of PCI DSS compliance. However, if you connect via API, which is a usual way of integration, you will have to comply with security rules. Please read this section twice. **This is the most important** - choice of integration method will be decisive if you have to or not go through annual external audits and all hassle connected with PCI DSS.

Assuming you do process card data, depending on what your role is, different levels will be applied to you. You can be a **merchant** or a **service provider**. In simple terms, if you do the work for yourself then you are a **merchant** if you want to further provide the service (intermediary) you are most likely a **service provider**. In card issuing projects you will rather be Service Provider because you offer cards to your users. Let me give some examples:

Service Provider - wallet, crypto wallet, money transfer organisation offering cards to own users etc.

Merchant - insurance company that wants to use card to send money to their users, lending company that wants to send card to users, corporation or firm giving business payment cards to their employees etc.

Who is according to PCI DSS "Merchant"
PCI DSS, or the Payment Card Industry Data Security Standard, defines a merchant as any entity that accepts payment cards (such as credit cards and debit cards) as a form of payment. The term "merchant" can encompass a wide range of businesses and organizations, including traditional retail stores, e-commerce websites, restaurants, hotels, and service providers that handle cardholder data.

Under PCI DSS, merchants are required to comply with a set of security standards and practices to protect the payment card data they handle. These security measures are designed to ensure the confidentiality and integrity of cardholder data, reduce the risk of data breaches, and protect both customers and the payment card industry as a whole.
PCI DSS compliance requirements can vary depending on the merchant's size and the volume of card transactions they process. Merchants are typically categorized into different levels based on their transaction volume, with higher-volume merchants facing more stringent compliance requirements.

There are 4 levels of compliance and requirements depending on volumes of cards and transactions.

Level of PCI DSS	Your business does	What you should do
4	· Less than 20 000 eCommerce transactions per year · Less than 1 million other transactions per year	· Complete an annual Self-Assessment Questionnaire (SAQ) · Conduct quarterly network scans by an Approved Scanning Vendor (ASV)
3	· 20 000 – 1 million transactions per year	· Complete an annual Self-Assessment Questionnaire (SAQ) · Conduct quarterly network scans by an Approved Scanning Vendor (ASV)
2	· 1-6 million transactions per year	· Complete an annual Self-Assessment Questionnaire (SAQ) or ROC conducted by a QSA · Conduct quarterly network scans by an Approved Scanning Vendor (ASV)
1	· 6 million + transactions per year	· Complete an annual internal audit · Conduct quarterly network scans by an Approved Scanning Vendor (ASV)

Who is according to PCI DSS "Service Provider"
According to the Payment Card Industry Data Security Standard (PCI DSS), a Service Provider is defined as any business or entity that is not a payment card brand (such as Visa or Mastercard) and is involved in the processing, storage, or transmission of payment card data on behalf of

another organization. Service Providers play a crucial role in the payment card ecosystem, as they offer various services to help businesses accept and process card payments more effectively and securely.

Service Providers can include a wide range of businesses, such as:

1. Payment processors
2. Payment gateways
3. Hosting providers
4. Managed security service providers
5. Data storage companies
6. Point-of-sale (POS) system providers
7. Customer relationship management (CRM) software providers
8. Software-as-a-Service (SaaS) providers

Service providers are categorized based on the services they provide and their interactions with payment card data. Here are some common classifications of service providers based on PCI DSS:

Level of PCI DSS	Your business does	What you should do
2	· < 300 000 transactions per year	· Complete an annual Self-Assessment Questionnaire (SAQ) · Conduct quarterly network scans by an Approved Scanning Vendor (ASV)
1 (Verestro has 1 level of PCI DSS)	· > 300 000 transactions per year	· Complete annual internal audit conducted by a Qualified Security Assessor (QSA) · Conduct quarterly PCI ASV scans

Verestro has the 1st level Service Provider of PCI DSS which means that we have to go through quarterly PCI ASV scans and an annual external audit performed by certified PCI DSS assessors. In accordance with the principles of PCI DSS Verestro is obliged to check that the partner is working according to PCI rules so we will be checking what the level of transactions and cards in your case is.

image-1713429427331.jpg

So let's remind our two possible scenarios:

Scenario 1 (The partner does not have any access to unencrypted PAN numbers) -> THIS IS THE BEST AND RECOMMENDED SCENARIO. In this scenario you will most likely use our SDKs and admin panel and full encryption of card data. Verestro will guide which Self-Assessment Questionnaire (SAQ A for merchants) is appropriate and ask a few questions (from SAQ). The document will have to be signed by the partner.

Scenario 2 (The partner can access unencrypted PAN numbers) -> in this scenario:

- Verestro will provide an Self-Assessment Questionnaire (SAQ), and ask a few questions. The document will have to be signed by the partner.
- The partner will perform quarterly PCI ASV (Approved Scanning Vendors) scans (cost around 1k EUR quarterly or less) - The partner can choose any provider from the PCI Security Standards Council (PCI SSC) or Verestro can recommend a supplier.
- Until the partner reaches 0,3 mln transactions/interactions annually with PAN numbers, the partner does not need to undergo an annual internal audit (in extreme situations, it is possible to require PCI internal audit from the partner).

If the partner plans to achieve 0,3 million transactions/interactions, there are two options:

- either the partner will move to a scenario that does not touch card numbers using some technology changes
- or the partner should perform an annual internal audit done by a PCI auditor (QSA)

If you would like to discuss your requirements in more detail and receive more information, please contact us.

Thanks for reading.

Revision #7
Created 18 April 2024 04:45:21 by Krzysztof Drzyzga
Updated 2 May 2024 12:19:34 by Krzysztof Drzyzga