Payment Services

Information sheet on the PA-DSS security standard

The globally applicable Payment Application Data Security Standard (PA-DSS) contains security guidelines for the development of payment applications that store, process or transfer card data during the payment process.

The use of PA-DSS-certified payment applications can considerably reduce the risk of data theft. PADSS also makes it easier for companies to comply with the security guidelines defined in the Payment Card Industry Data Security Standard (PCI DSS).

We have summarized the most important information about PA-DSS for you.

Why was PA-DSS introduced?

Investigation of various cases of card date theft revealed that they often were attributable to payment applications that were not adequately protected. That is why the global PA-DSS security standard was introduced in 2008.

What is the purpose of PA-DSS?

The use of certified payment applications contributes to the reduction of the risk of card data theft. PA-DSS supports solution providers with the development of new payment applications and helps merchants reach compliance according to PCI DSS (Payment Card Industry Data Security Standard).

What does PA-DSS contain?

The standard comprises 14 general requirements and around 90 detailed requirements as guidelines for the development of secure payment applications. The requirements are essentially concentrated on the following areas: Development, processes, implementation, encryption and access.

Who is required to comply with PA-DSS?

Payment application solution providers that store, process or transfer card data are required to comply with PA-DSS. The precondition is that these applications must be part of an authorization process and /or the payment processing and are sold to third parties.

Who is responsible for ensuring compliance with PA-DSS

The solution providers must primarily ensure the compliance of payment applications with PA-DSS. Distributors, integrators and merchants who buy, sell or install payment applications must ensure that the payment applications they deploy are PA-DSS-certified.

What application types are subject to PA-DSS?

- Series-produced payment applications that are sold to third parties and installed.
- Modular payment applications (only the modules with payment functions).
- Stand-alone payment terminals which:
  1. are connected to the merchant's system or network
  2. are not only connected to the payment processor (acquirer)
  3. do not provide secure remote maintenance of the payment application
  4. store sensitive card data (magnetic stripe data, CVV2, CVC2, CAV2, CID or PIN) after the authorization process.

Which application types are not subject to PA-DSS?

1. Customized individual solutions (no sales)
2. Applications developed by the merchant that are only used internally
3. Operating systems (Windows, Unix, etc.), data, administration systems (back office) and the like

These applications are reviewed within the scope of the merchant's PCI DSS certification.

Who may conduct a PA-DSS certification?

Payment applications must be approved and certified by a Payment Application Qualified Security Assessor (PA-QSA). These security assessors are accredited by the PCI Council. You can find a list of all approved PA-QSA's at:
https://www.pcisecuritystandards.org/security_standards/vpa/

For how long is the PA-DSS certificate valid?

The standard is revised every three years and published in a new version. The validity of a certification expires three years after publication of the new standard version. This means that compliance is ensured for at least three years.

However, payment applications must be validated every year. Revalidation by a PA-QSA may be required when changes are made to the payment application, depending on the nature of the changes.

What does certification cost and who pays?

The costs for the certification of a payment application vary. In addition to the scope and complexity of a payment application, the choice of security assessor (PA-QSA) also plays a role. The addition of a payment application to the PCI Council list upon successful certification costs USD 1,250 per payment application.

An administration fee of USD 500 per payment application is then charged on an annual basis.

Where can I find further information about PA-DSS?

You can find further information about PA-DSS on the PCI Council website:
https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

Their webinar on the topic of PA-DSS is also recommended:
http://www.webcastgroup.com/client/start.asp?wid=0800522084108

The current list of all certified payment applications:
https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html

110.0115.02 CHE_EN/04.2012

Your personal contact: www.six-payment-services.com/contact

SIX Payment Services Ltd
Hardturmstrasse 201
8005 Zurich
Switzerland

SIX Payment Services (Europe) S.A.
10, rue Gabriel Lippmann
5365 Munsbach
Luxembourg