Security for credit card payments for car parks

How to ensure PCI compliancy in SKIDATA PARCS environments

WHITEPAPER by Gerhard Daxer

SKIDATA®
KUDELSKI GROUP

How to tackle PCI – now and in the Future

Summary

This whitepaper provides helpful insights about PCI and the different options to handle PCI compliancy obligations in connection with SKIDATA PARCS. It also outlines how these different possibilities impact operations and costs in a car park environment.

Who needs to be PCI compliant?

Companies receiving credit card payments for goods and/or services are signing a "Merchant" contract with an acquiring bank. This merchant agreement also contains an obligation to be PCI compliant.

So, if a car park operator accepts credit card payments on site (merchant), then he has the obligation to be PCI DSS compliant.

PCI DSS Requirements

Build and maintain a secure network

- Install and maintain a firewall configuration to protect cardholder data.
- Don´t use vendor-supplied defaukts for system passwords and other security parameters.

Protect cardholder data

- Protect stored cardholder data.
- Encrypt transmission of cardholder data across open, public networks.

Maintain a vulnerability management program

- Protect alls systems against malware and regularly update antivirus software or programs.
- Develop and maintain secure systems and applications.

Implement strong access control measures

- Restrict access to cardholder data by businesses to know.
- Identify and authenticate access to system components.
- Restrict physical access to cardholder data.

Regularly monitor and test networks

- Track and monitor all access to network resources and cardholder data.
- Regularly test security system and processes.

Maintain an information security policy

- Maintain a policy that adresses information security for all personnel.

Merchant Categories

Merchants are categorized in different levels depending on their credit card payment transaction volume. Depending on the level, there are different obligations for proving PCI compliancy each year.
PCI Compliancy is an ongoing process, not a onetime effort.

LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
6M +	**1-6 M**	**20K - 1M**	**< 20K**
Process more than 6 million Visa transactions per year, regardless of channel. Be identified as Level 1 by any card association.	Process 1 to 6 million credit card transactions annually across all channels.	Process 20,000 to 1 million e-commerce credit card transactions annually.	Process fewer than 20,000 e-commcerce transactions annually, or process fewer than 1 million credit card transactions annually across channels.
SECURITY REQUIREMENTS			
Complete a ROC annually by a Qualified Security Assessor (QSA)*. This means an on-site audit needs to occur every year. Quarterly scans by an Approved Scanning Vendor (ASV)*. An AOC that verifies everything meets PCI standards.	Conduct an annual Self-Assessment Questionnaire (SAQ)*. Quarterly scans by an Approved Scanning Vendor (ASV). An AOC that verifies everything meets PCI standards.	Conduct an annual Self-Assessment Questionnaire (SAQ)*. Quarterly scans by an Approved Scanning Vendor (ASV). An AOC that verifies everything meets PCI standards.	Conduct an annual Self-Assessment Questionnaire (SAQ)*. Quarterly scans by an Approved Scanning Vendor (ASV). An AOC that verifies everything meets PCI standards.

The long PCI Track-Record of SKIDATA

SKIDATA already has a long history with PCI since we are providing PCI validated software versions for more than 15 years since the beginning of PCI now. We have been validating more than 12 major versions of our PARCS software in compliance with PCI PA DSS. In the meantime, security has an increased focus throughout SKIDATA, not only for software development, but also in the whole organization.

What is PCI?

The PCI Security Standards Council was created by American Express, VISA, Discover, MasterCard and JCB in 2006. PCI SCC is responsible for developing and managing the Payment Card Industry Data Security Standard (PCI DSS). This security standard was developed to encourage and enhance cardholder data security and provide consistency in data security globally.

PCI DSS is a set of rules and guidelines for organizations that store or process cardholder data. There is also a set of rules derived from PCI DSS for credit card reader hardware (PCI PTS) and payment application software (PADSS / SSF).

PCI SSC has established a certification process whereby hardware and software vendors can submit their products for validation by qualified security assessors, appointed by PCI SSC, so that they can be marketed to purchasers and end-users.

How does PCI and EMV fit together?

The Role of PCI DSS - The Payment Card Industry Data Security Standard (PCI DSS) contains 12 key technical and operational requirements set by the PCI Security Standards Council (PCI SSC). Rather than focusing on a specific category of fraud, the PCI DSS seeks to protect cardholder and sensitive authentication data anywhere this data is present within the payment eco-system.

The Role of EMV - EMV smartcards were designed and introduced to reduce fraud occurring in magnetic-stripe face-to-face environments, by using integrated-circuit (IC) based cards that use secret cryptographic keys to generate authentication and authorization data. EMV by itself does not protect the confidentiality of, or inappropriate access to sensitive authentication data and/or cardholder data. So EMV concentrates on a secure card communication (card and reader hardware).

How-To reach PCI Site Compliancy

Depending on a merchant's classification, processes for compliance usually follow these steps:

1. **Scope** – determine which system components and networks are in scope for PCI DSS
2. **Assess** – examine the compliance of system components in scope following the testing procedures for each PCI DSS requirement
3. **Report** – assessor and/or entity completes required documentation (e.g., Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC)), including documentation of all compensating controls
4. **Attest** – complete the appropriate Attestation of Compliance (AOC)
5. **Submit** – submit the SAQ, ROC, AOC, and other requested supporting documentation such as ASV scan reports to the acquirer (for merchants) or to the payment brand/requestor (for service providers)
6. **Remediate** – if required, perform remediation to address requirements that are not in place, and provide an updated report

What influences the PCI Compliancy costs?

It is the PCI "Scope" which has the major impact on PCI costs. The PCI "Scope" is defined by the Cardholder Data Environment (CDE). The CDE is the IT environment where credit card data are existing in, at the site. Within this CDE every PC and every application is within PCI scope.

This means every PC and every application must follow PCI rules. If there are applications within the CDE which are storing credit card data, then these applications must be PA DSS validated to prove PCI compliancy.

The PCI scope can be big or small depending on the type of credit card payment solution in place. The PCI related operative efforts and costs are directly depending on the size of the PCI scope.

SKIDATA supports several credit card acceptance methods

1. Real Time Authorization using Credit Card Authorization Server via magstripe (outdated)

- Credit cards are read and accepted by the SKIDATA coding unit
- Credit card transactions are authorized online at the acquiring bank
- Credit card PAN is stored within the parking system database
- The usage of PA DSS validated software is strongly recommended

Large scope - In this scenario, Parking.Logic is clear within PCI scope because cardholder data is processed and stored in the system. The whole parking system network with all its components is in PCI scope, which increases the efforts and the costs of compliancy.

2. Real Time Authorization using External Terminal Hardware (EMV/PTS Chip&Pin Solutions)

- Credit cards are read and accepted by a separate credit card terminal (and NOT within the SKIDATA proprietary coding unit)
- Credit card transactions are authorized online by the hardware terminal itself
- Credit card PAN is not stored within the parking system database
- Terminal hardware must be PCI PTS validated
- The usage of PA DSS validated software is strongly recommended if there is no network separation

» In this scenario the scope depends on the design and the of the local network:

A) Small scope - Parking.Logic can be out of PCI scope if the IT environment (network) of the hardware terminals (=CDE, cardholder data environment) is clearly separated from the Parking system network according to PCI rules. The PCI scope (and the related costs) can be reduced pretty much with this scenario, because Parking. Logic does not store any credit card data and is thus not within the PCI scope anymore.

B) Large scope - if the network of the hardware terminals is not properly separated from the parking, then the whole parking system is again fully in PCI scope and must be considered for PCI compliancy.

3. Real Time Authorization via External P2PE Terminal Solution (P2PE Chip&Pin Solutions)

- Credit cards are read and accepted by a separate credit card terminal (and NOT within the SKIDATA proprietary coding unit)
- Credit card transactions are authorized online by the hardware terminal itself
- Credit card PAN is not stored within the parking system database
- The whole payment solution is PCI P2PE validated

» **Small scope** - by using such a P2PE validated solution, Parking.Logic is out of PCI scope completely. P2PE solutions are reducing the PCI scope and thus also the effort and costs as much as possible.

Let's have a closer look on P2PE

A point-to-point encryption (P2PE) solution cryptographically protects credit card data from the point where a merchant accepts the payment card to the secure point of decryption. By using P2PE solutions, credit card data is unreadable until it reaches the secure decryption environment at the payment service provider or acquiring bank.

Nobody can decrypt credit card data through the whole data chain - from the hardware credit card terminal where the card is swiped on the on side to the payment service provider (or acquiring bank) environment on the other side.

» The PCI council offers the possibility to validate P2PE solutions. These validated P2PE solutions are listed as usual at the PCI council's website.

What does P2PE mean for the Site Compliancy of a Merchant?

P2PE solutions do not remove any obligations for PCI site compliancy, but they are taking out the pain of PCI. P2PE solutions are making life easier as the PCI scope is reduced significantly. Only the P2PE solution itself is "in scope" and as such relevant for the PCI site compliancy.

» Clear Advantages:

- For car park operators this means a reduction of scope in their annual PCI SAQ (Self-Assessment Questionnaire)
- PCI compliancy requirements are reduced significantly
- By using a P2PE solution there is no necessity to have a PCI PA DSS validated payment application any more
- At the end PCI site compliancy can be achieved more easily and more cost-effectively with less operational impacts

Self-Assessment Questionnaire	SAQ P2PE	SAQ D
Pages of Requirements	7	65
Requirement Areas		
Full Scope		●
Secure network		●
Protect Cardholder Data	●	●
Vulnerability management		●
Access control measures	●	●
Monitor networks		●
Personal policy and training	●	●

PCI – There are Changes Ahead

PCI SSC has announced the end of the PA DSS program - the program for payment application security validations and will replace it with a new standard called "SSF Software Security Framework". Currently listed PA-DSS applications will remain in effect under the PA-DSS programs until the applications reach their expiration date (end of Oct 2022). Afterwards PCI will move them to the "Usable for pre-existing deployments" section on their website.

» The Good News is:

- With Parking.Logic V15.x, SKIDATA will continue to deliver a PA DSS validated software beyond the end of the PA DSS program
- This version will have an extended maintenance period to ensure continuous support for PCI compliancy of our customers

SKIDATA post PA DSS era beyond Parking.Logic V15

We see P2PE solutions as the new security standard for credit card acceptance (card presence). By using P2PE solutions there is no necessity to have validated payment applications anymore (reduced scope). SKIDATA will therefore not pursue the validation of its PARCS software in compliancy with the PA DSS successor SSF (Software Security Framework) in the future.

SKIDATA strongly recommends migrating to P2PE solutions to achieve PCI site compliancy more easily and more cost-effectively - in addition, with less operational impacts.

SKIDATA currently offers different P2PE validated solutions

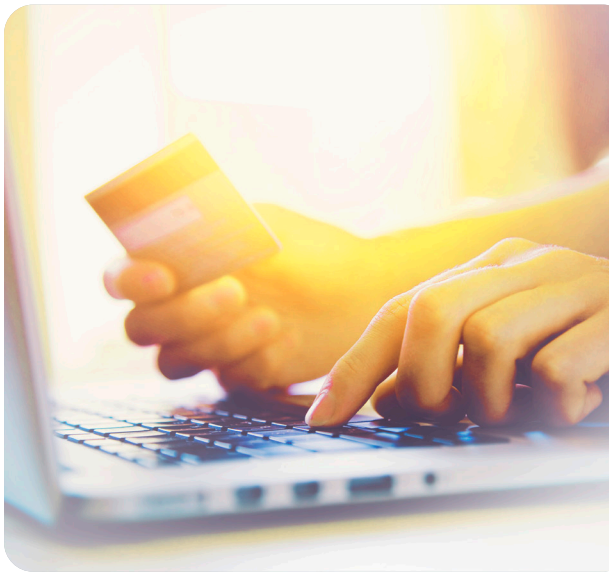
- CCV P2PE
- Windcave P2PE
- ADVAM P2PE
- 3C Integra Verifone 3CPOS P2PE

Being up-to-date and Secure is Vital for all our Business

Even if SKIDATA is not doing official PCI SSF validations for the PARCS software, we have processes and security measures in place for the development group and the whole organization to ensure top level quality and security for our PARCS software and hardware.

» Our secure development lifecycle includes among other things:

- Secure development guidlines
- Design and coding reviews
- Risk assessment procedure
- Automated unit testing
- Quality management and approval processes
- Cyclic penetration and security checks
- Ongoing security education and training
- Security by default attitude



There is an easy way to stay up to date

Security and availability are an increasing demand in these times. The risks of cyber-attacks and other digital threats are growing with every year and managing those risks is becoming more and more important to all of us.

To protect yourself from threats, it is imperative to have an up-to-date system with the latest operating system security patches and the latest parking system application patches. Security is not a status but a continuous process!

» The Good News is:

- SKIDATA offers with DSD (Digital Software Delivery) a service to download and install software and patches online, like what Microsoft offers with automatic updates
- High quality software from a trusted reliable source
- You define and configure the level of automation that fits best to your operation

» With many Benefits:

- Always up to date and secure
- Increased uptime and decreased manual efforts for software maintenance
- Time and cost saving due to automation and pre-installation of software
- Optimized software maintenance design with small and regular software packages

Source References

- **PCI DSS Quick Reference Guide** (https://www.pcisecuritystandards.org/)
- **PCI DSS** at a glance (https://www.pcisecuritystandards.org/)
- **SKIDATA** (https://www.skidata.com/en/parking/)

SKIDATA GmbH
Untersbergstraße 40 • 5083 Grödig/Salzburg
tel +43 6246 888-0 • fax +43 6246 888-7
info@skidata.com • www.skidata.com • Version 1.1 • 2022-06

SKIDATA®
KUDELSKI GROUP