Security Policy

Project: Primus Self Park
Document: Security.Policy
Revision n°: 1.0
Date: 1/4/2017
Author: PayTec AG
Status: Released

Released by:

<table>
<thead>
<tr>
<th>Position</th>
<th>Name</th>
<th>Date</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Revision history

<table>
<thead>
<tr>
<th>Revision n°</th>
<th>Date</th>
<th>Who</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>2016.11.18</td>
<td>PS</td>
<td>Initial creation</td>
</tr>
<tr>
<td>0.2</td>
<td>2016.11.24</td>
<td>PS</td>
<td>Review</td>
</tr>
<tr>
<td>0.3</td>
<td>2016.11.25</td>
<td>PS</td>
<td>Review findings</td>
</tr>
<tr>
<td>0.4</td>
<td>2016.11.28</td>
<td>PS</td>
<td>Update</td>
</tr>
<tr>
<td>1.0</td>
<td>2016.11.29</td>
<td>PS</td>
<td>Released</td>
</tr>
</tbody>
</table>
# Table of Content

1. Table of content .................................................................................. 3
2. Introduction ......................................................................................... 4
   2.1 Purpose ......................................................................................... 4
   2.2 Glossary and abbreviations ......................................................... 4
   2.3 References ................................................................................... 4
3. General Information ........................................................................... 5
4. Identification ....................................................................................... 5
   4.1 Product Label .............................................................................. 5
   4.2 Software version .......................................................................... 5
5. Guidance ............................................................................................. 6
   5.1 Inspection .................................................................................... 6
      5.1.1 At delivery ........................................................................... 6
      5.1.2 Periodic ............................................................................... 6
   5.2 Environment ................................................................................ 6
   5.3 Installation ................................................................................... 6
   5.4 Service Removal or Repair ......................................................... 6
   5.5 Decommission ............................................................................. 6
6. Security ................................................................................................ 7
   6.1 Hardware ..................................................................................... 7
   6.2 Software ....................................................................................... 7
   6.3 Tamper indication ........................................................................ 7
   6.4 Selftest ......................................................................................... 7
   6.5 Services and Roles ....................................................................... 7
   6.6 PIN confidentiality ....................................................................... 7
7. KEY Management ................................................................................. 8
   7.1 KEY Table .................................................................................. 8
   7.2 KEY Replacement ....................................................................... 8
   7.3 Cryptographic algorithms ........................................................... 8
8. System Administration ........................................................................ 8
   8.1 Software updates ......................................................................... 8
   8.2 Configuration settings ................................................................. 8
2 Introducion

This document addresses the proper use of Primus Self park (PSP) Terminal. The use of the device in an unapproved method leads to incompliance to the PCI [1] requirements. Inoperable devices, e.g. Tampered devices, need to be shipped back to PayTec for investigation and repairing.

2.1 Purpose

This document should provide indication to answer the security requirements listed in DTR B20 [2] as required by [1]

2.2 Glossary and abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSP</td>
<td>Primus Self Park</td>
</tr>
<tr>
<td>PED</td>
<td>PIN entry device</td>
</tr>
<tr>
<td>POI</td>
<td>Point of interaction</td>
</tr>
</tbody>
</table>

2.3 References

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Document</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>PCI_PTS_POI_SRvs4-1c.docx</td>
<td>4.1c</td>
</tr>
<tr>
<td>[2]</td>
<td>PCI_PTS_POI_DTRsv4-1b.pdf</td>
<td>4.1b</td>
</tr>
<tr>
<td>[3]</td>
<td>PayTec_Terminal_SDK.chm</td>
<td>4.0.x</td>
</tr>
</tbody>
</table>
3 General Information

The PSP is a PED designed to process debit- and credit card PIN based transactions in a unattended environment. It provides a Pinpad, Magstripe- and IC- card reader and a RS232 communication interface.

4 Identification

4.1 Product Label

The Product Label is placed on device bottom or rear side.

Up to date PCI information could be retrieved from https://www.pcisecuritystandards.org.

4.2 Software version

The PSP PED is a non-display device. The effective SW-versions of each installed package could be queried either from host device as documented in PayTec SDK [3] description or with PayTec provided Testapplication designed for type approvals at accredited test facilities. 3rd party developers must sign a NDA to get PayTec SDK [3].
5 Guidance

5.1 Inspection
Paytec suggest merchants and acquirer to implement regular inspections of PED.

5.1.1 At delivery
Paytec strongly advices the merchant or acquirer to visually inspect the PED as described in enclosed operating and installation manual.
Device serial number(s) mandatorily must match to serial number(s) listet on delivery note.

5.1.2 Periodic
- The Label on PED underside
- No additionally appearing signs like:
  - additional wires,
  - cables,
  - loosen screws,
  - torn label,
  - holes,
  - cracks, …
- Paytec unauthorized or unidentified attachments
- The ICC insertion area has no signs of scimming parts
- The keypad is still in firmly and normal condition

5.2 Environment
PSP PED is designed to operate in temperature range from 0 to 50°C up to 2000m above sea level. The device could be powered in a range from 5 to 9 VDC.

5.3 Installation
Operations and installation manual are shipped with PED to merchant or acquirer, including information
- Part list
- Installation instruction
- Activation procedure
- Security
- Repair and disposal

5.4 Service Removal or Repair
The PED should be dismounted and removed from service from authorized personnel only. Each removed PED must be returned to Paytec for either repair or disposal.

5.5 Decommission
Sensitive data must be erased before refurbishing the device or removing it permanently from service. The device shall go to tampered status, e.g. disassembly of the device, in this state sensitive data are erased.
6 Security
PSP PED is designed with most advanced encryption and tamper responsivities available these days.

6.1 Hardware
PSP PED hardware comes with several tamper and removal detection mechanisms. In case of a tamper detection, the PSP leads in inoperable state and must be shipped to Paytec for investigation. In case of remounting or replacing the PED the reactivation procedure as instructed in operations and installation manual must be processed.

6.2 Software
At system startup installed SW-packages must pass the selftest, which verifies the certificate and signature of application code, to reach operational state.

6.3 Tamper indication
In general, in a non-operational PED transactions could not be initiated. See also 6.4 Selftest.
The PSP PED is a non-display device. To get detailed PED-status information, a connected host device must follow the instructions documented in PayTec SDK [3] description or with PayTec provided Testapplication designed for type approvals at accredited test facilities. 3rd party developers must sign a NDA to get PayTec SDK [3].

6.4 Selftest
PSP PED selftest runs automatically at system start up and periodically at least 23 hours after system start up.
If the PSP PED indicates a selftest error the PED leads in inoperable state and should be replaced.

6.5 Services and Roles
PSP PED will be managed with Paytec designed and approved Tools to deal with the PED complying security rules and requirements.

6.6 PIN confidentiality
PSP PED provides a privacy shield, respecting PCI-requirements TA8, to support PIN confidentially in the transaction. In addition, the Cardholder should take care at PIN entry on PED.
7 KEY Management
On-Line PIN is not supported by PSP PED. As result of this, no key management techniques take place.

7.1 KEY Table

<table>
<thead>
<tr>
<th>Key Type</th>
<th>Purpose</th>
<th>Algorithm</th>
<th>Size (Bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root CA Certificate</td>
<td>Root Certificate</td>
<td>RSA</td>
<td>2048</td>
</tr>
<tr>
<td>Public Keys</td>
<td>Key Signing, Public Key verification</td>
<td>RSA</td>
<td>2048</td>
</tr>
</tbody>
</table>

7.2 KEY Replacement
If tamper protection mechanism has been triggered, the keys in PSP PED are erased irreversibly from device. In this case the PSP PED must follow 5.4.

Keys in a non-tampered PED could be changed by authorized personnel either remotely or on-site under respect of PCI-rules approved.

7.3 Cryptographic algorithms
PSP PED provides
- RSA (2048)
- 3-DES(128)
- AES(128)
- SHA-256

8 System Administration

8.1 Software updates
PSP PED security firmware certified and signed in Paytec security rooms could be loaded to secured PSP device. Cryptographically authenticated updates and patches could be loaded into the PED. Installer rejects and removes wrong or unknown certified software binaries.

8.2 Configuration settings
PSP PED is functional when receives by the merchant or aquirer. No security sensitive configuration settings are provided.