

PNC SAC - PED and clear text entry

Scope

There are certain situations where a PED must allow for entry of numeric information that leaves the PED in clear. This is a situation that may be used by a "dishonest terminal" to get a cardholder to enter the PIN in the wrong mode leading to a PIN exposure. Thus there has to be rules and limitations for such situations.

PNC SAC

The international set of rules (PCI - PED Security Requirements Manual) has focused on the control over the display that guides the cardholder during the transaction in order to limit the possibility to issue a misleading text. Such control is only possible in situations where the display (at least logically) is an integrated part of the PED. In a lot of self service terminals the display is totally independent of the PED. Also the mere use of such a display makes it practically impossible to have a formal certification process for all information to be shown on the display.

In PNC SAC there has been a discussion about how to handle the requirements for a PED without an integrated display. On the PNC SAC (at that time SÄKO-I) meeting of December, 2, 2004, a set of rules were decided. Based on new information and further discussions on the meeting of June, 21th, the rules were extended as defined below.

Rules for PED and clear text entry

Based on the available information PNC SAC, finds that the currently accepted implementations for clear text entry should be conformant to the PCI PED rules, since they are "clearly distinguishable" from PIN entry.

1. Clear numeric entry limited to a maximum of 3 digits, terminated by the ENTER key.
2. Clear numeric entry of unlimited length if preceded by a function key and terminated by the ENTER key.
3. Clear numeric entry of unlimited length, if the display texts are under the control of the PED security application either as constants in software or protected by a cryptographic MAC.

PNC SAC see, for the moment, no need to differentiate these rules depending on if the device is an EPP (without display) or a PED with integrated display.

Guideline update

This view will be incorporated in the existing guidelines (former SÄKO-I) at the earliest possible date.