Specification Bulletin No. 103
First Edition April 2012

Unpredictable Number generation

This specification update removes a statement from Book 4 regarding payment system specifications for Terminal UNs and advises terminal vendors of extended lab testing of UNs during type approval.

Effective Dates

The effective date is immediate.

Applicability

This Specification Bulletin applies to:

- *EMV Integrated Circuit Card Specifications for Payment Systems Version 4.3 Book 4 Cardholder, Attendant and Acquirer Interface Requirements*

Related Documents

- None

Description

This bulletin removes a statement from Book 4 regarding payment system requirements for Terminal Unpredictable Numbers (UNs) and provides notice to terminal vendors of extended UN testing during Type Approval.

Background

Ideally the Unpredictable Number generated by a terminal should (as noted in Specification Update Bulletin 50) be truly unpredictable even given access to all previous such numbers generated by the terminal and it should be infeasible for an attacker to control the next Unpredictable Number that the terminal generates.

Specification Change Notice

Please remove the sentence

An unpredictable number shall be generated in accordance with an individual payment system's specifications.

from the end of the first paragraph of Section 6.5.6 of Book 4.

Notice to Terminal Vendors

Terminal vendors are reminded that Bulletin SU50 (2006) states:

> *Ideally the Unpredictable Number generated by a terminal should be truly unpredictable even given access to all previous such numbers generated by the terminal and it should be infeasible for an attacker to control the next Unpredictable Number that the terminal generates.*

Terminal vendors are advised that the Type Approval ICS document is being extended to require the vendor to assert that the UN generator to be used with the kernel meets criteria as follows.

The vendor will be expected to assert that their UN generators produce numbers that are unpredictable and why this is the case. Possibilities include:

- approval by PCI,
- following international guidance on random number generation (e.g. ISO/IEC 18031) and satisfying international statistical tests (e.g. NIST SP 800-22).

Type Approval will introduce additional testing.