SRC
Security Research & Consulting GmbH

Emil-Nolde-Str. 7
53113 Bonn

Telefon: +49(0)228/2806-100
Telefax: +49(0)228/2806-199

E-mail: info@src-gmbh.de
Internet: www.src-gmbh.de

Verband Technical Cooperation ep2
c/o Advokaturbüro Utzinger
Toggwilerstrasse 90
8706 Meilen

Switzerland

Thomas Zell
thomas.zell@src-gmbh.de
ext: -174

December 8th 2016

PCI compliance of the ep2 v7 key derivation

To whom it may concern,

we confirm that the key derivation of the ep2 protocol as defined in section 8.9 – 8.11 of [ep2] meets the cryptographic requirements for PIN and PAN encryption as defined in the PCI standards (PCI DSS, PCI PA-DSS, PCI PIN, PCI PTS, PCI P2PE).

All PCI standards require conformance with [ISO11568] for key derivation:

- Requirement B11, K17 of [PTS],
- Requirement 20-3 [PIN], and
- Requirement of 6E-4.3 [P2PE].

The ep2 protocol implements a unique key per transaction (UKPT) scheme, which derives unique triple-length TDES keys for each device and each transaction using a method compliant with [ISO11568] section 5.4 “Key derivation”. This section stipulates that:

> *“The derived key generation procedure utilizes a non-reversible process, as illustrated in Figure 3, using the derivation key and data that uniquely identifies the target cryptographic device.”*

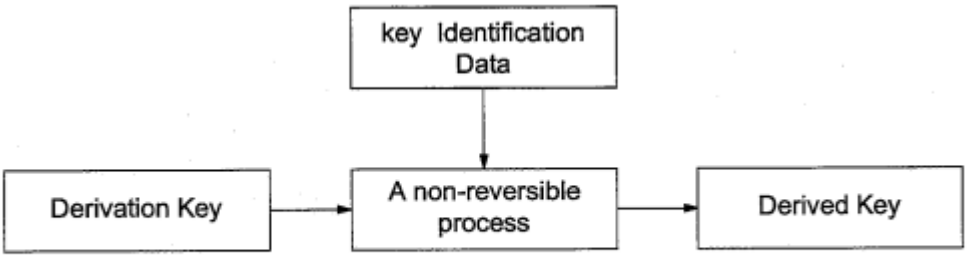

Figure 3 — Generation of a derived key

These elements are present in the ep2 key derivation processes. Three different cases are specified:

1. Diversification of the session key which is randomly generated for each transaction:

a) „Derivation Key“: A new triple-length TDES key is randomly generated for each transaction in the terminal using the PCI PTS approved random number generator.

b) „Key Identification Data“: A 24 byte constant C as defined in section 5.1.4 of [ep2], which is unique for each key purpose.

c) „Derived Key“: Derived session key used for Transaction Certificate generation, PIN encryption, MACing, data encryption, or key encryption.

2. Derivation of a base key for PAN Receipt encryption, which is unique per terminal:

a) „Derivation Key“: The acquirer randomly generates and stores a triple-length TDES key.

b) „Key Identification Data“: 24 bytes of SHA-256 hashed and truncated acquirer specific data that must be unique per terminal.

c) „Derived Key“: Terminal unique base key for PAN Receipt encryption.

3. Derivation of a PAN Receipt encryption key, which is unique per transaction:

a) „Derivation Key“: Terminal unique base key for PAN Receipt encryption.

b) „Key Identification Data“: 24 bytes of SHA-256 hashed and truncated concatenation of data which can be dynamically configured by the acquirer via a DOL.

c) „Derived Key“: Transaction unique key for PAN Receipt encryption.

In all cases the „non-reversible process“ is defined as follows: The Key Identification Data is encrypted with TDES in CBC mode with IV=0. The result is used as the Derived Key. It is not possible to calculate the Derivation Key from the Derived Key and the Key Identification Data without breaking the security of the TDES algorithm.

Additionally, minimum key lengths are defined in

- Definition of “Strong Cryptography” in [PCIGLOSS],
- Appendix E of [PTS],
- Normative Annex C of [PIN], and
- Normative Annex C of [P2PE].

All of these requirements are met by using triple-length TDES keys.

Under the conditions that

- the key generation processes of the acquirer are PCI compliant,
- the acquirer specific derivation base is unique per terminal, and
- the derivation data defined by the DOL are guaranteed to be unique per transaction,

the ep2 key derivation can be considered to be secure and is compliant with all PCI standards.

Please do not hesitate to contact the undersigned for any further details.

Best regards,

SRC Security Research & Consulting GmbH

Dr. Thomas Zell (PCI QSA (P2PE), PA-QSA (P2PE))

References:

[ep2] ep2 Security Specification, Version 7.0.0, December 8, 2016

[PCIGLOSS] Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS), Glossary of Terms, Abbreviations, and Acronyms, Version 3.2, April 2016

[PTS] Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI), Modular Derived Test Requirements, Version 5.0, September 2016

[PIN] Payment Card Industry (PCI) PIN Security Requirements, Version 2.0, December 2014

[P2PE] Payment Card Industry (PCI) Point-to-Point Encryption, Solution Requirements and Testing Procedures, Version 2.0 (Revision 1.1), July 2015

[ISO11568] ISO 11568-2:2012, Financial services -- Key management (retail) -- Part 2: Symmetric ciphers, their key management and life cycle, 2012-02-01

About SRC

SRC is an independent consultancy company that was founded in 2000 by four German banking service providers as the joint center of excellence for payment systems and IT security.

SRC is a widely recognized and well respected company with experienced and highly skilled employees, some of whom have been working as IT security consultants for more than twenty-five years. SRC's mission is to become the leading consulting company when it is about products and services around the creation, implementation and operation of secure systems – for the financial institutions or insurance companies, the retail sector, tourism industry, public services or manufacturers. SRC's professional services organization offers a wide variety of consulting, training and deployment support to its customers.

As an independent consultancy, SRC supports its customers in any question concerning IT security and thus designs, specifies, develops, evaluates, and certifies security applications in general, and in the areas of electronic payment transactions, chip card-, e- and m-commerce, as well as digital signatures or the security of computer networks in specific.

Already in 2003, SRC was the first company worldwide to successfully complete the process of accreditation with both MasterCard and Visa. Since then, SRC is authorized to conduct security assessments on behalf of the payment schemes.

SRC is one of very few companies worldwide that are awarded with accreditations as

- PCI Qualified Security Assessor (PCI QSA)
- PCI Approved Scanning Vendor (PCI ASV)
- PCI Payment Application Qualified Security Assessor (PA-QSA)
- PCI PIN Transaction Security testing lab (PCI PTS)
- PCI QSA (P2PE) and PA-QSA (P2PE) for the assessment of Point-to-Point-Encryption Solutions (P2PE)

by the PCI SSC.

SRC is an accredited "Logical Security" and "Physical Security" auditor for the assessment of plastic card personalization companies within in the MasterCard Global Vendor Compliance Program.

SRC is operating a Common Criteria security evaluation facility and is approved by the German Federal Office for Information Security (BSI) according to ISO/IEC 17025.

SRC has been cleared by the German Government to access information classified up to NATO-level "SECRET".