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

SRC
security consulting

Technical Cooperation ep2
c/o Gebert Treuhand
St. Gallerstrasse 58c
9500 Will

Switzerland

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

April 14th 2023

PCI requirements and the ep2 v8 protocol

To whom it may concern,

we confirm that the security specification of the ep2 protocol v8.x as defined in [ep2] is able to meet the applicable technical requirements for PIN and account data encryption and processing as defined in the following PCI standards [PCIDSS] (resp. [PCIGLOSS]), [PCIPTS], [PCIHSM], [PCIPIN], [PCIP2PE], [CPoC], [SPoC], and [MPoC]. Therefore, it is possible to implement the ep2 protocol in a PCI compliant way.

SRC reviewed the following items in detail:

- Algorithms and key strengths (*Note that RSA keys must have a length of 3072 bits in order to establish 128 bit AES keys, except for the allowance granted in [PCIPIN] and [PCIP2PE] requirement 10-1*)
- Key management and key derivations (see also [Equiv])
- PAN surrogate mechanism

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

Best regards,

SRC Security Research & Consulting GmbH

Dr. Thomas Zell (P2PE Assessor, P2PE Application Assessor)

PCI requirements and the Key Derivation Function (KDF)

we confirm that the key derivation of the ep2 protocol as defined in section 8.11 – 8.13 of [ep2] meets the applicable cryptographic requirements for PIN and account data encryption as defined in the PCI standards [PCIDSS] (resp. [PCIGLOSS]), [PCIPTS], [PCIHSM], [PCIPIN], [PCIP2PE], [CPoC], [SPoC], and [MPoC].

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

- Requirement B9 of [PCIPTS], resp. B10 of [PCIHSM], and
- Requirement 20-3 of [PCIPIN] and [PCIP2PE]

The ep2 protocol implements a unique key per transaction (UKPT) scheme, which derives unique 128-/256-bit AES keys (with an effective strength of 128 bits due to the key establishment mechanism used) 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.”*

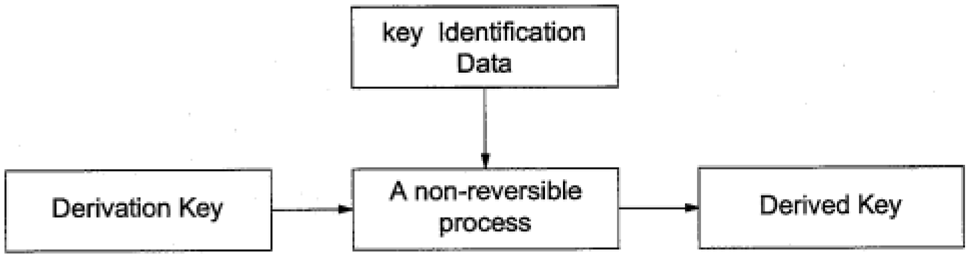

Figure 3 — Generation of a derived key

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 128-bit value is randomly generated for each transaction in the terminal using the PCI PTS approved random number generator.
   b) „Key Identification Data“: A 32 byte randomly generated salt and an 8 byte constant C as defined in section 5.1.4 of [ep2], which is unique for each key purpose.
   c) „Derived Key“: Derived 128-/256-bit AES 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 128-bit key.
   b) „Key Identification Data“: 32 bytes of SHA-256 hashed acquirer specific data that must be unique per terminal and a 32 byte acquirer specific salt.
   c) „Derived Key“: 128-bit terminal unique base key for PAN Receipt encryption.
3. Derivation of a PAN Receipt encryption key, which is unique per transaction:
   a) „Derivation Key“: 128-bit terminal unique base key for PAN Receipt encryption.
   b) „Key Identification Data“: SHA-256 hashed concatenation of 24 bytes of data, which can be dynamically configured by the acquirer via a DOL.

c) „Derived Key“: 128-bit AES Transaction unique key for PAN Receipt encryption.

In all cases, the „non-reversible process“ is defined as follows: HKDF scheme (extract-then-expand procedure) defined in [RFC5869] following the recommendations of [SP800-56C]. The following HKDF options are used:

- Hash Function: SHA-256
- Salt: <Salt>, 32 Bytes
- Input Keying Material Length: 16 Bytes
- Output Keying Material Length: 16 Bytes or 32 Bytes

Additionally, minimum key lengths are defined in

- Definition of “Strong Cryptography” in [PCIGLOSS],
- Appendix E of [PCIPTS],
- Normative Annex C of [PCIPIN], and
- Domain 5 Normative Annex C of [PCIP2PE].

All of these requirements are met by using 128-bit AES 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 does not violate any PCI requirements.

PCI requirements and the PAN surrogate mechanism

PCI DSS v4.0 introduced the new requirement 3.5.1.1, which requires the use of keyed cryptographic hashes to render the PAN unreadable. To take this into account, ep2 defines an HMAC-based surrogate mechanism, which uses a key loaded into the POI as a TR-31 key block.

References:

[ep2] eft/pos 2000 Security Specification, eftpos Engineering GmbH, Version 8.0.0, December 31 2021

[PCIDSS] Payment Card Industry (PCI) Data Security Standard (DSS), Requirements and Security Assessment Procedures, Version 4.0, March 2022

[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

[PCIPTS] Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Derived Test Requirements, Version 6.1, March 2022

[PCIHSM] Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) Modular Derived Test Requirements, Version 4.0, December 2021

[PCIPIN] Payment Card Industry (PCI) PIN Security Requirements and Testing Procedures, Version 3.1, March 2021

[PCIP2PE] Payment Card Industry (PCI) Point-to-Point Encryption Security Requirements and Testing Procedures, Version 3.1, September 2021

[CPoC] Payment Card Industry (PCI) Contactless Payments on COTS (CPoC), Security and Test Requirements, Version 1.0, December 2019

[SPoC] Payment Card Industry (PCI) Software-based PIN Entry on COTS (SPoC), Security Requirements, Version 1.1, June 2020

[MPoC] Payment Card Industry (PCI) Mobile Payments on COTS, Security Requirements, Version 1.0, November 2022

[RFC5869] HMAC-based Extract-and-Expand Key Derivation Function (HKDF), IETF, May 2010

[SP800-56C] Recommendation for Key-Derivation Methods in Key-Establishment Schemes, NIST, Rev. 2, August 2020

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

[Equiv] Review of the equivalence of ep2 communication protocol messages to Key Blocks according to PCI PIN Security requirements (TR-31 and TR-34), Prof. Dr. Ernst-Günter Giessmann, 2023-04-13

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 Secure Software Assessor
- PCI PIN Transaction Security testing lab (PCI PTS)
- P2PE Assessor and P2PE Application Assessor for the assessment of Point-to-Point-Encryption Solutions (P2PE)
- PCI Qualified PIN Assessor (QPA)
- PCI Card Production Security Assessor (CPSA)

by the PCI SSC.

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.