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

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

Switzerland

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

November 22nd 2023

PCI requirements and the ep2 PAN surrogate mechanisms

To whom it may concern,

we discuss how the ep2 mechanisms of generating PAN surrogate values relate to applicable PCI requirements.

Pepper based mechanism

The PAN is appended with a secret 128-bit salt value (“pepper”) and then hashed with SHA-256. The result of this operation is not considered to be cardholder data according to requirement 3.4 of [PCIDSS31] and requirement B24 of [PCIPTS]. It does, however, not meet the new requirement 3.5.1.1 introduced in [PCIDSS40] and is therefore no longer compliant after 01 April 2025.

SRC reviewed the following items in detail:

a) SHA-256 is considered to be “strong cryptography”.

b) Appending a secret 128-bit salt makes reversing the hash infeasible even if the truncated PAN is available at the same time.

c) The salt is managed in accordance with B24:

   1. unique per merchant (see also item (e))
   2. securely loaded (equivalent to a secret key)
   3. securely stored (equivalent to a secret key)

d) The use of the SKeyEnc key derivation mechanism to encrypt the salt for loading into a POI is compliant with [PCIPTS] key management requirements as

   1. the salt can be considered a key of an HMAC-like algorithm,
   2. other keys (KeyPANReceipt) are loaded in a separate session and therefore a completely independent key encryption key is enforced,
   3. the purpose is cryptographically bound within the protocol message (via MAC) and is loaded as a TR-31 key block in ep2 v8.0.

e) [PCIPTS] does not further define the term “unique per merchant”. In the PCI PTS scope, it is only required that the POI device implements a mechanism to securely load externally generated salt values and provide guidance documentation. The management of these values is in scope of [PCIDSS31], which does not make any specific statements about related procedures. It is recommended to follow the key management requirements described in requirement 3 of [PCIDSS31] and treat it equivalent to a secret key. PCI DSS allows sharing of keys with other PCI DSS compliant parties if that is required, as long as they are stored “in the fewest possible locations” (requirement 3.5.4 [PCIDSS31]).

HMAC based mechanism

A secret key is derived from a 128-bit secret loaded into the POI based on the expansion process defined in [RFC5869] using HMAC with SHA-256. As the derivation input, data defined by a configurable DOL is used. Therefore, this derivation is capable of generating a unique key for each PAN.

The result of applying the HMAC-SHA256 algorithm to the full PAN with this derived key is not considered to be cardholder data according to requirement 3.4 of [PCIDSS31], the new requirement 3.5.1.1 introduced in [PCIDSS40], and requirement B24 of [PCIPTS].

SRC reviewed the following items in detail:

a) HMAC-SHA256 is considered to be “strong cryptography” and a “keyed cryptographic hash”.

b) The secret HMAC-key makes reversing the hash infeasible even if the truncated PAN is available at the same time.

c) The secret HMAC-key can be considered as a “salt” that is managed in accordance with B24:

   1. unique per merchant (see also item (e))
   2. securely loaded (equivalent to a secret key)
   3. securely stored (equivalent to a secret key)

d) The use of the SKeyEnc key derivation mechanism to encrypt the key for loading into a POI is compliant with [PCIPTS] key management requirements and the HMAC-key is loaded as a TR-31 key block.

e) [PCIPTS] does not further define the term “unique per merchant”. In the PCI PTS scope, it is only required that the POI device implements a mechanism to securely load externally generated salt values and provide guidance documentation. The management of these values is in scope of [PCIDSS40]. The HMAC-key must be treated as a secret key according to requirement 3.5.1.1. PCI DSS allows sharing of keys with other PCI DSS compliant parties if that is required, as long as they are stored “in the fewest possible locations” (requirement 3.6.1.4 of [PCIDSS40]).

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

Best regards,

SRC Security Research & Consulting GmbH

Dr. Thomas Zell
22.11.2023 13:06 Uhr

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

References

[PCIDSS31] Payment Card Industry (PCI) Data Security Standard (DSS), Requirements and Security Assessment Procedures, Version 3.2.1, May 2018

[PCIDSS40] Payment Card Industry (PCI) Data Security Standard (DSS), Requirements and Security Assessment Procedures, Version 4.0, March 2022

[PCIPTS] Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Derived Test Requirements, Version 6.2, January 2023

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

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.