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

June 28th 2019

PCI compliance of the ep2 PAN surrogate mechanism

To whom it may concern,

we confirm that the ep2 mechanism of generating a PAN surrogate value is compliant with PCI: 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 [PCIDSS] and requirement K16 of [PCIPTS].

SRC reviewed the following items in detail:

- SHA-256 is considered to be "strong cryptography".
- Appending a secret 128-bit salt makes reversing the hash infeasible even if the truncated PAN is available at the same time.
- The salt is managed in accordance with K16.1 and K16.2:
  - unique per merchant
  - securely loaded (equivalent to a secret key)
  - securely stored (equivalent to a secret key)
- 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
  - the salt can be considered a key of an HMAC-like algorithm,
  - other keys (KeyPANReceipt) are loaded in a separate session and therefore a completely independent key encryption key is enforced,
  - the purpose is cryptographically bound within the protocol message (via MAC).

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:

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

[PCIPTS] Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI), Modular Derived Test Requirements, Version 5.1, March 2018

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".