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 22nd 2017

PCI compliance and the ep2 v7 protocol

To whom it may concern,

we confirm that the ep2 protocol v7.0.0 as defined in [ep2] is able to meet the technical requirements for PAN encryption and processing as defined in the PCI DSS standard v3.2 [PCIDSS]. Therefore, it is possible to implement the ep2 protocol in a PCI DSS compliant way.

SRC reviewed the following items in detail:

- Chapter 9 “Security Specification” of [ep2] meets the [PCIGLOSS] definition of “Strong Cryptography” under the condition that 2048 bit RSA keys are used:

  At the time of publication, examples of industry-tested and accepted standards and algorithms include AES (128 bits and higher), TDES/TDEA (triple-length keys), RSA (2048 bits and higher), ECC (224 bits and higher), and DSA/D-H (2048/224 bits and higher). See the current version of NIST Special Publication 800-57 Part 1 for more guidance on cryptographic key strengths and algorithms.
- [ep2] requires encrypting cardholder data (CHD) directly in the POI or PSP-System in a way that only the acquirer can decrypt it.
- [ep2] does not require storage of sensitive authentication data (SAD) after authorization.
- Chapter 10 “Interface Specification” and 11 “Data Dictionary” of [ep2] specify encryption of all PCI relevant data elements (CHD and SAD) in ep2 protocol messages.
- Use cases described in the [ep2] do not contradict any PCI DSS requirements.

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

[PCIDSS] Payment Card Industry (PCI) Data Security Standard (DSS), Requirements and Security Assessment Procedures, Version 3.2, April 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

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".