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

25th October 2021

To whom it may concern,

PCI requirements relevant for the ep2 component secret

The ep2 protocol defines a “component secret”, which allows the host to authenticate POIs, which are sending transactions. The following statements can be made:

- The “component secret” is not a cryptographic key since no cryptographic operations are performed with it. It can therefore be considered a password.
- The loading of the “component secret” could be considered a sensitive service according to [PTS] DTR B5, which means that there should be protection in place during loading, but it is not in scope of requirement B9 (Key Management). Also, key strengths equivalents defined in Appendix E do not have to be fulfilled with regards to the length of the secret.
- No current PCI standard requires that POIs are to use authentication, with one exception: [P2PE] requirement 4B-1.4. Outside of a P2PE solution POI authentication is entirely optional.
- Authenticating via component secret can be used to fulfil [P2PE] requirement 4B-1.4, since the use of cryptographic keys is not mandatory (“may occur”).

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

Yours sincerely,

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

SRC Security Research & Consulting GmbH

References:

[PTS] Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Derived Test Requirements, Version 6.0, June 2020

[P2PE] Payment Card Industry (PCI) Point-to-Point Encryption Security Requirements and Testing Procedures, Version 3.0, December 2019

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.

Today, SRC is one of very few companies worldwide that are awarded with PCI SSC accreditations and recognitions as

- PCI Qualified Security Assessor (PCI QSA)
- PCI Approved Scanning Vendor (PCI ASV)
- PCI Payment Application Qualified Security Assessor (PCI PA-QSA),
- PCI PIN Transaction Security Testing Lab (PCI PTS),
- PCI Contactless Payments on COTS and Software-Based PIN Entry on COTS (CPoC and SPoC) Security Testing Lab,
- PCI QSA (P2PE) und PA-QSA (P2PE) for the assessment of Point-to-Point-Encryption (P2PE) solutions and P2PE applications,
- PCI 3DS Assessor for validation of 3DS service providers according to PCI 3DS standard,
- PCI Qualified PIN Assessor (QPA) for PIN security assessments of service providers according to PCI PIN requirements,
- PCI Card Production Security Assessor (CPSA) for validation of card production entities according to PCI Card Production and Provisioning (PCI CPP) Logical and Physical Security Requirements.

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".