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

October 30th 2020

Use of triple length TDES in ep2 v7.x with regard to PCI SSC requirements

To whom it may concern,

in response to the announcement of NIST (cf. [SP800-131A] dated March 2019) to disallow the use of three-key TDES encryption after 2023, TeCo EP2 has invited SRC to analyse the potential impact on the ep2 protocol and its PCI compliance, considering that ep2 v7.x will remain in use until 2026-10-31.

With this letter, SRC would like to provide its expert opinion on this subject matter.

PCI SSC defines minimum cryptographic requirements in various standards and documents:

- PCI [PTS] and [HSM],
- PCI [PIN],
- PCI [P2PE] and
- PCI [CPoC] and [SPoC].

Note that the notion "Strong Cryptography" is defined only in the PCI DSS [Glossary], and there are no cryptographic requirements in the PCI DSS standard itself.

In the past, PCI has regularly adjusted its minimum cryptographic requirements based on NIST recommendations. However, payment specific particularities usually have been taken into account. One example is the widespread ongoing use of double length TDES based DUKPT or use of less than 2048 bit RSA keys in EMVCo specifications. Double length TDES is disallowed by NIST since 2015, but is still acceptable according to PCI for encryption with unique keys per transaction (excluding CPoC and SPoC).

PCI has recently started to pave the way for AES support by requiring ISO format 4 PIN block support in all POIs since PTS version 5.0. However, older PCI PTS v4.x approved models may still be deployed until April 2023, to which the lifetime of a POI adds before completion of migration and v4.x being phased out. Typically, the use of a device with a valid approval is revoked only if a specific device represents a significant threat to the payment systems because of a vulnerability.

Usually, PCI provides for migration periods for changing cryptographic requirements, in multiple stages and with comfortable grace periods, as can be seen for example with new cryptographic key block requirements in PCI PIN and P2PE.

Currently, PCI has not yet announced any deadline concerning the general termination of TDES use. However, some restrictions have already been put in place: e.g. PCI SSC disallowed non-unique-key-per-transaction based double length TDES encryption of cardholder data. This change was enforced without any pre-announcements, soon after NIST disallowed the algorithm in 2015.

Notably, ep2 v7.3.0 does not strictly meet the PCI CPoC and SPoC minimum cryptographic requirements referring to AES with 128 bits key length. Both [CPoC] and [SPoC] Program Guides though allow deviations from these requirements if an at least equivalent security level can be demonstrated. Concerning the use of TDES, SRC sees a risk that either the equivalence cannot be demonstrated or that the justification is not acceptable to PCI SSC.

In summary, SRC is convinced that ep2 v7.x can be used without significant changes until its planned end-of-life 2026-10-31. SRC does not see any challenges with regard to ep2 compliance with PCI requirements, with the exception of the a.m. risks in CPoC and SPoC programs. SRC is also not aware of any planned change and/or deadline with regard to the use of TDES. Nevertheless, SRC recommends upgrading to AES based cryptography for ep2 v8.0.0 in order to eliminate future compliance risk.

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:

[SP800-131A]	NIST Special Publication 800-131A, Revision 2, March 2019
[PTS]	Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Derived Test Requirements, Version 6.0, June 2020
[HSM]	Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) Modular Derived Test Requirements, Version 3.0, June 2016
[PIN]	Payment Card Industry (PCI) PIN Security Requirements and Testing Procedures, Version 3.0, August 2018
[P2PE]	Payment Card Industry (PCI) Point-to-Point Encryption Security Requirements and Testing Procedures, Version 3.0, December 2019

[Glossary]	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
[CPoC]	Payment Card Industry (PCI) Contactless Payments on COTS (CPoC), Program Guide, Version 1.0, December 2019
[SPoC]	Payment Card Industry (PCI) Software-based PIN Entry on COTS (SPoC), Program Guide, Version 1.2, June 2020

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".