

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

Switzerland

Thomas Zell

thomas.zell@src-gmbh.de

ext: -174

July 4th 2024

PCI CPoC/SPoC/MPoC and ep2 single zone security

To whom it may concern,

we discuss how the ep2 single zone security relates to the PCI CPoC, SPoC, and MPoC requirements.

1. SPoC requires the use of an external “SCRP” device, which re-encrypts the PIN before it is sent to the backend.
2. CPoC and MPoC allow for encrypting the data directly on the COTS.

Whereas, in the first case, it is not possible to implement the ep2 security directly on the COTS, there is no requirement in the second case that prevents this. Care has to be taken that requirement 1D-1.5 (MPoC) is met for any long-term keys such as the Key PAN receipt TRM.

The Component Secret can be stored in encrypted form on the COTS protected by white box cryptography as long as the white box cryptography itself is rotated according to 1B-2.4 (MPoC) requiring a re-encryption of the component secret.

SRC strongly recommends to further decrease the attack surface by including secrets, which are provided by the backend / A&M system and never stored on the COTS, in the key derivation for the protection key of the Component Secret, so that the Component Secret cannot be decrypted solely based on the information stored on the COTS.

[MPOC] defines the following roles:

- MPoC Software Vendor: This is an optional role of a third party providing the MPoC Software (SDK) (see Domain 1 of [MPOC]).
- Attestation and Monitoring Service Provider: This is an optional role responsible for deployment and operation of the attestation and monitoring component of the MPoC Software within a back-end environment (see Domain 3 of [MPOC]).
- MPoC Solution Provider: This is the entity that has overall responsibility for the implementation and management of an MPoC Solution. The MPoC Solution provider is responsible for ensuring that all requirements are met, including any requirements fulfilled by other organizations on behalf of the MPoC Solution provider.

Therefore, there is no specific restriction on who can be an MPoC Solution Provider. The same applies to CPoC Solutions.

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

Best regards,

SRC Security Research & Consulting GmbH

A handwritten signature in blue ink, appearing to read 'Peter Jung', with a long, sweeping horizontal line extending to the right.

Peter Jung (PCI CPoC/SPoC/MPoC Assessor)

References

- [CPOC] Payment Card Industry (PCI) Contactless Payments on COTS (CPoC), Security and Test Requirements, Version 1.0, December 2019
- [SPOC] Payment Card Industry (PCI) Software-based PIN Entry on COTS (SPoC), Test Requirements, Version 1.1, June 2020
- [MPOC] Payment Card Industry (PCI) Mobile Payments on COTS, Security and Test Requirements, Version 1.0.1, February 2023