Platform Security Evaluation Certificate

Please accept this document as confirmation of the EMVCo Security Evaluation Process.

Certificate Number: **PCN0199.05**

Date PCN Issued: **30 Jun 2023** **PCN Expiry date:** **30 Jun 2027**

Company Name: **Thales DIS France SAS**

Address: Avenue Pic de Bertagne
BP100
Gémenos Cedex 13881 France

Product Name : **Connected eSE 5.3.4**

Product Version: **v1.1 Rev. 01**

IC Manufacturer: STMicroelectronics (Rousset) SAS

IC Name: ST54L IC Version: rev. C

ICCN: ICCN0300 ICCN Issue Date: 04 Apr 2023

Platform Type: GlobalPlatform (open configuration)

Version Number: v2.3.1 (amdts A, B, C, D, E, F and H)

Security Laboratory: Serma

Conditions of Certification: User Guidance document(s) must be followed

Authorized by: Matheus Oliveira
Security Evaluation Working Group Chair
EMVCo, LLC
Date: 16 Oct 2026

Disclaimer: Although the secure implementation of any security mechanisms and product functionalities may be evaluated, the EMVCo Security Evaluation Process does not validate the cryptographic algorithms, methods and protocols themselves nor the absence of flaws or defects in the specifications used for product development.

The PCN number must be mentioned to all other vendors or when shipping the product. The use of the PCN number is limited to the product as detailed below. Please also reference the PCN number in any communication with EMVCo. The EMVCo Security Evaluation Process is intended to provide valuable and practical information relating to the general security performance characteristics and the suitability of use for smart card related products and IC chip-based tokens. The EMVCo Security Evaluation Process is designed to ensure a robust security foundation for these products at the product family and component level. The EMVCo Security Evaluation Process is an evolving process in relation to new attack techniques and technology. EMVCo therefore reserves the right to perform new/random security testing throughout the lifetime of the card which may impact certification. The full terms and conditions upon which EMVCo Compliance Certificates are issued by EMVCo are contained in the EMVCo Security Evaluation Process Document and the EMVCo Security Evaluation Certification Contract. The Product Provider, when distributing this EMVCo Compliance Certificate, shall deliver it in its entirety.

User Guidance Documents:

- D1595008/v1.0 - Operational guidance on CC platforms - Connected eSE 5.3.4

- D1595009/v1.0 - Operational guidance on CC platforms for VA - Connected eSE 5.3.4

- D1516176/v3.4 - Guidance for Secure application development on Thales Embedded Secure Solutions

- GPC_GUI_050/v2.0 - GPC_CompositionModel_SecurityGuidelinesForBasicAppln

- D1546158/v1.1 - Security Technical Note for guides of Thales Embedded Secure Solutions

- D1611592/v1.3 - Platform Identification and Configurability Connected eSE 5.3.4 v1.1 Rev. 01

Certification Reference Documents:

- EMVCo Security Evaluation Process, v5.5, January 2026
- Security Guidelines for Java Card, Multos and GlobalPlatform Implementations including Mobile Payments, v1.3, December 2022

Disclaimer: Although the secure implementation of any security mechanisms and product functionalities may be evaluated, the EMVCo Security Evaluation Process does not validate the cryptographic algorithms, methods and protocols themselves nor the absence of flaws or defects in the specifications used for product development.

The PCN number must be mentioned to all other vendors or when shipping the product. The use of the PCN number is limited to the product as detailed below. Please also reference the PCN number in any communication with EMVCo. The EMVCo Security Evaluation Process is intended to provide valuable and practical information relating to the general security performance characteristics and the suitability of use for smart card related products and IC chip-based tokens. The EMVCo Security Evaluation Process is designed to ensure a robust security foundation for these products at the product family and component level. The EMVCo Security Evaluation Process is an evolving process in relation to new attack techniques and technology. EMVCo therefore reserves the right to perform new/random security testing throughout the lifetime of the card which may impact certification. The full terms and conditions upon which EMVCo Compliance Certificates are issued by EMVCo are contained in the EMVCo Security Evaluation Process Document and the EMVCo Security Evaluation Certification Contract. The Product Provider, when distributing this EMVCo Compliance Certificate, shall deliver it in its entirety.