IC Security Evaluation Certificate

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

Certificate Number : ICCN0314

Date of issuance 17 Jun 2025 **Expiry Date: 17 Jun 2026**

Company: THALES DIS France SAS

Address: Arteparc - Bat D
Route de la Cote d'Azur
CS60105
Meyreuil 13590 France

Master Component: SIRIUS_CA_04

Hardware Revision: Rev. C

Child Lot 1: SIRIUS_CA_05
Child Lot 2: -
Child Lot 3: -
Child Lot 4: -
Child Lot 5: -

Manufacturing site(s): UMC Fab 12i (Singapore)

Firmware name / version: ROM Firmware rev. A - FLASH Firmware rev. 04 & 05

Crypto. library name / version: -

Other libraries name / version: RNG Post-processing library v1.0.8 & v1.1.1

Bootloader name / version: Loader v1.1 & v1.3

Security Laboratory: Leti

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

Authorized by: Alan Mushing
Security Evaluation Working Group Chair
EMVCo, LLC
Date: 15 Sep 2025

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 ICCN number must be mentioned to all vendors or when shipping the product. The use of the ICCN number is limited to the product as detailed below. Please also reference the ICCN 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:

- Sirius - User Manual, v0.14, 29 Jul 2025
- Secure 32 bits CPU Embedded Application Binary Interface (EABI), v0.6, March 2013
- S8 Instruction Set Architecture, v1.5rc, May 2023
- Sirius - Security Guidance, v0.13, 04 Jul 2025
- Sirius Loader - User Manual - v007 & v008, 02 Jun 2025
- Guidance - Secure Delivery, v1.2, 30 Nov 2021
- Sirius - Assembly Instructions, v0.2, 09 Nov 2023
- API Guide - Sirius_Firmware_Specification, v2.0, 20 Feb 2025
- SIRIUS Physical (TRUE) Random Generator (PTRNG) Derivation Function Library User Manual, v004, 17 Jul 2025
- SIRIUS PTRNG Startup procedure for AIS31, v1.3, 23 Jul 2025

Certification Reference Documents:

- EMVCo Security Evaluation Process, v5.4, July 2024
- Security Guidelines for Smart Card Integrated Circuits, v2.2, December 2022