TRUSTCB®

TRUST AND VERIFY

Certificate ID	SESIP-2100003-01
	TrustCB B.V. declares that
Product	STM32U585 TFM, Version 1.0.0 (based on TF-M Open Source version TF-M v1.0-RC2 and based on mcu_boot Open Source version, SHA1=a40b19976158b8d0d1016ba82dcd4f7c896efe37)
	of
Sponsor (and developer)	STMicroelectronics *in* Grenoble, France
	complies to the requirements described in the standard and ST
Standard	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.0, March 2020 **Based on** Common Criteria for Information Technology Security Evaluation (CC) Parts 1-3, Version 3.1 Revision 5 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3) COMMON CRITERIA
ST Reference	Security Target for STM32U585 family of device compliant with SESIP Profile for PSA Certified™ Level 3, version 2.0
	Summarized:
Assurance Package	SESIP3 *with* Physical Attacker Resistance *and* Software Attacker Resistance: Isolation of Platform SESIP™3
SESIP Profile	SESIP Profile for PSA Certified Level 3 V1.0ALP01
	As evaluated by:
Evaluation Facility	SGS Brightsight located in Barcelona, Spain
	Under scheme:
	SESIP™ TrustCB Scheme Procedures SESIP v2.1
Validity	Date of 1st issuance: 2021-07-23 Date of expiry: 2023-07-05
	Wouter Slegers, CEO