PSA Certified™ Security Assurance Certificate

psacertified™
level three

PSA Certified Level 3

Certificate Number:	0716053549921 - 10100
Date of Issue:	26/07/2021
Test Lab:	Brightsight
Certification Holder:	ST Microelectronics
Certified Product:	STM32U585 TFM
Description:	The STM32U5 series harnesses the security features of the Arm Cortex-M33 with TrustZone combined with ST security implementation and provide a new optimal balance between performance, power and security. STM32U585 is based on TF-M Open Source (version TF-M v1.0-RC2).
Hardware Version:	STM32U585 Die 482 Revision X
Software Version:	STM32U585 TFM v1.0.0 (STM32Cube_FW_U585_Security_certification V1.0.0)
Certification Type:	PSA Certified Level 3
Developer Type:	PSA Certified – Chip