




Certificate ID	SESIP-2400122-01	
	<i>TrustCB B.V. declares that</i>	
Product	STM32H573xx MCU version 1.3 with Secure Manager package version 1.2.2 (STM32Trust TEE Secure Manager)	
	<i>of</i>	
Sponsor (and Developer)	STMicroelectronics, 12 rue Jules Horowitz, 38000 Grenoble, FRANCE	
	<i>complies to the requirements described in Standard and ST Reference</i>	
Standard	<p>GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1, June 2021</p> <p>Based on ISO/IEC 15408-1:2009, -2 :2008, -3:2008, Common Criteria for Information Technology Security Evaluation (CC v3.1, rev 5), and ISO/IEC 18045:2008, Common Criteria Evaluation Methodology for Information Security Evaluation (CEM) v3.1, rev 5</p>	
ST Reference	STM32H573xx Security Target for STM32Trust TEE Secure Manager for PSA Certified™ Level 3 with SESIP Profile	
	<i>Summarised:</i>	
Assurance Package	<p>SESIP3 <i>with</i> Physical Attacker Resistance <i>and</i> Software Attacker Resistance – Isolation of Platform <i>and</i> Software Attacker Resistance – Isolation of Platform Parts <i>and</i> Software Attacker Resistance - Isolation of Application Parts</p>	
SESIP Profiles	<p>SESIP Profile for PSA Certified 3™ RoT Component Level 3 version 1.0 REL01</p> <p><i>As evaluated by:</i></p>	
Evaluation Facility	SGS Brightsight located in Delft, The Netherlands	
	<i>Under scheme:</i>	
Scheme	<p>SESIP <i>As described in</i> TrustCB Scheme Procedures v2.3</p>	
Validity	Date of issue:	2025-02-25
	Date of expiry:	2026-11-25
Certification Mark	<div>   </div>	
Signatory	Wouter Slegers, CEO	