


Certificate ID	SESIP-2400006-01	
	<i>TrustCB B.V. declares that</i>	
Product	CMRT RT-634 Root of Trust Core Version 2.2	
	<i>of</i>	
Sponsor (and Developer)	Rambus Inc. <i>in</i> San Jose, California, US	
	<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 v1.2, July 2023</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	SESIP Security Target for PSA Certified RoT Component Level 2 CMRT RT-634, version F dated 2024-02-20	
	<i>Summarised:</i>	
Assurance Package	SESIP2 <i>with</i> Software Attacker Resistance: Isolation of Platform	
SESIP Profile	SESIP Profile for PSA Certified RoT Component Level 2 version 1.0 REL 02	
	<i>As evaluated by:</i>	
Evaluation Facility	Riscure B.V. located in Delft, The Netherlands	
	<i>Under scheme:</i>	
Scheme	SESIP <i>As described in</i> TrustCB Scheme Procedures v2.3	
Validity	Date of issue: 2024-04-02 Date of expiry: 2026-03-28	
Certification Mark		
Signatory	Wouter Slegers, CEO	