TRUSTCB®
TRUST AND VERIFY

SESIP™

Certificate ID	SESIP-2300165-01
	TrustCB B.V. declares that
Product	RT-130 Root of Trust Core Version RT-130 FW4.2HW4.1
	of
Sponsor (and Developer)	Rambus Inc. *in* San Jose, USA
	complies to the requirements described in Standard and ST Reference
Standard	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1, June 2021 **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	SESIP Security Target for PSA Certified RoT Component Level 2 VaultIP RT-130, version F, 23023-11-24
	Summarised:
Assurance Package	SESIP2 *with* Software Attacker Resistance: Isolation of Platform
SESIP Profile	SESIP Profile for PSA Certified RoT Component Level 2 version 1.0 REL 02
	As evaluated by:
Evaluation Facility	Riscure B.V. located in Delft, The Netherlands
	Under scheme:
Scheme	SESIP *As described in* TrustCB Scheme Procedures v2.2
Validity	Date of issue: 2023-12-12 Date of expiry: 2025-11-24
Certification Mark	SESIP™2
Signatory	Wouter Slegers, CEO