




| | | |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Certificate ID | SESIP-2200036-01 | |
| | <i>TrustCB B.V. declares that</i> | |
| Product | OPTIGA [™] Trust M v3 SLS 32AIA010MK Version V3.00.2440 | |
| | <i>of</i> | |
| Sponsor (and Developer) | Infineon Technologies AG <i>in</i> Neubiberg, Germany | |
| | <i>complies to the requirements described in Standard and ST Reference</i> | |
| Standard | GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1, June 2021 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 |  |
| ST Reference | OPTIGA [™] Trust M v3 SLS 32AIA010MK Trusted subsystem, version 1.5 | |
| | <i>Summarised:</i> | |
| Assurance Package | SESIP3 <i>with</i> Physical Attacker Resistance | |
| SESIP Profile | SESIP Profile for PSA Certified [™] RoT Component Level 3, v1.0 REL 02 | |
| | <i>As evaluated by:</i> | |
| Evaluation Facility | SGS Brightsight 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: 2024-07-25 Date of expiry: 2026-05-28 | |
| Certification Mark |  |  |
| Signatory | Wouter Slegers, CEO | |