OPTIGA™ TPM SLB 9673 FW26.xx

OPTIGA™ TPM SLB 9673 FW26.xx は、強化されたセキュリティ機能を必要とするコネクテッド デバイスをターゲットとしたOPTIGA™ TPMファミリーの最新製品です。
この標準化された、すぐに使えるセキュリティソリューションは、I2Cインターフェイスを備えています。ネットワークインフラや、工場のロボットやPLC (Programmable Logic Controller) などの軽工業機械を識別、認証するための強固な基盤として機能します。さらに、データの完全性と機密性を保護します。
OPTIGA™ TPM SLB 9673 FW26.xxは、PQCで保護されたファームウェア更新メカニズム、拡張メモリ、および強力なアルゴリズムにより、将来的にも安定した動作を保証します。統合された復元機能により、NIST SP 800-193 Platform Firmware Resiliency Guidelinesに準拠したTPMファームウェアのリカバリーが可能です。OPTIGA™ TPM SLB 9673 FW26.xxは、「モノ」に固有の識別番号を付与し、IoTやネットワークに接続できるようにするものです。この番号は、ネットワーク上のIoT機器や装置の追跡やアクセス権の認証に利用することができます。偽造のリスクを回避するために、この番号は変更できないように保護されています。
プラットフォーム製造時に、アプリケーション固有のニーズに合わせてTPMを設定するためのコンフィギュレーションコマンド一式が用意されています。また、AESバルク暗号化、TPM固有IDの設定、エンドースメントプライマリーシードの設定など、セキュリティ機能が充実しています。

主な特長

- 最大1MHzのI²Cインターフェイス
- 拡張不揮発性メモリ (51 kB)
- 最新の暗号アルゴリズムに対応：RSA-4096まで、ECC NIST P384まで、SHA2-384まで
- TCG TPM2.0 (revision 1.59)、CCおよびFIPS認証
- XMSS署名によるPQC保護されたファームウェアアップグレード機構
- 薄型のUQFN-32パッケージ
- 拡張産業用温度範囲 (-40°C～+ 105°C)

主な利点

- 実績のある標準化されたターンキーセキュリティソリューション
- コモンクライテリアやFIPSの認証に基づく高い信頼性
- 前世代より暗号演算を高速化
- Linux OSプラットフォームとの統合が容易

競合製品に対する優位性

- XMSS署名によるPQC保護されたファームウェアアップグレード機構を備えた初のI2C TPMです。

製品関連情報/オンライン サポート

製品ページ

対象アプリケーション

- インフラ: ルーター
- 産業用オートメーション、ドライブ、PLC
- スマートビルディング: 監視カメラ
- EV充電
- 事業用: プリンター

製品概要およびユーザーマニュアルへのリンク

発注可能な部品番号	SP 番号	パッケージ
SLB9673XU20FW2610XTMA1	SP005722390	PG-UQFN-32
SLB9673AU20FW2610XTMA1	SP005722392	PG-UQFN-32