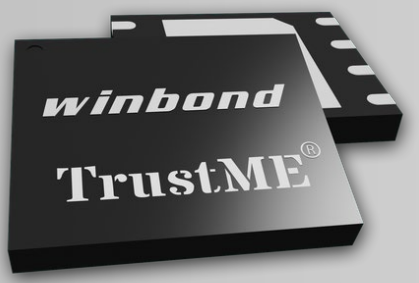
winbond
We Deliver

TrustME®
セキュアフラッシュメモリ-W77Q



標準SPIフラッシュメモリの置換え“Drop-In Replacement”から始める
セキュアフラッシュメモリ ― IoTセキュリティに革新を

実装の信頼性と拡張性を提供するセキュアフラッシュメモリ

ハードウェアセキュリティは堅牢なサイバーセキュリティの基盤となります。
セキュアストレージはハードウェアセキュリティの中核となります。

W77Qは既存のシリアルSPI NORフラッシュメモリ W25QJWファミリを継承

- ✓ 標準SPIフラッシュメモリを完全置換え可能（Drop-In Replacement）
- ✓ PCB基板やMPUの再設計不要

第三者機関による認定メモリ＝信頼を約束するソリューション！

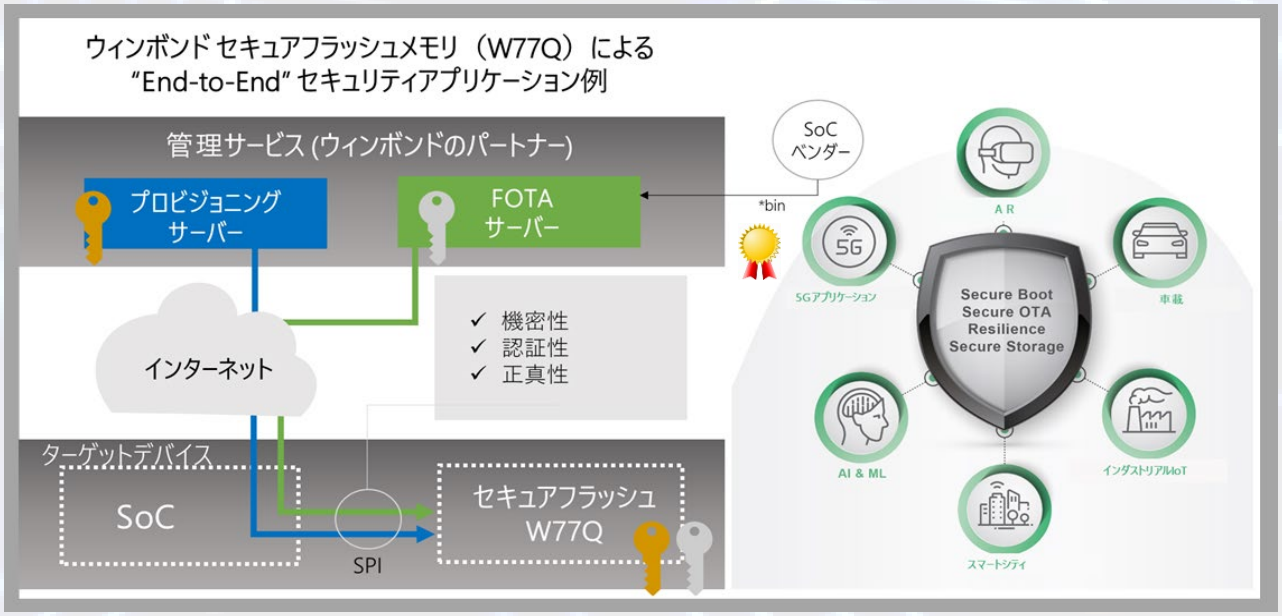
- ✓ 外部ラボにおける検証と評価
- ✓ CC EAL2[1)], SESIP[1)]

斬新なセキュリティ機能を搭載

- ✓ Root of Trust とセキュアブート
- ✓ セキュアOTA[2)] ファームウェアアップデート
- ✓ レジリエンシー（保護、検知、回復）
- ✓ セキュアデータストレージ

- ● CPUを用いないピュアなデジタルロジック設計アーキテクチャー
- ● コスト重視のプラットフォームに最適

[1)]: 申請中 [2)]: OTA = Over-The-Air



柔軟かつ幅広いメモリセキュリティ機能セット

W77Q TrustME® セキュアシリアルフラッシュメモリは、小パッケージで低消費電力を要求されるシステムにセキュアストレージを追加します。そのセキュリティレベルは、コモンクライテリア（Common Criteria）EAL2 セキュリティ認定要件を満たします。

W77Qは標準シリアルNORフラッシュメモリを完全置換え可能なメモリになっており、これまでのNORフラシュメモリと同じように使いつつ、さらに柔軟かつ高性能なセキュリティ機能を利用できます。すなわち、従来と同じeXecute In Place（XIP）によってコードフェッチ可能なセキュアコードストレージであり、またセキュアな鍵配置、管理およびストレージをサポートし、セキュアデータストレージや従来のデータストレージにもなります。

W77Qは洗練された暗号学的な通信チャネル（SoCとW77Q間、あるいはサーバーとW77Q間）を構築し、ユニーク鍵に紐づくデバイス個体認証、暗号学的なフラッシュメモリへのリード・ライトロック、データ正真性保護、セキュアファームウェアOver-the-Air（OTA）更新、Root-of-Trust（RoT）機能，セキュアリード・ライトイレース動作機能を持っています。

W77QシリーズのSPIは、Single、Dualおよび Quad モード、QPIモード動作（命令発行時からQuadモードを有効化）をサポートし、SPIクロック周波数は最大133 MHzまで、また Dual Transfer Rate（DTR）時は最大 66 MHzまでサポートします。

シングルダイセキュアソリューション

- コモンクライテリア（CC）EAL2に準拠
- IoTデバイスのためのセキュアRoot-of-Trust（RoT）
- 高速セキュアブート
- セキュアコード＆データストレージ
- アンチロールバック攻撃セキュアコード更新
- セキュアファームウェアOver-The-Air（OTA）更新
- ローカルおよびリモートでのセキュアチャネル構築（認証、暗号化、アンチリプレイ攻撃）
- ファームウェア正真性保護
- オンチップデータハッシュで高速コード認証処理
- 認証ウォッチドッグタイマーによるプラットフォームレジリエンシー
- セキュアユニークデバイスID
- 暗号学的セキュアライト保護
- セキュアな鍵プロビジョニングとストレージ
- リプレイ保護モノトニックカウンター

標準SPI NORフラッシュメモリを完全置換（Drop-In-Replacement）

- 業界最高速セキュアシリアルフラッシュメモリ
  - ✓ Execute In Place（XIP）
  - ✓ 133 MHz SPI Single/Dual/Quad/QPI
  - ✓ 66 MHz Dual Transfer Rate（DTR）Mode
  - ✓ 1ブロック当たり10万 回のイレース・ライトサイクル
  - ✓ 20年のデータリテンション
- リード・ライトアクセス制御
- Continuousリードとバーストリードモード（4KB境界で自動ラップアップ）
- 柔軟な4Kバイト単位のメモリ管理
- 4Kバイト単位のイレースブロック
  - ✓ ページプログラムモード（1コマンド当たり256バイトまで）
  - ✓ イレースプログラムSuspend & Resume
- ローパワー、シングル1.8V動作電源
- 広温度範囲動作
  - ✓ -40℃ ～ +105℃（産業グレードプラス）
- Known Good Die（KGD）をウェハーで提供
- パッケージ品: 8-pin SOP, 8-WSON, 16-pin SOP, 24-ball TFBGA

Website：www.winbond.com | Email：mkt_online.jp@winbond.com | TEL：045-478-1883

winbond