DEEPCOVER® EMBEDDED SECURITY

– DeepCover®エンベデッドセキュリティ –

Solution Guide

www.maximintegrated.com/jp/DeepCover

maxim integrated™

目次

Maximのセキュリティの歴史 …… 3

エンベデッドセキュリティ用DeepCover
ソリューション …… 3

DeepCoverセキュア認証用IC …… 3

ECDSA認証用IC …… 4

SHA-256認証用IC …… 4

1-Wireインタフェース…… 5

セキュア認証用ICのツールおよびサービス…… 5

出荷時鍵管理 …… 6

セキュア認証用ICの評価キット…… 6

セキュアマルチデバイスプログラマ …… 6

DeepCoverセキュアマイクロコントローラ…… 7

エンベデッドセキュリティ用DeepCover
セキュアマイクロコントローラ …… 7

金融トランザクション用DeepCover
セキュアマイクロコントローラ …… 8

セキュアARMベースマイクロコントローラ …… 8

磁気ヘッド用セキュアマイクロコントローラ…… 8

セキュアマイクロコントローラのツールセット…… 10

概要

高度なハードウェアベース技術による最適な性能と強度

私たちの世界は、ますますインターネットにつながるようになってきています。しかし、モノのインターネット(IoT)革命は、ユーザーが接続機器および基底のインフラストラクチャを信頼することができる場合にのみ成功します。過去においては、セキュリティは電子支払いシステムなどの専用アプリケーションでのみ問題とされていました。今日では、セキュリティはスマートグリッド、プロセス制御、ビルオートメーションなど、他にも多数のアプリケーションで必須要件になっています。

それと同時に、悪質なハッカーがより高度化し、オンラインコミュニティを介して先進的な攻撃方法を構築し、IoT機器に侵入しています。その結果、電子機器の設計者は新しい課題に直面しています。高度な攻撃に対する非常に堅牢なセキュリティの実装のみではなく、研究開発作業の最適化および低いBOMコストの維持も必要になります。ここでMaximのセキュリティに関する専門技術が手腕を発揮します。

Maximのセキュリティの歴史

図1. DeepCoverセキュリティの技術基盤

Maximは、「IoT」という言葉が生まれるはるかに以前からIoT市場にセキュリティを提供してきました。Maximは最初のセキュアマイクロコントローラを設計し、過去30年間にわたってデジタルセキュリティの設計に対する投資を続けてきました。クラウドへのデータの機密性と完全性を確保するポイントオブセール(POS)端末用ソリューションが、これらの製品の出発点となりました。この経験に基づいて、Maximは将来のセキュリティの課題に対応可能なセキュアマイクロコントローラおよびセキュア認証用ICの広範なポートフォリオを提供しています(図1)。

エンベデッドシステムのセキュリティ確保に関する長い経験から、MaximはICのみでは設計者のすべての課題を解決することができないことを理解しています。IC以外に、Maximはリファレンス回路図、ドライバ、ミドルウェア、通信スタック、およびサポートを提供し、市場投入までの時間の短縮を可能にします。また、Maximのシステムアプローチは、より高いセキュリティレベルを保証します。セキュアな出荷時プログラミングおよび鍵の管理を提供することで、お客様に大きな安心感を与え、その技術は業界内に並ぶものがありません。

エンベデッドセキュリティ用DeepCoverソリューション

エンベデッドシステムは、以下のような多数の脅威に晒されます。

- 偽造
- ハードウェアまたはソフトウェアIPの解析
- マルウェア注入またはファームウェア書き換え
- 傍受
- 個人情報盗難
- 不正なネットワーク接続
- 不正な再使用

セキュア機器認証、セキュアブート、および暗号化は、これらの攻撃に対する答えです。DeepCoverセキュア認証用ICとDeepCoverセキュアマイクロコントローラは、これらの技法を取り入れてお客様のプラットフォームの信頼性を確保します。

トラステッドプラットフォーム、IP保護、セキュアダウンロード、およびセキュア通信は、IoTノードのセキュリティで最も多い要件です。表1に、MaximのDeepCoverソリューションと一般的なIoTのニーズの対応関係を示します。

DeepCoverセキュア認証用IC

セキュア認証用ICは、固定関数暗号操作、セキュアキーストレージ、および多数の補助機能オプション(セキュアダウンロード/ブート処理、最終アプリケーションで使用するための保護された不揮発性メモリ、セキュアGPIO、デクリメント専用カウンタ、セッション鍵生成、真の乱数発生源、および保存データの暗号化R/Wなど)の基本セットを提供します。暗号強度に加えて、全デバイスは悪質なチップレベルのセキュリティ攻撃に対応する高度な物理保護を提供します。革新的な1-Wire®インタフェースの考案者であるMaximは、プリンタカートリッジ、医療用ディスポーザブル、バッテリパックなどの従来とは異なる形状に接続するデバイスの開発を先導しています。

表1. IoTのセキュリティニーズに対応するDeepCoverセキュリティソリューション

要件		DeepCoverセキュリティソリューション
信頼	機器認証	○
	使用制御/機能有効化	○
	セキュアブート/ダウンロード	○
	ルートオブトラスト	○
IP保護	ハードウェアとファームウェアのクローン防止	○
	ファームウェア暗号化	○
セキュア通信	証明書の配付および検証	○
	パケット暗号化	○
	完全なTLSサポート	○
	スモールメッセージ暗号化	○

セキュア認証用ICのアプリケーション

Maximのセキュア認証ソリューションは、以下のような広範なセキュリティ問題を解決します。

一般的なアプリケーション要件

- 製品の品質/安全性
- 偽造防止
- セキュアダウンロード/ブート
- 使用/機能制御
- IoT機器の完全性/真正性

対象製品の機能によって解決されるもの

- 双方向認証
- セキュアシステムデータストレージ
- セキュア使用回数カウント
- システムセッション鍵生成
- セキュアメモリ設定
- セキュアGPIO
- 乱数発生源

ECDSA認証用IC

DS28C36およびコンパニオンのDS2476は、非対称鍵および対称鍵暗号ツールの基本セットを、小型、低コストのソリューションで提供します。非対称パブリック鍵(公開鍵)機能はFIPS 186 P256ベースの楕円曲線(ECC)アルゴリズムでサポートされ、対称秘密鍵はFIPS 180/198 SHA-256 HMACでサポートされます。これらのデバイスは、動作の設定およびパブリック鍵機能と秘密鍵機能の使用が柔軟に行えます。最終アプリケーションの使用例には、双方向認証、システムデータのセキュアストレージ(たとえば、システム暗号鍵)、システムの重要データのセキュア検証、セキュアブート、およびセキュア使用制御などがあります。さらに、2つのGPIO端子が提供され、オプションのセキュア状態制御およびレベル検出を備えています。

DS2476は、DS28C36のコンパニオンコプロセッサで、アプリケーションのホストシステムマイクロコントローラがECCアルゴリズムに十分な計算リソースを備えていない場合、またはECDSAプライベート鍵やSHA-256システムシークレット(使用時)に必要なセキュアストレージがない場合に使用します。

DS28E35およびコンパニオンのDS2475は、DS28C36の完全な機能を必要としないアプリケーション用に縮小された機能セットを備えたECDSA認証用ICです。

表2に、MaximのDeepCover ECDSA認証用ICおよびコンパニオンコプロセッサを示します。

SHA-256認証用IC

DS28E15/DS28E22/DS28E25ファミリのデバイスは1-Wireインタフェースで動作し、ユーザーメモリサイズと動作電圧に関して数種類のオプションを提供します。DS2465は、1-Wireラインドライバを内蔵したコンパニオンコプロセッサで、システムSHA-256鍵のセキュアストレージを提供します。全デバイスは、FIPS 180ベースの双方向認証機能を提供します。DS28C22は、I²Cインタフェースによる SHA-256機能を提供します。

MAX66240/MAX66242は、SHA-256双方向認証を備えたNFC/RFIDトランスポンダです。MAX66242はこの機能を拡張し、RFエナジーハーベスティングのオプション、マスターまたはスレーブとして設定可能なI²Cインタフェース、および1つのGPIO端子を備えています。MAX66300は、ホストシステムNFCトランシーバおよびトランスポンダ用コンパニオンSHA-256 コプロセッサで、SHA-256システム鍵のセキュアストレージを提供します。

表3に、MaximのDeepCover SHA-256認証用IC、コンパニオンコプロセッサ、トランシーバ、およびレスポンダを示します。

表2. DeepCover ECDSA認証用デバイス

型番	タイプ	動作電圧	インタフェース	ユーザーEEPROM	パッケージオプション
DS28C36	認証用IC	3.3V	I²C	4kb	TDFN
DS2476	コプロセッサ			4kb	TDFN
DS28E35	認証用IC	3.3V	1-Wire	1kb	TSOC、TDFN
DS2475	コプロセッサ		I²C/1-Wire	—	SOT

表3. DeepCover SHA-256認証用デバイス

型番	タイプ	インタフェース	動作電圧	ユーザーEEPROM	パッケージオプション
DS28C22	認証用IC	I²C	3.3V	3kb	TDFN
DS2465	コプロセッサ	I²C/1-Wire	3.3V	0.5kb	TSOC
DS28E15	認証用IC	1-Wire	3.3V	0.5kb	SFN、TSOC、TDFN
DS28E22				2kb	TSOC、TDFN
DS28E25				4kb	SFN、TO92、TSOC、TDFN
DS24L65	コプロセッサ	I²C/1-Wire	1.8V	0.5kb	TSOC
DS28EL15	認証用IC	1-Wire		0.5kb	SFN、TDFN
DS28EL22				2kb	TDFN
DS28EL25				4kb	TDFN
MAX66240	認証用IC トランスポンダ	NFC	受動	4kb	SOIC、TDFN、8ピン WLP
MAX66242		NFC/I²C	受動 (3.3Vオプション)		
MAX66300	コプロセッサ トランシーバ	NFC/UART/SPI	3.3V、5V	1kb	TQFN

1-Wireインタフェース

Maximの1-Wireインタフェースソリューションは、これまで不可能だった領域におけるセキュア認証のための、汎用的で堅牢な、非常に信頼性の高い相互接続方法を提供します。これは、認証を必要とするサブアセンブリへの相互接続が1つの接点に限られている場合に特に有用です。IoTノード以外の例として、医療用センサー/器具、プラガブルモジュール、産業用コントローラ、プリンタカートリッジの認証、および一般的なIP保護などがあります。図2は、1-Wireが可能にする最終アプリケーションの例を示しています。

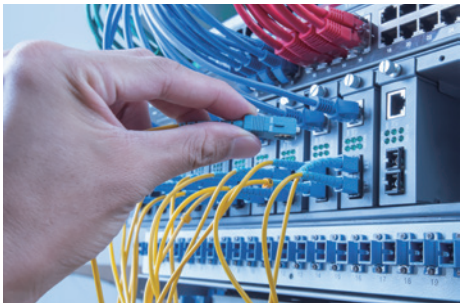
1-Wire製品の特長：

- 1つの接点ですべての制御および動作が可能
- Wireバスから電力を取得(「寄生電源」)
- 固有IDを各デバイスに出荷時設定
- マルチドロップ対応：1つのライン上で複数デバイスをサポート
- 優れたESD性能：8kV HBM (typ)

セキュア認証用ICのツールおよびサービス

リファレンスデザイン：

- MAXREFDES155：IoTにおけるエンベデッドセキュリティ - ECDSAによるパブリック鍵でセキュリティ確保されたデータ経路(図3)
- MAXREFDES143：SHA-256によるIoTセンサーの認証と通知
- MAXREFDES43：DS28C22 SHA-256によるXilinx® Zynq® ZedBoard™認証
- MAXREFDES44：DS28E35 ECDSAによるXilinx Zynq MicroZed™認証
- MAXREFDES34：DS28E15 SHA-256によるXilinx Spartan®-6認証

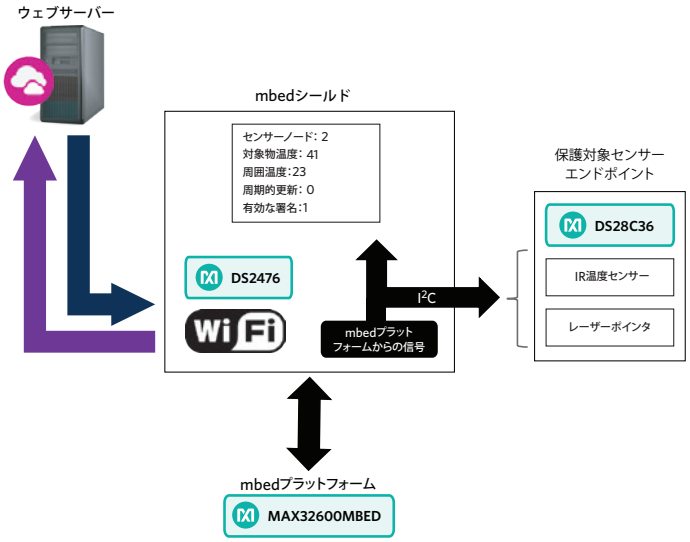


コンピュータ、周辺機器、およびケーブル

モノのインターネット

医療用消耗品

図2. 1-Wireによって実現されるセキュア認証アプリケーション



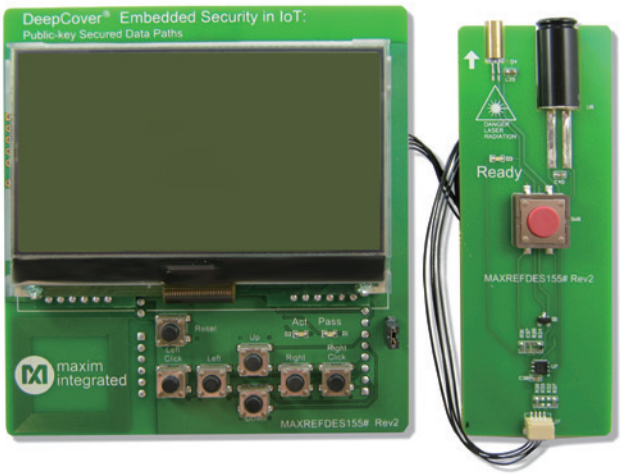


図3. MAXREFDES155リファレンスデザイン

セキュア認証用ICの出荷時鍵管理サービス

1883年にオランダの暗号学者であるAuguste Kerckhoffsが発表した鍵に関する基本的な暗号システムの原則は、今日でも同じように通用します。

「暗号システムは、たとえシステムに関する鍵以外のすべてが公知であってもセキュアであるべきである」

これを念頭に、最終アプリケーションでセキュア認証用ICを使用するOEMは、機器の最終顧客への納品前に鍵が設定されること、およびサプライチェーンのどのポイントでも鍵のセキュリティ侵害がないことを確保する必要があります。OEMに対する付加価値オプションとして、Maximは鍵の管理および設定サービスを提供し、製品出荷前に鍵、証明書、およびアプリケーションデータをセキュアにインストールしています。お客様のデータをMaximの工場に転送するためのセキュアプロセスには、お客様のコンピュータからMaximの製造環境へのデバイス設定の暗号化ファイル転送が含まれます。製造時またはサプライチェーンのどのポイントにおいても、シークレットまたはプライベート鍵のセキュリティ侵害がないことが確保されます。

詳細については、Maximの代理店、または営業担当者までお問い合わせください。

セキュア認証用ICの評価キット

表4に、各セキュア認証用デバイスの評価キットを示します。

セキュアマルチデバイスプログラマ

出荷時、OEM、およびディストリビュータのプログラミングサービスは大量生産を目的としていますが、プロトタイプ作成時や少量生産のアプリケーションにもセキュリティが必要です。マルチデバイスプログラミングシステムのDS9488-GP8は、1-WireおよびI^2Cインタフェースを備えたMaximの各種製品に、鍵、データ、およびデバイス設定情報をセキュアにインストールします。このシステムは、オプションで暗号化プログラミングファイルを1つのプログラマから別のプログラマにセキュアに移動することが可能で、必要に応じて異なる場所での開発とプログラミングをサポートします。ほとんどのデバイスパッケージ用のソケットアダプタが利用可能です。

表4. セキュア認証用ICの評価キット

型番	評価キット
DS28C36	DS28C36EVKIT
DS2476	
DS28E35	DS28E35EVKIT
DS2475	
MAX66242	MAX66300-24XEVKIT
MAX66240	
MAX66300	
DS28C22	DS28C22EVKIT

型番	評価キット
DS28E15	DS28E15EVKIT
DS28E22	DS28E22EVKIT
DS28E25	DS28E25EVKIT
DS2465	注を参照
DS28EL15	DS28EL15EVKIT
DS28EL22	DS28EL22EVKIT
DS28EL25	DS28EL25EVKIT
DS24L65	注を参照

注:DS2465およびDS24L65はDS28E15/DS28C22/DS28E25およびDS28EL15/DS28EL22/DS28EL25の評価キットに含まれています。

DeepCoverセキュアマイクロコントローラ

1990年代、Maximは最初のセキュアマイクロコントローラであるDS5200を設計しました。それ以来、Maximは将来の課題に対応するために、業界をリードするセキュリティ機能を開発するための投資を続けてきました。

エンベデッドセキュリティ用DeepCoverセキュアマイクロコントローラ

Maximは、アクティブタンパー応答技術の先駆者です。この技術は、タンパーの試みに対して即座にデバイスの鍵とシークレットを消去し、FIPS 140-2レベル3または4のセキュリティレベルを実現します。

アクティブタンパー応答技術は、動作にバッテリが必要です。バッテリを搭載することができない最終製品およびアプリケーション向けに、MaximはDeepCoverセキュア暗号コントローラのMAXQ1061を開発しました。このデバイスは耐タンパーEEPROMをベースとしており、バッテリが不要です(図4)。表5に、エンベデッドセキュリティアプリケーション専用に設計されたDeepCoverセキュアマイクロコントローラを示します。

MAXQ1061:DeepCoverセキュア暗号コントローラ

MAXQ1061は、ソフトウェアIP、通信、および収益モデルの機密性、真正性、および完全性を保護します。このデバイスは、IoTノード、コネクテッドエンベデッド機器、産業用ネットワーク、PLC、およびネットワーク機器に最適です。

エンベデッド、包括的暗号ツールボックスは、完全なSSL/TLS/DTLSサポートまでの鍵の生成とストレージを提供します。

このデバイスは、暗号化、ECDSAデジタル署名の計算、および検証を処理します。また、外部の汎用マイクロコントローラ用のセキュアブートローダとしても機能することができます。

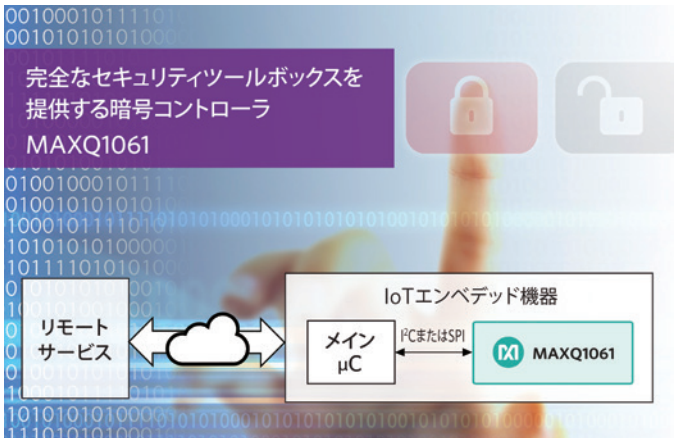


図4. MAXQ1061

主な特長:

- 非常にセキュアなキーストレージをシームレスにサポートする高度な暗号ツールボックス
- 証明書の配付を容易化
- 高レベルな機能によってSSL/TLS/DTLSの実装を簡素化
- 複数の通信インタフェースオプションによってホストプロセッサとの接続を簡素化
- 広範なホストソフトウェアライブラリを提供
- 広範なホスト/システムサービスによって柔軟性を高めシステムコストを削減
- 高速AESエンジンによるバルク暗号化
- ファームウェアの開発が不要

表5. エンベデッドセキュリティアプリケーション用DeepCoverセキュアマイクロコントローラ

型番	コア	周波数	キーストレージ	USB	I²C	SPI	対称暗号	非対称暗号	ハッシュアルゴリズム
MAXQ1061	内蔵ファームウェア		耐タンパーEEPROM		○	○	AES 128、256	ECDSA P-256、P-384、P-521 ECDH	SHA-256、SHA-384、SHA-512
MAX32555	Cortex® M3	60MHz	アクティブタンパー応答	○	○	○	AES 128、192、256 3DES	RSA 1024、2048 ECDSA P-256、P-384、P-521 ECDH	SHA-224、SHA-256、SHA-384、SHA-512
MAXQ1050	MAXQ30	20MHz	アクティブタンパー応答	○		○	AES 128、192、256	RSA 1024、2048 ECDSA P-192、P-256	SHA-224、SHA-256

金融トランザクション用DeepCoverセキュアマイクロコントローラ

消費者の決済の習慣は変化しています。ICカードが磁気ストライプカードに取って代わり、非接触決済はスマートカードまたはスマートフォンのいずれかによってサポートされるようになり、モバイルPOS端末によって小規模商店や家庭向けサービスでのカードの受け付けが可能になり、カウンタートップPOSシステムではタブレット形状の採用が進んでいます。それと同時に、各種の規格や決済方式はさらに高いセキュリティを要求するようになっています。消費者が期待する柔軟性をサポートするのと同時に、トランザクションのセキュリティを保証することが、金融トランザクションシステムの設計者にとっての決済の課題です。この分野におけるMaximの専門知識によって、これらの動向に対応する広範なセキュアマイクロコントローラの開発が実現しました。

たとえば、MAX32560セキュアマイクロコントローラ(図5)は、EMV準拠の非接触リーダーインタフェースを内蔵しているため、このデバイスはPCI-PTSセキュリティおよび非接触決済に対応した初めてのセキュアマイクロコントローラです。

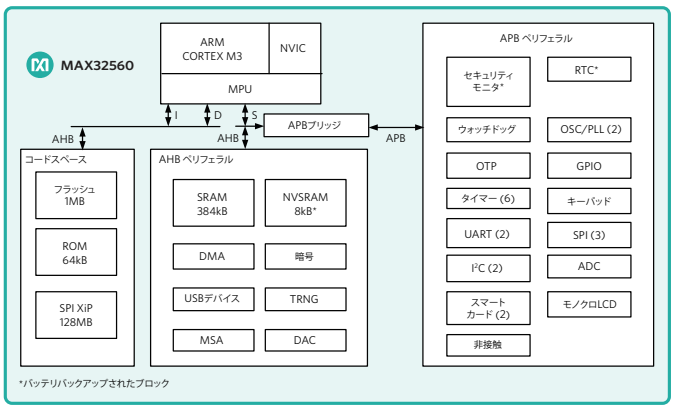


図5. MAX32560のブロック図

Maximのセキュアマイクロコントローラは、以下を特長とします。

- アクティブタンパー応答
- ハードウェア暗号アクセラレータ
- 金融トランザクション専用の内蔵アナログインタフェース
  - EMV準拠スマートカードPHY
  - 磁気ストライプカードリーダー
  - EMV非接触
- セキュリティモニタ内蔵
- 高度なセンサーによる外部タンパー検出

また、Maximの専門知識はICのみに留まりません。最新のセキュリティ機能を備えたセキュアマイクロコントローラの提供以外に、以下のものも提供しています。

- EMVソフトウェアスタック
- PCI-PTS評価レポート
- 暗号ライブラリ
- 完全Linux BSPおよびPCI-PTS準拠のMAX32590用Linuxコード
- PCI-PTSおよびEMV証明書のサポート

セキュアARMベースマイクロコントローラ

MaximのARM®ベースのセキュアマイクロコントローラ(図6)は、POSまたはモバイルPOSシステム、ピンパッド、または暗号化ピンパッド用のメインプロセッサまたはコプロセッサとして使用するために設計されました。

これらの製品は、多様なツール、ライブラリ、およびオペレーティングシステムを提供するとともに、最新の規格に準拠した高度なセキュリティ機能も提供します。この独自の組み合わせによって市場投入までの時間が短縮され、初回での認定取得の成功につながります。表6に、金融トランザクションアプリケーションに対応するDeepCoverセキュアマイクロコントローラを示します。

図6. MAX32560の評価キット

磁気ヘッド用セキュアマイクロコントローラ

PINトランザクションセキュリティ (PCI-PTS)規格が要求するカード所有者のデータ保護のレベルが高まっており、金融端末内で磁気カードのデータを高度に保護することが必要です。そのため、Maximは3トラックの磁気ストライプデータの読み取りとデコードを行い、アプリケーションプロセッサへの送信前にそれらを暗号化することができるマイクロコントローラ(図7)を設計し、高コストな物理保護の実装を不要にしました。表7および図8は、磁気ヘッドアプリケーション用に設計されたセキュアマイクロコントローラを示します。

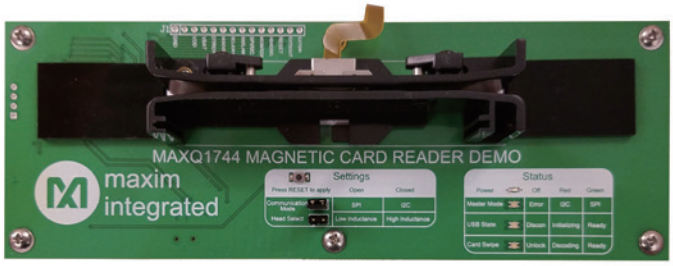


図7. MAXQ1744の評価ボード

表6. 金融トランザクションアプリケーション用DeepCoverセキュアマイクロコントローラ

	MAX32590	MAX32550	MAX32552	MAX32560	MAX32555
コア	ARM 926EJ-S	Cortex-M3	Cortex-M3	Cortex-M3	Cortex-M3
フラッシュ/SRAM	—/384KB	1MB/256KB	1MB/384KB	1MB/384KB	512KB/96KB
非接触インタフェース	—	—	—	内蔵	—
TFTコントローラ/モノクロLCD	内蔵/内蔵	内蔵/内蔵	なし/内蔵	なし/内蔵	なし/内蔵
クロック速度	384MHz	108MHz	108MHz	108MHz	60MHz
AES暗号化NVSRAM	24KB	8KB	8KB	8KB	1KB
ダイナミックセンサーペア	6	6	6	6	4
OTP	2KB	4KB	4KB	4KB	4KB
MSRデコーダ/スマートカードUART/スマートカードPHY	—/2/—	1/1/1	1/2/1	1/2/2	1/1/2
ADC	3チャネル10ビット	2チャネル10ビット	2チャネル10ビット	2チャネル10ビット	6チャネル10ビット
DAC	—	1チャネル8ビット	1チャネル8ビット	1チャネル8ビット	1チャネル8ビット
USBデバイス/SPI/UART/I²C	1/5/3/1	1/3/2/1	1/3/2/1	1/3/2/1	1/3/3/1
イーサネットMAC	内蔵	—	—	—	—
USBホスト	1	—	—	—	—
外部メモリ	NAND/NOR フラッシュ 暗号化 LPDDR	—	Quad SPI (XiP対応)	Quad SPI (XiP対応)	—
タイマー	3	6	6	6	8
GPIO	160	70	69	69	70
パッケージ	BGA324	BGA121	BGA121	BGA144	BGA121

表7. 磁気ヘッドアプリケーション用DeepCoverセキュアマイクロコントローラ

	コア/周波数	メモリ	インタフェース	暗号	その他
MAXQ1741	MAXQ20 (12MHz)	16kBフラッシュ 1kB SRAM	1 UART 2 SPI 1 I²C	AES	—
MAXQ1743	ターンキーエンベデッドファームウェアをMaximから提供		1 I²C 1 SPI	AES、3DES	—
MAXQ1744					超低電力: 450µA (カード読取り時)

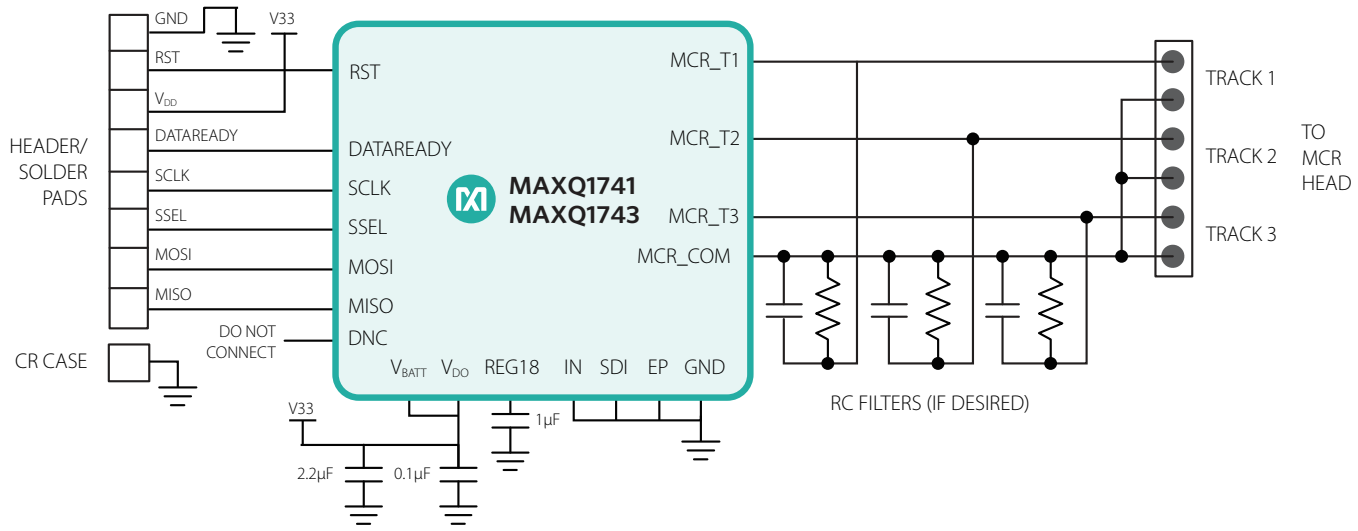


図8. MAXQ1741/MAXQ1743

セキュアマイクロコントローラのツールセット

Maximのセキュアマイクロコントローラ開発ボードは、広範なインタフェース一式を内蔵しています。これらのボードは、スマートカードコネクタ、磁気ストライプヘッド、キーボード、およびディスプレイなどの最も一般的な決済専用インタフェースを備えています。

MaximのARMベースのセキュアマイクロコントローラ開発ツールは、人気の高いオープンソースのIDE、コンパイラ、およびデバッガをベースとしています。ARMコアを活用することによって、これらのツールは開発時間を削減し、市場投入までの時間を短縮します。

さらに詳しく

詳細については、こちらをご覧ください：
www.maximintegrated.com/jp/DeepCover

マキシム・ジャパン株式会社
〒141-0032 東京都品川区大崎1-6-4 大崎ニューシティ 4号館20F

©2017 Maxim Integrated Products, Inc. All rights reserved. Maxim IntegratedおよびMaxim Integratedのロゴは、米国およびその他の国の管轄域におけるMaxim Integrated Products, Inc.の登録商標です。その他、記載されている会社名、製品名は各社の登録商標、または商標です。

Rev.3; June 2017