NXP®
MIFARE® SAM AV3

デバイスの暗号化性能の強化によって コネクテッド・システムを保護

柔軟な性能が得られるように設計された、この第3世代MIFAREセキュア・アクセス・モジュール （SAM） は、アクセス鍵のセキュリティを高めて資産を保護します。これにはMIFARE ICのサポートと、NXPのNTAG、ICODE、UCODEファミリの各「DNA」製品のサポートが組み込まれています。民生用機器、リーダおよびPOS端末、料金所、ドア・ロックなどの組込み型システム向けのセキュリティ・アドオンです。

主な特長

- MIFARE® SAM AV2との互換性
- MIFARE® DESFire® EV3、MIFARE® DESFire® Light、MIFARE Plus® EV2、MIFARE Ultralight® EV1の最新のセキュリティ機能をサポート
- UCODE® DNA、ICODE® DNA、NTAG® DNAをサポート
- Crypto1、TDEA（56、112、168）、AES（128、192、256）、SHA-1、SHA-225、SHA-256、RSA、ECCをサポート
- 柔軟な鍵の分散化
- 鍵のセキュアなダウンロードと保管
- 対称暗号化用の鍵エントリ x 128
  RSA用の鍵エントリ x 3、ECC非対称暗号化用の鍵エントリ x 8、EMV CA用の鍵エントリ x 48
- プログラマブルな機能によるコマンドとロジックのカスタマイズ
- ボー・レートが最大1.5 Mbit/sまで向上した ISO/IEC 7816インターフェース
- I²Cスレーブ・ホスト・インターフェース（HVQFNパッケージのみ）
- XモードによるNXPリーダICとの直接パス・スルー接続
- コモン・クライテリアEAL6+ (HW)、MIFAREセキュリティ認定 (SW)、FIPS 140-2 CAVP
- ウェハ、PCM 1.5スマート・カード・モジュール、またはHVQFN32パッケージで提供

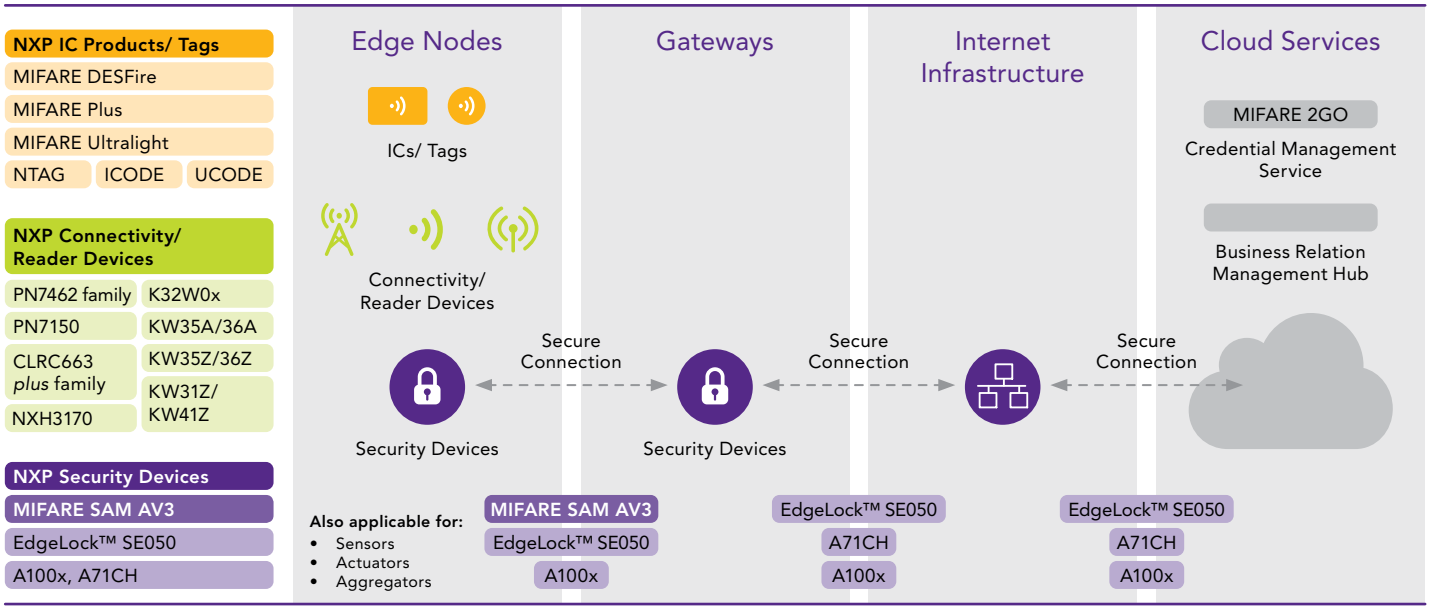
ターゲット・アプリケーション

- 公共交通
- アクセス管理
- ロイヤルティ・プログラムと少額決済
- 消耗品および部品の識別
- 道路通行料徴収
- 電気自動車の識別
- 民生用機器のオリジナリティとセキュリティの保護

主なメリット

- 機密性の高い鍵（マスタ鍵など）の強固な保護
- エッジ・コンピューティング・ノードの迅速かつ効率的な設計
- 直接パス・スルーのXモードでアプリケーションの性能を改善
- カスタマイズ可能なフロー、1コマンドで実行可能

コネクテッド・システムのアーキテクチャとNXPのソリューション



現在第3世代のMIFARE SAMアーキテクチャは、MIFARE ICに加え、NXPのNTAG、ICODE、UCODEファミリのDNA製品をサポートするように機能が拡張されています。これらのファミリ内のトランザクション・メッセージ認証コード(TMAC) を提供する製品タイプと併用できるように最適化されたMIFARE SAM AV3は、多種多様なアプリケーションで鍵のセキュリティを高め、資産を保護するのに役立ちます。

MIFARE SAM AV3は、プログラマブル・ロジックもサポートすることで柔軟性のレベルを引き上げているため、鍵の分散化のために独自のアルゴリズムを組み込むことや、ビジネス・フロー全体が1つの呼び出しだけで実行されるよう実装することができます。プログラマブル・ロジックのサポートにより、MIFARE SAM AV3の固有の暗号化関数を再利用しながら、独自のコードを開発することもできます。

資格、ツールへの投資、特別なスキルを求められるプロセスである、カスタマイズされたロジックの開発を簡素化するため、NXPは、MIFARE SAM AV3に特化したコード開発サービスやその他のサービスを提供する設計企業と提携しています。

MIFARE SAM AV3では、ますます重要性が高まる現在のアプリケーションすべてに簡単な方法でセキュリティを追加し、より迅速かつ効率的な設計を促進することができます。

効率的なXモード設定により、一部のNXP RFフロントエンドICと直接通信し、アプリケーションの性能を高めることができます。

全体的に見て、MIFARE SAM AV3の柔軟性とシンプルさは、組込み型の識別システムの保護に最適な特長と言えます。

特長

Product features	MIFARE SAM AV3
Memory	
Number of symmetric key entries	128
Number of asymmetric key entries	3 RSA 8 ECC 48 EMV CA
Interfaces	
ISO/IEC 7816	T=1 protocol for contact communication, 9.6 up to 1500 kbit/s data throughput
I²C host interface (in HVQFN package only)	Supports standard mode up to 350 kbit/s
Security	
Symmetric crypto	Crypto 1, TDEA- 56-112-168, AES-128-192-256
Asymmetric crypto	RSA (2048 bits), ECC (256 bits)

注文情報

Delivery Type	Part Type
Wafer	MF4SAM3U15
PCM 1.5 module	MF4SAM3X84
HVQFN32	MF4SAM3HN

www.nxp.jp

リリース日：2020年6月26日
ドキュメント番号：MIFARESAMAV3 Rev 2.2

www.MIFARE.net