NXPのクラウド接続向け IoTセキュリティIC 「A71CH」

プラグ&トラスト：IoT接続のセキュリティを迅速かつ容易に実現

ICレベルでRoot of Trust: 信頼の基点を提供するこのソリューションは導入が容易で、「チップからクラウドまで」の確かなセキュリティを手間なく実現できます。AWS、IBM Watson IoT Platform、Google Cloud IoT CoreなどIoTクラウドやIoTサービスに接続する際にセキュリティ・コードを記述する必要がなく、鍵を外部にさらしてしまうリスクもありません。

主な特長

- セキュアなゼロタッチ接続
- チップからエッジ、クラウドまでのエンド・ツー・エンド・セキュリティ
- ICレベルの信頼の基点のためのセキュアなクレデンシャル情報の注入
- 総合的な製品サポート・パッケージによる迅速なデザイン
- さまざまなMCU/MPUプラットフォームとの容易な統合

主なセキュリティ機能

- 認証情報への保護されたアクセス
- ホスト・プロセッサとのインターフェースを暗号化
- 証明書ベースのTLS設定（ECC NIST P-256）
- 事前共有鍵を使用するTLS設定（TLS-PSK）
- コネクションレス・メッセージ認証（HMAC）
- ECC鍵生成と署名検証
- 対称鍵導出
- 製品のマスター・シークレットを格納するセキュアな金庫（鍵ラップ、導出、ロック）
- 暗号化鍵注入
- NXPおよび認定パートナーによる信頼のプロビジョニング（オプション）

主なハードウェア機能

- I²C 400 kbpsのスレーブ・インターフェースを介してあらゆるMCU/MPUに容易にアクセス
- 標準温度範囲（-25～+85 °C、A7101CH）と拡張温度範囲（-40～+90 °C、A7102CH）
- HVSON8（4x4 mm）およびWLCSP（2x2 mm）のパッケージ

Amazon Web Services（AWS）、IBM Watson IoT Platform、Google Cloud IoT Coreなどのクラウドを利用するサブスクリプション型クラウド接続が登場したことで、Internet of Things（IoT）は身の回りの製品にも浸透し、IoTサービスの幅は広がり続けています。

クラウド・サービスの導入時には、ハッキング、データ漏えい、ボットネット攻撃など、IoTに関わる潜在的なリスクからすべてのデバイスを保護する必要があるため、セキュリティは常に気がかりです。クラウド接続の認証用の鍵と証明書は安全に秘匿し、IoTデバイスから送信されるデータは転送中にセキュリティで保護する必要があります。さらに、セキュリティ・メカニズムには、複数のメーカーが混在する大規模な環境にも効率的に導入できる拡張性の高さが求められます。

NXPのA71CHはこうしたニーズを満たすセキュリティICであり、あらゆる規模のIoT実装で高度なセキュリティを確保できます。パブリック・クラウドにもプライベート・クラウドにも対応する、導入の容易なプラグ&トラスト・セキュリティ・ソリューションとして、ハードウェア・ベースの実績あるセキュリティ・メカニズムを使用しゼロタッチの安全な接続を実現します。

NXPの開発済みのソフトウェアが書き込まれているので、お客様はセキュリティ・コードを記述する必要がなく、導入の容易なホスト・ソフトウェアは各種のMCU/MPUプラットフォームと簡単に統合できます。

A71CHは設計段階からセキュリティ対策が組み込まれ、セキュアな接続を確保できるよう最適化されています。また、ICレベルの鍵注入にも対応し、細かな設定なしでも信頼性の高いセキュリティをすぐに展開できます。

実証済みの性能

A71CHを開発したNXPは、決済、アクセス・コントロール、および電子パスポートなどのID認証といった、世界で最も要求水準の高いセキュリティ・アプリケーションの分野を牽引してきた実績があります。

IoTのセキュリティに特化したA71CHはオブジェクトの認証、データの保護、クラウドへのアクセスといったデバイスの最も重要な機能を保護し、ソフトウェアの完全性やロールバック保護をサポート。さらに、サービスの完全性とエコシステムの安全性を確保し、新しいビジネス・モデルのプラットフォームという役割も果たします。

A71CHはオプションで温度拡張品(-40～+90 °C、A7102CH)も用意されており、産業用規格を満たしています。また、長寿命設計により、汎用ストレージで25年以上のデータ保持期間、50万回以上の書込/消去耐性を実現しています。

ライフサイクル全体の保護

NXPでは、製造からフィールドまでの製品ライフサイクル全体で信頼を確保できるよう努めています。ダイ毎の鍵と証明書はシリコンベースで信頼の基点を提供できるように、安全性の認証を受けた製造施設でNXPが注入するか、認定パートナーが注入します。

これにより、A71CHを使用するIoTデバイスには後からセキュリティ機能を追加するのではなく、最初から組み込むことができます。

総合的な製品サポート・パッケージ

導入の容易なソリューションであるA71CHには、総合的な製品サポート・パッケージが付属しており、デザインインを簡略化するとともに、製品化までの時間を短縮することもできます。設計の負担を軽減する方法として、たとえばホスト・ソフトウェア・パッケージのOpenSSLエンジンの使用やmbedTLSの統合により、接続スタックとの連携が容易になります。また、主要な使用事例のサンプル・コード、詳細なアプリケーション・ノート、i.MXアプリケーション・プロセッサやLPC/Kinetisマイクロコントローラと互換性のある開発キットなど時間短縮につながる設計ツールも利用可能で、最終的なシステム統合が迅速化されます。

A71CHの使用事例

- クラウド・サービス、エッジ・コンピューティング・プラットフォーム、インフラストラクチャーへのセキュアな接続
- デバイス間の認証
- 原物証明/偽造防止
- セキュアな鍵ストレージ
- セキュアなクレデンシャル情報管理
- セキュアなデータ保護
- セキュアなコミッショニング・サポート
- エコシステムの保護

A71CHのターゲット・アプリケーション

- コネクテッド産業デバイス
- セキュリティ・システムとセンサ・ネットワーク
- ゲートウェイ
- スマート・シティ
- スマート・ホーム

Configuration	Orderable Part Number	Description	Package	12NC
Customer programmable	A7101CHTK2/T0BC2VJ	Security IC with standard temp range (-25 to +85 °C)	HVSON8, Reel	9353 680 97118
Customer programmable	A7102CHTK2/T0BC2AJ	Security IC with extended temp range (-40 to +90 °C)	HVSON8, Reel	9353 635 15118
Customer programmable	A7101CHUK/T0BC2HAZ	Security IC with standard temp range (-25 to +85 °C)	WLCSP, Reel	9353 694 82023
Customer programmable	A7102CHUK/T0BC2VAZ	Security IC with extended temp range (-40 to +90 °C)	WLCSP, Reel	9353 695 02023
Provisioned & Programmable	A7101CHTK2/T0BC2BJ	Security IC with standard temp range (-25 to +85 °C) Ready for IBM Watson IoT	HVSON8, Reel	9353 737 63118
Provisioned & Programmable	A7102CHTK2/T0BC2CJ	Security IC with extended temp range (-40 to +90 °C) Ready for IBM Watson IoT	HVSON8, Reel	9353 741 46118

Item	Description	12NC
OM3710/A71CHARD	A71CH Arduino-compatible development kit	9353 689 97598

Find all information on **www.nxp.com/A71CH**

Date of release: February 2019
Document Number: A71CH-LEAFLETJ REV 0 （原文:A71CH Leaflet 2018）