CRYPTO QUANTIQUE

RAエコシステムパートナーソリューション
CRYPTO QUANTIQUE® QuarkLink

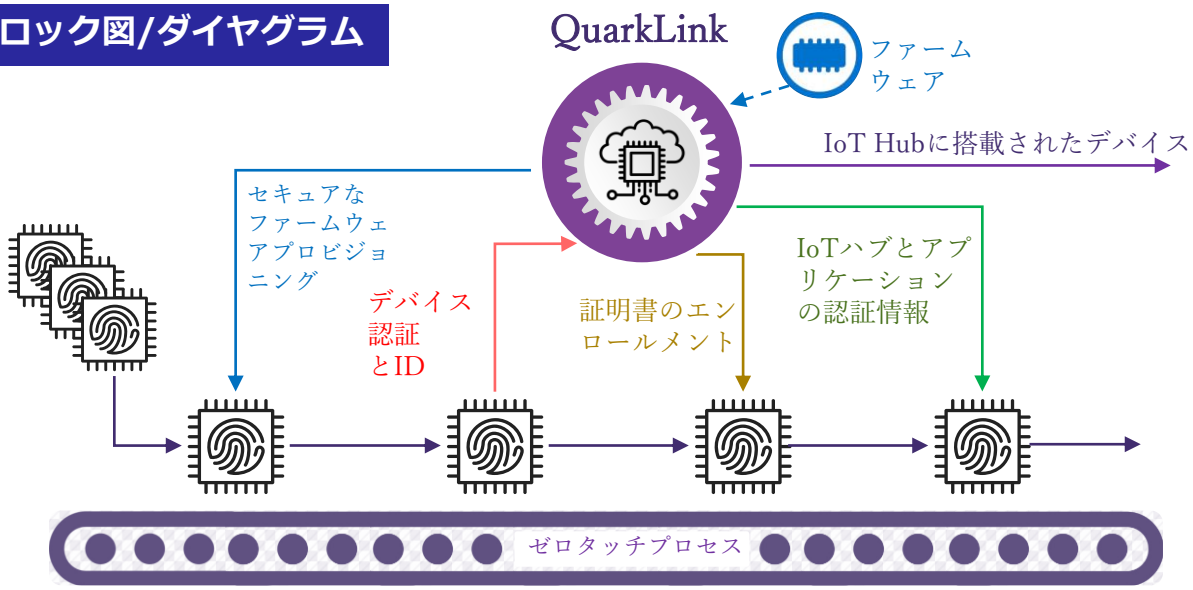
概要

Crypto Quantique® QuarkLinkは、IoT向けの簡単でスケーラブルなエンドツーエンドのセキュリティを実現するIoTセキュリティおよびデバイス管理プラットフォームです。セキュアなファームウェアのプロビジョニング、デバイスのオンボーディングとエンロールメント、証明書の管理を自動化し、ハードウェアからアプリケーションまでのゼロタッチセキュリティを証明するとともに、お客様にセキュリティ資産の完全なコントロールを提供します。RAファミリと一緒にすぐに使えます。

主な機能

- ハードウェアの「信頼の基点（Root of Trust）」に基づく、ゼロタッチのデバイス認証、オンボーディング、エンロールメント
- ファームウェアの暗号化により、非セキュアな環境での本番環境でのプログラミングを可能にし、**製造時にHSMやキーインジェクションは不要**
- 自動更新による証明書の管理と失効、 **外部CAは不要**
- プラットフォームに依存しない柔軟な導入が可能で、オンプレミスまたはクラウドでホストすることができ、鍵とファームウェアの完全な制御と完全に機能するプライベートPKIを提供します
- データはデバイスからアプリケーションまで暗号化され、どのような中間のクラウドでも見ることはできません

ブロック図/ダイヤグラム



ターゲット市場及び用途

- 家電製品
- 産業用IoT
- スマートシティ
- スマートホーム
- スマートセンサー

www.cryptoquantique.com

2021.10

CRYPTO QUANTIQUE

量子駆動型サイバーセキュリティ

偽造不可能な「量子的に安全な」ハードウェアの「信頼の基点」に基づく基礎的なエンド・ツー・エンドのサイバーセキュリティ

CRYPTO QUANTIQUE

Q:Architecture：シームレスなエンド・ツー・エンドのIoTセキュリティ

QDID：世界初の偽造不可能な「信頼の基点」

サイドチャネル攻撃に対する本質的な安全性

偽造できないデバイスアイデンティティ

は偽造を防ぐ

キーインジェクションのない、相関性のない複数のキー

QuarkLink: ユニバーサルセキュリティプラットフォーム

エンド・ツー・エンドのセキュリティアーキテクチャ

PKI管理、証明書の更新と失効

QDIDと、既存のサードパーティ製の信頼の基点にも対応

Crypto Quantique®のQ:Architectureは、ハードウェアとソフトウェアを使用して、量子物理学と暗号学の最先端技術を組み合わせ、強力で使いやすいIoTセキュリティを実現します。Q:Architectureは、シリコン、デバイス、クラウドプラットフォームの世界をシームレスにつなぐことで、IoTのセキュリティの概念を再定義します。

Crypto Quantique®の画期的な技術は、IoTエッジノードに不変のハードウェア信頼の基点を生成するプロセスを根本的に簡素化し、信頼されていない環境でのIoTエッジノードの安全なプロビジョニングとオンボーディングの問題を解決し、IoTエコシステムに現在存在するデバイスセキュリティの穴を塞ぐことができます。

主力製品は、半導体デバイス内部で無相関の複数の秘密鍵を生成するQDID（Quantum Driven Identity）の特徴を活かした、IoTのセキュリティを管理するHwSaaS（Hardware Security as a Service）です。このユニークな機能により、最終製品の製造/プロビジョニング時に **HSMの隠れたキーインジェクションが不要**です。

同時に、当社は、既存のMCU/CPUや信頼の基点で利用できるセキュリティを大幅に改善する必要性も認識しています。したがって、 **QuarkLinkは**、真のエンドツーエンドセキュリティのために、QDIDに加えて、 **既存のPUFやその他の信頼の基点をサポートし**、安全なファームウェアのプロビジョニング、認証されたオンボーディング、および簡単な鍵と証明書のライフサイクル管理を提供します。

当社の存在価値

当社は、ユーザーが自分のデバイスのセキュリティとプライバシーをコントロールし、デバイスごとに自分のセキュリティ認証情報を自動的に作成／維持できるような、ゼロトラストによるコネクテッド・ワールドのセキュリティを想定しています。
当社の使命は、IoTのオンボード化と管理のために、シームレスでエンドツーエンドのゼロトラスト・セキュリティを提供することです。
当社のシステムは、デバイスが生まれてから死ぬまでの間、安全を確保するように設計されています。
設計から製造、導入、運用までお客様をサポートします。

サービスとしてのハードウェアセキュリティ

当社の量子トンネリング効果をベースしたのシリコンIPは、接続されたデバイスが必要に応じて複数の改ざん不可能な暗号鍵を生成することを可能にし、デバイスの寿命が尽きるまで決して妥協しません。
当社の高度な暗号鍵のプロビジョニングとライフサイクル管理プラットフォームとの組み合わせにより、クラウドからチップまでの経済的なサイバーセキュリティを提供します。
当社のソリューションは、ハードウェアの信頼の基点を実装するためのコストを削減します。
当社のコアテクノロジーは、設計上、量子的に安全です。
当社は、暗号技術、電気工学、量子物理学のパイオニアです。