cpl.thalesgroup.com

THALES
Building a future we can all trust

タレスとISARA Corporation 耐量子セキュリティを備えたThales Luna HSMによるIoTの保護

問題

量子コンピューティングによって最新の暗号が解読され、安全かつ認証されたソフトウェア/ファームウェア更新であっても攻撃者が偽造できる可能性がある

大規模な量子コンピューティングが実現すると、現在の公開鍵暗号は解読されます。その結果、接続して処理するあらゆるものに広範な脆弱性がもたらされます。そのため、現在導入されている長寿命のコネクテッドデバイスには、量子時代が到来してもセキュリティを保たねばならないという特有の問題が生じます。なぜなら、物理的に埋め込まれた信頼の基点がソフトウェアとファームウェア更新の認証に使用されているからです。これらに耐量子性のあるトラストアンカー（信頼の要）が組み込まれていなければ、将来的に回収と更新が必要になり、多大な財務および物流の負担が生じます。ソフトウェア更新の保護は、克服すべき問題の1つにすぎません。

主なメリット

- 高価値のコネクテッドデバイス（IoT）を現在導入することで、コストのかかる回収や物理的な更新を将来必要とせず、量子の脅威から保護されることを確信できます。
- FIPS140-2認定の耐タンパ性のハードウェアセキュリティモジュール（HSM）により、耐量子鍵を安全に生成および管理できます。
- 標準化された耐量子公開鍵暗号を使用してシームレスにデジタル署名、具体的にはステートフルハッシュベース署名を生成できます。

鍵の状態管理に対する独自のアプローチを使用してステートフルハッシュベース署名の使用を簡素化します。この業界全体の課題を、Thales Luna HSMが解決します。

SARA

課題

標準化された耐量子セキュリティを使用して、現在および将来にわたりコネクテッドデバイスを保護する

コネクテッドデバイスを保護するには多面的なアプローチが必要です。強固なセキュリティを実現する重要な手段の1つは、信頼の基点を組み込むことです。これには通常、耐タンパ性のハードウェアセキュリティモジュール(HSM)内に鍵を保存する必要があります。現在、RSAやECCなどの非対称アルゴリズムが、量子の脅威に対して脆弱なデジタル署名に使用されています。幸いなことに、耐量子性を持つ代替技術はすでに存在していますが、まだ新しく、さらに管理しやすい実装という課題を考慮する必要があります。ステートフルハッシュベース署名は、耐量子性があり、成熟していて信頼性もありますが、秘密鍵を安全に利用または導入するには独自の状態管理手法が必要です。

ソリューション

標準化されたステートフルハッシュベース署名をコード署名に利用する耐タンパ性のHSM

Luna HSM Post Quantum Crypto Functionality Module(FM)は、ISARA Radiate™ Quantum-safe Toolkitを利用しており、ステートフルハッシュベース署名を現在のコード署名に使用できます。この実装には、秘密鍵を最適に保存してさまざまな要件を持つ運用環境で使用できるよう、速度またはサイズのいずれかを最適化した鍵圧縮のメカニズムが含まれています。HSMの重要な機能は、高可用性(HA)とディザスタリカバリ(DR)に対処する機能です。秘密鍵の状態管理を綿密に行い、ステートフルハッシュベース署名のHAおよびDR機能を実現する、さまざまな秘密鍵分割戦略を提供するメカニズムが実装されています。

ISARA Radiateを利用したLuna HSM Post-Quantum FMを使用するメリット

主な利点と機能は次のとおりです。

- 現在のすべての長寿命デバイスに将来性のある標準化された耐量子デジタル署名アルゴリズムを使用して、安全で認証されたソフトウェア/ファームウェア更新を将来にわたって長く提供できるようにします。
- FMは、IETFによって標準化されたステートフルハッシュベース署名、具体的にはHSS (Hierarchical Signature System) IETF RFC 8554、およびXMSS (eXtended Merkle Signature System) IETF RFC 8391のみを使用しています。
- IETFによって標準化され、まもなくNISTによってFIPSの承認を受ける、耐量子のステートフルハッシュベース署名を有効にします。
- ステートフルハッシュベース署名は、ドキュメント署名やコード署名などアイデンティティのユースケースに対する量子の脅威に直面した場合のクリプトアジリティ(暗号解読に敏速に対抗する能力)を可能にします。

ポスト量子リスク評価を受ける

ポスト量子リスク評価を受けるか、それを開始する重要性について弊社にお問い合わせください。そして、現在利用可能なソリューションを使用して量子時代に向けた準備をどのように開始できるかを検討してください。

ISARA Corporationについて

ISARA Corporationは、長年にわたって蓄積した実世界のサイバーセキュリティに関する専門知識を活かし、現在のコンピューティングエコシステムを量子時代まで守り続ける、アジャイルな耐量子セキュリティソリューション事業の世界的リーダーです。パートナーと連携して、シームレスな移行のための実用的で標準化されたソリューションを提供することで、企業や政府のために耐量子セキュリティへの道を切り開いています。

詳細な技術仕様については、cpl.thalesgroup.comまたはwww.isara.comをご覧ください。

タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。

決断の瞬間のための、確実なテクノロジー。

> cpl.thalesgroup.com <

お問い合わせ先 – cpl.jpsales@thalesgroup.com
すべてのオフィスの所在地と連絡先情報につきましては 、cpl.thalesgroup.com/ja/contact-usをご覧ください。