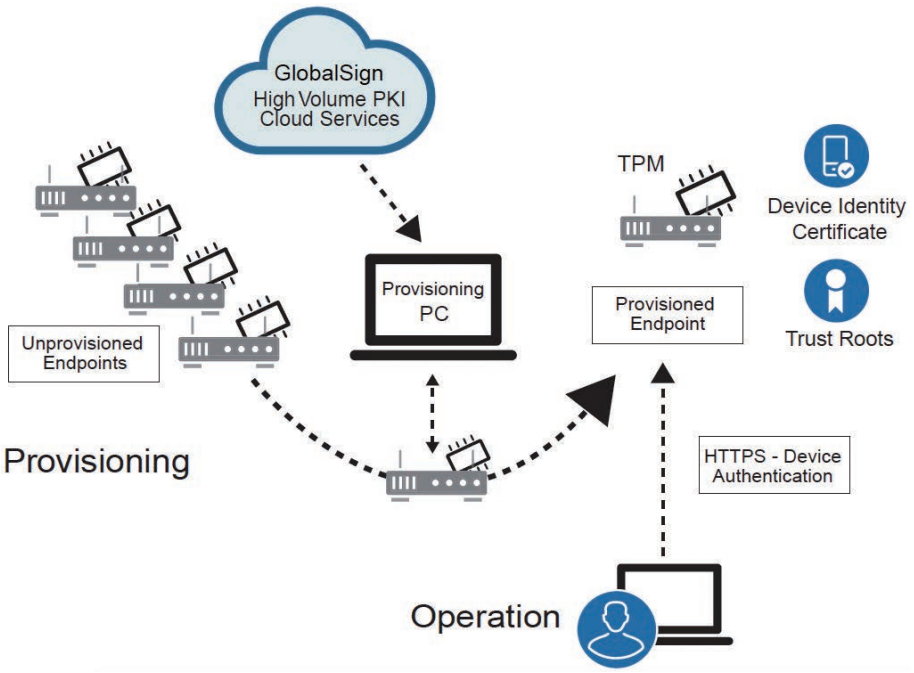
DATASHEET

マネージドPKI for IoT パートナーシップ導入事例

グローバルサインのマネージドPKI for IoT × インフィニオン社 OPTIGA™ TPM ～ハードウェアの安全な認証とコントロールを実現～

IoTプロバイダーは、機器の認証、データのプライバシーや完全性など、極めて重要なセキュリティ上の課題に対処する必要があります。IoT市場における大量発行に対応したグローバルサインのマネージドPKI for IoTと、インフィニオン社のOPTIGA™TPMを組み合わせた強固なデバイスIDのためのコンセプト検証（Proof of concept）にて、認証情報の保護におけるリスクを軽減し、実績あるソリューションをIoTスケールで構築するのに利用することができます。

グローバルサインとインフィニオン社のコンセプト検証は、IoTエンドポイントのプロビジョニングと運用において、どのようにすればPKI（公開鍵暗号基盤）とセキュアハードウェアをスケーラブルな形で活用できるかを明らかにしています。この2つの技術の統合は、信頼性をデバイスに付与していくモデルをIoTレベルのスケールで拡張させつつ、鍵の危殆化やID偽装といったリスクを軽減する方法を提示しています。両社の技術を連携させることで、グローバルサインのマネージドPKI for IoTを通じて証明書登録のステップを自動化するプロビジョニングPCを取り入れています。



連携内容

自動化されたデバイスプロビジョニング

- デバイスユニットの製造ラインで証明書の登録が可能
- IDを安全に生成
- ハイスピードなID処理に対応

暗号化デバイスIDの運用

- 強固な認証
- 暗号化された通信

IoTスケールでの強固なデバイスID

特長／コンポーネント	検証済み	その他で可能な実装
デバイスとのインターフェース	SSH／IP	RPC／Serial-RS-232-TTL
登録ボリュームとシーケンス	単一デバイスに対して連続して1つずつ	数百～数千のデバイスを並行させる証明書発行サービス
セキュアな暗号プロセッサ	インフィニオン社OPTIGA™ TPM	OPTIGA™ Trust P OPTIGA™ Trust E OPTIGA™ Trust
デバイス環境	Linux	Windows／RTOS／組み込み／あらゆるプラットフォーム
プロビジョニングプロセス	プロビジョニングPC上での実行	デバイス上で直接実行 クラウドサービスで実行
利用用途	デバイスIDと認証	デバイスの完全性／証明 セキュアブート コードサイニングとセキュアアップデート フィーチャーコントロール／ブランド
運用体系	サーバとして動くデバイス	クライアントまたはサーバとして動くデバイス ゲートウェイ／多階層 デバイス to デバイス
PKIの特長	プライベート階層のRSA 2048 CRL／OCSPサービスのない中期間用証明書	パブリック階層 ECC短期間または長期間証明書 CRL／OCSPサービス

IoTに必要なセキュリティとスケールに適したテクノロジー

PKI（公開鍵暗号基盤）

- あらゆるデバイスや機器に長年利用されてきたセキュリティ技術
- 必要不可欠な情報セキュリティへの対応力
- 相互運用性
- IoT市場における大量発行に対応

セキュアな暗号プロセッサ

- ハードウェア上での安全な鍵の管理と暗号運用
- インフィニオン社のOPTIGA™ TPMが提供

両社の連携

- 鍵の危殆化やID偽装といったリスクを軽減
- 信頼性をデバイスに付与していくモデルをIoTレベルのスケールで拡張

お問い合わせ専用ダイヤル
03-6370-6500
（受付時間：平日10:00～18:00）

GMOグローバルサイン株式会社
東京都渋谷区桜丘町26-1 セルリアンタワー
グローバルサイン 検索 https://jp.globalsign.com/