



ENTRUST



Entrustは、Polycomの 電話へのデジタル証明書 の統合を加速します



POLYCOMはVoIPセキュリティを強化するために、ENTRUST専門サービスチームとNSHIELD HSMを利用します

象徴的な三角形の会議電話で最もよく知られるPolycomは、世界中の同僚やパートナーとのコラボレーションをさらに容易かつ効率的にし、快適に行えるようにすることによって、1990年代前半にビジネスコミュニケーションを変革しました。同社のブランドは、IT購入者の間で品質、明瞭さ、利便性の代名詞であり続けています。ボイスオーバーインターネットプロトコル (VoIP) デバイスの市場が成長し、デスクトップから会議室に至るまでのVoIP電話のポートフォリオが拡大する中で、Polycomは電話に固有のIDを与えて電話を強化することを決め、潜在的な偽造者や詐欺者を阻止すると同時に、顧客やサービスプロバイダーのネットワーク上での電話の識別を容易にしました。どのような方法で？Entrust nShield®ハードウェアセキュリティモジュール (HSM) によって生成かつ保護されたデジタル証明書と暗号化鍵を使用します。

「当社のVoIPデバイスは、デジタル証明書を使用してネットワーク上で認証できます」と、Polycomの製品管理責任者であるMarek Dutkiewiczは述べています。「証明書は製造プロセスの一部として発行されるため、顧客やパートナーは、潜在的な偽造者や「なりすまし」を阻止すると同時に、簡単に認証を行うことができます。私たちの成功は、Entrust専門サービスチームによって展開されたEntrust nShield HSMに基づいています。」

「**Entrustは、カスタマイズされた安全なVoIPソリューションの設計および実装に必要な専門知識を提供してくれました。**」

- Marek Dutkiewicz, Polycom

VoIPの安全性の確保

VoIPには、従来の通信技術に比べて、コストの削減と、他のIPアプリケーションとの統合の可能性という2つの主な利点があります。ただし、他の形式のインターネットベースの通信と同様に、ネットワーク上のデバイスや人物のIDが不明であるなど、セキュリティ上の懸念があります。

従来、VoIP電話は識別目的でパスワードを使用していたため、明確なID検証が困難であり、エンドユーザーやサービスプロバイダーのセットアップに時間がかかりました。また、このパスワードベースのプロセスは、電話メーカーを偽造デバイスから保護できませんでした。

デジタル証明書は、パスワードベースのセキュリティのいくつかの課題を解決します。デジタル証明書はパスワードとは異なり、デバイスがそれ自体と参加するネットワークを認証できるようにする一意の識別子です。例えば、有効な証明書を持つデバイスは、承認されたサーバに接続されていることを検証でき、承認されたサーバはデバイスの真正性を確認できます。デジタル証明書が安全に生成および配布されている場合、それを偽造することはできず、「なりすまし」または偽造デバイスを簡単に識別できます。

「電話が「なりすまし」である可能性がある場合、通話が不正に発信され、不正確に請求されるリスクがあります」とDutkiewicz氏は説明します。「Polycomは、顧客とパートナーのニーズを満たすソリューションの提供に取り組んでおり、セキュリティも例外ではありません。デジタル証明書を使用して電話を識別す

ることで、セキュリティリスクを大幅に減らすことができます。私たちは、証明書とそれに対応する秘密鍵を生成し、それらを電話に配置し、製造プロセス全体でシステムを維持できるソリューションが必要であることに気づきました。」

専門家への依頼

Polycomはそのアプローチを決定した後、適切なソリューションと実装パートナーを探し始めました。Polycomはいくつかのテクノロジーベンダーやソリューション開発者とオプションについて話し合いましたが、1つの例外を除いて、Polycomが求めていた、次のすべてのものを提供するものではありませんでした：実証済みのテクノロジー、製造における暗号化鍵の生成とデジタル証明書の発行の経験、安全なエンドツーエンドプロセスを開発する能力。Entrust専門サービスチームは例外でした。このチームは、Entrust nShield HSMがデジタル証明書の発行と鍵生成プロセスをどのように保護するかを説明しました。最も重要なこととして、このチームは、Polycomの製造プロセスと統合されたソリューションを設計し実行する方法も理解していました。

「私たちはEntrust nShield HSMを使用し、Entrust専門サービスチームの支援を受け、ソリューションを実装することにしました」とDutkiewicz氏は述べました。「Entrustは、カスタマイズされた安全なVoIPソリューションの設計および実装に必要な専門知識を提供してくれました。」

「Entrustチームは、顧客の通話や当社を偽造から保護するプロセスの開発と実装を支援してくれました。」

- Marek Dutkiewicz, Polycom

効果的なプロセスの開発

Polycomのニーズを完全に満たすプロセスを設計するために、Entrust専門サービスチームはPolycomのスタッフと密接に協力しました。Polycomは、製造プロセス内で証明書がどのように機能してほしいかを説明し、Entrust専門サービスチームは、Polycomが求める機能を提供できるシステムについて詳しく説明しました。

Entrustコンサルタントは、北米にあるPolycomのデータセンターで、鍵を生成し、Microsoft認証局(CA)を使用してデジタル証明書に署名できるソリューションを開発しました。鍵の生成と証明書への署名はすべて、HSM環境内で行われます。その後、鍵と証明書は、タイのPolycomの製造施設にあるEntrust nShield HSMに転送されます。ここで、鍵と証明書は、新しく製造されたVoIP電話に配置されるまで、暗号化されて保存されます。

「当社のデータセンターで鍵と証明書を生成し、それらを製造施設と新しいデバイスに安全に転送したかったのです」とDutkiewicz氏は言います。「Entrustは、私たちが求め、必要としたものを提供してくれました。Entrustチームは、顧客の通話や当社を偽造から保護するプロセスの開発と実装を支援してくれました。」

安全な実行

Entrust専門サービスチームは、Entrust nShield HSM内の安全な実行環境であるnShield CodeSafeを使用して、証明書と鍵の生成、送信、デバイス挿入プロセスのエンドツーエンドの保護を可能にしました。CodeSafeを使用することで、Entrust nShield HSMは安全な環境内で様々なプロセスを実行できます。そのため、Entrust専門サービスチームは、電話用のペアの鍵を生成し、証明書署名を要求し、暗号化パッケージをPolycomの製造施設に送信するコードを作成しました。チームはまた、製造施設のHSM内で暗号化されたSSL(セキュアソケットレイヤー)接続を開始し、新しく製造された電話で終了するプロセスを設計しました。この接続により、電話への鍵と証明書の安全な送信が可能になります。

「当社のEntrust nShield HSMは、電話を識別する証明書と秘密鍵を安全に保ち、nShield CodeSafeは、世界中の半分の発行プロセスを保護します」とDutkiewicz氏は説明します。「このプロセスは、製造プロセスにデジタル証明書の発行を含めるための非常に効果的で安全な方法であることがわかりました。」

ENTRUST専門サービスとの提携のメリット：

- プロジェクト完了の加速化
- なりすましや偽造を防ぐための安全なプロセス
- 製造プロセスに合うようカスタマイズされたソリューション
- ハイテク製造に比類のない専門知識を提供

組織のプロファイル

Polycomは、テレプレゼンス、ビデオ、音声ソリューションの世界的リーダーであり、人々がどこにいても接続およびコラボレーションできるようにするユニファイドコミュニケーション (UC) ソリューションにおけるビジョンを持った企業です。今日の経済状況において、Polycomのソリューションは迅速なROIを提供し、顧客のコスト削減、生産性の向上、二酸化炭素排出量の削減を支援します。

Polycom UCソリューションの詳細については、www.polycom.comをご覧ください。

継続的な成功のための基盤

Polycomは、Entrust nShield HSMを使用したデバイス認証プロセスにより、偽造のリスクの低減と販売機会の増加という2つの主な最終的なメリットが得られると考えています。

「偽造デバイスがどんなに本物のように見えても、有効な証明書がなければ、認証されたVoIPネットワークをだますことはできません」とDutkiewicz氏は述べています。「Entrust nShield HSMは、製造から日常の使用までのプロセス全体の基盤となるものです。私はこれを銀行の金庫室と考えていますが、実際にはそれ以上に安全なものです。最も重要なことは、当然、これは顧客に利益をもたらすことです。顧客は、VoIPデバイスに関して、煩わしさのないセキュリティを確実に望んでいます。デジタル証明書は、当社の売り上げ増加および市場シェアの拡大に役立ちます。」

ENTRUSTについて

Entrustは、信頼性の高い本人認証、決済、データ保護を可能にすることにより、世界の動きを安全に維持します。今日、人々はこれまで以上に、国境を越えた移動、買い物、電子政府サービスへのアクセス、企業ネットワークへのログインといったさまざまな場面で、シームレスで安全なユーザー体験を求めています。Entrustは、これらすべてのインタラクションに対応した、他では見られない広範なデジタルセキュリティおよび資格情報発行用ソリューションを提供しています。2,500名以上の従業員とグローバルパートナーのネットワークを備え、150か国以上における顧客から支持されているため、世界における多くの委託組織から信頼を得ていることは不思議ではありません。

詳細は下記URLをご覧ください。
entrust.com/ja/HSM

