WHITE PAPER

digicert

セキュリティ、効率性、アジリティのためのPKIのアップデート

PKI技術は行き当たりばったりで企業に導入されることがしばしば見受けられ、柔軟性に欠け、非効率で、皮肉なことに安全性に欠ける状況を生み出しました。最新のPKIは、エコシステム全体を管理下に置くことで、既存の技術を取り壊して置き換えることなく、これらの問題を解決することができます。

旧来のPKIシステムに依存しているIT環境は、頻繁な機能停止に見舞われる可能性があり、保守に多大な労力を要し、現在および将来のセキュリティ標準への適合が困難です。可能な限りの更新を行なっても、新しい利用例をサポートし、ビジネスを混乱させることなく迅速に保護を導入するためのアジリティに欠けることがしばしばです。既存の PKI システムの多くは、過去 10 年間に企業が採用した技術やイニシアティブ、変化する業界規制や標準をサポートするために十分なアップデートができていません。

本稿では、この問題と解決策について触れます。PKIシステムをアップデートし、ビジネスをサポートし、次世代攻撃をブロックするための最良のポジションを確立した企業の例を紹介します。

最新のPKI事情

PKIの目的は、ネットワークのあらゆる場所、さらには独自システム内でもトラストを確立することです。PKIシステムへの依存は絶えず高まっているが、これらのシステムを管理する能力は追いついていません。

この問題は、同一企業内で別々の PKI 実装を行う「PKI サイロ」による開発で顕著に見受けられます。サイロは、合併や買収により引き起こされたのかもしれませんし、PKI 管理を一元化するという選択肢を考慮せず、あるいは考慮したにもかかわらず、特定のプロジェクトのために作成されたものかもしれません。その結果、無駄なオーバーヘッドが発生している可能性があります。サイロは個別に管理されなければならず、おそらくは異なるツールで、おそらくは異なるチームによって管理されます。マネジメントが統制を取っていなければ、方針、ガバナンス、運用が競合する恐れもあります。

組織全体、また多くの種類のソフトウェアで暗号処理は行われています。ソフトウェア・スタックの多くの段階において、PKI は、当事者を認証するため、またはアプリケーショ ン通信やプライバシーを目的として鍵やデータを交換するために使用されています。

このような通信は、システム内やネットワーク上で絶えず発生しており、組織のセキュリティはその正しい運用に依存しています。

エンタープライズにおけるPKIの役割

公開鍵/秘密鍵による暗号は、インターネット上や企業内の当事者がトラストを確立するためのメカニズムです。ユーザーが本人であることを証明するため、サーバーやその他のデバイスが本人の利用であることを証明するため、そしてデータを保護するための暗号鍵を交換するために利用されます。PKI（公開鍵基盤）は、信頼されたプロトコル、ライブラリ、業界標準を組み合わせたものであり、ユーザーとデバイスがプライバシー、安全性、効率性をもって情報を交換することを可能にします。PKIの役割の詳細はこちらへ。

全組織的な PKI 管理は比較的最近見かけられるようになった現象です。以前は、PKIを実装するアプリケーションが独自のツールやセキュリティ・ポリシーが含んでいた傾向があり、組織内のPKIサイロを招いていました。

同様の例はたくさんあります：

- VPNシステムはその性質上、ネットワーク毎に実装し、個別のIDおよび暗号機能をサポートする証明書を発行しています。
- マイクロサービス環境では一般に、コンテナの識別と暗号化のために独自のPKIを作成します。
- 多くのUEM（統合エンドポイント管理）システムは、認証のために独自の証明書を発行します。
- IoTデバイス管理プラットフォームは、多くの場合、管理ソフトウェアがデバイスを識別・制御するための特別なPKIを実装しています。

また、他のソフトウェアと同様に、合併や買収によって企業内に異なる PKI システムが導入されることも頻発しています。

行き当たりばったりのPKI

現代の組織では、技術の採用と成長はしばしば行き当たりばったりに陥りがちです。技術は、正式な計画の一部としてではなく、企業買収や上層部からのイニシアチブにより採用されることもあります。モバイル機器、クラウド・コンピューティング、DevOpsなど、PKIに強く依存する重要なインフラ機能は、運用するIT部門へ既成事実として導入されていることが多くあります。

これらも含めた多くの例では、PKI 機能はその導入目的のためだけに提供され、管理されたインフラストラクチャに統合されていない可能性が高いのです。その結果、PKI管理作業は、複数の担当者が多くの異なるツールを使用して、多くの場合同時に対応を行う必要が出てきています。同時に、一般的な組織の多くのシステムでは、PKIを使った強力な暗号通信と認証さえまだ実装されていないこともあります。

デジタル証明書とPKI

PKI 認証で利用される主なリソースは、デジタル証明書です。ユーザー、プログラム、モバイル機器、その他実行ソフトウェアなど、アクセスや利用を認証されるべきものを検証・識別します。その結果、管理下にある証書の数は飛躍的に増加し、今後も増え続けると言われています。2021年のPonemon Instituteの調査によると、一般的な企業では5万枚以上の証明書を管理しているといいます。現在では間違いなくはるかに増えたことでしょう。

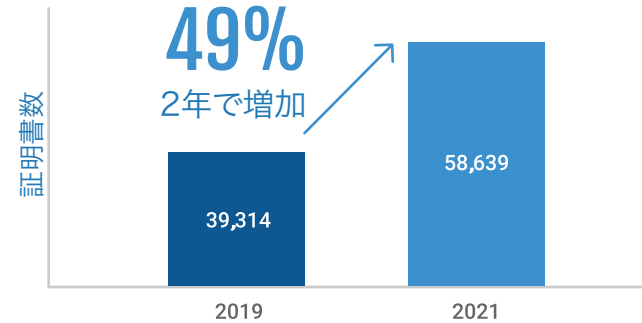
証明書にはそれぞれ有効期限があります。例えば、パブリックで信頼されたTLSサーバ証明書の最大有効期限は398日、つまり約13カ月ですが、クラウド・ワークロードのような社内通信用途で使用される証明書の寿命は劇的に短いです。証明書の更新を自動化する必要性は、特に証明書の数が増え、寿命が短くなる状況を鑑みると自明のことです。

証明書ライフサイクル管理で難しいのは、失効の管理です。CRL（証明書失効リスト）とOCSP（オンライン 証明書ステータス プロトコル）という2つの方法がありますが、どちらも効率的かつ大規模に実装するのは困難です。

証明書の有効期限が短い場合、失効させる必要はなく、その代わりすぐに有効期限切れにしてしまえば良いのです。証明書の失効と更新は、複数のシステムやプロセスにまたがってオーケストレーショ ンを行う必要があることが多い証明書運用の 2 つの例です。

頻発する業務停止

失効証明書は、PKI管理の不備に起因する障害やガバナンス・リスク&コンプライアンス（GRC）の失敗の一因に過ぎませんが、最も一般的なものです。証明書の総数と同様、今後その数は増えるでしょう。



Ponemon「IoTとPKIトレンド 2021」

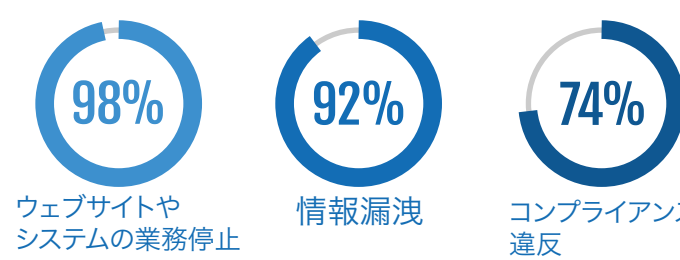
このような状況においても、手作業で更新される証明書の数は大量にあります。単に証明書を手動で更新する事がシステム停止の原因ではありません。大規模で複雑な組織では、担当者がどのような証明書を持っているのかさえ把握していないかもしれません。このような無秩序な状態では、技術計画や予算計画を立てることは不可能です。

システムをうまく管理していたとしても、障害が発生する可能性はあるため、最新の PKI では、障害が発生しても機能し、迅速に復旧できることが重要です。

従来のシステムの金銭的コスト

その性質上、PKIシステムを追加するたびに、保守・管理コストも追加されます。どのシステムも、十分な専門知識を持つ人（それを見つけるのはますます難しくなっています）が管理する必要があり、ソフトウェア自体には継続的なライセンスやメンテナンス費用がかかる場合があります。 これは、特に複数のシステムを扱う場合、大きな運用オーバーヘッドにつながる可能性があります。 システムがバラバラで、運用が細分化していると、可視化と管理に課題が生じ、障害やセキュリティ侵害のリスクが高まります。

最新の PKI プラットフォームの定義



2024年 デジタルトラストの実態調査

ディスカバリー、インベントリー、所有権

行き当たりばったりの企業 PKI に秩序をもたらすには、ディスカバリープロセスから始めます。最新のPKIは、ネットワーク内の到達可能なすべてをスキャンし、既存の証明書に関する他のシステムからのデータを取り込み、できれば資産追跡システムの一部として、IT計画を立てる為のインベントリを作成します。優れたディスカバリ・プロセスは、発行認証局に関係なく、かつパブリックおよびプライベートの別なく多くの種類の証明書を特定し、複数のPKI サイロを発見します。

これらは、内部CAまたはパブリックCAからデジタル証明書を発行するための個別のシステムです。それでは一体これらはどのように実装されたのでしょうか？これらは特定のアプリケーションをサポートするために個々に設置されたか、合併や社内統合の一環として追加された可能性が高いのです。その理由はそれぞれあったでしょうし、当時はどれも理に適っていたかもしれません。

このディスカバリー・プロセスでは、証明書の所有権を明確にし、ライフサイクル管理と予算報告業務を適切な担当者に割り当てることが重要です。同時に、PKI を使用するアプリケーションのインベントリと所有権も明確にすることができるでしょう。

“PKI”とは？　“P”は何の頭文字？

公開鍵暗号には公開鍵と秘密鍵が含まれ、PKIはこれらの運用を可能にするシステムとサービスを指します。「公開鍵／秘密鍵を利用するインフラ」と言っても、”P“はひとつしかなく、“パブリック “です。それは、秘密鍵が非公開で、インフラが公開されているからでしょう。

パブリックPKIは、規制は厳しい反面、様々な端末にルートが実装されているので利用が簡単ですが、コストが高く、プロファイルの自由度が少ないことが特徴です。そのためWeb通信やS/MIMEのような用途が明確な場合に利用されます。

組織内でプライベートPKIを利用することは一般的で、端末やシステム、WiFi、VPNのアクセス認証やKubernetesクラスタのように、特定のアプリケーションにセキュリティを追加するためにそれぞれ利用目的のプロファイルに合わせてセットアップされます。ただ自由度が高い反面、アクセス管理がしっかりしていないと、管理が十分に行われない「シャドーIT」化してしまう可能性もあり、退職者のアクセス権限で接続できてしまうなどセキュリティの穴にもなります。ディスカバリースキャンをして初めて顕在化することがあります。

ディスカバリーと所有権

統合された管理、分散可能な利用

最新のPKIプラットフォームは、統合された管理と監視を実現しながら、業務ごとに分散化された証明書の利用とライフサイクル管理を提供します。組織の各部門で組織全体の統一されたポリシーを遵守しつつ証明書の取得と利用を管理できるということを意味します。多くのクラウドソフトウェアと同様、最新のPKIは、ある程度のセルフサービスを提供するときに最もうまく機能します。

ここでいうセルフサービスとは何でしょう?PKI システムの一部は、証明書ライフサイクル管理システムであり、システムの使用に関するポリシ ーやインフラ管理を含む多くの機能を一元的に管理します。しかし、組織内の部署や個人は、ポリシーに従って多くの一般的な証明書ライフサイクル管理業務を実行できるはずです。

このために証明書ライフサイクル管理は、利用者が証明書を要求し取得できるアクセス可能なウェブ・ポータルまたは専用アプリケーションを提供し、PKI チームの支援を必要とする複雑な操作に関する支援を提供します。また、最新の PKI システムが、標準プロトコル、API、およびサービス統合といった容易な手法で、システムやデバイスへの自動的な証明書配布とインストールをサポートすることも重要です。

可能であれば一元管理することで、PKI システムを最も専門知識のある管理者の手に委ねることができ、レガシー PKI システムに割かれていた人員と予算を解放することも可能です。

パブリックと内部(プライベート)PKI利用例

多様なPKIを統合するには、あらゆる認証局と、クラウド、オンプレミス、ハイブリッドといったさまざまなアーキテクチャをサポートする必要があります。デジサートのようなパブリック認証局もありますが、アプリケーションによっては社内プライベート認証局の利用が適切です。いずれも同じように管理されるべきです。業界標準はパブリック認証局間の証明書の相互運用性を提供しますが、プライベート認証局にはそのような標準はありません。最新のPKIは、その両方に対応すべきですが、リスクの高いプライベート認証局の慣行を防止するインテリジェンスを備える必要があります。

それではなぜプライベートPKIを運営するのでしょうか? 大容量のコンテナ・ベースのアプリケーションなど、特定のアプリケーションは、短時間のタスクに大量の証明書を利用します。プライベートPKIが提供する認証と暗号化は、このようなワークロードや環境の安全性を確保する上で価値があります。 最も高性能なソリューションは、証明書要求に迅速に対応し、すべての操作を記録できるローカルのプライベート認証局 です。

このような状況であっても、アプリケーションが論理的に分離されている場合、プライベート認証局 はグローバルPKI ポリシーを使用して管理するのがベストプラクティスです。このようなガバナンス・スタイルを提供するマネージドPKIが、ほとんどの組織にとって理想的です。

多様なワークロードへの対応

最新の PKI システムは、エンドユーザー機器、サーバー、サービス、アプリケーション、コンテナ、VM など、あらゆるワークロードに適応可能です。オープン・スタンダードの長い歴史のおかげで、どのPKIシステムも一般的に他のどのシステムとも相互運用が可能です。 最新のシステムは、標準的なインターフェイスやベンダーとの統合をすることで、他のどのようなシステムやアプリケーションともすぐに連携できます。後述する通り、エンタープライズ・アーキテクチャとシームレスに相互運用・統合する能力は必須です。

柔軟な実装モデル

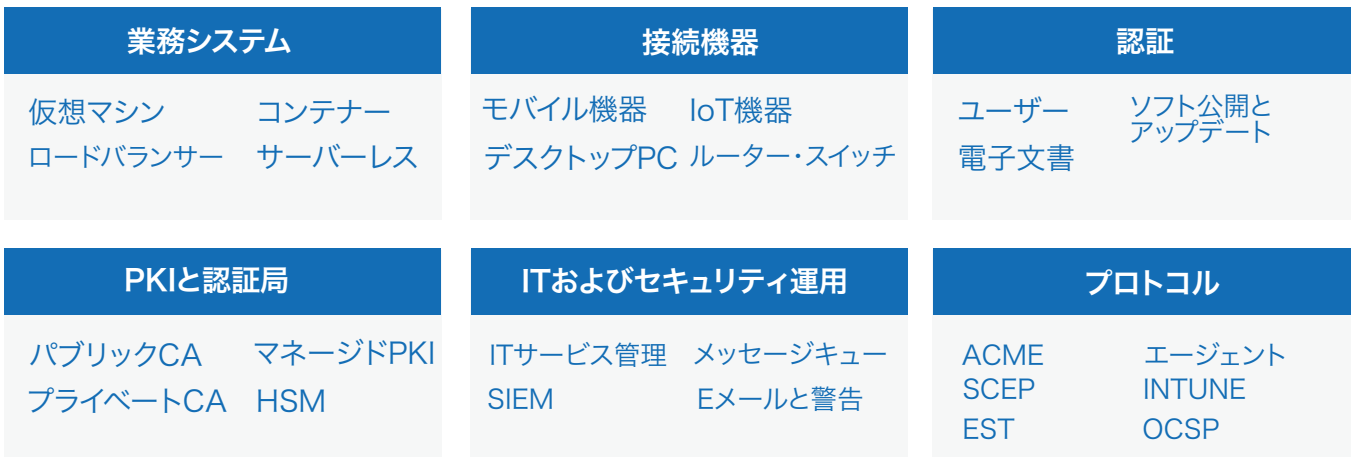
ハイブリッド実装は特に厄介で重要です。1つの論理アプリケーションは、オンプレミスのシステムと複数のクラウドにコンポーネントを保有することができます。また、専有機器に組み込まれたクライアント証明書やベンダー証明書を管理することも必要です。複雑な組織では、法的要件が異なる管轄区域で独自に活動する部門があり、適切な管理を行うための柔軟性が必要とされる場合もあります。

最新の PKI システムでは、このような状況における証明書の管理は、簡単ではないにせよ、論理的であるべきです。これには、従来のITインフラ向けのオンプレミス・ディレクトリ・サービスとの統合、クラウド・ネイティブ・アプリケーション向けのクラウド・プロバイダー証明書サービスとの互換性、ハイブリッド・セットアップ全体で証明書を管理する機能などが含まれます。これらの環境に一貫した管理ツールと自動化機能を提供することで、組織は証明書ライフサイクル・プロセスを合理化し、セキュリティ・リスクを回避することができます。

ワークフローと自動化

最新の PKI システムでは、証明書の失効などのイベントに必要な承認や、すべてのイベント(ある いは、少なくとも顧客が保管を希望するすべてのイベント)の記録管理など、主要な手順やワークフ ローが準備されています。

日常的なユースケースと特別なユースケースを自動化し、ユーザーエクスペリエンスを向上させ、管理者のオーバーヘッドを削減し、業務停止やセキュリティインシデントの原因となる設定ミスのリスクを減らす必要があります。



PKI エコシステム

レポート、分析、通知

また、多くの標準的レポートと、それらをカスタマイズする機能を提供する必要があります。例を挙げると

- インベントリーレポート
- 期限切れ証明書および期限切れ間近の証明書レポート
- 失効証明書レポート
- 組織のセキュリティ・ポリシー、業界標準、関連する政府規制への証明書準拠レポート

最新の PKI システムは、どの証明書がまだ脆弱な暗号アルゴリズムや鍵長を使用しているかといった、重要な問題を示す分析を提供すべきです。また、コスト分析を行い、コスト最適化の機会を提案することもできるでしょう。さらに証明書の管理の不備や規制遵守に関連したリスク評価を行うこともできるかもしれません。

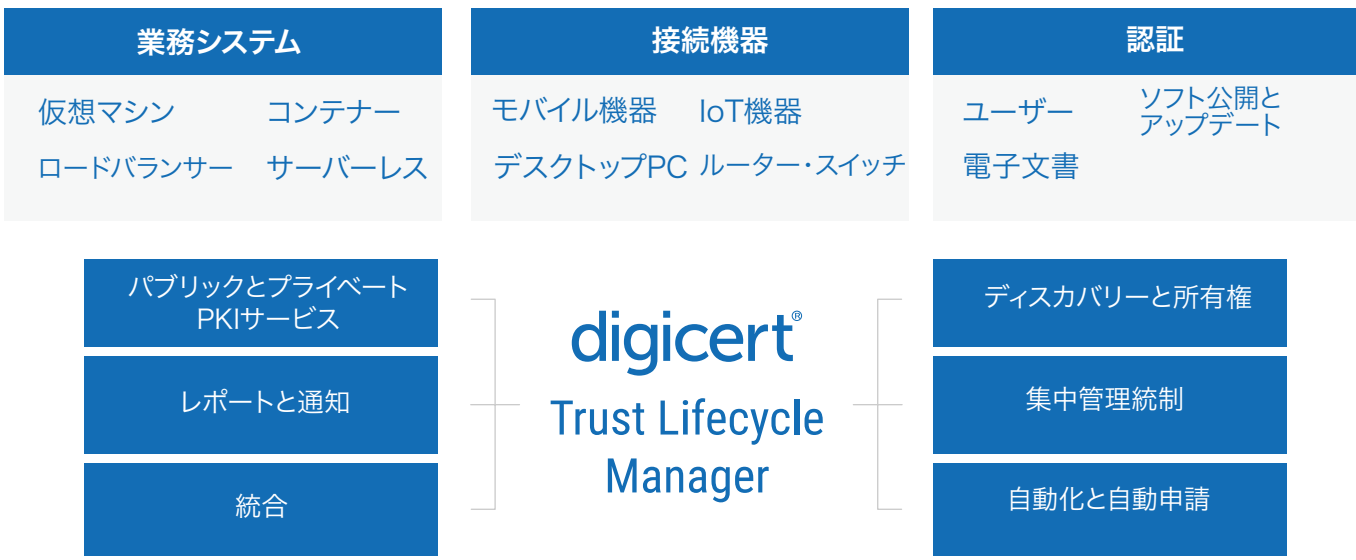
プロアクティブな面としては、最新の PKI は、多くのインシデントに対してユーザに警告を発し、インシデントのエスカレーションとコンフィギュレーションを可能にすべきでしょう。明らかなのは、有効期限が近づいている証明書への警告です。ほとんどの場合、証明書が自動的に更新されるように設定し、更新がいつ行われるかだけをアラートに表示させるのが最善でしょう。証明書の失効、ポリシー違反、システム外での証明書の発見を、適切なユーザに通知しなければなりません。もちろん、通知は、サービス管理とセキュリティ運用に関わる組織における慣行に従って行われるべきです。

エコシステムサポートの重要性

最後に、標準的なインターフェイスと独自のインターフェイスの両方を使用して、組織のエコシステム内の関連ソフトウェアと統合する必要があります。PKIエコシステムは広範かつ複雑で、相互運用性の点で完全標準化されていません。優れた最新のPKIは、Amazon Web ServicesやHashiCorpのような主要なクラウドサービスやDevOpsインフラストラクチャプロバイダーと直接統合し、ディスカバリプロセスを容易にし、集中管理を実現できます。

組織におけるPKIの範囲は意識せずとも拡大しているため、多くの組織でPKIを利用している製品が増加しています。Microsoft Windows をはじめとするOSは、ネット接続と認証にPKIを利用しています。OfficeやExchange ServerのようなMicrosoftのアプリケーション・プラットフォームは、ネット接続、認証、暗号化のためにPKIを広範囲に使用しています。アップルやグーグルの製品も同じ理由でPKIに依存しています。Adobe Acrobatやその他のPDFツールは、デジタル証明書を使用してPDFファイルにデジタル署名し、作成者の身元を証明します。例えば、コンサルタントが作成した独自アプリケーションは、規制遵守要件を満たすために、デジタル・トランザクションや通信が安全で検証可能であることを保証するために、PKIを利用することがあります。最新のPKIを利用することで、これらのすべてがより良く機能し、より安全になります。

この分野における主な特殊ケースは、WindowsとAzure上のMicrosoft Active Directoryです。1990年代に設計されたADはモダンで洗練されていたかもしれませんが、今日ではテクノロジーの離れ小島です。Microsoftは、NTLMやKerberosではなく、SAML、OAuth、OpenID Connectなどのプロトコルを使用するAzure Active Directory（現在はMicrosoft Entra Domain Services）で、最新の標準を目指しています。Azure ADは、多要素認証、条件付きアクセス、シングルサインオンを中核機能としています。



DigiCert Trust Lifecycle Manager

組織は、ユーザー、サーバー、ドメイン管理のためActive Directoryに大きく依存しているでしょう。しかし、モバイル機器、インターネットサービス、その他のリソースを別の手段で管理する必要もあります。PKIを必要とするアプリケーションは他にも多数あり、そのため最新のPKIは、多くのアプリケーションと可能な限りシームレスに統合すべきです。同様に開発者は、堅牢なPKIサポートを行う最も安全なDevOpsツールを使用してください。ウェブ・サーバー、ロード・バランサー、その他のアプリケーション・プラットフォームは、常に潜在的なPKIの需要があります。ファイアウォールやルーターなどのネットワーク機器も、安全な通信のためにPKIを利用しますし、モバイル・デバイス管理はPKIを広範囲に利用しています。このような例は枚挙にいとまがありません。

最新の PKI は、これらすべての管理を1つのシステムに統合し、組織が論理的に、他の PKI システムと協調して管理できるようにするべきなのです。

最新のPKIの実用例

紹介した最新のPKIソリューションというのは抽象的な考えではありません。それはすでに実現しており、一般的にはシステムアップデートプロジェクトや統合プロセスに直結しています。

以下は、アップデートに成功した例とそれに伴うメリットを紹介するための3つの顧客事例です。

金融サービスのセキュリティにおけるディスカバリー

ある大手金融サービス・グループは、管理が困難な多数のサイロ化された公開鍵基盤（PKI）システムに依存していました。時代遅れ、かつそれぞれ別の部署で管理するPKI環境は、期限切れ証明書による頻繁な機能停止をそれぞれ引き起こしていたのです。証明書は担当者がエクセルで管理し、全体的な可視化は行われていませんでした。また証明書を使用するシステムのIT管理者にPKIの専門知識がないこともあり、状況は悪化する一方でした。業務復旧のため元従業員に連絡を取らなければならない事態も発生しました。

同社は、DigiCert Trust Lifecycle Managerを利用して、環境にあるすべての証明書の包括的なディスカバリーを行い、見つかった証明書管理の所有権の割り当てからPKIのアップデートを開始しました。その結果、活動休止中のシステムに関連する未使用の証明書が、いまだにサイロ管理されていることも判明しました。

Trust Lifecycle Managerにより実現されたディスカバリー、インベントリ、および所有権設定のプロセスにより、同社は以下のことを実現しました：

- コスト削減と効率性の向上:不要な証明書やシステムの廃止を促進し、予算の節約と ITオペレーションの合理化を実現しました。
- セキュリティ体制の強化：PKI 環境に対する理解が深まったことで、脆弱性が特定され、使用されていないシステムの廃止により攻撃対象が減少しました。
- 管理の合理化:証明書管理をITチームの直接の管轄下に統合し、プロアクティブな管理を可能にし、PKIを起因とするシステム停止を減少させました。

自動化による業務の効率化

複数のデータセンターを利用し数千台の仮想マシンで複雑なITインフラを運用するあるテクノロジー企業は、証明書の数が増え、プロビジョニングとインストールに手作業が伴うため、証明書の管理に苦慮していました。

1枚の証明書のプロビジョニングとインストールには数時間を費やすことがあります。その上、証明書のインベントリやライフサイクルが可視化されていないため、有効期限切れや設定ミスに起因する障害のリスクが高まっているのです。

Trust Lifecycle Manager は、証明書のライフサイクル管理を自動化・合理化し、効率を大幅に改善し、業務の停止リスクを低減しました。

主な利点は以下の通りです：

- 自動申請の簡素化：構成テンプレートと自動化により、証明書のプロビジョニング時間を数時間から数分に短縮しました。
- 可視化の強化：証明書のディスカバリー・インベントリにより、監視が強化されました。
- セキュリティの向上：危殆化した証明書を失効させ、入れ替えを自動化し、セキュリティを強化しました。
- 効率の向上：多様なワークロードとのシームレスな統合とルーチンタスクの自動化により、ITの負担が軽減されました。

M&AにおけるPKIの盲点を克服

この大企業では、合併や買収によって引き受けたIT業務に関連する証明書管理の課題にしばしば驚かされていました。この複雑な環境には、オンプレミスやクラウドベースのインフラが含まれ、複数の認証局から発行された証明書が、さまざまなポリシーやプロセスで管理されていました。

複数の認証局、一貫性のないポリシー、集中管理の欠如による証明書の課題は、効率的な業務を妨げます。合併や買収は、新しい証明書在庫、一貫性にないポリシー・システムを導入することで、こうした課題を悪化させることに直結していました。その結果、期限切れまたは危殆化した証明書により引き起こされる業務停止、システム侵害、業務中断のリスクが増大していました。

同組織はPKIの刷新のためにデジサートを選びました。Trust Lifecycle Managerを使うことで、これらの課題に対処しました：

- 包括ディスカバリー：複数の CA および環境に分散している証明書を特定し、インベントリ化しました。
- 集中管理：証明書ポリシーとプロセスを統合し、効率的な管理を実現しました。
- 自動化：証明書の発行、更新、失効プロセスを合理化しました。
- 統合：既存の証明書管理システムとシームレスに統合しました。

暗号アジリティとPKIランドスケープ

PKIは、あらゆる領域におけるセキュリティの基本であるため、攻撃的および防御的なセキュリティ研究の豊富な分野です。長年にわたり、PKI に採用された標準の弱点に対処するため、多くの変更が採用されてきました。

行き当たりばったりのPKIでこのような変更を実施することは、非常に難しく、許容可能な時間軸で、ビジネスへの混乱を最小限に抑えながら移行に成功する可能性は低いのが現実です。

多くの例がありますが、そのひとつは鍵長です。計算能力が年々向上するにつれ、攻撃者はより短く、弱い鍵は侵害できるようになっています。最新のPKIシステムは、弱い鍵があるかどうかを判断し、より強い鍵への交換を促すことにも使われます。

また、研究者たちは過去にもいくつかの暗号アルゴリズムにおいて弱点・解読方法を発見してきました。これは特にハッシュ・アルゴリズムで何度も起こっており、広く利用されてきたMD5やSHA1ハッシュ・アルゴリズムの弱点は実証されています。最新のPKIシステムを導入している企業は、組織内の各部門により脆弱なアルゴリズムが利用されていないことを確認することができます。

しかし、最大の問題はこれからです。最近実現性が語られることが増えている量子コンピュータは、広く普及している暗号アルゴ

リズムの多くに対する攻撃を成功させる可能性があります。米国商務省標準化技術研究所(NIST)は長年この問題に取り組んでおり、初の耐量子コンピューター暗号標準を2024年に発表しました。アルゴリズムによっては、より大きな鍵を使うことで、“耐量子コンピューター “を実現できるものもありますが、完全にアルゴリズムを置き換えなければ使えないものもあります。

ハッシュ・アルゴリズムと同様、最新のPKIなしでこのプロセスを管理することは困難だと言わざるを得ません。最新のPKIシステムは、すでに新しいNISTの耐量子コンピューター暗号アルゴリズムのサポートを開始し初めています。しかし、発表済みの耐量子コンピューター暗号が、量子コンピューターやAIの進化、そして研究者により解読される可能性はあるので、何度も移行を繰り返す可能性も否めません。その際にPKI利用状況の全体像を可視化する機能は必須となるでしょう。

推奨

最新のPKIを採用することは、「古いものを新たに取り替える」提案で解決するものではありません。これにより、既存の暗号資産も安全かつ効率的に使用できるようつつ、新たな暗号に対応することが必要です。最新のPKIへの移行は複雑で時間がかかるものですが、幸いなことにやることは決まっています：

1. ディスカバリーと評価：現在の PKI システムを評価することから始めます。たとえすぐにアクションを起こさないとしても、ディスカバリーを行えば、目指すべき方向が定まるでしょう。どのような証明書を持っているかが分かり、PKIが組織内でどの程度利用（放置）されているかが分かります。多くの組織で、ディスカバリー・レポートにより多くの驚くべき事実が見つかり、秩序と統制が必要だと認識を改めることになるでしょう。それにより各PKI システムの長所、短所、改善点を特定し、ビジネス目標および各規制要件と PKI の整合性を評価すべきです。このアセスメントにより、PKIのアップデートの方向性が定まることでしょう。

2. ユースケースの優先順位付け：組織の業務を推進する重要なユースケースを決定する。優先順位の高い分野に対し、PKI のアップデートに取り組んでください。このアプローチは、利益の最大化と投資対効果をもたらすでしょう。

3. ポリシーとガバナンスの一元化：PKIを単一のシステムまたは階層に一元化することは、一部の組織には有効でありそれも一つの推奨です。しかし、より複雑な組織や特殊な実装方法でPKIを利用している場合、ポリシーと統制の一元化に重点を置き、ディスカバリーによる可視性を組み合わせることで、組織内でそれぞれ利用されている特定のユースケースに合わせて微調整することをお勧めします。

4. パブリックとプライベートの統合：パブリックとプライベートの PKI ユースケースを統一プラットフォームに統合することは、PKI のアップデートにおける取り組みとしては一般的です。そうすることで、管理が簡素化され、コストが削減され、セキュリティが向上するからです。統合に伴う潜在的なメリットと課題を評価し、それらの要件を満たすプラットフォームを選択してください。

最新の PKI を導入していない企業は、最新の PKIにより実現するプロセス自動化や証明書の期限切れにより発生する機能停止に直面します。また、無秩序な暗号インフラや不必要な証明書のために余分な管理リソースを必要とし、多額の費用を浪費する結果となります。

そのような無駄を省き、既存のエコシステムと相互運用でき、ビジネスを中断させることなく変更やアップグレードが可能なソリューションがこれから求められます。

DigiCertについて

インターネットをより安全に保護する方法を見いだすことがデジサートの原点です。耐量子コンピューター暗号（PQC）、TLS、PKI、IoTソリューションが、世界中の人々や企業から、1日に何百万回も、あらゆる場所で信頼されているのはそのためです。それがお客様から常に5つ星の評価をいただいている理由です。

Trust Lifecycle ManagerがどのようにPKIのアップデートを支援するかについてはこちらを確認ください。