WHITE PAPER



CodeMeter Certificate Vault

CodeMeter による証明書管理：快適性とセキュリティ

Marco Blume, Product Management WIBU-SYSTEMS AG
www.wibu.com

WIBU SYSTEMS

目次

はじめに 3
証明書とは 4
セキュアに証明書を保持するための原則 5
現場での課題 6
CodeMeter Certificate Vault の利点 6
CodeMeter Certificate Vault のユースケース 6
CodeMeter Certificate Vault のテクノロジー 7
標準インターフェイス 8
CodeMeter Certificate Vault の特徴的な機能 9
ユーザーモードで使用する CodeMeter Certificate Vault ドングル 11
ISV (独立系ソフトウェアベンダー) モードで使用する CodeMeter Certificate Vault ドングル 11
まとめ 11
用語集 11

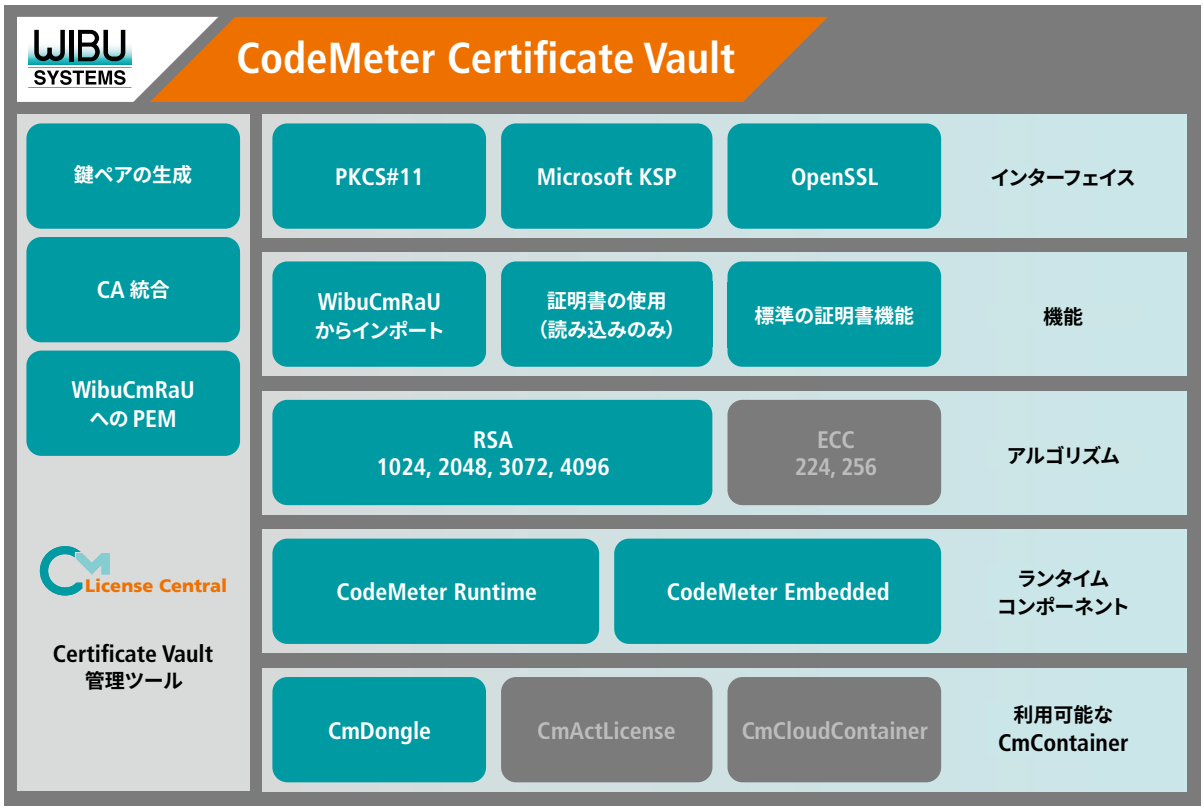


著者

2013 年より、組み込みシステム関連の製品および研究開発マネージャーとして WIBU-SYSTEMS AG に在籍。組み込みシステムの保護をはじめ、メーカー向けのカスタマイズコンセプトの開発、研究など、幅広い業務に従事。また Wibu-Systems 入社以前には、ATM やレジシステムのセキュリティ担当のプロダクトマネージャーを 11 年、その後、映像システムや産業オートメーションの組み込みスペシャリストを務めるなど、さまざまな組み込みシステムに関わる。

はじめに

CodeMeter Certificate Vault は、CodeMeter テクノロジーを基盤とし、CmStick 、CmCard 、CmASIC などの CodeMeter ハードウェアに X.509 証明書をセキュアに保存し、標準インターフェイスを介してアプリケーションから利用できる手段を提供します。CodeMeter Certificate Vault は CodeMeter ライセンス管理及び保護テクノロジーに加えて、もしくは、それらとは独立して使用することができます。



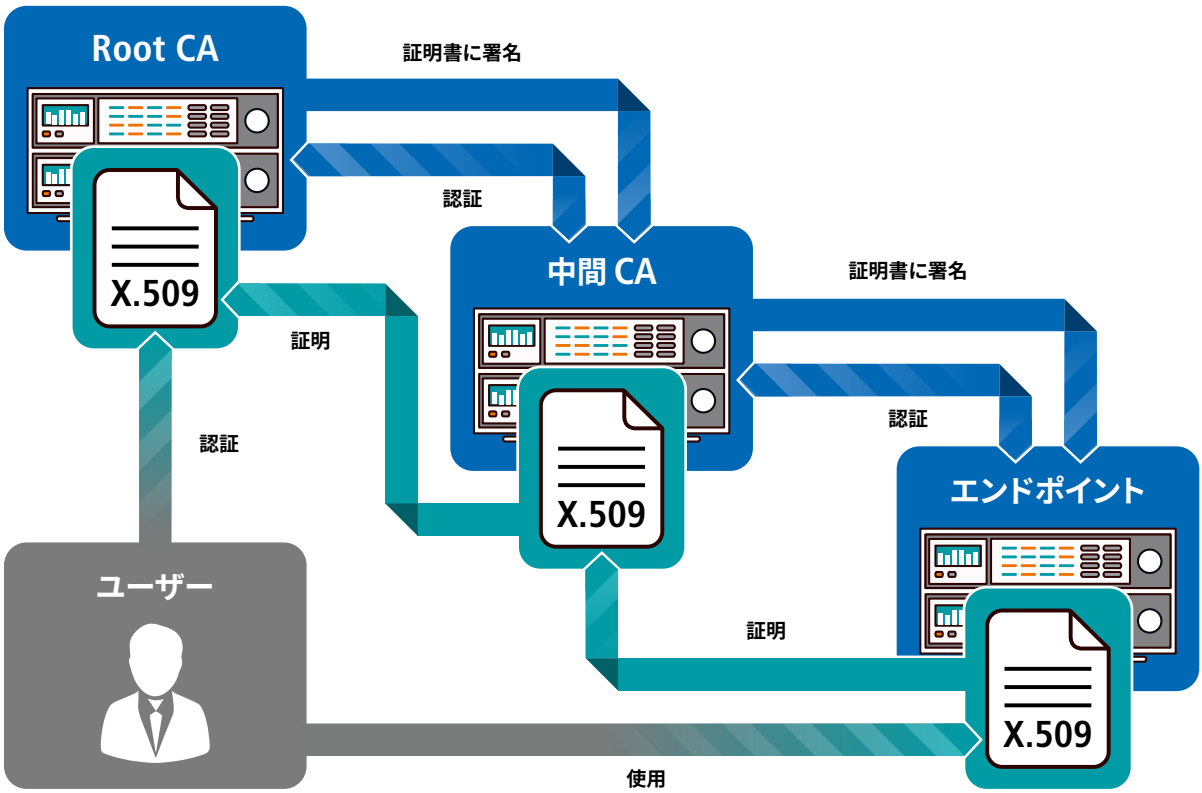
証明書とは

X.509 形式は、公開鍵基盤（PKI）のデジタル証明書における標準規格です。このような証明書は、真正性や身元を電子的に証明する役割を果たし、https 、OPC UA、MQTT などを介した暗号化通信や、電子メールの暗号化・署名によく使用されます。この標準規格では、X.509 証明書の構造と内容が詳細に定義されています。ユーザーに関する ID 情報に加え、バージョン番号、証明書のシリアル番号、使用されるアルゴリズム、所有者の公開鍵に関する情報、認証局（CA）によるデジタル署名、および拡張機能が含まれています。この形式により、X.509 は、PKI 証明書の標準として受け入れられています。

証明書は、PKI チェーン全体の末端に位置する 1 つのリンクでしかありません。チェーンは、リンクの最上位のルート証明書から下へと流れる階層構造を表しています。証明書に署名及び認証するエンティティは、CA と呼ばれ、証明書が、リクエストを送信したユーザー、デバイス、またはサービスの公開鍵と一致することを確認します。このように、CA はプロセス全体において重要な役割を担っています。CA は、証明書の作成・認証・失効を行うことができるなど、証明書を管理し、公開データベース上で利用可能にし、認証プロセスにおけるすべてのステップを記録しなければなりません。つまり、CA は、現実世界に置き換えると、パスポートを発行する公務員のような存在と言えます。市民がやって来ると、その身元を確認した上で、顔写真とデジタル化された指紋がバインドされたパスポートを発行します。現に最新のパスポートには、デジタル証明書と秘密鍵が組み込まれ、証明書の作成と管理という CA がもつ2つの役割が完全に融合された形になっています。

X.509 証明書の一般的な使用例

- 暗号化された https 接続の構築、Web サーバーと Web ブラウザ間でのデータ共有
- S/MIME 標準による電子メールの暗号化と署名
- デジタル文書へのデジタル署名
- ソフトウェアへのデジタル署名
- 通信利用のユーザー認証
- VPN（仮想プライベートネットワーク）の構築、暗号化ファイルの共有
- ID 証明（デジタルIDカード）



セキュアに証明書を保持するための原則

証明書は、デジタルデータの一部であり、ファイルシステム内のファイルやコンピューターのワーキングメモリに保管されています。すべての証明書は、非対称暗号化プロセスを通して特定の公開鍵と秘密鍵のペアに対して発行されます。そして、公開鍵は証明書に、その対となる秘密鍵は、証明書の所有者がもつデバイス上の別のファイルに保管されます。このシステムこそが、セキュリティリスクになり得るのです。従って、秘密鍵は、証明書の所有者以外がアクセスできないよう制限する必要があり、また保管場所が安全であるとしても、秘密鍵を定期的にその安全な環境から取り出し、CPU 上で暗号化処理を行う必要があります。但し、ここでも攻撃者に狙われる可能性が高まります。

想像してみてください。非常に高いフェンス、頑丈なドア、そして複雑な鍵、これら全てを備えた建物でさえも、鍵が安全に保管されていなければ、泥棒に侵入される可能性は十分あります。このシンプルな例から、どこに大きな危険が潜み、どこを重点的に保護すべきかわかるはずです。つまり、CA が上位階層に位置するほど、その保護を強化する必要があります。ソリューションとしては、インターネット上の https 通信（TLS）向けの証明書を発行する商用 CA 、または銀行や大企業に特化した、いわゆるハードウェアセキュリティモジュール（HSM）がよく使用されます。これらは閉じられたシステムであり、不正操作に対する堅牢性が特徴とされています。また証明書と鍵はセキュアな環境に保管され、設計にもよりますが、通常、そこから取り出すことは不可能です。鍵は、この保護された空間の中でのみ使用され、搭載されたプロセッサーでさえも外部からアクセスすることはできない構造になっています。従って、ユーザーは、システムにリクエストを送り、そこから必要な出力を受け取ることしかできません。すべての暗号化処理は、このシステム内部で行われ、万が一システムが攻撃されたり、開けられたりした場合には、鍵は自動的に削除される、もしくは使用できなくなります。これらの HSM は、データセンターに特化して設計され、さまざまな高性能暗号化処理に長けているため、多額の投資が必要となります。

また、ユーザー側では、証明書は、TPM モジュール（特に PC ユーザー向け）、あるいは別のセキュアエレメント（SE）のいずれかに格納されます。SE は、多種多様なフォームをもち、アプリケーションと通信するためにさまざまなインターフェイスや API（アプリケーションプログラミングインターフェイス）を使用します。非常に広く普及している標準規格の1つに、PKCS#11 があり、これはすでにCodeMeter Certificate Vault にとって不可欠な要素となっています。PKCS#11 をサポートするアプリケーションは、CodeMeter Certificate Vault を鍵の安全な保管場所として使用することができます。PKCS#11 インターフェイスは、鍵と証明書のセキュアな保管・使用に関連するすべてのプロセスを管理します。

現場での課題

証明書の扱いは、マニュアル作業が求められる場合、特に困難がいます。多くの現場において、マニュアルでの作業は望ましくないか、或いは避けられる理由にもなります。産業機械はネットに接続されていない場合が多いですが、その代わり、ダウンタイムを可能な限り最小限に抑えつつ自動で稼働しています。従って、メンテナンス・修理を担当する技術者は、証明書の存在と有効性をチェックする必要はありません。しかしそれに伴い、現場でのセキュアな通信とデバイスの整合性に関する基準の厳しさは、増しています。そこで、証明書管理の自動化と同時に安全性を確保する CodeMeter Certificate Vault の出番になります。

CodeMeter Certificate Vault の利点

CodeMeter Certificate Vault は、秘密鍵のセキュアな保管・使用を第一に考えて設計されています。これは、秘密鍵の整合性およびセキュリティを維持するという本質的な目的を達成するためです。CodeMeter Certificate Vault の標準インターフェイスは、既存のソフトウェア環境や、証明書、鍵の移動を可能にする手段への統合を容易にし、様々な条件やクライアントの要件に対応することができる汎用性の高いツールとなっています。CodeMeter Certificate Vault には、CodeMeter テクノロジーが使われており、これにより、CodeMeter ドングルや ASIC の使用、ソフトウェアまたはマシン機能のライセンシング、CodeMeter AxProtector によるソフトウェア内の IP（知的財産）保護などが可能です。

CodeMeter Certificate Vault のユースケース

ユースケース 1：ユーザー認証

サービスエンジニアは、適切な証明書の提示により身元を証明することで、デバイスへのアクセス権を得ることができます。この証明書とそれに付随する鍵は、CodeMeter 用 USB ドングルである CmStick または同様のコンテナに保存することができます。このソリューションは、例えば、ATM サービスを担う技術者に適しています。高水準の安全性が求められ、すべての手順を記録すべき作業であるため、訓練を積んだ公認の技術者のみがこの作業に適任とされます。

ユースケース 2：セキュアな通信のためのマシン認証

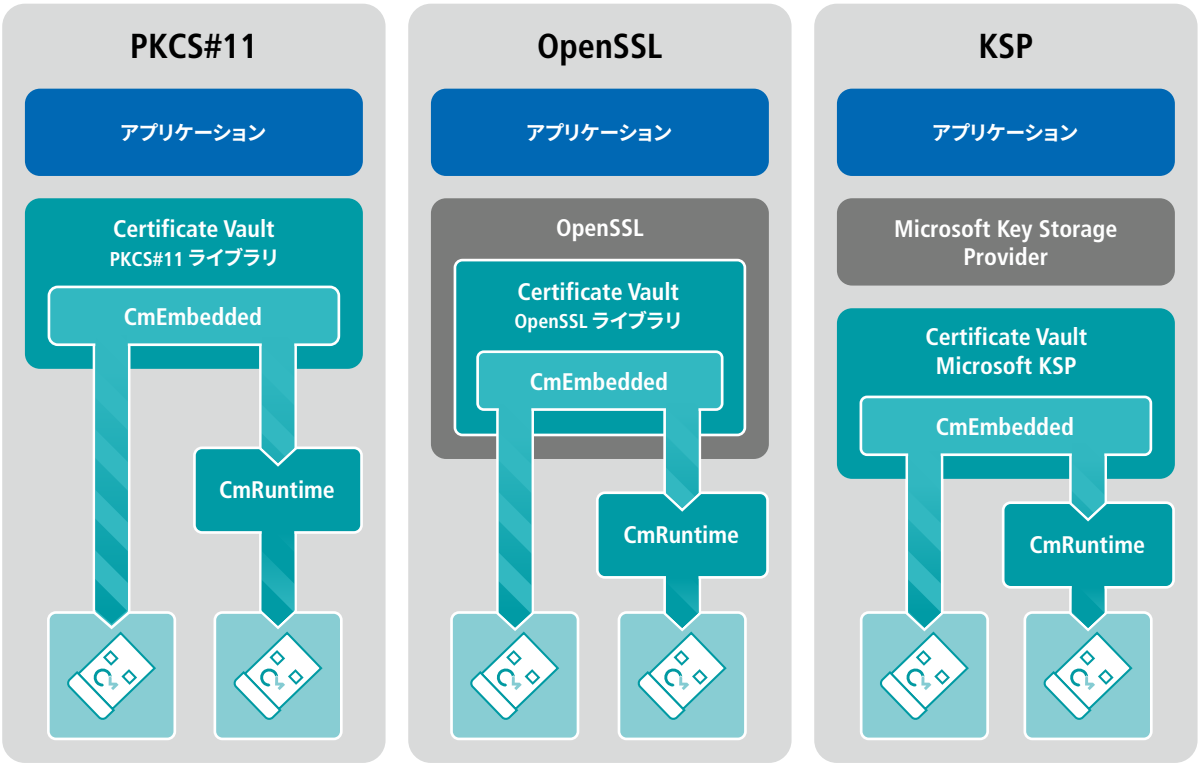
特定のデバイスにバインドされた証明書が必要となります。CodeMeter のドングルの一種である ASIC を使用し、そのセキュリティチップをデバイスの内部に永続的に組み込むことが理想的です。また、特定のハードウェアエンティティがネットワーク内で一意に識別でき、セキュアに通信できる必要があります。例えば、OPC UA のような標準プロトコルを介した、より大規模なインダストリアルネットワークの一部となっている PLC やスマートセンサーが例として挙げられます。このプロトコルは、OpenSSL フレームワークを使用して X.509 証明書を処理し、ネットワーク内の通信を保護します。この設定プロセスにおいて、CodeMeter Certificate Vault は、証明書のセキュアな保管場所と秘密鍵による暗号化処理のためのセキュアなエンジンを提供する役割を担います。

ユースケース 3：PKI の作成

VPN 接続、メール署名、またはプロセス文書における真正性の証明として使用する証明書を作成・署名する場合、署名者の秘密鍵の保護が不可欠となります。このように、本ユースケースは特に機密性の高さが求められます。

CodeMeter Certificate Vault のテクノロジー

CodeMeter CertificateVault は、標準 API を介して既存の環境へ簡単に統合することができます。特に、専用ライブラリをインターフェイスとして利用することで、より統合が容易になります。必要なのは、証明書と鍵が組み込まれた CmDongle のみです。ドングルとの通信に必要なコンポーネントもすでに含まれているため、ライブラリは、目的に沿って統合された CodeMeter Embedded スタックへのアクセス、あるいは統合されたランタイムブリッジを用いた、ローカル CodeMeter Runtime へのアクセスが可能です。



標準インターフェイス

インターフェイスは、通常、セキュアな通信を実現するために使用され、CodeMeter Certificate Vault とセキュアな証明書・鍵の処理との橋渡しを行います。

以下 3 つのインターフェイスは、それぞれ個別に、または組み合わせて使用することができます。

PKCS#11 ライブラリ

PKCS は、RSA Security 社によって開発・公開された暗号化規格群です。特に RSA アルゴリズムは、1990 年代から非対称暗化方式として使用され、最も普及しています。また、CodeMeter Certificate Vault で使用される X.509 証明書の基盤となっています。
PKCS#11（別名：Cryptoki）は、HSM やスマートカードのような暗号トークン（コンポーネント）のために用意された API に関連するものです。API は、暗号化オブジェクト（例：デジタルキー、X.509 証明書）と、それらオブジェクトによる暗号化処理の両方を定義・実装します。

PKCS#11 は、プラットフォーム間で動作し、暗号化コンポーネントの特定の細部からアプリケーションコードを完全に分離させます。そして、PKCS#11 の機能を利用するには、このコードを使用し、コマンド LoadLibrary() で CodeMeter Certificate Vault PKCS#11 ライブラリをアプリケーションにロードするだけです。

OpenSSL ライブラリ

OpenSSL は、オリジナルの SSL (Secure Sockets Layer) であり、TLS (Transport Layer Security) のために動作し、ネットワークプロトコル、一連の暗号化手段、および証明書の要求・作成・管理を行うコマンドラインツールを提供しています。OpenSSL 標準ライブラリは、暗号化と復号を可能にする一般的な暗号化機能をはじめとした、さまざまなツールを備えています。

前述した PKCS#11 は、鍵の保管場所へのインターフェイスとしてのみ機能する一方、OpenSSL は、より強力なアプリケーションとして、https、OPC UA、MQTT などのネットワークプロトコルやアプリケーションのトランスポートを暗号化することができます。

OpenSSL は、署名要求以降のプロセス全体を処理する CA として機能することもできます。

しかしながら、OpenSSL は、鍵や証明書の管理ソリューションではありません。証明書と鍵は、通常、ファイルシステム上に保管されるため、攻撃者の標的となる可能性が高くなります。但し、CodeMeter Certificate Vault から OpenSSL を起動することで、鍵と証明書の保管は全てドングルのセキュアな環境で処理することができます。

Microsoft Windows KSP

Microsoft Key Storage Provider (KSP) は、Windows アプリケーションの代わりに証明書と鍵を管理するデータベースです。鍵は単独で使用することができます。つまり、CodeMeter Certificate Vault が証明書を KSP に保管しつつ、秘密鍵をドングルに残し、すべての処理をドングル内で実行できます。KSP と CodeMeter Certificate Vault は、必要に応じて連動することで、これらの処理をリダイレクトします。

プラットフォームと設計

PKCS#11 ライブラリは、Linux、Microsoft Windows、macOS で、OpenSSL ライブラリは、Linux、Microsoft Windows で利用可能です（x86 と ARM の32/64 ビットシステムで作動）。KSP ライブラリは、Microsoft Windows のみで利用可能です。

CodeMeter Certificate Vault は、シングルライブラリ（PKCS#11、OpenSSL、および KSP 用に個別で入手可能）で構成されています。このライブラリには、ドングルまたは ASIC 内の CodeMeter チップと通信するために必要となるすべてのコンポーネントが含まれます。

証明書は通常、署名要求と署名済み証明書を用いて、所定の手順で CmDongle へ転送されます。秘密鍵は、CmDongle 内で作成され、そのまま保存されます。但し、代わりに、一元的に生成された公開鍵と秘密鍵のペアが組み込まれた証明書を、CodeMeter の暗号化リモート更新手順を使用して CmDongle にロードすることも可能です。

Windows の場合、CertVaultManager は、CodeMeter Certificate Vault と KSP 間のインターフェイスを担う GUI ツールとなります。

CodeMeter Certificate Vault の特徴的な機能

証明書を扱う際の最大の課題は、必要な場所に、証明書と鍵を運ぶための手段です。

このプロセスが自動化され、ユーザーが、公開鍵と秘密鍵のペアの作成、CA による証明書への署名に一切関与しないことが理想でしょう。しかし実際、署名された証明書と鍵のペアは、ユーザーへ送られ、ユーザーが所有するファイルシステム（通常はハードドライブ）に保存されるという、より簡単な方法が好まれています。但しこのような方法では、攻撃者は、鍵を盗み、証明書にアクセスすることが容易にできてしまいます。さらに証明書がユーザーもしくは所有するデバイスにセキュアにバインドされていない場合、攻撃者は、ユーザー ID を盗み、信頼できるエンティティ（生身の人間またはデジタルデバイス）になりすますこともできてしまうのです。

以下では、IoT デバイスに証明書を付与するための適切な手段を中心に、証明書と鍵のペアをターゲットデバイスに組み込む方法（初期に導入もしくは後日にアップデートする方法）を 3 つご紹介します。

オプション 1：一般的なプロセス

一般的に受け入れられているプロセスでは、常にユーザーが所有するデバイスが起点となります。証明書がまだ手元にない、例えば、ユーザーが既存の環境に統合しようと考えている新規デバイスの場合、CodeMeter チップがランダムな秘密鍵を作成し、セキュアな保管場所に格納することで、新しい鍵のペアが作成されます。その後、秘密鍵から公開鍵が導出され、デバイスがその秘密鍵で署名された証明書を作成します。証明書には、必須の公開鍵に加え、デバイスのシリアル番号などの情報を含めることができます。そして、証明書は、証明書署名要求（CSR）の認証を受けるために CA へ送られます。この CA は、ネットワークオペレーターのデータセンターに信頼できるインスタンスとして記憶されます（CodeMeter Certificate Vault が CA 向けの鍵の保管場所として機能するコンピューター、あるいは外部 CA でも可）。続いて、リクエストを受信し、その真正性を自動または手動でチェックし、CA の秘密鍵で証明書にデジタル署名をします。最終的に、署名された証明書は転送され、ユーザーが所有するターゲットデバイスに保存されます。

証明書を更新する場合においても、同様のプロセスを経ますが、ここでは、鍵のペアの新規作成は不要です。

デバイスの秘密鍵も CA の秘密鍵も、セキュアな CodeMeter チップから取り出すことができないため、デジタル転送中の証明書は改ざんから保護されます。また、証明書をコピーできたとしても秘密鍵がないため、攻撃者にとって何のメリットもありません。

プロセス全体は、CodeMeter Certificate Vault の OpenSSL および PKCS#11 インターフェイスを介して自動化され、ユーザーのニーズに合わせてカスタマイズすることができます。



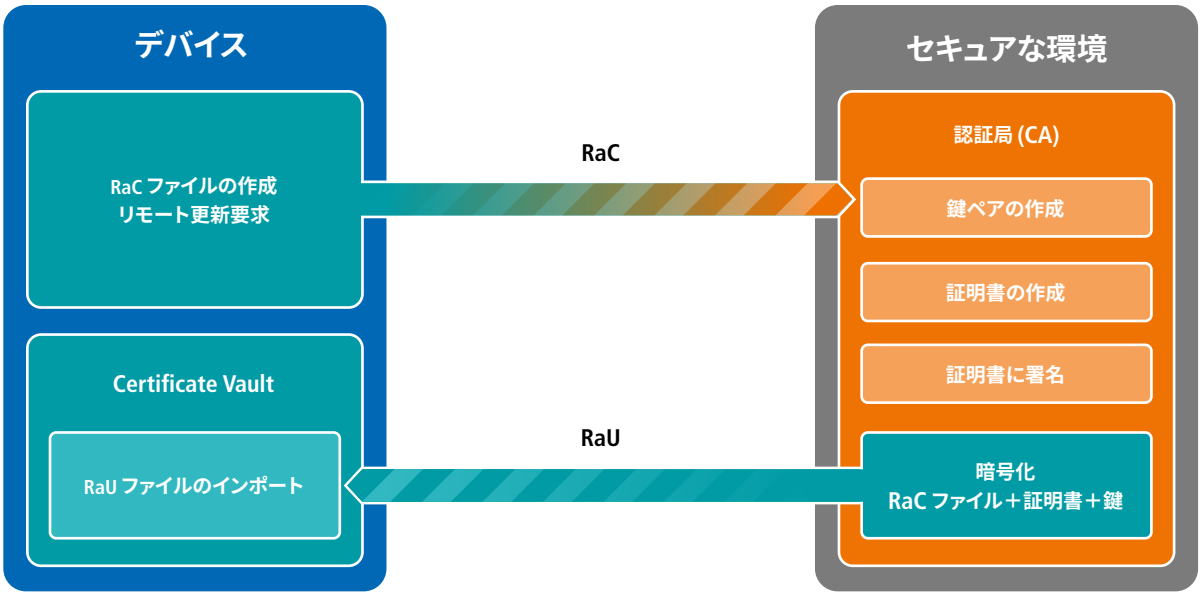
オプション 2: CA が作成・直接配布する証明書

CA が証明書と鍵のペアを作成し、それを直接 CodeMeter CertificateVault に供給できるとオプション1よりも簡単なプロセスとなります。但し、この場合、ユーザーが所有するデバイスにある秘密鍵が、セキュアなハードウェアに保管されることなく、オープンな状態で送信される瞬間があります。従って、秘密鍵は、CodeMeter Certificate Vault とセキュアな CodeMeter チップに届くまでは、盗難や不正操作に見舞われる危険性があります。つまり、このアプローチはシンプルで魅力的ではありますが、送信中やデバイスの RAM 上で攻撃者が秘密鍵を傍受できないことが保証されているセキュアな環境でしか使用すべきではありません。特に、キャッシュメカニズムやファイルシステムのゴミ箱フォルダは、脆弱な部分としてしばしば見落とされるため、注意が必要です。



オプション 3: CA が作成し、コンテナのセキュアなリモート更新ファイルによって配布される証明書

オプション 2 では、リスクについて紹介しましたが、多くの場合、証明書を一元的に作成することが正しい選択であることに変わりはありません。そこで、オプション 3 では、実行可能なソリューションを示します。本オプションでは、鍵のペアと署名証明書は、CA のセキュアな環境で作成され、同様にセキュアな CodeMeter リモート更新プロセスを通じて配布されます。このプロセスを実行するため、デバイス側では、更新要求 (CodeMeter *.RaC ファイル) を作成し、CodeMeter Certificate Vault 管理ツールを用いて、証明書と鍵のペアをリモート更新ファイル (*.RaU ファイル) として安全に保存します。このファイルは、確立された CodeMeter のリモート更新手順のもと、暗号化・署名され、ターゲットデバイスにある CodeMeter チップ内でのみ復号されます。全ての送信プロセスは、暗号化によりセキュアであり、容易に自動化も可能です。



ユーザーモードで使用する CodeMeter Certificate Vault ドングル

CodeMeter Certificate Vault は、ローカルで管理可能な数の証明書を扱う、小規模～中規模の運用に適した選択肢です。ユーザーは、Wibu-Systems によって事前にプログラムされたドングルを受け取ります。ドングルには、CodeMeter Certificate Vault のライセンスと 8 つの証明書、それに付随する鍵を保管する領域が含まれます。さらにカスタマイズ可能なパスワードが設定されており、初回起動時に変更が可能です。これにより、前述のインターフェイスを用いて、ドングル上に証明書を作成・保存することができますが、リモートプログラミング用の CodeMeter エンティティは不要です。この場合、一般的なプロセス（オプション 1）または一元的な作成・配布（オプション 2）を介した、証明書の作成・配布が可能です。

本オプションでは、一定数の証明書保管が可能であるため、CA の構築、ルート鍵のセキュアな保管に適しています。また、事前にプログラムされた CodeMeter ドングルにより、CodeMeter Certificate Vault からユーザーが所有するソフトウェア環境への統合を容易に行うことができます。

ISV（独立系ソフトウェアベンダー）モードで使用する CodeMeter Certificate Vault ドングル

本モードでは、クライアントは、オプション 1 ～3 をすべて処理するためのマスターキーとして、ファームコード（クライアント固有の鍵を含）を持つ独自のファームセキュリティボックス（FSB）を使用します。ユーザーモードとは異なり、ドングルはあらかじめプログラムされていないため、USB ドングルから SD カード、または ASIC に至るまで、あらゆるタイプのドングル（クライアントがすでに所有する CmDongle も可）を CodeMeter Certificate Vault に搭載することができます。これにより、クライアントがもつ既存のエコシステム、プロセス、PKI インフラへの容易なカスタマイズ統合だけでなく、CodeMeter のライセンシングシステムおよび CodeMeter AxProtector による保護とのシームレスな統合が可能なります。

まとめ

CodeMeter Certificate Vault は、証明書と鍵をセキュアなハードウェア内に保存できます。

CodeMeter Certificate Vault は、IT の標準規格に基づいたセキュアな証明書を使用し、CodeMeter のライセンシングとソフトウェア保護機能を補完。さらに単独での運用も可能です。

PKCS#11 インターフェイスにより、鍵の保管するデバイスとの接続に広く使用されている標準規格をサポートします。OpenSSL インターフェイスは、セキュアな通信を実現する標準実装の 1 つであり、証明書を安全に保管し、より高水準のセキュリティを提供します。

Microsoft KSP の CodeMeter Certificate Vault への接続が可能となります。

証明書と鍵は、既存の標準ルートを通じて送信可能です。要に応じて、セキュリティを保持しつつ、別のルートを選択することも可能になります。

CodeMeter Certificate Vault は、CodeMeter の機能を拡張し、セキュリティアーキテクチャーにおけるより普遍的なビルディングブロックを構築します。

用語集

略語	定義	略語	定義
OPC UA	OPC Unified Architecture –データモデルに基づく M2M (Machine to Machine) 通信向けの通信プロトコル	**CA**	Certificate Authority（認証局）
MQTT	MQ Telemetry Transport – M2M (Machine to Machine) 通信向けのシンプルなプロトコル	**TLS**	Transport Layer Security
S/MIME	Secure/Multipurpose Internet Mail Extensions – メールを暗号化するためのインターフェイス	**TPM**	Trusted Platform Module
PKCS#11	Part of the Public Key Cryptography Standards – 暗号化トークンへのアクセスに特化	**X.509**	PKI の標準規格
PKI	Public Key Infrastructure（公開鍵基盤）	**HSM**	Hardware Security Module

Wibu-Systems について

ドイツ本社



WIBU-SYSTEMS AG
Zimmerstrasse 5
76137 Karlsruhe, Germany
Telephone: +49 721 93172-0
sales@wibu.com | www.wibu.com

Wibu-Systems は 1989 年に Oliver Winzenried と Marcellus Buchheit の 2 名により創設された非公開企業で、ソフトウェアライセンシング市場における革新的なセキュリティテクノロジのグローバルリーダーです。

Wibu-Systems の包括的かつ様々な賞を受賞したソリューションはソフトウェアベンダや PC, PLC, 組込, モバイル,クラウド環境の形態でアプリケーションが提供されているインテリジェント機器メーカに対してデジタルアセットやノウハウの保護、ライセンシング、セキュリティのためのユニークかつ国際的に特許取得済みのプロセスを提供します。

Wibu-Systems はそのモットーである “Perfection in Protection, Licensing and Security”, を基に、ソフトウェアメーカやインテリジェントデバイスメーカの知的財産を非合法/不正利用、リバースエンジニアリング、タンパ攻撃、妨害/破壊工作から守り、ERP, CRM, 電子商取引プラットフォームに統合することで新しいデジタルビジネスモデルの創造に貢献します。

Wibu-Systems オフィス

WIBU-SYSTEMS 株式会社
日本
+81 45 565 9710
info@wibu.jp

WIBU-SYSTEMS USA, Inc.
米国: +1 800 6 Go Wibu
+1 425 775 6900
sales@wibu.us

WIBU-SYSTEMS (Shanghai) Co., Ltd.
上海: +86 21 5566 1790
北京: +86 10 8296 1560/61
info@wibu.com.cn

WIBU-SYSTEMS BV/NV
オランダ: +31 74 750 14 95
ベルギー: +32 2 808 6739
sales@wibu.systems

WIBU-SYSTEMS LTD
英国 | アイルランド
+44 20 314 747 27
sales@wibu.systems

WIBU-SYSTEMS SARL
フランス
+33 1 86 26 61 29
sales@wibu.systems

WIBU-SYSTEMS
スペイン | ポルトガル
+34 91 123 0762
sales@wibu.systems

WIBU-SYSTEMS
北欧 | バルト諸国
+46 8 5250 7048
sales@wibu.systems

Wibu-Systems は、プログラムまたはこのドキュメントを事前の通知なしに変更する権利を明示的に留保します。

© 2023 WIBU-SYSTEMS AG – Blurry Box®, CmReady®, CodeMeter®, SmartBind®, SmartShelter®, および Wibu-Systems® は、WIBU-SYSTEMS AG の登録票商標です。このドキュメントで使用されているその他すべてのブランド名および製品名は、それぞれの所有者の商号、サービスマーク、商標、または登録商標です。

5062-023-07 / 2023-09-29

Cover: istock.com/BrianAJackson