より強固な成りすまし対策を実現するICカードソリューション“TrustSigner認証拡張セット”

IC-card Solution Software "TrustSigner for Authentication Package"

最近，金融機関などで不正送金の事件が多発しており，その対策に苦慮している。攻撃者は，利用者の端末にマルウェアを感染させた上で，金融機関の認証情報を取得し，不正送金を行う。IDパスワード認証ではセキュリティレベルが低いため，不正アクセスによって損害額が甚大になる金融機関等のシステムではPKI(Public Key Infrastructure)を採用し，証明書による個人認証を行うことによってセキュリティレベルを高めている。しかし，多くのシステムでは利用者端末上に秘密鍵を含む証明書を保管しているため，マルウェアに感染した場合には，不正送金を防ぐことが難しい。

その対策として，秘密鍵は利用者端末上ではなくICカード等の媒体に保管し，端末利用時にはその媒体を持っていなければ認証できないようにして，セキュリティレベルを更に高めておくことが重要である。これは2要素認証技術と呼ばれ，ICカードに設定したPIN(Personal Information Number)を知っていることと，ICカードそのものを持っていることの2つの要素がそろわなければ正しい認証ができないという仕組みである。

三菱電子署名ソフトウェア“MistyGuard＜TrustSigner＞認証拡張セット”(以下“TrustSigner認証拡張セット”という。)は，ICカードに格納された電子証明書を活用し，SSL(Secure Socket Layer)クライアント認証を実現するクライアントソフトウェアで，利用者による簡単な操作でICカード内に秘密鍵を含む電子証明書を格納し，認証情報の不正取得防止を実現する。このソフトウェアは，次の特長を持っている。

(1) CSR(Certificate Signing Request)による証明書発行をサポート

(2) PKCS(Public-Key Cryptography Standards)＃12形式の証明書のインポートをサポート

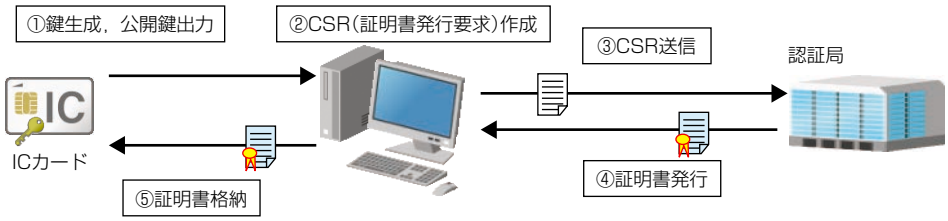
(3) ICカードの再利用が可能

CSRによる証明書発行では，秘密鍵がICカード内に生成されるため，外部に漏れることがない。また，ICカードには複数の証明書を格納することができるため，証明書を更新する際に古い証明書と新しい証明書を同じICカードに格納することができる。さらに，PIN情報の入力誤り等でICカードがロックされた場合でもフォーマッタによって初期化することが可能であり，証明書更新時やロック時にICカードを再発行することなく利用でき，利便性が高いものとなっている。また，システム側の改修もCSP(Cryptography Service Provider)名称とタイプ情報の変更だけで容易に対応することが可能である。

セキュリティの向上が今後ますます要求され，ICカード等を使った2要素認証のニーズが更に増えてくるものと想定される。その中で，TrustSigner認証拡張セットは重要な役割を果たす製品である。

TrustSigner認証拡張セットの機能

機能名	機能
CSP機能	ICカードを利用したSSLクライアント認証を行うオンライン発行に対応してブラウザ経由でICカードに証明書を書き込む。
ICカード パスワード変更ツール	ICカードに設定されたPIN(パスワード)を変更する。
ICカードフォーマッタ	ICカードの初期化(フォーマット)を行う。
ICカードリーダライタ 選択ツール	インストールされているICカードリーダライタの中から使用するICカードリーダライタに対応したドライバを選択する。
ICカード 証明書管理ツール	ICカードに格納されている証明書情報の確認，削除，PKCS#12形式証明書の追加登録を行う。
TrustSigner 認証拡張セットVersion	インストールされているTrustSigner認証拡張セットのバージョンと適用されたパッチを確認する。
Windows(注) 証明書ストア登録ツール	ICカード中の証明書情報を表示し，証明書をWindows証明書ストアへ登録する。 ※SSLクライアント認証で利用するために必要



TrustSigner認証拡張セットによる証明書管理機能

＜取り扱い：三菱電機インフォメーションシステムズ㈱ TEL：03-5445-7319＞

情報セキュリティを支える認証局構築パッケージ“CERTMANAGER”

Implementation Package "CERTMANAGER" for Certificate Authority System

インターネット上のデータの送受信におけるデータの暗号化や送受信者の相互認証は，セキュリティ上重要なファクタである。PKI(Public Key Infrastructure)は，インターネット上の暗号技術として極めて重要な基盤で，一般的なものとして使用されている。PKIを使った電子証明書は，利用者の公開鍵を使用して相手の正当性を確認をすることができるため，利用者は，お互いに電子証明書を交換し，メール等の通信文を暗号化することが可能となっている。また，電子署名法では，電子証明書を使った電子署名が手書きの署名や押印と同等に扱われることが規定されているため，普及が進んでいる状況にある。電子証明書は認証局と呼ばれる第三者機関から発行され，その認証局を信用することによって成り立つ。そのため，電子証明書を発行する認証局は，十分なセキュリティを確保して確たる信頼性を持った機関であることが必要である。

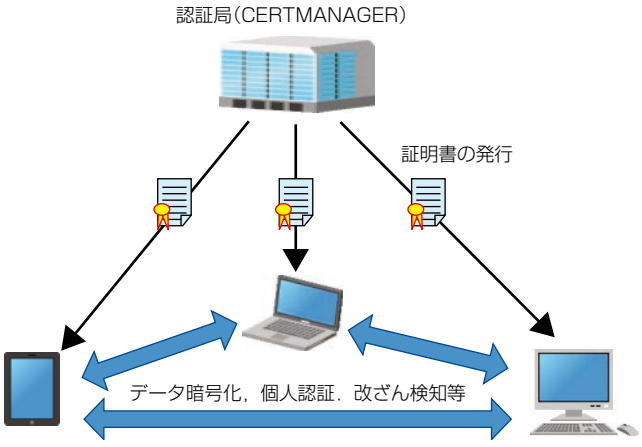
“MistyGuard＜CERTMANAGER＞”(以下“CERTMANAGER”という。)は，十分なセキュリティを確保した認証局を構築するためのパッケージ製品である。

CERTMANAGERは2006年に“セキュリティ設計仕様書”が，情報セキュリティの国際標準規格“ISO／IEC15408情報技術セキュリティ評価基準”に適合しているとの確認を独立行政法人情報処理推進機構から受けた。また，国が定める特定認証業務の認定を受けた業者にも採用されており，官公庁，認証サービス事業者，医療機関など多数の導入実績がある。

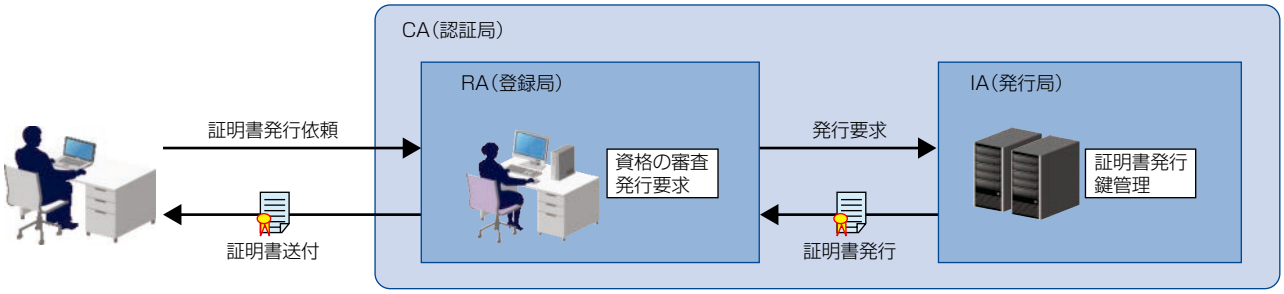
認証局はCA(Certificate Authority)と呼ばれ，電子証明書申請者の本人性を審査・確認し，主として登録業務を行う機関であるRA(Registory Authority)と，証明書を発行する機関であるIA(Issuing Authority)とで構成される。RAが複数あったりRAとIAが統合されたりとシステム構成が異なってくるが，CERTMANAGERでは１つのハードウェア内にIAとRAを組み込む等，柔軟な対応が可能である。

CERTMANAGERで発行する証明書は国際標準ITU-X.509に準拠しており，PKCS(Public-Key Cryptography Standards)＃12と呼ばれるファイル形式のものからICカードへの一括発行等，様々なニーズに対応した発行方法を用意している。安全面では，最も重要となる認証局の秘密鍵はHSM(Hardware Security Module)と呼ばれる専用ハードウェアに保管され，鍵を厳重に保護している。さらに，当社が考案した共通鍵暗号アルゴリズム“MISTY”に基づいた暗号ライブラリを利用し，安全かつ高速な処理を実現している。

三菱電機インフォメーションシステムズ㈱(MDIS)は，CERTMANAGERから発行された電子証明書を使って署名や検証を行う数多くの製品群を提供し，電子証明書の発行から電子署名を使ったソリューションまで幅広い対応を実現している。



CERTMANAGER



認証局でのRAとIAの役割

＜取り扱い：三菱電機インフォメーションシステムズ㈱ TEL：03－5445－7319＞