



広範囲な用途をサポートする認証サーバは、共通アプリケーションとして即時利用が可能で、強力な認証モジュールを提供しており、異なった認証メカニズムを容易に統合的に、統合することが可能になります。独創的でエンドツーエンドなトークン・ライフサイクル・マネジメント・モジュールはトークン・ロジスティック・マネジメントを大幅に効率化します。

資格証明情報とデータの保護のためのエンドツーエンド暗号化 (E2EE)

AccessMatrix UAS E2EEモジュールは資格証明情報とデータの盗難を効果的に保護する、ソフトウェアと改ざん防止機能搭載のハードウェア・セキュリティ・モジュール(HSM)を統合的にサポートします。これらが提供しているエンドツーエンドのセキュリティは、クライアントのウェブ・ブラウザから入力されるクレジットカード番号や暗証番号、パスワードのような機密情報を保護するよう設計されています。結果的に、エントリーポイントから最終比較ポイントまで機密情報を暗号化することができます。静的なログインID/暗証番号はユーザのオンライン識別を確認する共通認証の一つです。顧客の暗証番号情報の保護は、ユーザのパスワードや暗証番号の生成、割り当て、変更、リセットの際においてエンドツーエンドの保護を保証するために、銀行やオンラインショップ、アプリケーションプロバイダなどのサービスプロバイダにとって、トピックの重要な一つとなりつつあります。これはまた、特にシステム管理者のような内部関係者が暗証番号情報を盗む、または被害者のアカウント情報にアクセスし情報を入手できるように顧客パスワード内容を変更するといった脅威から保護します。

AccessMatrix UASの提供するE2E暗号モジュールの利点

- ・暗証番号を生成する信頼性のある、ウェブサーバのような中間階層を含んだハードウェア以外での**100%の保証の提供**。誰も知ることのできないユーザパスワード/暗証番号の提供。
- ・機密情報の**漏えい防止**及び重要オンラインビジネストランザクション送信時のトランザクションデータに対する機密性と整合性の維持
- ・リプレイアタックを使用したハッカーからの**セキュリティアタック回避**
- ・強力な認証メソッドやユーザを主体としたアクティビティラッキングのサポートによる拡張性の高い認証及び監査ポリシーなどの**セキュリティ拡張**
- ・強固な実績を持つセキュリティソリューションの配布によって実現される導入コストとプロジェクトリスクの削減による**ROIの最大化**
- ・強力なレポート能力による**コンプライアンスの保証**

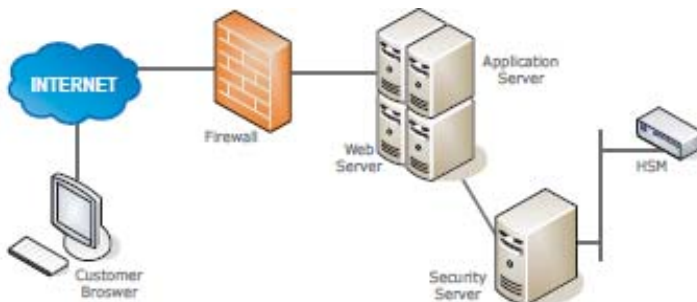
“金融管理局は、ウェブサーバと金融機関のシステム基盤のインターナルシステム間で送信される間、機密情報データは暗号化されることを期待しています。金融機関のシステム基盤の場合は、データ処理に対し、顧客デバイスと機関内部システム間のすべての通信路でデータを暗号化できるよう、高機密情報(たとえば顧客のパスワードなど)の伝送の際に強力に“エンドツーエンド”で暗号化することを考えるべきです。たとえ、金融機関のシステム基盤のウェブサーバもしくは内部ネットワークが侵入されたとしても、高機密データが危険にさらされないことを保障する助けとなるでしょう。”と香港金融管理局は述べています。

インターネットベースアプリケーションのビジネス及び技術課題

ビジネスがますますオンラインへと移り変わっていくにつれて、セキュリティの必要性が高まっています。特にインターネットは企業が製品とサービスの範囲拡張とともに新しいマーケットへと到達する為の主たる機会を提供します。しかしながらインターネットのアクセス容易性と発展性はまた利益とリスクの両方をもたらすのです。ウェブの存在はセキュリティ上の課題によって脅かされています。監査証跡やデータの機密性、法規制の順守を保障する一方、オンラインサービスプロバイダは取引を行うための流通チャネルを安全かつセキュアに保つ保証をせねばなりません。今日、インターネットベースアプリケーションは顧客の暗証番号や他の機密データの漏洩の可能性を防ぐために、ウェブブラウザとウェブサーバ間に Secure Socket Layer (SSL) といったシンプルなセキュリティ手法を採用しています。しかしながら標準的SSL技術はインターネット自体による攻撃要因から保護することができるだけなのです。データがウェブサーバに届くとき、データは自動的に平文フォームに変換されます。故にデータは攻撃に対してオープンになってしまっているのです。この情報漏洩の可能性への対処として、多くの企業や政府の管理機関はデータが入ってきた時点から最終的に有効化されるまで、またはアプリケーションによって使用されるまで機密情報が保護され続けることを保証するエンドツーエンドな暗号化ソリューションを推奨しています。

“顧客の暗証番号と他の機密データに関する暗号化セキュリティは可能な限りエンドツーエンドで保護されなければならない。これはデータが入ってきた時点から、複合化と認証が行われる最終的なシステムの到着点まで、暗号化プロセスが全く損なわれないことがないことを意味している。”

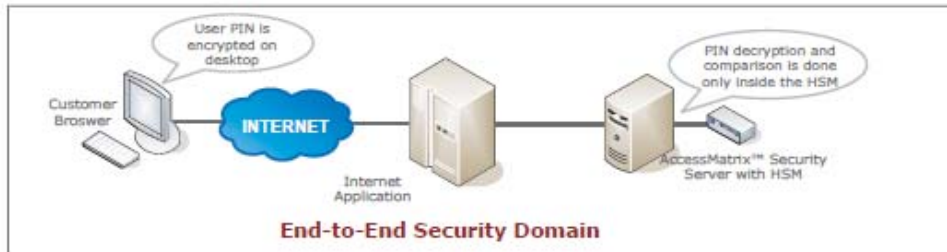
シンガポール金融管理庁インターネットバンキング技術危機管理ガイドライン
Version 3.0, June 2008



AccessMatrix UAS E2EEは、SSL複合化プロセスによって“平文”とされてしまったり、セキュア通信の盗聴やウェブサーバのなりすましによって機密データを悪用されるようなセキュリティ脅威に対して厳密に対処しています。

E2EE概要

E2EEはクライアントアクセスデバイスとハードウェアセキュリティモジュール間でセキュアなチャネルを作ります。このチャネル内においてクライアントアクセスデバイスでパスワードは暗号化され、AccessMatrixセキュリティサーバによって認証プロセスは管理されます。パスワードは組織の中の物理的にセキュアに配置されたHSMによって、照合のために複合されるだけです。その際、パスワードと他の機密データ、ましては組織のアプリケーションやサーバにさえ決して危険にさらされることはありません。AccessMatrixセキュリティサーバとHSMは保証された不正利用防止を提供する為の統合的ソリューションとして機能します。



E2EEのパスワード保護はどのように機能するのか？

- i. ユーザがインターネットバンキングサービスなどのサービスプロバイダのページへログインした際、アプレットはクライアントブラウザからログイン情報やその他の機密情報暗号化の為に公開鍵とともにダウンロードされます。
- ii. ユーザIDと暗証番号情報内のユーザキーを、アプレットが公開鍵で暗号化し、サーバへの登録処理を行います。
- iii. 暗号化情報がサーバに到達すると、サーバはユーザから受信した暗号化情報と、セキュリティサーバ内のデータベースにある対応する暗号化された暗証番号を、照合検証の為にHSMへ渡します。複合化と暗証番号の照合はセキュアなHSMデバイスの不正利用防止された環境内でのみ実施されます。そうして資格証明情報はユーザ入力直後、システム中で完全に暗号化されたままで保たれます。
- iv. こうして一度検証されHSMからの応答がOKなら、システムに対しユーザは認証に成功したことになり、その後ユーザは割り当てられた機能を実行する為に利用開始可能となります。

製品の特長

AccessMatrix UASを含むあらかじめ統合され、テストされたE2EEソリューションとFIPSに適合したHSMデバイスは統合に対する手間を削減し、セキュリティアプリケーションに対しパスワードを保護するE2Eの導入を短期間で行います。これはE2Eの保護要件に対し、以下のような特長を持っています。

- i. アプリケーション統合の為にセキュリティサービスAPIの使いやすさ、及びHSM統合の煩雑性を排除。
- ii. きめ細かい管理者委任とユーザ管理を実現する拡張性の高い管理モジュールの提供。
- iii. アクセス活動とセキュリティ違反を記録するユーザ中心のレポート機能を有する包括的な監査とレポートモジュール。
- iv. ユーザのブラウザ上での資格証明暗号に対するソリューションの導入容易性。
- v. 主なHSMデバイスのブランドに対する実績あるHSMインターフェイスの提供。
- vi. メールを統合しメールの印刷を保護するPINメーラーインターフェイスのカスタマイズ性。
- vii. パスワード履歴やパスワードの無変更パスワード品質チェックなどのきめ細やかなパスワードポリシーの提供
- viii. 証明書やハードウェアOTPトークン、スマートカード、生体デバイスなどの認証メカニズムを含む認証モジュールの拡張性。
- ix. 厳しいサービスレベルの確保及び大規模な運用要件を満たす拡張性と信頼性を兼ね備えた機能の提供。

AccessMatrix UAM TECHNICAL ARCHITECTURE

AccessMatrixサーバ

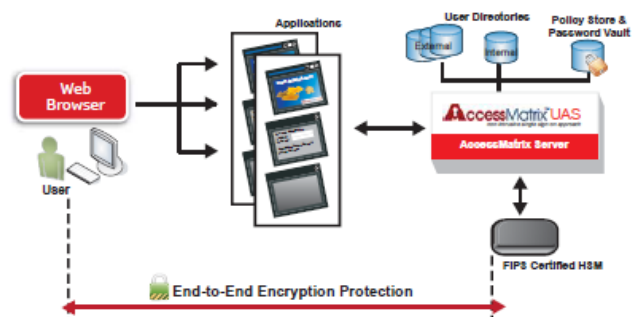
AccessMatrixサーバはポリシー、ユーザアプリケーション、ユーザ権限、ユーザ情報保持や管理の委任などに対する管理と実施機能を担います。また、AccessMatrixサーバは集中型の、認証、セッション管理、監査ログ、コンプライアンスレポート機能を有します。

- ・サーバOSプラットフォーム: Microsoft Server 2003/2008, IBM AIX/zLinux, Sun Solaris, HP-UX, Linux
- ・Java Runtime: JRE1.5以上
- ・アプリケーションサーバ: Oracle BEA Appl Server, IBM Websphere and Apache Tomcat

外部ユーザ情報

AccessMatrix Serverは、データ重複やデータ同期化を避けるためにユーザストアがある外部のユーザレジストリとのネイティブ統合を実現します。

サポートレポジトリ: Active Directory, Open LDAP, IBM LDAPやJDBC互換データベース



ポリシーストア

全てのポリシーやユーザ、アプリケーション、ユーザアプリケーション権限のセントラルレポジトリ。ユーザの証明書情報は暗号化されています。

・サポートデータベース: Microsoft SQLServer, Oracle RDBMS, IBM DB2 and Sun MySQL

FIPSに適合したHSM

セーフネット: Protect Host Server EFT HSM, Luna SP HSM