



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一的に、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。

Out of Band -One Time Password for Strong Authentication and Atuthorization

AccessMatrix UASのアウトオブバンド(OOB)ワンタイムパスワードモジュールは二分割された認証チャネルを使ってセキュアな認証ソリューションを提供します。このOOB OTPソリューションはGSMショートメッセージサービス(SMS)やユーザがアプリケーションとやりとりを行うチャネルとは異なったe-mailやその他どんなメッセージ送信メカニズムをも経由してユーザにワンタイムパスワードを提供します。ユーザがウェブサイトにアクセスする際、OTPはユーザによって決められたSMSやe-mailを経由してユーザ自身のモバイル電話に送られます。そうすることによって、ユーザとパスワードを横取りするために、本物同様に見える二つのウェブサイトにアクセスさせるトリック攻撃であるフィッシング攻撃を防ぐ助けになります。AxMxUAS-OOB OTPモジュールのアーキテクチャは特許取得済みのAccessMatrixテクノロジーをベースにしています。モバイルデバイスはいまや既存のIDやパスワード認証や認証プロセスを強化するワンタイムパスワードを受け取るセキュリティトークンとなり得ます。OTPの生成には有効期限切れの仕組みを定義することができ、複雑性(長さフォーマットの)は組織のセキュリティポリシーにのっとって定義されます。

AccessMatrix UAS-OOB OTP エンドツーエンドなOTPライフサイクルマネジメント

- **OTPコンフィグレーション**
管理者はwebベースのアドミンコンソールを通じてOTPポリシーを定義することができます。
 ・有効期限
 ・OTPの長さ
 ・OTPフォーマット(数字、アルファベット、英数字)
 ・送信メッセージテンプレート
 ・チャンネル送信
 ・ワンタイムユーザvsマルチユーザ
 ・退職者への制限
- **OTPの生成**
APIコールのパラメータを通じてOTPを生成する為のパラメータを決定することができます。
- **OTPデリバリー**
管理者はSMSメールまたはサポートされたあらゆる方式を通じたOTPに対する送信メソッドを指定することができます。
- **OTP検証**
開発者はOTP情報の検証を行うAPIを利用することができます。
- **監査証跡**

AccessMatrixUAS OOB OTPモジュールはOTP使用を追跡し、監査要件に対処するために、改ざん防止機能のついた詳細な監査履歴情報を提供します。更に管理者権限ユーザまたは一般ユーザのセキュリティ違反を監査することのできる柔軟性のあるレポート機能を持っています。

AccessMatrix UASの提供する OOB OTPモジュールの利点

- AccessMatrixUASの柔軟な統合フレームワークときめ細やかなセキュリティポリシーを通じた強力なOTP認証ソリューションの**導入容易性**
- フィッシング攻撃を軽減するOOB認証による**セキュリティ拡張**
- OTP生成と照合オプションを提供する**HSMハードウェアの活用**
- 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**
- ユーザアクティビティやセキュリティ違反をレポートする強力なレポート機能による**コンプライアンスの保証**

製品の特長

• 柔軟性の高い統合フレームワーク

AccessMatrixUAS OOB OTPモジュールは早期にアプリケーション統合や導入を実現するシンプルAPIを提供します。USMIはパスワード、認証方法、時間、およびアクセス制限を管理するエンタプライズワイドなセキュリティポリシーを自動的に実行するファイシリティを提供しています。

• ビルトインRadiusサーバ

AccessMatrixUAS OOB OTPモジュールはファイヤーウォール、ネットワークデバイス、VPNサーバまたはRadius認証プロトコルをサポートするどんなサーバプラットフォームやあらゆるアプリケーションに対して強力な認証方式を提供するRADIUSをサポートするため、Radiusサーバをビルトインしています。

• 外部ユーザストアとのネイティブ統合

AccessMarixセキュリティサーバはLDAPプロトコルやJDBCを通じた外部ユーザ情報ストアとしてLDAPやActive Directoryのような多くのユーザレジストリをサポートします。これはユーザ情報との同期処理を必要とせずにAccessMatrixセキュリティサーバと既存ユーザレジストリとの統合を可能にします。AccessMatrixセキュリティサーバは統合に対する作業を簡素化することができるよう、外部ユーザ情報にアクセスすることができます。スキーマの変更は必要ありませんし、外部ユーザ情報に情報を書き込む必要もありません。

・キー管理及び暗号プロセスを実現する実績あるHSMインターフェイス

AccessMatrixUASは、十分な説明責任をもった企業内のコンピューティングリソースに対して、マスターキーを保護し、最適な暗号化プロセスパフォーマンスを陣つ原子、HSM内でOTP生成と照合のカスタムロジックをサポートするHSMデバイスとの統合を実現します。

・拡張性と可用性

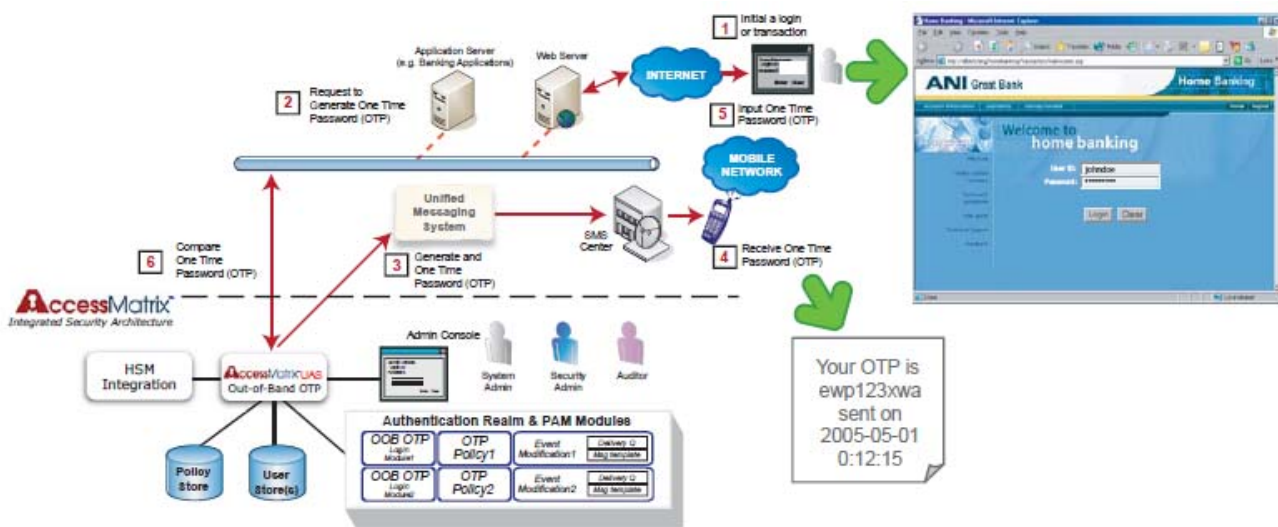
AccessMatrixUASは大規模な展開に対して、厳しいサービスレベルの維持と引用要件を満たす実績ある拡張性と信頼性を提供します。

・特許取得技術-管理と委任を実現する階層モデル

AccessMatrixUASは、十分な説明責任を担った企業内のコンピューティングリソースに対するユーザアクセスを管理する為の全ての組織構造レベルにおいてセキュリティ管理者を任命することを可能にします。

AccessMatrix UAS-OOB OTP概要

ログイン要求や認証トランザクション要求が発生すると、ランダムワンタイムパスワード(OTP)はAccessMatrixセキュリティサーバによって生成され、OTPはトランザクションを開始した顧客のモバイルデバイスに送信されます。



ユーザはモバイルデバイスからトランザクションを完了するためにユーザからの入力を持っているウェブページへOTP認証コードを入力します。ユーザがサーバにOTP情報を登録すると、AccessMatrixセキュリティサーバは生成されたOTPとユーザによって入力されたOTPの情報を比較することでOTP情報を検証します。OTPが合致したらトランザクションは完了し、監査証跡情報がロギングされます。もしOTP情報が合致しなかった場合、ユーザはOTPの再入力を要求されます。事前に定義された失敗可能トライ回数を超えるとトランザクションはキャンセルされ、イベントはロギングされます。

AccessMatrix UAS OOB OTP TECHNICAL ARCHITECTURE

AccessMatrixサーバ

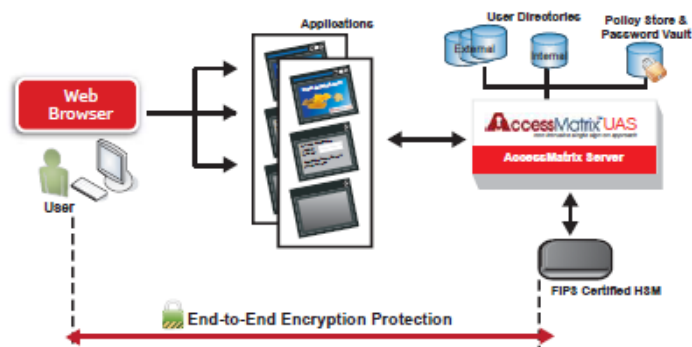
AccessMatrixサーバはポリシー、ユーザアプリケーション、ユーザ権限、ユーザ情報保持や管理の委任などに対する管理と実施機能を担います。また、AccessMatrixサーバは集中型の、認証、セッション管理、監査ログ、コンプライアンスレポート機能を有します。

- ・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情報がある外部のユーザ登録情報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使用権限のセントラルレポジトリと、ユーザ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

AccessMatrix UASはsafenet,nCipher,IBM,UtimacoなどメジャーなHSMベンダ製品と統合実績があります。