



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。

Vasco DigiPass Token Authentication And Token Management Module

AccessMatrix™ Universal Authentication Server (UAS)は、二要素認証(2FA)ソリューションに対するビジネス要件に適応するようVasco DigiPassトークンの迅速な展開を可能にします。事前に統合および検証済みの2FAソリューションは統合に要する手間を低減し、インターネットバンキングアプリケーションやセキュアなリモートアクセスを実現するエクストラネットアプリケーションをはじめ、セキュリティに厳しいアプリケーションに対応したVasco DigiPassの導入・展開を最短にします。AccessMatrix UASはVascoを即時利用可能なレベルにまで統合したことによって、Vasco DigiPassトークンが持つ全てのセキュリティ機能を活用することができます。AccessMatrix UASは認証(同期とチャレンジレスポンス両方)、承認、署名照合、ホストリターンコード照合などの全てのトークン機能を提供できるようVascoのVACMANNコントローラライブラリと密接に統合されています。また、日常的に重要なオペレーションであるトークンの発行やPINメーラ、トークン紛失、同期不可といったトークンロジスティックの様々な側面に適合できるよう高度なトークンマネジメント機能を提供します。

AccessMatrix UAS-VTM

エンドツーエンドトークンライフサイクル管理

- **トークンのイニシャライズとカーネルパラメータ定義**
工場でのイニシャライズまたは社内での初期化両方をサポート。Vascoカーネルパラメータの定義が可能。

- **トークンシードのインポート**
アドミンコンソールを通じたAccessMatrixUASのポリシーストアへの暗号化されたDPX(seed)のインポート

- **トークンの割り当て**
ユーザに割り当てられたトークンの情報はアプリケーション内またはAccessMatrix ポリシーストア内に保存されます。トークン割り当ては自動的または手動割り当てモードを使用し、管理者によって行われます。

- **トークンの割り当て解除/フリーズ/フリーズ解除**
トークンの状態はヘルプデスクやトークンステータスをトラックする管理者によってアドミンコンソールから、割り当て解除/フリーズ/紛失/故障へと変更することができます。

- **トークンの再同期**
トークンは時間経過によりセキュリティサーバとの同期処理が実行されないことがあります。AccessMatrixUASは自動同期機能や、ヘルプデスクによる手動同期、トークン再同期セルフサービス機能を有しています。

- **トークンのロック解除**
トークンはユーザがトークンの暗証番号を忘れていたり、トークンによって許容される暗証番号入力トライ回数を超えた場合にロックされます。(これはトークンモデルに依存します。この場合、ユーザはヘルプデスクにロック解除を要求せねばなりません代わりにウェブベースのセルフサービスファイシリティを使用しトークンのロック解除を行うことができます。

- **トークンOTP検証**
アプリケーションはAPIコールを使用したユーザが提示したOTPを検証します。レスポンスオンリー、チャレンジレスポンス、署名及びホストレスポンスコードなどをサポートしています。

- **監査証跡**
AccessMatrixUASはOTP使用を追跡し、監査要件に対処する為に改竄防止機能の付いた詳細な監査証跡情報を提供します。更に管理者とユーザのアクティビティやセキュリティバイオレーションを監査することのできる柔軟性のあるレポート機能を提供しています。

- **レポート**
AccessMatrix UASはアクセスに伴うアクティビティやセキュリティバイオレーションなどをレポートするユーザセトリックなレポート機能を提供しています。



AccessMatrix UAS Vascoトークン管理モジュールの利点

- **Vasco認証ソリューションの迅速な展開**
柔軟性の高い統合フレームワーク、きめ細やかなセキュリティポリシー及びe2eトークン管理機能。
- **拡張性のある認証サーバ機能**
PAM (Pluggable Authentication Model)を通じて多種多様な認証メソッドのサポートと新規メソッド
- **柔軟性の高いアドミニストレーションモデル**
組織構造に対応して、容易で且つ効率的にアプリケーションのパーミッションやユーザ制限、セキュリティポリシーを導入することのできる、特許
- **取得済み階層ベースの管理及び委任モデルの提供。**
- **信頼性と可用性**
信頼性、可用性、拡張性といった要件に追従する自動フェイルオーバー、ホリゾンタル及びバーティカルスケーリングの標準装備
- **HSMによるアドバンスドセキュリティ**
トークンシードやVacmanコントローラのソフトウェア
アキーをHSM内部に補完する強力な保護機能の提供。
- **ROIの最大化**
確実な実績を持つセキュリティソリューションの提供によって実現される導入コストとプロジェクト

製品機能・Vascoトークンに対するエンドツーエンド・トークン管理

AccessMatrix UAS-VTMは、トークン管理、アプリケーション統合、OTP比較、自動再同期、トークン紛失、トークン交換といったVascoトークンのライフサイクルを管理する利便性の高い手法を提供します。

・Vascoセキュリティ機能の総合的サポート

AccessMatrix UAS-VTMはVasco Vacmanコントローラとのシームレスな統合を実現し、Vascoの高度なセキュリティ機能をサポートする拡張性の高いAPIを提供します。

- ・タイム及びチャレンジベースのワンタイムパスワード生成(同期・非同期モード両方)
- ・トランザクション詳細ベースの電子署名生成
- ・二要素認証
- ・2-way手動認証((Host Verification Code)
- ・いつでもどこでも行えるポータブルユーザ認証

・Vaso DigiPassトークンの包括的サポート

AccessMatrix UASはVasco DigiPassトークンの製品ライン全てで動作することが保証されています。:ハードトークン、ソフトトークン、ウェブトークン、バーチャルトークン

・多要素認証によるユーザアイデンティティの拡張

アプリケーションはまた、アプリケーションの大幅な変更を必要とせずにスマートカード、生体デバイスなど他の認証メカニズムとの共存をサポートするAccessMatrix UASの機能を活用することができます。

・内蔵型Radiusサーバ

AccessMatrix UAS はファイアーウォール、ネットワークデバイス、VPNサーバなどRadius認証プロトコルをサポートするサーバプラットフォームや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、ビルトインされたRadiusサーバをビルトインしています。

・PINメーラーインターフェイス

PINメーラがトークン割り当てのユーザ情報とPIN情報に基づいて生成されるようにAccessMatrix UAS-VTMはPINメーラオプションを提供します。

・拡張性統合手法

AccessMatrix UAS VTMは二つの統合オプションを提供します。1つはOTPトークン認証サービス提供の為にブラックボックスとしてAccessMatrix UAS VTMを使用するものです。この統合オプションに対して手間や時間の浪費及びAccessMatrix UASに対するユーザ情報のプロビジョニングなどを必要としません。これは統合を非常に簡素化し、市場の要求に対する時間をも低減してくれるでしょう。2つ目のオプションはトークン認証やトークン管理、トークン関係の管理サービスを行うユーザに対してAccessMatrix UAS VTMを活用することです。このソリューションはあらゆるユーティリティやモジュールを使用可能にするUASシステム内にユーザ情報をプロビジョニングする必要があります。

・外部ユーザ情報とのネイティブ統合

AccessMatrixサーバは、LDAPやJDBCを通じて外部ユーザストアとして、LDAPやActiveDirectoryといった多くのユーザレジストリサービスをサポートします。この機能は、ユーザ情報の同期処理を行うことなく、AccessMatrix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の実現化を実現するため外部ユーザ情報に対しアクセスすることができます。スキーマ変更や外部ユーザ情報に対する書き込みも必要としません。

・特許取得技術-管理と委任を実現する階層モデル

AccessMatrix UASは、企業内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説明責任を維持しながら管理するため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。

・キー管理や暗号化プロセスに対する実績あるHSMインターフェイス

マスターキーを保護して、最適の暗号の処理能力を可能にするHSMデバイスによる実績ある統合だけでなく、AccessMatrix UASはトークンシードを保護する為の暗号化をサポートし、OTPの比較はHSM内部で行います。

・拡張性と可用性

AccessMatrix UASは厳しいサービスレベルと大規模なデプロイメント要件を満たすことのできる実績ある拡張性と信頼性を提供します。

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, Apache Tomcat

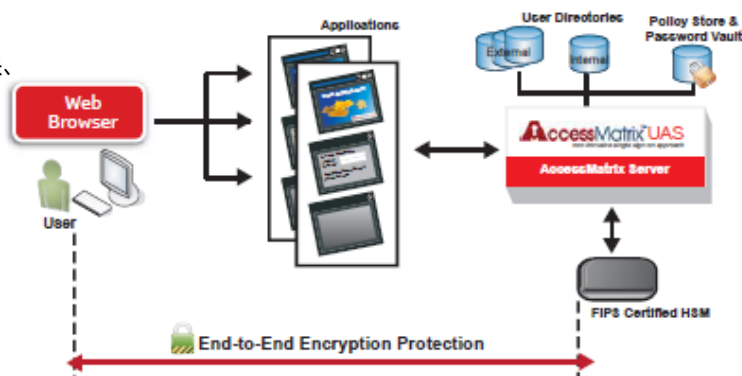
外部ユーザ情報

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

Vasco Vacmanコントローラ

Vasco DigiPassトークンとのシームレスな統合の実現と完全なトークンセキュリティ機能をサポートするためAccessMatrixサーバはVasco Vacman コントローラに組み込まれています。



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。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, 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