



RED HAT CERTIFICATE SYSTEM

PKI (公開鍵暗号基盤) 対応のセキュアで拡張性の高いシステム構築

CERTIFICATE SYSTEMとは？

Red Hat Certificate Systemでは、強力なセキュリティフレームワークによりユーザ識別情報を管理し、情報通信のプライバシーを確かなものとします。以前はNetscape Certificate Management Systemとして知られていたRed Hat Certificate Systemは、識別情報管理の主要機能に対応し、企業全体へのPKI (公開鍵暗号基盤) の導入、構築を簡素化します。

その役割とは？

Red Hat Certificate Systemは強力な認証、シングルサインオンおよびセキュアな情報通信の処理に必要なシングルおよびデュアルキーX.509v3認証の発行、更新、一時停止、取り消しなどの管理を行います。

注目する理由

Red Hat Certificate Systemを利用することで、お客様のネットワーク、アプリケーション、データデバイスそしてユーザによるセキュリティフレームワーク内の操作が可能になり、認証済みのユーザのみが適切なリソースにアクセスできるようになります。

概要

- ユーザ識別情報の管理を行うPKI (公開鍵暗号基盤) の構築および保守に関するサポート
- 公開済みのAPIを通しサードパーティのセキュリティソフトウェアおよび既存のアプリケーションと容易に一元化
- 管理者がエンドユーザとの最小限のやり取りでスマートカード上ヘリアルタイムで証明書の要求およびインストールを行うことを実現
- 無数のデジタル証明書の管理を実現
- 暗号キーのキーリカバリをサポート
- 高可用性を実現する広範囲のアーキテクチャをサポート
- 他のPKI (公開鍵暗号基盤) デプロイメントとのクロス証明書をサポート
- グローバルプラットフォーム準拠のスマートカードの使用(tokens)をサポートし、鍵管理を簡素化

強力な認証機能

パスワードとは異なり、証明書は容易に再発行することができます。信用のある発行元により発行されたデジタル署名済みの証明書が、ユーザ識別情報を検証し、識別情報の盗難を防止します。

セキュアな通信を可能に

ミッションクリティカルな情報の保護は、セキュリティを意識する企業にとって非常に重要です。Red Hat Certificate SystemはX.509v3証明書を発行し、企業がネットワークを経由して発信するクリティカルな情報と機密性の高い電子メールトラフィックの双方を暗号化します。

シングルサインオンの有効化

シングルサインオンとは、一つのパスワードで一度ログインすると、ネットワーク上に再度パスワードを送信せずにユーザがアクセス権を持つ全サーバへのアクセス権を得ることができるというものです。

シングルサインオンには、ユーザおよび管理者の両者にメリットがあります。ユーザは一度のログインで複数のリソースへアクセスすることができ、管理者にはサーバのメンテナンスが簡素化するというメリットがあります。また、パスワードの紛失に関する問い合わせが減ることにより、ヘルプデスクへの問い合わせが減少し、企業のコスト削減にもつながります。

Red Hat Certificate Systemにより発行される企業のLDAPディレクトリ上に生成されるデジタル証明書は信頼性の高いシングルサインオンをサポートします。さらに、グローバルプラットフォームに準拠したスマートカードのサポートにより、小型のスマートカード上に証明書を配布することができ、企業内のどのコンピュータからでも自動的にシングルサインオンすることが容易になります。

柔軟性のある配備

Red Hat Certificate Systemは、企業のセキュリティポリシーおよびセキュリティソリューションといった既存資産に柔軟に対応することができます。設定もインストールも容易な為、企業が様々なエクストラネットおよびイントラネットアプリケーションを利用するためにそれをカスタマイズすることも可能です。

また、サードパーティ製品との一元化を用意する機能が備わっております。(APIのカスタマイズによる認証、ポリシーモジュールの拡張)そしてIT管理者がユーザおよびグループにアクセス制御を割り当てることを可能にする認証フレームワークです。

高拡張性および高管理性

Red Hat Certificate Systemは従業員、パートナー企業、顧客間で、大規模に配布できるように設計された広範囲かつ高パフォーマンスのアーキテクチャを提供します。また管理者の権限、ログ、ユーザおよびグループ管理などに役立つ集約化されたウェブベースの管理ツールがあります。共有タスクを容易に自動化できるコマンドラインインターフェースも利用可能です。

クローン機能により、既存のアーキテクチャを維持しながら、高い可用性と拡張性を実現することができます。

セキュリティ機能の向上

Red Hat Certificate Systemは、FIPS 140 -1 レベル2の認定済みで、レベル3の認定済みハードウェアで使用可能です。ハードウェアの署名は非常に複雑なCA署名キーを保護し、容易にアクセスできるデスクトップからは隔離されます。

アプリケーションの統合

Red Hat Certificate Systemにより、ウェブベースの認証、署名、仮想プライベートネットワーク、ルータおよびS/MIMEの配置が可能になります。Red Hat Directory Serverと完全に一元化しその他のセキュリティソリューションとも容易に一元化できるため、企業の既存資産を有効活用することができます。

ソフトウェア署名

業界標準のRSAを使用した証明書の署名
(SHA-256またはSHA-512 ハッシュによるRSA署名)
署名済みの監査ログをサポート

柔軟なポリシー

階層構造の証明書の権限設定が可能
企業独自の証明書管理ポリシーに適用できるカスタマイズ可能なポリシーテンプレート
既存データベースの発行済みAPIを経由した自動のオンライン認証をサポート
その他のPKIによるクロス証明をサポートし、CAが他のCAに対し、相互認証した証明書の生成、署名を行うことが可能

管理の軽減

HTTP、HTMLおよびSSLなどのウェブプロトコルを使用してネットワーク上で証明書の要求、提供およびインストールを実行可能
証明書および証明書の取り消しリストをLDAP準拠のディレクトリサービスに配布
SSL暗号化および認証サービスを利用したネットワーク上のコンピュータからRed Hat Certificate Systemの遠隔管理が可能
Red Hat Directory Serverとの一元化を実現
その他のPKIによる相互認証をサポートし、CAが他のCAに対し相互認証した証明書の生成、署名を行うことが可能
管理者によるアクセス制御の割り当てを可能にする認証フレームワークを提供

アプリケーションの統合

ウェブ形式の署名およびS/MIMEを含め強力な認証、署名あるいは暗号化を必要とする認証ベースのアプリケーションと統合可能
認証プラグインを利用して既存のセキュリティ環境と一元化様々なブラウザ上で個人証明書を管理可能
NSSセキュリティツールキットと統合することで、カスタムアプリケーションにPKI サポートを追加可能

オープン標準のサポート

SSL準拠のクライアントおよびサーバの証明書を発行
S/MIMEを利用した証明書を発行
業界標準のX.509v3パブリックキー証明書の作成、署名および発行
暗号化、ハッシュ法および署名のためのDSAおよびRSAパブリックキーアルゴリズムをサポート
PKCS #11、CMRF (要所有の証明)およびCMCのような基準に依拠した証明書要求のサポート
クライアントおよびサーバは、オンライン証明書ステータスプロトコル(OCSP)を通じてRed Hat Certificate Systemと取り消しの確認に関する通信を行うことが可能
一定の間隔で、証明書を持つクライアントおよびサーバからダウンロード可能な証明書取り消しリスト(CRL)を発行
Certificate Systemの全アーキテクチャと一元化されたビルトイン形式のOCSPレスポンスを標準装備。これにより、クライアントとサーバはオンライン証明書ステータスプロトコル(OCSP)を通じてRed Hat Certificate Systemと取り消しの確認に関する通信を行うことが可能
グローバルプラットフォーム準拠のスマートカードをサポートし、初期登録、キーアーカイブ、PINリセットおよびキーリカバリなどのあらゆるキー管理を大幅に簡素化

拡張可能なソリューション

APIおよび認証などの機能拡張のためのカスタムプラグインの開発ツールを提供
既存のカスタムビジネスロジックおよびレガシーアプリケーションの利用が可能
ユーザID、パスワードおよびPIN情報の収集を行う登録テンプレートを提供。HTMLベースのテンプレートは、簡単にカスタマイズして他の認証モジュール向けの特定の情報の収集を実行することが可能

柔軟なアーキテクチャ

シングルおよびデュアルキー証明書の発行、更新、一時停止取り消しが可能
クライアント、サーバおよび仮想プライベートネットワーク(VPN)クライアントおよびルータなどのネットワークデバイスからの認証要求をサポート
暗号キーの長期保存のためのキーリカバリーをサポート
モジュラーシステムデザインにより、Registration Manager、Certificate Manager、Data Recovery ManagerおよびOCSP Managerを含むコンポーネントが、複数システム(クラスタ構成など)上で稼働し拡張性を向上させる登録権限をサポート
下位の証明書発行元を生成することなく証明書発行元のクローン作成を許可することで拡張性が向上
パフォーマンスを向上させるため、任意のハードウェアアクセラレーションによるSSLクライアント認証を使用し、全コンポーネント間の通信を暗号化
ブラウザまたはスマートカードへのユーザ証明書のインストールを許可
セキュリティクライアントをカスタマイズすることで、デスクトップキーの管理タスクのためのユーザーインターフェースを提供し、Registration Managerと個々のユーザ信号間の通信のためのグローバルプラットフォームプロトコルの使用を促進
セキュリティクライアントは、簡素化したインターフェースを提供するため、PINのリセットなどのデスクトップ管理タスクをサポートし、カスタマイズされた情報を利用することで完全な登録の設定が可能

サポートされるプラットフォームとシステム要件

ハードウェア	構成	OS
Sun	SPARC	Solaris9 (32bit/64bit)
Intel	Pentium	Red Hat Enterprise Linux v.3/v.4 (32bit)

必要メモリ容量：最小256MB
必要ディスク容量：最小200MB

詳しい内容につきましては、下記弊社ウェブページをご覧ください。
製品、サービス <http://www.jp.redhat.com/software/>
組込み <http://www.jp.redhat.com/embedded/>
トレーニング <http://www.jp.redhat.com/training/>
サポート <http://www.jp.redhat.com/support/>

メールでのお問い合わせ先：sales-jp@redhat.com