

Microsoft Windows Server ActiveDirectory 証明書サービスパッケージ



※写真はイメージです。

Microsoft® Windows® Server 2008ベース 自社認証局に必要な商品サービスパッケージ

社内で必要とされる証明書を手軽に発行し、Windows®スマートカードログオンやリモートデスクトップ サービスなどにおいて証明書を利用した運用が可能になります。既設AD連携*¹やUSBトークン・ICカード管理運用サポートもオプションでご提供。

▶ ActiveDirectory証明書サービスパッケージ構成

①②H/W&OS

Windows Server 2008 と最適なサーバハードウェアで構成します。

③PKIリポジトリ

PKIのリポジトリとしてWindows Server 標準搭載Active Directoryのディレクトリサービスを活用して実現します。ADを利用することで、ドメイン参加ユーザへの証明書の配布や更新運用が軽微になります。

既設ドメインサーバ(AD)から新設するプライベートCAパッケージ内PKIリポジトリにユーザ情報を反映することが可能です。

④証明書発行

Active Directory 証明書サービスを利用して、証明書の発行や更新、管理の多くを実現します。また、これらの煩雑な業務を面倒な手続きなしに運用できる自動化することも可能です。

⑤デバイス管理

Windowsスマートカードログオン証明書など、USBトークンやICカードに格納して運用したい場合に利用します。USBデバイスとの連携は、Microsoft Minidriverで連携できるデバイスを活用することでPIN変更などは管理者の手を煩わせる事無く運用可能です。

⑥導入支援サービス

認証局設計、認証局構築、環境設置などのシステム管理者でも普段聞き慣れないPKIの専門的な設計は、ペンティオにお任せください。お客様ごとに最適な構成で構築をご支援させていただきます。



▶ 発行する証明書の主な用途

- イン트라ネットサイトのSSL保護
- Windowsのスマートカード認証
- S/MIMEによる電子メール保護(社内のみ)
- ターミナルサービスやリモートデスクトップ接続のネットワークレベル認証
- 暗号化ファイルシステム
- カスタムアプリケーションのコード署名
- IPSecによる通信トラフィックの保護
- 802.1x 有線/無線LAN認証
- L2TPやSSTPによるVPNの認証



▶ Pentio USB Token / IC Card 連携のメリット

▶ デバイスで生成の証明書要求で 秘密鍵流出がないので安全

証明書をリクエストするユーザーは、USB Token / IC Card内部で生成された公開鍵を元に証明書発行(署名)要求をします。ペンティオの認証局Windowsパッケージは、証明書発行要求に対し証明書を発行し、提供します。



これにより、秘密鍵はUSB Token / IC Card内部から取り出せないで、デジタル鍵(秘密鍵)の流出を防ぐことができます。一般的な認証局で発行された証明書(PKCS#12形式)を受け取る場合は、秘密鍵の取り扱いに慎重になる必要があります。

▶ 証明書を直接デバイスに格納し、 管理者PCにも秘密鍵は残らず安全

ペンティオのActiveDirectory証明書サービスパッケージは、認証局で発行された証明書をUSB Token / IC Cardデバイスに直接格納することができます。直接格納とは、証明書を要求するユーザーが持つUSB Token / IC Cardを、ユーザーが使用するPCに接続した状態で、AD証明書サービスで発行された証明書をAD経由でデバイスに直接格納する運用のことです。この際、管理者PCやユーザーPCのハードディスクにも証明書情報が保存されない事を意味します。

▶ ICカード対応カードプリントシステム

ICカード対応カードプリントシステムSTR-300は、AD証明書サービスで発行した証明書をICカードに格納焼き込み、同時に券面印刷をするプリンタと券面デザインレイアウトソフトウェアのパッケージシステムです。



▲STR-300

⇨ 証明書発行の詳細

Active Directory 証明書サービスの概要

● 証明機関 (CA)

ルート CA と下位 CA は、証明書をユーザー、コンピューター、およびサービスに発行し、証明書の有効性を管理する際に使用されます。

● CA Web 登録

Web 登録により、Web ブラウザーから CA に接続し、証明書を要求して証明書失効リスト (CRL) を取得することができます。

● オンライン レスポンダー

オンライン レスポンダー サービスは、特定の証明書の失効状態要求を受け入れ、それらの証明書の状態を評価して、要求された証明書状態情報を含む署名付きの応答を返信します。

● ネットワーク デバイス登録サービス

ネットワーク デバイス登録サービスにより、ドメイン アカウントを持っていないルーターや他のネットワーク デバイスが証明書を取得できるようになります。

● 証明書の登録 Web サービス

証明書の登録 Web サービスを使用すると、ユーザーやコンピューターが HTTPS プロトコルを使用した証明書の登録を実行できます。証明書の登録ポリシー Web サービスと合わせて使用することで、クライアント コンピューターがドメインのメンバーでない場合や、ドメインメンバーが自身のドメインに接続していない場合に、ポリシー ベースの証明書の登録を可能にします。

● 証明書の登録ポリシー Web サービス

証明書の登録ポリシー Web サービスを使用すると、ユーザーやコンピューターが証明書の登録ポリシー情報を取得できます。証明書の登録 Web サービスと合わせて使用することで、クライアント コンピューターがドメインのメンバーでない場合や、ドメインメンバーが自身のドメインに接続していない場合に、ポリシー ベースの証明書の登録を可能にします。

● 鍵の強度

秘密鍵の作成に使用される暗号化プロバイダー、鍵長、ハッシュ関数、などは下記の中から選択することができます。

暗号化プロバイダー:

鍵長: RSA: 512、1024、2048、4096、8192、16384bits (CA公開鍵は512bita~)

DSA:

ハッシュ関数: MD2、MD4、MD5、SHA1、SHA256、SHA384、SHA512



⇨ ActiveDirectory証明書サービスパッケージ (Microsoft Windows Server 2008版) 仕様

機能部位	内容	詳細
証明書発行	証明書発行枚数	制限なし
	証明書形式	X.509 Ver3
	公開鍵方式	RSA方式
	鍵長	RSA: 512、1024、2048、4096、8192、16384bits (CA公開鍵は512bita~) DSA:
	ダイジェストアルゴリズム	MD2、MD4、MD5、SHA1、SHA256、SHA384、SHA512
	証明書配布	Webエンロール、SCEPエンロール
	証明書失効リスト	DER形式、PEM形式
	証明書失効情報伝達	OCSP、http、CRLファイル
管理機能	発行可能な証明書	クライアント証明書、コンピュータ証明書、認証局証明書
	SCEP対応	SCEP対応VPN機器やVPNクライアントソフトからオンラインで証明書を要求および取得可能
	証明書一括生成	PKCS#12形式発行
	イベント通知メール	証明書の発行や失効、有効期間切れアラートなどをメールで通知
	バックアップ/リストア	
	Web証明書トークン書込み	Webブラウザ経由でトークンに証明書を書込
トークン管理	証明書書込みツール	PCからトークンへ証明書を書込むためのツール
	トークン初期化	SO-PINの設定、PINポリシーの設定、デフォルトPINの設定
OS	ロック解除	リモートおよびローカルでロック解除
		Microsoft® Windows® Server 2008 日本語版
H/W	シャーシ	外形寸法: 42.7×447×546.1mm (高さ×幅×奥行き) 11.80kg (最大構成)

⇨ 代表的な連携ソリューション

⇨ Webサイト認証 Apache/IIS

代表的なWebサーバであるApacheとIISでのアクセス認証ができます。

⇨ 業務サーバ/グループウェア認証(SSO)

リバースプロキシ型シングルサインオン(SSO)との組み合わせで、グループウェアや複数の業務サーバへのアクセス認証を、1回の証明書(秘密鍵)認証でできるようになります。

⇨ ネットワークストレージ認証(WebDAV)

PCのブラウザからWebサーバ上のファイルやフォルダを簡単にアップロード/ダウンロードできるWebDAVで、PKI証明書によるアクセス認証を実施できます。

⇨ リモートアクセス認証 FirePassシリーズ

SSL-VPNアプライアンスとの組み合わせで、セキュアなリモートアクセスが可能になります。



⇨ 無線LAN認証 Enterpas Std

RADIUSサーバとの組み合わせで、強固で使い勝手のよい無線LAN認証基盤を構築できます。



⇨ PDF文書電子署名 Adobe® Acrobat®

PDF文書作成時にPKI証明書(秘密鍵)を用いて、デジタル署名を利用できます。



ペンティオ株式会社

[PKIソリューション事業部]

〒160-0004 東京都新宿区四谷2-4 久保ビル3F

Tel.03-5919-0971 Fax.03-5919-0980 <http://www.pentio.com/>

2010年10月