

Windows 7 と Windows Server 2008 R2で実現するPKI

マイクロソフト株式会社

GMOグローバルサイン株式会社

渡辺 清

浅野 昌和

はじめに

- ▶ Windows 7及びWindows 2008 R2は現在製品候補版(Release Candidate)段階であり、本日の情報は最終リリース時と異なる可能性があります。

アジェンダ

- ▶ 背景
- ▶ PKI 拡張
 - ▶ サーバ統合
 - ▶ 現状シナリオの改善
 - ▶ HTTP ベース Enrollment
- ▶ 強固な認証 (Strong Auth)

Windows PKI

▶ 戦略的投資

- ▶ Windows 2000, Windows XP, Windows Vista と投資し続ける

▶ 現状の機能:

- ▶ サーバ役割: CA, OCSP, SCEP
- ▶ クライアント: API, UI, クライアントサービス
- ▶ アクティブディレクトリ統合
- ▶ プロトコルやアプリケーション採用

▶ 参考情報 :

- ▶ <http://technet.microsoft.com/en-us/library/cc753254.aspx>
- ▶ <http://technet.microsoft.com/en-us/library/cc770357.aspx>

PKI トレンド

- ▶ 政府(US, Europe) – 最大証明書発行者!!!
- ▶ 中小企業はPKIソリューション要望
- ▶ 大企業は異種環境に対応するPKI
- ▶ アプリケーションは証明書を承認トークンとして利用(Short-Lived)
- ▶ 業界は、X.509証明書を拡張
 - ▶ Extended Validation (EV) 証明書
 - ▶ Logo types
- ▶ Advanced crypto の利用検討

Windows 7へ投資

強固な認証

Public Key Infrastructure

サーバ
統合

現在のシナリ
オの改善

HTTPベース
Enrollment

サーバ統合

Short-Lived証明書の発行/DB書込み選択

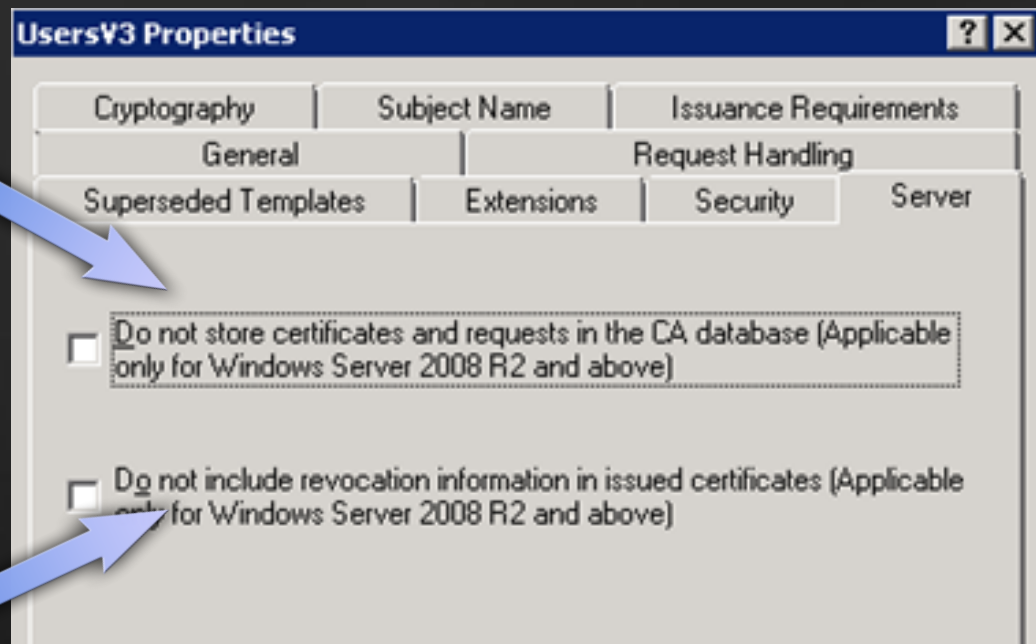
- ▶ 新PKI シナリオとしてshort-lived証明書
 - ▶ Network Access 保護 (NAP)
 - ▶ OCSP 署名証明書
- ▶ DB増大に対する次善策
 - ▶ 専用サーバ利用又はDB削除等のDB管理
- ▶ Windows Server 2008 R2
 - ▶ 管理者によって、認証局(CA)がDBに証明書を書込むかどうか設定可
 - ▶ !!! x64 サポートのみ

サーバ統合

Short-Lived証明書の発行/DB書込み選択

DB書込み選択

CRL発行選択



サーバ統合

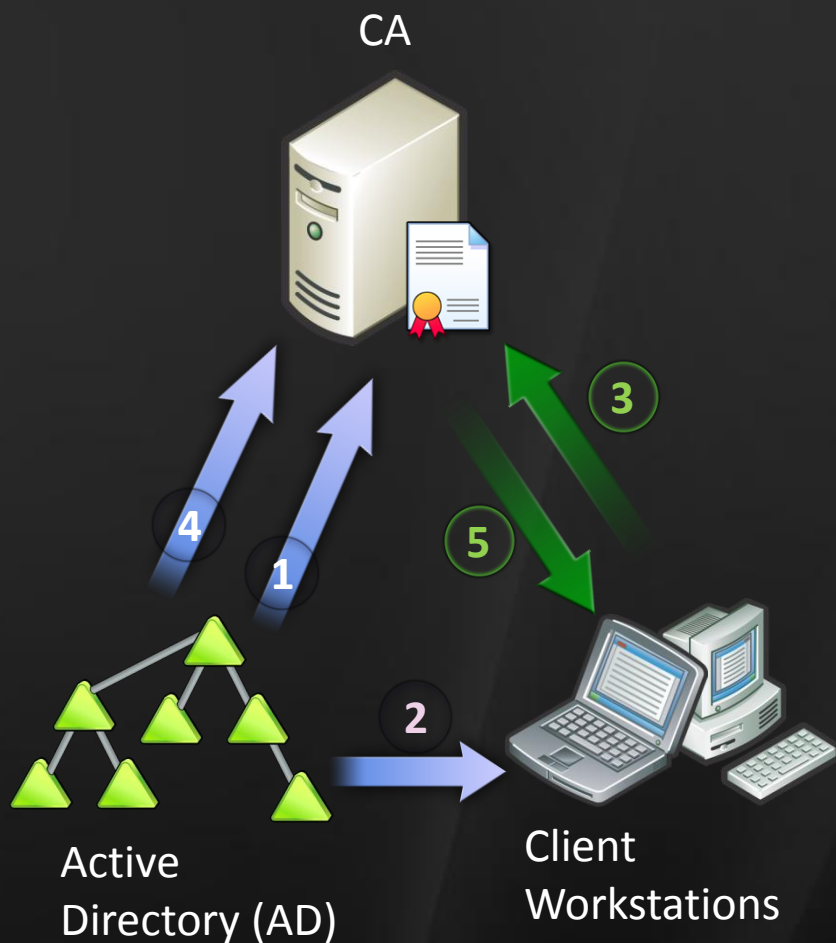
サーバコア サポート

- ▶ 認証局(CA)はサーバコアのサポート
 - ▶ ロカルコマンド群
 - ▶ リモート管理UX
 - ▶ HSMベンダの鍵管理

サーバ統合 フォレスト間登録

現状

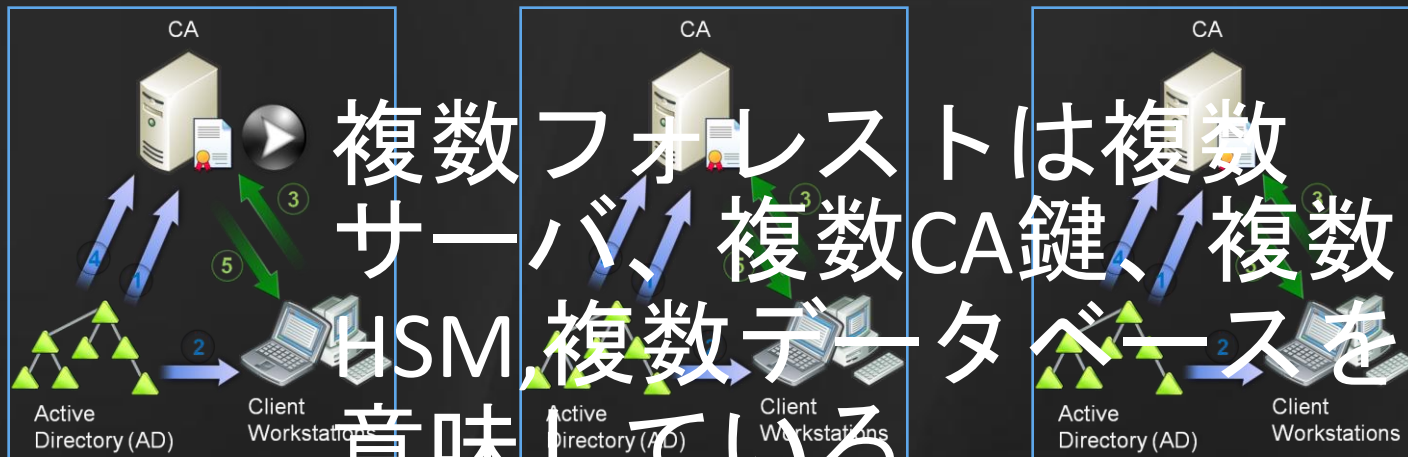
シングルフォレスト



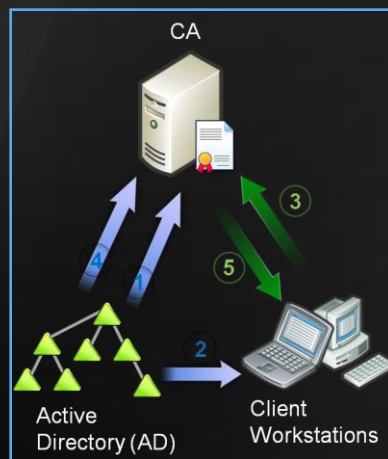
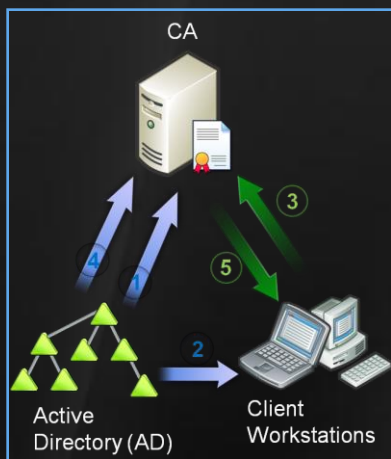
1. CAはADから証明書テンプレートを読み込む
2. クライアントはADから証明書テンプレートを読み込む
3. クライアントはCAへ証明書リクエストを送信
4. CAはADのクライアント情報から主体名を生成
5. CAは証明書を発行し、クライアントへ返信

現状

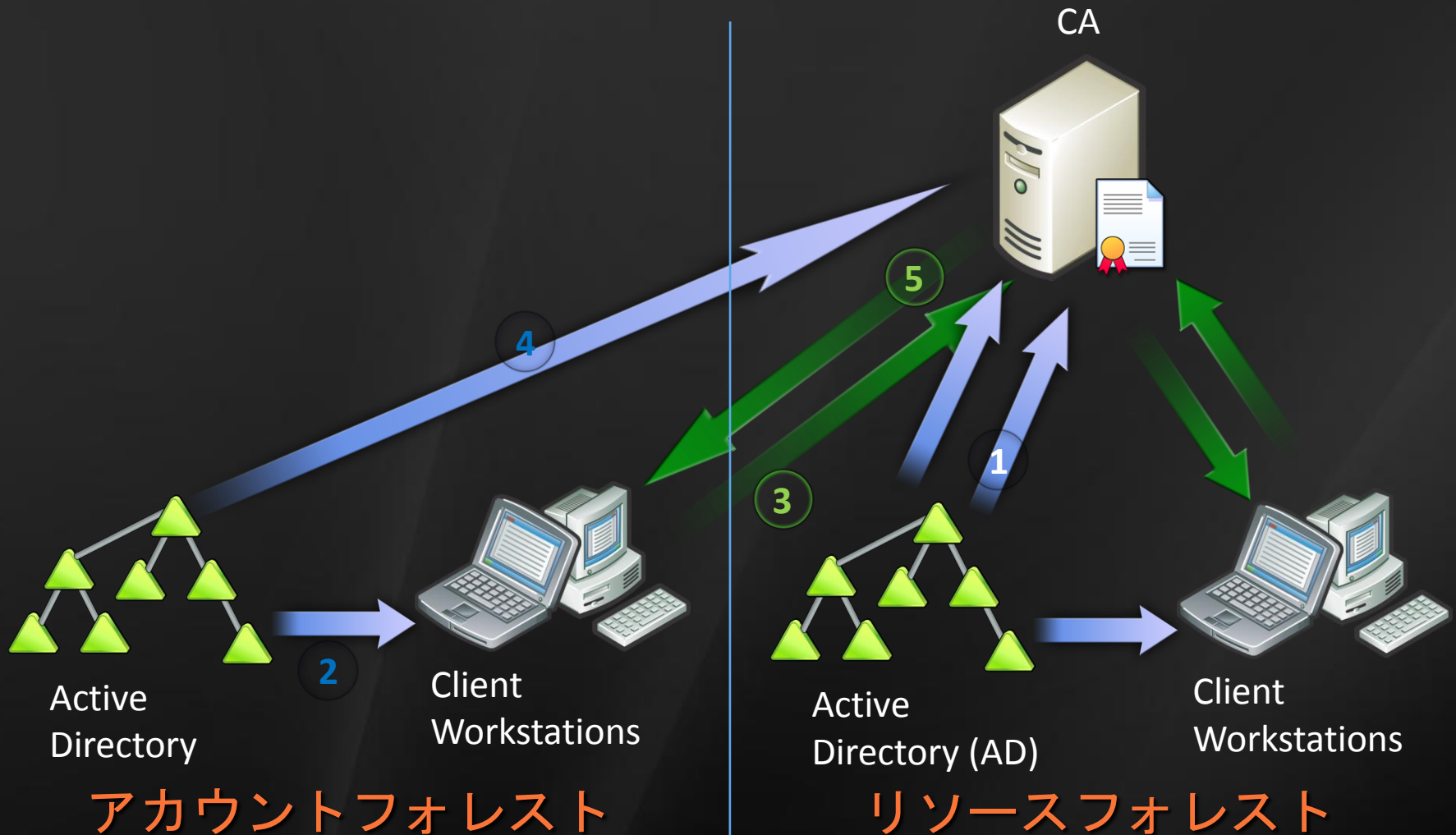
複数フォレスト



複数フォレストは複数サーバ、複数CA鍵、複数HSM、複数データベースを意味している



これから フォレスト間登録



サーバ統合

フォレスト間登録

- ▶ Windowsはフォレスト間の証明書登録と発行をサポート予定。
 - ▶ アカウントとリソースフォレストのADフォレストの双方向信頼関係が必要
 - ▶ Windows Server 2008 R2 CAが必要
 - ▶ クライアントは Windows XP以上が必要

サーバ統合

フォレスト間登録:管理

- ▶ CAはリソースフォレストのテンプレートを読み込む
- ▶ クラインとは、アカウントフォレストのテンプレートを読み込む
- ▶ リソースフォレストとアカウントフォレストのテンプレートは、シンクしているかどうか確かめる必要あり
 - ▶ 初期の発行時
 - ▶ その後のメンテナンス時

サーバ統合：サマリ

1. NAP管理の簡素化
2. サーバコアへのインストール
3. フォレスト間登録のサポート

Windows 7へ投資

強固な認証

Public Key Infrastructure

サーバ
統合

現在のシナリ
オの改善

HTTPベース
Enrollment

現在のシナリオ改善

Standard エディションのV2 テンプレートサポート

- ▶ W2K へV1証明書テンプレート導入
- ▶ W2K3へ V2証明書テンプレート導入
 - ▶ W2K3 Standard エディションは未サポート
- ▶ W2K8 へV3証明書テンプレート導入
 - ▶ W2K8 Standardエディションは未サポート
- ▶ Standard エディションのWindows Server 2008 R2
へインストールされたCAは全ての証明書テンプレートバージョンをサポートする予定
 - ▶ 自動登録のサポート
 - ▶ 鍵archivalのサポート
 - ▶ その他

現在のシナリオ改善

Best practice analyzer

- ▶ ほとんどのサポートCallは、設定ミス
- ▶ Windows Server 2008 R2 はBest Practice Analyzer (BPA) ツールの導入予定
- ▶ CAがルールを設定し、CA設定変更後、BPA ツールで確認が可能

現在のシナリオ改善

Best practice analyzer

BPA スキャン

The screenshot displays the Windows Server Manager interface for a server named 'Server Manager (27-3289B231A)'. The left-hand navigation pane shows a tree view with categories: Roles (Active Directory Certificate, Active Directory Domain Se, Application Server, Web Server (IIS)), Features, Diagnostics, Configuration, and Storage. The main pane is titled 'Active Directory Certificate Services' and contains the following sections:

- Summary:** Shows 3 warnings and 129 informational events in the last 24 hours. Includes a 'Go to Event Viewer' link.
- System Services:** All Running. A table lists the following services:

Display Name	Service Name	Status	Startup Typ
Active Directory Certificate Ser...	CertSvc	Running	Auto
World Wide Web Publishing Ser...	w3svc	Running	Auto
- Description:** Creates, manages, and removes X.509 certificates for applications such as S/MIME and SSL. If this service is stopped, certificates will not be created. If this service is disabled, any services that explicitly depend on it will fail to start.
- Compliance:** A table showing scan results for 7/18/2008 1:25:43 PM:

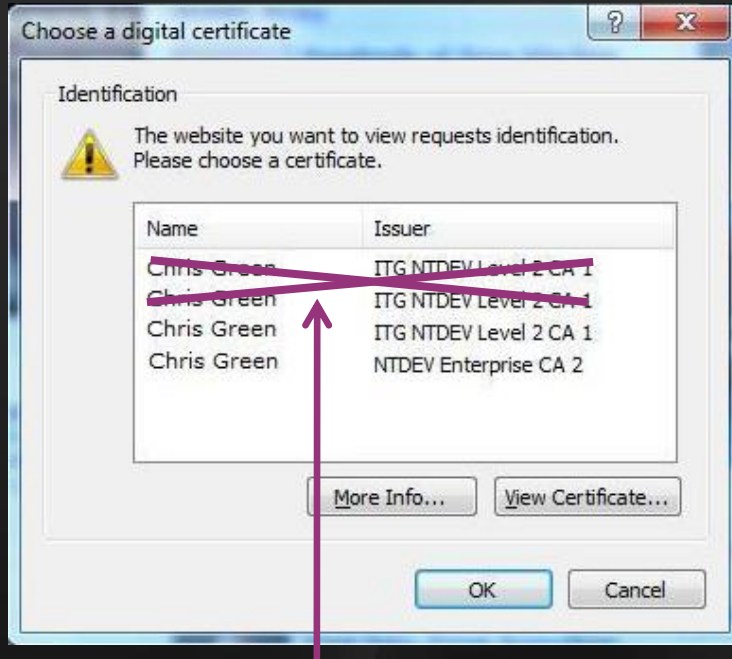
Non-Compliant (0)	Excluded (0)	Compliant (3)	All (3)
Severity	Title	Category	
- Role Services:** 4 installed. Includes a 'Scan this Role' button and other actions like 'Exclude Result', 'Include Result', 'Properties', 'Copy', and 'Help'.
- Resources and Support:** A section for additional information.

A large blue arrow points from the 'BPA スキャン' button on the left towards the 'Scan this Role' button in the Role Services section of the screenshot.

現在のシナリオ改善

証明書選択

Windows Vista



複数アーカイブされた証明書

Windows 7

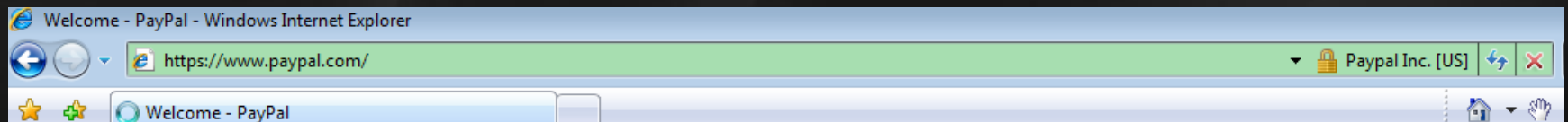


ソフトウェアベースかスマートカードベースかを見分けるアイコン

現在のシナリオ改善

エンタープライズSSL EV 証明書

- ▶ ルートCAがextended validation (EV) ルートであり、EV ポリシーOIDが必要
- ▶ グループポリシーで設定可



現在のシナリオ改善：サマ リ

1. v2 証明書テンプレート
2. Best Practice Analyzer
3. 証明書選択
4. エンタープライズSSL EV 証明書

Windows 7へ投資

強固な認証

Public Key Infrastructure

サーバ
統合

現在のシナリ
オの改善

HTTPベース
Enrollment

HTTP ベースのEnrollment 設計ゴール

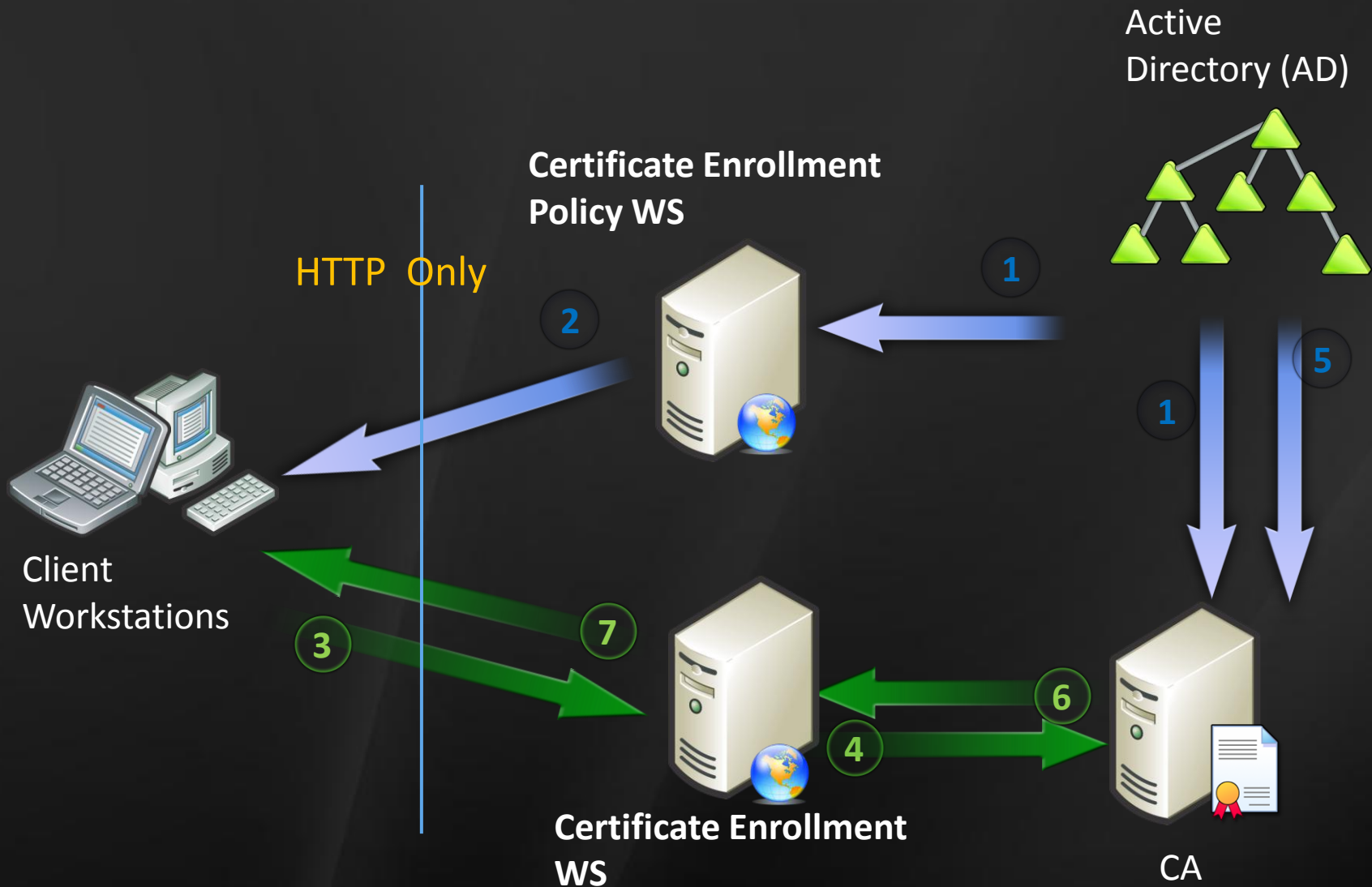
Windows PKIクライアントを利用した新しいシナリオ：

1. パブリックCA発行のサーバ証明書
2. 会社間の証明書発行
 - ▶ パートナーシナリオ等
3. ドメイン非参加クライアントへの発行
4. B2C 発行！
 - ▶ 銀行サイトが証明書発行
5. その他

HTTP ベースのEnrollment デザイン概要

- ▶ 証明書登録用に2つのHTTPベースプロトコル規定
- ▶ その新しいプロトコルに基づきクライアントサービス実装
- ▶ サーバサイドもそれらプロトコルを実装
- ▶ 認証局様、他ISV様と相互接続 (Interoperability)の活動

HTTP ベースのEnrollment



HTTP ベースのEnrollment

自動登録の拡張

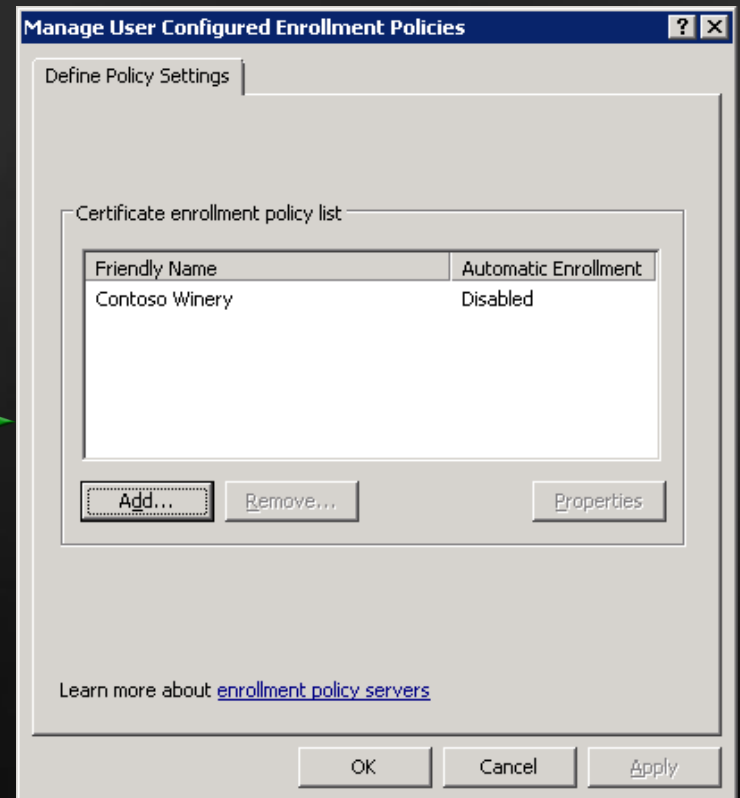
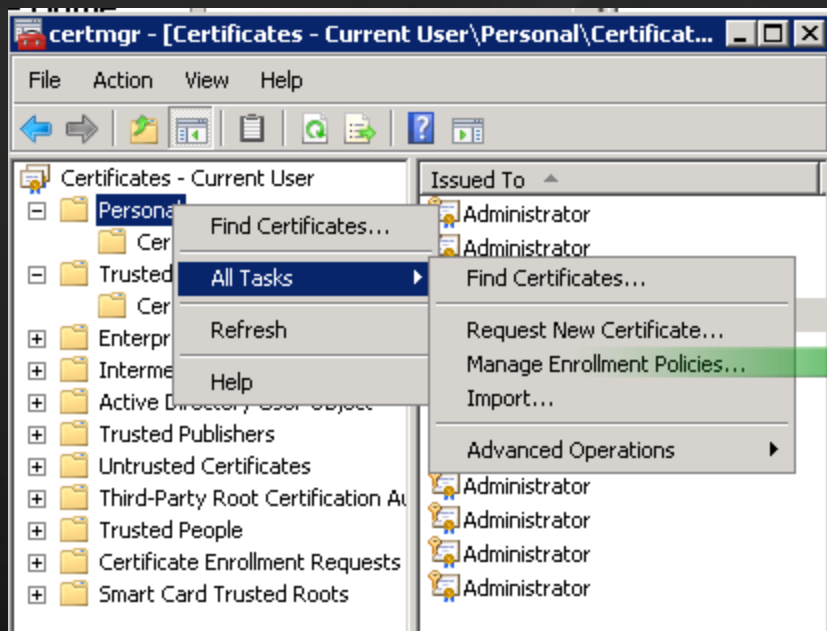
- ▶ クライアント用に設定された”登録ポリシー”
毎に正しい証明書が登録、発行される仕組み
 - ▶ 両プロトコルに”client role”を実装
 - ▶ ポリシサーバURLリストを維持
 - ▶ ポリシサーバから返信された登録ポリシーの
キャッシュ保持
 - ▶ ドメイン非参加（ワークグループ）環境で実施

HTTP ベースのEnrollment 認証

- ▶ Windowsクライアントはポリシサーバ及び登録サーバに同じ認証機能を利用する
 - ▶ ケルベロス
 - ▶ Username/Password
 - ▶ 証明書ベース
- ▶ クレデンシャル保存サポート(オプション)
- ▶ proof of possessionによる更新
- ▶ SSLが必須

HTTP ベースのEnrollment

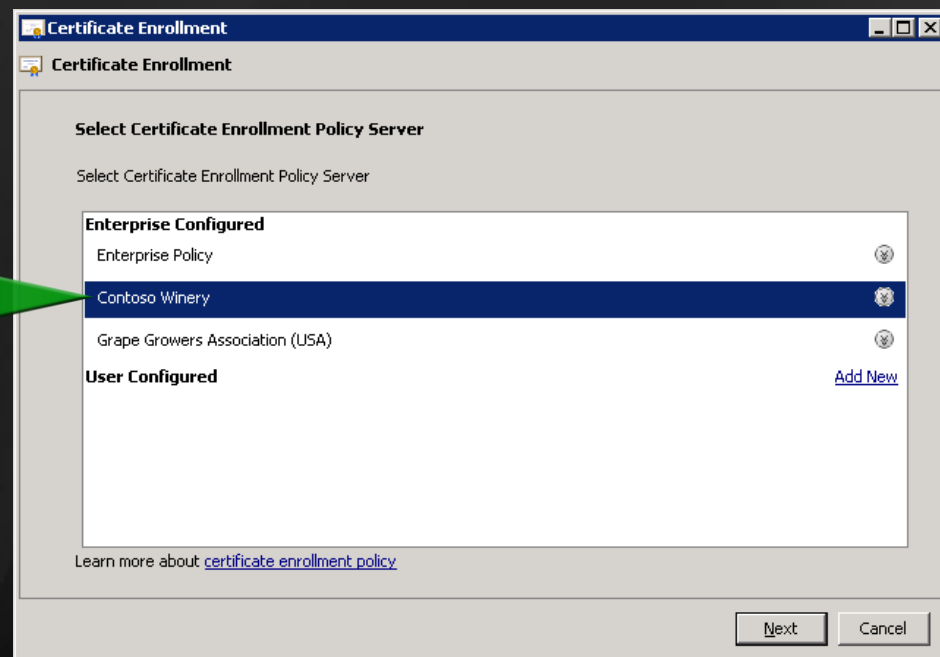
Enrollmentポリシー画面



HTTP ベースのEnrollment 証明書ウィザード

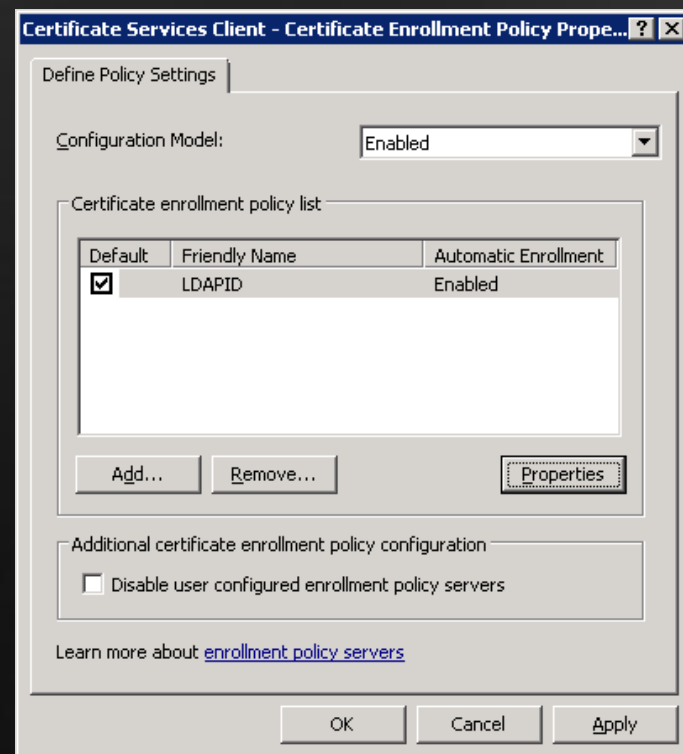
▶ Enrollmentウィザードの追加ステップ

Enrollment
ポリシートリ



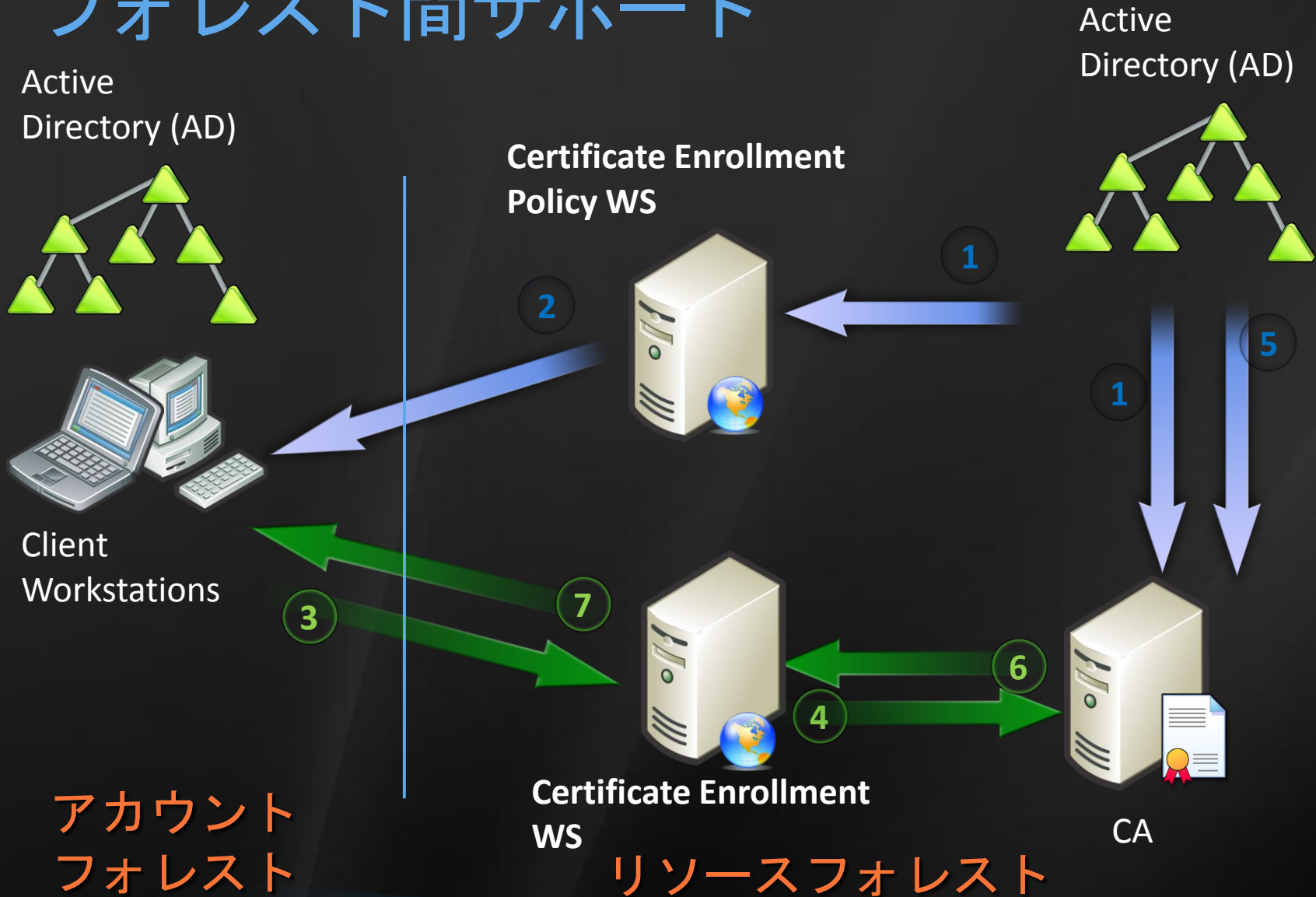
HTTP ベースのEnrollment グループポリシー画面

- ▶ クライアントへポリシーサーバを公開 (Publish)
- ▶ ポリシサーバURIの検証
- ▶ 同じ画面でローカルポリシーやユーザ設定



HTTP ベースのEnrollment

フォレスト間サポート



アカウント
フォレスト

リソースフォレスト

HTTP ベースのEnrollment

ウェブサーバシナリオ: 発行と更新

- ▶ 管理者がウェブサーバにログイン
- ▶ 管理者がIEブラウザを開き、CAサイトにアクセスし、アカウント作成
- ▶ 管理者はユーザアカウント制御を許可し以下を実施:
 - ▶ ポリシサーバのURLをローカルに登録
 - ▶ ポリシサーバ用にクレデンシャルを設定
 - ▶ ポリシサーバに登録
 - ▶ 動的な登録ポリシ
 - ▶ 発行が完了すると、証明書がインストールされる

HTTP ベースのEnrollment

ウェブサーバシナリオ: 失効からの回復

- ▶ ポリシサーバエントリ用の設定
 - ▶ User/Password クレデンシャル設定
 - ▶ 自動登録許可
- ▶ CAによる証明書失効、新しいCRL公開
- ▶ 旧CRL失効後、8時間内に：
 - ▶ サーバは新しいCRLダウンロード
 - ▶ サーバは既存証明書は失効と記される
 - ▶ サーバはポリシサーバからポリシをダウンロードし、新しい証明書を発行

HTTP ベースのEnrollment

ウェブサーバシナリオ: 動的ポリシー更新

- ▶ ポリシサーバエントリ用の設定
 - ▶ 例えば、SSL 1年 1024 鍵長のポリシー
 - ▶ ポリシの毎週アップデート
- ▶ CA が2048に鍵長を変更し、ポリシーを変更する
- ▶ 1 週間内に:
 - ▶ サーバは新しいポリシーをダウンロード
 - ▶ サーバは現行証明書を保存(Archived)として記す
 - ▶ サーバは新しい証明書を発行

GMOグローバルサイン
Win7統合及び
デモ



Enrollmentアーキテクチャのコンセプト

Enrollment
Client



**Policy
Authority**



Provides certificate enrollment policy to a requestor

**Certification
Authority**



Receives, processes and responds to certificate requests

**Authentication
Authority**



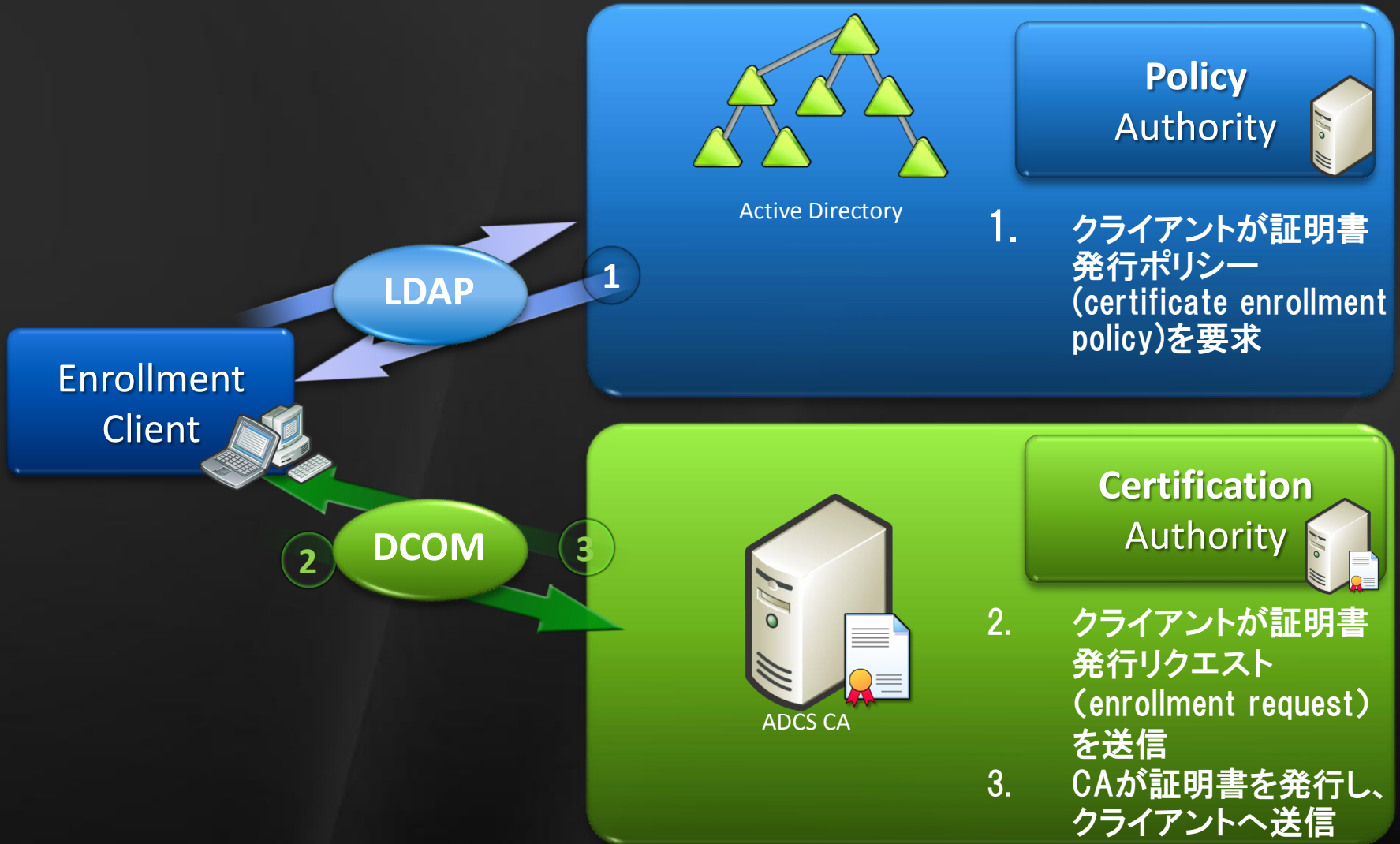
Provides or validates authentication information

**Identity
Authority**

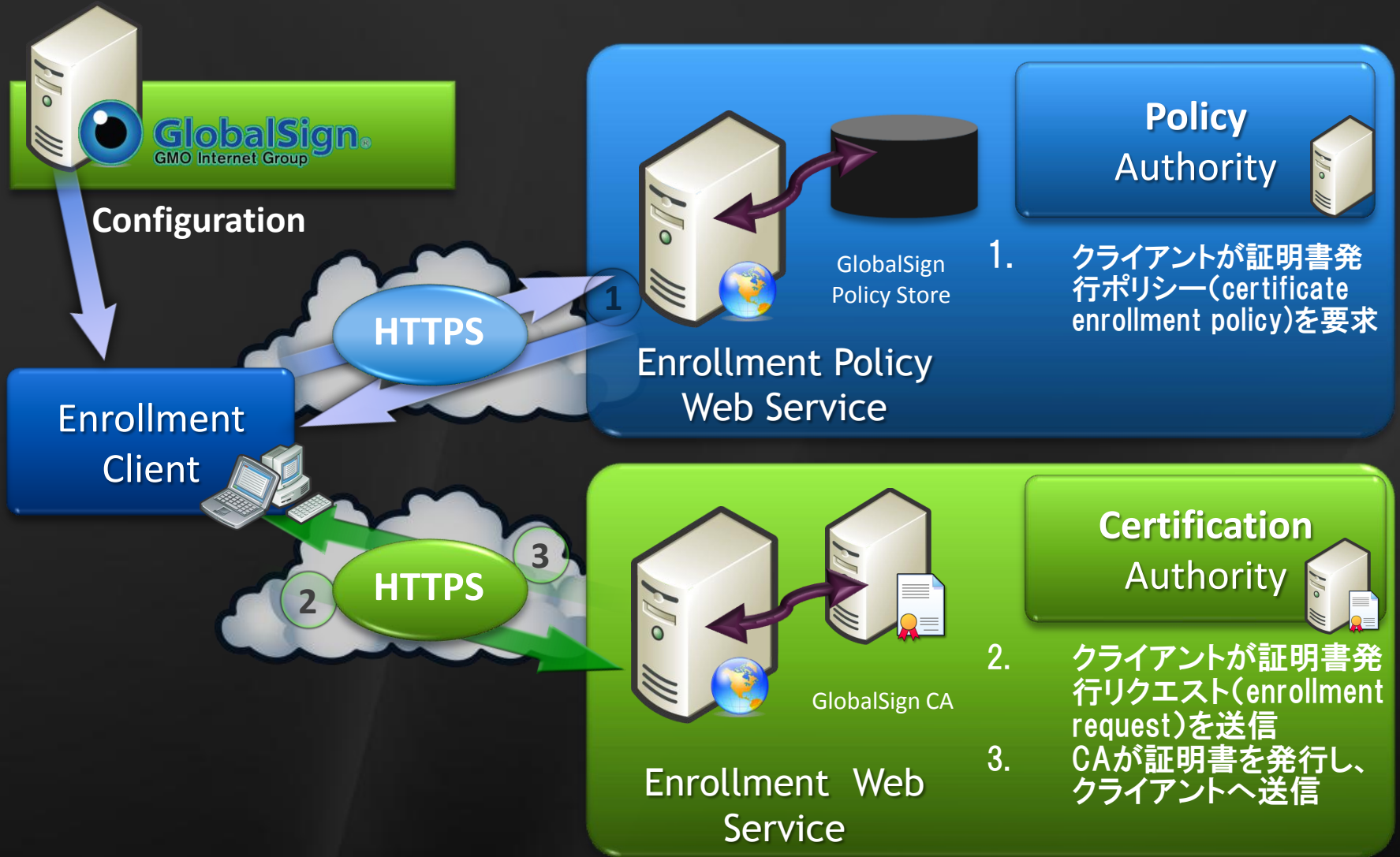


Provides identity information

旧来のWindowsのEnrollmentアーキテクチャ



GlobalSign の登録アーキテクチャ

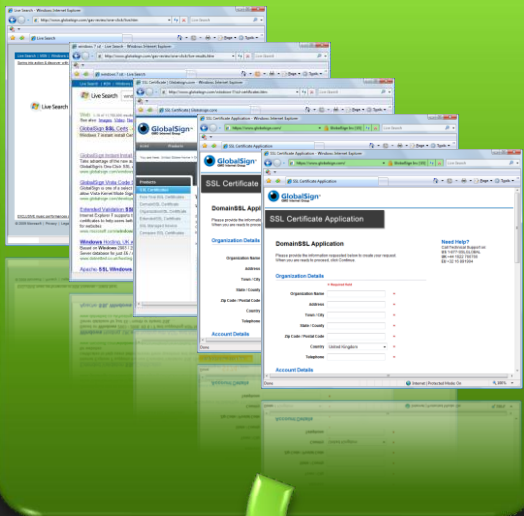


証明書 の Enrollment Web Services

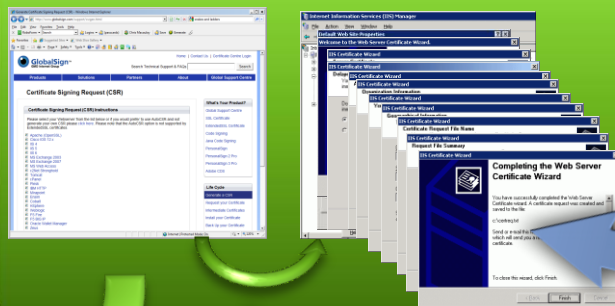
- ▶ 2つの Web Services プロトコル
 - ▶ Certificate Enrollment Policy [MS-XCEP]
 - ▶ Certificate Enrollment [MS-WSTEP]
- ▶ HTTPS ベースで、ファイアウォールとの親和性が高い
- ▶ 実用的な実装
- ▶ 企業内CA以外のCAとの接続が可能に
 - ▶ Web SSLを目的としたパブリックルートにつながる証明書の利用や、PKIホスティング
- ▶ 企業内PKIをより良いものに
 - ▶ 構築済みのPKI環境を、少ない労力と少ないコストで拡張可能

現在のSSL証明書の発行形態

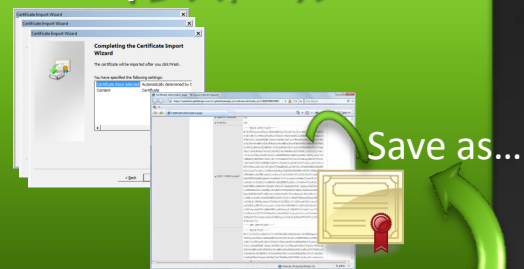
登録(購入)



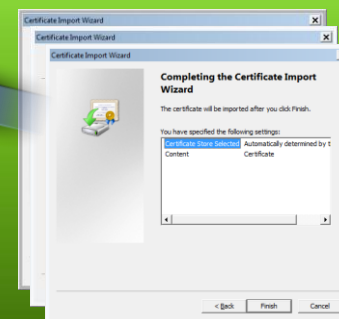
CSR生成



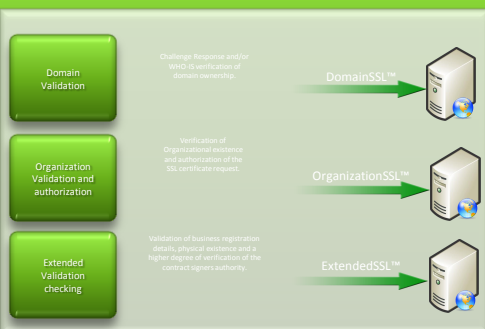
中間CA証明書のインストール



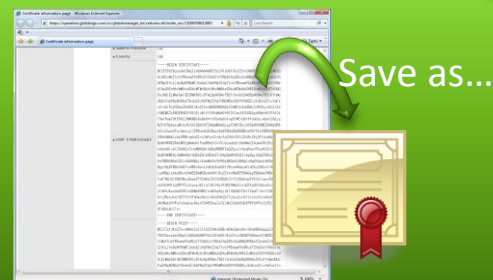
証明書のインストール



審査

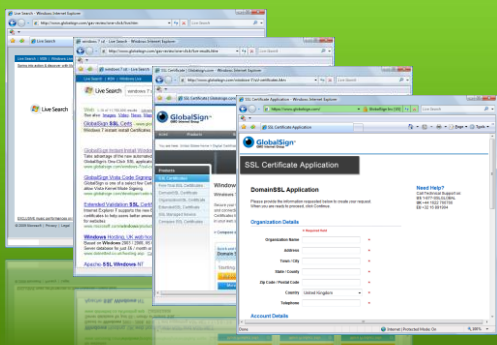


証明書

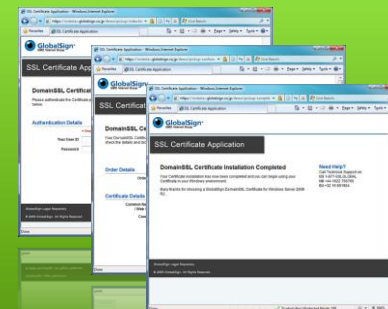


新しいSSL 証明書の発行形態

登録(購入)



発行要求とインストール



審査



新しいWindows PKIアーキテクチャをベースにした証明書発行サービス

- ▶ CSRの生成が不要
- ▶ 証明書の購入・インストールプロセスがシンプルになり、ユーザの負担が軽くなる
- ▶ 証明書の更新を自動的に行うことができる!
 - ▶ 証明書の有効期間をWindowsがハンドリングし、自動的に証明書の発行要求をおこなう

Windows 7へ投資

強固な認証

Public Key Infrastructure

サーバ
統合

現在のシナリ
オの改善

HTTPベース
Enrollment

強固な認証

Biometric

- ▶ Biometric デバイスの新プラットフォーム
 - ▶ 指紋認証にフォーカス
 - ▶ 今後のCertificationプログラムに基づく新ドライバーモデル
- ▶ ユーザUXと統合
 - ▶ Windows ログオン, ローカル及びドメイン
 - ▶ デバイスや機能検出
- ▶ エンタープライズ管理
 - ▶ グループポリシーでBiometricの無効化
 - ▶ アプリケーション利用のみ、Windowsログオンは禁止

強固な認証

SmartCard

- ▶ スマートカード Plug-and-Play
 - ▶ Windows UpdateとWSUS/SUSに基づくドライバーインストール
 - ▶ ログオン以前でのドライバーインストール
 - ▶ アドミン権限無しでのドライバーインストール
- ▶ スマートカードクラス mini-driver
 - ▶ NIST SP800-73-1 (PIV) サポート
 - ▶ INCITS GICS (Butterfly) サポート
- ▶ Windows 7 スマートカードフレームワーク改善
 - ▶ Biometric に基づいたスマートカード案ロックのサポート改善
 - ▶ Secure Key Injectionの新しいAPI

強固な認証

ECC ベースのスマートカードログオン

- ▶ Windows 7 は以下をサポート予定:
 - ▶ ECC 証明書のスマートカード
 - ▶ ECC 証明書を利用したログオン

強固な認証：サマリ

1. Biometric
2. スマートカード

Q & A

関連リソース

▶ Windows 7

- ▶ <http://www.microsoft.com/japan/windows/windows-7/default.aspx>

▶ Windows 2008 R2 RC

- ▶ <http://www.microsoft.com/japan/windowsserver2008/prodinfo/R2.msp>

▶ Windows 2008 R2 PKI

- ▶ [http://technet.microsoft.com/ja-jp/library/dd448537\(WS.10\).aspx](http://technet.microsoft.com/ja-jp/library/dd448537(WS.10).aspx)

Microsoft[®]

© 2008 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.