



# Windows Server 2008 のPKI機能

渡辺 清 CISSP

*Security Architect and Senior Consultant  
Security Center of Excellence, Microsoft*

# アジェンダ

- PKI 概要
- Windows Server 2008 PKI機能
  - 暗号(Cryptography)
  - 登録(Enrollment)
  - 管理(Manageability)
  - 失効(Revocation)
- アップグレード及びマイグレーション

# MSのPKI ビジョン

“It just works”

認証局インフラストラクチャは...

- 簡単に展開し設定できる
- 簡単に監視し維持できる
- ユーザフレンド理で小コスト
- アプリケーションのサポート
- 安全、準拠、且つ標準ベース

# アプリケーション統合

広範囲プラットフォームとシナリオサポート



# アジェンダ

- PKI 概要
- Windows Server 2008 PKI機能
  - 暗号(Cryptography)
  - 登録(Enrollment)
  - 管理(Manageability)
  - 失効(Revocation)
- アップグレード及びマイグレーション

# 暗号: 概要

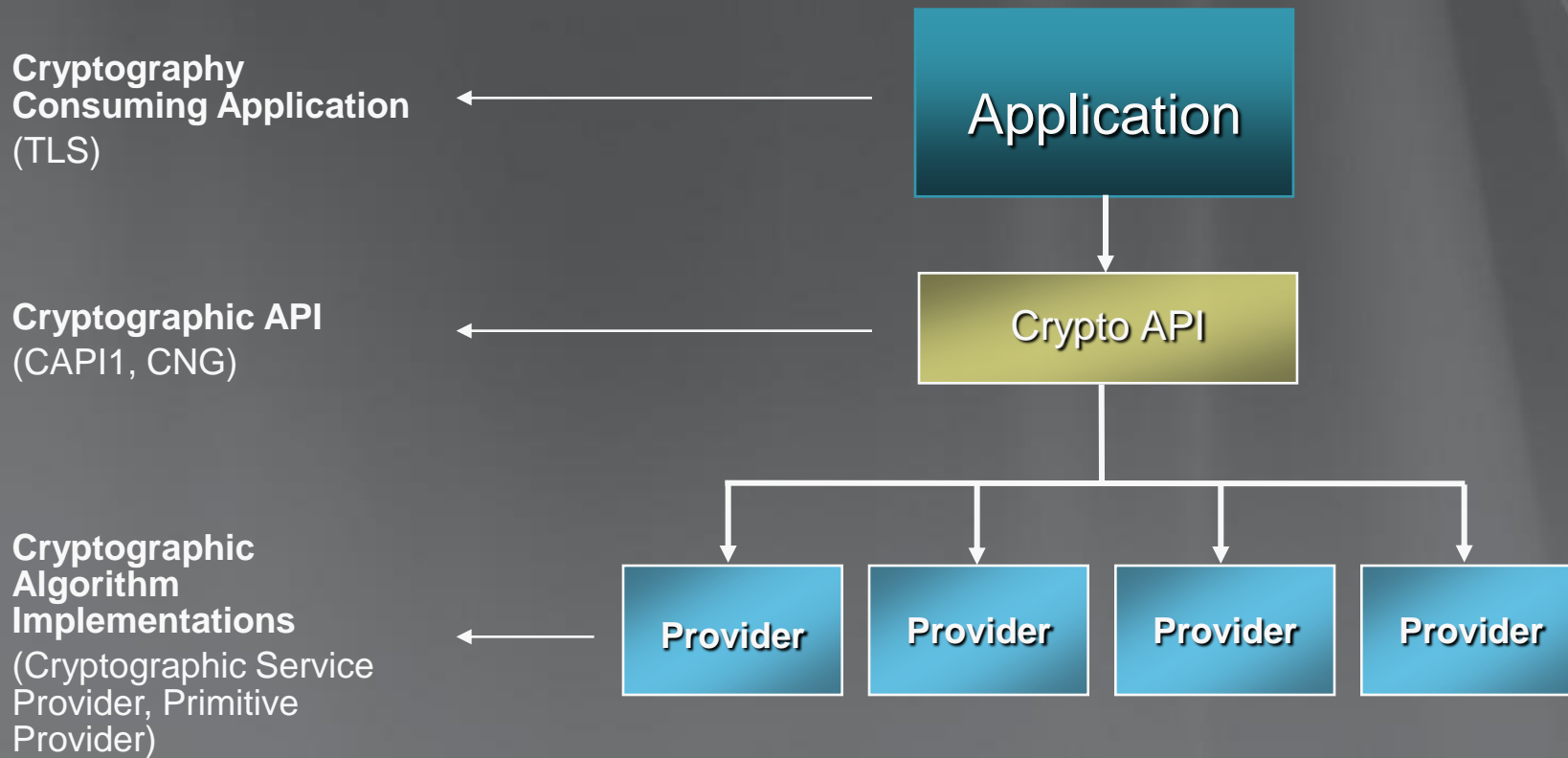
- 新しい要求: Suite-B Algorithms
  - ECC, AES, SHA2
  - 米国政府の要件
  - 企業もSHA2を要件としている
- **C**rypto **N**ext **G**eneration - CNG
  - CryptoAPIの次期バージョン
  - より簡単な開発、展開
  - カーネルモード及びユーザモードでの利用
  - FIPS 140認定、CC認定(Long-term key storage and audit)
  - Suite-B algorithmsのネイティブサポート
    - ECDSA: P256, P384, P521
    - ECDH: P256, P384, P521
    - SHA2: 256, 384, 512
    - AES: 128, 192, 256

# 暗号：詳細

- **Server + client コンポーネント**
  - Suite-B ベースのcertificates発行
- **PKI 設定**
  - All crypto 関連設定の簡素化
- **PKI フレキシビリティ**
  - 新しい暗号アルゴリズムのplug-in 化
    - CAPIはハードコードされたアルゴリズムのみ
- **プロトコル/アプリケーション**
  - TLSとS/MIME のSuite-B利用可

# CNG: 詳細

- アーキテクチャ





# CNG: 詳細

- **Primitive Functions** *BCrypt \**
  - Low level algorithm 実装
  - メモリで動作
  - ユーザとカーネルモード
- **Key Storage Functions** *NCrypt \**
  - 永続的な鍵保存及びハンドリング
  - ユーザモード
  - 暗号操作は、primitives を利用
  - デフォルトで分離されたプロセスで動作
- **CryptoConfig Functions**
  - ACLで設定データベースを保護
  - ドメイン及びローカルで設定

# CNG: Crypto Agilityの周辺

Cryptographic agility は以下の要求を満たそうとするもの:

- 旧暗号Primitiveの入替
- 新しい暗号Primitiveを追加
- どのPrimitiveを利用するかをポリシ化して実装

⋮  
⋮

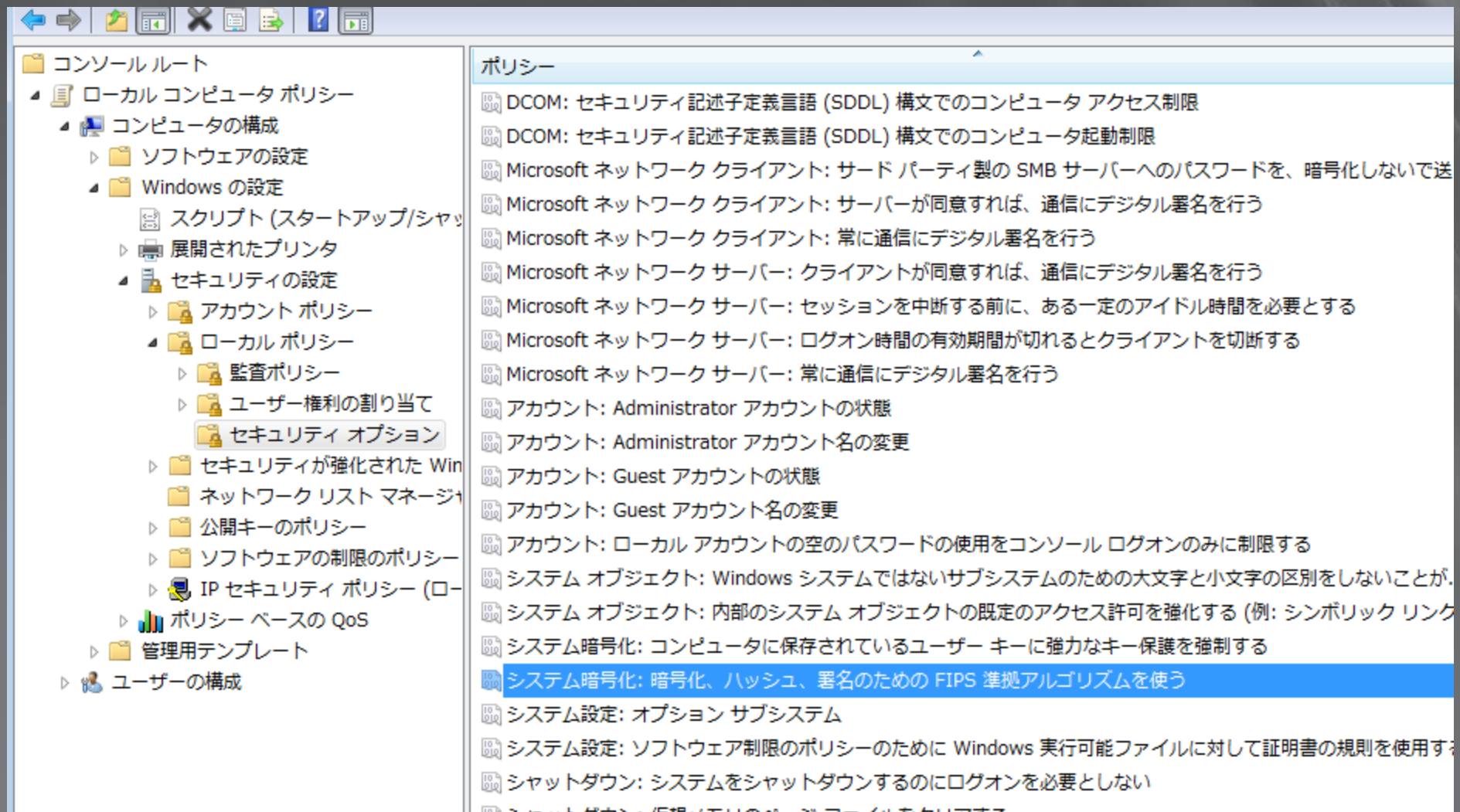
アプリケーション自身の実装を変更しないために . . .

# CNG: Crypto Agilityの周辺

- Providerを意識しなくてもよい。どうやって？
- この辺り。
  - アルゴリズムをリクエスト。システムがベストのものを返す。
    - プロバイダをリスト(Enumerateする)化する
      - [BCryptEnumRegisteredProviders](#)
    - プロバイダのプロパティをチェック
      - [BCryptQueryProviderRegistration](#)
    - 特定のプロバイダを選択
      - [BCryptRegisterProvider](#)
- 今後よりよいPrimitive実装があれば、それを選ぶように、実装しておく。

# まとめ知識 : Group Policy

- FIPS準拠アルゴリズムの強制 (Dev用)



# アジェンダ

- PKI 概要
- Windows Server 2008 PKI機能
  - 暗号(Cryptography)
  - 登録(Enrollment)
  - 管理(Manageability)
  - 失効(Revocation)
- アップグレード及びマイグレーション

# 登録 UI

- 新規 UI
  - 改善ポイント (XPベースのUIから)
    - ユーザビリティ
    - サポート
  - 追加機能
    - 代理登録
    - 有効期限通知

# 登録 API

- **問題点**

- 旧APIはメンテが難しい; 利用が複雑;  
ActiveXの利用

- **解決方法**

- xenroll.dll と scrdernl.dllリタイヤ
- 新 API
  - COM-ベース OOD (Object Oriented Design)
  - 新 クラス階層
  - 開発者にやさしい – 簡単に理解でき、コーディングし  
やすい

# Credential ローミング

- **問題点**

- 証明書と秘密鍵は特定マシーンに属する

- **副作用**

- CAの負荷増
- 利用が難しい(E.g. S/MIME)

- **Solution**

- Credential ローミング Services が全ての credentials をユーザマシーンにアクティブディレクトリを利用して配布
- クライアントはXP SP2より以上で可能



# アジェンダ

- PKI 概要
- Windows Server 2008 PKI機能
  - 暗号(Cryptography)
  - 登録(Enrollment)
  - 管理(Manageability)
  - 失効(Revocation)
- アップグレード及びマイグレーション

# 企業内 PKI

- **問題点**

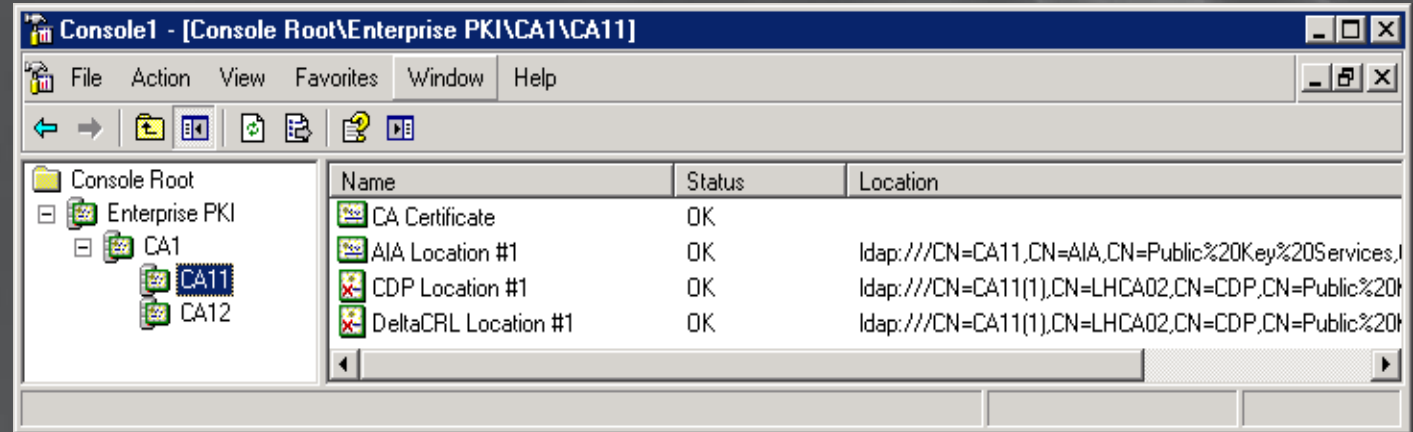
- 複数CAのステータス検証

- **解決方法**

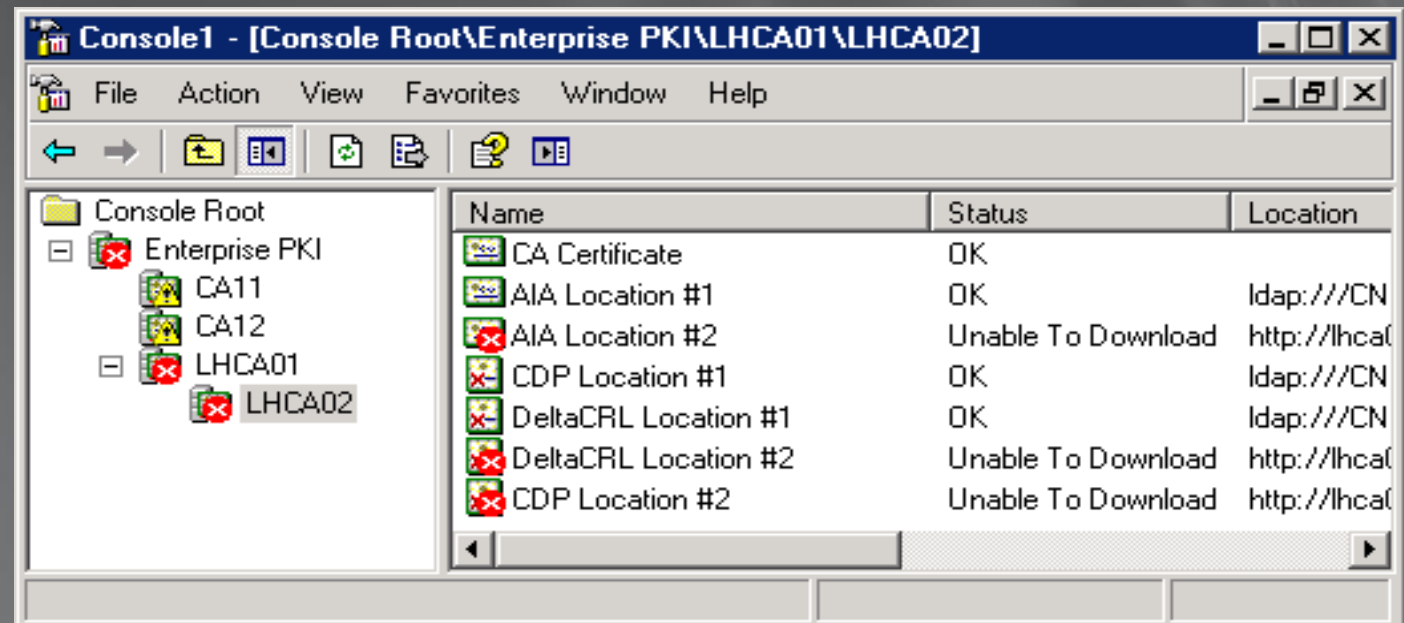
- Enterprise PKIはフォレスト内の全てのCAのステータス確認可能

# 企業内 PKI

健全な PKI



不健全な PKI



# モニタリング

- **問題点**

- 証明書サービスの状態やパフォーマンスが分りにくい、監視しにくい。

- **解決方法**

- 新しいCA用のパフォーマンスカウンタを追加
- CA 及び OCSP MOM 2005管理パック追加

# 代理登録 Agent

- **問題点**

- PKI 登録 Agentはフォレスト内の全てのタイプの証明書を全てのユーザに対して代理で発行できる権限がある

- **解決方法**

- 代理登録Agentに制限を持たせる
  - 代理登録Agentを操作できるユーザの制限
  - 代理登録Agentで利用できるテンプレートの制限

# 代理登録 Agent

登録 Agents

テンプレート  
制限

ユーザ制限

CA11 Properties

General Policy Module Exit Module  
Extensions Storage Certificate Managers  
Enrollment Agents Auditing Recovery Agents Security

For more information see [Delegated Enrollment Agents](#).

Do not restrict enrollment agents  
 Restrict enrollment agents

Enrollment agents:

PKIDEM02\RA1EnrollAgents	Add...
PKIDEM02\RA2EnrollAgents	Remove

Certificate Templates:

Contoso Smartcard Logon	Add...
	Remove

Permissions:

Name	Access	Add...
PKIDEM02\RA1users	Allow	Remove
		Deny

OK Cancel Apply

# その他PKI 改善点

- CA クラスタ
  - 2ノードActive/Passive
- DB 検索/フィルタ パフォーマンス改善
  - UI 及び certutil
- MSCEP との統合

# アジェンダ

- PKI 概要
- Windows Server 2008 PKI機能
  - 暗号(Cryptography)
  - 登録(Enrollment)
  - 管理(Manageability)
  - 失効(Revocation)
- アップグレード及びマイグレーション



# 失効

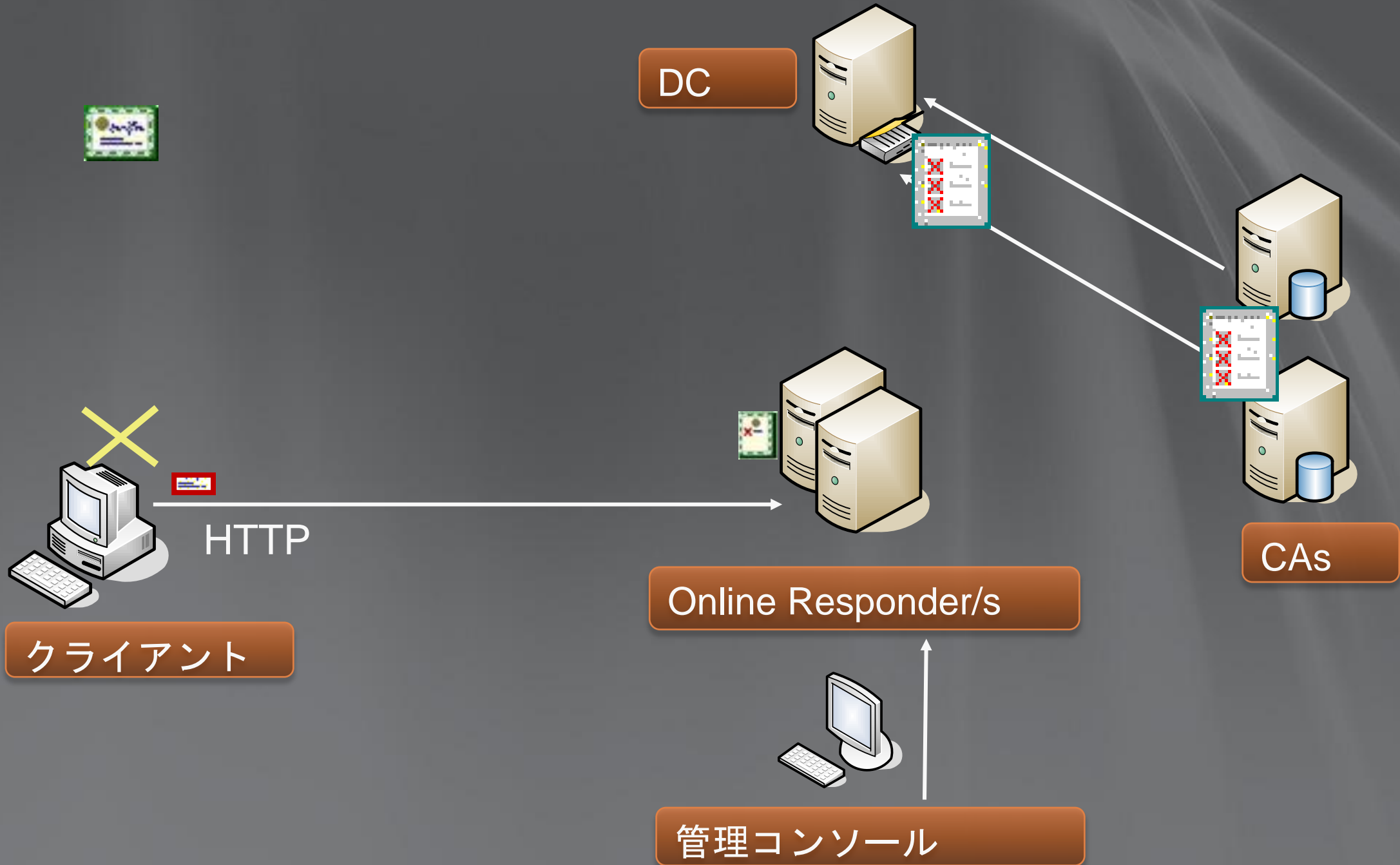
- **問題点**

- CRL ベースの失効は全てのシナリオに適切ではない
  - CRLsのファイルサイズが膨大
  - ダイアルアップ接続
  - ブート時の失効確認

- **解決方法**

- 新しいOCSPクライアント - Vista
- 新しいOCSP Responder - Server 2008
- OCSP stapling - Kerberos と SSL protocols

# OCSP



# OCSP サーバ

- RFC 2560 準拠
- Responder 機能
  - Caching機能
  - NONCE及びNo-NONCEリクエスト
  - 複数CAs
  - 監査
- 追加機能
  - セットアップ統合
  - MOM 管理パック
  - OCSP テンプレート- 展開簡素化

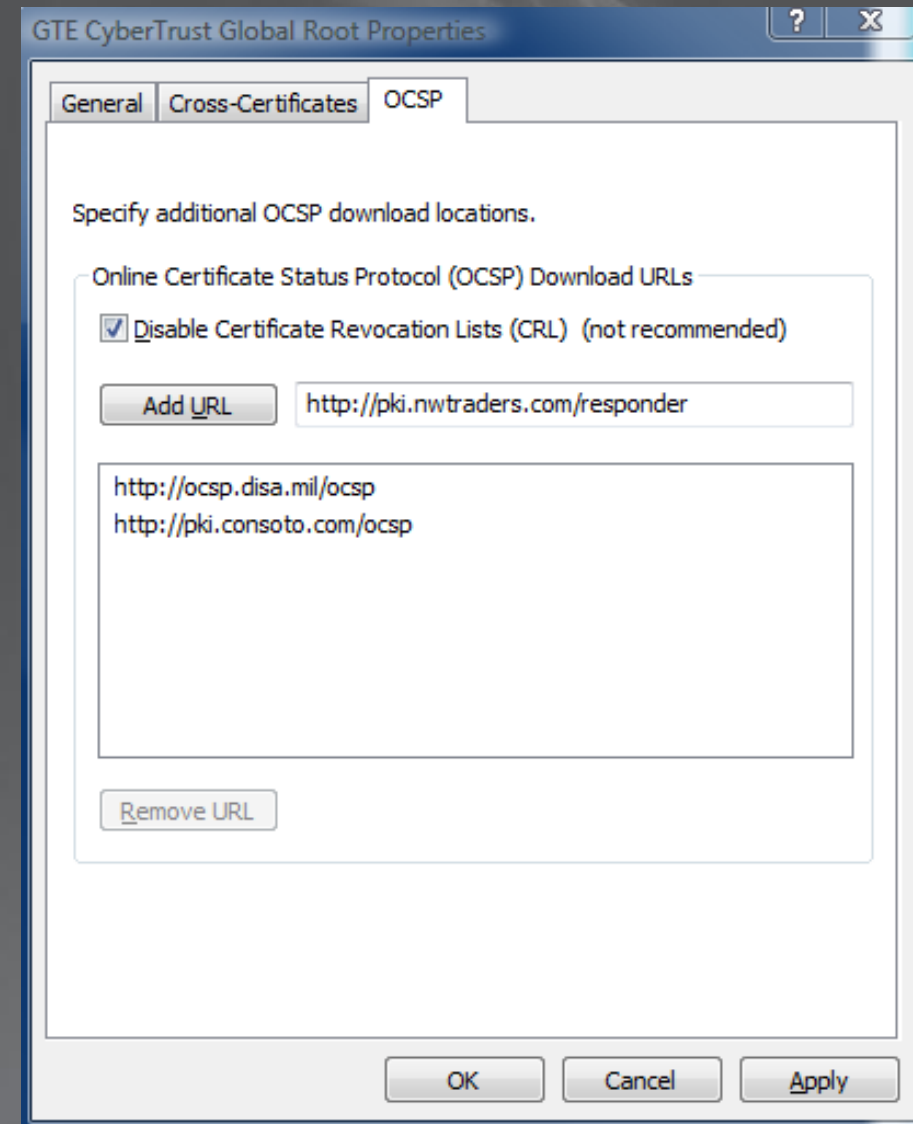
# OCSP 設定オプション

- サーバ

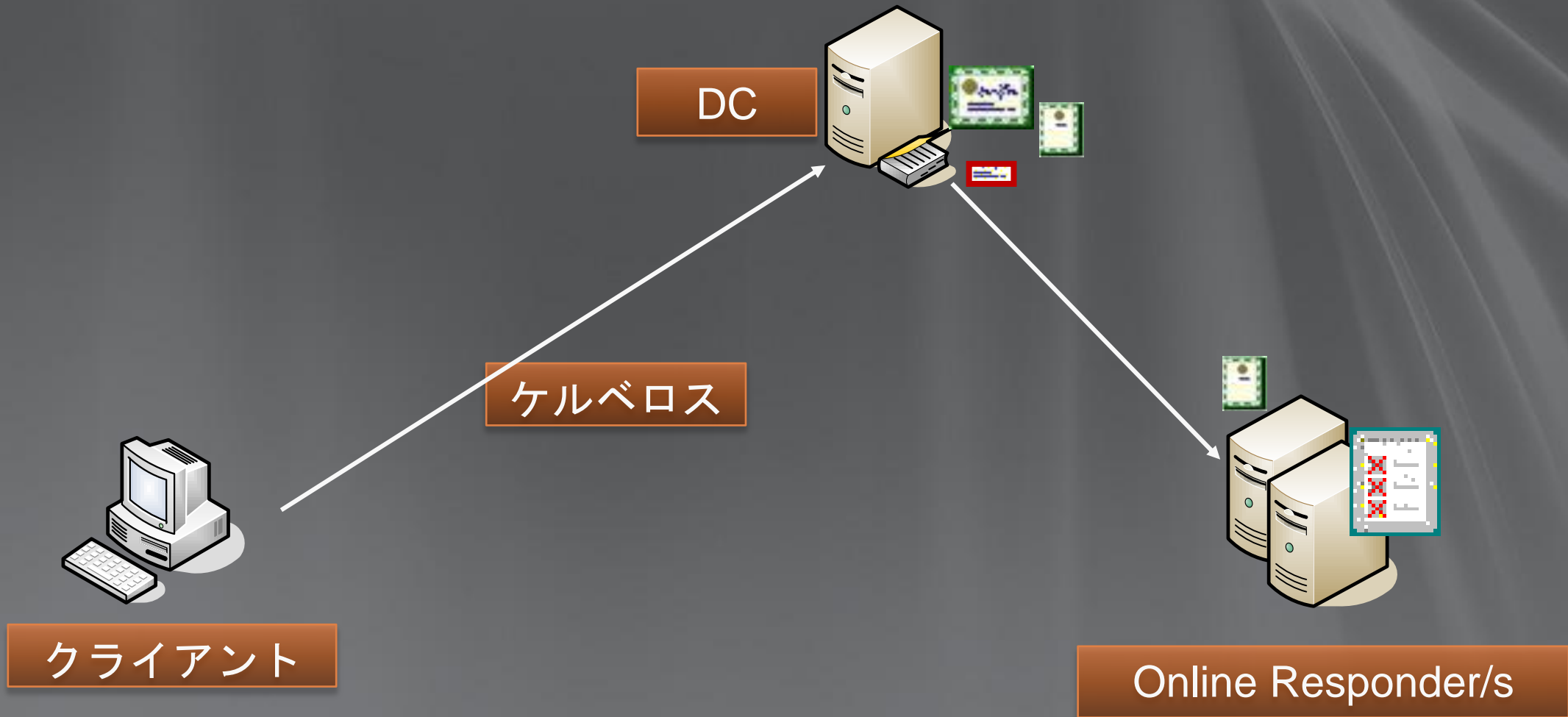
- Cache サイズ
- 監査リクエスト/設定
- CRL 設定
- OCSP 署名証明書

- クライアント

- OCSP よりCDPが優先
- OCSP URL 上書き(Vista SP1)
- レスポンスの寿命延長



# ケルベロス Stapling



# プロトコル Stapling

- ケルベロス及びTLSでの追加
    - サーバが自分自身の証明書の失効ステータスを取得
    - サーバが失効ステータスをキャッシュ
    - サーバがプロトコルハンドシェイク時に失効ステータスを送信
    - クライアントが失効ステータスを利用し証明書を検証
- クライアントおよびOCSPサーバの通信を

# アジェンダ

- PKI 概要
- Windows Server 2008 PKI機能
  - 暗号(Cryptography)
  - 登録(Enrollment)
  - 管理(Manageability)
  - 失効(Revocation)
- アップグレード及びマイグレーション

# アップグレードマトリックス

アップグレード From	Windows Server 2008へアップグレード		
	Standard	Enterprise	Datacenter
Windows Server 2003 Standard (SP1, SP2, R2)	✓	✓	
Windows Server 2003 Enterprise (SP1, SP2, R2)		✓	
Windows Server 2003 Datacenter (SP1, SP2, R2)			✓

## サポート範囲

Windows Server 2008 Beta3 → Windows Server 2008 RC

Windows Server 2008 RC → Windows Server 2008 RTM



# アップグレード: CA

- Active Directory
  - AD スキーマ変更なし
    - 例外: Credential ローミング - Windows Server 2003 は推奨するスキーマ変更あり
  - Group Policy 変更
    - 有効期限通知
    - Credential ローミング

# マイグレーション: CA

- Windows Server 2008の新しいサポート
  - クロスアーキテクチャのマイグレーション
    - Windows Server 2003 x86でバックアップし、Windows Server 2008 x64でリカバー
  - 違うマシン名でのマイグレーション
  - 2ノードハードウェアクラスタへのマイグレーション

# 新しいオンライン資料(英語)

## TechNet Site

<http://technet2.microsoft.com/windowsserver2008/en/servermanager/activedirectorycertificateservices.aspx>

## OCSP Whitepaper

<http://www.microsoft.com/downloads/details.aspx?FamilyID=46dc26d6-af47-43f0-b3de-521831fe09d6&displaylang=en>

## CA Whitepaper

<http://www.microsoft.com/downloads/details.aspx?FamilyID=9bf17231-d832-4ff9-8fb8-0539ba21ab95&DisplayLang=en>

## Microsoft SCEP Whitepaper

<http://www.microsoft.com/downloads/details.aspx?FamilyID=e11780de-819f-40d7-8b8e-10845bc8d446&DisplayLang=en>

# Q&A

# **Microsoft<sup>®</sup>**

*Your potential. Our passion.<sup>™</sup>*

© 2007 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.