Overview su Online Certificate Status Protocol (OCSP)

di Nicola Ferrini

MCT – MCSA – MCSE – MCTS – MCITP

Introduzione

La revoca dei certificati digitali consiste nel rendere non più valido un certificato prima della scadenza. Le motivazioni di questa revoca possono essere le più disparate:

- Il certificato è stato smarrito
- Il certificato non era richiesto
- Un nuovo certificato è stato emesso per lo stesso utente, computer, servizio, programma, ecc.
- Il computer dove è conservata la chiave privata del certificato non è sicuro o è stato rubato

In una infrastruttura PKI (Public Key Infrastructure), le CRL (Certificate Revocation List) contengono tutte le informazioni sui certificati che sono stati revocati o sospesi dalla Certification Authority e vengono utilizzate per determinarne la validità. In genere i computer client scaricano dalla CA la CRL aggiornata, ma spesso ci sono problemi di latenza o di dimensione della stessa CRL , che impediscono il normale download e successivo controllo delle CRL.

Infatti col tempo le CRL possono contenere troppe informazioni in merito allo storico di tutti certificati revocati ed diventare molto pesanti. Per questo motivo sono state introdotte le **Delta CRL**, ma il problema comunque rimane.

Per questo motivo in Windows Server 2008 è stato introdotto il servizio OCSP (Online Certificate Status Protocol), che si occupa di validare e controllare le revoche dei certificati. A differenza delle CRL, il servizio è sincrono e questo significa che i client non mantengono localmente una copia locale delle CRL. Quando viene effettuata una richiesta all'Online Responder, questo fornisce informazioni esclusivamente sulla validità del certificato di cui è stato richiesto il controllo.

Queste informazioni sono firmate digitalmente e vengono comunicate attraverso il protocollo HTTP. Il responder OCSP comunica che il certificato indicato nella richiesta è 'good', 'revoked' o 'unknown'. Se non riesce a processare la richiesta comunica un codice di errore.

L'OCSP può essere installato su qualsiasi computer con Windows Server 2008 Enterprise o Datacenter Edition, mentre i dati relativi alle revoche dei certificati possono essere forniti da qualsiasi CA installata su Windows Server 2008 o Windows Server 2003. Inoltre il servizio OCSP, che in genere non è installato sullo stesso computer che ospita la CA, può ricevere dati (sui certificati digitali revocati) sia da più CA contemporaneamente che da CA di Terze Parti, cioè non Microsoft.

Spiegazione

Installiamo il servizio OCSP utilizzando il Server Manager di Windows Server 2008. Come ho precedentemente spiegato il servizio viene in genere installato su un computer differente rispetto alla CA, ma per comodità in questa demo lo installeremo sulla stessa macchina.

Aggiungiamo quindi il *Role Service* richiesto e tutti gli altri servizi necessari all'installazione dell'Online Responder utilizzando il Server Manager di Windows Server 2008, come mostrato nella figura 1.

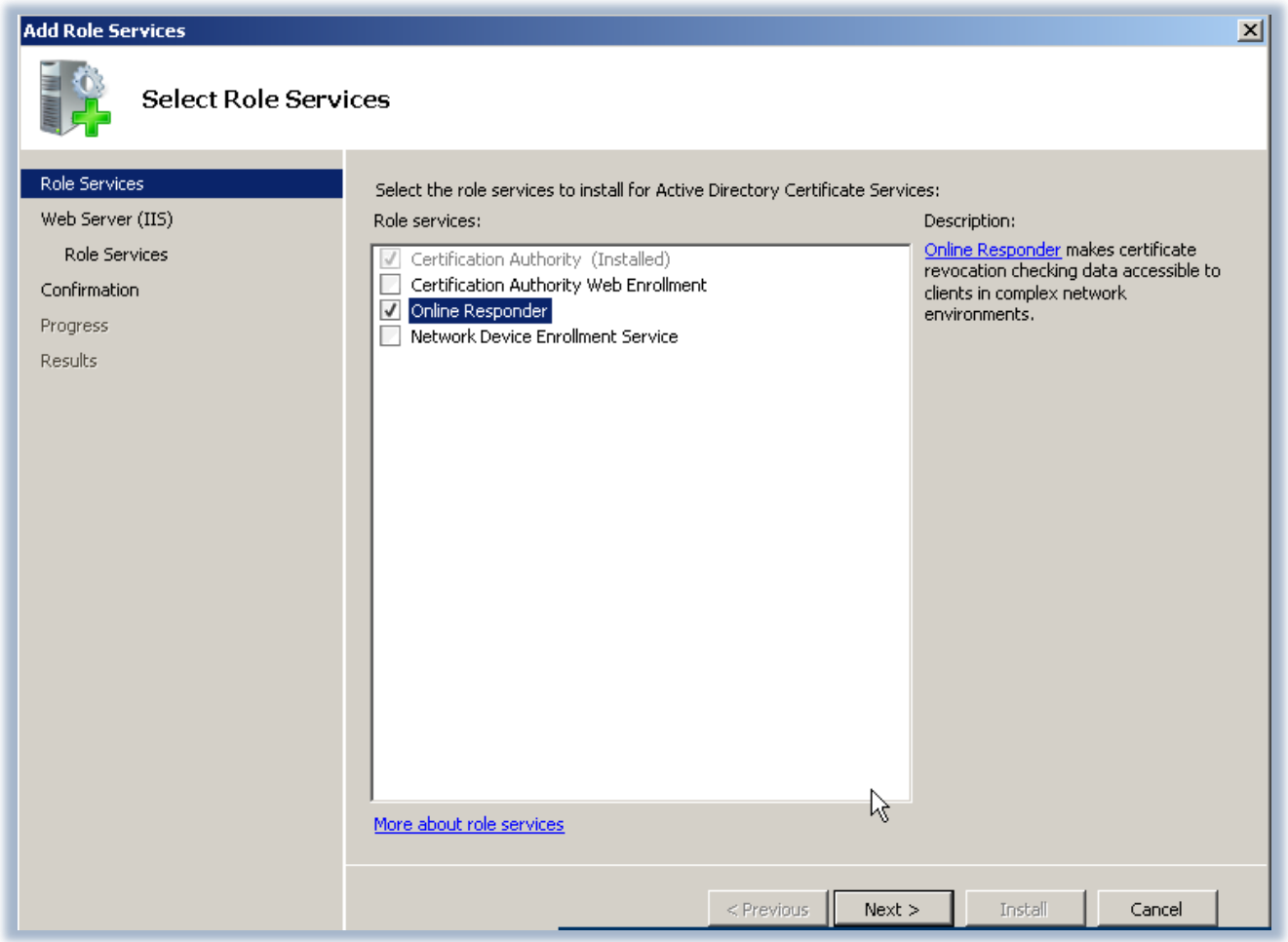

Figura 1 : Installazione del Role Service "Online Responder"

Dopo aver installato il servizio, è necessario configurare l'**Online Responder Certification Signing** utilizzando lo snap-in di gestione della Certification Authority. Scegliendo le proprietà della CA e navigando fino alla scheda **Extension**, scegliamo di configurare le AIA (**Authority Information Access**), cioè le posizioni dove gli utenti potranno reperire le informazioni sui certificati emessi dalla CA, come mostrato in figura 2.

Come si può vedere dalla figura, è possibile reperire queste informazioni in diversi modi, sia utilizzando il protocollo LDAP, sia il protocollo HTTP ed anche sotto forma di file da condividere in rete con gli utenti.

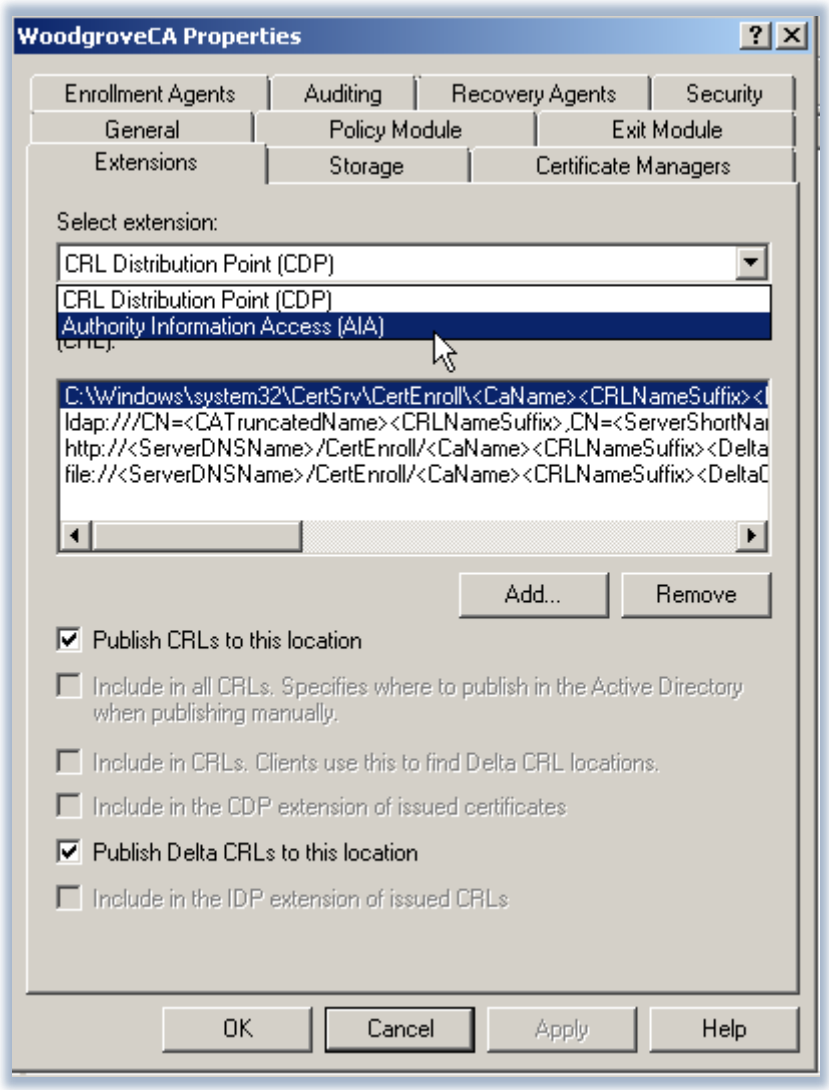

Figura 2: Modifica delle Extensions della CA

Aggiungiamo quindi una nuova location specificando il percorso del nostro Online Responder, il nome del server che ospita la CA e la directory virtuale in cui verranno pubblicate le informazioni sulle revoche, che è stata creata automaticamente al momento dell'installazione del servizio e che si chiama di default "ocsp".

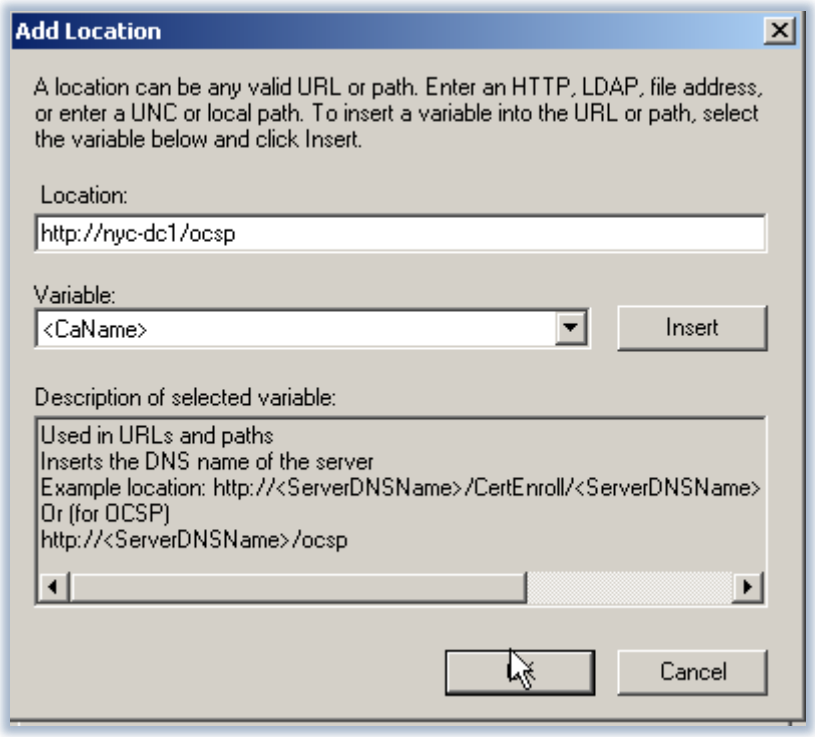

Figura 3: Modifica della location della Authority Information Access

Dopo aver riavviato il servizio della CA per rendere operative le modifiche, è necessario modificare il Template del certificato *OCSP Response Signing* in modo tale che tutti gli **Authenticated Users** possano fare l'Enroll del certificato, come mostrato in figura 4.

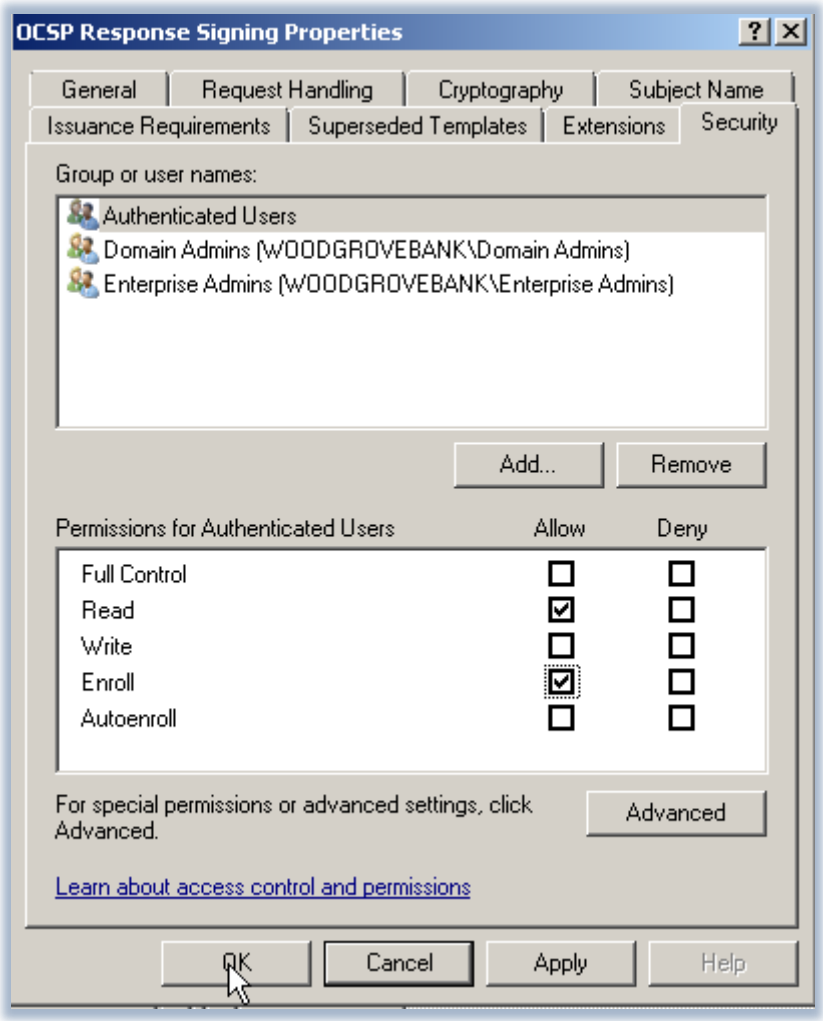

Figura 4: Propeirtà del Template del OCSP Response Signing

Abilitiamo il nuovo certificato creato facendo **l'Issue** del template. Il nuovo template verrà mostrato poi nella lista insieme a tutti gli altri Certificate Template gestiti dalla nostra CA, come mostrato in figura 5.

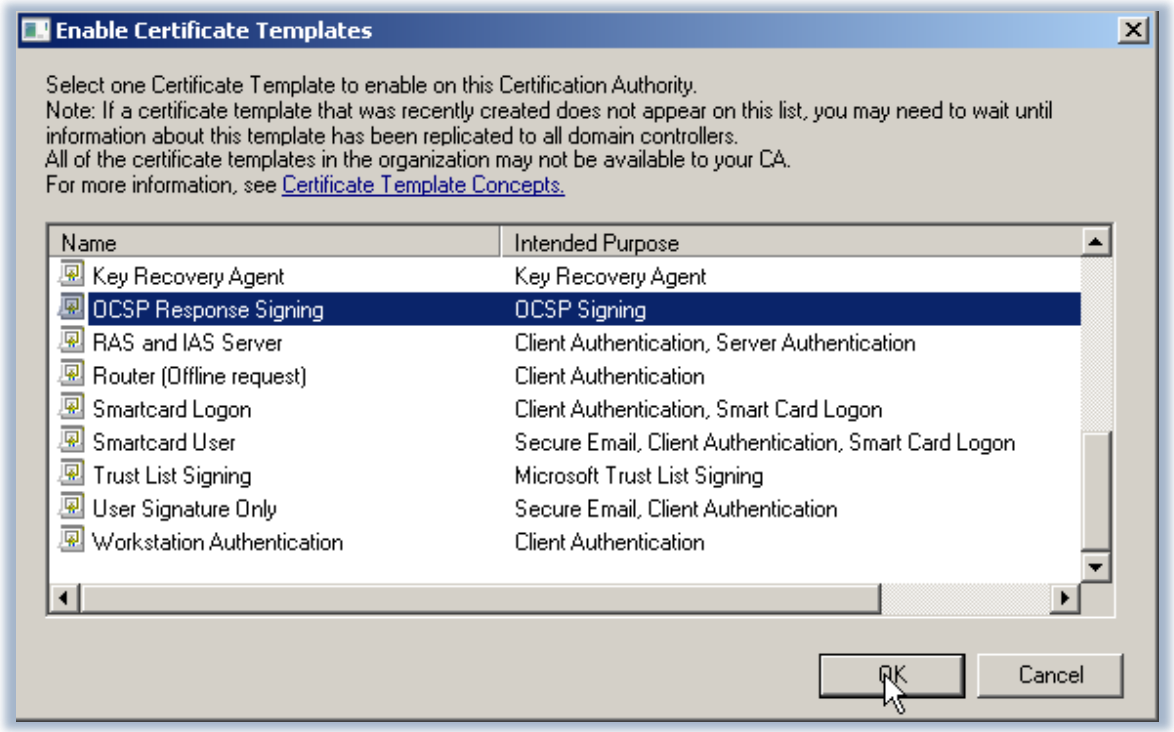

Figura 5: Abilitazione del Template OCSP

Da questo momento in poi possiamo gestire **l'Online Responder** utilizzando l'apposito snap-in che è stato creato al momento dell'installazione del servizio tramite il Server Manager, come mostrato in figura 6.

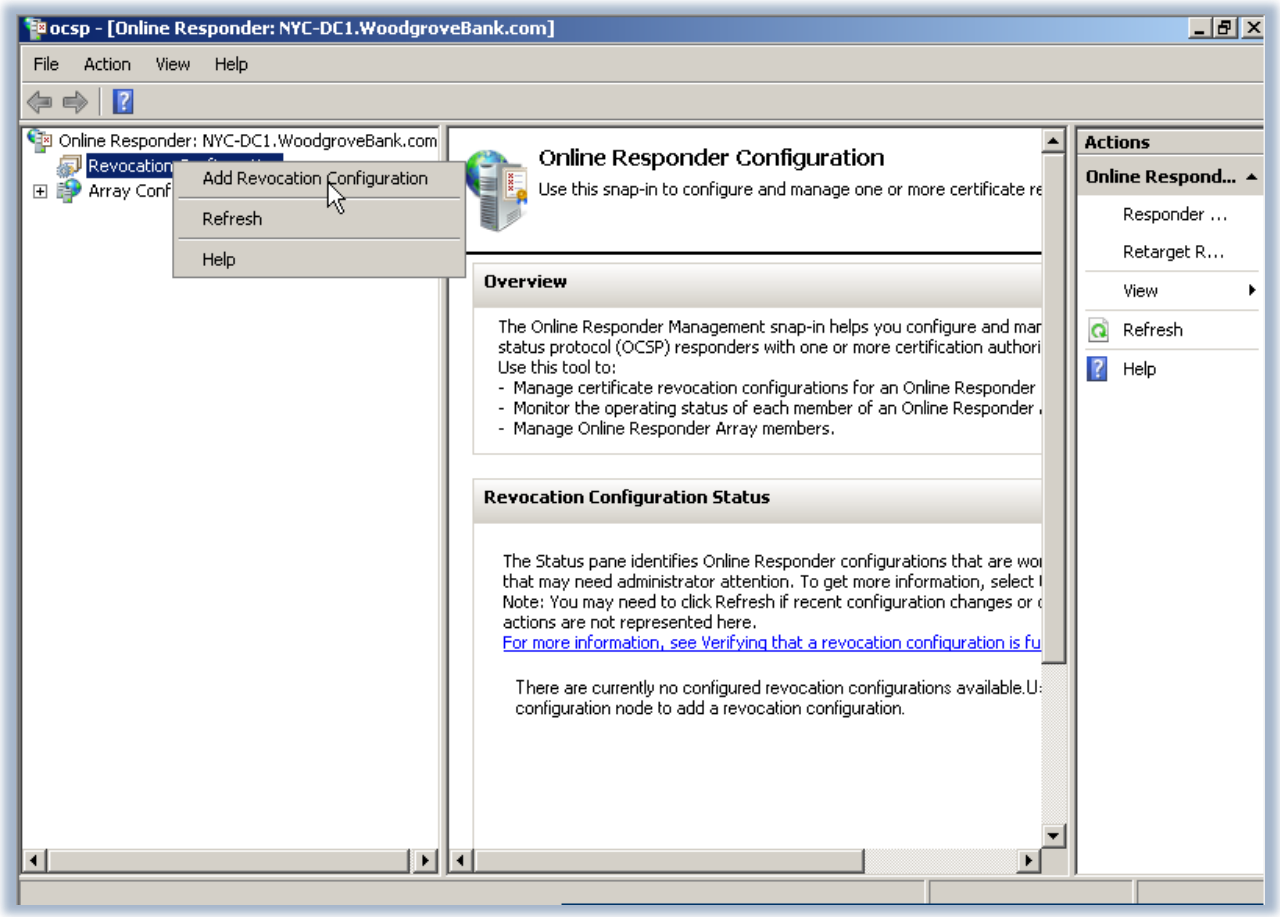

Figura 6: Snap-in di gestione dell'Online Responder

Aggiungiamo ora al nostro Online Responder la configurazione delle revoche facendo partire l'apposito wizard **Add Revocation Configuration**. Nella prima schermata del wizard inseriamo un nome per identificare la CA e nella schermata successiva specifichiamo la location del certificato della CA che vogliamo associare alla nostra Revocation Configuration, come mostrato in figura 7.

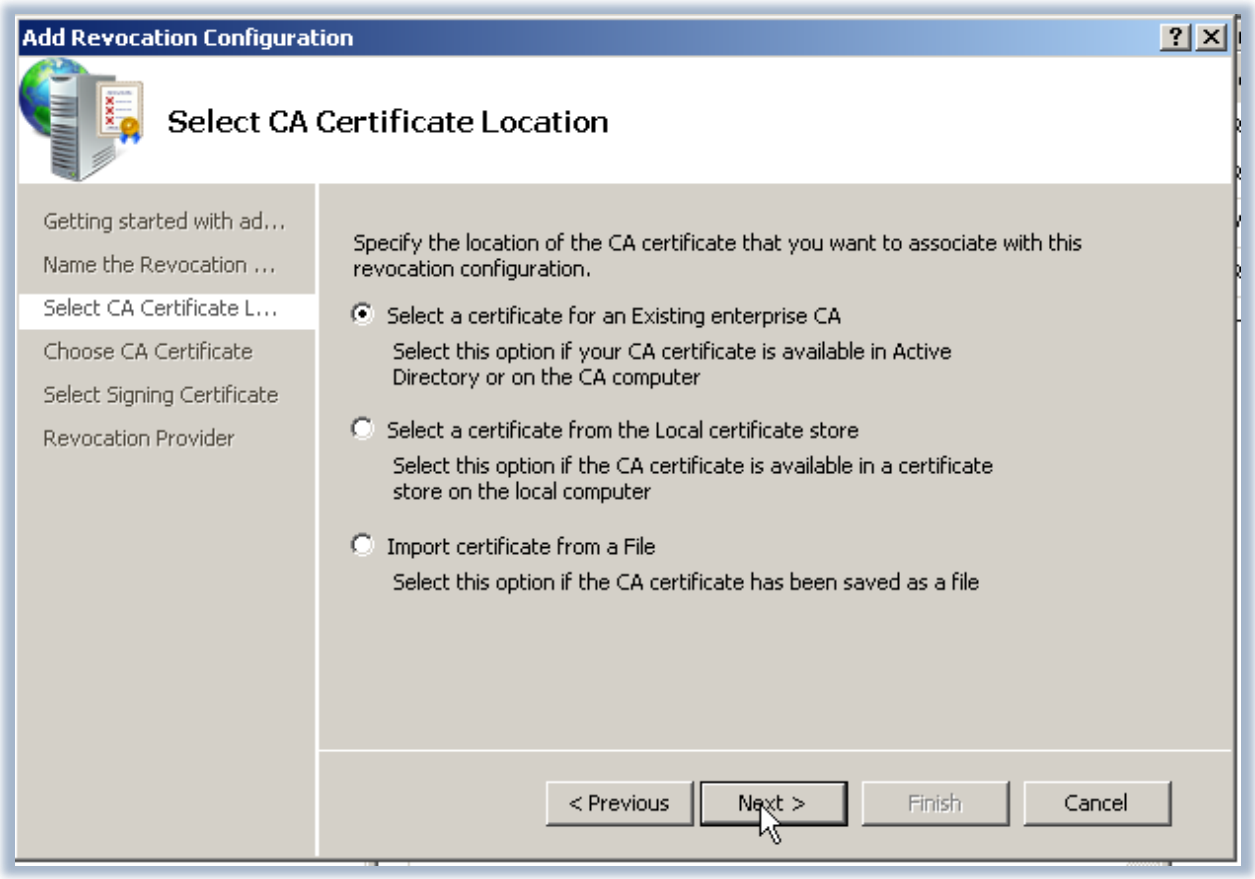

Figura 7: Scelta del certificato della CA

Nella schermata successiva facciamo il Browse del certificato relativo alla nostra CA cercando in Active Directory e scegliendo tra le CA disponibili, come mostrato in figura 8.

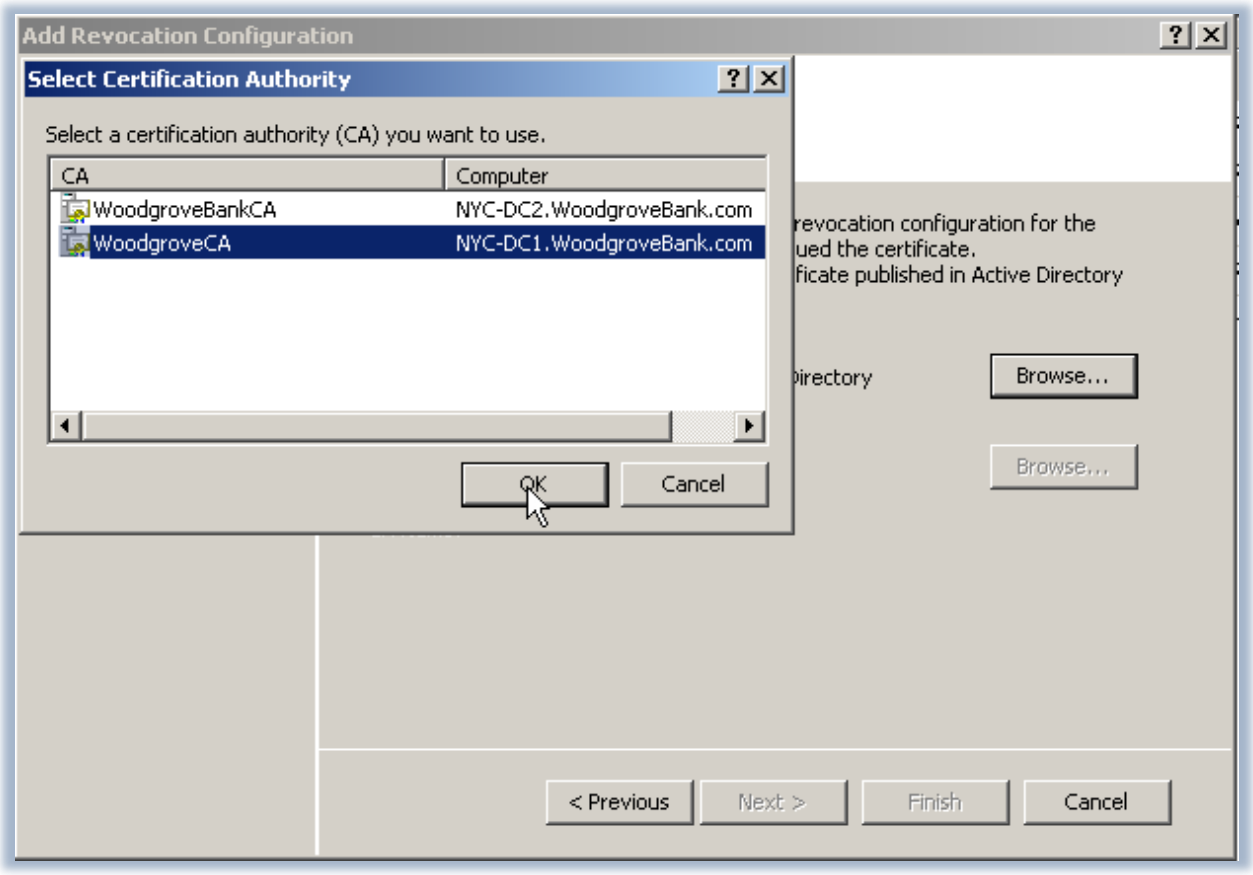

Figura 8: Scelta della CA da utilizzare per l'Online Responder

A questo punto il nostro Online Responder automaticamente farà l'Enroll del certificato che gli abbiamo indicato, come mostrato in figura 9.

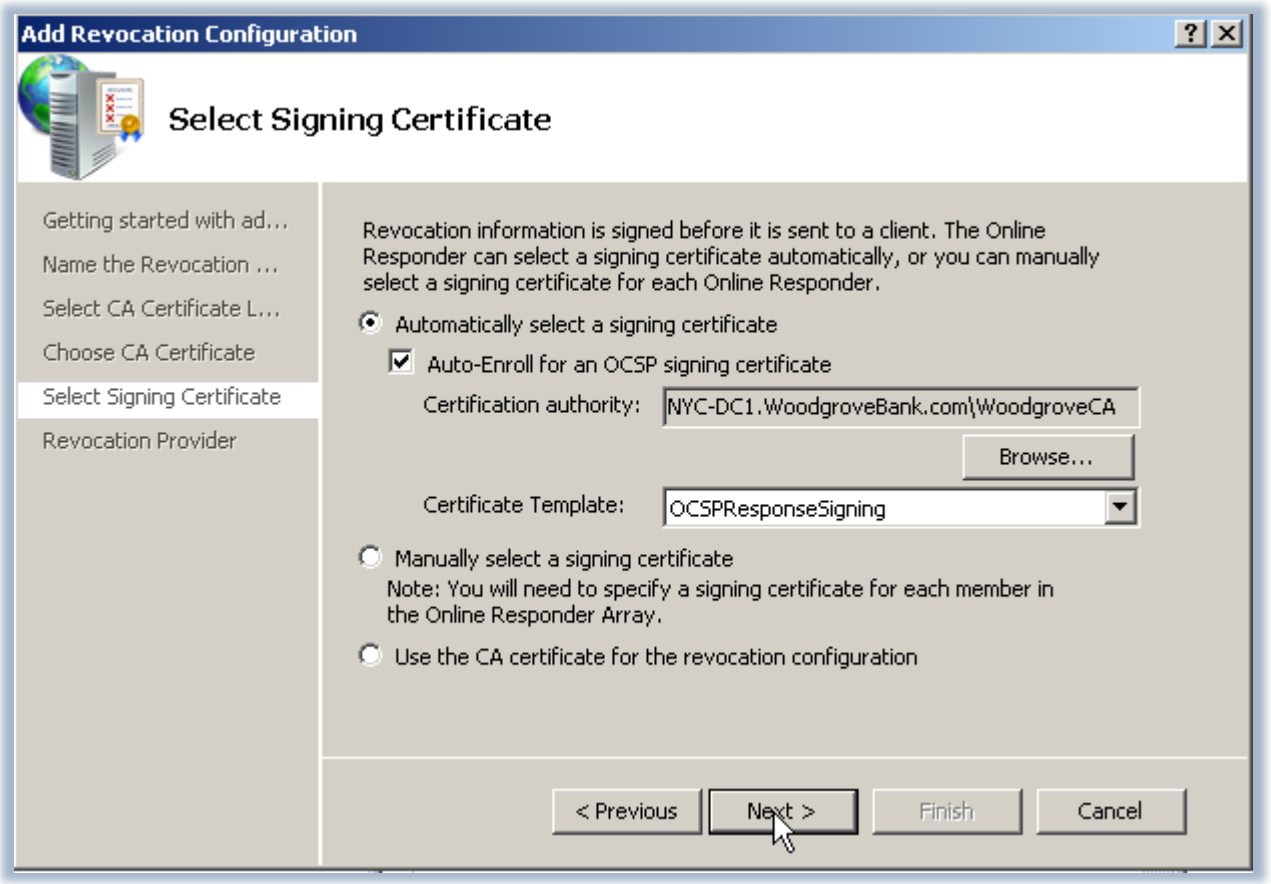

Figura 9: Enroll automatico del certificato indicato

Il **Revocation Provider** (cioè il componente dell'Online Responder che si occupa di processare le richieste sullo stato dei certificati) a questo punto viene inizializzato e può cominciare a rispondere alle richieste degli utenti, come mostrato in figura 10.

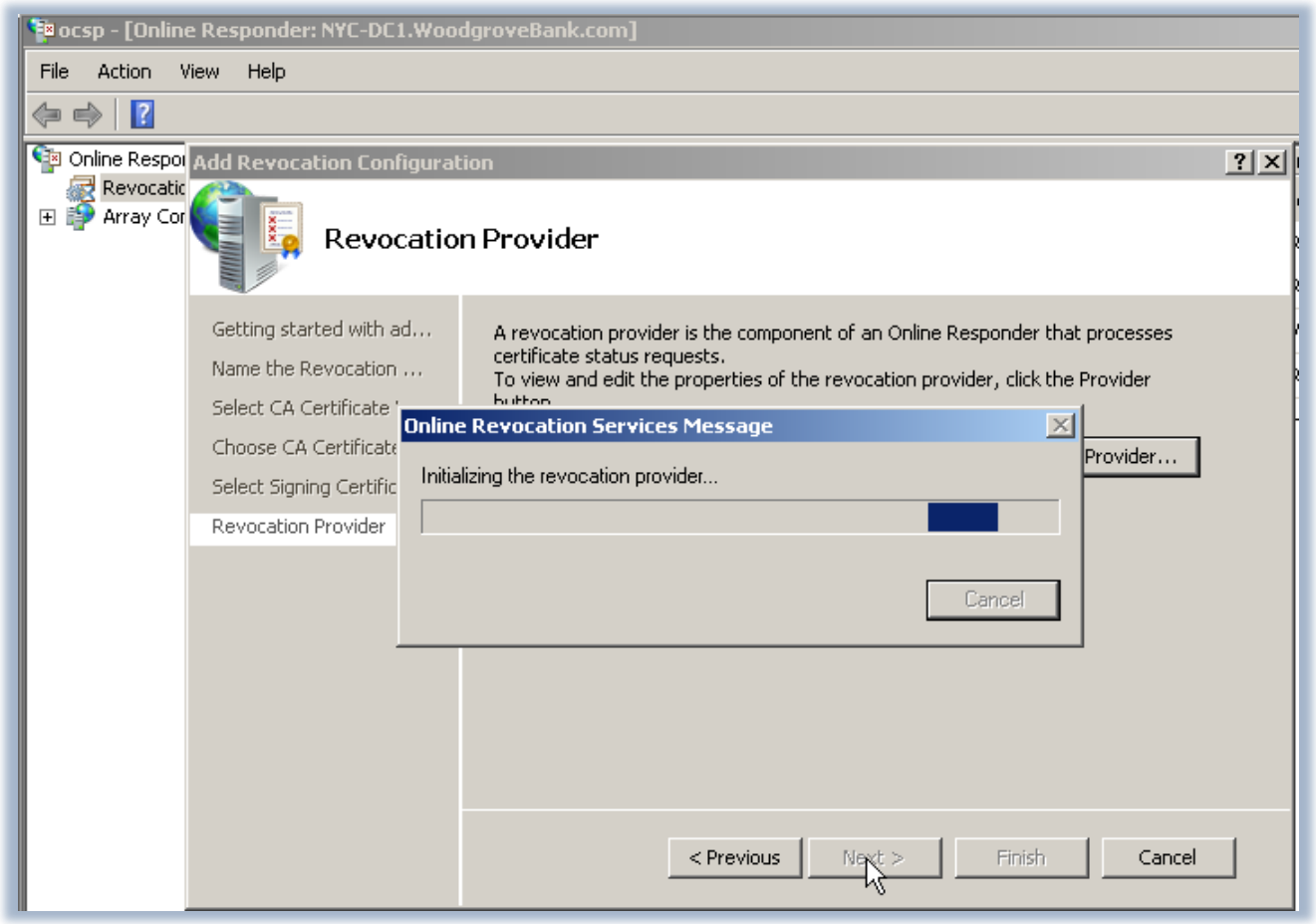

Figura 10: Inizializzazione del Revocation Provider

Un Online Responder può ricevere le liste CRL da più Certification Authority, come precedentemente indicato. Se si hanno diversi Online Responder è possibile configurare degli **Array** di più computer collegati tra di loro, in modo tale che possano tutti processare le richieste sullo stato dei certificati. I computer membri dello stesso array avranno le stesse configurazioni generali e le stesse configurazioni di revoca. Per ogni array dovrà essere inoltre definito un server che avrà il ruolo di **Array controller**. Questo server si occuperà di risolvere i conflitti di sincronizzazione tra i vari server dell'array e andrà ad applicare tutte le informazioni più aggiornate sulle configurazioni delle revoche.

I Browser che attualmente supportano il controllo OCSP sono:

- Internet Explorer 7 su Vista (non XP)
- Tutte le versioni di Firefox (Firefox 3 lo supporterà di default)
- Safari su Mac OS X

Conclusioni

Le due opzioni per pubblicare le informazioni sulle revoche dei certificati sono le CRL e l'Online Responder. Gli Active Directory Certificate Services di Windows Server 2008 permettono agli utenti di scaricare le CRL aggiornate oppure di utilizzare il nuovo Online Certificate Status Protocol (OCSP). Con la seconda opportunità è possibile velocizzare i tempi di risposta sui controlli da effettuare sulla revoca del singolo certificato, evitando i timeout creati dalle CRL o dalle Delta CRL.

Links

http://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol

http://technet2.microsoft.com/windowsserver2008/en/library/045d2a97-1bff-43bd-8dea-f2df7e270e1f1033.mspx?mfr=true