

Una generica autorità di certificazione (Certification Authority o più brevemente CA) è costituita principalmente attorno ad un pacchetto software che memorizza i certificati, contenenti le chiavi pubbliche degli utenti e firmati dall'autorità di certificazione, in una directory.

Nei sistemi Windows questo compito è affidato al componente Servizi certificati, la cui versione 1.0 è stata introdotta quale opzione aggiuntiva ad Internet Information Server con l'Option Pack di MS Windows NT 4.0.

Vediamo adesso quelle che sono le caratteristiche generali di una autorità di certificazione, dopo di che passeremo ad analizzare il funzionamento del componente Servizi certificati 2.0 ed a descriverne la procedura di installazione.

Per quanto riguarda la configurazione e gli aspetti operativi come il backup ed il ripristino, vi rimando alla lettura dell'ottima guida in italiano a corredo del prodotto.

Perchè utilizzare un'autorità di certificazione

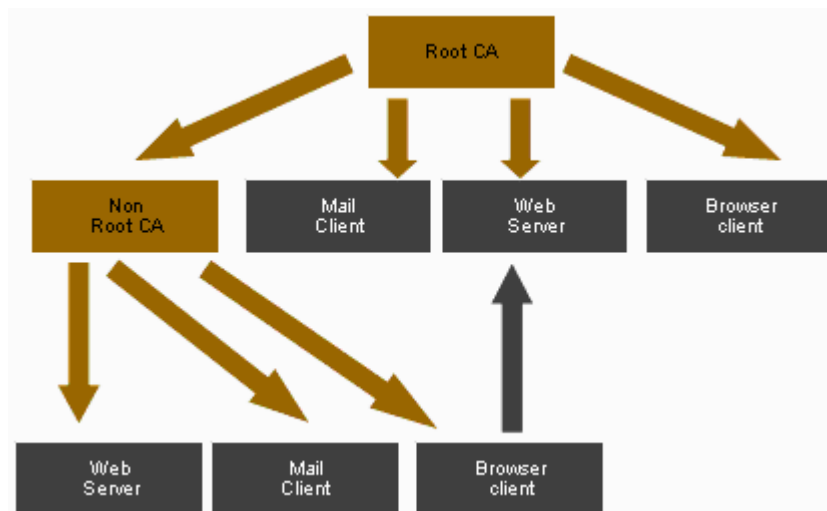
Se utilizzata con pacchetti software che ne sfruttano le potenzialità garantisce agli utenti che il mittente sia colui che dice di essere, che il destinatario sia la sola persona a poter leggere la posta e che il messaggio ricevuto corrisponda esattamente a quello inviato.

Un'autorità di certificazione è un'estensione logica di un centro di distribuzione di chiavi. Il centro di distribuzione delle chiavi fornisce la chiave pubblica degli utenti a chiunque ne faccia richiesta, non vi è un periodo di validità per la chiave, né l'utente è sicuro che la chiave sia realmente quella dell'utente richiesto. Quindi, un utente malintenzionato che cerca di rubare informazioni private potrebbe usare un attacco di tipo uomo nel mezzo per intercettare la vera chiave pubblica e sostituirla con la propria, permettendogli quindi di decifrare i dati.

L'autorità di certificazione elimina questi problemi. Invece di fornire chiavi pubbliche, l'autorità di certificazione distribuisce certificati. Questi certificati contengono un periodo di validità, prima e dopo del quale la chiave pubblica non può essere utilizzata per verificare una firma. Oltre a questo, il certificato viene firmato con la chiave privata dell'autorità di certificazione, facendo diventare il tutto difficilmente modificabile da un utente malintenzionato che voglia attuare l'attacco di tipo uomo nel mezzo.

Gerarchia delle autorità di certificazione

In base a quanto abbiamo visto è facile intuire che ogni autorità di certificazione verrà ad essere inserita in un suo ambito operativo o più in generale verrà ad occupare una delle due posizioni evidenziate in questo schema:



potremmo avere cioè autorità con funzione di radice di una gerarchia oppure come appartenenti ad una gerarchia esistente.

Certificati

In base al ruolo assegnato, l'autorità di certificazione è in grado di rilasciare diverse tipologie di certificati:

- **Certificati di CA:**
 - Utilizzati per validare altri certificati emessi dalla CA;
 - Devono essere caricati nel browser per validare un server.
- **Certificati server:**
 - Emessi da una CA per validare un server (che sia esso web o altro).
- **Certificati client:**
 - Emessi da una CA per validare un client (e-mail e browser)

Funzionamento

Il componente Servizi certificati si basa sull'uso di diversi elementi, in larga misura mediati dal mondo OSI.

X.500

Le specifiche di questa raccomandazione ISO sono nate dall'esigenza di facilitare la comunicazione e la cooperazione fra entità o oggetti, definiti nel senso generico del termine, residenti su una rete di comunicazione.

Le funzionalità X.500 permettono all'utente di indirizzare le entità utilizzando nomi mnemonici o convenzionali al posto dei complessi indirizzamenti di rete a cui tali oggetti vengono associati.

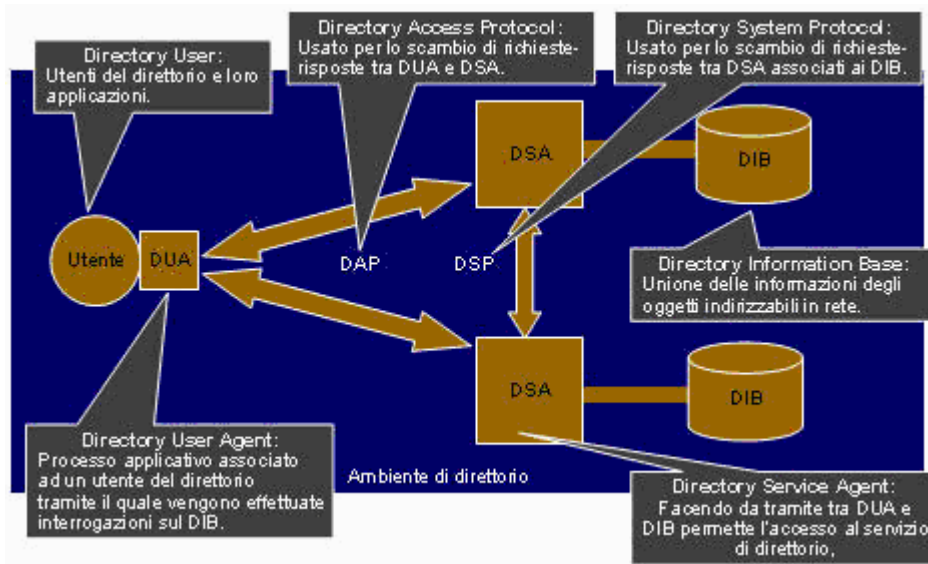
Un esempio di questa filosofia potrebbe essere facilmente dato da NETBIOS nel quale un sistema viene identificato univocamente da un nome mnemonico piuttosto che dal reale indirizzo utilizzato al livello trasporto.



In pratica, X.500 può essere considerato come un protocollo di comunicazione a livello applicativo, che è parte integrante dell'insieme dei protocolli OSI i cui servizi mettono a disposizione un archivio, associato ad un servizio di direttorio, orientato alla comunicazione, che riporta gli oggetti presenti nella rete, fornendo inoltre gli strumenti per attribuire loro un nome e la modalità per indirizzarli.

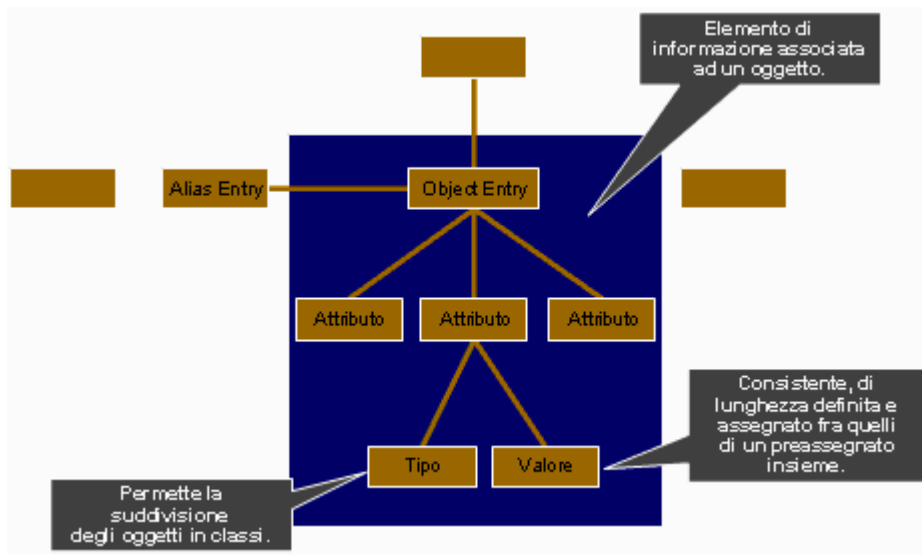
Modello di servizio: Directory Service

Vediamo ora schematizzati gli elementi costituenti un generico servizio di direttorio (Directory Service):



Directory Information Tree

Gli elementi contenuti all'interno delle DIB sono caratterizzati da questa struttura:



Servizio nome

All'interno della specifica X.500, la raccomandazione X.520 definisce il nome distinguente (Distinguished Name) come combinazione di quell'insieme minimo di attributi e delle loro associazioni (valori) che permettono l'identificazione univoca di una entry all'interno del DIT. Ad esempio:

```
c=IT, st=Genova, l=Chiavari, o=amagri.it, ou=Ricerca e sviluppo, cn=Antonio Magri
```

E' importante notare che la rappresentazione dell'oggetto deriva dall'uso corretto dello schema, ad esempio:

```
cn=Antonio Magri, ou=Accounting, o=amagri, c=IT
cn=Antonio Magri, o=amagri, ou=Ricerca e sviluppo, c=IT
```

rappresentano due oggetti differenti.

I principali attributi sono:

Attributo	Sintassi	Descrizione
country	c	Nazione all'interno della quale risiede il soggetto. Es.: C=IT
state	st	Stato o provincia di appartenenza. Es.: st=Genova
locality	l	Località di residenza del soggetto. Es.: l=Chiavari
common name	cn	Nome completo della persona o dell'oggetto definito dall'entry. Es.: cn=Antonio Magri cn=Amministratore di rete cn=Stampante di rete
organization	o	Organizzazione al quale il soggetto appartiene. Es.: o=amagri.it
organizational unit	ou	Unità all'interno dell'organizzazione. Es.: ou=Ricerca e sviluppo

Certificati X.509

I certificati X.509 vengono dichiarati utilizzando il linguaggio formale ASN.1 (Abstract Syntax Notation 1, è utilizzato per specificare strutture dati ed ha una sintassi simile al Pascal) e prevedono l'utilizzo di uno schema di codifica a chiave pubblica combinato con il sistema delle firme digitali.

Da notare che l'algoritmo RSA, per le chiavi pubbliche, è raccomandato, ma non strettamente richiesto. Vediamo ora la struttura di un generico certificato:

VERSIONE
NUMERO DI SERIE
IDENTIFIC. ALGORIT.
FORNITORE
PERIODO VALIDITA'
OGGETTO
INFO CHIAVE PUB.
FIRMA

- **Versione:** Rappresenta la versione del formato del certificato; il valore predefinito è il formato del 1988.
- **Numero di serie:** E' il numero univoco assegnato al certificato dell'utente dall'autorità di certificazione.
- **Identificatore dell'algoritmo:** Indica l'algoritmo utilizzato per firmare il certificato e tutti i parametri associati.
- **Fornitore:** E' l'autorità di certificazione che ha rilasciato e firmato il certificato.
- **Periodo di validità:** Il periodo di validità è indicato da due date; il certificato non è valido, né prima della prima data, né dopo la seconda.
- **Oggetto:** E' l'utente a cui è stato rilasciato il certificato.
- **Informazioni sulla chiave pubblica:** E' la chiave pubblica dell'utente, insieme con un identificatore che indica l'algoritmo per il quale si utilizza la chiave stessa.
- **Firma:** Message Authentication Code (MAC). Deriva dall'applicazione di una funzione hash (usando come algoritmo o SHA-1 o MD-5) non invertibile a tutti i campi del certificato, a parte quello della firma, e dalla successiva codifica del risultato utilizzando la chiave privata dell'autorità di certificazione.

Qualsiasi utente può decodificare la firma utilizzando la chiave pubblica dell'autorità di certificazione.

La firma elettronica ha lo scopo di autenticare l'autorità di certificazione che ha rilasciato il certificato assicurando che il certificato sia stato veramente rilasciato dall'autorità di certificazione indicata.

I certificati X.509 rilasciati dall'autorità di certificazione vengono memorizzati nella directory X.500 in questo modo qualsiasi utente può accedere alla directory X.500 e ottenere la chiave pubblica di un altro utente.

E' compito dell'autorità di certificazione verificare la validità dei certificati, aggiornare l'elenco dei certificati revocati e utilizzare queste informazioni per aggiornare la directory X.500.

Un certificato può essere revocato prima della scadenza quando:

- La sicurezza della chiave privata dell'utente o dell'autorità di certificazione è stata in qualche modo compromessa;
- L'utente non è più certificato dall'autorità di certificazione corrente.

I certificati X.509 vengono utilizzati da Privacy-Enhanced Mail (PEM), Pretty Good Privacy (PGP), Secure Sockets Layer (SSL) e Secure HyperText Transfer Protocol (S-HTTP)

Liste revoca certificati

Le CRL sono liste di certificati che non sono più validi perché la chiave privata che li accompagna viene persa, rubata o compromessa. Quando un utente si accorge che la propria chiave privata è compromessa, lo notifica all'autorità di certificazione che aggiunge il certificato alla CRL. In questo modo, in caso di furto, un utente che si spaccia come legittimo non sarà validato quando cercherà di utilizzare la chiave privata per firmare un documento.

Installazione

L'installazione del componente Servizi certificati presuppone che siano state effettuate in precedenza alcune procedure:

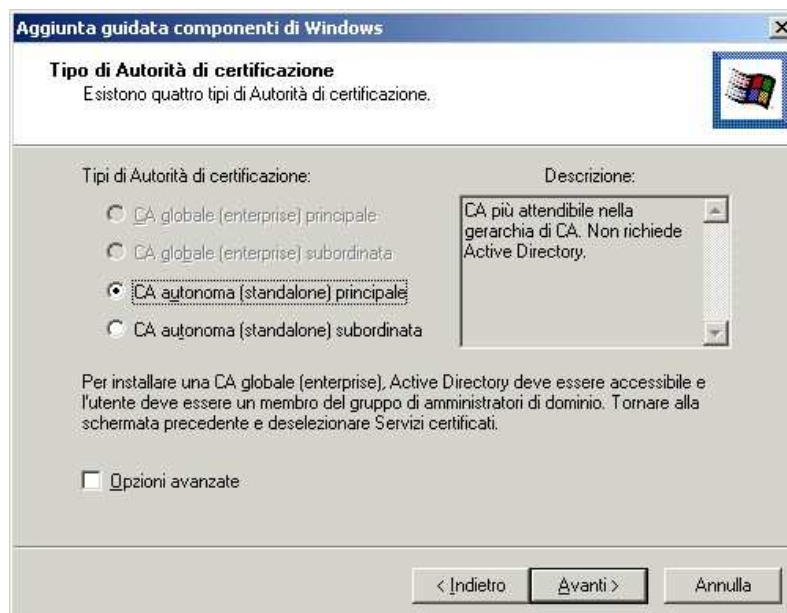
- **Creazione della cartella che conterrà i certificati ed i file di configurazione:** la cartella deve avere impostato il permesso di accesso in lettura per tutti e deve risiedere obbligatoriamente nel sistema che ospiterà il servizio;
- **Installazione di Internet Information Services:** necessario per le operazioni di verifica degli elenchi CRL e per l'utilizzo dell'interfaccia web rivolta all'utente.

Una volta creata la cartella ed installato IIS, si passerà ad installare il componente Servizi certificati.

Per fare questo, dopo aver fatto clic su start, scegliere Impostazioni e quindi Pannello di controllo. Fare doppio clic su Installazione applicazioni ed avviare l'Aggiunta guidata componenti Windows.

In questa selezionare la casella di controllo Servizi certificati. Verrà visualizzato un messaggio di avviso che ci ricorderà che una volta installato il servizio non sarà più possibile modificare il nome e l'appartenenza al dominio del sistema. Confermare l'operazione e quindi selezionare Avanti.

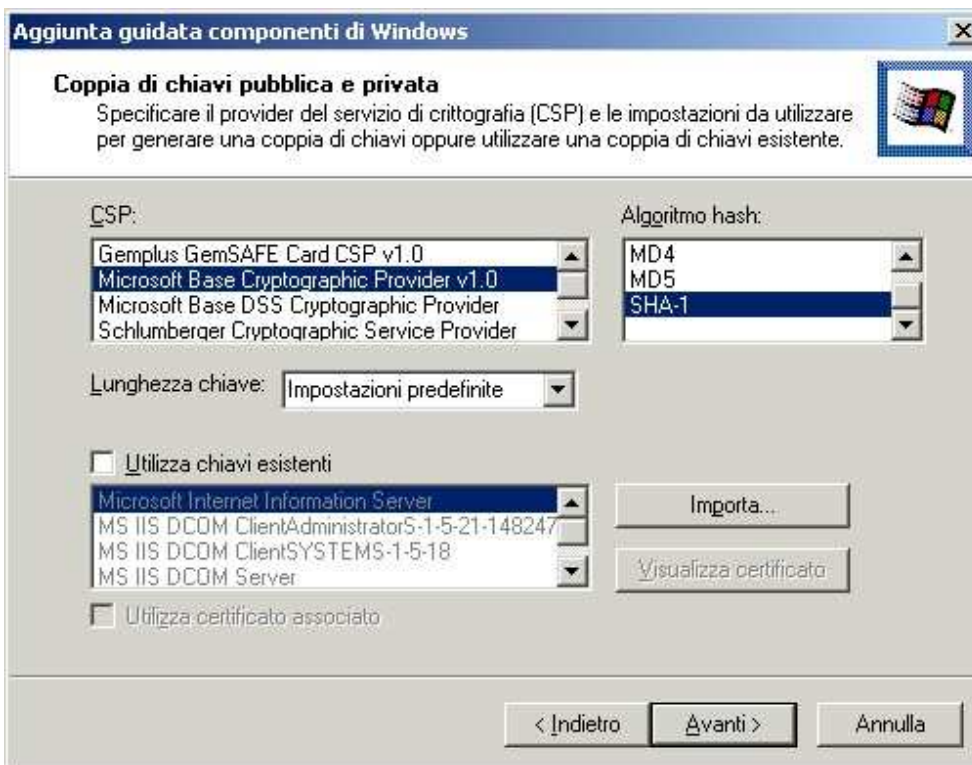
La procedura guidata ci chiederà di scegliere tra le possibili tipologie di autorità di certificazione:



E' possibile configurare il componente Servizi certificati secondo una delle modalità seguenti:

- **CA globale (enterprise) principale:** rappresenta la radice di una eventuale gerarchia di autorità **interna** all'organizzazione. Il servizio sfrutta Active Directory e richiede la presenza di un dominio.
- **CA globale (enterprise) subordinata:** si inserisce come membro subordinato in una gerarchia **interna** esistente previo ottenimento del relativo certificato di CA da parte della autorità di livello superiore. Anche questa opzione richiede la presenza di Active Directory.
- **CA autonoma (standalone) principale:** rappresenta la radice di una eventuale gerarchia di autorità **esterna** all'organizzazione. Il servizio non sfrutta Active Directory e non richiede la presenza di un dominio.
- **CA autonoma (standalone) subordinata:** si inserisce come membro subordinato in una gerarchia **esterna** esistente previo ottenimento del relativo certificato di CA da parte della autorità di livello superiore.


Nel nostro caso, visto che non è stata rilevata la presenza di Active Directory, saranno selezionabili solo le due modalità che non ne fanno uso. Scegliamo quella principale, quindi spuntiamo Opzioni avanzate e clicchiamo su Avanti. Ci comparirà la finestra di configurazione delle opzioni avanzate:



In questa abbiamo la possibilità di:

- **scegliere il provider crittografico da utilizzare (CSP):** predefinito Microsoft Base Cryptographic Provider;
- **decidere la lunghezza della chiave:** utilizzando il provider predefinito (Microsoft Base Cryptographic Provider) la lunghezza predefinita della chiave è di 512 bit. Per una CA principale la lunghezza della chiave deve essere di almeno 2048 bit. Questa opzione non è disponibile se si utilizzano chiavi già esistenti;
- **cambiare l'algoritmo di hash usato:** algoritmo predefinito SHA-1;
- **utilizzare o importare ulteriori chiavi e relativi certificati:** permette di riutilizzare coppie di chiavi esistenti invece di generarne di nuove. Utile durante la procedura di ripristino.

Una volta effettuate le nostre scelte, proseguiamo con Avanti. Nella finestra successiva di verranno chiesti i dati di identificazione della CA:



Aggiunta guidata componenti di Windows

Informazioni identificazione Autorità di certificazione (CA)
Immettere le informazioni per identificare la CA

Nome CA: amagriCA

Organizzazione: amagri

Unità organizzativa: Ricerca e sviluppo

Città: Chiavari

Provincia: Genova Paese: IT


Posta elettronica: info@amagri.it

Descrizione CA: CA di esempio

Valida: 2 anni Scade: 13/07/2005 15.40

< Indietro Avanti > Annulla

dopo aver riempito i campi a nostra disposizione, facendo particolare attenzione al nome della CA ed alla durata temporale della chiave (opzione modificabile solo all'interno di una installazione CA principale), scegliendo Avanti, ci verrà visualizzata una nuova finestra con la possibilità di definire la posizione di archiviazione dei dati:



Aggiunta guidata componenti di Windows

Posizione di archiviazione dei dati
Specificare la posizione di archiviazione per i dati di configurazione, database e registro

Database certificati: C:\WINNT\System32\CertLog Sfoglia...

Registro database certificati: C:\WINNT\System32\CertLog Sfoglia...

Archivia le informazioni di configurazione in una cartella condivisa
Cartella condivisa: C:\CACconfig Sfoglia...

Mantieni database certificati esistenti

< Indietro Avanti > Annulla

L'opzione di archiviazione in una cartella condivisa può essere deselezionata se si utilizza il servizio Active Directory ma rappresenta l'unica possibilità per pubblicare i certificati in tutti gli altri casi.

Installando una CA nella stessa posizione di una CA installata in precedenza, la casella di controllo Mantieni database certificati esistente risulterà selezionata per impostazione predefinita.

Una volta configurate le opzioni a nostra disposizione, selezioniamo Avanti. Visto che è necessario installare i componenti web, e solo se Microsoft Internet Information Services (IIS) è installato, verrà visualizzata una finestra di dialogo in cui se ne chiede l'interruzione. Fare clic su OK.

Verrà visualizzata la finestra di dialogo Installazione componenti in corso. Attendere il completamento dell'installazione quindi fare clic su Fine.

Verifica dell'installazione

Per verificare l'installazione di Servizi certificati, eseguire una delle operazioni seguenti:

- Al prompt dei comandi digitare net start e quindi verificare che Servizi certificati sia in esecuzione. È il modo più semplice per verificare che il servizio sia installato correttamente.
- Per una CA globale, fare clic sul pulsante Start, scegliere Programmi, quindi Strumenti di amministrazione e infine Gestione certificati per avviare l'applicazione e quindi richiedere un certificato.
- Per una CA autonoma, richiedere un nuovo certificato utilizzando Microsoft Internet Explorer per connettersi all'indirizzo <http://<indirizzo CA>/certsrv>