4u S.r.l.

4Sign

Suite di Firma Digitale

4Sign è un prodotto software orientatato a gestire il ciclo completo di firma digitale basata sui certificati X.509, in termini di:

1. gestione di una **Registration Authority centrale**, eventualmente interoperante con una Struttura Anagrafica centrale di licenze e utenti;
2. gestione di una o piú **Certification Authorithy centrali**, interoperanti con la Registration Authority ed eventualmente con la Struttura Anagrafica;
3. gestione delle **attivitá di richiesta, acquisizione e gestione** locale dei **certificati X.509 degli utenti** operanti all'interno di una licenza;
4. gestione delle **attivitá di firma dei documenti e di verifica dei documenti firmati**, con l'utilizzo di certificati X.509, sia su dispositivi hardware (SmartCard, eToken) che su dispositivi software.

4Sign è costituito da:

- un Database centrale di Registration e Certification Authority (RA/CA-DB)
- un Web di amministrazione di RA/CA-DB
- un insieme di CGI per la gestione on-line del Client di Gestione dei Certificati
- un Client di Gestione dei Certificati
- un Client di Firma Digitale
- un insieme di Librerie Dinamiche (server e client) per la gestione crittografica dei certificati

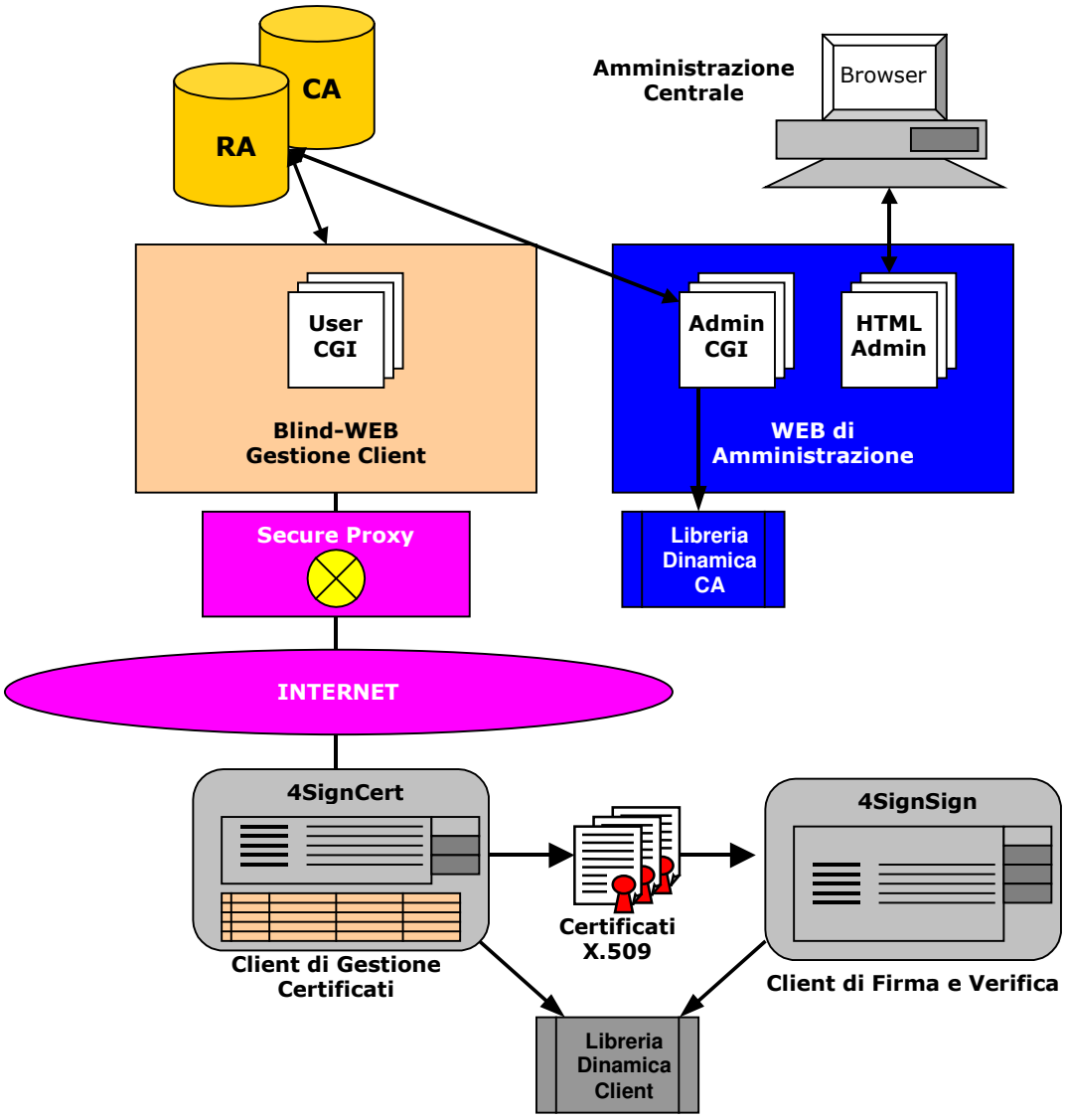
Il database centrale RA/CA-DB (utilizzato sia per le operazioni di amministrazione centrali che per il supporto delle operazioni degli utenti per la richiesta e l'emissione di certificati) è organizzato in più sezioni:

- Tabelle Operatori (operatori, profili, log)
- Tabelle di RA (licenze, ruoli, utenti)
- Tabelle di Supporto RA (nazioni, regioni, province, comuni)
- Tabelle di CA (CA, policy, ruoli, richieste, certificati, CRL)
- Tabelle degli Eventi (eventi, codici)

4Sign è una infrastruttura **multi-CA**, in grado di gestire in outsourcing strutture RA/CA di firma per conto terzi, o comunque di differenziare le *line* applicative interne ad una azienda (commerciali, finanziarie, produttive, …) che richiedono strutture di RA/CA personalizzate.

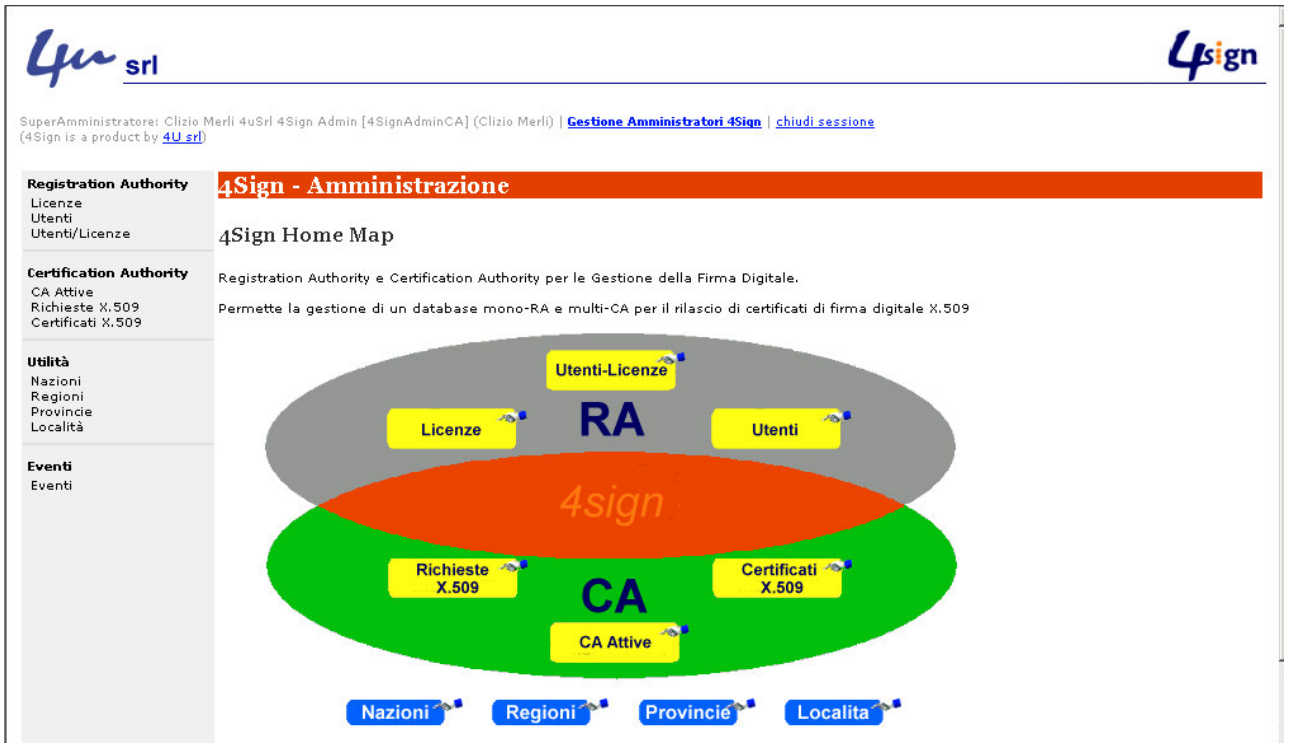
Ogni entità esterna gestita in outsourcing e/o ogni *line* applicativa interna viene identificata da 4Sign mediante una **Licenza**, ovvero di un **Gruppo Chiuso di Utenza**. All'interno di ogni Gruppo 4Sign gestisce una o più CA. 4Sign è quindi orientato alla **certificazione degli utenti nell'ambito di Gruppi Chiusi di Utenza** (Licenze) per la **gestione della firma digitale** dei documenti.

La **Registration Authority di 4Sign è unica**, in quanto i compiti di notarizzazione affidati ad una RA sono indipendenti dalle CA gestite e dai relativi gruppi. Per contro 4Sign gestisce **differenti CA per la singola RA** nell'ambito di un unico database centrale, identificando le singole CA in base ad un codice identificativo univoco. 4Sign non certifica gli utenti finali se non sono associati ad un gruppo chiuso di utenza (licenza).



4Sign: Architettura Generale e Componenti

Il sito **Web di Amministrazione di RA/CA** è accessibile solo a livello centrale in modalità protetta (https), con il supporto di certificati di navigazione sia server che client. I certificati di navigazione client sono utilizzati dal sito per autenticare e autorizzare gli operatori centrali (amministratori), in base alle relative profilature funzionali.

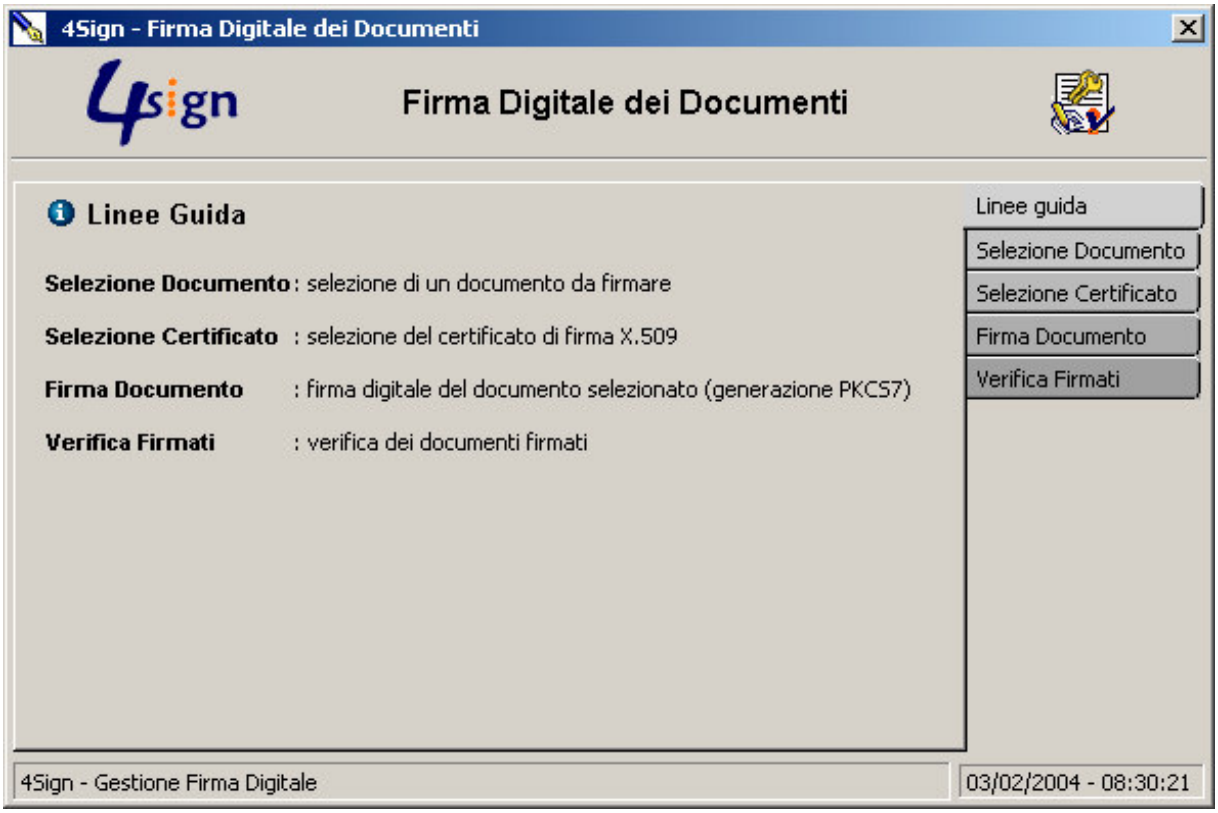


Il **Client di Gestione dei Certificati** è un pannello grafico che permette all'utente di:

- preparare le richieste dei certificati per gli utenti associati a una licenza (con il supporto del RA/CA-DB tramite le User-CGI), con il supporto dei dispositivi crittografici locali, sia software che hardware;
- trasmettere le richieste di certificazione al centro per la firma;
- ricevere dal centro i certificati X.509 firmati da una CA;
- registrare localmente i certificati X.509 firmati (unitamente alle rispettive chiavi segrete e ai certificati della CA firmataria) nei dispositivi crittografici locali;
- esportare i certificati X.509 di firma debole in formato PKCS12.

Il **Client di Firma e Verifica** è un pannello grafico che permette all'utente remoto di:

- selezionare e visionare i documenti da firmare;
- selezionare e verificare il certificato X.509 di firma dai dispositivi crittografici locali;
- effettuare la firma digitale del documento selezionato con il certificato selezionato e con il supporto del relativo dispositivo crittografico;
- verificare i documenti firmati, estraendo i documenti originali dopo la verifica;
- visualizzare i documenti verificati.



Approccio OpenSource

I componenti client e server di 4Sign sono stati sviluppati con l'obiettivo della piena e completa portabilitá su differenti piattaforme. Di conseguenza sono stati adottati per lo sviluppo vari tool opensource, selezionati per essere interoperativi con differenti piattaforme (Unix, Microsoft Win32, in futuro MacOS). In particolare, per quanto riguarda Microsoft Windows, l'unico punto di riferimento è l'interfaccia Win32, comune a tutte le versioni di Windows.

I tool opensource adottati per lo sviluppo dei client 4Sign sono:

Apache Web Server opensource.

PHP package opensource che opera come Application Server associato ad Apache (per la realizzazione del sito di Amministrazione centrale, Admin-CGI).

FOX package opensource C++ di gestione dei pannelli grafici (opera in ambiente Unix, MacOs, Win32).

cURL package opensource C++ di gestione della comunicazione client/server tra il Client di Gestione dei Certificati e le CGI (UserCGI) che operano al centro (RA/CA) sotto il controllo di un server WEB: opera come client HTTP (porta 80) o HTTPS (porta 443).

eCGI (easy CGI) package opensource C++ di supporto alla implementazione delle UserCGI di accoglienza alle richieste del Client di Gestione dei Certificati: permette tra l'altro la facile gestione delle funzioni di upload, che potranno essere richieste nelle future versioni del Client di Firma Digitale per tasmettere al centro i file firmati.

OpenSSL package opensource C per la gestione della crittografia e dei certificati X.509.

NSS-Mozilla package opensource C per la gestione della crittografia e dei certificati X.509 con interfaccia PKCS11 verso i dispositivi di gestione dei certificati (Token).