

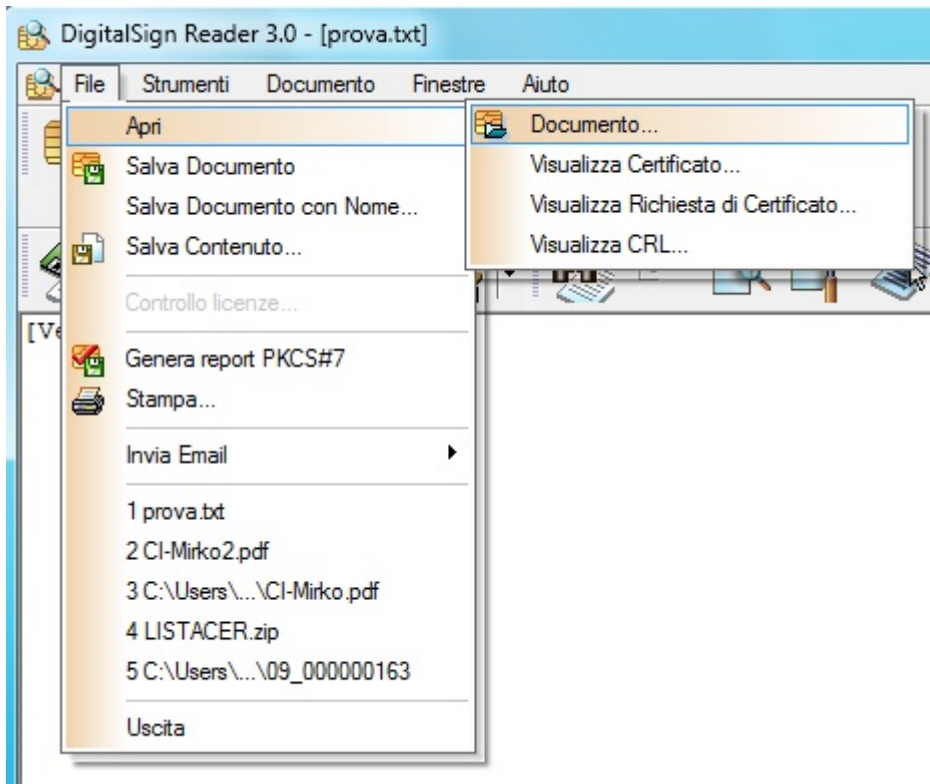
Verifica delle firme elettroniche

La mail che il cliente riceve quando vengono recapitati i RDP contiene due tipologie di files: i file pdf, e i file pdf.p7m, ciascun rapporto di prova sarà fornito in entrambi i formati. Il primo

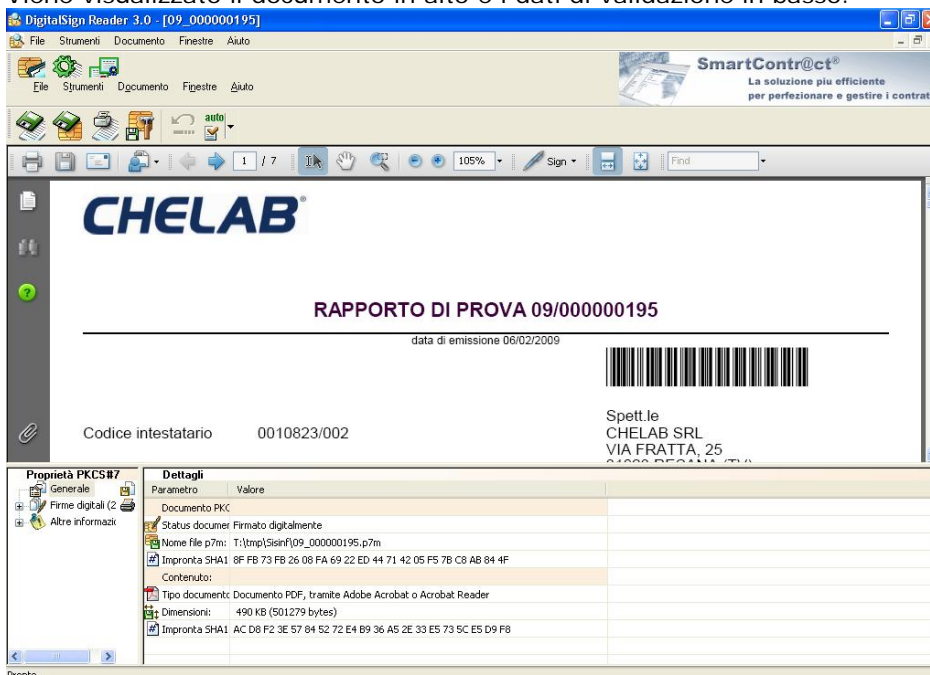
Il formato p7m è il formato tipo dei documenti con firma elettronica e può essere immaginato come una busta nel quale vengono messi il file pdf e le sue firme digitali.

Per aprire il file p7m occorre installare sul vostro sistema uno dei programmi freeware che servono allo scopo, nel nostro caso, a scopo esemplificativo, utilizzeremo DigitalSign Reader della Comped.

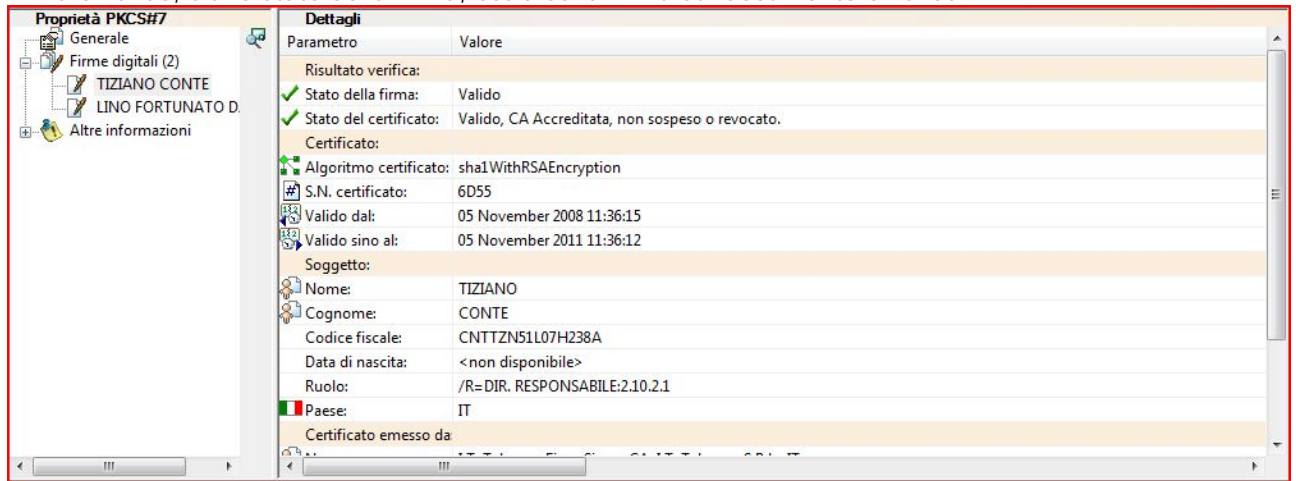
- 1) Attivare il programma
- 2) Aprire il file



Viene visualizzato il documento in alto e i dati di validazione in basso.



- 3) Eseguire la verifica (in alcuni software, come DigitaSign, è automatica quindi non serve)
- 4) Visualizzare le firme
Sul riquadro in basso a destra dove ci sono le "Proprietà PKCS#7", premere l'icona [+] a sinistra della dicitura "Firme digitali"
- 5) Visualizzare la verifica
Sul riquadro a destra compaiono gli stati di verifica lo stato del certificato, ossia se il certificato di firma è valido, sia lo stato della firma, ossia se la firma sul documento è valida.



La verifica avviene combinando le firme apposte sul documento con i certificati di chiave pubblica che vengono reperiti dal software di lettura. La verifica può dare esito negativo generalmente per i seguenti motivi:

- 1) Non sono reperibili i certificati di chiave pubblica dei firmatari dal software di lettura
- 2) I certificati di firma dei firmatari sono scaduti
- 3) I certificati di firma sono stati stati revocati
- 4) Il documento è stato manomesso

Non sono reperibili i certificati di chiave pubblica dei firmatari dal software di lettura

Il software generalmente accede ad un database dove sono memorizzate le chiavi pubbliche dei firmatari. Quindi utilizza queste chiavi per verificare le firme. Il reperimento dei certificati con le chiavi pubbliche necessarie può avvenire in due modi:

- Via internet
- Importazione manuale

Via internet

Ad esempio DigitalSign richiede all'avvio di reperire da Internet l'elenco dei certificatori accreditati (gli enti autorizzati dal CNIPA a rilasciare certificati di firma digitale) e delle liste di revoca, che sono le liste pubbliche dei certificati che, per qualsiasi motivo, sono stati revocati dal certificatore.

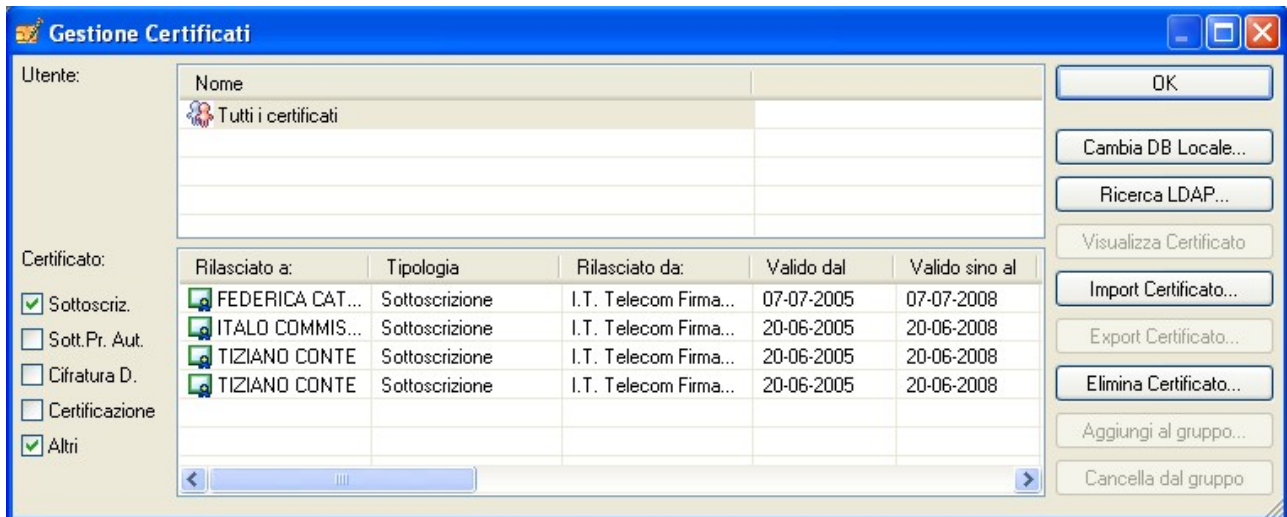
In questo modo la verifica delle firme non passa per il database locale dei certificati di firma ma utilizza internet per fare le opportune verifiche.

Importazione manuale

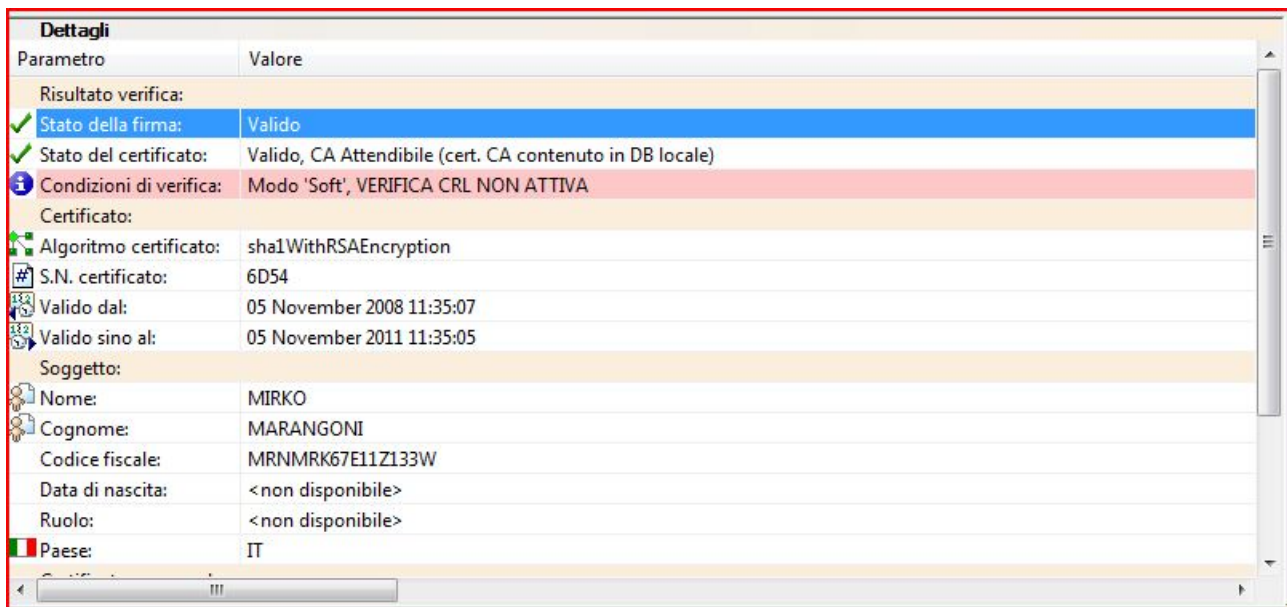
Dai link in basso è possibile scaricare i certificati di firma in uso in Chelab srl per importarli sul DB locale dei certificati del software di lettura. Ad esempio, aprendo DigitaSign e accedendo alla voce "Gestione DB locale dei certificati" è possibile importare i file .cer scaricati utilizzando il bottone a destra "Import certificato" e selezionando i file .cer scaricati.

I file .cer possono anche essere mandati via mail.

Ad esempio, per visualizzare le chiavi importate su DigitalSign Reader, ci si posiziona sul menù a discesa Strumenti, e si accede alla voce "Gestione DB locale dei certificati" nel quale sono evidenziati i certificati che sono stati importati nel database locale.

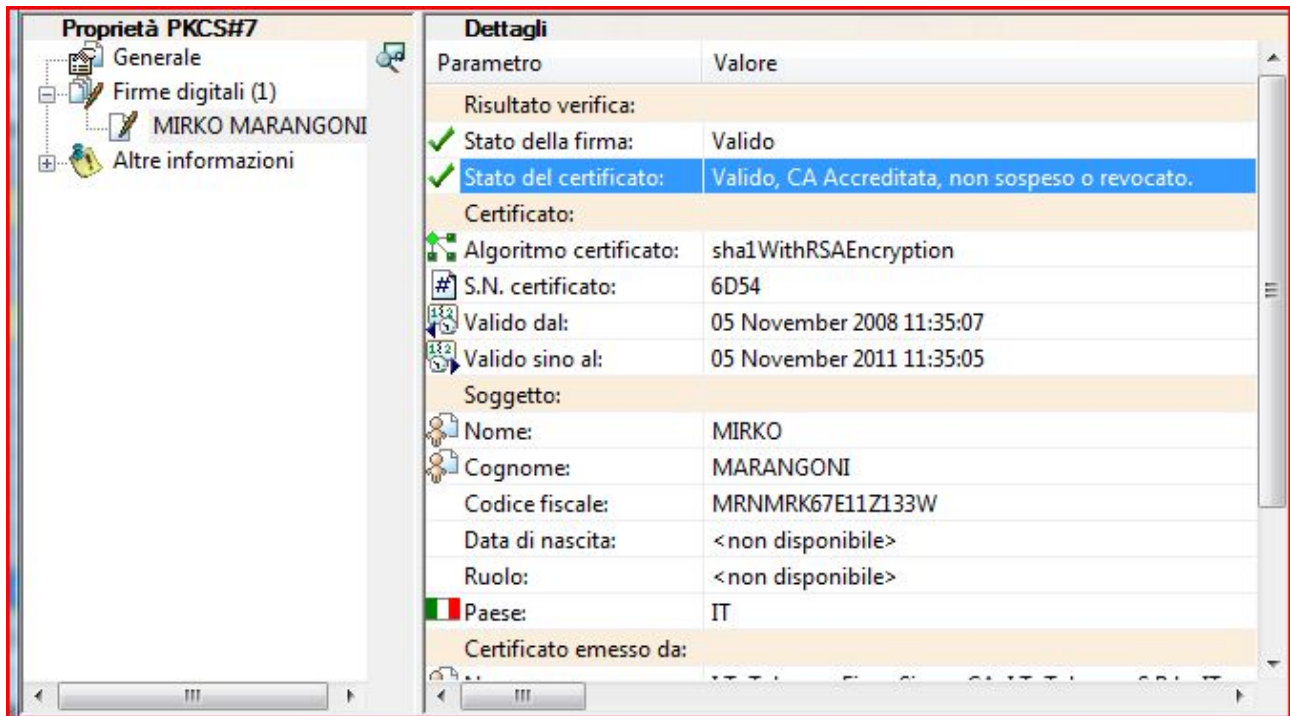


Attenzione che la gestione in locale dei certificati non permette l'aggiornamento continuativo delle liste di revoca e dei certicatori qualificati, la verifica viene definita "soft" e si concretizza con una visualizzazione del genere:



I certificati di firma dei firmatari sono scaduti

In questo caso in corrispondenza dei dati di dettaglio delle firme sono presenti le date di inizio e fine validità dei certificati di firma. Se alla data della verifica sono scadute, lo stato del certificato risulta invalidato.



Scarica i certificati di firma

Dott. Tiziano Conte (come direttore del laboratorio)
Dott. Tiziano Conte (come chimico professionista)
Dott. Italo Commissati
Dott. Lino Da Col
Dott. Riccardo Zuccherato
Dott. Andrea Boscolo
Dott. Stefano Cazzaro

I certificati di firma sono stati revocati

Il certificatore accreditato ha la possibilità di revocare dei certificati di firma (ad esempio un firmatario denuncia lo smarrimento del suo certificato di firma). La revoca viene registrata dal certificatore su una apposita lista (certificate revoke list, CRL).

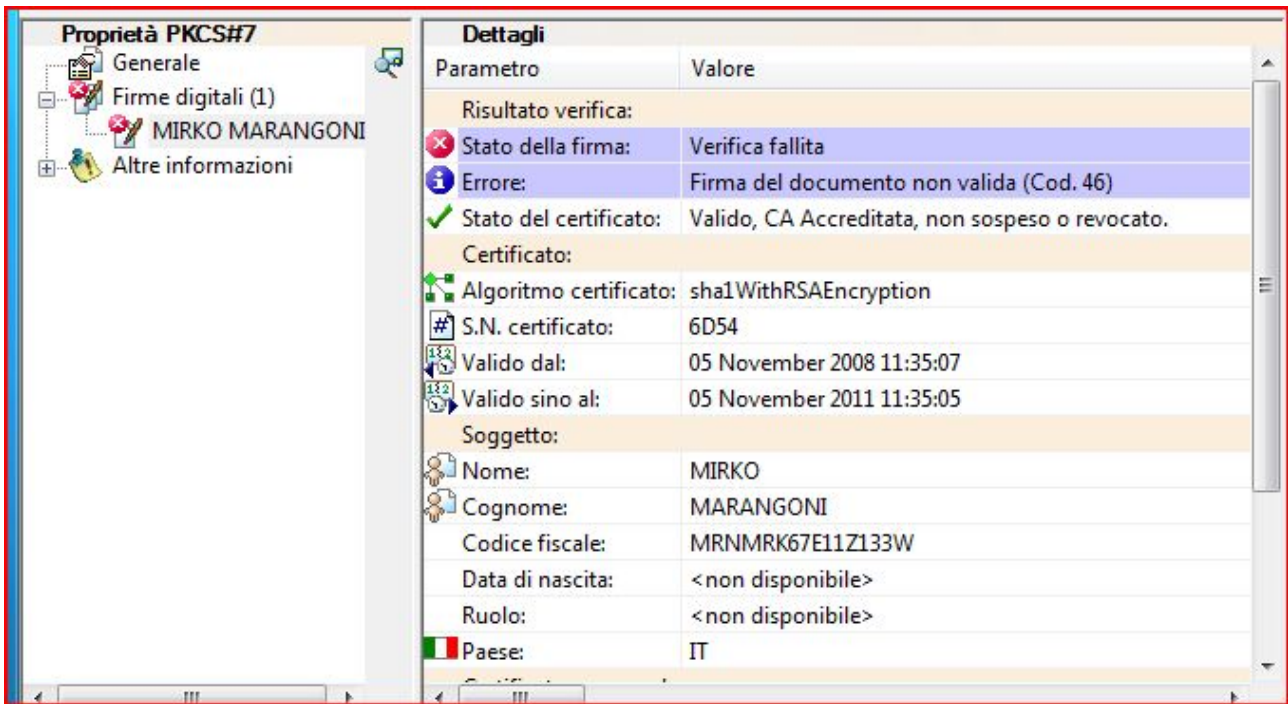
Generalmente la verifica della revoca può avvenire solo se il software di lettura è collegato ad internet e quindi la può scaricare regolarmente. Se il certificato entra in una CRL, lo stato del certificato risulta invalidato.

Come detto in precedenza, per questo tipo di verifica è necessaria la connessione ad internet.

Il documento è stato manomesso

Questo è uno dei vantaggi della gestione documentale con firma elettronica. Se un solo bit del documento è cambiato, il processo di verifica fallisce e lo stato delle firme risulta invalidato. Questa funzionalità garantisce sia l'integrità, ossia che il documento firmato non è alterabile, sia la non ripudiabilità, ossia che la firma apposta sul documento è assolutamente riconducibile al firmatario.

Esempio di firma invalidata.



Domande frequenti

Non è possibile caricare le CA accreditate e le CRL perché non riesco a connettermi al sito. Può dipendere dal fatto che l'accesso ad internet della rete sia effettuato attraverso un server proxy. A questo scopo è necessario modificare le impostazioni internet del software di lettura mettendo le informazioni del proxy che potrà fornirvi il vostro amministratore della rete.

Ad esempio, su DigitalSign, si va in Strumenti, poi in Opzioni e si seleziona la linguetta Configurazione Internet.

