


”Info Camere“



Decreto 156/2011
Elezioni Consigli camerali -
Ricezione elenchi delle
organizzazioni imprenditoriali

.....	1
Scopo del documento.....	3
Nota iniziale.....	3
CCIAA - Impostazione del processo.....	3
CCIAA - Esportazione e pubblicazione certificato di cifratura.....	3
Schema di principio dell'intero processo.....	6
Associazione – Importazione ed utilizzo certificato/i di cifratura.....	6
CCIAA – Decifratura e verifica firme.....	9

"InfoCamere"

Scopo del documento

Il presente documento intende dare delle indicazioni procedurali in merito alle direttive ricevute con il decreto 156/2011 riguardante il rinnovo dei componenti del consiglio e l'elezione della giunta delle Camere di Commercio, in particolare ci riferiamo alle procedure di cifratura ed invio degli elenchi associati da parte delle organizzazioni imprenditoriali.

Di seguito viene quindi presentata un esempio di soluzione dei punti della procedura che richiedono una qualche attenzione ed indicazioni di tipo tecnico.

Nota iniziale

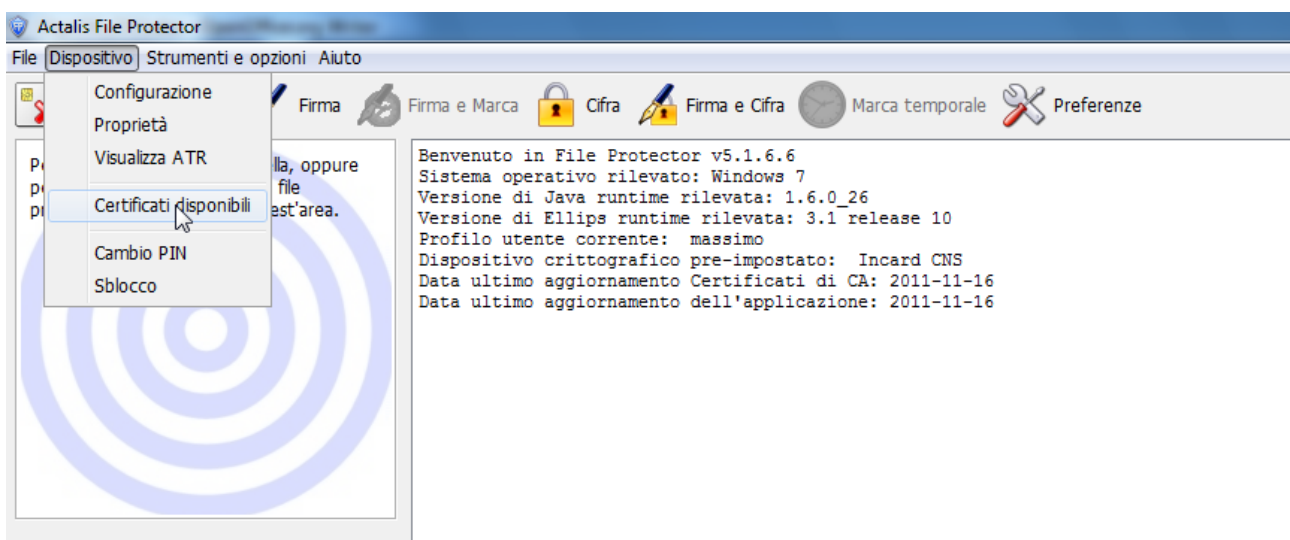
All'interno del documento ci riferiremo spesso allo strumento software *File Protector* (scaricabile dal sito <http://www.card.infocamere.it>, ove è anche presente il link ad una guida rapida all'uso), per indicare con esempi grafici le operazioni da effettuarsi con i certificati digitali. Per chi utilizzasse una applicazione differente le operazioni da eseguire rimangono ovviamente le stesse, tenendo conto delle particolarità di ciascuno strumento.

CCIAA - Impostazione del processo

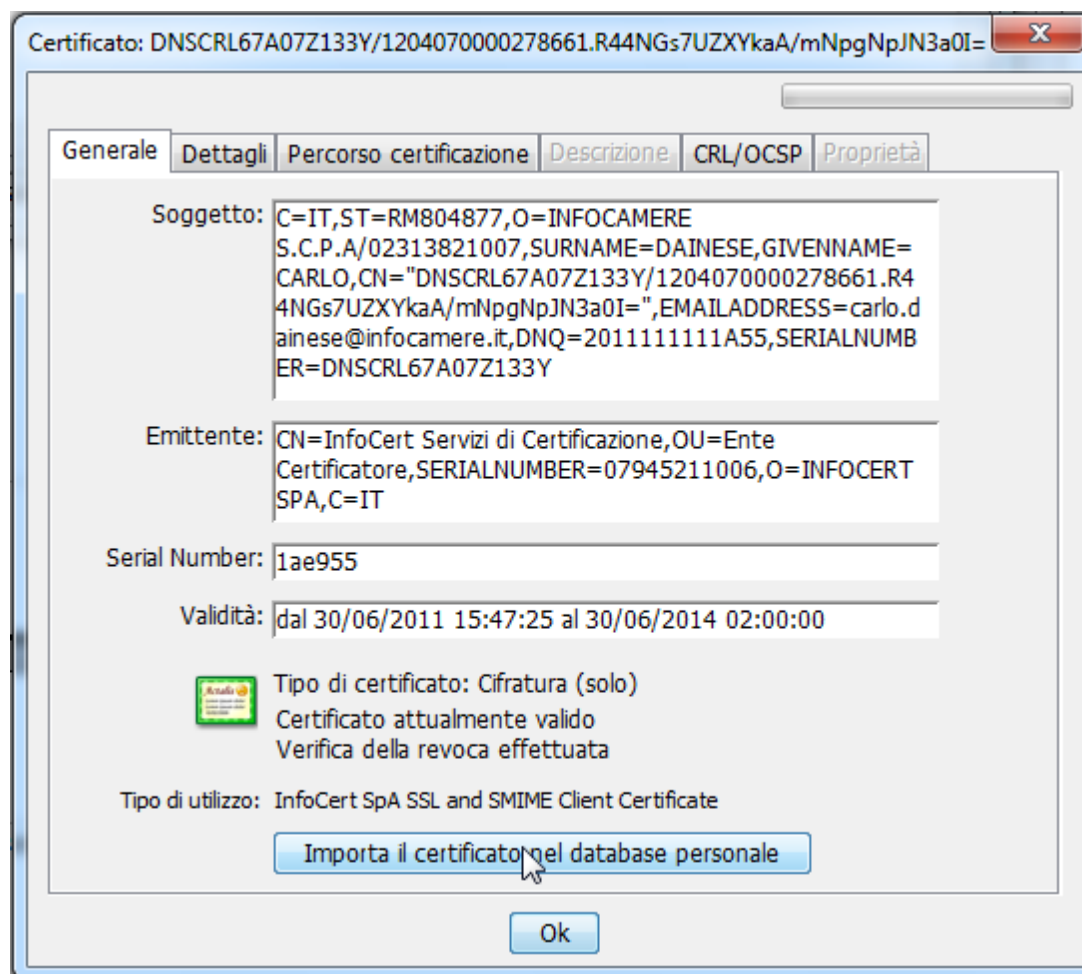
L'ente camerale nominerà un responsabile della procedura di ricezione dei files di elenco inviati dalle associazioni imprenditoriali indicate nel decreto. Tale responsabile, come persona fisica, sarà titolare e depositario di un certificato CNS da utilizzarsi nel procedimento come certificato di cifratura. A tal scopo, connesso il dispositivo hardware di supporto (smart card/token usb) contenente il certificato, per renderlo poi disponibile alle associazioni, sarà necessario per prima cosa esportarlo.

CCIAA - Esportazione e pubblicazione certificato di cifratura

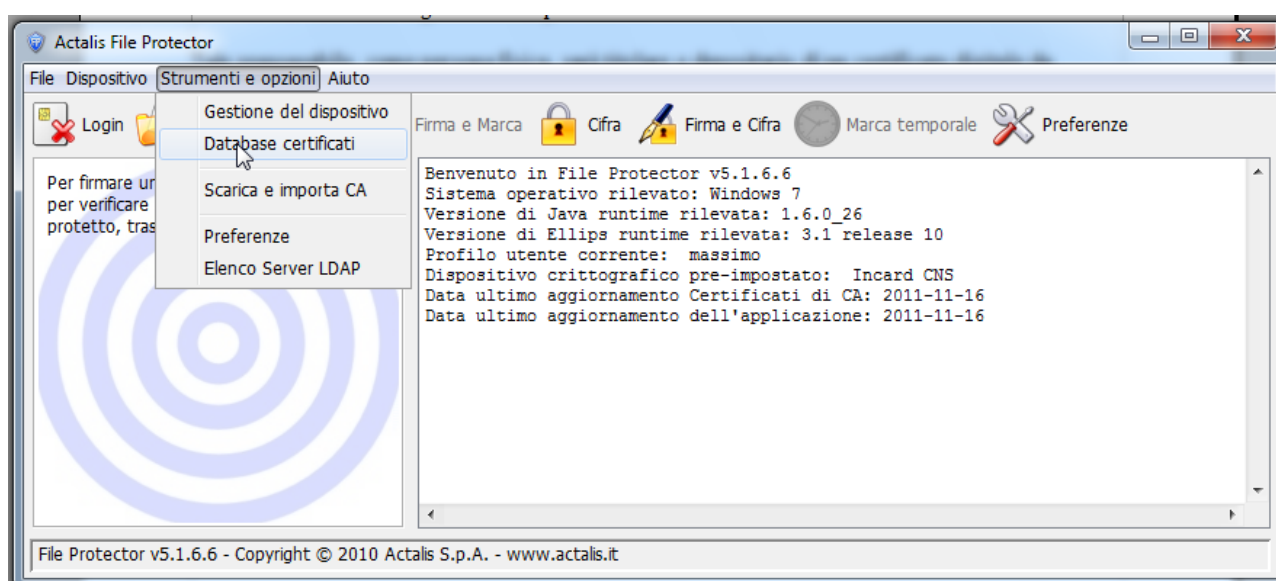
Riferendosi allo strumento File Protector, la procedura di esportazione si esegue in modo semplice. Apertura di File Protector > Dispositivo > si visualizzano i certificati disponibili (inserendo il PIN se non si è già loggati)



Qualora il certificato di cifratura non sia già presente nel database personale lo si inserisce nel modo seguente

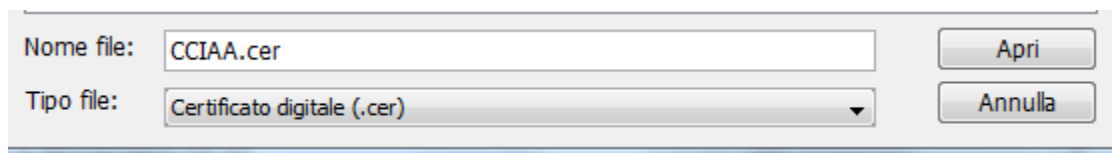
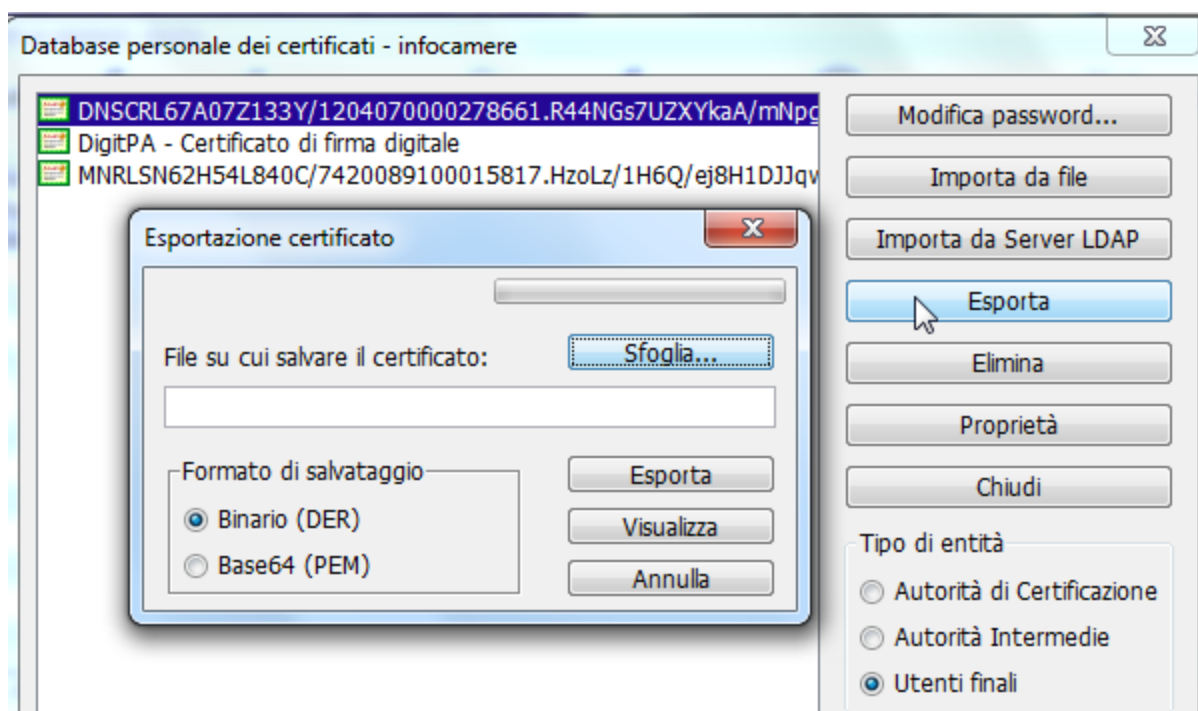


Dal database certificati, per estrarre il certificato è poi sufficiente selezionare il tipo di entità



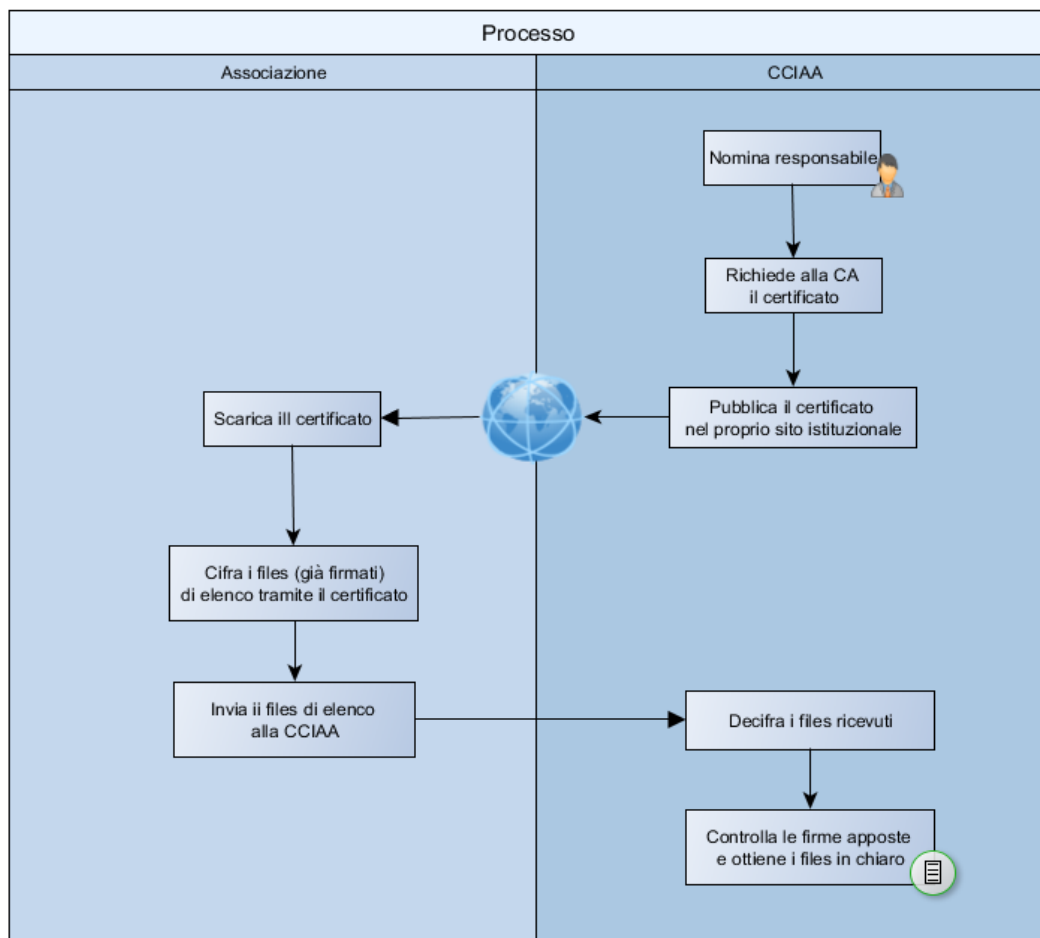
”InfoCamere”

corretto e, dopo aver indicato il certificato che si vuole esportare, cliccando sul tasto Esporta e indicando tramite il tasto Sfoggia il file destinazione (estensione .cer) nel proprio file system, si avvia la procedura di salvataggio.



Una volta ottenuto il certificato estratto (es. CCIAA.cer), tale file dovrà essere reso disponibile alle associazioni con un' opportuna modalità di pubblicazione online, ovvero scaricabile dal proprio sito istituzionale.

Schema di principio dell'intero processo

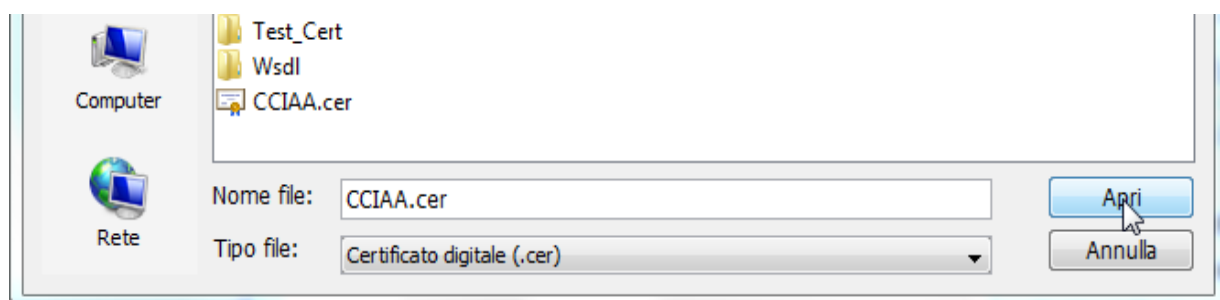
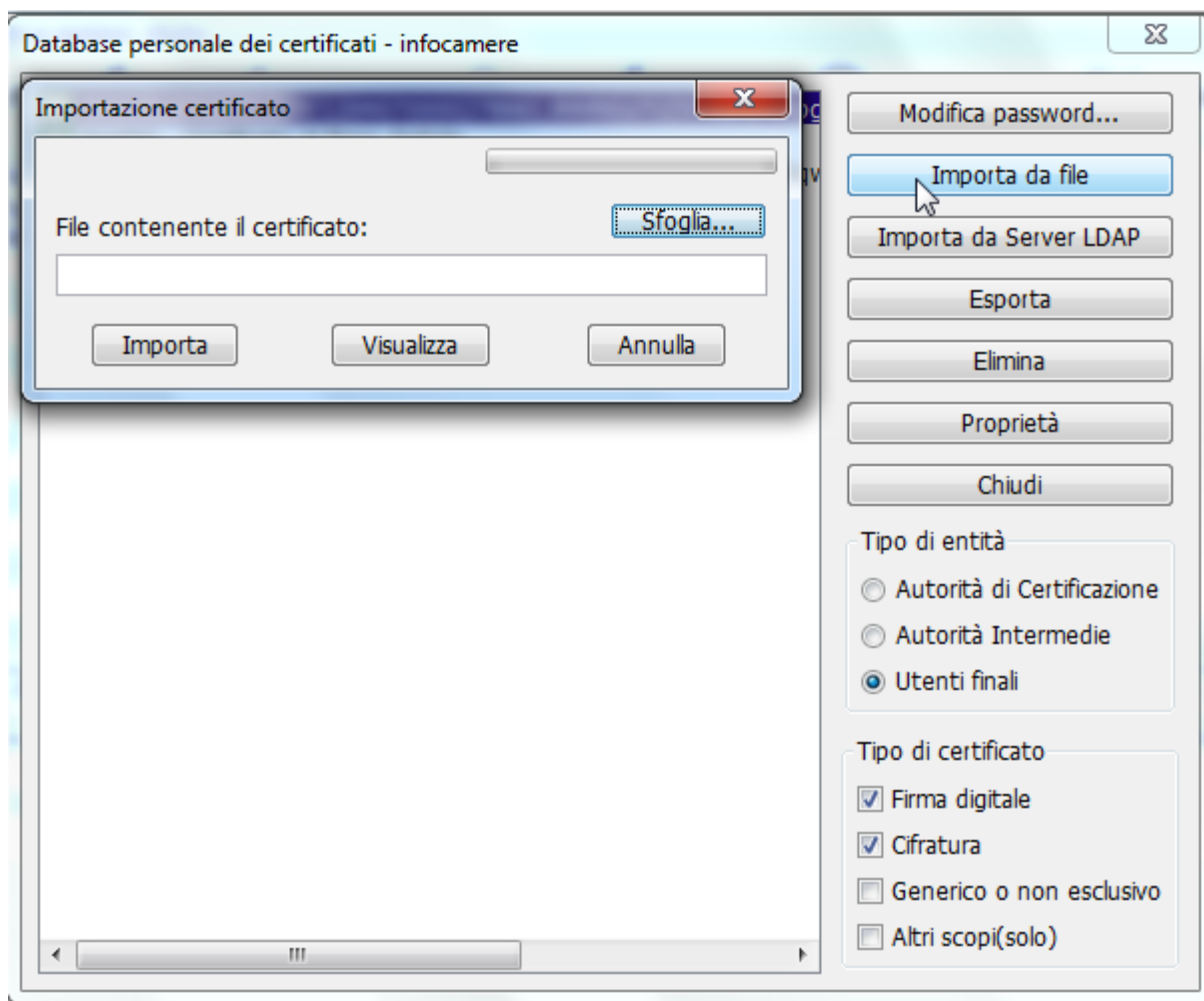


Associazione – Importazione ed utilizzo certificato/i di cifratura

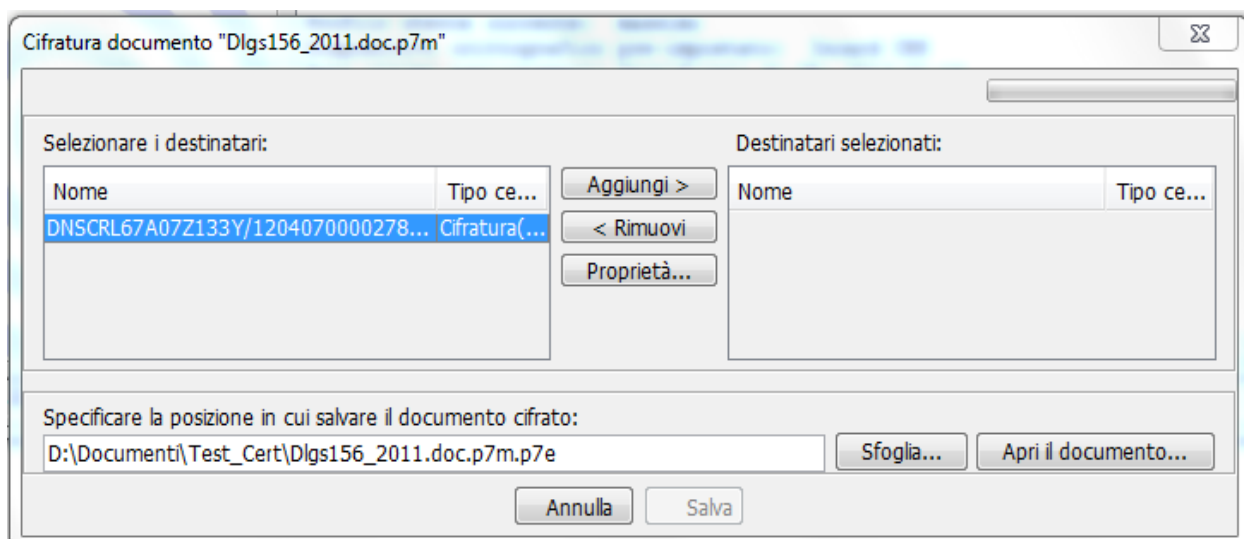
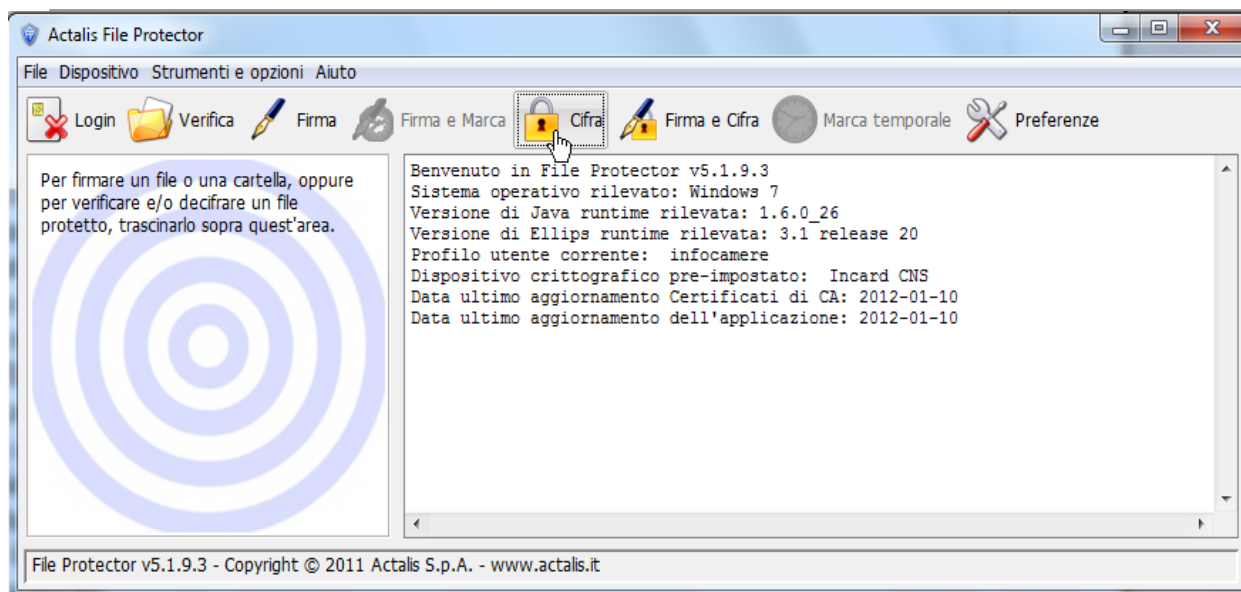
Il certificato esportato e successivamente pubblicato dall'ente camerale dovrà essere utilizzato come certificato di cifratura dalle organizzazioni tenute all'invio dei files contenenti l'elenco delle imprese associate. Per prima cosa le organizzazioni dovranno quindi scaricare (ovvero salvare) i certificati. Ipotizziamo quindi una associazione in possesso sia dei certificati sia dei files di elenco, già sottoscritti con firma digitale, come richiesto dal decreto. Per applicare il certificato per la cifratura utilizzando File Protector facciamo riferimento a quanto indicato nella guida rapida all'uso (http://www.card.infocamere.it/infocamere/pub/manuali-operativi_3185).

Per prima cosa quindi, dopo l'avvio di File Protector, ciascun certificato andrà opportunamente importato. Dal database dei certificati clickando su Importa da file e indicando il file presente nel file system attraverso il tasto Sfoglia è possibile importare e rendere utilizzabili i certificati precedentemente scaricati.

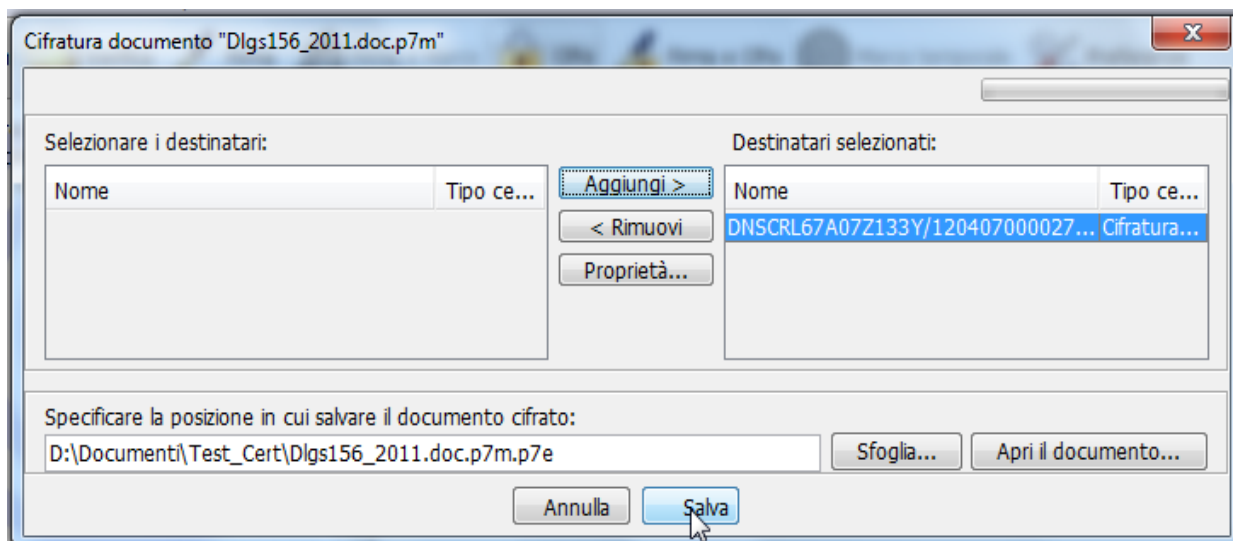
"InfoCamere"



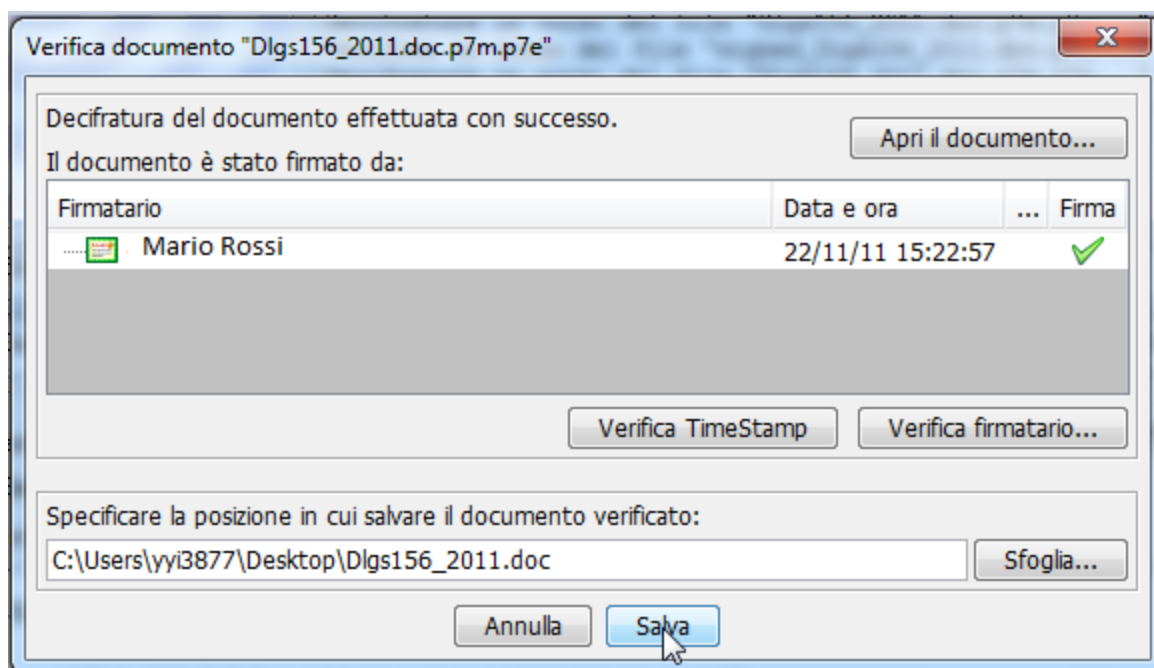
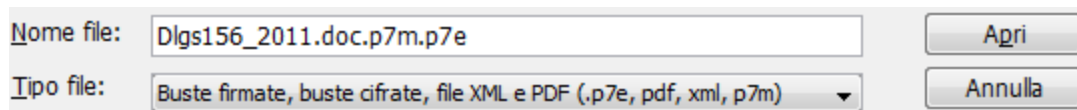
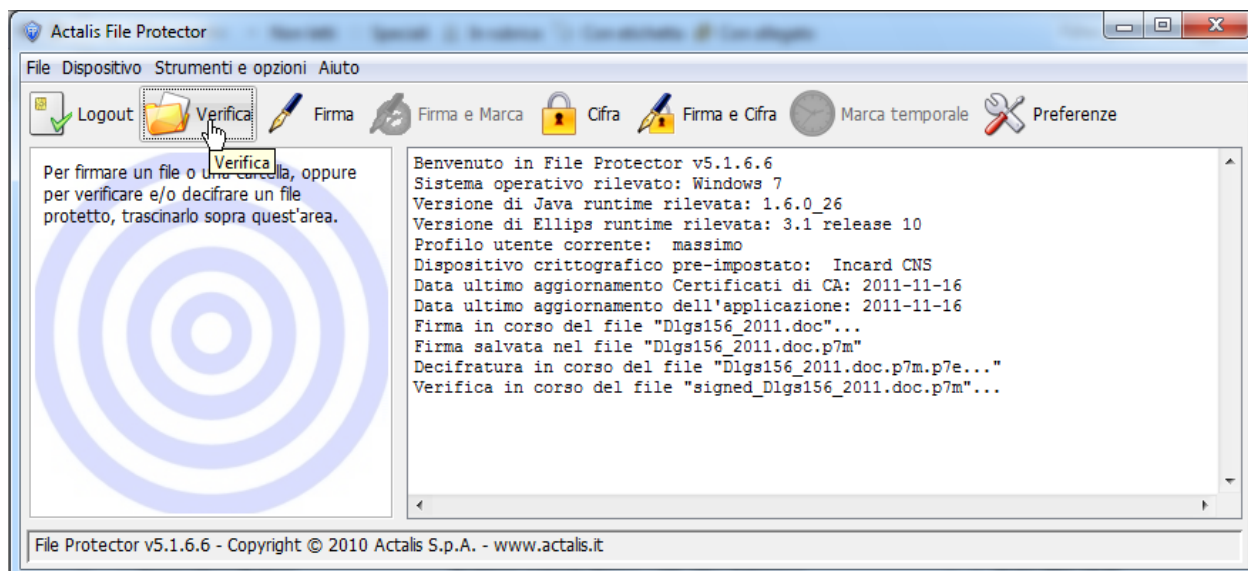
Una volta importato il certificato sarà possibile cifrare i documenti di elenco (già firmati in modalità standard → estensione .p7m, evitando firma di tipo pdf o xml) indicando come destinatario proprio i certificati appena inseriti e salvando il file risultato della cifratura.



Applicando la cifratura ai files (precedentemente firmati digitalmente) richiesti dal decreto, si ottengono i files da inviare all'ente camerale.



Il responsabile della procedura nominato dall'ente camerale utilizzerà il certificato di cui dispone per controllare che l'invio dei files sia stato eseguito correttamente. Il primo passo è decifrare i files ricevuti. Per fare questo opererà il login sul dispositivo (ovvero inserirà il PIN) e effettuerà la verifica dei file cifrati con quel certificato. Clickando su Verifica, selezionando il file da verificare si attiva il processo che porta



"InfoCamere"

alla decifratura e quindi, in caso positivo, all'individuazione del file di elenco originariamente compilato dalla associazione mittente e la firma digitale da essa applicata. Se le verifiche procedono correttamente l'ente camerale archiverà i files ricevuti e considererà i dati contenuti per le funzioni previste dalla legge. Qualora la decifratura non andasse a buon fine, i files in chiaro non potrebbero essere ottenuti ed archiviati.