Istruzioni per cifrare i file

Cifratura di un documento

La **crittografia asimmetrica** è un tipo di cifratura che consente lo scambio di informazioni in modo sicuro, evitando i rischi della tradizionale crittografia simmetrica connessi allo scambio di un'unica chiave (es. una *password* o un PIN) necessaria per la codifica/decodifica delle informazioni.
La crittografia asimmetrica è basata su una duplice chiave:

- la **chiave pubblica**, che può essere distribuita a chiunque, serve a cifrare un documento destinato a chi possiede la relativa chiave privata (rende illeggibile il messaggio a chiunque non sia in possesso della chiave privata);
- la **chiave privata**, personale e segreta, utilizzata dal destinatario per decifrare un documento cifrato con la chiave pubblica.

In tal modo il documento cifrato con una chiave pubblica, potrà essere decifrato solo con la corrispondente chiave privata.
Pertanto, la crittografia degli elenchi con la chiave pubblica (disponibile sul sito internet camerale nell'apposita sezione), garantisce che il contenuto degli stessi sia decifrabile esclusivamente dal Segretario Generale, dott. Pierluigi Medeot, responsabile del procedimento a cui è affidato il certificato di cifratura.

Dopo aver predisposto gli elenchi degli associati in formato elettronico (.xls / .xlsx / .ods) e in formato PDF/A ed aver provveduto all'apposizione della firma digitale sugli stessi, si può procedere con l'eventuale crittografia di entrambi i documenti. (Tale modalità è alternativa all'utilizzo della busta chiusa sigillata).

Requisiti

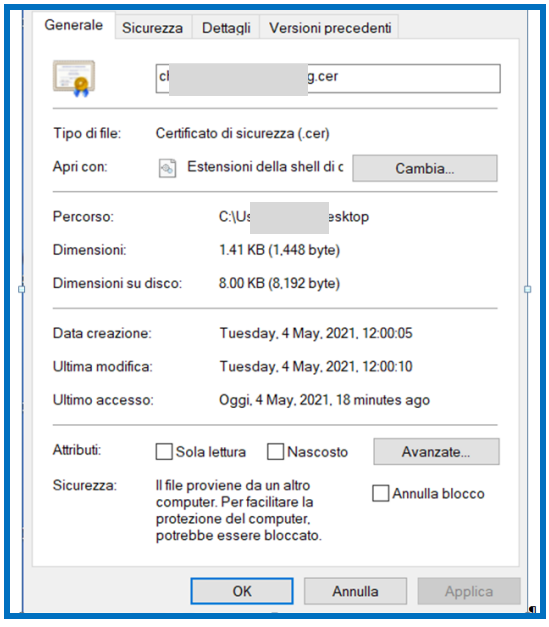
a. software File Protector installato sul proprio computer

oppure

b. possesso di una CNS su token USB

Preliminarmente, **scaricare** il certificato pubblico di cifratura pubblicato sul sito camerale nella apposita sezione "*Chiave pubblica per la cifratura*" e **salvarlo** in una cartella del proprio computer.

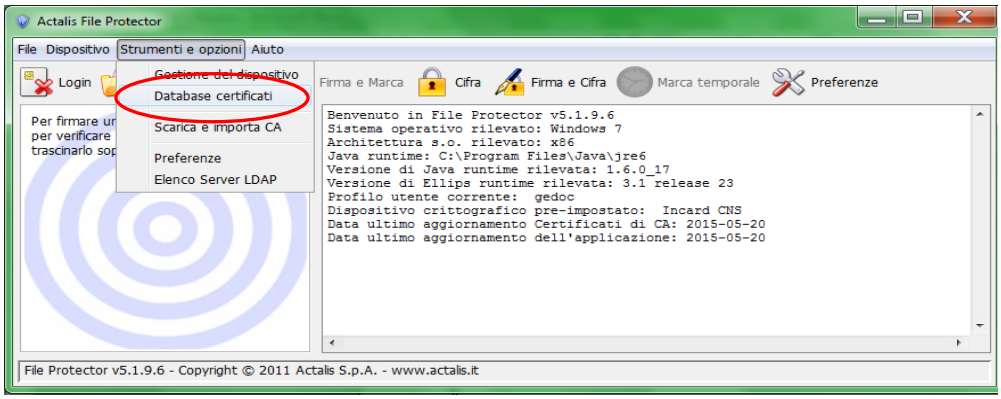
È opportuno verificare che il file abbia estensione **.cer** (e che quindi venga riconosciuto come un Certificato di sicurezza) facendoci click sopra col tasto destro del mouse e selezionando Proprietà.



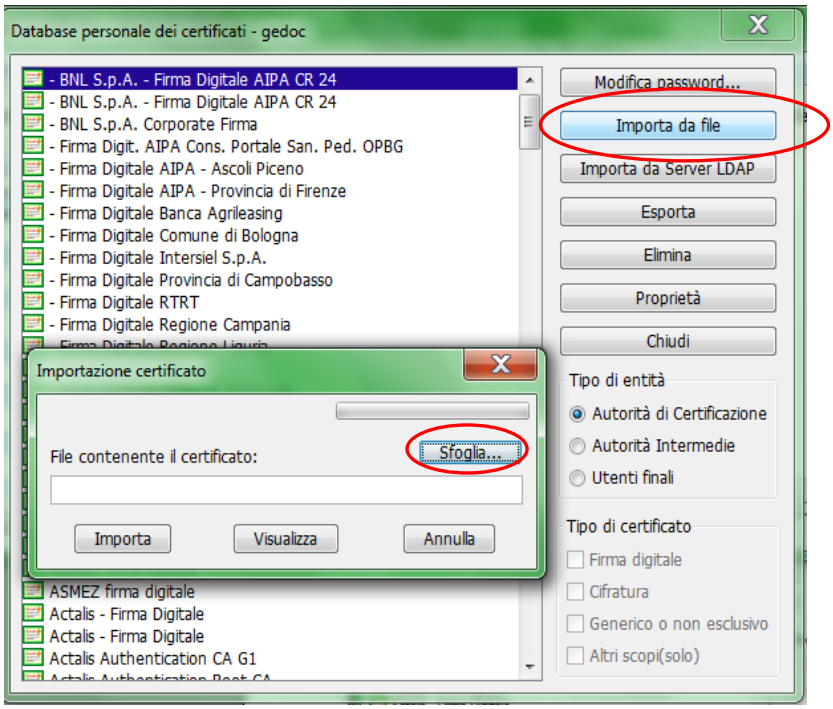
a. Cifrare il documento con File Protector

Avviare **File Protector**.

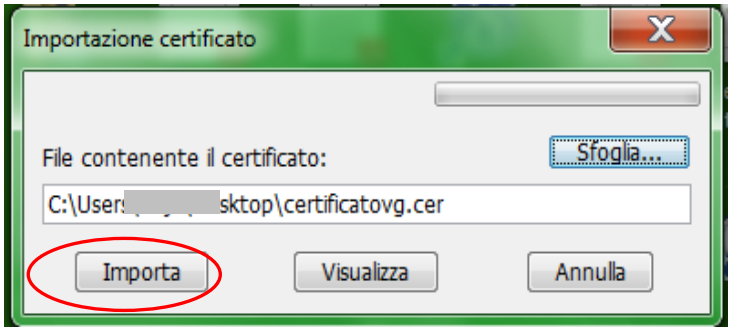
Dal menu **Strumenti e opzioni** selezionare **Database certificati.**



Nella finestra "*Database personale dei certificati*" selezionare **Importa da file** e nella successiva maschera cliccare su **Sfoglia..**

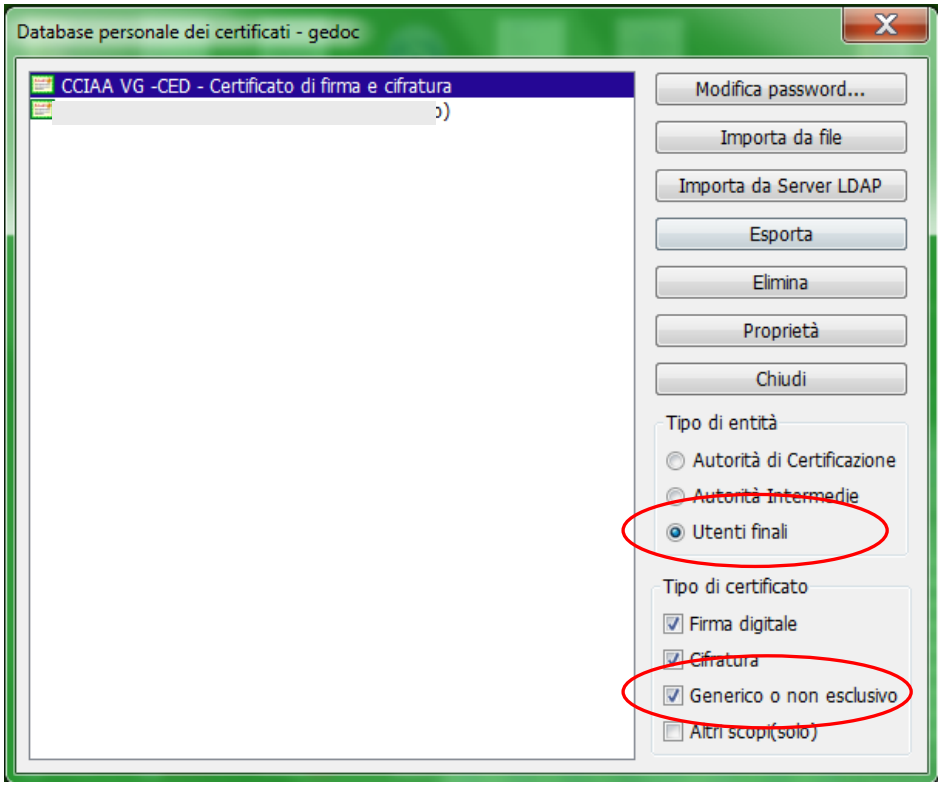


Dalla finestra che appare in seguito "*Apertura file*" **selezionare il certificato** precedentemente scaricato (Chiave pubblica per la cifratura) e cliccare su **Apri.**

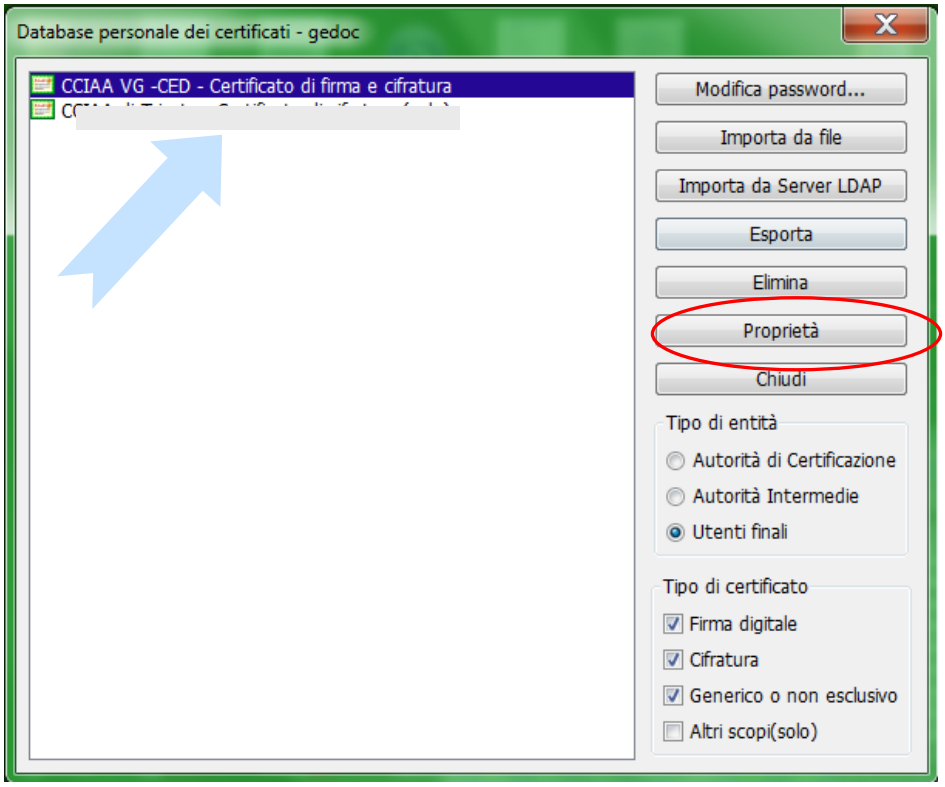


e poi nella maschera "*Importazione certificato*" cliccare su **Importa**.

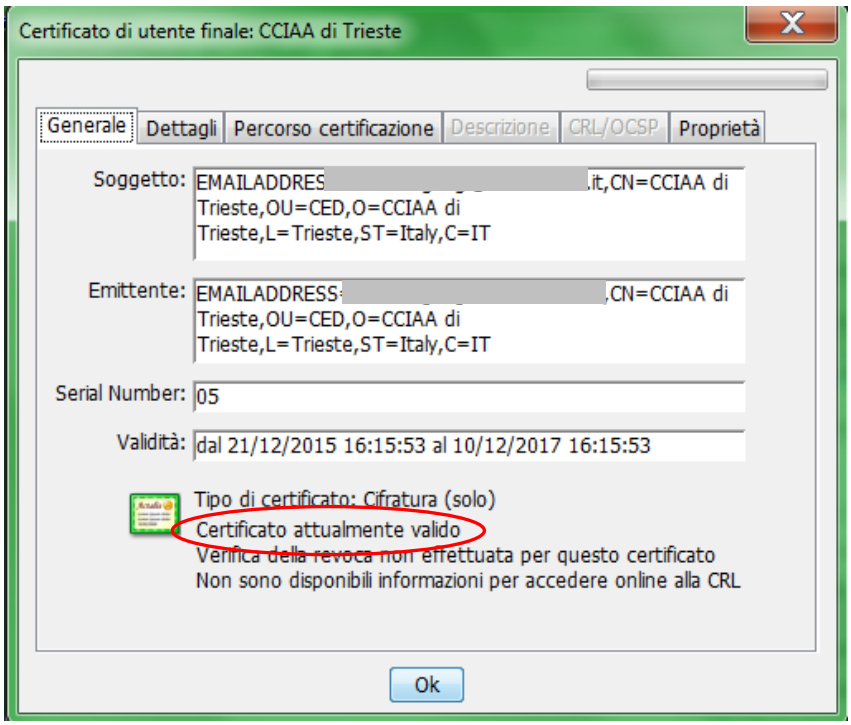
Se l'operazione è stata eseguita correttamente appare il messaggio "*Importazione del certificato eseguita con successo*".



Nella finestra "*Database personale*…" il certificato risulterà visibile mettendo il segno di spunta su **Utenti finali** (Tipo entità) e **Generico o non esclusivo** (Tipo di certificato).

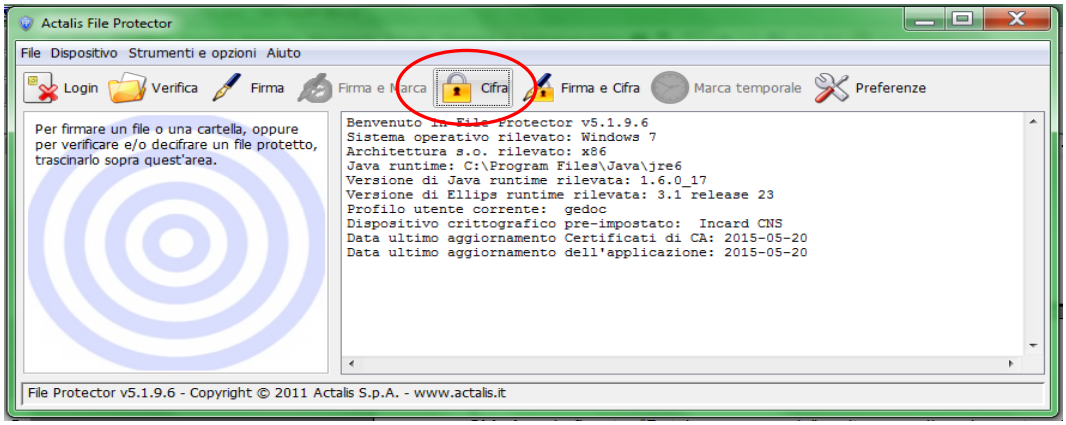


Selezionare il codice identificativo del certificato e cliccare su Proprietà per verificare se la dicitura "*Certificato attualmente valido"* è presente nelle proprietà del certificato



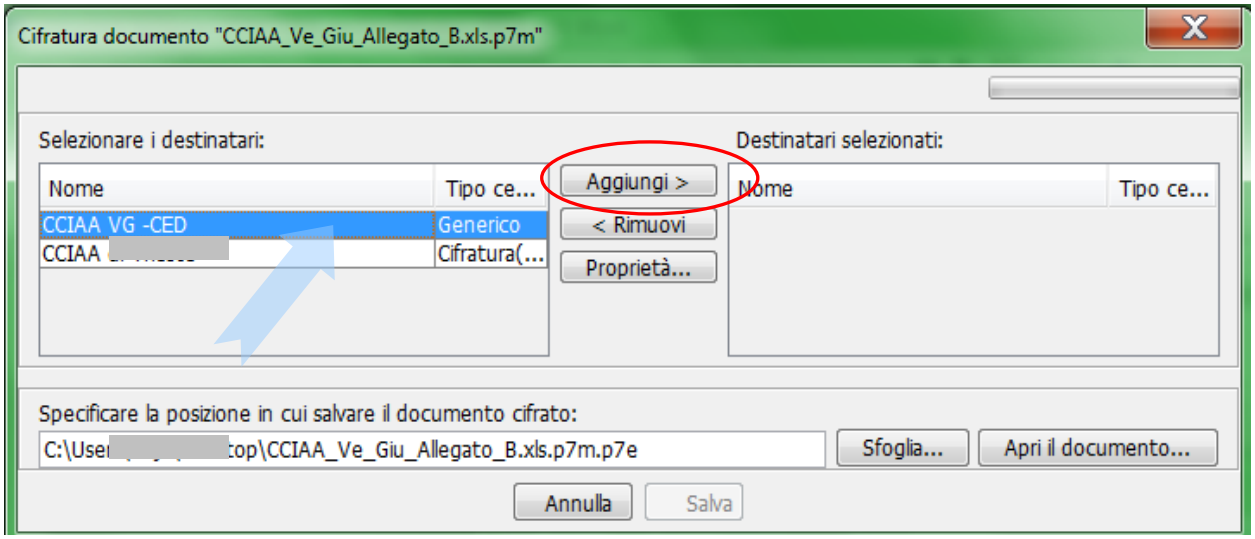
Verificare che ci sia la dicitura "*Certificato attualmente valido*" come nella figura soprastante.

Chiudere la finestra "*Database personale*" e ritornare alla schermata principale di File Protector.



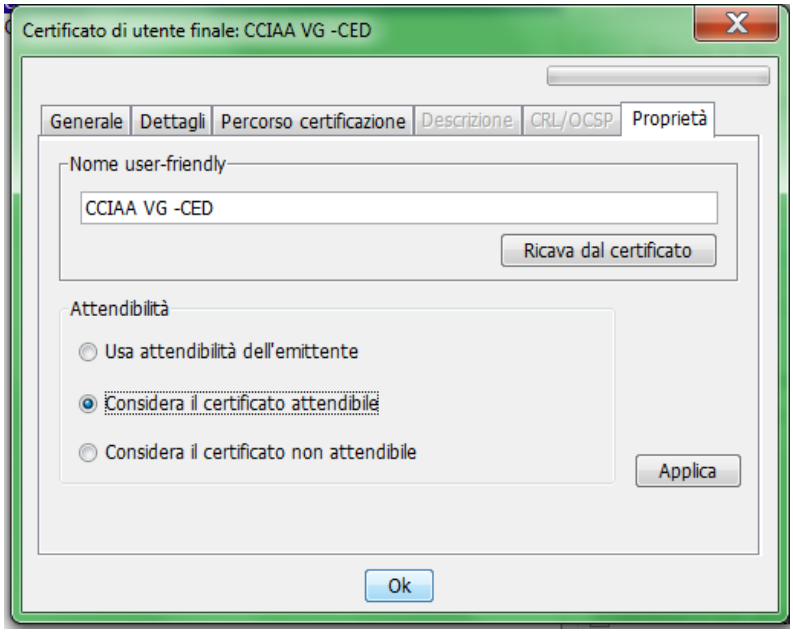
Selezionare l'icona **Cifra**

Dalla finestra che appare, **selezionare il file .p7m** che deve essere sottoposto a cifratura (*che dovrà quindi essere precedentemente firmato digitalmente e salvato sul proprio computer*)

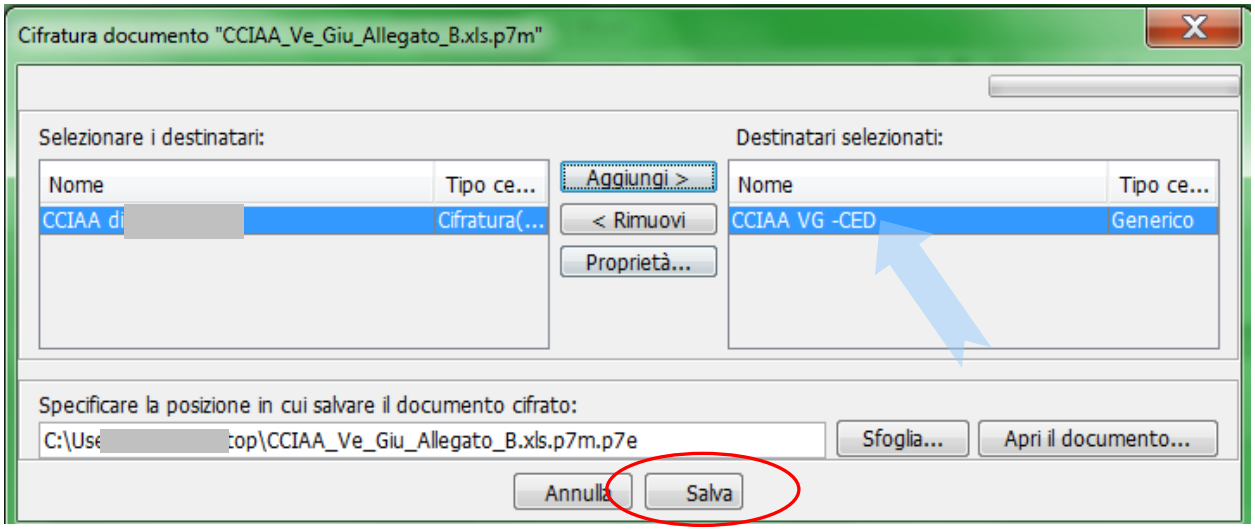


Nella finestra "*Cifratura documento…*" selezionare il certificato e cliccare su **Aggiungi** per spostarlo nella colonna di destra

Nel caso in cui al posto di tale dicitura sia presente un messaggio del tipo *"Il certificato dell'emittente non è contenuto nel database dei certificati"*, selezionare **Proprietà**



….. spuntare quindi la voce **Considera il certificato attendibile** nella sezione "*Proprietà*" e selezionare il tasto **Applica**. Nella finestra di conferma *"Salvataggio avvenuto correttamente"* selezionare **OK**, e nuovamente **OK**



Terminare la procedura con il pulsante **Salva** che si attiva dopo aver aggiunto il certificato.

Se l'operazione è stata eseguita correttamente appare il messaggio "*Documento cifrato e salvato correttamente*".

Il file cifrato viene automaticamente salvato nella stessa cartella dell'originale, con lo stesso nome e con l'ulteriore estensione .**p7e**

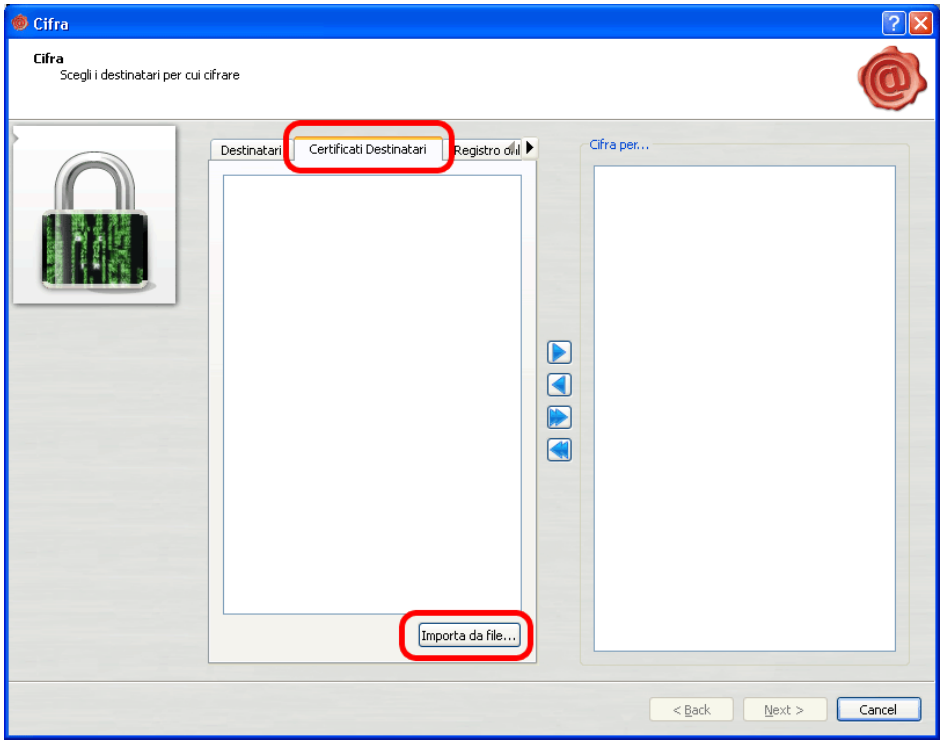
b. Cifrare il documento con Token USB

Collegare il Token USB al computer. Se il software di gestione non appare automaticamente, cliccare su Risorse del computer > Aruba Key > Autorun.exe.

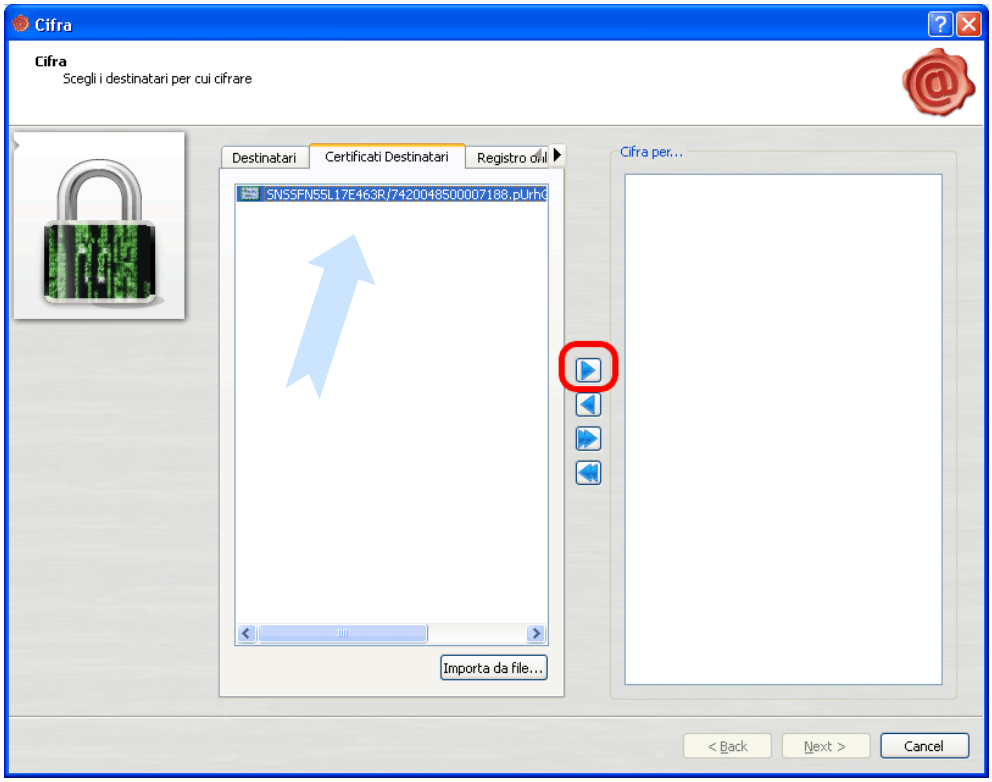
Quando appare la finestra Token USB, cliccare su **Utilità** e poi su **Cifra.**

Dalla finestra "*Apri*" che appare **selezionare il file .p7m** da cifrare (*che dovrà quindi essere precedentemente firmato digitalmente e salvato sul proprio computer)* e cliccare su **Apri.**

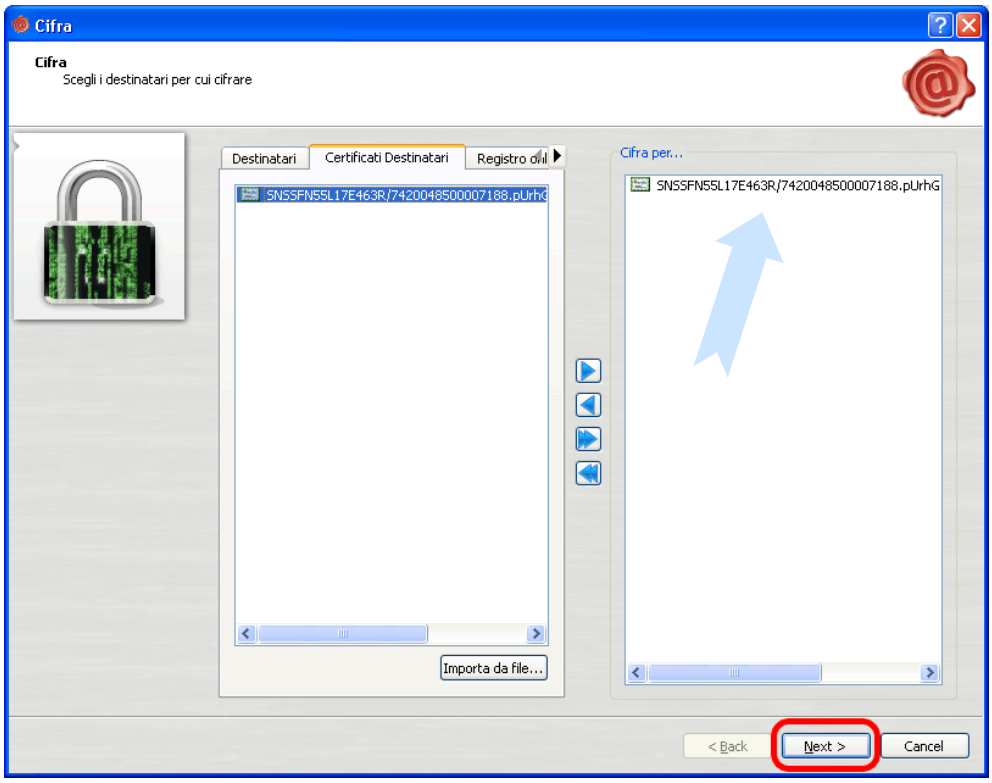
Nella successiva finestra selezionare la voce **Certificati destinatari** e cliccare **Importa da file.**



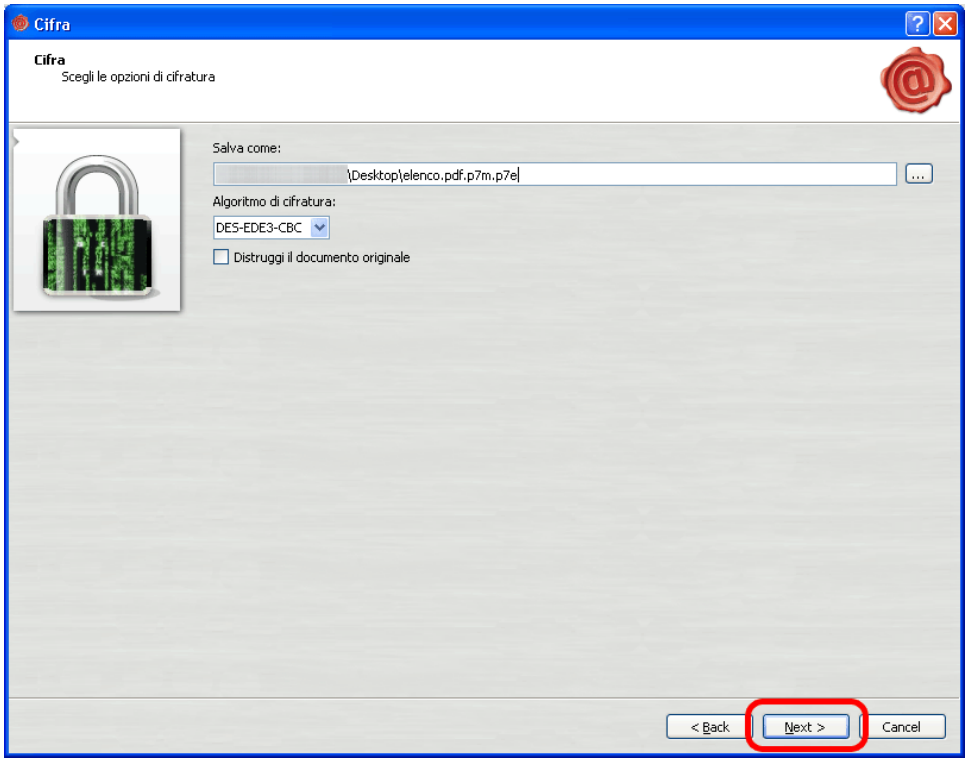
Appare la finestra “*Open*” dove selezionare il certificato da importare e quindi cliccare su **Open**.



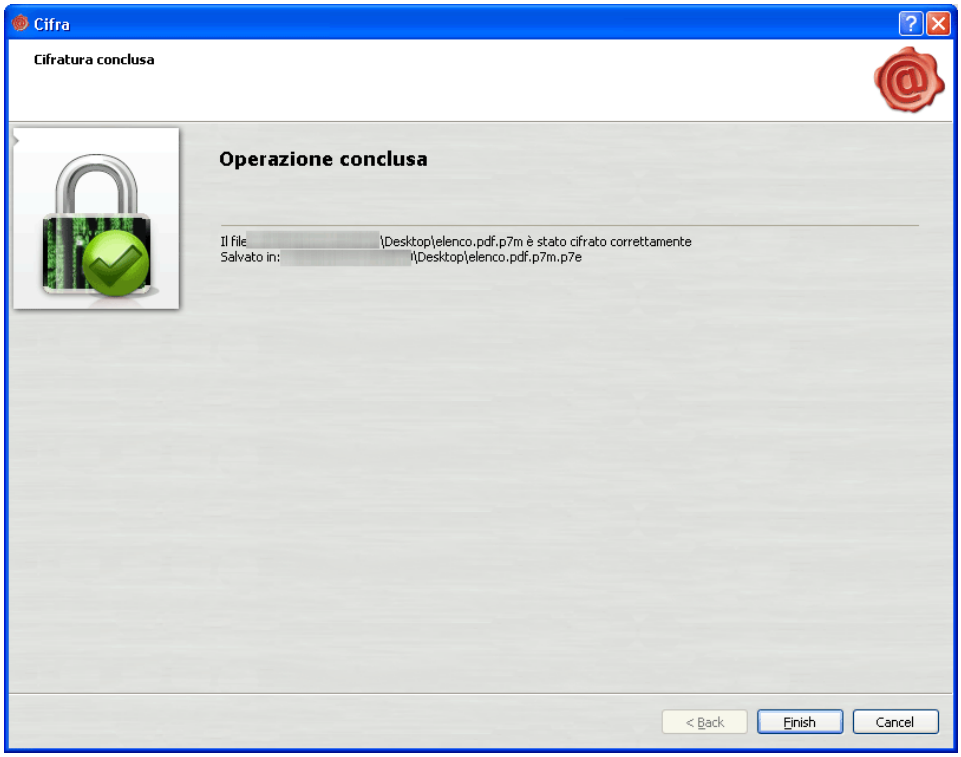
Nella finestra “*Cifra*” selezionare il certificato nella colonna di sinistra e cliccare su ▶ per farlo apparire anche nella colonna di destra.



Cliccare quindi su **Next.**



Premere nuovamente su **Next** senza modificare i campi presenti.



Se l'operazione è stata eseguita correttamente appare la finestra "***Operazione conclusa***" in cui sarà anche indicata la posizione in cui il file cifrato è stato salvato.

Cliccare su **Finish.**