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.

Dopo aver predisposto gli elenchi degli associati in formato elettronico (**csv**) 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).

Come cifrare il documento

I file da cifrare devono essere preventivamente firmati digitalmente e in formato Cades (estensione file p7m) utilizzando una cns o un token.

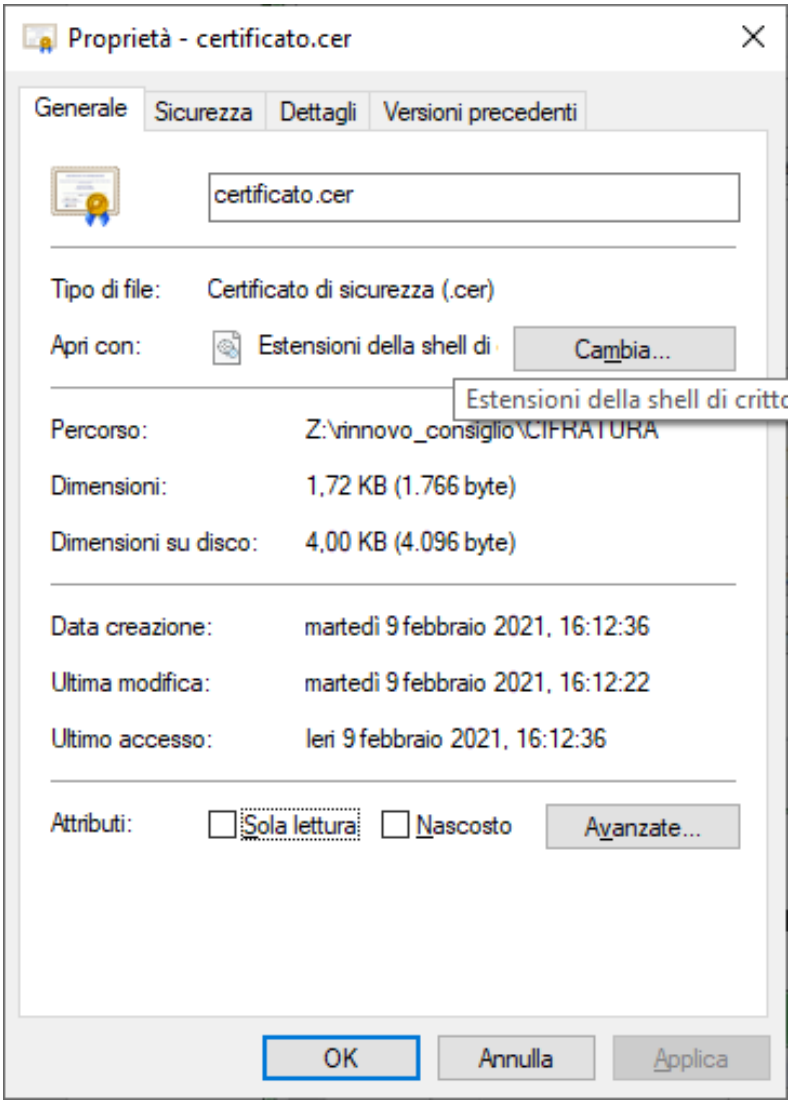
Con una cns si può utilizzare il software FileProtector – sezione A oppure il software Dike – sezione C.
Con un token si può utilizzare il software presente nel token – sezione B.

a. Cifrare il documento con File Protector

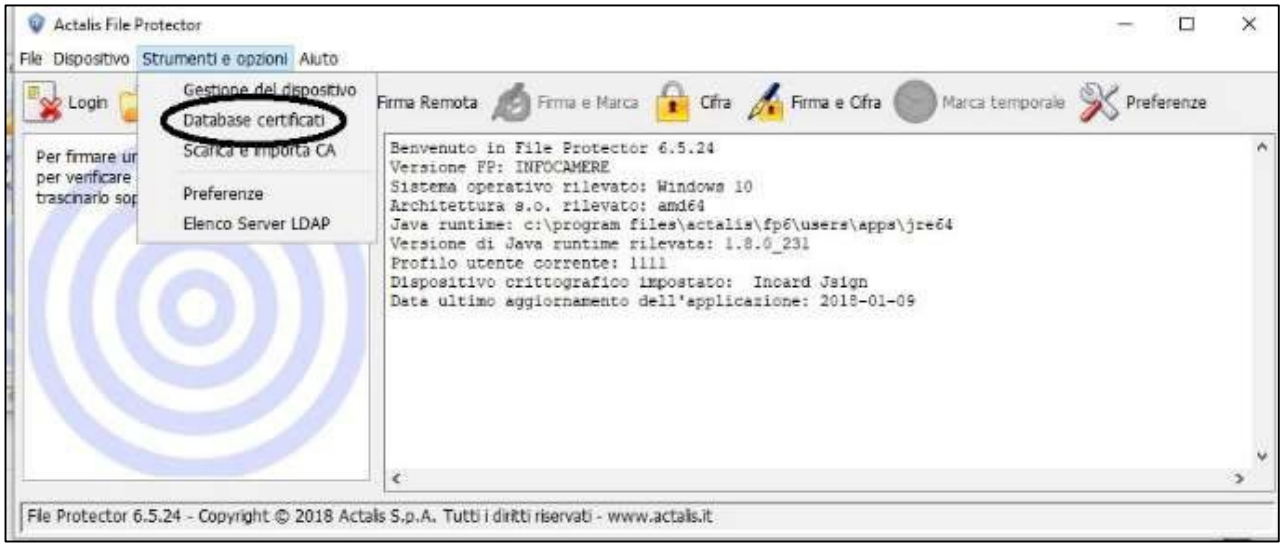
E' necessario avere installato File Protector scaricabile alla pagina
https://www.card.infocamere.it/infocard/pub/download-software_5543

Scaricare la cartella compressa "Chiave pubblica per cifratura" contenente il certificato di cifratura (nome file: **certificato.cer**) pubblicata sul sito della CCIAA di Palermo ed Enna al link https://www.paen.camcom.gov.it/it/file/3008, estrarre il file **certificato.cer** e **salvarlo** in una cartella del proprio computer.

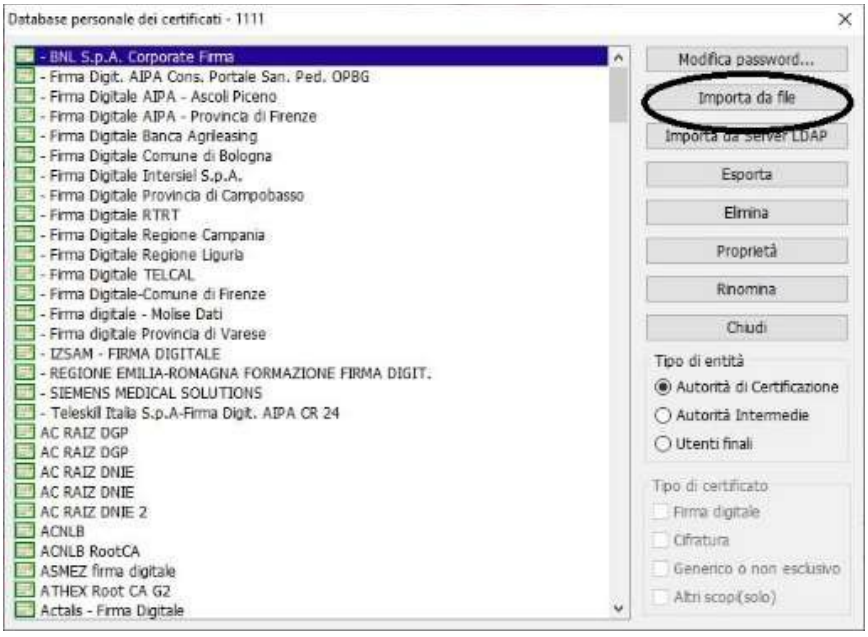
E' opportuno verificare che il file abbia estensione .cer (e che quindi venga riconosciuto come un Certificato di sicurezza) facendoci click sopra col tasto destro del mouse e selezionando Proprietà.



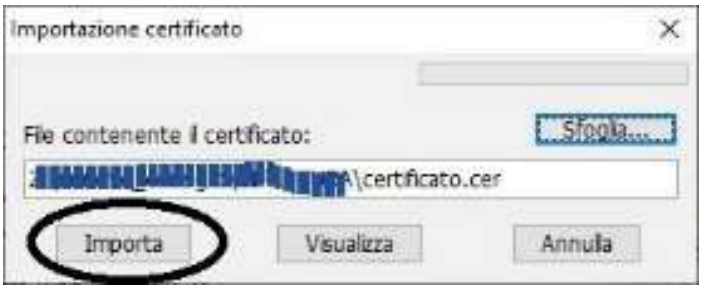
Avviare File Protector e dal menu **Strumenti e opzioni** selezionare **Database certificati**.



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

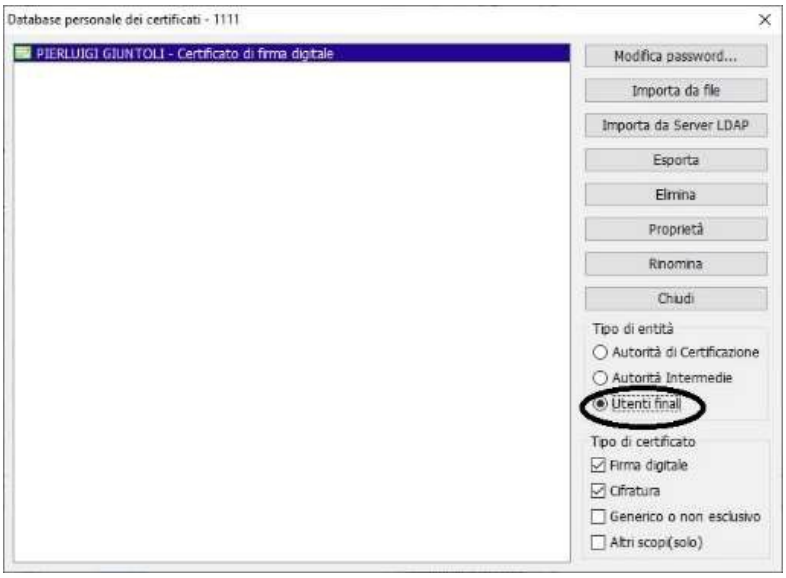


Dalla finestra che appare in seguito “Apertura file” **selezionare il certificato** certificatovg.cer precedentemente scaricato e cliccare su **Apri.**



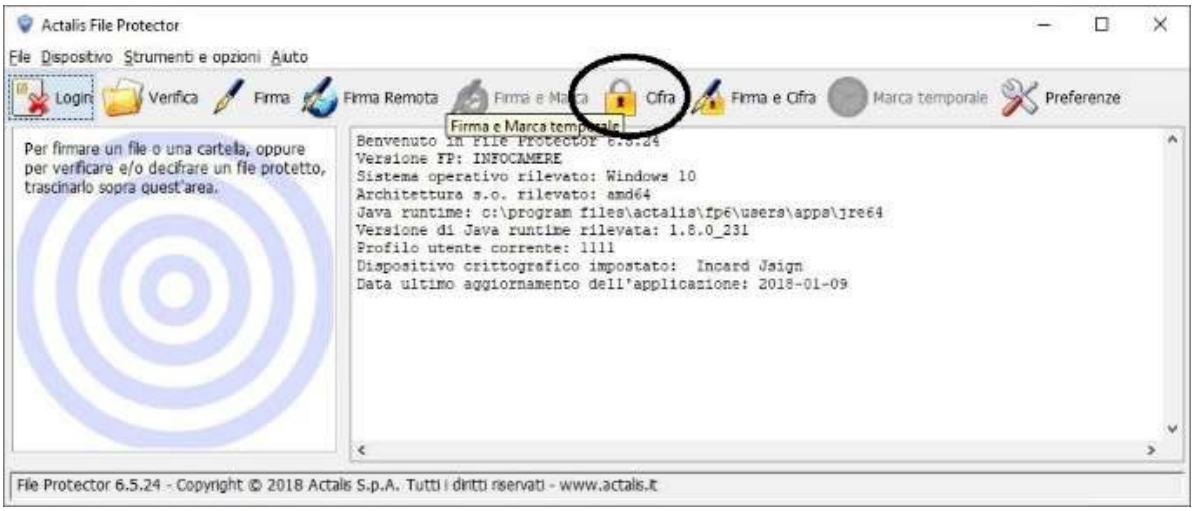
e poi nella maschera “Importazione certificato” cliccare su **Importa.**

Se l’operazione è stata eseguita correttamente appare il messaggio “Importazione del certificato eseguita con successo”.



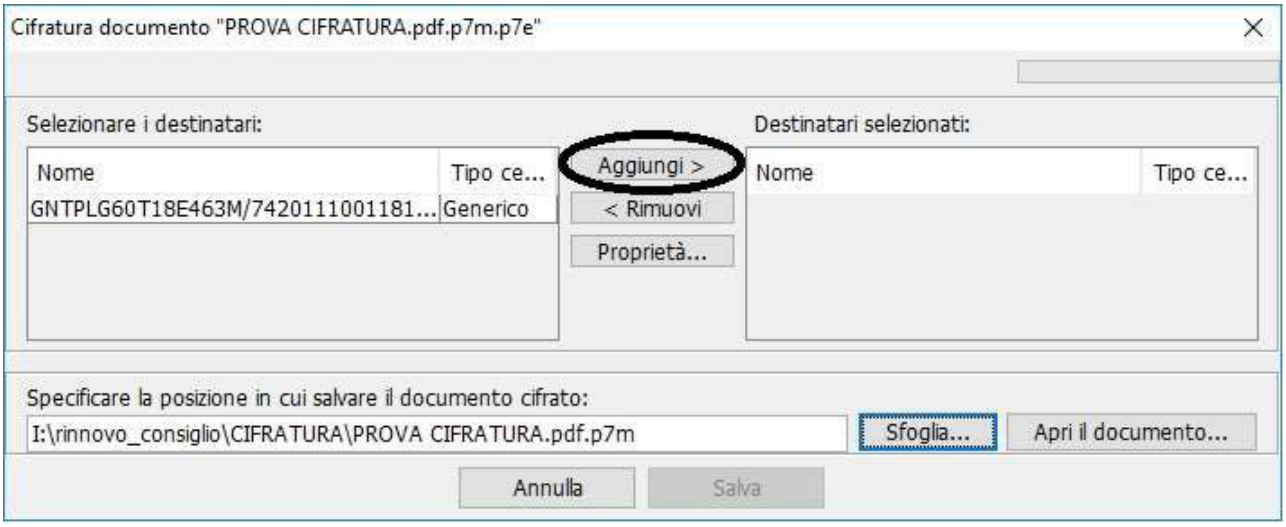
Nella finestra “Database personale…” il certificato risulterà visibile mettendo il segno di spunta su **Utenti finali** (Tipo entità).

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 in formato CADES estensione p7m e salvato sul proprio computer*)



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

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

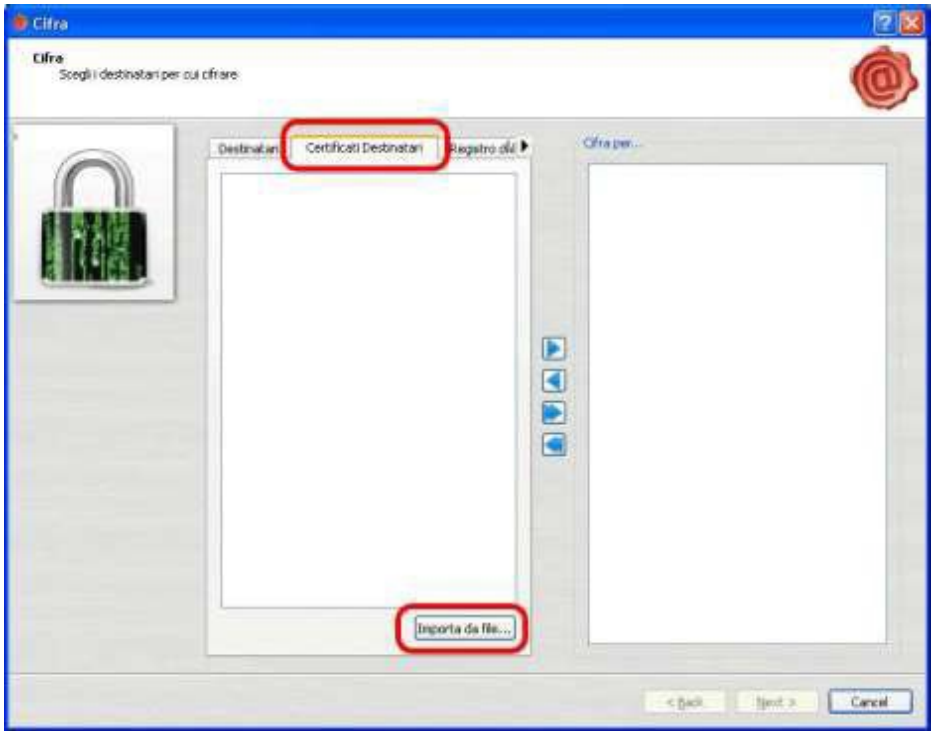
Scaricare la cartella compressa “Chiave pubblica per cifratura” contenente il certificato di cifratura (nome file: **certificato.cer**) pubblicata sul sito della CCIAA di Palermo ed Enna al link https://www.paen.camcom.gov.it/it/file/3008, estrarre il file **certificato.cer** e **salvarlo** in una cartella del proprio computer.

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

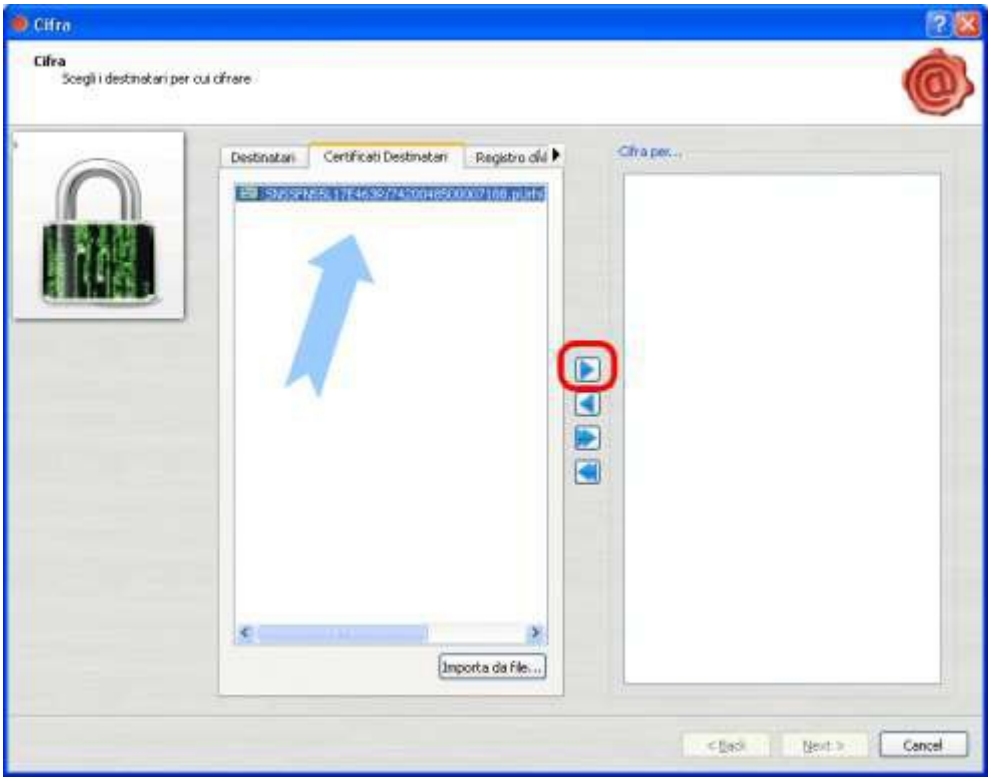
Quando appare la finestra Token USB, cliccare su **Utilità** e poi su **Cifra.**

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.**

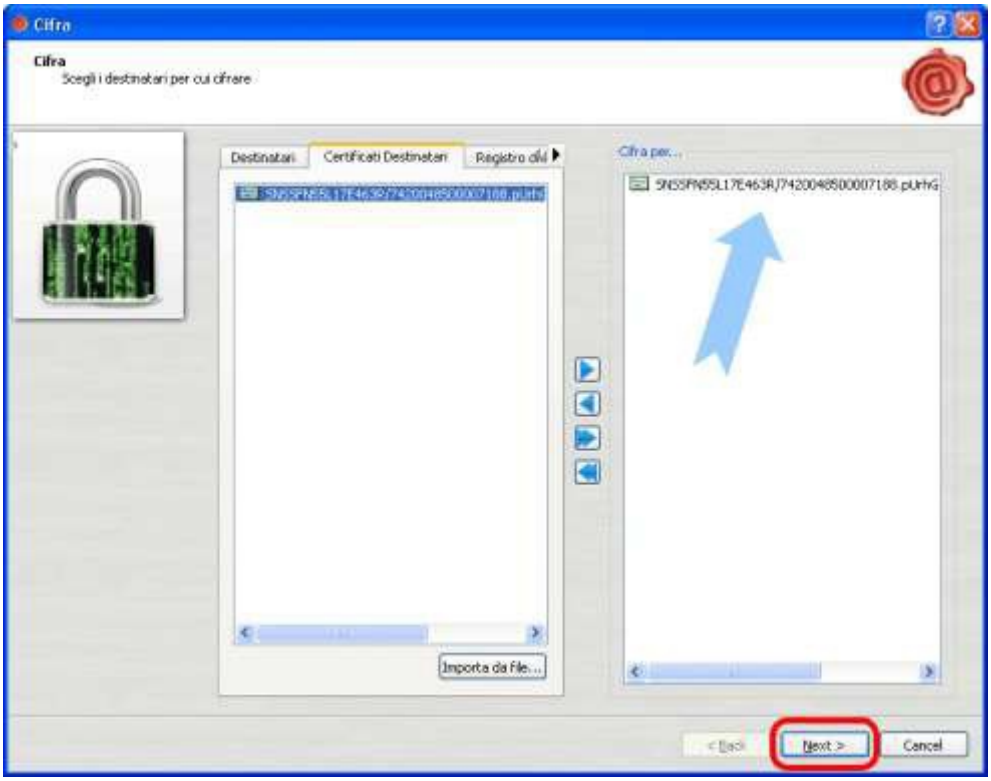
Nella successiva finestra selezionare la linguetta **Certificati destinatari** e cliccare **Importa da file.**



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



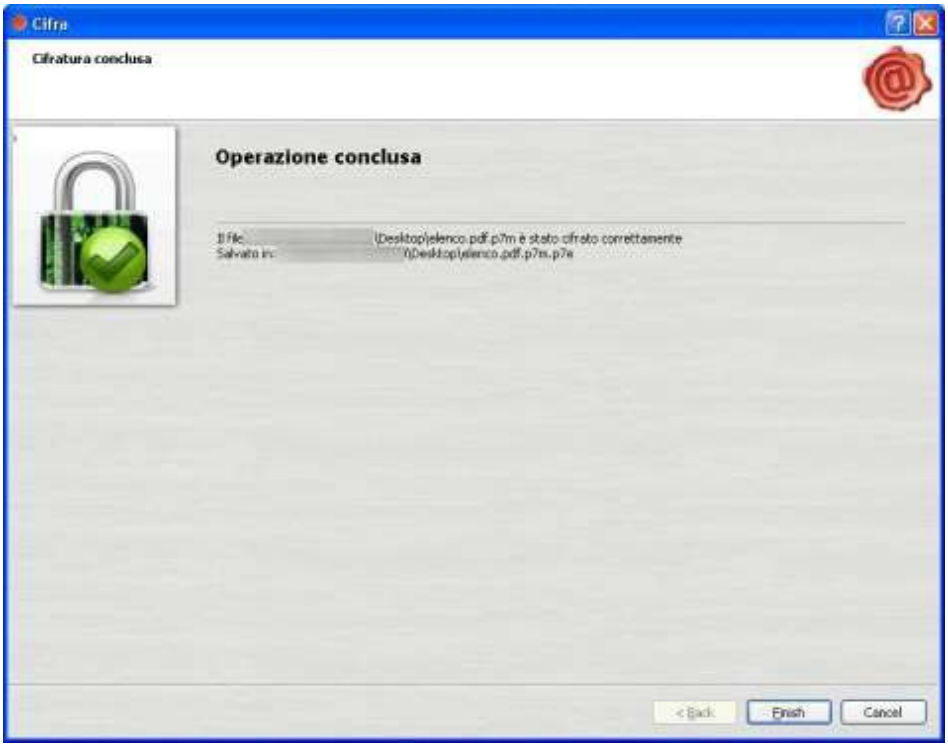
Nella finestra “Cifra” selezionare il certificato nella colonna di sinistra e cliccare su ▶ per farlo apparire anche nella colonna di destra.



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.



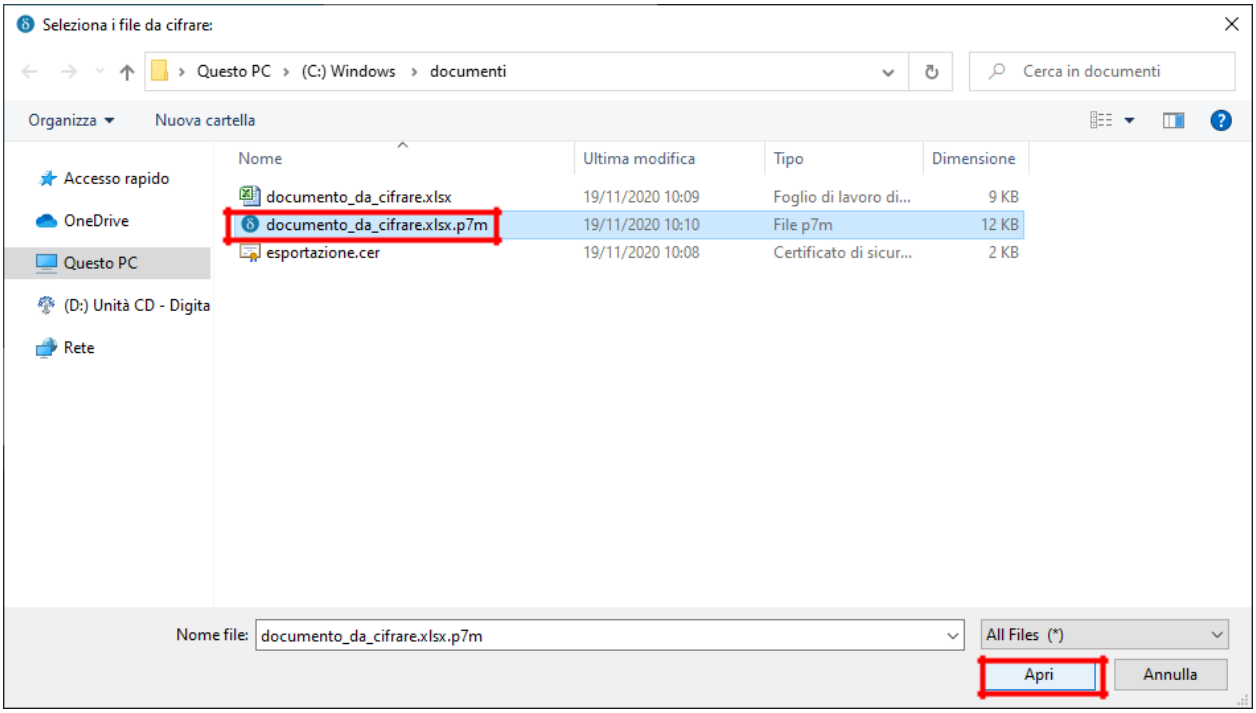
c. Cifrare il documento con Dike

Scaricare il software DikeIC dal sito http://www.card.infocamere.it sezione “Download software di firma” e procedere all’installazione

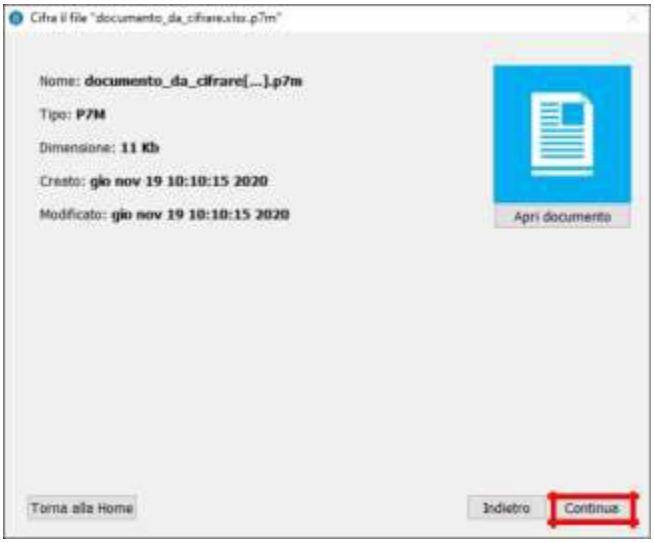
Scaricare la cartella compressa “Chiave pubblica per cifratura” contenente il certificato di cifratura (nome file: **certificato.cer**) pubblicata sul sito della CCIAA di Palermo ed Enna al link https://www.paen.camcom.gov.it/it/file/3008, estrarre il file **certificato.cer** e **salvarlo** in una cartella del proprio computer.

Aprire il software DikeIC, spostarsi con il mouse sul simbolo del lucchetto e selezionare la voce “CIFRA”.

Nella finestra che si apre selezionare il file da cifrare (precedentemente già firmato digitalmente in formato CADES estensione p7m) e cliccare su APRI.

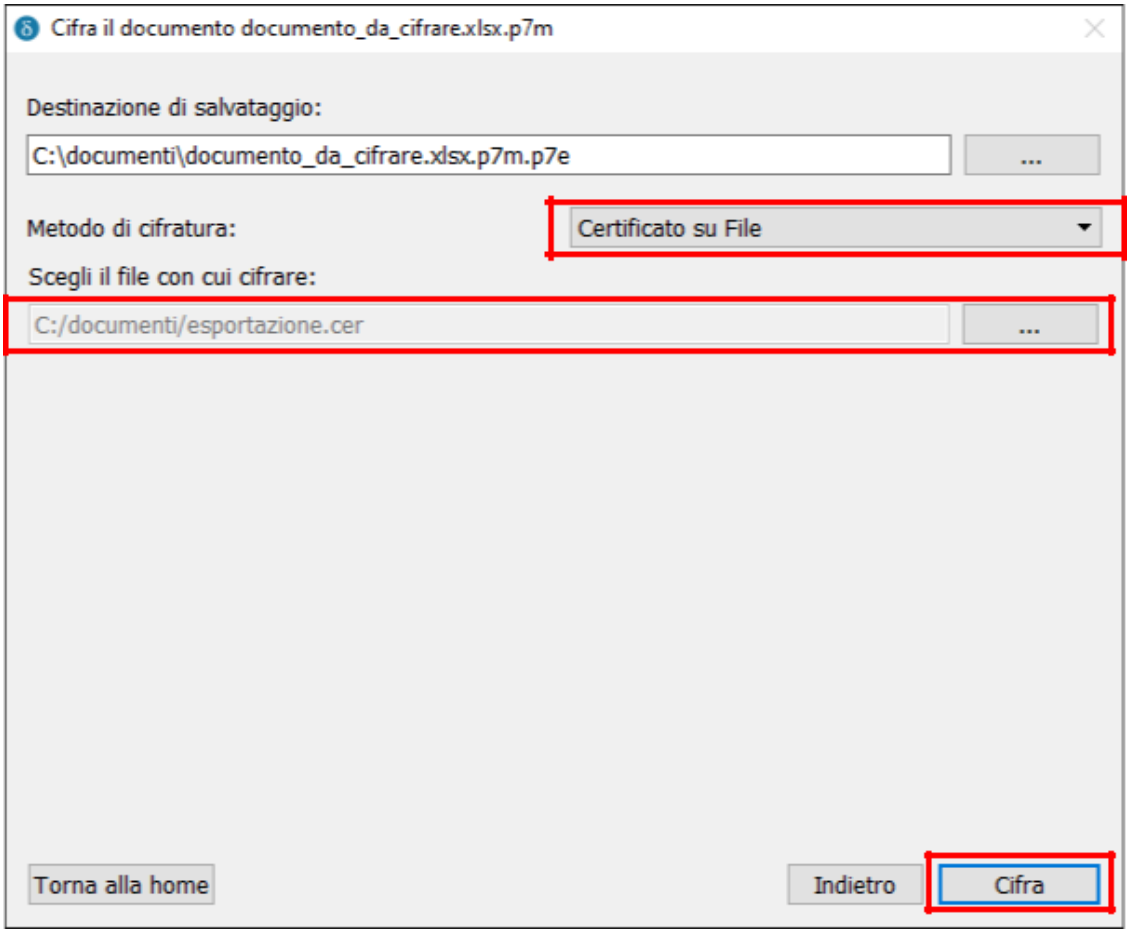


Nella finestra di riepilogo che compare cliccare su CONTINUA.



Nella finestra successiva:

- **Destinazione di salvataggio:** cartella in cui sarà salvato il file cifrato, di default è la stessa del file originale, con estensione P7E.
- **Metodo di cifratura:** aprire il menu a tendina e **selezionare CERTIFICATO SU FILE.**
- **Scegli il file con cifrare:** cliccare sul pulsante … e **selezionare il file di chiave pubblica** precedentemente scaricato.
- **Cliccare su CIFRA.**



La finestra successiva mostra il messaggio di conferma relativo alla cifratura.