BANCA D'ITALIA
EUROSISTEMA

MANUALE DI UTILIZZO DEL SOFTWARE DI FIRMA E CIFRATURA "ARUBA SIGN"

PKI BI PUBLIC KEY INFRASTRUCTURE

Febbraio 2025 v1.6

Sommario

Glossario

PKCS#12	PKCS #12 definisce un file contenitore di diversi oggetti crittografici, come ad esempio certificati e chiavi private.
LDAP	Lightweight Directory Access Protocol: RFC4511. È un protocollo che fornisce l'accesso a servizi di directory distribuiti che agiscono in conformità ai modelli di dati e servizi X.500.
CA	Certification Authority: componente di una PKI con compito di gestione del ciclo di vita dei certificati
PKCS#7	(CMS - Cryptographic Message Syntax) è una sintassi standard per la memorizzazione di dati firmati e/o crittografati
CAdES	Formato di firma introdotta dalla Decisione di esecuzione (UE) 2015/1506). Tutti i file possono essere firmati con questo formato; viene creata una busta crittografica che contiene il file da firmare.
PAdES	Formato di firma introdotta dalla Decisione di esecuzione (UE) 2015/1506). Tipologia di firma applicabile al solo formato PDF
XAdES	Formato di firma introdotta dalla Decisione di esecuzione (UE) 2015/1506). Tipologia di firma applicabile al solo formato XML.
FEA	La firma elettronica avanzata (FEA) è un particolare tipo di firma elettronica. «*insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati*»
OCSP/CRL	L'OCSP (Online Certificate Status Protocol) è un'alternativa all'elenco di revoca dei certificati (CRL) ed è utilizzato per verificare se un certificato digitale è valido o se è stato revocato
Funzione HASH	Le funzioni hash (SHA1, SHA2, ecc) sono funzioni che dato un input (es. file, stringa di lunghezza arbitraria) produce una sequenza di bit (o una stringa) di lunghezza fissa.

1. Introduzione

Il *tool ArubaSign* è un software che consente di utilizzare i certificati elettronici per:

- firmare un documento;
- cifrare un documento;
- verificare la validità della firma con cui è stato sottoscritto un documento;
- decifrare un documento cifrato;
- apporre marche temporali;
- verificare gli utenti per cui è stato cifrato un file.

Alcune operazioni, quali la firma di un documento o la decifratura di un documento crittografato, richiedono che l'utente disponga di un certificato elettronico residente su dispositivo crittografico, come una smart card o un token USB, oppure su file in formato PKCS#12.

Per svolgere altre operazioni, quali la cifratura di un documento, occorre invece disporre dei certificati elettronici con la **chiave pubblica** dei destinatari. Tali certificati possono risiedere su un archivio locale del PC su cui è installato il *tool* oppure essere disponibili su un server LDAP raggiungibile attraverso la rete (il destinatario potrà decifrare il documento utilizzando il proprio certificato elettronico, c.d. **chiave privata** – cfr. infra).

2. Concetti di base

Il certificato

Il certificato è un piccolo file contenente informazioni essenziali per la verifica della firma:

- il nome ed il codice fiscale dell'utente titolare (es. Mario Rossi, RSSMRA30A01H501I);
- il nome dell'azienda di appartenenza, se applicabile;
- il nome dell'ente certificatore (es. Banca d'Italia);
- la data di inizio e la data di fine validità;
- la chiave pubblica del titolare;
- altre informazioni di servizio.

Il certificato viene rilasciato all'utente da un ente terzo fidato, detto certificatore (*Certification Authority*, CA).

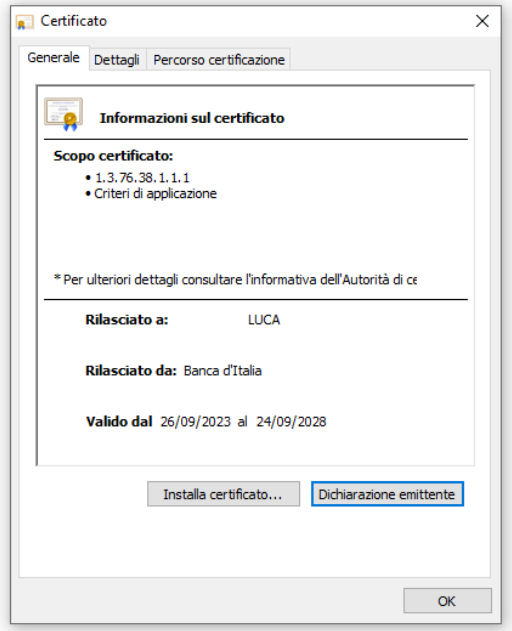

Figura 1 - Certificato digitale

Cifratura (crittografia)

La cifratura (detta anche crittografia[1]) di un documento è un'operazione con la quale si rende quel documento completamente illeggibile per chiunque, ad eccezione di chi possiede la chiave che permette di decifrarlo, ossia riportarlo "in chiaro". La cifratura, dunque, permette di assicurare la confidenzialità di informazioni riservate.

Crittografia asimmetrica

Per crittografia asimmetrica, conosciuta anche come crittografia a chiave pubblica, si intende un tipo di crittografia nel quale ad ogni attore coinvolto nella comunicazione è associata una coppia di chiavi: la chiave pubblica, che deve essere distribuita, e la chiave privata, appunto personale e segreta.

[1] Anche se spesso i termini sono utilizzati come sinonimi, la crittografia è più propriamente la tecnica che permette di cifrare il documento, mentre la cifratura è l'applicazione della chiave crittografica al documento in maniera da renderlo inintelligibile.

La proprietà fondamentale è che se si usa una chiave per cifrare, l'unico modo per decifrare è utilizzare l'altra. In questo esempio andremo a mostrare come, con l'ausilio delle chiavi, si riesce a implementare la proprietà di *confidenzialità*.

Obiettivo: Marco vuole inviare un documento cifrato a Roberto.

Condizioni iniziali: Roberto possiede una coppia di chiavi, una privata nota solo al possessore ed una pubblica nota a tutti.

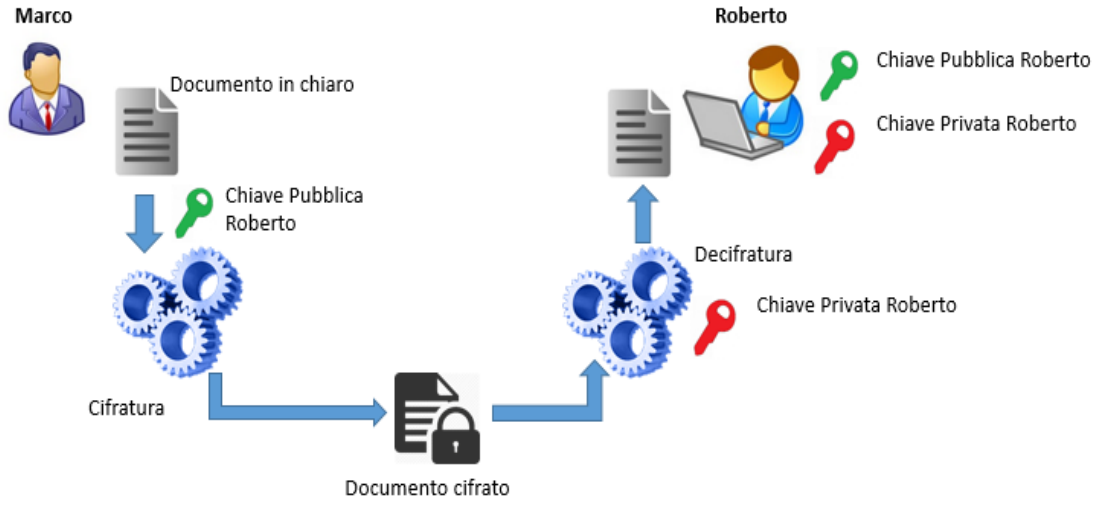

Figura 2 Crittografia asimmetrica

Flusso:

1. Marco cifra il documento con la chiave pubblica di Roberto
2. Il documento cifrato è spedito a Roberto
3. Roberto decifra il documento con la sua chiave privata

Firma digitale

La firma digitale è un'operazione con la quale si genera un codice crittografico che dimostra l'identità e l'integrità di un documento. In altre parole, la firma digitale permette di verificare che il documento:

- è stato firmato da una ben precisa persona;
- non ha subito modifiche successivamente all'apposizione della firma.

La firma digitale si basa su algoritmi crittografici che richiedono il possesso, da parte dell'utente, di una chiave privata e di un corrispondente certificato.

Figura 3- Smart card

Figura 4 - Token USB

La chiave privata ed il certificato sono normalmente memorizzati su un dispositivo elettronico simile ad una carta di credito, chiamato smart card, oppure su un token USB (in entrambi i casi si tratta di microchip con funzionalità crittografiche).

In fase di generazione della firma, è necessario digitare il PIN della propria smartcard o dispositivo USB.

Dopo aver generato una firma digitale, questa viene solitamente salvata in un file detto busta crittografica; la busta contiene normalmente anche il documento di partenza ed il certificato del firmatario, così da tenere insieme tutte le informazioni necessarie per la verifica.

Esistono diversi formati di busta crittografica[2]; il più diffuso è quello conosciuto come PKCS#7 (in tal caso il file ha l'estensione P7M).

Affinché la firma digitale abbia un pieno valore legale (in tal caso si parla di firma qualificata), devono essere rispettate diverse norme di legge che stabiliscono requisiti relativi alle chiavi, al certificato, alla smartcard, al certificatore, al formato della busta crittografica, eccetera.

Firma digitale con crittografia asimmetrica

Per capire facilmente cosa è la firma digitale, proveremo a spiegarla con l'aiuto dell'immagine.

Obiettivo: Alice vuole la certezza che il documento che ha ricevuto (in chiaro) provenga da Bob e non sia stato modificato.

Condizioni iniziali: Bob possiede una coppia di chiavi, una privata nota solo al possessore ed una pubblica nota a tutti.

[2] In base alla Decisione di esecuzione (UE) 2015/1506, sono ammessi i formati CAdES (*.p7m), PAdES (*.pdf), XAdES (*.xml).

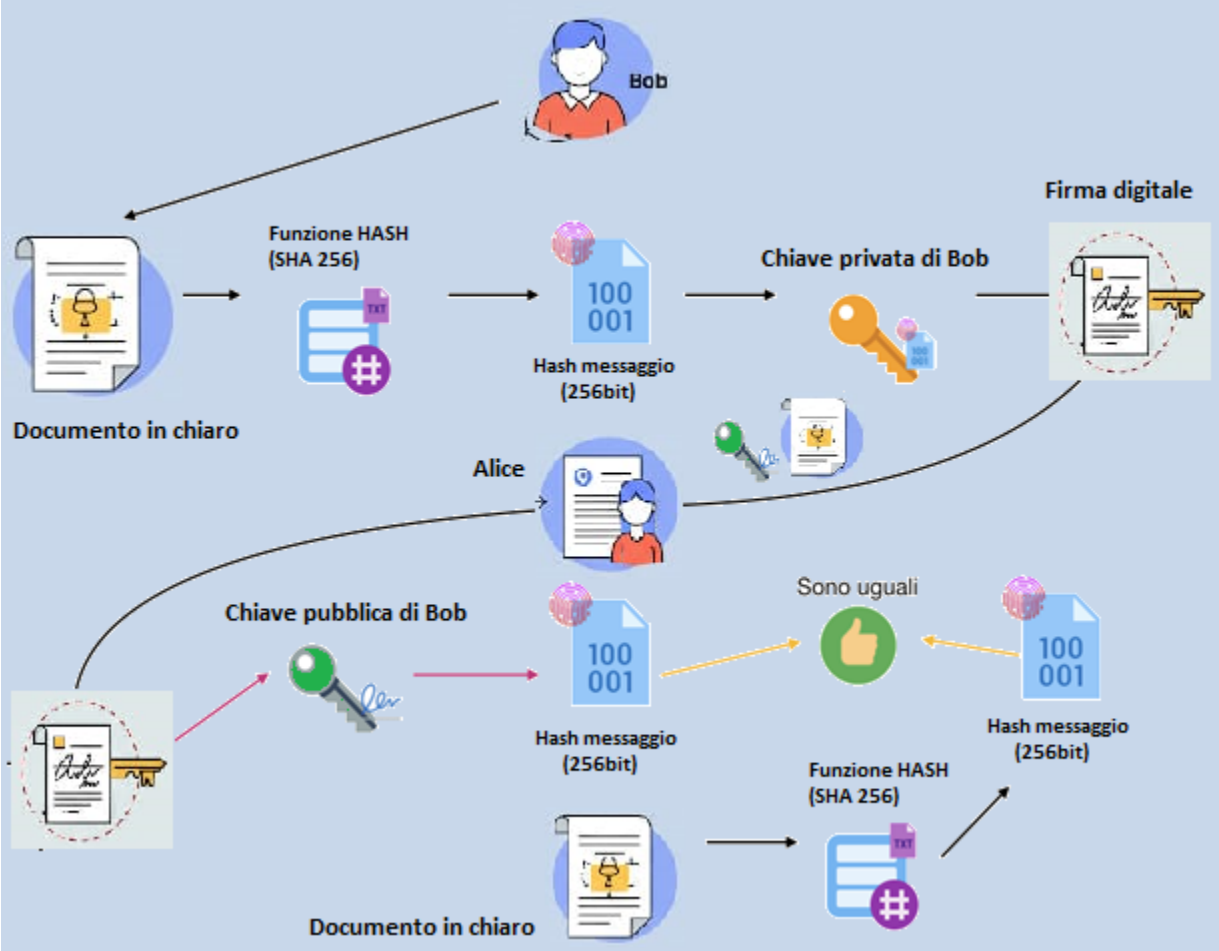

Figura 5 Firma digitale

1. Bob applica l'algoritmo di hash (SHA256 ad esempio) sul messaggio in chiaro, ottenendo così il **digest,** che rappresenta la così detta 'impronta digitale' del documento ossia una rappresentazione unica e compatta delle informazioni originali contenute nel documento.
2. Utilizza la sua chiave privata per cifrare il **digest.** Ottenendo così la firma digitale e l'autenticazione.
3. Invia ad Alice il messaggio in chiaro, la firma (ossia il digest cifrato) e la sua chiave pubblica.
4. Alice applica sulla firma la chiave pubblica di Bob ottenendo così il digest.
5. Alice applica sul messaggio in chiaro lo stesso algoritmo di hash (SHA256) ottenendo a sua volta il digest del messaggio.
6. Alice confronta il digest appena ottenuto con quello ricevuto da Bob. Se i digest sono uguali la firma è stata verificata e siamo sicuri che il messaggio non è stato alterato.

N.B.: ricorda che se il messaggio cambia il digest non è più lo stesso.

3. Link e menu contestuale

Per accedere alla procedura, è possibile utilizzare l'icona sul desktop, creata durante l'installazione del tool o in alternativa tramite la funzionalità di ricerca del sistema operativo.

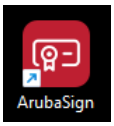

Figura 6 Icona sul dekstop

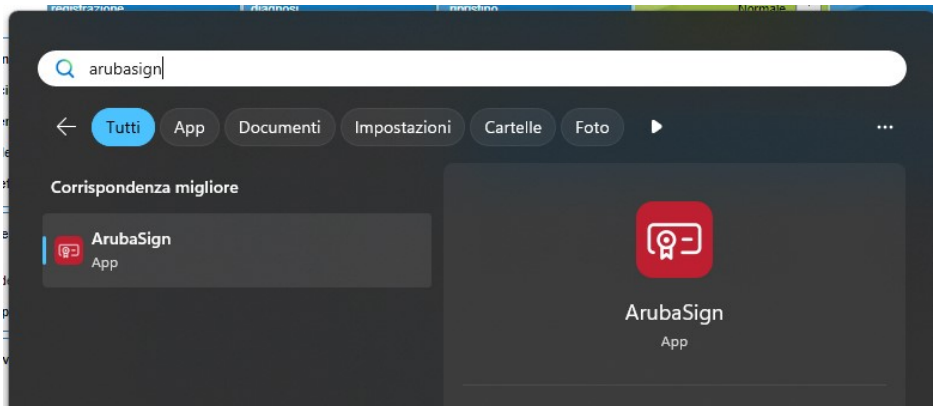

Figura 7 Ricerca del tool tramite ricerca di windows

Le funzionalità di ArubaSign, una volta che il software è installato, vengono richiamate anche dal menu contestuale che si apre cliccando con il tasto destro sul nome di un file:

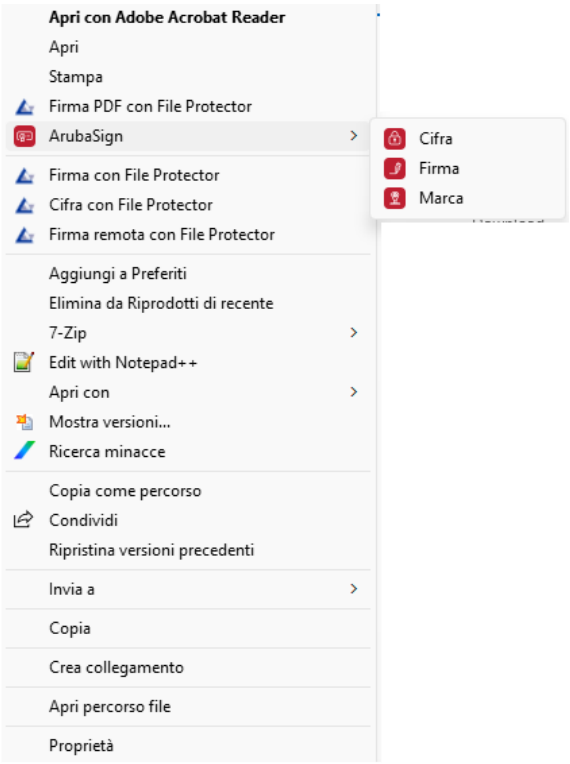

Figura 8 Menu contestuale di Aruba Sign

4. Primo Avvio e layout di Base

Il *tool ArubaSign* si presenta al primo avvio con un piccolo *wizard*, dove presenta un *layout* rinnovato, un menu di navigazione con TAB e una modalità di apposizione della firma grafica ridisegnata.

Figura 9 Schermata di benvenuto al primo avvio

4.1. Funzionalità

Questo menu permette l'abilitazione e disabilitazione dei TAB. È possibile abilitare i seguenti pannelli:

- Cifra
- Decifra
- Marca (temporale)
- Destinatari file Cifrati

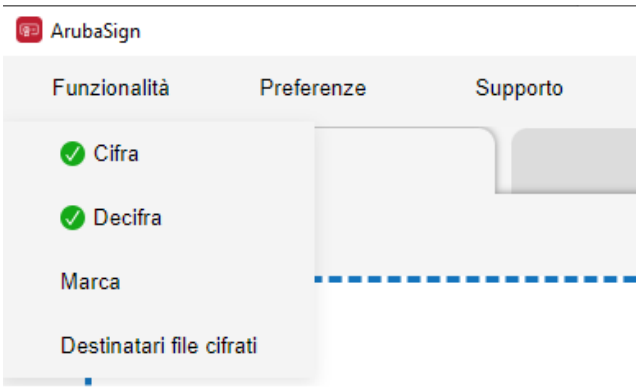

Figura 10 Lista delle funzionalità abilitabili

Le singole funzionalità saranno analizzate in dettaglio nel seguito.

4.2. Preferenze

Il pannello preferenze dispone delle seguenti categorie:

- Generali
- Funzionalità
- Firma
- Firma Grafica PAdES
- Verifica
- Gestione carta
- Database certificati
- Avanzate

Figura 11 Categorie di personalizzazione del tool

4.2.1. Generali

In questo pannello è possibile scegliere la lingua del *layout*, selezionare la cartella di destinazione dei file firmati ed eventualmente aprirla automaticamente dopo aver apposto la firma.

È inoltre configurabile il fuso orario della data utilizzata durante la firma. Di norma dovrebbe essere UTC, ma settando il *timezone* in figura si allinea a quello usato in Italia.

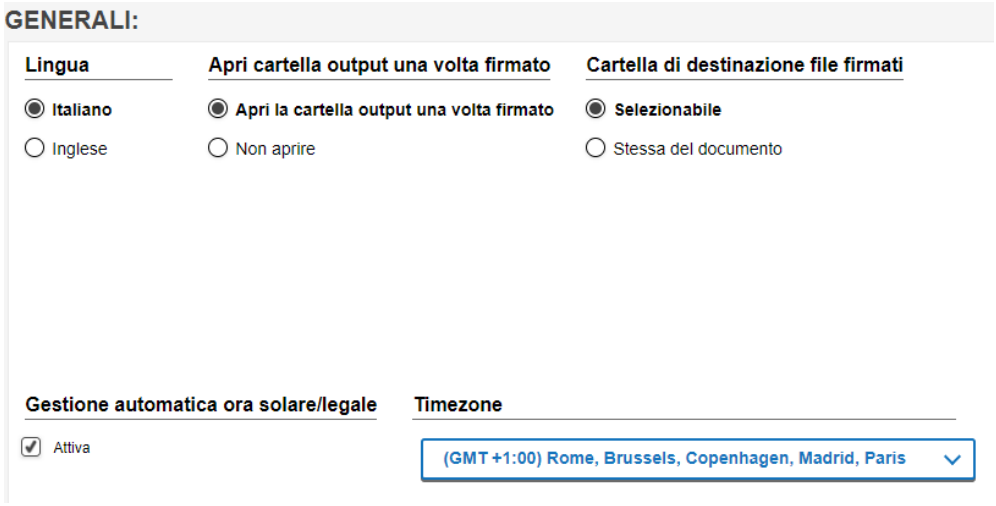

Figura 12 Personalizzazioni di natura generale

4.2.2. Funzionalità

Questo pannello permette l'abilitazione dei TAB di Cifra, Decifra e marca temporale, impostandone l'abilitazione automatica all'avvio.

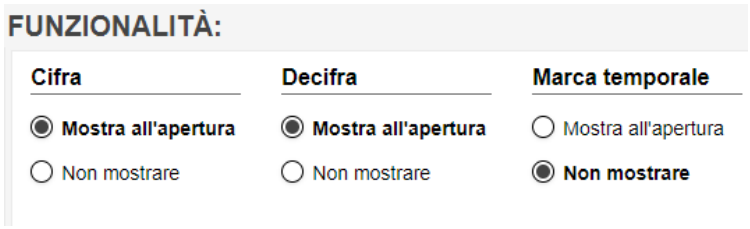

Figura 13 Personalizzazione dei Tab/funzionalità da mostrare all'avvio

4.2.3. Firma

Questo pannello imposta le preferenze della firma, intesa come formato di firma in base alla tipologia di file, sia esso PDF o XML. In basso, l'opzione di abilitare la marca temporale per ogni apposizione di firma.

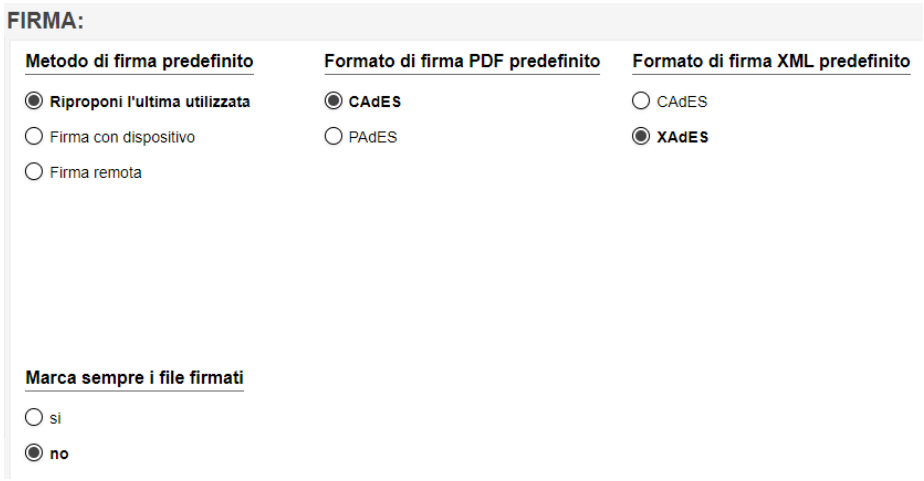

Figura 14 Personalizzazioni per la firma digitale

4.2.4. Firma Grafica PAdES

La firma PAdES grafica è configurabile in dettaglio, abilitando un'immagine che può essere anche personalizzata, aggiungendo al glifo anche attributi quali la data, la località e il motivo.

Infine, per gli aspetti di compatibilità, è possibile mantenere il formato documentale PDF/A.

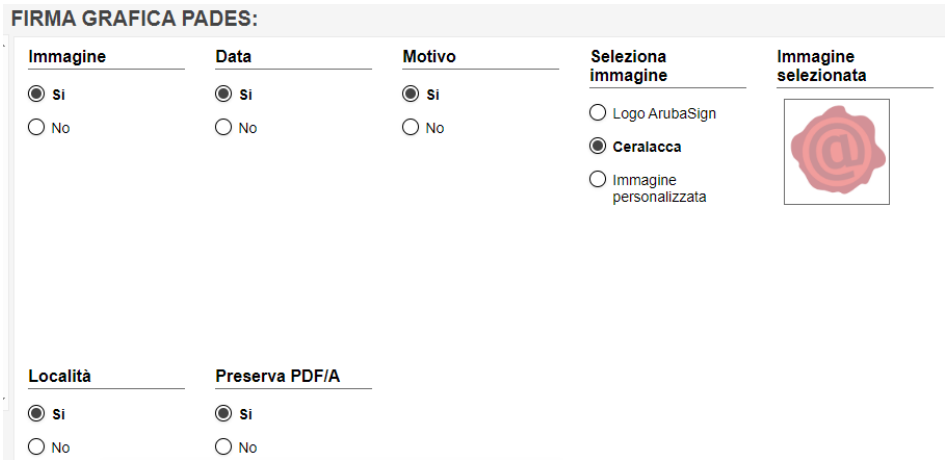

Figura 15 Personalizzazioni firma PAdES

4.2.5. Verifica

In questo pannello è possibile personalizzare l'esperienza utente durante la verifica di un file firmato. Si noti la possibilità di abilitare anche la verifica FEA (Firma Elettronica Avanzata, non qualificata) e il meccanismo di verifica dello stato di un certificato (OCSP/CRL).

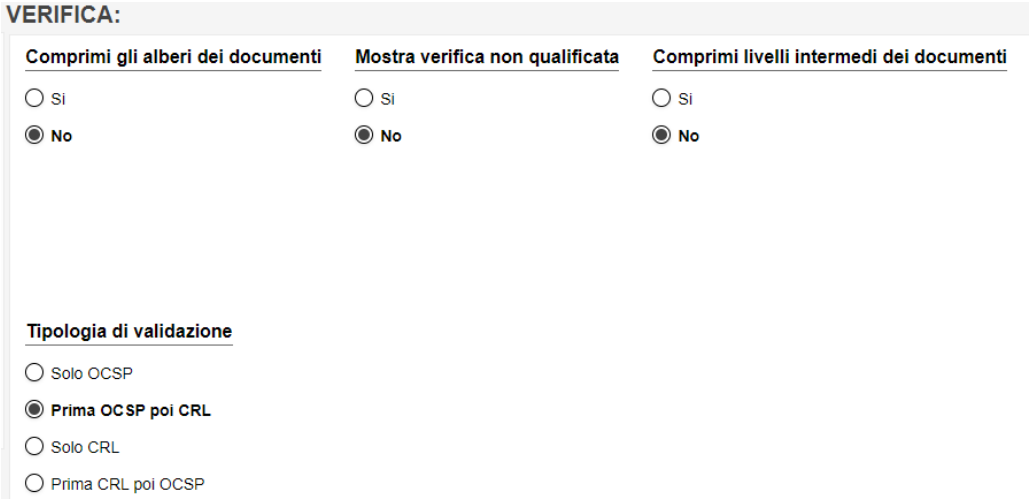

Figura 16 Opzioni per la verifica di un file firmato

4.2.6. Gestione carta

Questo pannello è di grande utilità nella gestione del dispositivo crittografico (smart card), nei casi di cambio PIN, sblocco e cambio PUK.

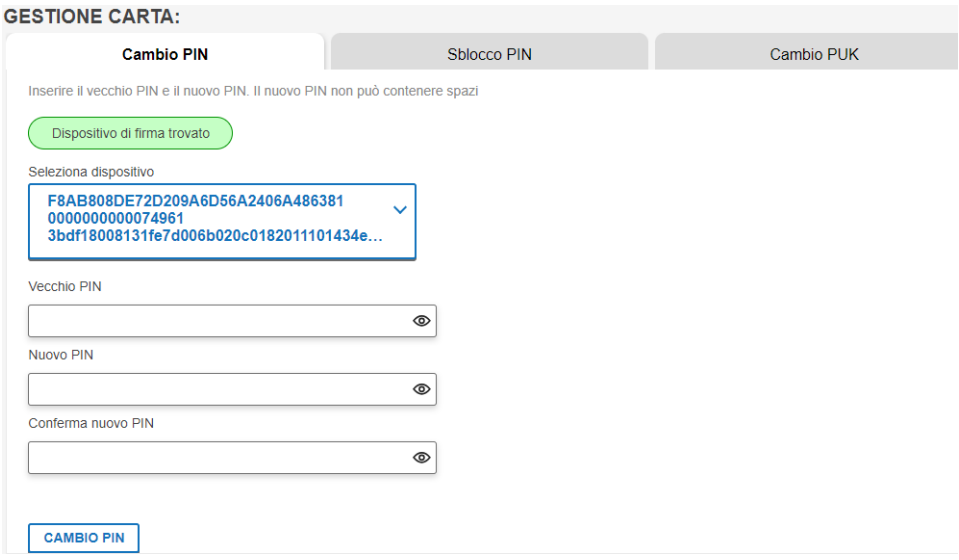

Figura 17 Form per la modifica del PIN

4.2.7. Database certificati

Questo pannello mostra la lista dei certificati contenuti nel suo Database interno. Si possono distinguere i certificati delle Autorità di certificazione (CA), tra cui quelle contenute nelle *trusted list*

eIDAS, ma possono essere caricati anche certificati personali o di terzi utilizzabili nella crittografia di file. È possibile l'importazione sia da file che dai server LDAP di Banca d'Italia.

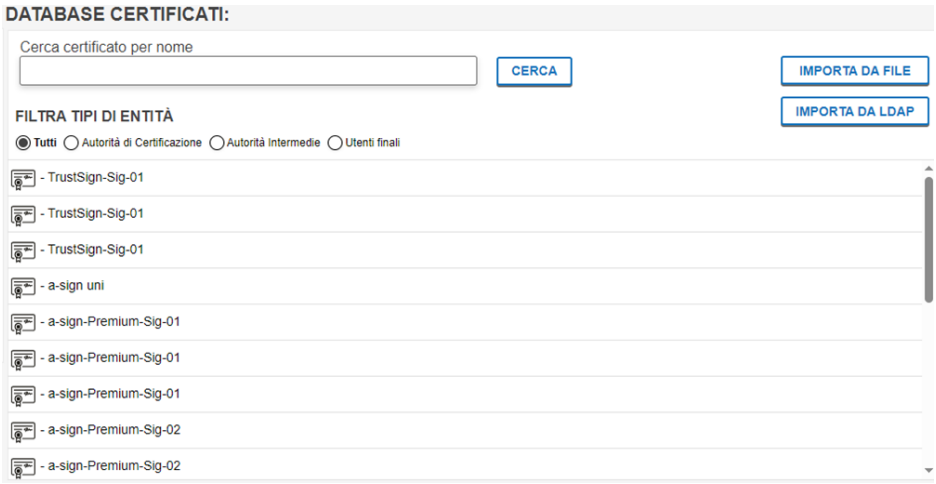

Figura 18 Repository dei certificati affidabili censiti nel tool

4.2.8. Avanzate

In questa sezione è possibile abilitare il log del *tool*, eventualmente con un livello di verbosità crescente e la possibilità di esportarlo.

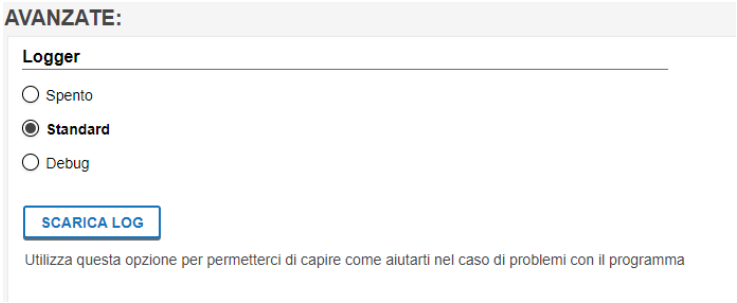

Figura 19 Abilitazione Logger

4.3. Supporto

In questa sezione è possibile navigare tra le opzioni di supporto all'utilizzo del *tool*. Tramite pulsante Videoguide si aprirà il sito del produttore con utili videoguide a supporto delle varie operazioni disponibili; l'opzione "Guida OnLine" è un collegamento al presente manuale, mentre il pulsante finale rimanda al piccolo *wizard* che è stato presentato al primo avvio del *tool*.

Figura 20 Lista delle modalità di supporto all'uso del prodotto

5. Firmare e verificare un file

Per poter firmare un file, è necessario disporre di almeno un certificato valido di firma sulla propria smart card.

Nel caso in cui la smart card contenga più di un certificato, in fase di firma sarà necessario scegliere il certificato desiderato.

Si può avviare la firma digitale di un file in tre modi diversi, descritti di seguito:

- dall'esterno dell'applicazione, attraverso il menu contestuale di Windows;
- dall'interno di *ArubaSign*, mediante la funzionalità di "*Drag&Drop*";
- dall'interno di *ArubaSign*, selezionando il file da una cartella.

Qualsiasi dei metodi evidenziati inizializzerà il pannello del TAB firma, come da figura.

In base alla tipologia del file, il menu a tendina “Seleziona il formato di firma” si valorizzerà con tutte le possibili tipologie compatibili[3] (es. P7m per tutte le tipologie di file, PAdES per i file di tipo PDF e XAdES per i file in formato XML).

Figura 21 Pannello per l'apposizione della firma

Si evidenzia che:

- è possibile editare contestualmente il nome del file firmato e la personalizzazione del percorso dove sarà salvato il file;
- aggiungere arbitrariamente altri file così da eseguire anche firme massive/multiple in un solo blocco.

[3] In alcuni scenari è proposta anche la firma PAdES, suggerendo una implicita conversione in PDF prima della firma.

5.1. Firma PAdES grafica

Nei casi in cui sia possibile apporre una firma grafica, il *tool* automaticamente la propone.

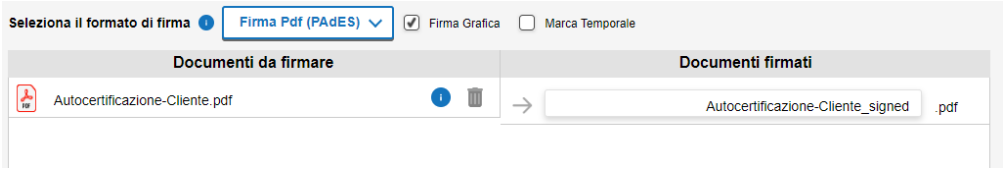

Figura 22 Evidenza della possibilità di apporre una firma grafica

Continuando poi nella fase successiva, tramite il pulsante “prosegui” verrà proposta una *preview* del documento in cui andare a selezionare col mouse l’area da utilizzare per apporre il glifo della firma digitale.

Cliccando sul menu Opzioni, a destra del pannello, compariranno le funzionalità di personalizzazione di tale glifo.

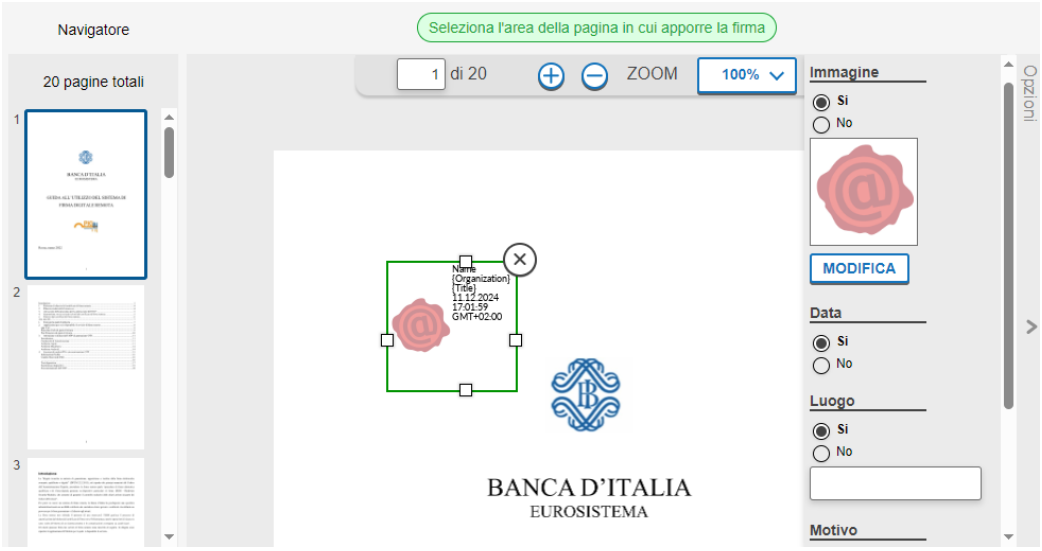

Figura 23 Selezione dell'area dove verrà apposto il glifo della firma digitale

A completamento di questa fase e dopo aver cliccato su “Prosegui e Firma” compare il pannello in figura per la selezione della modalità di firma: Firma remota o Firma con dispositivo (smart card/token).

Figura 24 Form per la selezione della modalità di firma digitale

Nella firma con dispositivo, verrà automaticamente popolato il menu a tendina con i certificati di firma disponibili e dopo aver compilato anche il campo PIN si potrà procedere con la Firma.

A verifica del buon esito della firma comparirà il *pop-up* in figura e nel caso si sia scelta, tra le opzioni, l'apertura della cartella dopo la firma, anche quest'ultima.

Figura 25 Popup di stato per la corretta apposizione della firma

5.2. Firme multiple

Ad un medesimo documento possono essere apposte più firme digitali; si parla in tal caso di "firme multiple". Questo consente di dimostrare che più persone hanno assunto la paternità e/o la responsabilità del documento, eventualmente in momenti diversi, così come spesso avviene nel caso della tradizionale firma autografa (basti pensare ai contratti, ai bilanci, ecc.).

Esistono tre tipologie di firme multiple:

- firme "a matrioska";
- firme parallele (anche dette indipendenti);
- contro-firme (anche dette annidate).

5.2.1. Firme "a matrioska"

Il primo tipo si ottiene semplicemente firmando una busta crittografica P7M (che contiene un documento già firmato). Questa operazione digitale equivale, nel mondo della carta, a firmare una busta che contiene un documento firmato, ciò che in effetti a volte viene fatto (si pensi alle buste che contengono le offerte in risposta a bandi di gara). Per effettuare una firma "a matrioska" è sufficiente selezionare un file firmato e risottomettere la firma. Ogni firma aggiungerà un livello al file, come da evidenze nel paragrafo seguente.

5.2.1.1. Verifica Firme "a matrioska"

Nell'esempio andremo a vedere come ad un file, firmato più volte, venga aggiunto un ulteriore livello di firma.

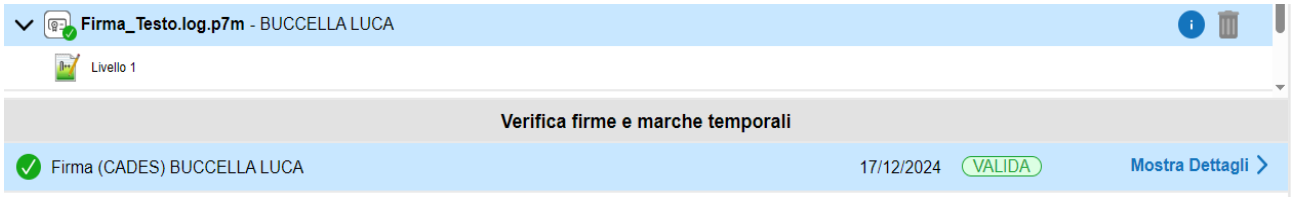

Figura 26 File firmato digitalmente una sola volta

In questo esempio il file è firmato 2 volte (2 livelli), con l'evidenza del firmatario ad ogni nodo nella struttura ad albero rappresentante i firmatari.

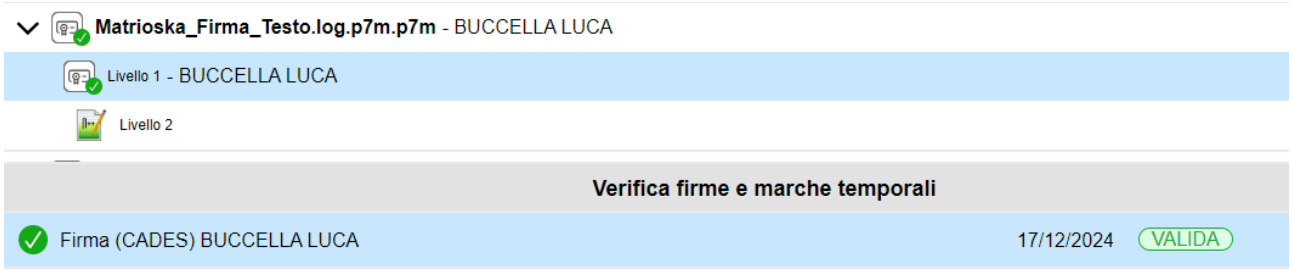

Figura 27 File firmato digitalmente due volte

Con questo approccio è possibile aggiungere N livelli di firma.

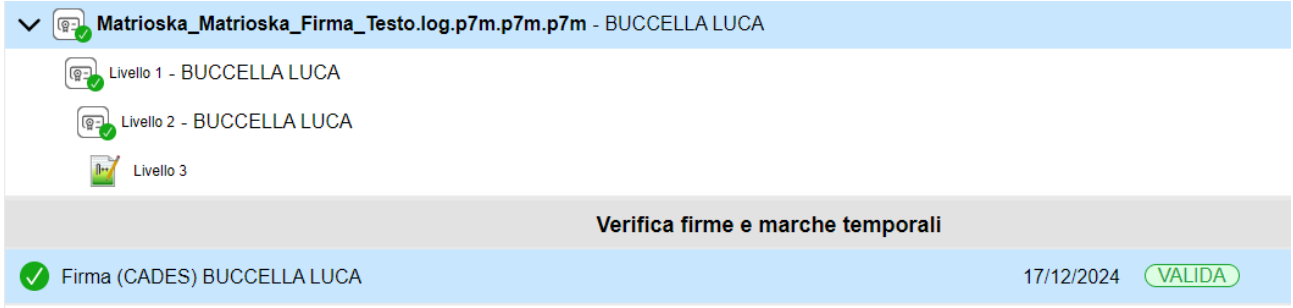

Figura 28 File firmato digitalmente tre volte

5.2.2. Firme parallele

Il secondo tipo di firma multipla (detta parallela o indipendente) consiste nell'aggiungere ulteriori firme "a fianco" della prima, dove ciascuna firma mantiene la sua indipendenza (ogni firmatario firma gli stessi dati che firmano gli altri). Questa operazione digitale equivale, nel mondo della carta, ad apporre più firme, da parte di persone diverse, in calce al medesimo documento. Per aggiungere una firma indipendente, cliccare sul bottone "Aggiungi firma" nella finestra mostrata in fase di verifica.

Figura 29 Pulsante per aggiunta di una firma parallela

5.2.2.1. Verifica Firme parallele

Nell'esempio possiamo notare come un file multi-firmato abbia un solo livello di firma, ma due firme distinte. La schermata evidenzia che le due firme sono allo stesso livello; pertanto, entrambi i firmatari hanno firmato il documento originario indipendentemente.

Figura 30 Verifica firme parallele

5.2.3. Firme annidate

Il terzo tipo di firma multipla (detta controfirma o annidata) si ottiene firmando una firma già esistente, e conservando il risultato (detto contro-firma) all'interno della medesima busta. Facendo questo, il secondo firmatario in pratica approva o "convalida" la prima firma. A sua volta, la seconda firma può essere firmata da una terza persona, e così via.

Per aggiungere una controfirma, selezionare una firma nella sezione di dettaglio della specifica firma e selezionare il bottone "**Aggiungi controfirma**". In fase di verifica, si potrà constatare che il

documento contiene la contro-firma (notare la rappresentazione ad albero nel paragrafo successivo).

5.2.3.1. Verifica Firme annidate

Anche in questo esempio, come nel caso delle firme parallele, possiamo notare che esiste un solo livello di firma, ma diversamente dal precedente c'è una relazione tra le due firme: la seconda dipende dalla prima andando ad evidenziare che la controfirma esprime la volontà di firmare il documento principale e la prima firma digitale apposta.

Figura 31 Verifica firme annidata (notare evidenza "contro firma")

6. Cifrare un file

Nel caso in cui si abbia necessità di cifrare un file, è sufficiente, previa abilitazione dello specifico TAB, trascinare il file tramite la tecnica del *Drag&Drop* oppure selezionandolo tramite il pulsante "Seleziona documenti".

Figura 32 Pannello per la cifratura dei file

Una volta selezionato, il/i file saranno raccolti in tabella, con la possibilità di aggiungerne anche altri all'occorrenza tramite il pulsante evidenziato.

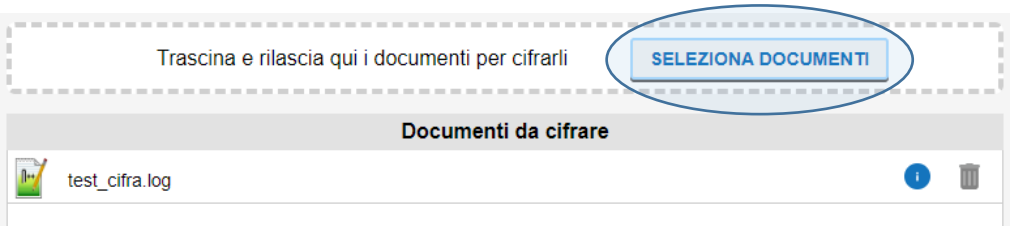

Figura 33 Inserimento ulteriori file da cifrare

Cliccando infine sul pulsante "**Prosegui e Cifra**" apparirà il pannello per la selezione dei certificati da utilizzare per la crittografia del file.

Figura 34 Opzioni di selezione del certificato di cifratura da utilizzare

È possibile selezionare il certificato nelle seguenti modalità:

- cercando sui server LDAP di banca, quali il *domain controller* (*Active Directory*) oppure i *server* della PKI;
- aggiungere un file selezionandolo manualmente, sia tramite il pulsante "Aggiungi da file" sia tramite "Seleziona certificati";
- aggiungerlo dal proprio Badge/smart card.

N.B.: selezionando l'opzione "Solo certificati validi", saranno evidenziati ed usati solo quelli conformi.

Figura 35 Filtro dei soli certificati validi tra quelli selezionati

6.1. Cifrare un file per un collega

Nel caso in cui si voglia cifrare un file per un collega, è sufficiente selezionare il pulsante “Cerca da LDAP” dal pannello in figura.

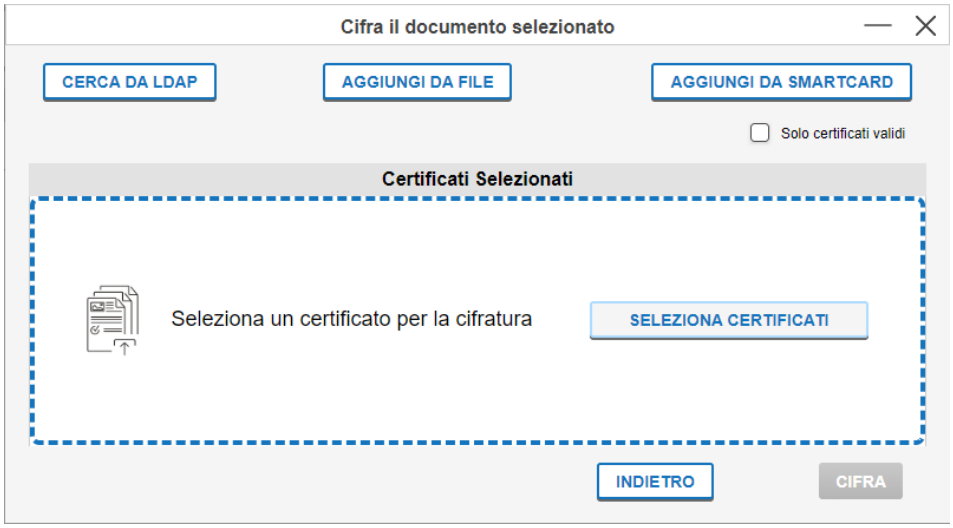

Figura 36Pannello di preselezione sorgente del certificato di crittografia da utilizzare

Successivamente, dalla finestra di ricerca, inserire i parametri di ricerca e cliccare su “Cerca”. Nella tabella sottostante apparirà la lista dei certificati disponibili che rispettano i parametri inseriti. Selezionare, tramite apposito pulsante, il certificato da utilizzare.

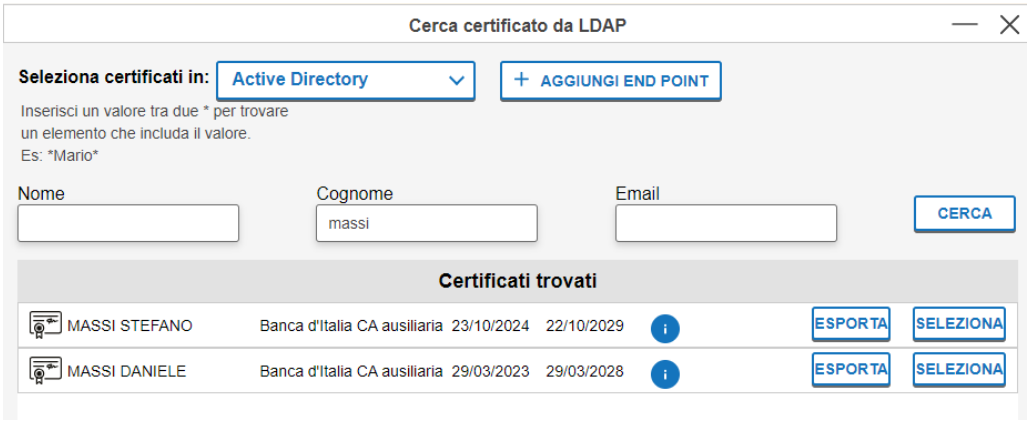

Figura 37 Seleziona certificato dopo ricerca LDAP

È possibile effettuare ricerche successive; il *tool* memorizzerà la lista dei certificati “selezionati” e al termine li riepilogherà in tabella.

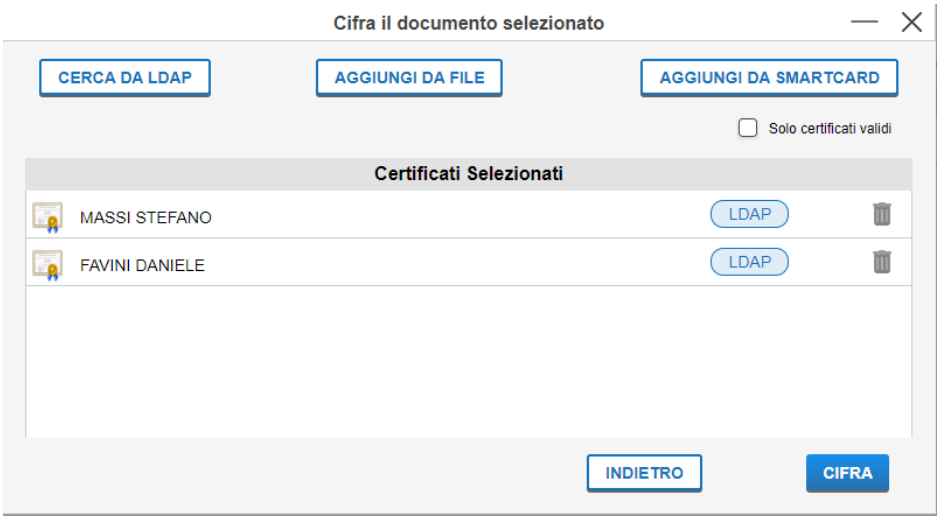

Figura 38 Riepilogo dei certificati per cui sarà effettuata la crittografia

Il processo si concluderà dopo aver premuto il pulsante “Cifra” con il pop-up in figura.

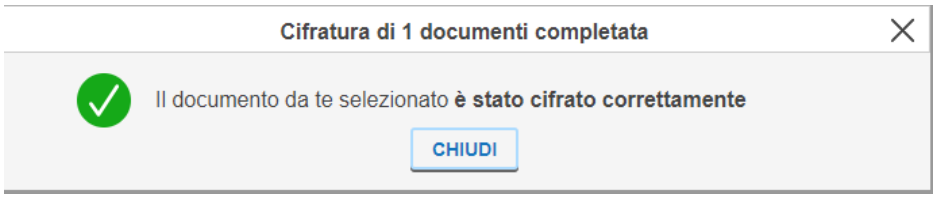

Figura 39 Popup di corretta cifratura del file

7. Decifrare un file

Nel caso in cui si abbia necessità di decifrare un file è sufficiente, previa abilitazione dello specifico TAB, trascinare il file tramite tecnica del *Drag&Drop* oppure selezionandolo tramite il pulsante “Seleziona documenti”.

Figura 40 Selezione Tab "Decifra"

Dopo aver selezionato il/i file verrà proposta una finestra di riepilogo con i file selezionati a cui si potranno aggiungere o rimuoverne altri file.

Cliccando sul pulsante “**Prosegui e Decifra**” verrà proposta una finestra di riepilogo dei file raggruppati per certificato (sono riportati il numero seriale e la *Certification Authority* per ognuno dei certificati usati per cifrate lo specifico file).

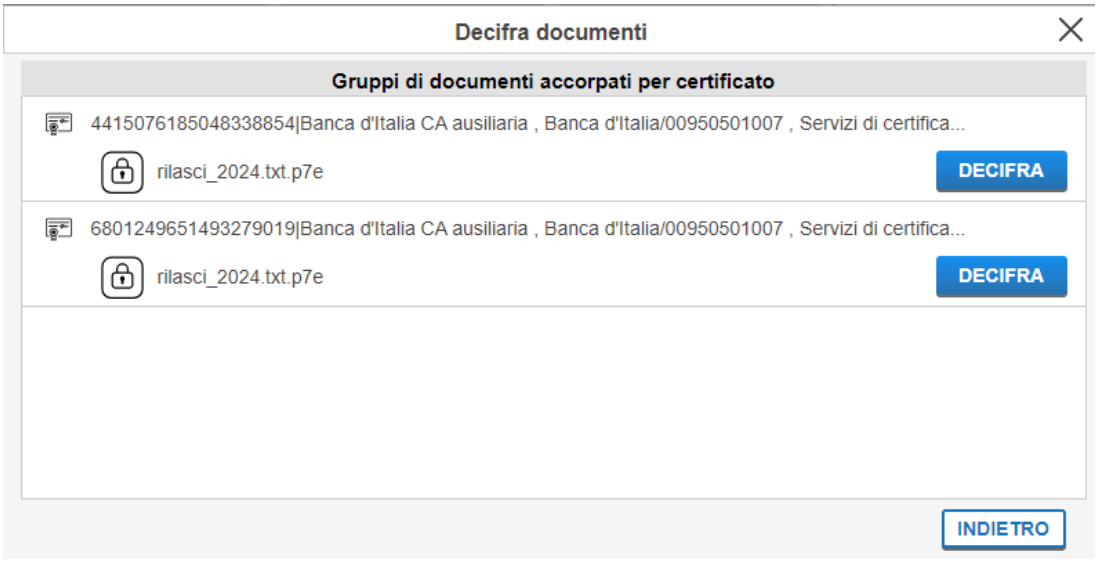

Figura 41 Tabella di riepilogo dei certificati per cui è stato cifrato il/i file

Cliccando sul pulsante ”**Decifra**” verrà proposto quale contenitore usare per decifrare (smart card o file pkcs12). Nel caso in cui non venga trovato alcun certificato utile alla decrittografia, tra quelli resi disponibili, verrà mostrata una finestra di errore come in figura.

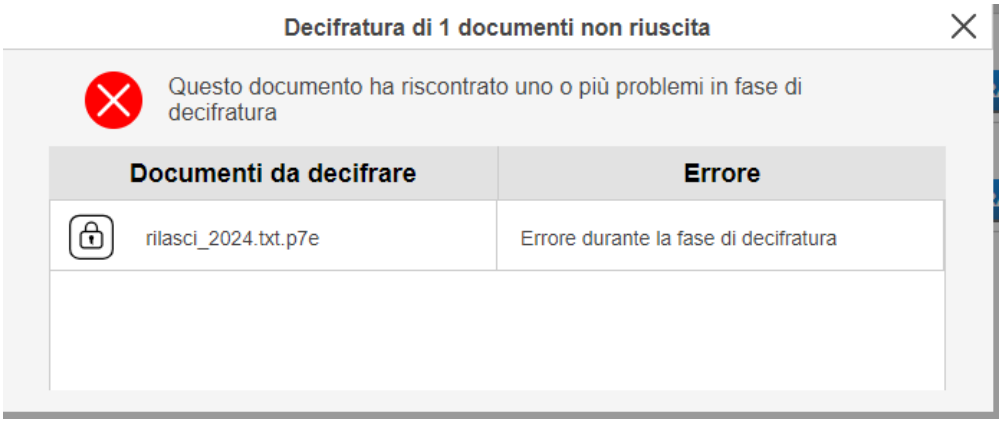

Figura 42 Popup di errore alla decifratura

8. Marcare temporalmente un file

Nel caso in cui si abbia necessità di marcare temporalmente un file, è sufficiente, previa abilitazione dello specifico TAB, trascinare il file tramite la tecnica del *Drag&Drop* oppure selezionandolo tramite

il pulsante “Seleziona documenti”. Successivamente, dalla finestra di riepilogo sarà possibile scegliere lo specifico formato[4] e procedere con l’apposizione della marca.

Figura 43 Pannello aggiunta marca temporale

9. Destinatari file cifrati

Il *tool* mette a disposizione anche la funzionalità di recupero della lista degli utenti per cui è stato cifrato un file, tramite il menu “**Funzionalità**” e il link “**Destinatari file cifrati**”.

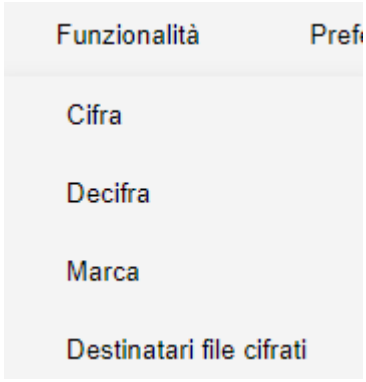

Figura 44 Tendina di selezione della funzionalità "Destinatari file cifrati"

[4] **Formato TSR**: è il formato più semplice e contiene solo l'impronta del file, NON tutto il file, e l'evidenza informatica della marcatura effettuata. Per verificare un file TSR è necessario disporre del file originale che si è marcato.

Formato TSD: è un formato che contenere sia l'evidenza della marca temporale (il file con formato TSR) che il file stesso sottoposto a marcatura, per questo motivo il file stesso può essere sottoposto a procedura di verifica in quanto contiene tutte le informazioni necessarie al controllo.

Selezionando un file, o una specifica cartella, il *tool* recupererà per ogni file la lista dei nominativi (con relativo numero seriale del certificato) per i quali è stato cifrato lo specifico file. Sarà anche mostrato lo stato attuale del certificato (opzionalmente anche con verifica via CRL).

Figura 45 Tabella di estrazione dei destinatari di un file cifrato