COR Difesa

Ministero della Difesa

Kit di Firma

Suite di Firma, Cifra, Marcatura e Verifica

Manuale Utente

Versione 5.5.2.4

Autore:	Ministero Della Difesa – S.M.D. COR Difesa
Versione:	5.5.2.4
Data del documento:	Gennaio 2024
No Doc.:	PTC-PDS-4920

Contenuto

Sintesi Direzionale 4

1 Introduzione 5

1.1 Requisiti software 5

1.2 Requisiti hardware 6

1.3 Limiti noti 6

1.3.1 Estensioni file dei documenti 6

1.3.2 Limiti della firma PDF 7

1.3.3 Limiti della firma XML 7

2 Procedure di installazione e disinstallazione 8

2.1 Installazione di Kit di Firma 8

2.2 Aggiornamento di Kit di Firma 11

2.3 Disinstallazione di Kit di Firma 12

2.4 Software aggiuntivo 13

2.4.1 Installazione di Smart Card API 13

2.5 Possibili problemi 13

2.5.1 Avvisi di sicurezza 13

2.5.2 Aggiornamento fallito 17

3 L'applicazione Kit di Firma 18

3.1 Primo avvio dell'applicazione 21

3.2 Messaggistica di errore 22

3.3 Operazioni di Firma 23

3.3.1 Formato CAdES 29

3.3.2 Formato PAdES 36

3.3.3 Formato XAdES 41

3.3.4 Formato ASiC-E 48

3.3.5 Dettagli sulle operazioni di Firma 58

3.3.6 Firma Multipla 65

3.4 Operazioni di Marcatura Temporale 70

3.4.1 Creazione di un documento Time Stamped Data 72

3.4.2 Richiesta di una Time Stamp Request 73

3.4.3 Richiesta di un Time Stamp Token 75

3.4.4 Creazione di un contenitore ASiC-E TST 77

3.4.5 Estensione di un contenitore ASiC-E TST 78

3.5 Operazioni di Cifra 80

3.5.1 Aggiunta di un Destinatario da Store 88

3.5.2 Aggiunta di un Destinatario da File 89

3.5.3 Aggiunta di un Destinatario da LDAP 91

3.6 Operazioni di Verifica 93

3.6.1 Verifica di un documento firmato 93

3.6.2 Casi particolari di documenti firmati 105

3.6.3 Verifica di marche temporali 117

3.7 Operazioni di Decifra 126

3.8 Operazioni di anteprima del documento 130
3.8.1 Anteprima di documenti generici 132
3.8.2 Anteprima di documenti testuali 135
3.8.3 Anteprima di documenti XML e XAdES 135
3.9 Certification Authority Accreditate 139
3.9.1 Aggiornamento manuale della lista 140
3.9.2 Visualizzazione della lista 144
3.10 Configurazione 146
3.10.1 Servizi 146
3.10.2 Avanzate 147
3.10.3 Proxy 149
3.10.4 PAdES 151
3.10.5 Aspetto 155
3.10.6 Impostazioni Predefinite 156
3.10.7 Assistenza 157
3.11 Informazioni sugli aggiornamenti 159
3.12 Gestione della smart card 160
3.12.1 Informazioni sulla carta 160
3.12.2 Attivazione della Carta 163
3.12.3 Gestione dei PIN della carta 164
4 Ulteriori informazioni 167
4.1 Produrre documenti in formato PDF/A 167
4.2 Registrare una sessione di lavoro su Windows 7 e successivi 172
4.3 Problemi noti 173

Sintesi Direzionale

Il presente manuale fa riferimento alla procedura di installazione dell'applicazione **Kit di Firma** e al suo utilizzo.

Nella sezione *Introduzione* viene introdotta l'applicazione Kit di Firma, le principali funzionalità e i requisiti software e hardware dell'applicazione. Segue una sezione che elenca le *Procedure di installazione e disinstallazione*. Le funzionalità dell'applicativo vengono dettagliate nella sezione *L'applicazione Kit di Firma*.

1 Introduzione

Kit di Firma è l'applicazione desktop completa per la firma digitale, la cifra/decifra, la marcatura temporale, la verifica della firma e la verifica delle marcature temporali secondo le normative europee e italiane in ambito di firma digitale e marcatura temporale.

Kit di Firma permette di eseguire le seguenti operazioni:

- Firma digitale e qualificata di un documento in formato PKCS#7 Signed Data, CAdES, PAdES, XAdES, ASiC, con la possibilità di aggiungere marcature temporali della firma e di aggiungere informazioni per la lunga conservazione.
- Firma digitale e qualificata parallela di un documento in formato PKCS#7 Signed Data, CAdES, XAdES, ASiC, con la possibilità di aggiungere marcature temporali della firma e di aggiungere informazioni per la lunga conservazione.
- Verifica dei documenti firmati digitalmente nei formati PKCS#7 Signed Data, CAdES, PAdES, XAdES, ASiC con o senza marcature temporali e con uno o più livelli di firme parallele e controfirme
- Controfirma digitale e qualificata di un documento in formato PKCS#7 Signed Data, CAdES, PAdES, XAdES, ASiC con la possibilità di aggiungere marcature temporali della firma e di aggiungere informazioni per la lunga conservazione.
- Cifra di un documento o di documenti multipli in formato CMS Enveloped Data e decifra di un singolo documento cifrato, con la possibilità di scelta dei certificati a cui cifrare da LDAP, dallo store di Windows o da file.
- Marcatura temporale di un documento in formato TSD, TSR, TST, ASiC e verifica delle marcature temporali nei formati suddetti
- Supporto delle CA accreditate nei paesi membri della Comunità Europea per la firma qualificata, con aggiornamento online delle liste stesse dai corrispondenti siti web
- Firma multipla di documenti in formato CAdES, PAdES e XAdES

Tutte le operazioni con i certificati vengono eseguite utilizzando i certificati contenuti nello store di Microsoft Windows. In questo modo è possibile utilizzare certificati installati localmente sulla workstation dell'utente o su qualunque tipo di dispositivo crittografico (token USB o smart card) purché di questo siano installati i corrispondenti middleware (o driver) per il loro utilizzo (ad esempio *Smart Card API* per le CMD-1, CMD-2/Modello ATe e le CMCC).

La distribuzione dell'applicazione si compone dei seguenti file:

NOME FILE	DESCRIZIONE
SmartCardAPI.x86.Setup.exe	Middleware di comunicazione con il Modello ATe per sistemi Windows a 32bit
SmartCardAPI.x64.Setup.exe	Middleware di comunicazione con il Modello ATe per sistemi Windows a 64bit
Manuale Utente Smart Card API.pdf	Manuale utente del middleware di comunicazione con la CMD

L'installazione verrà dettagliata nelle sezioni seguenti. Tutto il software citato in questo manuale è anche disponibile sul sito ufficiale https://pki.difesa.it/tsp

1.1 Requisiti software

Per il corretto funzionamento del software sono richieste le seguenti componenti software:

- Microsoft Windows Vista o Microsoft Windows 7, 8, 8.1, 10
- **Microsoft .net Framework 4.6**, scaricabile dal sito Microsoft o in automatico dal nuovo sistema di installazione
- **Microsoft Windows Installer 4.5**, scaricabile dal sito Microsoft o in automatico dal nuovo sistema di installazione

Per l'anteprima dei documenti è necessario che sul PC sia installato il relativo software di visualizzazione (ad esempio Acrobat Reader per i file pdf, Microsoft Word o Microsoft Word Viewer per i file doc, ecc...).

1.2 Requisiti hardware

Per il corretto funzionamento del software sono richieste le seguenti componenti hardware:

- PC desktop
- Lettore smart card nel caso si vogliano utilizzare certificati su smart card (CMD-1 e CMD-2/ATe)

1.3 Limiti noti

1.3.1 Estensioni file dei documenti

Alcuni formati di documenti, dopo una operazione crittografica (ad esempio firma, cifra, marcatura), cambiano estensione nel proprio nome. Ad esempio, se si firma in formato CAdES un documento Word chiamato **Esempio.doc**, il documento prodotto sarà chiamato **Esempio.doc.p7m**.

Tuttavia, a causa delle impostazioni predefinite di Windows, è possibile che sia attivata l'opzione che nasconde le estensioni per i documenti di tipo noto: in tal caso il documento Esempio.doc.p7m apparirà a video come Esempio.doc nonostante il differente formato. Si consiglia quindi di disattivare questa opzione da **Pannello di Controllo** (*Control Panel*), **Opzioni Cartella** (*Folder Options* o *File Explorer Options*), **Visualizzazione** (*View*), deselezionare **Nascondi le estensioni per i tipi di file conosciuti** (*Hide extensions for known file types*) e confermare con il tasto OK.

In ogni caso, anche se l'opzione è attivata, l'applicazione salverà i documenti con l'estensione corretta.

1.3.2 Limiti della firma PDF

Per quanto riguarda la firma di documenti PDF esistono delle limitazioni note e insormontabili causate dalle politiche implementate da alcune vecchie versioni di applicativi software di Adobe utilizzati per generare documenti PDF firmabili o firmati.

Alcune versioni di applicativi Adobe per la generazione di file PDF consentono di impostare sul documento prodotto una opzione che abilita la possibilità di eseguire firme digitali sul documento PDF utilizzando Adobe Reader e il suo strumento di firma "visuale". Tale caratteristica viene inserita come proprietà del documento PDF all'interno di un campo firmato digitalmente utilizzando un certificato emesso da una Certification Authority di Adobe. Il PDF prodotto può esser detto "firmabile". Adobe Reader abilita quindi la funzione di firma visuale solo se riconosce tale proprietà come firmata da una CA Adobe. Inoltre, qualunque firma digitale venga apposta a un documento PDF firmabile con o senza altre firme apposte con software Adobe, questa azione renderà il documento non più firmabile (e spesso non più valido) in quando Adobe Reader si rifiuta di considerare documenti firmati da altri strumenti.

Ne consegue che:

- A un documento firmabile prodotto da software Adobe, sarà possibile apporre firme solo con strumenti della stessa famiglia di Adobe
- A un documento prodotto da altro software, sarà possibile apporre firme solo con strumenti che non siano della famiglia di Adobe

Nelle ultime versioni di Acrobat Reader è tuttavia possibile eseguire l'operazione di firma "visuale" anche se nel PDF non è indicato tale caratteristica. Tuttavia, se questa caratteristica è stata indicata nel PDF, valgono le considerazioni sopra.

Infine, il formato PAdES consente solo di aggiungere controfirme a un documento già firmato. Non esiste quindi il concetto di firma parallela ma solo quello di *revisioni* successive dello stesso documento di base.

1.3.3 Limiti della firma XML

Se un documento XML è stato firmato utilizzando un software di terze parti, è necessario assicurarsi che tale software abbia predisposto il documento XML in modo che si possano aggiungere ulteriori firme senza compromettere quelle esistenti.

In termini tecnici, essendo il formato XAdES un formato di busta crittografica che aggiunge la firma all'interno del documento firmato, in ogni firma apposta è necessario indicare che la firma è stata eseguita sui tag XML del documento ad esclusione di quello di firma (*ds:Signature*) e i suoi nodi XML discendenti. Il software deve quindi aggiungere al tag *ds:Reference* principale una trasformazione di tipo XPath che escluda *ds:Signature* come da specifica IETF RFC 3275, sezione 6.6.3, pagina 52 (http://www.ietf.org/rfc/rfc3275.txt).

2 Procedure di installazione e disinstallazione

Dalla versione 4, Kit di Firma è fornito con una nuova modalità di installazione chiamata *ClickOnce*, la quale permette di avviare l'installazione direttamente da una pagina web messa a disposizione e che soprattutto consente l'aggiornamento automatico del software senza interventi dell'utente. Inoltre, ClickOnce permette di installare l'applicazione senza necessità di avere diritti di amministratore sul PC.

Il software di contorno, come Smart Card API, invece continua a mantenere i soliti requisiti dei rispettivi fornitori.

2.1 Installazione di Kit di Firma

L'applicazione Kit di Firma è l'applicazione vera e propria che realizza le funzionalità di Firma, Cifra, Verifica dei documenti.

Aprire il browser Internet e collegarsi alla seguente URL:

https://pki.difesa.it/tsp

Apparirà una schermata simile alla seguente:

Scorrere il testo fino alla sezione **Applicazioni Software**:

Clickare sul link **Suite di Firma**, in basso alla finestra apparirà un messaggio simile al seguente:

Premere il tasto **Esegui**, apparirà un messaggio simile al seguente:

Dopo alcuni istanti apparirà la seguente schermata:

Premere il tasto **Installa**, comparirà una schermata simile che indica lo stato del download e l'installazione:

Al termine dell'installazione, l'applicazione partirà in automatico e sul desktop apparirà la seguente icona:

All'interno del menu Start dell'utente apparirà la seguente voce di menu:

2.2 Aggiornamento di Kit di Firma

Dalla versione 4, Kit di Firma è in grado di aggiornarsi automaticamente nel momento in cui una nuova versione viene pubblicata sul sito web.

Il meccanismo di aggiornamento funziona nel seguente modo:

- Kit di Firma esegue il controllo della disponibilità di aggiornamenti nel momento in cui viene chiusa l'applicazione con l'apposito tasto in alto a destra della finestra
- Se è disponibile un aggiornamento, al prossimo avvio dell'applicazione Kit di Firma, verrà eseguito il download e l'installazione della nuova versione in automatico

L'aggiornamento sarà eseguito da una schermata simile alla seguente:

Al termine del download e dell'installazione, l'applicazione partirà in automatico.

2.3 Disinstallazione di Kit di Firma

Per disinstallare l'applicazione installata in modalità standard, aprire il **Pannello di Controllo** (**Control Panel**) di Windows, lanciare l'applicazione **Programmi e funzionalità** (**Programs and Features**), selezionare nella lista la voce **Kit di Firma** e clickare sul tasto **Disinstalla**:

Seguire i passi del wizard fino al completamento dell'operazione:

2.4 Software aggiuntivo

2.4.1 Installazione di Smart Card API

Il software **Smart Card API** è il middleware che gestisce la comunicazione tra le applicazioni utente e la smartcard CMD/ATe. Per l'installazione fare riferimento al manuale **Manuale Utente Smart Card API**.

2.5 Possibili problemi

2.5.1 Avvisi di sicurezza

Se durante l'installazione dell'applicazione dovessero apparire dei messaggi di errore circa l'attendibilità dell'autore del pacchetto, è bene prestare attenzione:

Dopo aver clickato **Esegui**:

E dopo aver clickato **Esegui**:

Si consiglia di installare prima di tutto i certificati delle Certification Authority del Ministero della Difesa sul proprio PC e poi rieseguire l'installazione. Se anche dopo aver installato i certificati dovesse apparire lo stesso messaggio, allora è probabile che il software sia contraffatto. Consultare il supporto tecnico.

Il pacchetto di installazione è firmato da un certificato particolare che può essere consultato durante l'installazione dell'applicazione:

Clickando sul link sotto la voce **Editore** si può visualizzare il certificato di firma.

Su Windows 10 e superiori, nonostante il certificato della CA del Ministero della Difesa sia installato correttamente sul PC, dopo il download dell'applicazione, compare un ulteriore messaggio simile al seguente:

Clickare sul link **More Info** (**Ulteriori informazioni**):

Infine, clickare il pulsante **Run anyway** (**Esegui comunque**).

2.5.2 Aggiornamento fallito

Nel caso in cui per qualche problema l'aggiornamento dell'applicazione non venga completato correttamente e l'applicazione dovesse risultare non più utilizzabile, si consiglia di procedere alla disinstallazione dell'applicazione (sezione 2.3) e alla sua reinstallazione ex-novo (sezione 2.1).

3 L'applicazione Kit di Firma

Per lanciare l'applicazione Kit di Firma si può o utilizzare l'icona sul desktop:

Oppure si può utilizzare la voce **Kit di Firma** presente nel menu Start di Windows, sotto il menu **Ministero della Difesa**, **PKI Trust Center**.

Una volta lanciata l'applicazione, apparirà una schermata simile alla seguente:

Nella seguente schermata viene rappresentata la suddivisione dell'interfaccia grafica:

Nella sezione **Toolbar delle funzioni principali** si trovano i pulsanti clickabili corrispondenti alle funzionalità principali dell'applicazione. In **Informazioni sull'applicazione e il documento caricato** viene visualizzato il nome completo del file aperto nell'applicativo e la versione attuale dell'applicazione. **Area principale dell'applicazione** contiene la finestra corrispondente alla funzionalità scelta dalla toolbar (principale o secondaria). **Barra di stato** mostrerà lo stato della lista delle CA accreditate e degli eventuali aggiornamenti disponibili. **Toolbar delle funzioni minori** si trovano I pulsanti clickabili corrispondenti alle funzionalità di supporto dell'applicazione.

Durante le operazioni che richiedono più passi di elaborazione, verrà mostrata una finestra di stato al cui interno viene riportata l'informazione riguardo il passo corrente:

Quando la finestra viene mostrata, l'applicativo sta eseguendo un'operazione che richiede un tempo d'attesa: durante questo tempo è necessario attendere il completamento dell'operazione eseguita.

Per eseguire le varie operazioni, consultare le sezioni seguenti del documento. Punto di base per partire è la schermata home dell'applicazione (indicata con l'icona 🏠 nella toolbar). Da questa schermata è possibile aprire uno o più file o tramite il tasto **apri file** oppure tramite trascinamento sull'area della pagina. A seconda della tipologia di documento aperto, verrà eseguito un percorso differente:

- Se si apre un solo documento non firmato, l'applicativo si posiziona automaticamente nella funzione di firma
- Se si apre un solo documento firmato, l'applicativo si posiziona automaticamente nella funzione di verifica ed esegue la verifica delle firme
- Se si apre una sola marca temporale, l'applicativo si posiziona automaticamente nella funzione di verifica ed esegue la verifica della marca
- Se si aprono più documenti firmati o no, l'applicativo si posiziona automaticamente nella funzione di firma multipla

Se si preferisce, è possibile eseguire l'apertura di un documento direttamente dalla sezione desiderata. Se invece si vuole eseguire un'altra operazione sul documento aperto, è necessario soltanto clickare la funzione desiderata dalla toolbar con il documento ancora caricato in memoria. Ad esempio, se si desidera cifrare un documento: si apre il documento dalla schermata home, l'applicazione si posiziona sulla funzione di firma, l'utente clicka sul tasto cifra.

A causa dei nuovi meccanismi di sicurezza di Microsoft Windows Vista e 7, per poter trascinare un documento dal desktop o da Windows Explorer a un'altra applicazione, come Kit di Firma, è necessario che queste vengano eseguite con lo stesso utente. Si consiglia quindi di NON avviare mai l'applicazione Kit di Firma come amministratore (*Esegui come amministratore* o *Run as administrator*), altrimenti non sarà possibile eseguire il trascinamento, in quanto il desktop e Windows Explorer solitamente vengono eseguiti come utente normale e non come amministratore.

3.1 Primo avvio dell'applicazione

Al primo avvio, l'applicazione Kit di Firma cercherà di scaricare automaticamente la lista firmata dei paesi membri dell'unione europea e la lista delle CA Accreditate dell'Italia. Per eseguire il download sarà quindi necessaria la connessione a Internet e attendere circa un minuto per il download e la verifica delle due liste. Lo stato dell'operazione viene visualizzato all'interno di una finestra di stato.

Nel caso non si avesse connessione a Internet, sarà comunque possibile eseguire il download in modo manuale dall'applicazione stessa (si veda la sezione 3.9.1 per i dettagli). Si consiglia comunque di non procedere con le operazioni di firma e verifica in assenza di una lista valida delle CA Accreditate per non compromettere i risultati della firma o ottenere falsi negativi durante la verifica.

A ogni successivo avvio dell'applicazione, se la lista dei paesi membri della comunità europea e/o la lista delle CA Accreditate dell'Italia sarà scaduta o aggiornata, l'applicazione eseguirà automaticamente l'aggiornamento della lista scaduta o aggiornata.

3.2 Messaggistica di errore

Durante il normale utilizzo dell'applicativo, nel caso di problemi dovuti all'errato comportamento dell'utente, i messaggi di errore sono simile al seguente:

Invece, nel caso si dovesse verificare un errore di sistema non dovuto a un errato comportamento dell'utente, l'errore mostrato sarà simile al seguente:

Clicando su **Dettagli errore**, si aprirà una ulteriore area di dettaglio che riporta informazioni utili al supporto tecnico per aiutare nella soluzione del problema:

Nel caso infatti si volesse segnalare un problema, si consiglia di allegare oltre alla schermata dell'errore, anche le informazioni contenute nel riquadro. Per semplicità, clickando sul link "**Copia messaggio seguente negli appunti**", il messaggio completo verrà copiato egli appunti del PC, pronto per essere incollato ad esempio nel testo di una e-mail.

3.3 Operazioni di Firma

L'applicazione Kit di Firma è in grado di eseguire operazioni di firma digitale su qualsiasi tipo di documento o file di cui si dispone.

L'applicazione è in grado di eseguire tre tipi di firma:

- ***Firma***: si appone la prima firma al documento
- ***Firma parallela***: si appone una firma ulteriore al documento già firmato allo stesso livello della prima firma
- ***Controfirma***: si appone una firma ad una firma già apposta al documento

È possibile quindi creare una struttura di firma gerarchica, come mostrato nella figura seguente:

L'applicazione gestisce in fase di firma differenti formati di busta crittografica:

- ***CAdES – Cryptographic Message Syntax Advanced Electronic Signature***: può essere prodotto a partire da un documento in qualsiasi formato. Il risultato della prima firma sarà un nuovo documento al cui interno viene immagazzinato il documento firmato e tutte le informazioni sulla firma in formato ASN.1 binario. La busta crittografica assume una nuova estensione **.p7m** e nel caso di firme successive, queste vengono aggiunte alla struttura di base

- ***PAdES – PDF Advanced Electronic Signature***: può essere prodotto solo a partire da un PDF al quale vengono aggiunte tutte le informazioni sulla firma all'interno del PDF stesso. La busta crittografica continua ad essere un PDF visualizzabile con il proprio applicativo preferito e mantiene l'estensione **.pdf**

- ***XAdES – XML Advanced Electronic Signature***: può essere prodotto solo a partire da un file XML al quale vengono aggiunte tutte le informazioni sulla firma all'interno dell'XML stesso nel formato XML. La busta crittografica continua ad essere un XML utilizzabile con il proprio applicativo preferito e mantiene l'estensione **.xml**

- ***ASiC-E CAdES – Extended Associated Signature Container with CAdES***: può essere prodotto a partire da uno o più file di qualunque tipo, i quali vengono inseriti all'interno di un archivio Zip insieme a un indice firmato in formato CAdES Detached[1]. La busta crittografica è quindi un unico archivio Zip standard utilizzabile anche con il proprio applicativo preferito e assume una nuova estensione **.asice** . Alla stessa busta potranno poi essere aggiunte in futuro firme parallele/controfirme per lo stesso gruppo di file, oppure aggiungere nuovi file e firmare il nuovo indice. La struttura sarà quindi differente da quella descritta graficamente in precedenza:

[1] Il formato standardizzato ASiC prevede 4 possibili combinazioni per i contenitori di firme: ASiC-S CAdES, ASiC-S XAdES, ASiC-E CAdES e ASiC-E XAdES. La differenza tra ASiC-E ed ASiC-S consiste nel numero di documenti che è possibile includere nel contenitore: uno solo per ASiC-S, illimitati per ASiC-E. La differenza tra ASiC CAdES e ASiC XAdES è il differente formato della busta crittografica che protegge l'indice dei documenti: CAdES Detached e XAdES Detached. Secondo il Regolamento EU N. 910/2014 (anche detto eIDAS) è richiesto il supporto di uno solo tra i 4 formati. L'applicazione Kit di Firma supporta ASiC-E CAdES per la firma, mentre per la verifica supporta tutti i 4 formati.

In tutti e 4 i casi è possibile apporre firme secondo 4 profili di base specificati in ambito europeo. Ogni documento potrà contenere firme eseguite con profili di base differenti:

- ***B-Level*** – *Basic Level*: indicato nell'applicazione con l'abbreviazione **B**, indica una firma con allegato un insieme base di attributi

- ***T-Level*** – *Trusted Time for signature existence*: indicato nell'applicazione con l'abbreviazione **T**, indica una firma conforme al livello B e contenente una marca temporale della firma attestante l'apposizione della firma in una data e ora certificate

- ***LT-Level*** – *Long Term*: indicato nell'applicazione con l'abbreviazione **LT**, indica una firma conforme al livello LT e con allegate tutte le informazioni che permettono la verifica della firma in momenti remoti rispetto al momento dell'apposizione della firma, ovvero i certificati di CA/TSA e le informazioni di revoca (OCSP/CRL)

- ***LTA-Level*** – *Long Term with Archive time-stamps*: indicato nell'applicazione con l'abbreviazione **LTA**, indica una firma conforme al livello LT e con una particolare marcatura temporale detta "di archiviazione" che ne attesta la validità nel tempo

Nel caso particolare di un documento firmato PAdES-LTA, per ogni firma digitale, verrà aggiunto contestualmente un ulteriore oggetto simile a un "firmatario" e corrispondente alla marca temporale di archiviazione (Archive Time Stamp, ATS) e la struttura sarà del seguente tipo:

Se il documento da firmare o già firmato è in un particolare formato, sarà possibile produrre documenti firmati in varie combinazioni di formati:

Se documento è…	Prima Firma produce…	Firma Parallela produce…	Controfirma produce…
PDF	PAdES CAdES ASiC-E	-	-
PAdES	-	Non prevista	PAdES
XML	CAdES XAdES ASiC-E	-	-

Se documento è…	Prima Firma produce…	Firma Parallela produce…	Controfirma produce…
XAdES	-	XAdES	XAdES
Generico	CAdES ASiC-E	-	-
CAdES	-	CAdES	CAdES
ASiC-E	-	ASiC-E	ASiC-E

Riguardo il nome del documento dopo la firma varranno le seguenti considerazioni a seconda della busta di firma scelta:

- Prima firma CAdES: il nome del documento firmato sarà identico a quello originale con aggiunta l'estensione .p7m (ad esempio Fattura.docx diventerà Fattura.docx.p7m)
- Prima firma PAdES: il nome del documento firmato sarà come quello originale ma con il suffisso "**_Firmato**" e la stessa estensione .pdf (ad esempio Fattura.pdf diventerà Fattura_Firmato.pdf). In questo modo non si rischierà di sovrascrivere il documento originale[2].
- Prima firma XAdES: il nome del documento firmato sarà come quello originale ma con il suffisso "**_Firmato**" e la stessa estensione .xml (ad esempio Fattura.xml diventerà Fattura_Firmato.xml). In questo modo non si rischierà di sovrascrivere il documento originale[3].
- Prima firma ASiC: il nome del contenitore firmato sarà sempre ContenitoreFirme_*[DATA]*.asice (ad esempio ContenitoreFirme_2017_05_17_12_57_30.asice)
- Nel caso invece di aggiunta di una firma parallela o controfirma, in tutti i formati di firma il nuovo documento prodotto sovrascriverà il precedente perché verrà mantenuto lo stesso nome, si consiglia quindi di conservare una copia del file precedente o di specificare un nuovo nome file se si vuole conservare la versione precedente.

Per tutte le operazioni di firma verrà sempre utilizzato l'algoritmo di firma **RSA** e l'algoritmo di hashing **SHA-256**.

In tutte le operazioni di firma, l'applicazione Kit di Firma farà in modo di agevolare l'utente nell'operazione senza che quest'ultimo debba eseguire troppe operazioni che si discostino dalla base. L'applicazione quindi:

- Si ricorderà sempre l'ultimo certificato utilizzato dall'utente durante l'ultima firma
- Userà il profilo di firma T-Level in modo da aggiungere sempre una marca temporale sulla firma
- Userà il formato PAdES nel caso il documento da firmare sia in formato PDF, XAdES nel caso il documento da firmare sia in formato XML, CAdES in tutti gli altri casi
- Userà sempre il servizio Time Stamp predefinito
- Nel caso di firma PAdES, compilerà automaticamente le impostazioni della firma PDF a partire da quelle specificate nella configurazione (si veda 3.10.4 per i dettagli)

Per eseguire un'operazione di firma, è necessario prima di tutto caricare il documento in memoria. Premere il seguente tasto dalla toolbar:

Apparirà la seguente schermata:

[2] Se non si gradisce questa modalità, è possibile disattivarla nei settaggi dell'applicazione
[3] Se non si gradisce questa modalità, è possibile disattivarla nei settaggi dell'applicazione

Da questa schermata premere il tasto apri nuovo file per caricare in memoria il documento da firmare utilizzando il pulsante **apri nuovo file** sulla sinistra:

Selezionare il documento da aprire e premere il tasto **Apri**. Da questo punto in poi, a seconda della tipologia di firma, consultare la sezione corrispondente (3.3.1, 3.3.2, 3.3.3). Nella sezione 3.3.4 vengono riportati alcuni dettagli su particolari operazioni.

È possibile iniziare l'operazione di firma anche dalla schermata home dell'applicazione utilizzando il pulsante **apri file**:

- Caricando un documento non firmato, Kit di Firma passerà automaticamente alla sezione firma
- Caricando un documento già firmato, Kit di Firma passerà automaticamente alla sezione verifica e verificherà il documento. Al termine della verifica passare alla sezione di firma tramite il tasto firma della toolbar.

3.3.1 Formato CAdES

3.3.1.1 Firma CAdES di un documento

Una volta caricato in memoria un documento generico, apparirà una schermata simile alla seguente:

Se non si è mai eseguito una firma precedentemente, oppure il certificato usato precedentemente è su una smart card che non è attualmente inserita nel lettore, apparirà una schermata simile alla seguente:

Se si vuole visualizzare il documento caricato fare click sul link **Visualizza File** in alto nella colonna a sinistra (consultare la sezione 3.8 per maggiori informazioni), altrimenti proseguire scegliendo il certificato da usare clickando sulla tendina nella sezione **Scelta del Certificato**:

Una volta scelto il certificato per la prima volta, o se si è già pronti, scegliere il profilo di firma (B-Level, T-Level, LT-Level LTA-Level), e spuntare la casella in basso:

Il pulsante **firma digitalmente** si attiverà e premendolo si eseguirà la firma digitale. Se la chiave privata corrispondente al certificato è immagazzinata su una smart card, l'applicazione richiederà l'inserimento anche del PIN Carta e del PIN Firma.

Al termine dell'operazione di firma, apparirà un messaggio simile al seguente:

Premendo il tasto **SI** il documento firmato sarà salvato nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di firma è terminata.

3.3.1.2 Firma parallela CAdES di un documento

Una volta caricato in memoria un documento già firmato in formato CAdES, apparirà una schermata simile alla seguente:

Se non si è mai eseguito una firma precedentemente, oppure il certificato usato precedentemente è su una smart card che non è attualmente inserita nel lettore, sarà necessario scegliere il certificato dalla tendina nella sezione **Scelta del Certificato**.

Una volta scelto il certificato per la prima volta, o se si è già pronti, scegliere il profilo di firma (B-Level, T-Level, LT-Level, LTA-Level), e spuntare la casella in basso:

Il pulsante **firma parallela** si attiverà e premendolo si eseguirà la firma parallela. Se la chiave privata corrispondente al certificato è immagazzinata su una smart card, l'applicazione richiederà l'inserimento anche del PIN Carta e del PIN Firma.

Al termine dell'operazione di firma, apparirà un messaggio simile al seguente:

Premendo il tasto **SI** il documento firmato sarà salvato nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di firma è terminata.

3.3.1.3 Controfirma CAdES di un documento

Una volta caricato in memoria un documento già firmato in formato CAdES, apparirà una schermata simile alla seguente:

Se non si è mai eseguito una firma precedentemente, oppure il certificato usato precedentemente è su una smart card che non è attualmente inserita nel lettore, sarà necessario scegliere il certificato dalla tendina nella sezione **Scelta del Certificato**.

Una volta scelto il certificato per la prima volta, o se si è già pronti, scegliere il profilo di firma (B-Level, T-Level, LT-Level, LTA-Level), selezionare la firma a cui apporre la controfirma nella sezione **Alberatura Firme Documento** e spuntare la casella in basso:

Il pulsante **controfirma** si attiverà e premendolo si eseguirà la controfirma della firma selezionata. Se la chiave privata corrispondente al certificato è immagazzinata su una smart card, l'applicazione richiederà l'inserimento anche del PIN Carta e del PIN Firma.

Nell'esempio mostrato l'alberatura è molto semplice, in alcuni casi potrebbe essere più complessa, come mostrato nella seguente immagine. Per agevolare la visualizzazione della gerarchia, viene indicata anche una numerazione gerarchica:

Al termine dell'operazione di firma, apparirà un messaggio simile al seguente:

Premendo il tasto **SI** il documento firmato sarà salvato nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di firma è terminata.

3.3.2 Formato PAdES

Per tutte le operazioni di firma nel formato PDF si consiglia di firmare documenti PDF nel solo formato **PDF/A-1b**: tale formato è un particolare tipo di formato PDF studiato appositamente per la firma digitale a norma e la firma digitale a lunga conservazione in quanto vincola la produzione dei documenti PDF a particolari restrizioni che evitano la contraffazione del PDF dopo la firma (misure contro la sostituzione dei font, eliminazione degli script, ecc...). Consultare la sezione 4.1 per alcuni consigli su come produrre documenti in formato PDF/A.

Sull'apertura del documento PDF, viene eseguito un controllo sul formato del documento e a seconda se il documento PDF dichiara di essere conforme o meno allo standard PDF/A, viene visualizzato un messaggio:

Sulla verifica dei documenti firmati PAdES, se il documento PDF originale dichiara di essere conforme allo standard PDF/A, viene visualizzato un messaggio informativo:

3.3.2.1 Firma PAdES di un documento

Una volta caricato in memoria un documento PDF non firmato, apparirà una schermata simile alla seguente:

Eventualmente è possibile visualizzare l'anteprima del documento caricato facendo click su **Visualizza file** (consultare 3.8 per maggiori dettagli).

Se non si è mai eseguito una firma precedentemente, oppure il certificato usato precedentemente è su una smart card che non è attualmente inserita nel lettore, sarà necessario scegliere il certificato dalla tendina nella sezione **Scelta del Certificato**.

Una volta scelto il certificato per la prima volta, o se si è già pronti, scegliere il profilo di firma (B-Level, T-Level, LT-Level, LTA-Level), impostare i **Settaggi PDF** se desiderato (consultare 3.3.5.2 per maggiori dettagli) e spuntare la casella in basso:

Il pulsante **firma digitalmente** si attiverà e premendolo si eseguirà la firma digitale. Se la chiave privata corrispondente al certificato è immagazzinata su una smart card, l'applicazione richiederà l'inserimento anche del PIN Carta e del PIN Firma.

Al termine dell'operazione di firma, apparirà un messaggio simile al seguente:

Premendo il tasto **SI** il documento firmato sarà salvato nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di firma è terminata.

3.3.2.2 Controfirma PAdES di un documento

Per poter apporre una controfirma a un documento PDF già firmato è necessario che siano verificate le condizioni espresse nella sezione 1.3.1 riguardo il software utilizzato per apporre le firme precedenti.

Una volta caricato in memoria un documento già firmato in formato PAdES, apparirà una schermata simile alla seguente:

Se non si è mai eseguito una firma precedentemente, oppure il certificato usato precedentemente è su una smart card che non è attualmente inserita nel lettore, sarà necessario scegliere il certificato dalla tendina nella sezione **Scelta del Certificato**.

Una volta scelto il certificato per la prima volta, o se si è già pronti, scegliere il profilo di firma (B-Level, T-Level, LT-Level, LTA-Level), impostare i **Settaggi PDF** se desiderato (consultare 3.3.5.2 per maggiori dettagli) e spuntare la casella in basso:

Il pulsante **controfirma** si attiverà e premendolo si eseguirà la controfirma della firma selezionata. Se la chiave privata corrispondente al certificato è immagazzinata su una smart card, l'applicazione richiederà l'inserimento anche del PIN Carta e del PIN Firma.

Al termine dell'operazione di firma, apparirà un messaggio simile al seguente:

Premendo il tasto **SI** il documento firmato sarà salvato nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di firma è terminata.

3.3.3 Formato XAdES

3.3.3.1 Firma XAdES di un documento

Una volta caricato in memoria un documento XML non firmato, apparirà una schermata simile alla seguente:

Eventualmente è possibile visualizzare l'anteprima del documento caricato facendo click su **Visualizza file** (consultare 3.8 per maggiori dettagli).

Se non si è mai eseguito una firma precedentemente, oppure il certificato usato precedentemente è su una smart card che non è attualmente inserita nel lettore, sarà necessario scegliere il certificato dalla tendina nella sezione **Scelta del Certificato**.

Una volta scelto il certificato per la prima volta, o se si è già pronti, scegliere il profilo di firma (B-Level, T-Level, LT-Level, LTA-Level) e spuntare la casella in basso:

Il pulsante **firma digitalmente** si attiverà e premendolo si eseguirà la firma digitale. Se la chiave privata corrispondente al certificato è immagazzinata su una smart card, l'applicazione richiederà l'inserimento anche del PIN Carta e del PIN Firma.

Al termine dell'operazione di firma, apparirà un messaggio simile al seguente:

Premendo il tasto **SI** il documento firmato sarà salvato nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di firma è terminata.

3.3.3.2 Firma Parallela XAdES di un documento

Per poter aggiungere una firma a un documento XML già firmato è necessario fare una premessa:

- Se il documento XML è stato firmato con il software Kit di Firma, è possibile apporre la firma parallela senza problemi

- Se il documento XML è stato firmato utilizzando un software di terze parti, è necessario assicurarsi che tale software abbia predisposto il documento XML in modo che si possano aggiungere ulteriori firme senza compromettere quelle esistenti. In termini tecnici, essendo il formato XAdES un formato di busta crittografica che aggiunge la firma all'interno del documento firmato, in ogni firma apposta è necessario indicare che la firma è stata eseguita sui tag XML del documento ad esclusione di quello di firma (*ds:Signature*) e i suoi nodi XML discendenti. Il software deve quindi aggiungere al tag *ds:Reference* principale una trasformazione di tipo XPath che escluda *ds:Signature* come da specifica IETF RFC 3275, sezione 6.6.3, pagina 52 (http://www.ietf.org/rfc/rfc3275.txt).

Una volta caricato in memoria un documento già firmato in formato XAdES, apparirà una schermata simile alla seguente:

Se non si è mai eseguito una firma precedentemente, oppure il certificato usato precedentemente è su una smart card che non è attualmente inserita nel lettore, sarà necessario scegliere il certificato dalla tendina nella sezione **Scelta del Certificato**.

Una volta scelto il certificato per la prima volta, o se si è già pronti, scegliere il profilo di firma (B-Level, T-Level, LT-Level, LTA-Level), e spuntare la casella in basso:

Il pulsante **firma parallela** si attiverà e premendolo si eseguirà la firma parallela. Se la chiave privata corrispondente al certificato è immagazzinata su una smart card, l'applicazione richiederà l'inserimento anche del PIN Carta e del PIN Firma.

Al termine dell'operazione di firma, apparirà un messaggio simile al seguente:

Premendo il tasto **SI** il documento firmato sarà salvato nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di firma è terminata.

3.3.3.3 Controfirma XAdES di un documento

Per poter apporre una controfirma a un documento XML già firmato è necessario fare una premessa:

- Se il documento XML è stato firmato con il software Kit di Firma, è possibile apporre la controfirma senza problemi
- Se il documento XML è stato firmato utilizzando un software di terze parti, è necessario assicurarsi che tale software abbia predisposto il documento XML in modo che si possano controfirmare firme preesistenti e senza compromettere quelle esistenti. In termini tecnici, la controfirma è la firma apposta al nodo XML contenente la firma controfirmata (*ds:SignatureValue*). Per poter specificare che la controfirma si riferisce a una firma particolare, è necessario che questa riporti un attributo *Id* nel tag XML *ds:SignatureValue*.

Una volta caricato in memoria un documento già firmato in formato XAdES, apparirà una schermata simile alla seguente:

Se non si è mai eseguito una firma precedentemente, oppure il certificato usato precedentemente è su una smart card che non è attualmente inserita nel lettore, sarà necessario scegliere il certificato dalla tendina nella sezione **Scelta del Certificato**.

Una volta scelto il certificato per la prima volta, o se si è già pronti, scegliere il profilo di firma (B-Level, T-Level, LT-Level, LTA-Level), selezionare la firma a cui apporre la controfirma nella sezione **Alberatura Firme Documento** e spuntare la casella in basso:

Il pulsante **controfirma** si attiverà e premendolo si eseguirà la controfirma della firma selezionata. Se la chiave privata corrispondente al certificato è immagazzinata su una smart card, l'applicazione richiederà l'inserimento anche del PIN Carta e del PIN Firma.

Nell'esempio mostrato l'alberatura è molto semplice, in alcuni casi potrebbe essere più complessa, come mostrato nella seguente immagine. Per agevolare la visualizzazione della gerarchia, viene indicata anche una numerazione gerarchica:

Al termine dell'operazione di firma, apparirà un messaggio simile al seguente:

Premendo il tasto **SI** il documento firmato sarà salvato nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di firma è terminata.

3.3.4 Formato ASiC-E

Il formato ASiC-E, essendo un "contenitore" di più documenti, presenta delle differenze rispetto ai precedenti formati, in quanto oltre a firmare un gruppo di documenti, permette anche di aggiungere ulteriori documenti a un archivio preesistente e su questo nuovo gruppo, creare una nuova struttura di firme gerarchiche.

3.3.4.1 Firma ASiC-E di un gruppo di documenti

Per eseguire una firma in formato ASiC-E è possibile procedere in più modi:

- Se si vuole includere un solo documento nel contenitore, si apre il documento (da pulsante o con trascinamento) e poi si sceglie il formato tramite il tasto **ASiC** nella sezione **Tipo**.

- Se a questo punto si vogliono aggiungere ulteriori documenti, premendo il tasto **aggiungi file** verranno caricati i nuovi documenti senza passare alla firma multipla. Se invece si vuole includere solo un documento si procede direttamente con la firma:

- Se si vuole includere direttamente più documenti nel contenitore, si caricano i documenti (da pulsante o con trascinamento) come se si volesse eseguire una firma multipla e poi si usa il tasto **passa a firma** in basso nella schermata di riepilogo della firma multipla:

Nel momento in cui vengono caricati più documenti per la firma ASiC-E, la schermata di firma mostra il numero di documenti caricati e si presenta nel seguente modo:

Se non si è mai eseguito una firma precedentemente, oppure il certificato usato precedentemente è su una smart card che non è attualmente inserita nel lettore, sarà necessario scegliere il certificato dalla tendina nella sezione **Scelta del Certificato**.

Una volta scelto il certificato per la prima volta, o se si è già pronti, scegliere il profilo di firma (B-Level, T-Level, LT-Level, LTA-Level) e spuntare la casella in basso:

Il pulsante **firma digitalmente** si attiverà e premendolo si eseguirà la firma digitale. Se la chiave privata corrispondente al certificato è immagazzinata su una smart card, l'applicazione richiederà l'inserimento anche del PIN Carta e del PIN Firma.

Al termine dell'operazione di firma, apparirà un messaggio simile al seguente:

Premendo il tasto **SI** il contenitore firmato sarà salvato nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di firma è terminata.

3.3.4.2 Firma Parallela ASiC-E di un gruppo di documenti

Una volta caricato in memoria un contenitore già firmato in formato ASiC-E, apparirà una schermata simile alla seguente:

Come si nota nell'immagine precedente, l'alberatura delle firme è differente rispetto a quanto visto in precedenza negli altri formati CAdES, PAdES e XAdES, in quanto sono presenti anche gli insiemi di documenti (*Gruppo 1* e *Gruppo 2* nell'esempio) e la loro corrispondente alberatura di firme. Per eseguire quindi la firma parallela, è necessario selezionare a quale **Gruppo** di documenti aggiungere la firma[4].

Se non si è mai eseguito una firma precedentemente, oppure il certificato usato precedentemente è su una smart card che non è attualmente inserita nel lettore, sarà necessario scegliere il certificato dalla tendina nella sezione **Scelta del Certificato**.

[4] Per visualizzare quali documenti sono protetti all'interno del gruppo, è possibile consultare l'elenco all'interno della sezione di verifica dell'applicazione.

Una volta scelto il certificato per la prima volta, o se si è già pronti, scegliere il profilo di firma (B-Level, T-Level, LT-Level, LTA-Level), scegliere il gruppo dall'alberatura e spuntare la casella in basso:

Il pulsante **firma parallela** si attiverà e premendolo si eseguirà la firma parallela (nell'esempio mostrato, verrà apposta la Firma 1.3). Se la chiave privata corrispondente al certificato è immagazzinata su una smart card, l'applicazione richiederà l'inserimento anche del PIN Carta e del PIN Firma.

Al termine dell'operazione di firma, apparirà un messaggio simile al seguente:

Premendo il tasto **SI** il contenitore firmato sarà salvato nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di firma è terminata.

3.3.4.3 Controfirma ASiC-E di un gruppo di documenti

Una volta caricato in memoria un contenitore già firmato in formato ASiC-E, apparirà una schermata simile alla seguente:

Come si nota nell'immagine precedente, l'alberatura delle firme è differente rispetto a quanto visto in precedenza negli altri formati CAdES, PAdES e XAdES, in quanto sono presenti anche gli insiemi di documenti (*Gruppo 1* e *Gruppo 2* nell'esempio) e la sua corrispondente alberatura di firme. Per eseguire quindi la controfirma, è necessario selezionare su quale **Firma** eseguire la controfirma, facendo attenzione al gruppo[5].

Se non si è mai eseguito una firma precedentemente, oppure il certificato usato precedentemente è su una smart card che non è attualmente inserita nel lettore, sarà necessario scegliere il certificato dalla tendina nella sezione **Scelta del Certificato**.

Una volta scelto il certificato per la prima volta, o se si è già pronti, scegliere il profilo di firma (B-Level, T-Level, LT-Level, LTA-Level), scegliere la firma dall'alberatura e spuntare la casella in basso:

[5] Per visualizzare quali documenti sono protetti all'interno del gruppo, è possibile consultare l'elenco all'interno della sezione di verifica dell'applicazione.

Il pulsante **controfirma** si attiverà e premendolo si eseguirà la controfirma della firma selezionata (nell'esempio mostrato, verrà apposta la Firma 1.3.1). Se la chiave privata corrispondente al certificato è immagazzinata su una smart card, l'applicazione richiederà l'inserimento anche del PIN Carta e del PIN Firma.

Al termine dell'operazione di firma, apparirà un messaggio simile al seguente:

Premendo il tasto **SI** il contenitore firmato sarà salvato nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di firma è terminata.

3.3.4.4 Firma di un nuovo gruppo di documenti

Una volta caricato in memoria un contenitore già firmato in formato ASiC-E, apparirà una schermata simile alla seguente:

Come si nota nell'immagine precedente, l'alberatura delle firme è differente rispetto a quanto visto in precedenza negli altri formati CAdES, PAdES e XAdES, in quanto sono presenti anche gli insiemi di documenti (*Gruppo 1* e *Gruppo 2* nell'esempio) e la sua corrispondente alberatura di firme. Per creare quindi un nuovo gruppo di documenti da firmare, è necessario selezionare il **Contenitore di base**.

Se non si è mai eseguito una firma precedentemente, oppure il certificato usato precedentemente è su una smart card che non è attualmente inserita nel lettore, sarà necessario scegliere il certificato dalla tendina nella sezione **Scelta del Certificato**.

Una volta scelto il certificato per la prima volta, o se si è già pronti, scegliere il profilo di firma (B-Level, T-Level, LT-Level, LTA-Level), scegliere il **Contenitore di base** dall'alberatura e spuntare la casella in basso:

Il pulsante **firma parallela** si attiverà e premendolo si aprirà una nuova finestra nella quale è possibile scegliere quali documenti includere all'interno del nuovo gruppo:

- Nella parte in alto vengono mostrati i documenti già presenti nel contenitore:

- I documenti con il segno di spunta ☑ vengono inclusi nel nuovo gruppo. I documenti selezionati in questo modo vengono condivisi quindi tra più gruppi e firmati dalla nuova alberatura di firme sottostanti.
- I documenti con il segno di spunta ☐ non vengono inclusi nel nuovo gruppo. I documenti non selezionati rimangono nel contenitore ma vengono firmati nei gruppi preesistenti o futuri.

► Nella parte in basso vengono mostrati i nuovi documenti da aggiungere al contenitore:
- Con il pulsante ⊕ è possibile selezionare un documento dal disco della propria workstation
- Con il pulsante ⊖ è possibile eliminare dalla lista un documento aggiunto per sbaglio.

Quando si è pronti, premere il tasto **conferma** per proseguire (nell'esempio mostrato, verrà creato il Gruppo 2 e apposta la Firma 2.1). Se la chiave privata corrispondente al certificato è immagazzinata su una smart card, l'applicazione richiederà l'inserimento anche del PIN Carta e del PIN Firma.

Al termine dell'operazione di firma, apparirà un messaggio simile al seguente:

Premendo il tasto **SI** il contenitore firmato sarà salvato nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di firma è terminata.

3.3.5 Dettagli sulle operazioni di Firma

3.3.5.1 Anteprima del documento

Una volta caricato in memoria il documento su cui effettuare le operazioni di firma, è possibile visualizzare il contenuto del documento all'interno dell'applicativo stesso in modo da visualizzare ciò che poi si andrà a firmare. Dopo aver caricato il documento:

Clickare il link **Visualizza File** in alto nella colonna a sinistra per passare alla visualizzazione del documento caricato (consultare la sezione 3.8 per maggiori informazioni).

3.3.5.2 Caratteristiche della firma PDF

Kit di Firma permette di specificare diverse caratteristiche che la firma PDF avrà all'interno del documento PDF firmato prodotto.

Nel momento dell'apposizione della firma, è possibile scegliere queste caratteristiche nella sezione **Settaggi PDF** della finestra seguente:

Le varie opzioni sono:

- **Blocca documento dopo la firma**: indica in che modo produrre il PDF firmato. Selezionando la casella si sceglie di produrre un PDF firmato a cui non potranno essere aggiunte altre firme (*certificazione*), non selezionando la casella si sceglie di produrre un PDF firmato al quale potrenno essere aggiunte altre firme mediante il concetto di *revisioni*. La modalità di blocco non sarà selezionabile nel caso si voglia apporre una controfirma. Inoltre, per poter apporre controfirme, non è possibile selezionare la casella quando si esegue la prima firma, in quanto tutte le altre successive invalideranno tutte le firme. Per questo motivo non è possibile bloccare il documento nel caso di firme con profilo LT ed LTA, in quanto le informazioni aggiunte alla firma, avvengono dopo la firma stessa e quindi ne invaliderebbero subito la firma.

  Il concetto di **revisione** di un PDF indica la possibilità di modificare in modo incrementale il documento di base aggiungendo o modificando elementi del PDF dopo la prima versione. A ogni salvataggio, l'applicativo aggiungerà queste informazioni come se fossero una nuova versione (una revisione). Nel caso della presenza delle firme digitali, ogni firma digitale apposta a un PDF attesta tutte le varianti fino a quel momento e, nel caso degli applicativi di firma e verifica, ogni firma corrisponderà quindi a una revisione. Se non si desidera questo comporamento, è necessario quindi usare il blocco del documento durante la prima firma.

  Un documento PAdES con la prima firma di tipo certificazione apparirà nel seguente modo (si noti anche che questo tipo di firma blocca i campi form eventuali del PDF):

  Un documento PAdES con firme di tipo revisione apparirà nel seguente modo:

È da notare che dopo una firma è possibile apportare modifiche al documento PDF con appositi strumenti di modifica PDF. Per evitare situazioni in cui un utente malevolo faccia apparire a video un PDF diversamente dalla versione firmata dall'utente precedente, durante la verifica sono stati aggiunte delle funzioni di ispezione del documento (consultare la sezione 3.6.2.4 per maggiori informazioni).

- **Ruolo/Qualifica**: è un campo di testo (opzionale) che appare solo nel riquadro di firma grafico e che può essere usato per indicare delle informazioni ulteriori sul firmatario. Il testo viene visualizzato subito sotto il nome del firmatario in colore grigio.
- **Luogo**: indica il luogo in cui si esegue la firma PAdES (opzionale). Il testo non viene visualizzato nel riquadro ma viene incluso nella parte "digitale" della firma.
- **Motivazione**: indica la motivazione della firma PAdES (opzionale). Il testo viene sia visualizzato nel riquadro di firma nella parte sottostante (con un a capo automatico), sia incluso nella parte "digitale" della firma
- **Posizione riquadro firma**: indica se posizionare il riquadro firma sulla *Prima pagina* o sull'*Ultima pagina*.
- **Posizione all'interno della pagina**: indica in quale zona della pagina inserire il campo form, ovvero in alto a sinistra, in alto a destra, in basso a sinistra, in basso a destra.
- **Mostra riquadro firma nel documento:** indica se visualizzare graficamente o no il riquadro della firma sulla pagina del documento PDF quando questi viene aperto con un visualizzatore PDF.
- **Mostra l'immagine nel riquadro firma:** indica se visualizzare una immagine all'interno del riquadro della firma. L'immagine viene configurata all'interno dei settaggi dell'applicazione (consultare la sezione 3.10.4 per maggiori dettagli e su alcuni consigli su come ottenere un risultato ottimale) e viene mostrata graficamente nella parte in basso a destra del riquadro di firma.

A seconda dei vari settaggi indicati sul PDF verrà mostrata una firma visuale simile alla seguente:

I campi mostrati vengono avvalorati nel seguente modo:

- In *Firmato Digitalmente da/Signed by* viene inserito in automatico il Common Name del certificato di firma utilizzato, solitamente nome e cognome del titolare
- Subito sotto appare il Ruolo/Qualifica indicato nei settaggi
- *In Data/On Date* viene inserito in automatico e indica la data in cui si esegue la firma
- *Motivazione/Reason* viene mostrato solo se queste vengono indicate nei settaggi (il campo va a capo automaticamente su più righe)
- Infine, l'immagine che si sceglie di inserire, allineata in basso a destra.

Oltre alle posizioni predefinite ai 4 angoli della pagina, è possibile anche posizionare il riquadro della firma in una posizione diversa da quelle predefinite e con dimensioni personalizzate, disegnando il riquadro direttamente sulla pagina desiderata nel documento.

Per eseguire l'operazione, premere il seguente pulsante:

Si aprirà l'anteprima del documento PDF:

Posizionarsi prima di tutto sulla pagina desiderata utilizzando la toolbar in alto:

Scelta la pagina, disegnare un rettangolo direttamente sulla pagina con il mouse:

Eventualmente spostare il riquadro trascinandolo con il mouse e quando si è pronti premere il tasto conferma. Se invece si vuole ricominciare, disegnare nuovamente il riquadro nel punto della pagina desiderato.

Una volta confermata la posizione, nella pagina precedente l'icona apparirà di colore verde e alcune opzioni saranno deselezionate a conferma che la posizione del riquadro è stata personalizzata:

A questo punto procedendo con la firma del documento, il risultato sarà qualcosa di simile:

3.3.5.3 Firma non qualificata

Se si vuole apporre una firma senza utilizzare un certificato di firma qualificata, al momento dell'avvio dell'operazione di firma, è possibile scegliere il certificato deselezionando l'opzione **Usa Firma Digitale** nella sezione **Scelta del Certificato**:

A questo punto aprire il menu a tendina e scegliere il certificato da utilizzare:

Selezionare il certificato desiderato ed eseguire l'operazione di firma.

Si noti che, una firma eseguita con un certificato non qualificato, verrà considerata non valida dal punto di vista legale. Utilizzare quindi questa funzionalità solo in casi particolari nei quali si desidera eseguire firme non qualificate.

3.3.6 Firma Multipla

L'applicazione Kit di Firma fornisce una funzionalità di firma assistita che permette di firmare una serie di documenti in maniera semi automatizzata. Questa funzionalità, nonostante aggiunga un certo livello di automatismo, garantisce comunque i principi di base della firma digitale (consultare la sezione 13.2 della *Guida alla Firma Digitale* fornita da AGID per maggiori informazioni http://www.agid.gov.it/sites/default/files/linee_guida/guida_alla_firma_digitale_2009_a_0_0_0.pdf):

- L'utente può visionare il documento da firmare prima della firma,
- L'utente deve selezionare il certificato di firma,
- Nel caso di certificato di firma su smart card, l'utente deve inserire il PIN di Firma a ogni operazione di firma

Per avviare la firma multipla esistono vari modi:

- Dalla schermata home, trascinare i documenti desiderati sulla schermata dell'applicazione
- Dalla schermata home, premere il tasto **apri file**, selezionare i documenti desiderati e premere il tasto Apri
- Se si è già caricato un documento all'interno della schermata firma, premere il tasto **aggiungi file** e selezionare i documenti da aggiungere

Appena l'applicazione individua la situazione di più documenti caricati, viene attivata la funzione di firma multipla:

Nella schermata verranno mostrati tutti i documenti pronti per essere firmati, facendo riferimento alla seguente schermata:

Viene mostrato nell'ordine:

1. Il tipo di documento caricato
2. Il nome del documento caricato (e, in casi particolari, alcune informazioni extra)
3. Il link per visualizzare l'anteprima del documento
4. Un pulsante per rimuovere il documento dall'elenco
5. Una barra di scorrimento che indica lo stato di esecuzione dell'operazione
6. Una barra di stato che indica la fase attuale di firma
7. Un'icona che indica in verde che l'operazione di firma è stata eseguita, in arancione che è in attesa, in grigio che non è stata avviata

Clickare il tasto **avanti** per passare al secondo passo della procedura:

Selezionare la casella di spunta in basso e premere il tasto **firma digitalmente**, l'applicazione mostrerà lo stato di elaborazione dei singoli documenti. Se tutti i documenti sono in formato PDF, sarà possibile scegliere anche di firmarli in formato PAdES e impostare i settaggi relativi al PAdES.

Durante l'elaborazione dei documenti, verrà richiesto il PIN Carta e PIN Firma se la chiave privata del certificato usato si trova su smart card. Al termine dell'elaborazione verrà mostrato l'esito:

Premere il tasto **SI** per scegliere dove salvare tutti i documenti firmati:

Scegliere la cartella destinazione e premere il tasto **OK**. I documenti verranno salvati tutti e verrà mostrato un messaggio di riepilogo:

Premere il tasto **ok** per terminare.

Da notare che a seconda dei documenti caricati nella firma multipla, l'applicazione si comporterà in un modo diverso:

- Se tutti i documenti caricati sono in formato PDF si potrà scegliere di eseguire la firma PAdES o CAdES
  - Se tra questi documenti, alcuni sono già firmati digitalmente in formato PAdES e si sceglie la firma PAdES, per questi verrà eseguita la controfirma PAdES. In questo caso assicurarsi di impostare le opzioni del box di firma in modo che il nuovo rettangolo grafico di firma non ricopra quelli preesistenti.
- Se tutti i documenti caricati sono in formato XML, si potrà scegliere di eseguire la firma XAdES o CAdES
- In tutti gli altri casi e in situazioni miste, si potrà scegliere solo la firma CAdES

Al fine di agevolare le operazioni di firma multipla, nella schermata di riepilogo, viene indicato il tipo di documento sotto il nome del file:

Ministero Difesa Kit di Firma v.4.5.0.0 - File Caricati: 7
HOME | SMARTCARD | CA ACCREDITATE | SETTAGGI
verifica
firma
marca
cifra
decifra
Lista File Caricati
File Caricati
7
Tipo File
-
aggiungi file
TEST_NEW.pdf
Dichiara conformità PDF/A (ISO 19005-1)
.PDF
Visualizza File
In Attesa...
TEST_PDFA_F1.pdf
Documento conforme PDF/A già firmato (PAdES)
.PDF
Visualizza File
In Attesa...
TEXT.txt
.TXT
Visualizza File
In Attesa...
TEXT.txt.p7m
Documento già firmato (CAdES)
.P7M
Visualizza File
In Attesa...
WORD.docx
.DOCX
Visualizza File
In Attesa...
pulisci
esegui firma asic invece che la firma multipla
avanti

3.4 Operazioni di Marcatura Temporale

L'applicazione Kit di Firma è in grado di eseguire operazioni di marcatura temporale su qualsiasi tipo di documento o file di cui si dispone, producendo quattro differenti formati di marcatura:

- ***TSD – Time Stamped Data***: è un'unica struttura con all'interno il documento e la marca temporale, secondo lo standard RFC 5544. La procedura consiste nel richiedere una marca temporale per il documento attualmente caricato e nel creare un file con all'interno sia la marca temporale, sia il documento stesso. Si può quindi parlare in questo caso di una marca temporale *attached* al documento. È anche possibile includere la CRL della Time Stamping Authority al momento della richiesta di marcatura temporale, ciò serve a provare la validità che aveva in quel momento il certificato della Time Stamping Unit che ha emesso la marca temporale. La busta crittografica prodotta sarà salvata con l'aggiunta dell'estensione **.tsd** al nome del documento originale.

- ***TSR – Time Stamp Response***: è la risposta esatta del servizio di marcatura temporale. Questa risposta comprende oltre alla marca temporale, anche ulteriori informazioni aggiunte dal servizio, come lo stato della risposta. Questo tipo di marcatura non contiene il documento marcato, ma solo il suo hash. La busta crittografica prodotta sarà salvata con l'aggiunta dell'estensione **.tsr** al nome del documento originale.

- ***TST – Time Stamp Token***: è la marca temporale vera e propria, senza altre informazioni. In questo caso di parla di una marca temporale detached al documento, in quanto essa va conservata insieme al documento originale. Questo tipo di marcatura non contiene il documento marcato, ma solo il suo hash. La busta crittografica prodotta sarà salvata con l'aggiunta dell'estensione **.tst** al nome del documento originale.

- ***ASiC-E TST – Extended Associated Signature Containers with Time Stamp Token***: è un archivio zip contenente uno o più documenti e un indice marcato temporalmente in formato TST. Lo stesso archivio può essere esteso nel tempo aggiungendo altri documenti e marcando il nuovo indice. La busta crittografica prodotta sarà salvata con il nome ContenitoreMarcature_*[DATA]*.**asice** (ad esempio ContenitoreMarcature_2021_12_14_16_32_28.asice)

Per tutte le operazioni di marcatura temporale verrà sempre utilizzato l'algoritmo di hashing **SHA-256**.

Per eseguire un'operazione di marcatura temporale, è necessario prima di tutto caricare il documento in memoria. Premere il seguente tasto dalla toolbar:

Apparirà la seguente schermata:

Sulla parte sinistra, premere il tasto a**pri nuovo file**. Apparirà una schermata per la scelta del documento:

Selezionare il documento desiderato e premere il tasto **Apri** (o **Open**). Il documento verrà caricato in memoria e l'applicazione mostrerà la seguente informazione:

Il nome del documento apparirà sia nel titolo della finestra, sia sulla parte sinistra della schermata. A questo punto si potrà scegliere il formato di marcatura temporale e richiederla effettivamente.

Se prima di procedere si volesse visualizzare una preview del documento, clickare sulla voce **Visualizza File** nella parte sinistra della schermata sotto l'icona del documento. Il documento verrà aperto utilizzando l'applicazione associata al formato del documento stesso.

3.4.1 Creazione di un documento Time Stamped Data

Dalla schermata di marcatura, scegliere la voce **timestamp data**, eventualmente cambiare i parametri della richiesta o il servizio di marcatura da utilizzare se differente da quello predefinito:

Quando pronti, premere il tasto **marca**. L'operazione sarà avviata e al termine verrà mostrato l'esito.

Nel caso di esito positivo verrà mostrata la seguente schermata:

Premendo il tasto **SI** la marca temporale sarà salvata nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di marcatura temporale è terminata.

3.4.2 Richiesta di una Time Stamp Request

Dalla schermata di marcatura, scegliere la voce **timestamp response**, eventualmente cambiare il servizio di marcatura da utilizzare se differente da quello predefinito:

Quando pronti, premere il tasto **marca**. L'operazione sarà avviata e al termine verrà mostrato l'esito.

Nel caso di esito positivo verrà mostrata la seguente schermata:

Premendo il tasto **SI** la marca temporale sarà salvata nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di marcatura temporale è terminata.

3.4.3 Richiesta di un Time Stamp Token

Dalla schermata di marcatura, scegliere la voce **timestamp token**, eventualmente cambiare il servizio di marcatura da utilizzare se differente da quello predefinito:

Quando pronti, premere il tasto **marca**. L'operazione sarà avviata e al termine verrà mostrato l'esito.

Nel caso di esito positivo verrà mostrata la seguente schermata:

Premendo il tasto **SI** la marca temporale sarà salvata nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di marcatura temporale è terminata.

3.4.4 Creazione di un contenitore ASiC-E TST

Dalla schermata di marcatura, scegliere la voce **contenitore asic-e timestamp token**, eventualmente cambiare il servizio di marcatura da utilizzare se differente da quello predefinito:

È possibile anche inserire più di un documento all'interno del contenitore, semplicemente selezionando più di un documento nella finestra che viene mostrata clickando **apri nuovo file**. In questo caso la finestra sarà simile alla seguente:

In entrambi i casi, quando pronti, premere il tasto **marca**. L'operazione sarà avviata e al termine verrà mostrato l'esito.

Nel caso di esito positivo verrà mostrata la seguente schermata:

Premendo il tasto **SI** la marca temporale sarà salvata nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di marcatura temporale è terminata.

3.4.5 Estensione di un contenitore ASiC-E TST

Come detto in precedenza, la caratteristica principale dei contenitori ASiC-E TST è che questi possono essere estesi nel tempo aggiungendo nuovi documenti al loro interno e marcandoli temporalmente. Per eseguire questa operazione, caricare un contenitore ASiC-E TST preesistente nella schermata di marcatura e scegliere la voce **contenitore asic-e timestamp token**:

Quando pronti, premere il tasto **marca** si attiverà e premendolo si aprirà una nuova finestra nella quale è possibile scegliere quali documenti includere all'interno del nuovo gruppo:

- Nella parte in alto vengono mostrati i documenti già presenti nel contenitore:
  - I documenti con il segno di spunta ☑ vengono inclusi nel nuovo gruppo. I documenti selezionati in questo modo vengono condivisi quindi tra più gruppi e marcati.

- I documenti con il segno di spunta ☐ non vengono inclusi nel nuovo gruppo. I documenti non selezionati rimangono nel contenitore ma vengono marcati nei gruppi preesistenti.

► Nella parte in basso vengono mostrati i nuovi documenti da aggiungere al contenitore:
- Con il pulsante ⊕ è possibile selezionare un documento dal disco della propria workstation
- Con il pulsante ⊖ è possibile eliminare dalla lista un documento aggiunto per sbaglio.

Quando si è pronti, premere il tasto **conferma** proseguire. L'operazione sarà avviata e al termine verrà mostrato l'esito.

Nel caso di esito positivo verrà mostrata la seguente schermata:

Premendo il tasto **SI** la marca temporale sarà salvata nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece si potrà specificare un percorso alternativo. Nella schermata successiva, il caso del percorso predefinito:

Premere il tasto **ok**, a questo punto l'operazione di marcatura temporale è terminata.

3.5 Operazioni di Cifra

L'applicazione Kit di Firma è in grado di eseguire operazioni di cifra asimmetrica di qualsiasi tipo di documento o file di cui si dispone, creando una busta crittografica nel formato **CMS Enveloped Data**. L'algoritmo di cifra utilizzato sarà l'**Advanced Encryption Standard (AES)** con chiave a lunghezza **256bit** e **Cipher-block chaining (CBC) (AES256CBC)**.

La cifra asimmetrica permette di cifrare lo stesso documento a più certificati destinatari. Per questo motivo si parlerà di **Destinatari** da scegliere da tre differenti sorgenti:

- **store**: lo store dei certificati di Windows al cui interno vengono immagazzinati i certificati di cui si possiede la chiave privata e i certificati degli altri utenti. Lo store è locale alla postazione di lavoro dell'utente.
- **file**: un file contenente il certificato da utilizzare come destinatario
- **LDAP**: un servizio remoto di directory LDAP a cui collegarsi per ricercare i certificati dei destinatari

L'operazione di cifratura può essere eseguita su un solo documento o su più documenti contemporaneamente usando la stessa lista di destinatari.

Per eseguire un'operazione di cifra, dalla schermata principale dell'applicazione, clickare il seguente tasto dalla toolbar:

Apparirà la seguente schermata:

SELEZIONE DEI DOCUMENTI DA CIFRARE

Per aggiungere uno o più documenti da cifrare è possibile:

- Trascinare da Explorer di Windows i documenti sull'area indicata al centro

- Aggiungere uno o più documenti tramite il tasto **aggiungi documenti** a sinistra. Apparirà una schermata per la scelta di uno o più documenti:

Selezionare il documento desiderato o più di uno[6] e premere il tasto **Apri** (o **Open**).

- Aggiungere intere cartelle di documenti tramite il tasto **aggiungi cartella** a sinistra. Prestare attenzione al fatto che questa modalità aggiunge tutti i documenti contenuti nella cartella e nelle eventuali sottocartelle ricorsivamente.

Selezionare la cartella da aggiungere e premere il tasto **OK**.

[6] Per selezionare più file contemporaneamente, clickare sulle singole voci con il tasto sinistro del mouse mentre si tiene premuto il tasto Ctrl sulla tastiera

LA LISTA DEI DOCUMENTI PRONTI PER LA CIFRA

A prescindere dal modo utilizzato per selezionare i documenti da cifrare, l'applicazione visualizzerà la lista dei documenti scelti e sarà sempre possibile aggiungere altri documenti usando uno dei metodi indicati in precedenza:

Tenendo in considerazione la singola voce nell'elenco:

Viene mostrato nell'ordine:

1. Il tipo di documento caricato
2. Il nome del documento caricato
3. Il link per visualizzare l'anteprima del documento (se possibile)
4. Un pulsante per rimuovere il documento dall'elenco
5. Una barra di scorrimento che indica lo stato di esecuzione dell'operazione
6. Il nome completo del documento comprensivo di cartella
7. Una barra di stato che indica la fase attuale di cifra durante l'operazione massiva
8. Un'icona che indica in verde che l'operazione di cifra è stata eseguita, in arancione che è in attesa, in grigio che non è stata avviata

SCELTA DEI DESTINATARI A CUI CIFRARE

Quando si è pronti, clickare sul tasto **avanti** per passare al secondo passo della procedura, ovvero la scelta dei destinatari:

A questo punto è necessario indicare nella lista chiamata **Destinatari** i certificati a cui cifrare il documento e questi possono essere scelti utilizzando i tre pulsanti in alto a destra indicati come **Disponibili**:

Utilizzando una delle tre opzioni di scelta e seguire i dettagli nelle seguenti sezioni (3.5.1, 3.5.2 e 3.5.3):

- ***Aggiungi Destinatario Store***: il certificato verrà ricercato all'interno dello store di Windows del PC dell'utente (3.5.1)
- ***Aggiungi Destinatario File***: il certificato verrà caricato da un file (3.5.2)
- ***Aggiungi Destinatario LDAP***: il certificato verrà ricercato e scaricato da un server LDAP (3.5.3)

Durante la scelta dei certificati destinatari, la schermata apparirà in modo simile alla seguente:

Nella lista **Destinatari** vengono visualizzati tutti i certificati fin qui scelti:

- Premendo il tasto , il certificato selezionato verrà rimosso dalla lista
- Premendo il tasto , del certificato selezionato verranno mostrati i dettagli
- Premendo il tasto , il certificato selezionato sarà salvato nello store dei certificati di Windows nello spazio Altri Utenti. Questa opzione è utile se si vuole creare una rubrica di utenti a partire da certificati recuperati da file o da LDAP e non doverli ogni volta recuperare dalle sorgenti originali.

Una volta completata la lista scegliendo i certificati da una qualunque sorgente, è possibile avviare la cifra dei documenti tramite il tasto **cifra** in basso a destra. L'opzione invece a sinistra serve a indicare all'applicazione di ignorare la configurazione globale dell'applicazione riguardo la cartella di lavoro (si veda sezione 3.10.2 per maggiori dettagli) e salvare tutti i documenti cifrati insieme al documento originale nel suo percorso: ogni documento cifrato si distingue dall'originale in chiaro per via della nuova estensione **.p7m** aggiunta al nome.

L'OPERAZIONE DI CIFRA

Una volta clickato sul tasto **cifra**, l'applicazione passerà nuovamente alla lista dei documenti, ma questa volta mostrerà lo stato dell'operazione di cifra su tutti i documenti scelti:

Al termine verrà mostrato un messaggio di conferma per il salvataggio dei documenti:

Clickando **NO** non si procede al salvataggio, clickando invece **SI** tutti i documenti cifrati verranno salvati in formato **CMS Enveloped Data** con estensione **.p7m** nei percorsi scelti e verrà mostrata una conferma con il riepilogo dei singoli documenti:

Premere il tasto **ok**, a questo punto l'operazione di cifra è terminata.

MODALITÀ ALTERNATIVE PER AVVIARE L'OPERAZIONE DI CIFRA

Per eseguire un'operazione di cifra, è anche possibile iniziare in altri modi:

- Dalla schermata principale dell'applicazione, aprire o trascinare un singolo documento e poi premere il seguente tasto dalla toolbar:

- Dalla schermata principale dell'applicazione, aprire o trascinare più di un documento. L'applicazione passerà alla procedura di firma multipla, ma invece di eseguire la firma clickare sul tasto indicato (**passa a cifra multipla**):

In queste due modalità, si passerà direttamente alla lista dei documenti però con già i documenti caricati:

A questo punto si procede come spiegato precedentemente.

3.5.1 Aggiunta di un Destinatario da Store

Premendo il tasto **store**, apparirà una schermata di selezione certificato. In **Personale** sono contenuti i certificati di cui si possiede la coppia di chiavi. Tale scelta si effettua solitamente se si vuole cifrare il documento anche a sé stesso. Se invece si vuole cifrare il documento per un altro utente, i certificati si possono trovare in **Altri Utenti**:

Selezionare il certificato desiderato e premere il tasto ←:

Il certificato scelto verrà aggiunto alla lista **Destinatari**. Aggiungere gli altri destinatari da una qualunque sorgente e al termine premere il tasto **Cifra**. L'operazione di cifra verrà eseguita e comparirà un messaggio di conferma.

3.5.2 Aggiunta di un Destinatario da File

Premendo il tasto **file**, apparirà una schermata di selezione certificato.

Premere il tasto cerca, apparirà una schermata di selezione file:

Scegliere il file desiderato con il certificato e premere il tasto **Apri**:

Il certificato caricato verrà visualizzato nella parte destra, se è quello desiderato, premere il tasto

Il certificato scelto verrà aggiunto alla lista **Destinatari**. Aggiungere gli altri destinatari da una qualunque sorgente e al termine premere il tasto **Cifra**. L'operazione di cifra verrà eseguita e comparirà un messaggio di conferma.

3.5.3 Aggiunta di un Destinatario da LDAP

Premendo il tasto **ldap**, apparirà una schermata di ricerca certificato:

Inserire i parametri di ricerca (**Cognome**, **Nome** e **ID Carta** da 9 caratteri della CMD/ATe), scegliere eventualmente il servizio LDAP (**Server**) su cui concentrare la ricerca e premere il tasto **cerca**:

I risultati della ricerca verranno mostrati nella lista a destra. Per evitare di utilizzare certificati non corretti, Kit di Firma considererà soltanto certificati non scaduti e non revocati, per questo motivo la procedura di ricerca potrebbe impiegare qualche minuto soprattutto nel caso di certificati per il quale non è disponibile un servizio di OCSP (ad esempio quelli delle CMD-1). Selezionare il certificato desiderato e premere il tasto ←:

Il certificato scelto verrà aggiunto alla lista **Destinatari**. Aggiungere gli altri destinatari da una qualunque sorgente e al termine premere il tasto **Cifra**. L'operazione di cifra verrà eseguita e comparirà un messaggio di conferma.

3.6 Operazioni di Verifica

L'applicazione Kit di Firma è in grado di verificare documenti crittografici nei seguenti formati:

- Documenti Firmati:
  - ***CAdES***: documenti generici firmati secondo le normative europee con firme secondi i profili di base B, T, LT ed LTA
  - ***CMS Signed Data***: documenti generici firmati
  - ***PKCS#7 Signed Data***: documenti generici firmati
  - ***XAdES***: documenti XML firmati secondo le normative europee con firme secondi i profili di base B, T, LT ed LTA
  - ***XMLDSIG:*** documenti XML firmati secondo le specifiche di base internazionali
  - ***PAdES***: documenti PDF firmati secondo le normative europee con firme secondi i profili di base B, T, LT ed LTA
  - ***PDF Signed***: documenti PDF firmati secondo le specifiche di base internazionali
  - ***ASiC-E CAdES***: contenitori di documenti firmati secondo le normative europee con firme CAdES secondi i profili di base B, T, LT ed LTA
  - ***ASiC-E XAdES***: contenitori di documenti firmati secondo le normative europee con firme XAdES secondi i profili di base B, T, LT ed LTA
  - ***ASiC-S CAdES***: contenitori con documento firmato secondo le normative europee con firme CAdES secondi i profili di base B, T, LT ed LTA
  - ***ASiC-S XAdES***: contenitori con documento firmato secondo le normative europee con firme XAdES secondi i profili di base B, T, LT ed LTA

- Marche Temporali:
  - ***TSD***: documenti Time Stamped Data
  - ***TSR***: marche temporali Time Stamp Response
  - ***TST***: marche temporali Time Stamp Token
  - ***ASiC-E TST***: contenitori di documenti e marche temporali
  - ***ASiC-S TST***: contenitori con documento e marca temporale

Ognuno di questi formati verrà trattato dall'applicativo in una modalità differente. I dettagli sono indicati nelle sezioni seguenti.

3.6.1 Verifica di un documento firmato

Per eseguire un'operazione di verifica di un documento firmato, è necessario prima di tutto caricare il documento in memoria. Premere il seguente tasto dalla toolbar:

Apparirà la seguente schermata:

Premere il pulsante **apri nuovo file**:

Scegliere il documento da verificare e premere il pulsante Apri, sarà avviata la procedura di verifica del documento e al termine apparirà l'esito:

La verifica potrebbe impiegare un tempo che dipende da diversi fattori:

- Lentezza della rete o dei servizi che espongono la CRL o il servizio OCSP
- Verifica dello stato di un certificato esclusivamente da CRL per mancanza del servizio OCSP
- Numero di firmatari del documento
- Dimensioni del documento firmato

Sulla schermata dell'esito vengono rappresentate diverse informazioni:

- Sulla sezione a sinistra:
  - Un link per visualizzare il documento firmato (consultare 3.8 per maggiori informazioni)
  - Il nome del documento firmato
  - Il tipo di documento
  - Il tipo di firma e la versione di riferimento della normativa
  - L'esito della verifica (verificato senza errori ✓, verificato con avvisi ⚠, verificato con errori gravi ✗)
  - Un pulsante per salvare il documento firmato originariamente (**salva contenuto**) nella stessa cartella del documento firmato
  - Un pulsante per salvare il documento firmato originariamente (**salva contenuto come**...) in una cartella specifica
  - Un pulsante per chiudere tutto (**pulisci**)

- Sulla sezione a destra:
  - L'alberatura dei firmatari
  - Le **Opzioni di Verifica** ovvero la data in cui eseguire la verifica e se salvare l'esito della verifica anche in un formato XML (per utenti avanzati)

Nella sezione a destra della schermata, come detto, viene mostrata l'alberatura delle firme apposte a un documento. Per ogni firma viene evidenziato lo stato dei singoli controlli che l'applicazione esegue per poter poi determinare la validità della singola firma e conseguentemente dell'intero documento firmato. Accanto a ogni nodo della struttura ad albero, è presente il pulsante tramite il quale è possibile chiudere la sotto alberatura, o il pulsante per espanderla.

Un firmatario verrà mostrato come un singolo oggetto di questo tipo:

Le varie sezioni indicano informazioni differenti come dettagliato nel seguito. Inoltre, per ogni sezione viene indicato l'esito della verifica e tramite il pulsante è possibile mostrare i dettagli della singola sezione. In ogni sezione, nei dettagli viene riportata una particolare sezione chiamata Messaggi all'interno della quale si trovano una serie di informazioni , degli avvisi e degli errori .

CERTIFICATO

Indica le informazioni sul certificato del firmatario e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Per visualizzare i dettagli del certificato del firmatario, clickare il link **Visualizza Certificato**:

Clickando sul link nella sezione **Emesso da** è possibile visualizzare le informazioni sulla CA che lo ha emesso, con il pulsante **salva** è possibile salvare su file il certificato, con il pulsante **chiudi** si chiude la finestra.

Clickando invece sulla pagina **DETTAGLI** è possibile visualizzare le informazioni dettagliate sul certificato:

CERTIFICATO CA

Indica le informazioni sul certificato della Certification Authority che ha emesso il certificato del firmatario e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Per visualizzare i dettagli del certificato del firmatario, clickare il link **Visualizza Certificato**:

Clickando sul link nella sezione **Emesso da** è possibile visualizzare le informazioni sulla CA che lo ha emesso, con il pulsante **salva** è possibile salvare su file il certificato, con il pulsante **chiudi** si chiude la finestra.

Clickando invece sulla pagina **DETTAGLI** è possibile visualizzare le informazioni dettagliate sul certificato come visto in precedenza.

FIRMA

Indica le informazioni sulla firma o firma parallela e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Viene indicato anche il profilo di base cui fa riferimento la firma (lettera tra parentesi a sinistra o dicitura Tipo).

Nel caso di firme PAdES con profilo LT ed LTA, oltre ai dettagli indicati in 3.6.2.1, in corrispondenza dei messaggi vengono anche mostrate le informazioni sui certificati delle CA/TSA e sulle validità OCSP/CRL aggiunti al documento nel momento della firma:

CONTROFIRMA

Indica le informazioni sulla controfirma e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Viene indicato anche il profilo di base cui fa riferimento la controfirma (lettera tra parentesi a sinistra o dicitura Tipo).

Nel caso di firme PAdES con profilo LT ed LTA, oltre ai dettagli indicati in 3.6.2.1, in corrispondenza dei messaggi vengono anche mostrate le informazioni sui certificati delle CA/TSA e sulle validità OCSP/CRL aggiunti al documento nel momento della firma:

TS FIRMA

Se presente, indica le informazioni sulla marca temporale della firma e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Tramite il link **Salva Marca Temporale** è possibile salvare la marca temporale su disco. Con il link **Visualizza Certificato TSU** è possibile visualizzare i dettagli del certificato del servizio TSU:

Tramite il link **Visualizza Certificato TSA** è possibile visualizzare i dettagli del certificato della CA che ha emesso il certificato della TSU, ovvero la TSA:

TS DI ARCHIVIAZIONE

Nel caso di documenti CAdES e XAdES, se presente, indica le informazioni sulla marca temporale di archiviazione e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Tramite il link **Salva Marca Temporale** è possibile salvare la marca temporale su disco. Con il link **Visualizza Certificato TSU** è possibile visualizzare i dettagli del certificato del servizio TSU come visto in precedenza. Tramite il link **Visualizza Certificato TSA** è possibile visualizzare i dettagli del certificato della CA che ha emesso il certificato della TSU, ovvero la TSA, come visto in precedenza.

TS DOCUMENTO

Nel caso di documenti CAdES, se presente, indica le informazioni sulla marca temporale del documento e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Tramite il link **Salva Marca Temporale** è possibile salvare la marca temporale su disco. Con il link **Visualizza Certificato TSU** è possibile visualizzare i dettagli del certificato del servizio TSU come

visto in precedenza. Tramite il link **Visualizza Certificato TSA** è possibile visualizzare i dettagli del certificato della CA che ha emesso il certificato della TSU, ovvero la TSA, come visto in precedenza.

VALIDITÀ

Indica le informazioni sullo stato di validità del certificato del firmatario e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive. Le informazioni visualizzate riguardano principalmente la validità secondo la data di scadenza, la revoca, la sospensione e il modo in cui la validità è stata ricavata, ovvero tramite il servizio OCSP o tramite CRL.

Clickando il link **Visualizza Certificato OCSP** è possibile visualizzare il certificato del servizio OCSP utilizzato per il controllo:

Se invece lo stato viene controllato tramite CRL, vengono mostrate le seguenti informazioni:

Clickando il link **Visualizza CRL** è possibile visualizzare la CRL scaricata per il controllo:

3.6.2 Casi particolari di documenti firmati

3.6.2.1 Firme eseguite con Sigilli Elettronici

All'interno dei documenti firmati, se alcune firme sono state eseguite con certificati di **Sigillo Elettronico**[7], queste verranno mostrate in modo da distinguerle dalle Firme Elettroniche Qualificate mediante icone e messaggi particolari:

Nei dettagli del "Sigillo" verranno mostrati i dettagli ricavati dai QcStatements (QcType):

[7] https://www.agid.gov.it/sites/default/files/repository_files/tipologie_di_firme_e_sigilli_elettronici_v1_dicembre_2019.pdf

3.6.2.2 Firme di tipo Firma Elettronica Avanzata (FEA)

All'interno dei documenti firmati, se alcune firme sono state eseguite con certificati di **Firma Elettronica Avanzata** (**FEA**, o in inglese **Advanced Electronic Signature** (**AdES**)) come, ad esempio, quello presente sulla Carta di Identità Elettronica[8] italiana (CIE), queste verranno mostrate in modo da distinguerle dalle Firme Elettroniche Qualificate mediante icone, colarazione e messaggi particolari, per distinguerle dalle normali Firme Elettroniche Qualificate (FEQ):

Nei dettagli della "Firma" verranno mostrati i dettagli:

[8] Per informazioni sulla FEA tramite CIE e su quali tipi di documenti possono essere firmati con questa modalità, far riferimento al seguente documento: https://www.cartaidentita.interno.gov.it/cittadini/firma-con-cie/

3.6.2.3 Firme PAdES e profilo di base LTA

Nel caso di documenti firmati in PAdES e con firme secondo il profilo di base LTA, le informazioni mostrate riguardo la marca temporale di archiviazione, aggiunta alla firma per prolungarne la validità, vengono mostrate in modo leggermente differente:

L'icona indica un differente tipo di "firmatario" e le informazioni sul Certificato e il Certificato CA si riferiscono rispettivamente al servizio TSU e alla sua TSA e non a un firmatario vero e proprio.

MARCATURA

Indica le informazioni sulle informazioni della marcatura e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

TS DOCUMENTO

Indica le informazioni sulla marca temporale di archiviazione (chiamata marca temporale documento nel caso del PAdES) e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Tramite il link **Salva Marca Temporale** è possibile salvare la marca temporale su disco. Con il link **Visualizza Certificato TSU** è possibile visualizzare i dettagli del certificato del servizio TSU come visto in precedenza. Tramite il link **Visualizza Certificato TSA** è possibile visualizzare i dettagli del certificato della CA che ha emesso il certificato della TSU, ovvero la TSA, come visto in precedenza.

3.6.2.4 Firme PAdES e revisioni

Nel caso di documenti firmati nel formato PAdES, per agevolare la verifica e l'analisi delle variazioni tra una firma e l'altra, oltre che dopo l'ultima firma, alle informazioni indicate nella sezione 3.6.1 sono presenti ulteriori strumenti:

1. Nella sezione di visualizzazione delle informazioni sui firmatari al centro, la sezione Firma contiene due link per visualizzare e salvare il documento PDF che l'utente firmatario ha firmato in quel preciso momento, quindi la **Revisione *n***:

   Il link **Visualizza revisione** aprirà il documento PDF in visualizzazione, mentre **Salva revisione** salverà la porzione del PDF sulla postazione.

2. Nella sezione informativa sul formato del documento in alto a sinistra, è presente un link chiamato **Visualizza documento completo**, tramite il quale è possibile visualizzare il documento PDF nella sua interezza. Questa funzione permette quindi di visualizzare il documento così com'è attualmente, comprensivo di modifiche oltre l'ultima firma apposta:

3. Nella sezione con l'esito riassuntivo della verifica in basso a sinistra, un pulsante chiamato **report revisioni** permetterà di produrre un report di tutte le modifiche apportate al documento PDF tra una firma e l'altra, nonoché dopo l'ultima firma:

Facendo click sul tasto **report revisioni**, apparirà una finestra simile alla seguente:

Come si nota in questo esempio:

- La Revisione 1, corrispondente alla prima firma, attesta la versione iniziale del documento.
- La Revisione 2, corrispondente alla seconda firma, attesta il documento precedente nel quale sono stati compilati due campi form (Cognome richiedente e Email 2).
- Dopo la seconda firma al documento sono state apportate delle modifiche riportate nell'apposita sezione (compilazione del campo form Località e data). A questo tipo di modifiche bisogna prestare particolare attenzione, in quanto aprendo il PDF con un visualizzatore, ci si troverà di fronte all'ultima versione salvata, versione che potrebbe essere differente da quella firmata dai precedenti firmatari.

Facendo click sui titoli delle sezioni, verrà mostrato il documento PDF corrispondente alla revisione:

REVISIONE 1:

REVISIONE 2:

DOCUMENTO INTERO:

Un documento senza varianti dopo l'ultima firma apparirà nel seguente modo:

3.6.2.5 Firme ASiC

Nel caso di contenitori di firme ASiC, verranno visualizzate le informazioni sulla tipologia del contenitore, ovvero una delle sue 4 combinazioni ASiC-E CAdES, ASiC-E XAdES, ASiC-S CAdES e ASiC-S XAdES:

Inoltre, l'alberatura delle firme presenterà alcune differenze, in quanto vengono mostrate anche le informazioni riguardo i vari gruppi di documenti:

GRUPPO DOCUMENTI

Indica le informazioni sui documenti che sono protetti nella relativa alberatura delle firme. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Gruppo documenti Numero 1 (5 documenti protetti)

Nome Manifesto: META-INF/ASiCManifest_f75e2ddc-ec4d-4f4a-8abb-991e71bf6b23.xml
Nome Oggetto Firmato: META-INF/signature_94407dda-1288-483a-9928-81a8c5be000a.p7s

Documenti protetti

Documento	Protetto da
PDF.pdf	META-INF/signature_94407dda-1288-483a-9928-81a8c5be000a.p7s
PDF-1A.docx	META-INF/signature_94407dda-1288-483a-9928-81a8c5be000a.p7s
PDF-1A.pdf	META-INF/signature_94407dda-1288-483a-9928-81a8c5be000a.p7s
WORD.docx	META-INF/signature_94407dda-1288-483a-9928-81a8c5be000a.p7s
XmlDocument.xml	META-INF/signature_94407dda-1288-483a-9928-81a8c5be000a.p7s

Aprendo il contenitore ASiC con un'applicazione in grado di gestire gli archivi Zip, ad esempio WinRAR, è possibile agire sui singoli documenti:

La cartella META-INF contiene tutti i file che servono a proteggere i vari gruppi di documenti, ovvero gli indici e le firme:

3.6.2.6 Firme XAdES di nodi singoli

Il Kit di Firma produce documenti firmati con busta XAdES dove la firma copre l'intero documento XML. Esistono però alcuni strumenti in grado di firmare singoli nodi del documento XML, lasciandone altri scoperti dalla firma. Per mostrare questa condizione, l'applicazione mostrerà delle informazioni differenti: prima di tutto la possibilità di visualizzare solo la porzione del documento XML firmata tramite il link **Visualizza nodo firmato** in corrispondenza della Firma:

La finestra di visualizzazione mostrerà soltanto il nodo firmato:

Se invece si vuole visualizzare l'intero documento firmato, usare il consueto link **Visualizza File** a sinistra della finestra (sezione 3.8.3).

Nei dettagli della firma verrà invece mostrato l'identificativo del nodo firmato nel campo **Codice** (nel nostro esempio il nodo con identificativo NCOMP):

3.6.2.7 Opzioni di verifica

Nella parte in basso della schermata di verifica, è presente una sezione chiamata **Opzioni di Verifica**:

Di solito una verifica viene eseguita automaticamente da Kit di Firma utilizzando le impostazioni migliori per verificare un documento, ovvero considerare come data di firma, la data della marca temporale della firma, oppure se non presente, usare la data corrente. Se invece il documento non presentasse la marca temporale di firma e si volesse specificare una data differente per la verifica, selezionare l'opzione **Verifica ad una data specifica** apparirà una nuova schermata:

Scegliere dal calendario la data da utilizzare ed eventualmente l'ora e premere il tasto **verifica** per rieseguire la verifica del documento utilizzando queste nuove impostazioni.

Per gli utenti più esperti è anche possibile produrre un report della verifica del documento in formato XML. Selezionare l'opzione **Produci l'esito della verifica in formato XML**, scegliere il formato del documento XML (**XML** per il formato custom dell'applicativo, **ETSI PlugTests** per il formato usato durante gli eventi ETSI Plug Test) e premere il tasto **verifica**. Al termine della verifica apparirà la seguente schermata:

Premere il tasto **salva risultato verifica**, apparirà un messaggio di conferma:

Premendo il tasto **SI** la marca temporale sarà salvata nella cartella predefinita (come scelto in fase di configurazione), premendo il tasto **NO** invece non si salverà nulla. Nel caso positivo, apparirà la seguente conferma:

Il nome del file dell'esito sarà sempre del tipo *NOMEORIGINALE*_**esito.xml** . Un file di esito conterrà le informazioni visualizzate graficamente ma in formato testuale XML:

```xml
<?xml version="1.0"?>
- <VerifyResponse>
    <VerifiedContent>JVBERi0xLjQKJYCAgIAKMSAwIG9iago8PC9UeXBlIC9DYXRhbG9nIC9QYWdlcyAzIDAgUiAvTWV0YWRhdGEg
  - <Errors>
      <Error type="SIGN" signerCode="Signature1" errorLevel="INFORMATION" code="PADESAC1">I permessi di accesso
        garantiti per questo documento sono: Nessun cambiamento permesso; qualunque cambiamento al documento
        ne invaliderà la firma.</Error>
      <Error type="CERT" signerCode="Signature1" errorLevel="INFORMATION" code="ERR992">Il certificato è stato
        emesso da una Certification Authority Accreditata</Error>
      <Error type="OCSP" signerCode="Signature1" errorLevel="INFORMATION" code="ERR198">Stato del certificato
        verificato su servizio OCSP</Error>
      <Error type="CTS" signerCode="Signature1" errorLevel="INFORMATION" code="ERR301">Content Time Stamp non
        presente.</Error>
      <Error type="STS" signerCode="Signature1" errorLevel="INFORMATION" code="ERR992">Il certificato è stato emesso
        da una Certification Authority Accreditata</Error>
      <Error type="STS" signerCode="Signature1" errorLevel="INFORMATION" code="ERR198">Stato del certificato
        verificato su servizio OCSP</Error>
      <Error type="SIGN" signerCode="Signature1" errorLevel="INFORMATION" code="ERR873">La firma è stata eseguita
        con un certificato emesso da una Certification Authority della E.U. (IT)</Error>
    </Errors>
  - <Signers>
    - <Signer type="SIGNATURE" code="Signature1" signatureAlgo="sha256WithRSAEncryption" digestAlgo="sha256"
      fatherCode="" level="1">
        <DNUser>dnQualifier=ZZAA00060, CN=DAMIANO DIEGO DE FELICE, SERIALNUMBER=IT:[redacted],
          G=DAMIANO DIEGO, SN=DE FELICE, OU=Esercito Italiano, O=Ministero della Difesa/97355240587,
          C=IT</DNUser>
        <CNUser>DAMIANO DIEGO DE FELICE</CNUser>
        <DNIssuer>CN=Ministero della Difesa - CA di Firma Digitale, SERIALNUMBER=97355240587, OU=S.M.D. - C.do
          C4 Difesa, O=Ministero della Difesa, C=IT</DNIssuer>
        <CNIssuer>Ministero della Difesa - CA di Firma Digitale</CNIssuer>
        <Certificate>MIIHjjCCBXagAwIBAgIIWFmwIW8WnSYwDQYJKoZIhvcNAQELBQAwgZ4xCzAJBgNVBAYTAklUMR8wHQ
        <Signers/>
        <SigningTime>04/23/2015 11:56:12</SigningTime>
        <SigningTimeUTC>04/23/2015 09:56:12</SigningTimeUTC>
        <SignatureTimeStamp>04/23/2015 11:55:25</SignatureTimeStamp>
        <SignatureTimeStampUTC>04/23/2015 09:55:25</SignatureTimeStampUTC>
        <SignatureTimeStampUnit>MIIGsjCCBJqgAwIBAgIIUxh+8XnrUOEwDQYJKoZIhvcNAQELBQAwgZ4xCzAJBgNVBAYTAkl
        <SignatureTimeStampToken>MIIJ4wYJKoZIhvcNAQcCoIIJ1DCCCdACAQMxDzANBglghkgBZQMEAgEFADB+BgsqhkiG9w
      </Signer>
    </Signers>
  </VerifyResponse>
```


3.6.3 Verifica di marche temporali

Per eseguire un'operazione di verifica di una marca temporale, è necessario prima di tutto caricare il documento in memoria. Premere il seguente tasto dalla toolbar:

Apparirà la seguente schermata:

Premere il pulsante **apri nuovo file**:

Scegliere il documento da verificare e premere il pulsante **Apri**, sarà avviata la procedura di verifica del documento e al termine apparirà l'esito. La schermata sarà differente a seconda del tipo di marca temporale aperta.

3.6.3.1 Marche Temporali di tipo Time Stamped Data

Se si sceglie di verificare una marca temporale di tipo Time Stamped Data (solitamente con estensione .tsd), apparirà la seguente schermata:

Il tutto è molto simile a quanto già descritto per la verifica dei documenti firmati, cambierà invece la parte a destra della schermata:

Per accedere invece al documento allegato, è possibile visualizzarlo tramite il link **Visualizza File** in alto a sinistra oppure salvarlo su disco tramite il pulsante **salva contenuto**.

CERTIFICATO

Indica le informazioni sul certificato del servizio TSU e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Per visualizzare i dettagli del certificato dela TSU, clickare il link **Visualizza Certificato** come visto in precedenza.

CERTIFICATO CA

Indica le informazioni sul certificato della Certification Authority che ha emesso il certificato della TSU, ovvero la TSA, e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Per visualizzare i dettagli del certificato della CA della TSU, clickare il link **Visualizza Certificato** come visto in precedenza.

TS DOCUMENTO

Se presente, indica le informazioni sulla marca temporale del documento e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Tramite il link **Salva Marca Temporale** è possibile salvare la marca temporale su disco. Con il link **Visualizza Certificato TSU** è possibile visualizzare i dettagli del certificato del servizio TSU come visto in precedenza. Tramite il link **Visualizza Certificato TSA** è possibile visualizzare i dettagli del certificato della CA che ha emesso il certificato della TSU, ovvero la TSA, come visto in precedenza.

VALIDITÀ

Indica le informazioni sullo stato di validità del certificato della TSU e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive. Le informazioni visualizzate riguardano principalmente la validità secondo la data di scadenza, la revoca, la sospensione e il modo in cui la validità è stata ricavata, ovvero tramite il servizio OCSP o tramite CRL.

Clickando il link **Visualizza Certificato OCSP** è possibile visualizzare il certificato del servizio OCSP utilizzato per il controllo. Se invece lo stato viene controllato tramite CRL clickando il link **Visualizza CRL** è possibile visualizzare la CRL scaricata per il controllo.

Infine, se durante la creazione del documento TSD fosse stata inclusa anche la CRL corrispondente alla TSU, questa sarà visualizzabile tramite il link **Visualizza CRL allegata**.

3.6.3.2 Marche Temporali di tipo Time Stamp Token e Time Stamp Response

Se si sceglie di verificare una marca temporale di tipo Time Stamp Token (solitamente con estensione .tst) o una marca temporale di tipo Time Stamp Response (solitamente con estensione .tsr), apparirà la seguente schermata:

Il tutto è molto simile a quanto già descritto per la verifica dei documenti firmati, cambierà invece la parte a destra della schermata:

CERTIFICATO

Indica le informazioni sul certificato del servizio TSU e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Per visualizzare i dettagli del certificato dela TSU, clickare il link **Visualizza Certificato** come visto in precedenza

CERTIFICATO CA

Indica le informazioni sul certificato della Certification Authority che ha emesso il certificato della TSU, ovvero la TSA, e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Per visualizzare i dettagli del certificato della CA della TSU, clickare il link **Visualizza Certificato** come visto in precedenza

FIRMA

Indica le informazioni sulla firma della marca temporale e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

VALIDITÀ

Indica le informazioni sullo stato di validità del certificato della TSU e l'esito della sua verifica. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive. Le informazioni visualizzate riguardano principalmente la validità secondo la data di scadenza, la revoca, la sospensione e il modo in cui la validità è stata ricavata, ovvero tramite il servizio OCSP o tramite CRL.

Clickando il link **Visualizza Certificato OCSP** è possibile visualizzare il certificato del servizio OCSP utilizzato per il controllo. Se invece lo stato viene controllato tramite CRL clickando il link **Visualizza CRL** è possibile visualizzare la CRL scaricata per il controllo.

CONTROLLO CORRISPONDENZA

Una marca temporale di tipo TSR o TST non contiene al suo interno il documento originale dal quale è stata calcolata. Per controllare se una marca temporale corrisponde a un documento, è possibile utilizzare la sezione **Opzioni di Confronto** nella parte in basso alla schermata:

Clickare il pulsante , si aprirà una schermata per selezionare il documento:

Selezionare il documento con cui confrontare e premere il pulsante **Apri**:

Il documento con cui confrontare verrà caricato. A questo punto premere il pulsante confronta e visionare l'esito del confronto. In caso positivo:

In caso negativo:

3.6.3.3 Contenitori di marche temporali ASiC

Nel caso di contenitori di marcature temporali ASiC, verranno visualizzate le informazioni sulla tipologia del contenitore, ovvero una delle sue 2 combinazioni ASiC-E TST e ASiC-S TST:

Inoltre l'alberatura delle marcature presenterà alcune differenze, in quanto vengono mostrate anche le informazioni riguardo i vari gruppi di documenti:

Le informazioni sulle marche temporali sono le stesse già dettagliate nella sezione 3.6.3.2.

GRUPPO DOCUMENTI

Indica le informazioni sui documenti che sono protetti dalla relativa marca temporale. Aprendo i dettagli, è possibile visualizzare informazioni aggiuntive:

Aprendo il contenitore ASiC con un'applicazione in grado di gestire gli archivi Zip, ad esempio WinRAR, è possibile agire sui singoli documenti:

La cartella META-INF contiene tutti i file che servono a proteggere i vari gruppi di documenti, ovvero gli indici e le marcature temporali:

3.7 Operazioni di Decifra

L'applicazione Kit di Firma è in grado di decifrare documenti nel formato **PKCS#7 Enveloped Data** o **CMS Enveloped Data**.

Per eseguire un'operazione di decifra, è necessario prima di tutto caricare il documento in memoria. Premere il seguente tasto dalla toolbar:

Apparirà la seguente schermata:

Sulla parte sinistra, premere il tasto a**pri nuovo file**. Apparirà una schermata per la scelta del documento:

Selezionare il documento desiderato e premere il tasto **Apri** (o **Open**). Il documento verrà caricato in memoria e l'applicazione inizierà il processo di decifra (se la chiave privata è immagazzinata sulla smart card, verrà richiesto il PIN della carta). Se si possiede la chiave privata necessaria a decifrare il documento, la decifra avrà successo e apparirà la seguente schermata:

Dopo aver premuto il tasto **ok**, verrà mostrato l'esito della decifra:

I certificati destinatari della cifra di cui non si possiede la chiave privata vengono mostrati in rosso come **Certificato Sconosciuto**, gli altri invece normalmente. A questo punto se si volesse visualizzare il documento cifrato, clickare sul link **Visualizza File** sul lato sinistro della finestra. Se invece si vuole estrarre il documento cifrato e salvarlo su disco, premere il pulsante **salva decifrato** sul lato sinistro della finestra: il documento verrà salvato nella stessa cartella del documento cifrato. Se invece si vuole specificare un nome e un percorso, fare click su **salva decifrato come**....

Se invece non si possiede la chiave privata necessaria a decifrare il documento, la decifra non avrà successo e apparirà la seguente schermata:

Dopo aver premuto il tasto **ok**, verrà mostrato l'esito della decifra:

Tutti i certificati destinatari della cifra di cui non si possiede la chiave privata vengono mostrati in rosso come **Certificato Sconosciuto**.

3.8 Operazioni di anteprima del documento

Durante le operazioni di firma, verifica, cifra, decifra e marcatura temporale, è possibile visualizzare un'anteprima del documento che si sta gestendo nella relativa fase.

A seconda dell'operazione che si sta eseguendo, l'anteprima del documento è visualizzabile da un link posizionato sulla schermata dell'applicazione:

FIRMA DI UN DOCUMENTO

Una volta caricato il documento da firmare, tramite il link **Visualizza file** in alto a sinistra:

FIRMA DI PIÙ DOCUMENTI

Una volta caricati i documenti da firmare, tramite il link **Visualizza file** in corrispondenza del singolo documento nella lista:

MARCATURA TEMPORALE DI UN DOCUMENTO

Una volta caricato il documento da marcare, tramite il link **Visualizza file** in alto a sinistra:

CIFRA DI UNO O PIÙ DOCUMENTI

Una volta caricato uno o più documenti da cifrare, tramite il link **Visualizza file** in corrispondenza del singolo documento nella lista:

DECIFRA DI UN P7M DI CIFRA

Una volta decifrato con successo un P7M di cifra, tramite il link **Visualizza file** in alto a sinistra:

VERIFICA DI UN DOCUMENTO FIRMATO (CADES E XADES) O MARCATO (TSD)

Una volta verificato con successo un documento firmato, tramite il link **Visualizza file** in alto a sinistra:

VERIFICA DI UN DOCUMENTO FIRMATO PADES

Una volta verificato con successo un documento firmato in PAdES, tramite il link **Visualizza documento completo** in alto a sinistra, oppure tramite il link **Visualizza revisione** in corrispondenza della singola firma a destra:

Nella visualizzazione del report delle revisioni, facendo click sul nome della revisione (ad es. Revisione 1 (Signature1)):

3.8.1 Anteprima di documenti generici

A prescindere dall'operazione che si sta eseguendo, all'attivazione della visualizzazione dell'anteprima, verrà visualizzata una finestra simile alla seguente (un PDF nell'esempio):

A seconda se sul computer è installata l'applicazione associata all'estensione del documento, questo verrà visualizzato all'interno della finestra stessa, ma potranno capitare casi in cui non sia possibile visualizzarli in questa modalità ed apparirà una finestra simile:

Facendo click su **Apri** (**Open**) verrà aperto il documento con l'applicazione associata, ad esempio in Word:

E la finestra di anteprima mostrerà un messaggio simile al seguente, di cui non ci si deve preoccupare:

Nel caso apparisse la finestra precedente e non sia stato possibile visualizzare l'anteprima, è sempre possibile provare ad aprire il documento con l'applicazione associata tramite il link **qui** nella parte superiore della finestra:

3.8.2 Anteprima di documenti testuali

Nel caso di visualizzazione di documenti testuali, questi verranno visualizzati come semplice testo nella finestra:

I documenti con le seguenti estensioni saranno visualizzati sempre come testo: ".xml", ".txt", ".log", ".cnf", ".conf", ".cfg", ".config", ".asc", ".css", ".dtd", ".cs", ".vb", ".h", ".cpp", ".c", ".hpp", ".xsl", ".xslt", ".xsd".

3.8.3 Anteprima di documenti XML e XAdES

Nel caso particolare dei documenti XML e XAdES, se questi sono accompagnati da un documento di stile (XSL o XSLT), l'applicazione permette in automatico di applicare il foglio di stile e visualizzare a video il documento trasformato (solitamente in HTML).

FOGLIO DI STILE RECUPERABILE NEL PERCORSO INDICATO NELL'XML/XADES

Nell'esempio seguente un documento firmato XAdES con indicato un foglio di stile e il foglio di stile è presente nel percorso:

Nel caso invece si volesse visualizzare la versione testuale dell'XML, è possibile farlo facendo click sull'apposito link nella parte in alto della finestra:

FOGLIO DI STILE NON RECUPERABILE DAL PERCORSO INDICATO

Se il foglio di stile non è presente nello stesso percorso indicato nel documento XML/XAdES, allora verrà mostrato un messaggio di errore simile al seguente:

- Facendo click su **SI**, sarà possibile indicare il foglio di stile se si dispone di esso sul proprio PC:

Selezionando il foglio di stile dal percorso locale e facendo click su Apri (Open), in caso di successo si aprirà l'anteprima del documento XML trasformata, altrimenti la visualizzazione testuale.

- Se invece si seleziona **NO**, l'XML/XAdES verrà mostrato in formato testuale.

DOCUMENTO XML/XADES SENZA INDICATO IL FOGLIO DI STILE

Nel caso il documento non presenti l'indicazione del foglio di stile, questo verrà visualizzato normalmente in formato testuale:

Se però si dispone del foglio di stile per la visualizzazione, è possibile applicarlo tramite l'apposito link nella parte superiore della finestra:

Si prosegue quindi come indicato in precedenza.

3.9 Certification Authority Accreditate

L'applicazione Kit di Firma è in grado di verificare se i certificati utilizzati per apporre le firme, sono stati rilasciati da una Certification Authority (CA) accreditata presso un ente che gestisce il processo di certificazione delle CA stesse (ad esempio in Italia AgID, ex DigitPA, ex CNIPA). Per poter utilizzare questa funzionalità è necessario tenere aggiornata periodicamente tale lista all'interno dell'applicazione. La lista delle CA accreditate è solitamente disponibile su Internet ed è firmata con un certificato dell'ente che la emette. In più, per favorire l'interoperabilità tra i paesi membri della comunità europea, a livello centrale la comunità europea emette una lista contenente l'elenco di tutti gli stati membri e la relativa organizzazione che emette a sua volta la propria lista delle CA accreditate. L'applicazione Kit di Firma utilizza quindi la lista europea per poi scaricare la lista dell'Italia.

L'applicazione Kit di Firma visualizza lo stato di aggiornamento di tale lista nella schermata principale, in basso:

Nel caso la lista fosse in procinto di scadere (7 giorni prima della scadenza), apparirà un messaggio simile al seguente:

Nel caso la lista fosse scaduta, apparirà un messaggio simile al seguente:

Nel caso invece la lista non fosse disponibile in Kit di Firma, apparirà un messaggio simile al seguente:

In questo caso si consiglia di aggiornare la lista appena possibile.

Come detto in precedenza, comunque l'applicazione Kit di Firma esegue il controllo della scadenza/aggiornamento della lista a ogni avvio e nel caso fosse possibile, scarica la versione aggiornata della lista del paese predefinito in automatico.

3.9.1 Aggiornamento manuale della lista

Per aggiornare la lista delle CA Accreditate manualmente, dalla piccola toolbar in alto a destra:

Clickare sulla voce **CA ACCREDITATE**, apparirà la seguente schermata:

Assicurarsi di avere una connessione a Internet e premere il pulsante **aggiorna la lista europea** e attendere che la lista sia scaricata da Internet. Al termine sulla sinistra apparirà la lista dei paesi membri:

Premere il pulsante **certificato lista europea** e controllare che il certificato di firma corrisponda a quello solitamente usato della comunità europea:

Premere il tasto **chiudi** per tornare alla schermata precedente e selezionare lo stato del quale scaricare la lista (Italia è il valore predefinito):

Premere il tasto per procedere con il download della lista nazionale, se tutto va bene, la lista delle CA dello stato apparirà nella parte destra della finestra:

L'applicazione Kit di Firma controlla automaticamente che il certificato che ha firmato la lista nazionale corrisponda con quello dichiarato nella lista europea, comunque, se si vuole controllare, tramite il pulsante **certificato lista nazionale** è possibile visualizzare il certificato di chi ha firmato la lista nazionale:

A questo punto è possibile utilizzare la lista aggiornata premere il tasto in alto a sinistra oppure la voce **HOME** dalla toolbar in alto a destra per tornare alla schermata precedente.

Se si volesse scaricare anche le CA Accreditate di un altro paese, selezionare il paese nella lista a destra e premere il pulsante come fatto per l'Italia. Il procedimento è il medesimo.

3.9.2 Visualizzazione della lista

Per visualizzare la lista delle CA Accreditate, dalla piccola toolbar in alto a destra:

Selezionare la voce **CA ACCREDITATE**, comparirà una lista simile alla seguente:

Le CA sono raggruppate per Trust Service Provider (TSP) corrispondente (nell'esempio **Ministero della Difesa**). Per ogni CA viene anche mostrato il tipo di certificato di CA e la sua storia.

Le CA indicate con il nome in rosso corrispondono a certificati di CA cessate, quelle con la data di scadenza in rosso corrispondono a certificati di CA scaduti. Per visualizzare il certificato della CA, selezionare il certificato e premere il tasto **certificato certification authority**:

Nel caso invece in cui si volesse visualizzare il certificato dell'ente che gestisce la lista, premere il pulsante **certificato lista nazionale**:

Se si vuole visualizzare le CA Accreditate di un altro paese e si è già provveduto a scaricarle, cambiare il paese nella lista a sinistra, apparirà la lista delle CA corrispondenti nella parte destra.

3.10 Configurazione

Per configurare l'applicazione Kit di Firma, dalla piccola toolbar in alto a destra:

Clickare sulla voce **SETTAGGI**, apparirà la seguente schermata:

3.10.1 Servizi

Per cambiare le impostazioni relative ai servizi online usati dall'applicazione, posizionarsi nella sezione **SERVIZI**:

Nella sezione **Server LDAP**, è possibile configurare i servizi LDAP da utilizzare durante la ricerca dei certificati per le operazioni di cifra.

Per aggiungere un nuovo server, inserire il **Nome** e la **URL** complete nella sezione **Aggiungi Server LDAP** e clickare il pulsante ⊕. Il nuovo server verrà aggiunto nella lista sopra. Per cancellare invece un server, selezionarlo dall'apposita lista e premere il pulsante ⊖. Il server verrà rimosso dalla lista. Se invece si volesse variare le informazioni di un server, eseguire doppio click sull'elemento nella lista, variare le informazioni in **Nome** e **URL** e premere il pulsante ⊕. Le informazioni aggiornate verranno riportate nella lista.

Nella sezione **Server TSU**, è possibile configurare i servizi TSU da utilizzare durante le operazioni di firma e marcatura temporale.

Per aggiungere un nuovo server, inserire il **Nome** e la **URL** complete nella sezione **Aggiungi Server TSU** e clickare il pulsante ⊕. Il nuovo server verrà aggiunto nella lista sopra. Per cancellare invece un server, selezionarlo dall'apposita lista e premere il pulsante ⊖. Il server verrà rimosso dalla lista. Se invece si volesse variare le informazioni di un server, eseguire doppio click sull'elemento nella lista, variare le informazioni in **Nome** e **URL** e premere il pulsante ⊕. Le informazioni aggiornate verranno riportate nella lista. Per cambiare l'ordine di preferenza dei servizi, selezionare l'elemento nella lista e premere il pulsante ⌃ per spostarlo in alto o ⌄ per spostarlo in basso.

Al termine delle variazioni, premere il pulsante **salva modifiche**.

3.10.2 Avanzate

Per cambiare le impostazioni avanzate, posizionarsi nella sezione **AVANZATE**:

Nella sezione **Cartella di Lavoro** è possibile scegliere dove verranno salvati i documenti firmati, marcati o cifrati dall'applicazione Kit di Firma:

- **Cartella Documenti**: Tutti i documenti prodotti saranno salvati nella cartella *Documenti* di Windows
- **Cartella del Documento Originale**: Tutti i documenti prodotti saranno salvati nella stessa cartella del documento originale. Ad esempio, se si firma un documento Word nella cartella C:\Lavoro\, il documento firmato sarà salvato nella cartella del documento Word, ovvero C:\Lavoro\.
- **Richiedi Sempre**: Ogni volta che l'applicazione produrrà un nuovo documento, verrà chiesto all'utente dove salvarlo.
- **Cartella Specifica**: Tutti i documenti prodotti saranno salvati sempre in una cartella specificata tramite l'apposita opzione:

Premere il tasto a destra del percorso visualizzato, apparirà una finestra di scelta:

Scegliere la cartella desiderata e premere il tasto **OK**.

Nella sezione **Documenti crittografici**, è possibile disattivare l'aggiunta del suffisso "_Firmato" ai file firmati PAdES e XAdES (**Non aggiungere il suffisso '_Firmato' al nome dei documenti firmati**)

Nella sezione **Verifica Firmatari**, è possibile indicare se si desidera mantenere in memoria una cache delle CRL scaricate ed elaborate (**Mantieni in memoria la cache delle CRL**). La cache sarà svuotata alla chiusura dell'applicazione.

È possibile infine scegliere il paese della comunità europea predefinito (**Paese Predefinito**). Tale paese sarà quello per il quale l'applicazione verificherà automaticamente a ogni avvio la lista delle CA Accreditate ed eseguirà il download. Si sconsiglia di cambiare il valore Italia.

Al termine delle variazioni, premere il pulsante **salva modifiche**.

3.10.3 Proxy

L'applicazione è in grado di utilizzare in maniera predefinita le impostazioni del proxy già configurate per il browser Internet Explorer e quindi per Windows (Panello di Controllo, Opzioni Internet, Connessioni, Impostazioni LAN). Nel caso in cui si voglia impostare comunque un proxy differente per il collegamento a Internet, è necessario impostare le opzioni nella sezione corrispondente. Posizionarsi nella sezione **PROXY**:

Selezionare la voce **Usa i seguenti settaggi**:

Inserire le informazioni preferite e salvare le impostazioni con il pulsante **salva modifiche**.

3.10.4 PAdES

Per cambiare le impostazioni relative al formato PAdES, posizionarsi nella sezione **PADES**:

Nella sezione **Impostazioni PAdES predefinite**, è possibile inserire la configurazione che si desidera utilizzare in automatico a ogni firma PAdES:

- Ruolo/Qualifica
- Luogo
- Motivazione
- Larghezza riquadro firma
- Posizione riquadro firma
- Posizione all'interno della pagina
- Mostra riquadro firma nel documento
- Mostra l'immagine nel riquadro firma

Per quanto riguarda la configurazione della **Larghezza riquadro firma** c'è la possibilità di personalizzare la larghezza del box in base alle proprie esigenze scegliendo tra quattro possibili dimensioni predefinite:

- Standard
- Media
- Grande
- Massima

Tale impostazione è modificabile solamente nei settaggi PADES; tutte le altre, invece, anche durante l'operazione di firma PAdES.

Per quanto riguarda la configurazione dell'immagine nella firma, si utilizza la sottosezione **Immagine nel riquadro firma**:

L'immagine inclusa nel riquadro ha un aspetto rettangolare in modo da mostrare adeguatamente le firme autografe, si consiglia quindi di preparare una immagine in formato rettangolare in cui la larghezza è tre volte l'altezza. In ogni caso, l'immagine verrà scalata automaticamente alle dimensioni di 210x70 pixel.

Per evitare incongruenze durante le operazioni di firma, l'immagine della firma verrà legata ai dati del certificato usato per la firma digitale, in particolare con il Codice Fiscale presente nel proprio certificato di firma digitale.

Per caricare l'immagine quindi, inserire la smart card nel lettore, attendere che i certificati siano letti completamente da essa e clickare sul pulsante **carica**[9].

Apparirà un avviso che spiega quanto appena detto:

Fare click su **OK**. Verrà mostrata una finestra in cui scegliere il proprio certificato di firma digitale:

[9] L'immagine viene salvata all'interno delle impostazioni utente in maniera cifrata, utilizzando un meccanismo del sistema operativo che consente di decifrarla solo all'utente che l'ha cifrata sulla stessa postazione. Se si cambia utente o postazione, è necessario ricaricare l'immagine nell'applicazione.

Se il certificato mostrato è il proprio certificato di firma digitale, fare click su **OK**, altrimenti clickare su **Altre opzioni** (**More choices**) e selezionarlo quindi dalla lista che appare. Fare click su **OK** quando terminato.

Apparirà quindi una finestra per scegliere una immagine (in formato PNG, JPEG o BMP):

Selezionare l'immagine desiderata e clickare su **Apri** (**Open**). La finestra dei settaggi verrà aggiornata mostrando l'anteprima dell'immagine scelta:

Se invece si vuole rimuovere l'immagine, utilizzare il pulsante **elimina**. Se desiderato, selezionare l'opzione **Mostra l'immagine nel riquadro firma** in modo da non dover selezionare questa opzione ogni volta durante le operazioni di firma.

Oltre all'immagine di una firma autografa è possibile inserire qualunque tipo di immagine. Se si intende inserire ad esempio un logo, si consiglia di preparare un logo all'interno di una immagine rettangolare. Aluni esempi di seguito.

Un logo con un testo a lato:

Solo un logo a destra e uno spazio bianco a sinistra:

L'immagine viene visualizzata nel riquadro di firma allineata in basso a destra, per ottenere i risultati migliori, utilizzare quindi la funzione per disegnare il riquadro di firma in modo da ottenere risultati di questo tipo:

	Con firma autografa: Con il primo logo e note:
	Con firma autografa senza note: Con il primo logo senza note: Con il secondo logo senza note:

Se invece si decide di usare la posizione predefinita di uno degli angoli, con una immagine il riquadro apparirà in un modo simile al seguente (ad esempio in alto a sinistra):

Al termine delle variazioni, premere il pulsante **salva modifiche**.

3.10.5 Aspetto

Per cambiare le impostazioni di visualizzazione dell'applicazione, posizionarsi nella sezione **ASPETTO**:

Scegliere le impostazioni preferite, l'applicazione applicherà in tempo reale le variazioni.

3.10.6 Impostazioni Predefinite

Nel caso in cui fossero state cambiate per sbaglio delle impostazioni di cui non si ricorda più il valore iniziale e si volesse tornare alle impostazioni predefinite, posizionarsi nella sezione **IMPOSTAZIONI PREDEFINITE**:

Premere il tasto **ripristina impostazioni predefinite**, apparirà una schermata simile alla seguente:

3.10.7 Assistenza

Per ottenere informazioni su come contattare il supporto sull'applicazione, posizionarsi nella sezione **ASSISTENZA**:

Clickando sul link alla pagina web si aprirà automaticamente il browser sulla pagina indicata. Clickando sull'email si aprirà automaticamente l'applicazione predefinita di e-mail con una email di base già pronta:

3.11 Informazioni sugli aggiornamenti

L'applicazione Kit di Firma è in grado come detto di aggiornare sé stessa nel momento in cui viene rilasciato un aggiornamento. Solitamente l'aggiornamento avviene in maniera automatica senza l'intervento dell'utente. In più, Kit di Firma è in grado anche di controllare la disponibilità di aggiornamenti su applicazioni extra comunque richieste (ad esempio le Smart Card API).

All'interno dell'applicazione, la disponibilità di aggiornamenti, o la mancanza del software vengono mostrati nella barra di stato dell'applicazione. A seconda dei vari casi, verranno mostrati messaggi differenti.

Nel caso un'applicazione richiesta non sia installata, verrà mostrato il seguente messaggio:

Clickando sul link nel messaggio, si aprirà automaticamente il browser Internet direttamente sulla pagina dove sono riportate le istruzioni per eseguire il download e l'installazione del software indicato.

Nel caso invece di disponibilità di un aggiornamento di un'applicazione richiesta, verrà mostrato il seguente messaggio:

Clickando sul link nel messaggio, si aprirà automaticamente il browser Internet direttamente sulla pagina dove sono riportate le istruzioni per eseguire il download e l'aggiornamento del software indicato.

Nel caso di presenza di aggiornamenti dell'applicazione Kit di Firma stesso, verrà mostrato il seguente messaggio:

In questo caso però, l'aggiornamento verrà eseguito automaticamente al prossimo avvio dell'applicazione.

3.12 Gestione della smart card

La sezione di gestione della smart card permette di attivare la carta per l'utilizzo dei certificati a seconda del tipo di carta e chip. In particolare:

- Nel caso della CMD-2/Modello ATe con chip ST-Incard (seriali con iniziali MMDA, MMDB, MMDC e MMDM), la carta viene consegnata all'utente con il solo certificato di Firma Qualificata e relativo PIN Firma bloccato. È possibile quindi usare la sezione per sbloccare la funzione di firma sulla carta, visualizzare le informazioni sulla carta e sul certificato di Firma Qualificata.

- Nel caso della CMD-2/Modello ATe con chip Oberthur o IDEMIA (seriali con iniziali MMDD e successivi, ad esclusione di MMDM), la carta viene consegnata all'utente con tutte le chiavi dei certificati bloccate (ovvero Autenticazione CNS, Firma Qualificata, Cifra/Decifra) e PIN Firma bloccato. È possibile quindi usare la sezione per sbloccare le chiavi private e il PIN Firma, visualizzare le informazioni sulla carta e sul certificato di Firma Qualificata. Se non si procede con l'attivazione, non sarà possibile quindi usare la carta né per accedere ai siti web, né firmare, nè decifrare documenti.

In entrambi i casi, tutte le successive operazioni riguardanti la gestione del PIN Carta e del PIN Firma vanno eseguite con l'applicazione Smart Card Manager del pacchetto Smart Card API.

Per accedere alla sezione di gestione della carta, dalla piccola toolbar in alto a destra:

Clickare sulla voce **SMARTCARD**, apparirà la seguente schermata:

L'applicazione rimane in attesa che la carta venga inserita in uno dei lettori di smart card del proprio PC e che l'utente clicki il tasto **procedi** per poi mostrare le funzionalità disponibili. Prima di premere il tasto procedi, attendere che la carta sia stata completamente letta dal software di monitoraggio della smart card (Smart Card Monitor , per evitare conflitti di accesso alla smart card stessa).

3.12.1 Informazioni sulla carta

Dopo aver clickato il tasto **procedi**, appariranno le informazioni sulla carta a seconda del tipo.

Nel caso di CMD-2/Modello ATe con chip ST-Incard, apparirà una schermata simile alla seguente:

Nel caso di CMD-2/Modello ATe con chip Oberthur o IDEMIA, apparirà una schermata simile alla seguente se la carta non è stata mai attivata:

Oppure una schermata simile alla seguente se la carta è stata già attivata in precedenza:

Nel caso di carta sconosciuta, apparirà una schermata simile alla seguente.

Tutte le operazioni seguenti vanno eseguite con la CMD inserita nel lettore di smartcard. Tutte le operazioni vengono eseguite scegliendo la sezione apposita nel riquadro sulla sinistra.

Facendo click su **leggi certificati** invece, verranno lette le informazioni sui certificati a bordo della carta e a seconda dei certificati presenti sulla carta, verranno mostrati in basso dei pulsanti per visualizzarne i dettagli:

Facendo click su uno dei tasti su indicati, verranno mostrati i dettagli sul certificato corrispondente a bordo della carta stessa:

3.12.2 Attivazione della Carta

Per attivare la carta CMD-2/Modello ATe, è necessario utilizzare il *PIN di Firma* della propria CMD-2/Modello ATe. Posizionarsi nella sezione **ATTIVA**:

Inserire il PIN di Firma (**Inserire PIN di Firma**) e premere il tasto **attiva**. Se l'operazione va a buon fine, apparirà un messaggio di conferma:

A questo punto si consiglia di cambiare il PIN Firma tramite l'applicazione Smart Card Manager del pacchetto Smart Card API. Prima di utilizzare la carta, sfilare e reinserire la carta nel lettore di smart card e attendere che la carta sia stata completamente letta dal software di monitoraggio della smart card (Smart Card Monitor , per fare in modo che la carta sia letta correttamente dopo lo sblocco).

Da questo momento sarà possibile usare la Firma Qualificata con le carte con chip ST-Incard, mentre con le carte con chip Oberthur sarà possibile usare i 3 certificati (Autenticazione CNS, Firma Qualificata, Cifra/Decifra).

Se l'operazione non va a buon fine, invece del messaggio di conferma, appare un messaggio del genere:

Prestare attenzione all'inserimento del PIN di Firma: nel caso fosse inserito in modo errato per più di 3 volte, nel caso delle carte con chip ST-Incard la Firma Digitale non sarà più sbloccabile e sarà necessario riemettere una nuova carta per poter firmare digitalmente. Nel caso di carte con chip Oberthur invece, tutti i certificati non saranno più sbloccabili e sarà necessario riemettere una nuova carta per poter autenticarsi, firmare digitalmente e decifrare documenti.

3.12.3 Gestione dei PIN della carta

In questo gruppo di sezioni è possibile gestire i PIN Carta e PIN Firma della propria carta. Per gestire il PIN Firma della carta, è necessario avere installata la versione 3.84 o successiva delle Smart Card API (anche dette CMDAPI). Nel caso di carte Oberthur e IDEMIA, le funzioni di gestione del PIN appariranno solo nel caso la carta sia stata attivata la prima volta.

Per ridurre gli errori, in ogni box di inserimento è presente l'icona per visualizzare il valore immesso prima di usarlo.

3.12.3.1 Verifica PIN Carta

In questa sezione è possibile verificare il PIN Carta della propria carta.

Prestare attenzione a:

- Non sbagliare il PIN Carta per 3 volte di seguito, in tal caso sarà necessario prima sbloccare il PIN Carta tramite apposita sezione
- Non utilizzare questa sezione prima di aver attivato la prima volta la propria carta.

Inserire il **PIN Carta** attuale e fare click sul tasto **procedi** per eseguire l'operazione.

3.12.3.2 Cambio PIN Carta

In questa sezione è possibile impostare un nuovo PIN Carta tramite il PIN Carta attuale della propria carta.

Prestare attenzione a:

- Non sbagliare il PIN Carta per 3 volte di seguito, in tal caso sarà necessario prima sbloccare il PIN Carta tramite apposita sezione
- Non utilizare questa sezione prima di aver attivato la prima volta la propria carta.

Inserire il **PIN Carta** attuale, il **Nuovo PIN Carta** (2 volte per verifica) e fare click sul tasto **procedi** per eseguire l'operazione.

3.12.3.3 Sblocco PIN Carta

In questa sezione è possibile sbloccare il PIN Carta tramite il PUK Carta della propria carta.

Prestare attenzione a:
- Non sbagliare il PUK Carta per 10 volte di seguito, in tal caso la carta diventerà inutilizzabile.
- Non utilizare questa sezione prima di aver attivato la prima volta la propria carta.

Inserire il **PUK Carta**, il **Nuovo PIN Carta** (2 volte per verifica) e fare click sul tasto **procedi** per eseguire l'operazione. E' comunque possibile riusare il PIN Carta precedente.

3.12.3.4 Verifica PUK Carta

In questa sezione è possibile verificare il PUK Carta della propria carta.

Prestare attenzione a:
- Non sbagliare il PUK Carta per 10 volte di seguito, in tal caso la carta diventerà inutilizzabile.
- Non utilizare questa sezione prima di aver attivato la prima volta la propria carta.

Inserire il **PUK Carta** e fare click sul tasto **procedi** per eseguire l'operazione.

3.12.3.5 Cambio PIN Firma

In questa sezione è possibile impostare un nuovo PIN Firma tramite il PIN Firma attuale della propria carta.

Prestare attenzione a:

- Non sbagliare il PIN Carta per 3 volte di seguito, in tal caso sarà necessario prima sbloccare il PIN Carta tramite apposita sezione
- Non sbagliare il PIN Firma attuale per 3 volte di seguito, in tal caso sarà necessario prima sbloccare il PIN Firma tramite apposita sezione.
- Non utilizzare questa sezione prima di aver attivato la prima volta la propria carta.

Inserire il **PIN Carta**, **PIN Firma** attuale, il **Nuovo PIN Firma** (2 volte per verifica) e fare click sul tasto **procedi** per eseguire l'operazione.

3.12.3.6 Sblocco PIN Firma

In questa sezione è possibile sbloccare il PIN Firma tramite il PUK Firma della propria carta.

Prestare attenzione a:

- Non sbagliare il PIN Carta per 3 volte di seguito, in tal caso sarà necessario prima sbloccare il PIN Carta tramite apposita sezione
- Non sbagliare il PUK Firma per 10 volte di seguito, in tal caso la carta diventerà inutilizzabile.
- Non utilizzare questa sezione prima di aver attivato la prima volta la propria carta.

Inserire il **PIN Carta**, **PUK Firma**, il **Nuovo PIN Firma** (2 volte per verifica) e fare click sul tasto **procedi** per eseguire l'operazione. E' comunque possibile riusare il PIN Firma precedente.

4 Ulteriori informazioni

4.1 Produrre documenti in formato PDF/A

Fino alla versione 4.4.0.0 dell'applicazione, era possibile convertire direttamente da Kit di Firma alcuni tipi di documenti in formato PDF/A utilizzando una stampante PDF opportunamente pilotata per produrre documenti in formato PDF/A. Per sopraggiunta obsolescenza di questo software di supporto, dalla versione 4.5.0.0 è stata rimossa questa funzionalità. Per questo motivo è l'utente di Kit di Firma che deve produrre documenti in formato PDF/A. In questa sezione, alcuni consigli su come procedere con gli strumenti più diffusi.

ACROBAT READER

Acrobat Reader indica se un PDF è in formato PDF/A mostrando un banner nella finestra di visualizzazione. È possibile quindi utilizzare questo strumento per capire se un PDF è già in formato PDF/A o no:

MICROSOFT WORD

Nel momento in cui si decide di convertire il proprio documento in formato PDF, sulla schermata di salvataggio:

Selezionare come formato il PDF tramite l'opzione **Save as type** (**Salva come**) e clickare il tasto **Options**... (**Opzioni**...):

Selezionare l'opzione **PDF/A compliant** (**Conforme a PDF/A**) in basso nella sezione **PDF options** (**Opzioni PDF**) e clickare su **OK**.

MICROSOFT EXCEL

Nel momento in cui si decide di convertire il proprio documento in formato PDF, sulla schermata di salvataggio:

Selezionare come formato il PDF tramite l'opzione **Save as type** (**Salva come**) e clickare il tasto **Options**... (**Opzioni**...):

Selezionare l'opzione **PDF/A compliant** (**Conforme a PDF/A**) in basso nella sezione **PDF options** (**Opzioni PDF**) e clickare su **OK**.

LIBREOFFICE

Qualunque tipo di documento si utilizzi (Write, Calc, Impress, ecc…), è possibile esportare in PDF il documento:

Dal menu **File**, **Export As**, **Export as PDF**…:

Selezionare **Archive PDF/A-1a (ISO 19005-1)** e clickare il tasto **Export**.

PDFCREATOR 3

Quando l'applicazione che si sta usando non supporta nativamente la conversione in PDF/A, è possibile convertire il documento in PDF/A utilizzando la stampa PDF. Procedere quindi con la stampa:

Selezionare la stampante **PDFCreator** e procedere con **Print** (**Stampa**):

Selezionare come profilo **PDF/A (conservazione a lungo termine)** e clickare su **Salva**.

4.2 Registrare una sessione di lavoro su Windows 7 e successivi

Nel caso si esegua Kit di Firma su un sistema operativo Microsoft Windows 7 e successivi, è consigliato l'utilizzo dello strumento **Problem Steps Recorder** (PSR) di Windows per la registrazione delle sessioni di lavoro.

Nel caso di un errore ricorrente attivare l'applicazione Problem Steps Recorder lanciando il comando **psr.exe** dal menu *Start*, *Esegui*, apparirà la seguente schermata:

Quando si è pronti per registrare, avviare la registrazione con **Start Record** ed eseguire tutti i passi con le applicazioni che poi portano al verificarsi dell'errore. Durante la registrazione, l'applicazione indicherà il tempo di registrazione a destra:

Quando si ritiene di aver terminato la registrazione, premere il pulsante **Stop Recording**. L'applicazione PSR chiederà di salvare la registrazione con un nome in un percorso a scelta. Indicare il

nome e il percorso e allegare il file ZIP prodotto ai file di log della segnalazione di errore. La registrazione contiene informazioni molto utili alla risoluzione del problema da parte del team di sviluppo e/o supporto.

4.3 Problemi noti

ACCESSO NEGATO A CARTELLE

Se al termine di un'operazione di firma, l'applicazione riporta un errore simile al seguente:

(in inglese: *Access Denied. Before opening files in this location, you must first add the web site to your trusted sites list, browse to the web site, and select the option to login automatically.*). È possibile che il percorso predefinito di salvataggio dei documenti firmati non sia accessibile all'utente corrente.

Soluzione: Nella sezione **Settaggi**, scegliere la sottosezione **Impostazioni Predefinite** e clickare il pulsante **ripristina impostazioni predefinite**.

ERRORE "IL FILE CONTIENE UN VIRUS O SOFTWARE POTENZIALMENTE INDESIDERATO"

Se durante l'utilizzo dell'applicazione, dovesse venir mostrato un messaggio di errore "il file contiene un virus o software potenzialmente indesiderato", la causa è dovuta al software di antivirus/antimalware installato sulla postazione, il quale ha in sospeso un aggiornamento delle definizioni o del software stesso.

Soluzione: Far completare l'aggiornamento e riavviare il PC.

ERRORE "LUNGHEZZA DELLA MATRICE…"

Se durante l'apertura di un documento firmato PAdES, appare l'errore *"Lunghezza della matrice di origine insufficiente. Controllare srcindex, la lunghezza e i limiti inferiori della matrice"*:

L'errore è dovuto al fatto che il documento PDF una volta firmato, è stato poi aperto e salvato con un applicativo che lo ha modificato salvandolo quindi in maniera compressa e, conseguentemente, cambiando le dimensioni del documento facendo perdere i riferimenti della firma.

Soluzione: Prestare attenzione nel momento in cui si apre il PDF nelle applicazioni di visualizzazioni, a non dare la conferma al salvataggio del documento. Per i documenti invece con questo problema, sono danneggiati e dovranno essere firmati nuovamente.

PERDITA DELL'ASSOCIAZIONE AI DOCUMENTI

In alcune situazioni in cui più di un'applicazioni di firma/verifica si associano automaticamente alle estensioni delle buste crittografiche (ad es .p7m, .asics, ecc…), l'applicazione Tool di Verifica potrebbe non essere più l'applicazione associata in modo predefinito alle varie estensioni, oppure non esistere alcuna associazione.

Soluzione: è possibile eseguire una semplice procedura:

Individuare un documento firmato (ad esempio un CAdES con estensione .p7m), tenendo premuto il tasto SHIFT della tastiera, clickare con il tasto destro del mouse sull'icona. Nel menu contestuale apparirà una voce **Apri con** (**Open with**):

Selezionare tale voce, si aprirà una nuova finestra con una lista di possibili applicazioni:

Nella lista, selezionare **Libreria di supporto per la distribuzione dell'applicazione ClickOnce** (**ClickOnce Application Deployment Support Library**) e attivare **Usa sempre il programma selezionato per aprire questo tipo di file** (**Always use this app to open .p7m files**) e premere il tasto **OK**. A questo punto l'associazione verrà ripristinata e sarà possibile nuovamente i file .p7m con l'azione del doppio-click.

Su sistemi operativi superiori a Windows 7, ad esempio Windows 10, la procedura è simile ma cambiano le schermate:

temp_AUT...
How do you want to open this file?
Keep using this app
ClickOnce Application Deployment Support Library
New
Other options
Look for an app in the Store
More apps
Always use this app to open .p7m files
OK