



DikeIC 2.0
Manuale utente

Δike

Sommario

1	Introduzione al documento	3
1.1	Novità introdotte rispetto alla precedente emissione	3
1.2	Scopo e campo di applicazione del documento	3
2	Installazione e primo utilizzo DikeIC	5
2.1	Installazione Windows	5
2.2	Installazione Ubuntu Linux	8
2.3	Installazione MAC	8
2.4	Aggiornamento	9
3	Guida alla firma dei documenti con DikeIC.....	10
3.1	Cosa occorre	10
3.2	Firma di un documento singolo	10
3.2.1	Impostazioni e firma P7M.....	11
3.2.2	Impostazioni e firma PDF	14
3.2.3	Impostazioni e firma XML.....	17
3.3	Firma di più documenti.....	18
3.3.1	Impostazioni per firma P7M.....	18
3.3.2	Impostazioni per firma PDF	19
3.3.3	Impostazioni per firma XML.....	20
3.3.4	Firma multipla	21
3.3.5	Firma remota: configurazione ed uso.....	22
4	Marca temporale.....	25
4.1	Marcatura di documenti	25
4.2	Associazione marche a documenti	27
4.3	Separazione marche da documenti	29
5	Verifica	31
6	Controfirma	36
7	Come cifrare e decifrare un file	38
7.1	Cifrare un file	38
7.2	Decifrare un file	40

1 Introduzione al documento

1.1 Novità introdotte rispetto alla precedente emissione

Versione/Release n° :	1.1	Data Versione/Release :	30/03/2017
Descrizione modifiche:	Correzioni tipografiche		
Motivazioni :			

1.2 Scopo e campo di applicazione del documento

La firma digitale è la possibilità, legalmente riconosciuta e normata, di firmare un documento digitale. Così come la firma autografa sul documento cartaceo, la firma digitale può essere apposta su un documento informatico.

La tecnologia alla base della firma digitale garantisce, inoltre, che il documento firmato non possa essere successivamente modificato senza invalidare la firma stessa, e consente di associare al documento una data ed un'ora certe, attraverso il meccanismo della marca temporale.

DikeIC è il software InfoCert che consente le seguenti funzionalità:

- per uno o più file:
 - la firma digitale p7m (formato CADES), che può essere apposta in modalità “attached”, cioè integrata nel file cui si riferisce, o “detached”, cioè solo associata dal file firmato cui si riferisce;
 - la firma digitale pdf (formato PADES), per i file in formato pdf;
 - la marcatura temporale, che può essere apposta in modalità “attached”, cioè integrata nel file cui si riferisce, o “detached”, cioè solo associata dal file firmato cui si riferisce;
 - la verifica della firma e/o delle marche temporali;
 - la cifratura e la decifratura
- per singolo file:
 - la controfirma (di validazione).

Sono inoltre disponibili le seguenti UTILITY :

- impostazione dei parametri per la Marcatura Temporale;
- configurazione del proxy http;
- verifica della disponibilità delle marche temporali;
- separazione di marche temporali da documenti MIME;
- associazione di una marca temporale a un documento.

Ogni funzionalità può essere attivata cliccando sulla corrispondente icona del menu.

Ogni file, una volta firmato, se non già presente, assumerà l'estensione:

- .p7m : in caso di firma attached
- .p7s : in caso di firma detached

Per quanto riguarda la funzione di marcatura, un file una volta marcato assumerà l'ulteriore estensione:

- .tsd oppure .m7m (a seconda del formato richiesto) se la marcatura è di tipo attached
- .tsr in caso di marcatura detached.

2 Installazione e primo utilizzo DikeIC

Per installare DikeIC, scaricare il software ed il suo manuale di installazione dal sito www.card.infocamere.it

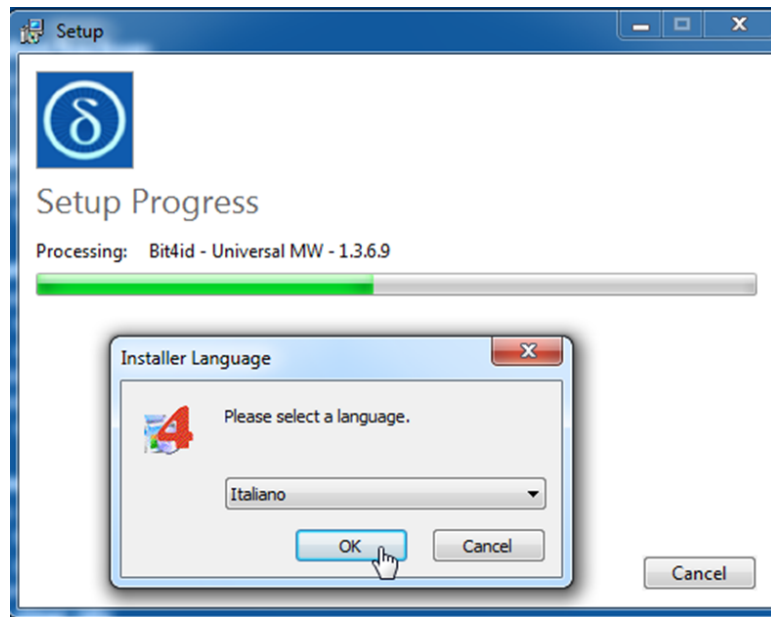
Per utilizzare un dispositivo Smart card per apporre firme digitali occorre inoltre dotarsi di un apposito lettore USB.

2.1 Installazione Windows

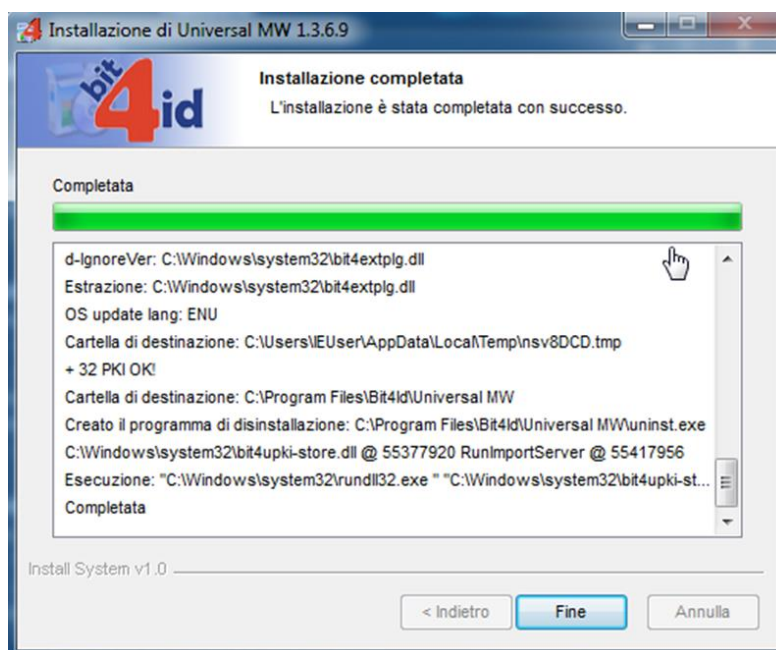
Scaricare DikeIC dal sito www.card.infocamere.it ed eseguirlo con un doppio click. Prendere visione ed accettare la licenza d'uso e selezionare "Installa".



Il programma eseguirà in sequenza l'installazione sia del software driver necessario alla gestione dei dispositivi emessi dalle Camere di Commercio Industria Artigianato e Agricoltura nazionali sia l'installazione del software DikeIC.

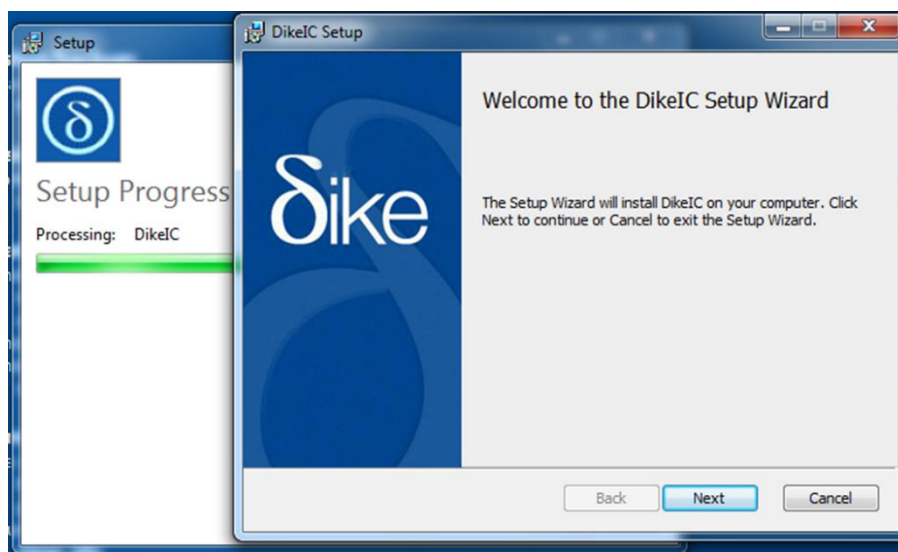


Cliccare su “OK” per procedere all’installazione del driver.



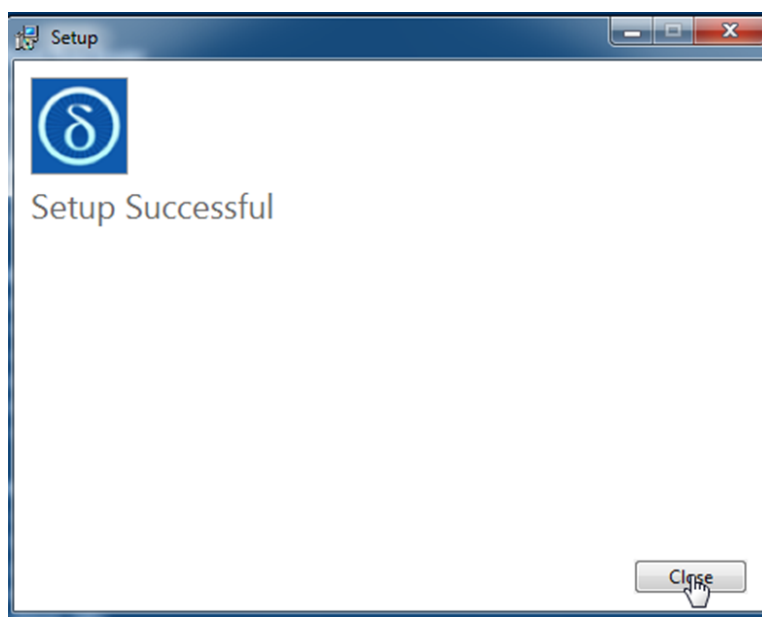
Cliccare su “Fine” per terminare l’installazione del driver.

Verrà avviata automaticamente l’installazione di DikeIC.



Cliccare “Next” per procedere.

Completata l’installazione di DikeIC, chiudere la finestra del Setup cliccando su “Close”.

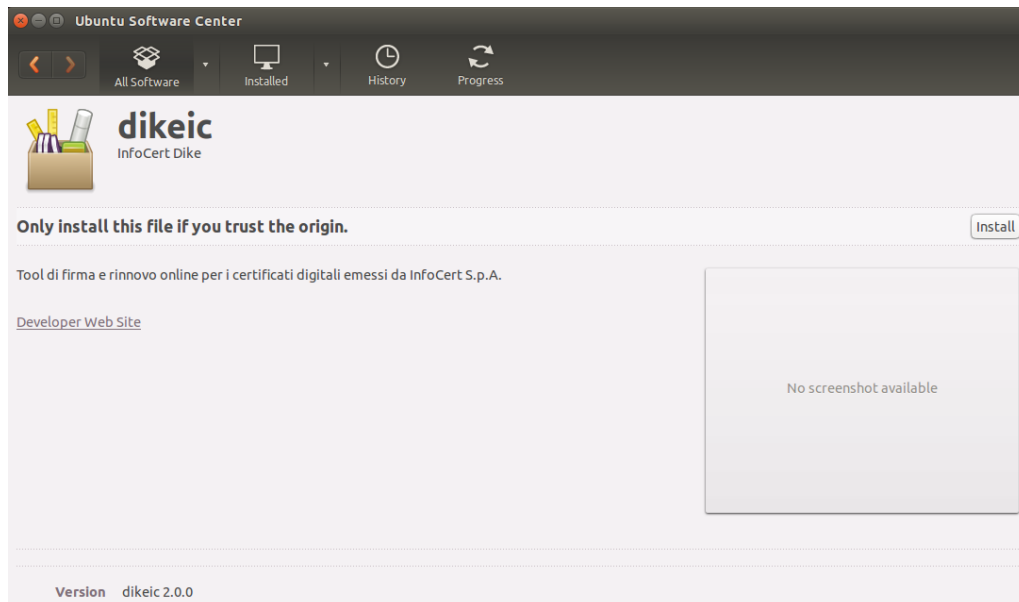


Sul Desktop è ora presente l’icona per avviare di DikeIC



2.2 Installazione Ubuntu Linux

Una volta scaricato il file .deb per la propria piattaforma, con doppio click si aprirà la finestra di installazione di Ubuntu Software Center. Un click su “Installa” avvia il processo di installazione.



Inserire le credenziali dell’account amministratore quando richiesto.

Al termine dell’installazione è possibile lanciare il software cercando “DikeIC” tra le applicazioni installate nel PC o presenti sulla dockbar.



2.3 Installazione MAC

Una volta scaricato il file .dmg per la propria piattaforma, con doppio click si aprirà la finestra che inviterà l’utente a trascinare l’icona di **DikeIC** sulla cartella **Applicazioni**: l’operazione può essere fatta direttamente nella stessa finestra, selezionando col cursore del mouse l’icona del software, trascinandola e rilasciandola sopra l’immagine della cartella dedicata alle applicazioni.



Una volta fatta quest'operazione, si aprirà la cartella Applicazioni: nella lista delle applicazioni compare ora anche l'icona di **DikeIC**.



Cliccando sull'icona è possibile aprire il programma.

2.4 Aggiornamento

DikeIC permette di usufruire del meccanismo di aggiornamento automatico del software.

Il controllo e l'eventuale scaricamento dell'aggiornamento vengono effettuati in modalità automatica se è attiva una connessione ad Internet. Una volta scaricato l'aggiornamento l'utente riceverà una notifica per decidere se procedere con l'installazione subito o rimandare ad un secondo momento.

Se rimandata, la richiesta di installazione degli aggiornamenti scaricati verrà riproposta al successivo avvio del software, o dopo qualche ora, se il programma rimane in esecuzione.

3 Guida alla firma dei documenti con DikeIC

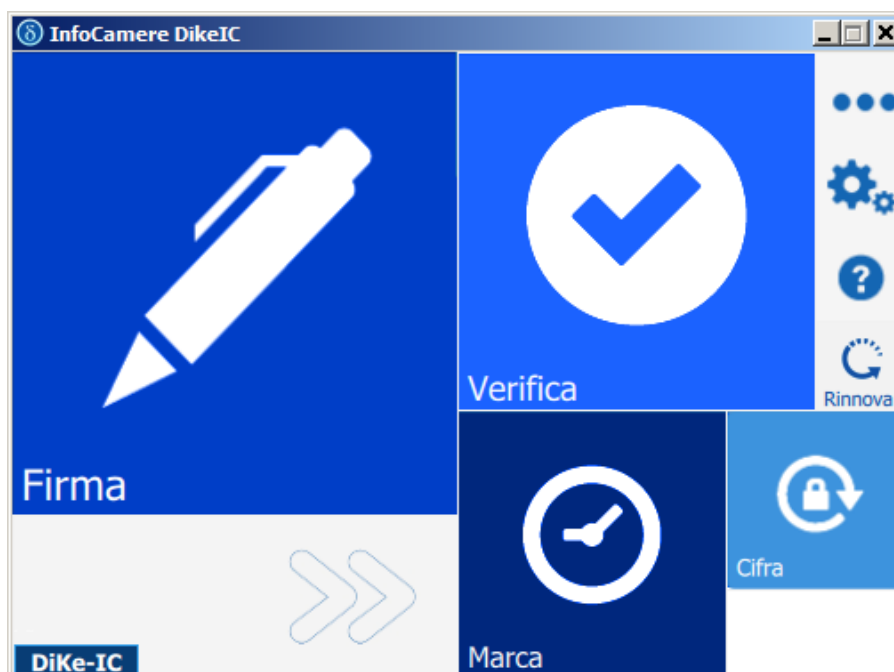
DikeIC permette di firmare digitalmente e di marcare temporalmente un documento digitale. Permette inoltre di verificare la validità di una firma e di una marca temporale apposte su un documento.

3.1 Cosa occorre

1. Un certificato di sottoscrizione valido, ospitato su dispositivo fisico o disponibile in modalità remota;
2. Il PIN del dispositivo fisico oppure i codici personali (PIN e OTP) per l'utilizzo della firma remota;
3. Un documento digitale da firmare;
4. La versione di DikeIC per il sistema operativo presente sulla stazione di lavoro. Le funzioni e i comandi presenti in DikeIC non cambiano nei diversi ambienti. Le minime differenze riscontrabili sono legate ai sistemi operativi e riguardano il nome assunto dai comandi di selezione dei documenti (Apri piuttosto che Scegli) e la chiusura del programma.

3.2 Firma di un documento singolo

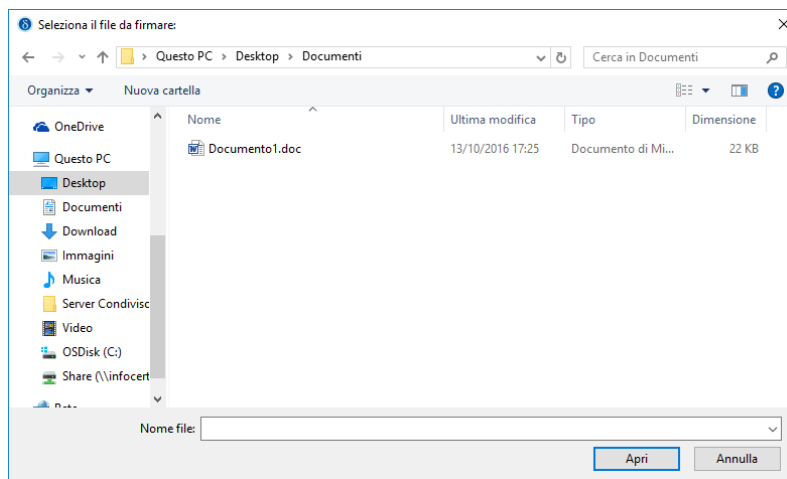
Passando il mouse sul riquadro "Firma" il pannello ruota ed è possibile visualizzare all'elenco delle funzioni di firma.



Sono a disposizione tutte le funzioni di firma, compresa la Firma multipla che permette di selezionare un gruppo di documenti e di firmarli con un'unica autenticazione PIN.

3.2.1 Impostazioni e firma P7M

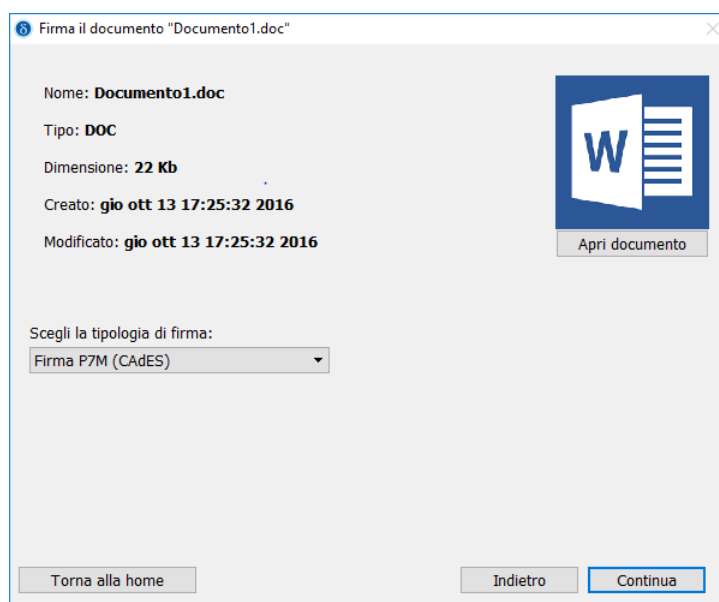
Per firmare un file è innanzitutto necessario cliccare su **Firma**: verrà richiesto di scegliere il file che si desidera firmare. Basta evidenziarlo e cliccare su **Apri** (o, in alternativa, cliccare due volte sul file).



Per i file in formato diverso da pdf, DikeIC, una volta caricato il file, ne presenta gli estremi (nome, tipo, dimensione, date di creazione ed ultima modifica) e mette a disposizione il pulsante **“Apri documento”** per visualizzarlo mediante il software predefinito per la relativa gestione (Microsoft Word nell’immagine d’esempio).

Selezionando un documento in formato pdf, DikeIC imposta automaticamente la tipologia di firma in standard PAdES e presenta anche un riquadro di visualizzazione che contiene il documento e che permette di scorrerlo, di ingrandirlo o di produrne un’anteprima. Servirà reimpostare “Scegli la tipologia di firma:” a “Firma P7M (CAAdES)” per procedere come per i documenti in formato differente.

Procedere con un clic sul pulsante **“Continua”**.



Prima di iniziare il processo di firma vero e proprio, DikeIC verifica che ci sia a disposizione un certificato di

sottoscrizione con il quale firmare.

Firma il documento "Documento1.doc"

Nessun certificato disponibile.
[Aggiungi certificato remoto](#) Aggiorna

Inserisci il PIN:

Destinazione di salvataggio:
 ...

☐ Marca il documento in formato CAdES-T

[Inserisci le credenziali](#)

☐ Aggiungi informazioni per la verifica a lungo termine (LTV)

Torna alla home Indietro Firma

Qualora, come nell'immagine precedente, non sia connesso al PC alcun dispositivo, si presentano due possibilità:

- Collegare al computer un dispositivo e cliccare su **Aggiorna**;
- Cliccare su **"Aggiungi certificato remoto"** e configurare il proprio certificato di firma remota in DikeIC;

Proseguiamo scegliendo la prima opzione e vediamo che vengono visualizzati i dati relativi al certificato del dispositivo e al firmatario: ora si può procedere alla firma.

Firma il documento "Documento1.doc"

Scegli il certificato
SC/BK di manuel (201650233321) Aggiorna

Inserisci il PIN:

Destinazione di salvataggio:
 ...

☐ Marca il documento in formato CAdES-T

[Inserisci le credenziali](#)

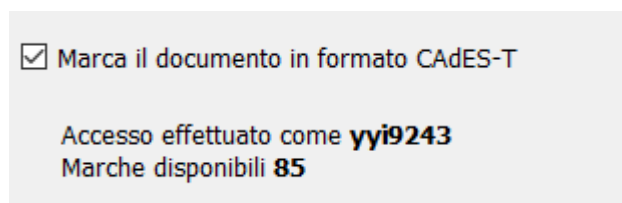
☐ Aggiungi informazioni per la verifica a lungo termine (LTV)

Torna alla home Indietro Firma

Innanzitutto è necessario digitare il PIN del certificato con cui si sta firmando il documento: una volta digitato il codice, il pulsante **“Firma”**, fino ad ora oscurato, diventerà cliccabile.

In secondo luogo si deve scegliere dove salvare il documento firmato (**“Destinazione di salvataggio”**): DikeIC propone il salvataggio del nuovo file nella medesima cartella in cui si trova il file originale da firmare. Se si desidera cambiare l'impostazione predefinita, basta cliccare sul pulsante coi tre puntini e scegliere dove generare il file firmato.

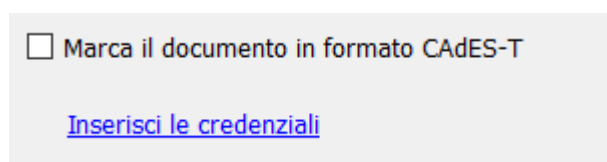
Se si vuole non solo firmare il file, ma anche marcarlo temporalmente, si deve utilizzare l'opzione **“Marca il documento in formato CAdES-T”**. Se si è già provveduto in precedenza a configurare le credenziali di marche temporali all'interno del programma, verrà visualizzata la user e il numero di marche disponibili.



☒ Marca il documento in formato CAdES-T

Accesso effettuato come **yyi9243**
Marche disponibili **85**

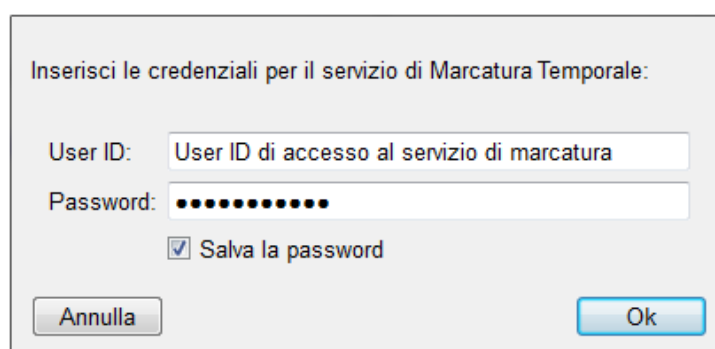
Se invece quest'operazione non è mai stata fatta, viene visualizzato il link **“Inserisci le credenziali”**:



☐ Marca il documento in formato CAdES-T

[Inserisci le credenziali](#)

Cliccando su questo link o evidenziando il quadratino accanto alla dicitura **“Marca il documento in formato CAdES-T”**, appare un popup con due campi in cui inserire user e password per il servizio di marcatura.



Inserisci le credenziali per il servizio di Marcatura Temporale:

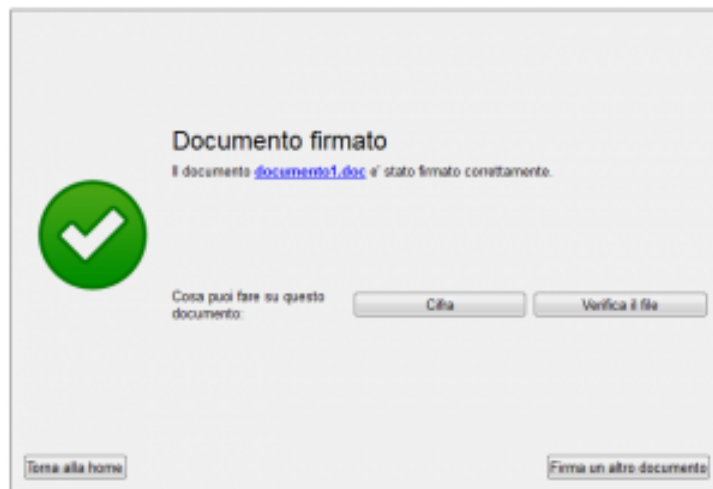
User ID:

Password:

☒ Salva la password

Dopo aver inserito le proprie credenziali, cliccare **“Ok”** per completare la configurazione.

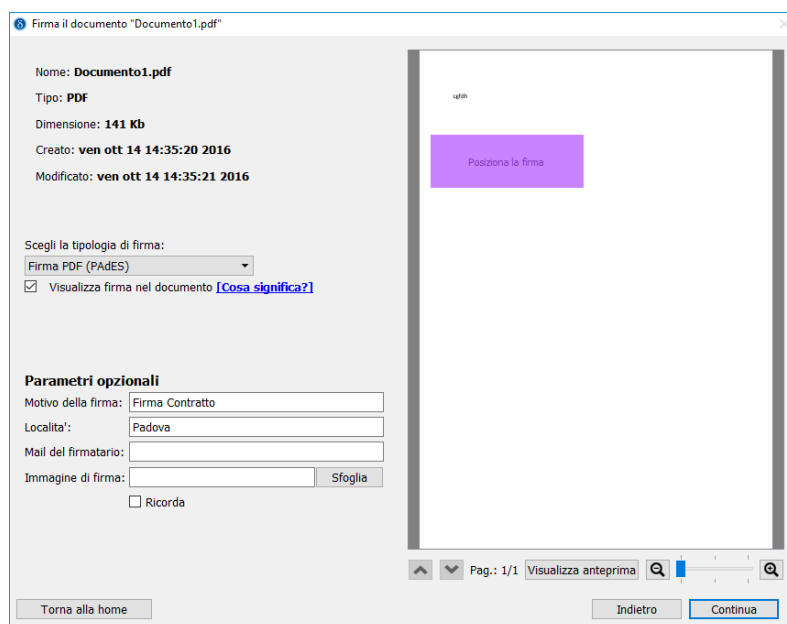
Un clic sul pulsante **“Firma”** conclude il processo di firma del documento; DikeIC confermerà l'avvenuta firma (e marca, se richiesta) con un messaggio a video.



3.2.2 Impostazioni e firma PDF

La **firma PDF** (PAdES) è un tipo di firma digitale che può essere apposta solo su documenti digitali in formato pdf. Conseguentemente DikeIC la propone solo nel momento in cui, all'atto della firma, il file da firmare caricato sul software è in formato pdf.

In questo caso, DikeIC presenta gli estremi del documento (tipo, dimensione, ecc.) nonché un riquadro di visualizzazione che lo contiene e che permette di scorrerlo, di ingrandirlo o di produrne un'anteprima.



Come mostrato nel menu a tendina “**Scegli la tipologia di firma**”, il documento firmato manterrà l’estensione .pdf, cioè la firma sarà standard PAdES. È possibile comunque scegliere di firmare il documento in modalità CADES, ovvero con estensione p7m.

Cliccando sul quadratino accanto a “**Visualizza firma nel documento**”, si ha la possibilità di aggiungere all’interno del testo del documento che si va a firmare, in un punto che lo stesso firmatario può stabilire, un segno grafico contenente gli estremi della firma. Inoltre, una volta sottoscritto il documento, sarà possibile verificare la firma cliccando sul medesimo segno.

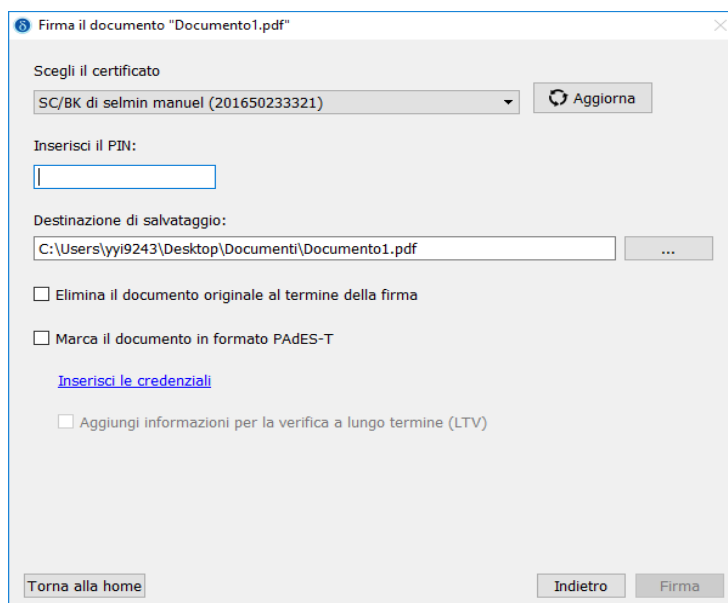
I dati che appariranno nell’annotazione grafica sono quelli che è possibile digitare nella sezione “**Parametri opzionali**”, eccezion fatta per l’indirizzo e-mail del firmatario, che sarà comunque visibile all’atto della verifica del file firmato. Ecco i possibili parametri inseribili:

- Il **motivo** per il quale si sta apponendo la firma. Alcuni esempi: accettazione delle clausole contrattuali, accettazione delle clausole vessatorie del contratto, espressione del mio consenso al trattamento dei dati personali ai sensi della L. 196/2003, ecc.;
- Il **luogo** di apposizione della firma;
- Un **indirizzo e-mail** del firmatario;
- L’**immagine della firma autografa** del firmatario, il quale ha la possibilità di caricarla, dopo averla scansionata e salvata sul proprio PC. E’ ammesso solo il formato .jpg. È molto importante tenere a mente che questo segno grafico **NON ha alcun valore legale** e **NON è in alcun modo la firma digitale**.

E’ possibile, usando il puntatore del mouse, posizionare nel documento il rettangolo **giallo** che appare sullo schermo e che ha una dimensione fissa. Una volta stabilita la posizione, il rettangolo assumerà una colorazione **viola**. La scelta della parte del documento dove inserire il segno grafico è a discrezione del firmatario.

Terminata quest’operazione, si può procedere cliccando sul **Continua**, in basso a destra.

Da qui, la procedura è identica a quella della firma p7m, vista in precedenza. La riportiamo qui di seguito per comodità.



The screenshot shows a Windows-style dialog box titled "Firma il documento 'Documento1.pdf'". It contains the following elements:

- A label "Scegli il certificato" above a dropdown menu showing "SC/BK di selmin manuel (201650233321)". To the right is an "Aggiorna" button with a refresh icon.
- A label "Inserisci il PIN:" above a text input field.
- A label "Destinazione di salvataggio:" above a text input field containing "C:\Users\yy9243\Desktop\Documenti\Documento1.pdf" and a browse button "...".
- Two checkboxes: "Elimina il documento originale al termine della firma" and "Marca il documento in formato PAdES-T".
- A blue hyperlink "Inserisci le credenziali".
- A checkbox "Aggiungi informazioni per la verifica a lungo termine (LTV)".
- At the bottom, three buttons: "Torna alla home", "Indietro", and "Firma".

Innanzitutto è necessario digitare il PIN del certificato con cui si sta firmando il documento: una volta digitato il codice, il pulsante **“Firma”**, fino ad ora oscurato, diventerà cliccabile.

In secondo luogo si deve scegliere dove salvare il documento firmato (**“Destinazione di salvataggio”**): DikeIC propone il salvataggio del nuovo file nella medesima cartella in cui si trova il file originale da firmare. Se si desidera cambiare l’impostazione predefinita, basta cliccare sul pulsante coi tre puntini e scegliere dove generare il file firmato.

Se si desidera non solo firmare il file ma anche marcarlo temporalmente, si deve utilizzare l’opzione **“Marca il documento in formato PAdES-T”**. Se si è già provveduto in precedenza a configurare delle credenziali di marche temporali all’interno del programma, verrà visualizzata la user e il numero di marche disponibili; in caso contrario, sarà visualizzato il link **“Inserisci le credenziali”**, cliccando sul quale sarà possibile configurare all’interno del programma le proprie credenziali di marcatura.

Un clic sul pulsante **“Firma”** conclude il processo di firma del documento; DikeIC confermerà l’avvenuta firma (e marca, se richiesta) con un messaggio a video.

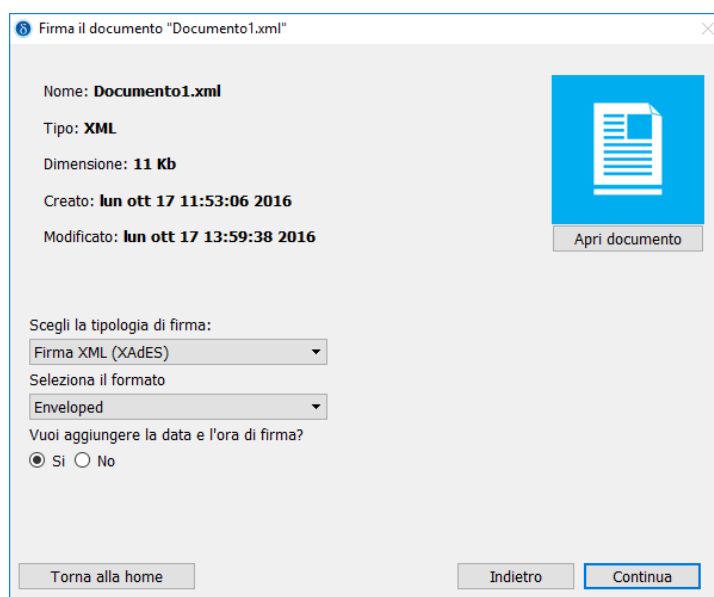


Cliccando su **Aggiungi un firma al PDF**, sarà possibile aggiungere un'ulteriore firma al documento appena firmato.

3.2.3 Impostazioni e firma XML

La **firma XML** (XAdES) è un tipo di firma digitale che può essere apposta solo su documenti digitali in formato xml. Conseguentemente DikeIC la propone solo nel momento in cui, all'atto della firma, il file da firmare caricato sul software è in formato xml.

In questo caso, DikeIC presenta gli estremi del documento (tipo, dimensione, ecc.) e il pulsante **“Apri documento”**, che permette di visualizzarlo.



Come mostrato nel menù a tendina il documento firmato manterrà l'estensione “.xml”, cioè la firma sarà

standard XAdES.

È possibile comunque firmare il documento in modalità CAdES o CAdES detached ricorrendo alle opzioni presenti nello stesso menù a tendina **“Scegli la tipologia di firma”**.

Il menù **“Seleziona il formato”**, inoltre, offre la possibilità di scegliere il formato di dettaglio della firma. Le opzioni previste sono:

- ✓ **Enveloped**, quando la firma fa parte del documento, ne diviene un elemento (la firma è inclusa nel documento da firmare);
- ✓ **Enveloping**, quando la firma contiene tutti i dati del documento firmato (il documento firmato è incluso nella firma);
- ✓ **Detached**, quando il documento da firmare e la firma digitale sono da mantenere separati;

E' possibile, inoltre, evidenziare la relativa opzione, aggiungere **la data e l'ora della firma**.

Dopo aver stabilito le caratteristiche della firma XAdES da apporre, si può procedere con un clic sul pulsante **“Continua”**. Da qui, la procedura è identica a quella della firma CAdES, vista in precedenza.

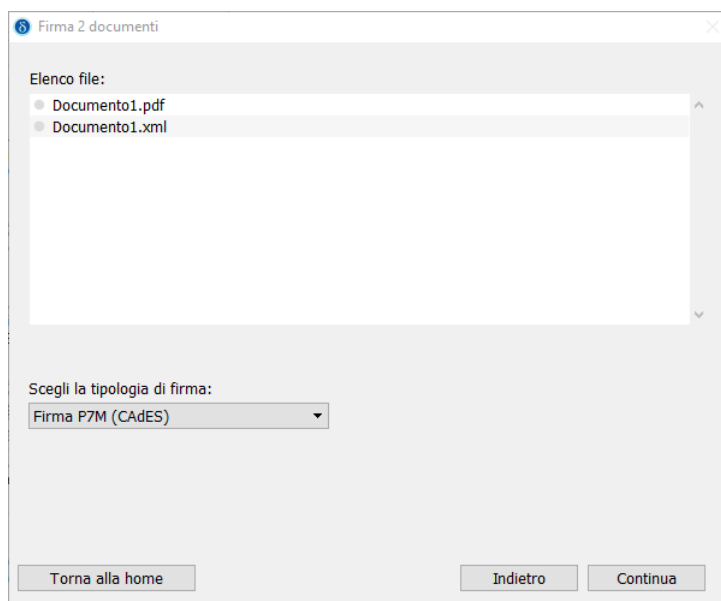
3.3 Firma di più documenti

DikeIC permette di apporre una firma digitale su più documenti in un'unica sessione: le modalità differiscono in relazione al tipo di documenti che si devono firmare e al tipo di firma che si desidera apporre. In tutti i casi, per iniziare la procedura di firma di più file, si deve cliccare su **“Firma Multipla”** sull'home page del programma e selezionare **i file che si desidera firmare**, i quali **devono obbligatoriamente essere presenti tutti nella stessa cartella**.

3.3.1 Impostazioni per firma P7M

Se è stato selezionato un gruppo di documenti con estensioni diverse (ovvero non tutti pdf né tutti xml), sarà possibile apporre firme:

- ✓ **standard CAdES**, riconoscibili per l'ulteriore *estensione* **“.p7m”** qualunque sia quella originale dei file da firmare;
- ✓ **standard CAdES detached**, riconoscibili per l'ulteriore *estensione* **“.p7s”** attribuita ai file che contengono le firme digitali.



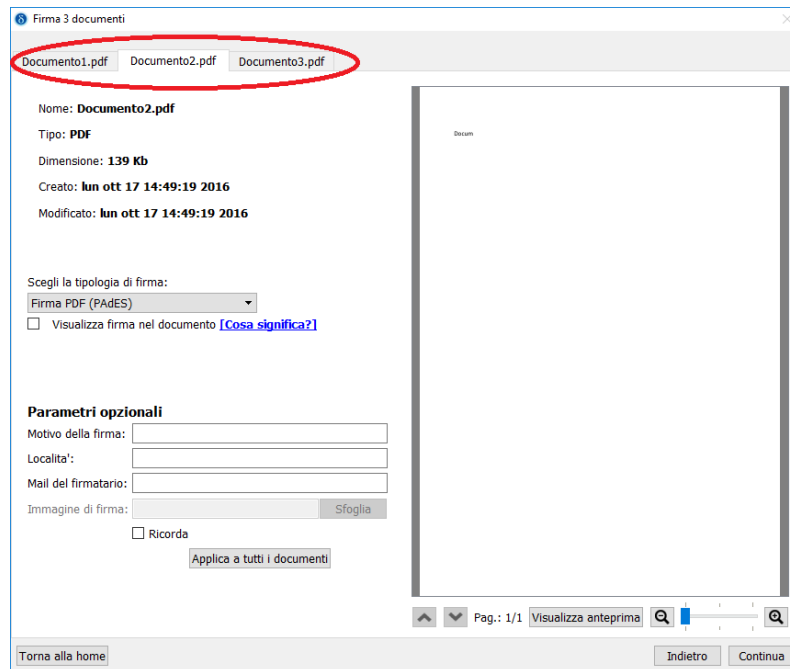
Al termine, procedere con un clic sul pulsante **“Continua”**.

3.3.2 Impostazioni per firma PDF

Se sono stati selezionati esclusivamente documenti con estensione **“.pdf”**, sarà possibile apporre firme:

- ✓ **standard PAdES**, riconoscibili perché mantengono *l'estensione .pdf* originale;
- ✓ **standard CAAdES**, riconoscibili per l'ulteriore *estensione .p7m* aggiunta a quella originale dei file;
- ✓ **standard CAAdES detached**, riconoscibili per l'ulteriore *estensione .p7s* attribuita ai file che contengono le firme digitali.

Al momento della firma, saranno disponibili tanti riquadri di visualizzazione (che contengono i documenti e consentono di scorrerli, di ingrandirli o di produrne un'anteprima) quanti sono i documenti selezionati. Per passare da un documento all'altro sarà sufficiente scorrere le etichette poste nella parte superiore della finestra.



Le impostazioni di firma (**tipologia di firma**, **parametri opzionali** e la posizione del **segno grafico**) sono le stesse descritte nel paragrafo dedicato alla firma pdf, anche se, sarà in questo caso necessario definirle per ognuno dei documenti da firmare. Se le impostazioni fossero le medesime per tutti i documenti sarebbe possibile, una volta definite quelle del primo, selezionare l'opzione "**Applica a tutti i documenti**" per estenderle automaticamente a tutti gli altri.

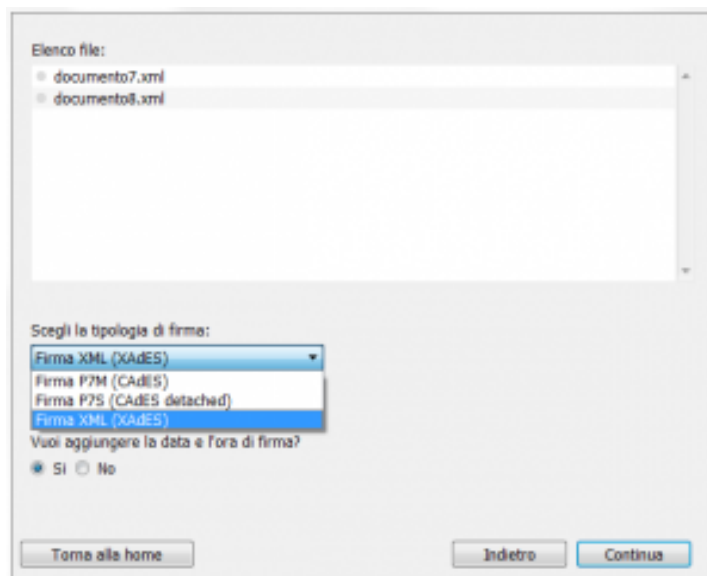
ATTENZIONE: i parametri opzionali e il segno grafico sul testo del documento sono caratteristiche dei soli file firmati in **formato PAdES** (firma pdf) e non saranno impostabili sui documenti che si è scelto di firmare in formato diverso.

Al termine, procedere con un clic sul pulsante "**Continua**".

3.3.3 Impostazioni per firma XML

Se sono stati selezionati esclusivamente documenti con estensione **.xml**, sarà possibile apporre firme:

- ✓ **standard XAdES**, riconoscibili perché mantengono l'*estensione .xml* originale;
- ✓ **standard CAdES**, riconoscibili per l'ulteriore *estensione .p7m* aggiunta a quella originale dei file;
- ✓ **standard CAdES detached**, riconoscibili per l'ulteriore *estensione .p7s* attribuita ai file che contengono le firme digitali.



Elenco file:

- documento7.xml
- documento8.xml

Scegli la tipologia di firma:

- Firma XML (XAdES)
- Firma P7M (CAdES)
- Firma P7S (CAdES detached)
- Firma XML (XAdES)

Vuoi aggiungere la data e l'ora di firma?

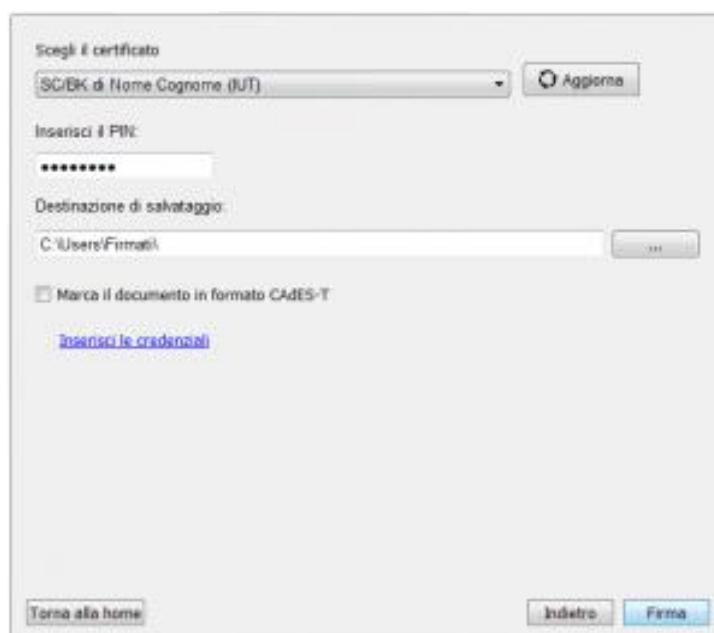
☒ Sì ☐ No

Torna alla home Indietro Continua

Al termine, procedere con un clic sul pulsante **“Continua”**.

3.3.4 Firma multipla

In tutti i casi, che si stia eseguendo una firma multipla CAdES, PAdES o XAdES, dopo aver cliccato sul pulsante **“Continua”** si arriva alla fase di inserimento PIN, del tutto analoga a quella descritta nel paragrafo 3.2.1, che ripetiamo per comodità.



Scegli il certificato

SC/BK di Nome Cognome (IUT) Aggiorna

Inserisci il PIN:

Destinazione di salvataggio:

C:\Users\Firmati\ Salva

☐ Marca il documento in formato CAdES-T

[Inserisci le credenziali](#)

Torna alla home Indietro Firma

Innanzitutto è necessario digitare il PIN del certificato con cui si stanno firmando i documenti: una volta digitato il codice, il pulsante **“Firma”**, fino ad ora oscurato, diventerà cliccabile.

In secondo luogo, si deve scegliere dove salvare i documenti firmati ("**Destinazione di salvataggio**"): DikeIC propone il salvataggio dei nuovi file nella medesima cartella in cui si trovano i file originali da firmare. Se si desidera cambiare l'impostazione predefinita, basta cliccare sul pulsante coi tre puntini e scegliere dove generare i file firmati.

Se si desidera non solo firmare i file ma anche marcarli temporalmente, si deve utilizzare l'opzione "**Marca il documento in formato CAdES-T**". Se si è già provveduto in precedenza a configurare delle credenziali di marche temporali all'interno del programma, verrà visualizzata la user e il numero di marche disponibili; in caso contrario, sarà visualizzato il link "**Inserisci le credenziali**", cliccando sul quale sarà possibile configurare all'interno del programma le proprie credenziali di marcatura.

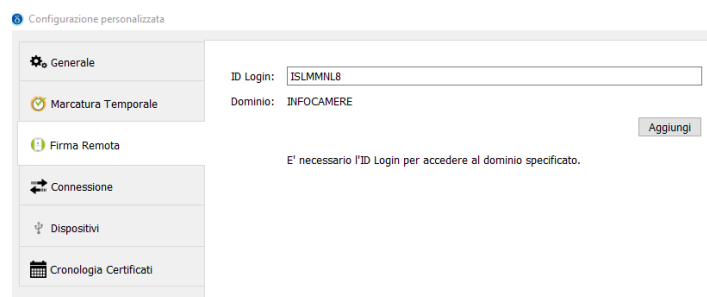
Un clic sul pulsante "**Firma**" conclude il processo di firma dei documenti; DikeIC confermerà l'avvenuta firma (e marca, se richiesta) con un messaggio a video.



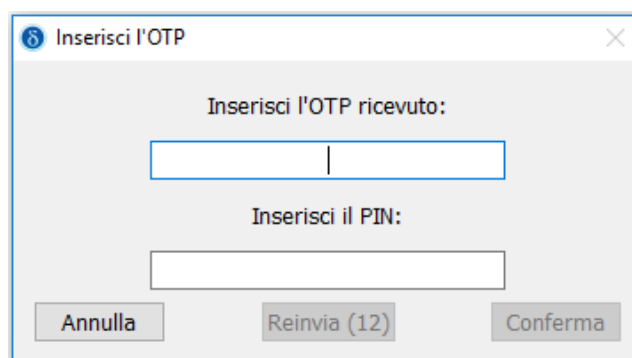
3.3.5 Firma remota: configurazione ed uso.

La **configurazione del certificato di firma remota** è un'operazione semplice che dev'essere compiuta prima di iniziare l'attività: si tratta di associare al software i dati del proprio certificato di firma remota, in modo che il sistema sappia quale certificato usare quando viene richiesta una firma.

La prima cosa da fare è cliccare sull'icona delle impostazioni sull'home page del programma (i due ingranaggi reperibili in alto a destra) e, sulla schermata che ne risulta, cliccare il tab "**Firma remota**". Viene richiesto di inserire l'**ID Login**, una stringa di caratteri che consta del codice fiscale del titolare preceduto da una lettera identificativa. L'**ID Login** viene attribuito e comunicato al Titolare al momento dell'attivazione del certificato di firma remota.

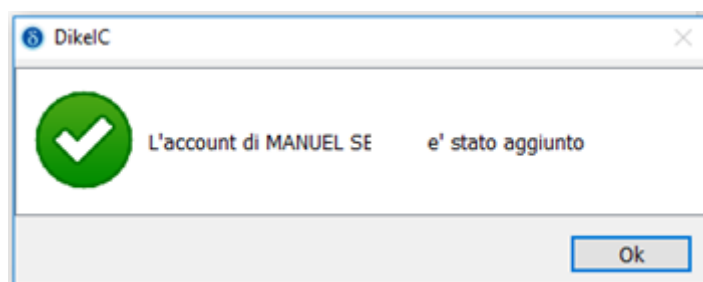


Una volta inserito l'ID Login, cliccare **“Aggiungi”**: viene visualizzato un pop-up all'interno del quale vengono richiesti **OTP** e **PIN**.



- **OTP**: si tratta di un codice di otto cifre che viene inviato al cellulare indicato nella richiesta di firma remota presentata presso la Camera di Commercio Industria Agricoltura Artigianato, quando si giunge a questa pagina: lo si troverà, dunque, tra gli sms in arrivo.
- **PIN**: si tratta del PIN del certificato, stabilito durante la procedura di attivazione della firma remota. Anche in questo caso si tratta di un codice di otto cifre.

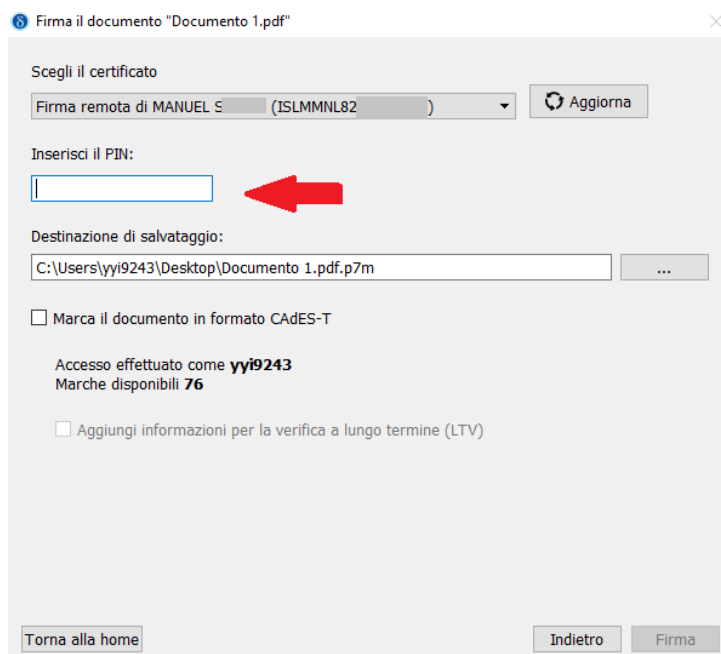
Il pulsante **“Reinvia”** è da utilizzarsi se non si è ricevuto alcun OTP, mentre si deve cliccare sul pulsante **“Conferma”**, che diventa cliccabile solo una volta riempiti i due campi, per procedere.



Dopo il riscontro dei dati inseriti, verrà data conferma dell'avvenuta associazione tra l'account di firma remota e DikeIC. **E' possibile inserire più account**: in questo caso il programma chiederà, al momento della firma, quale certificato utilizzare per firmare.

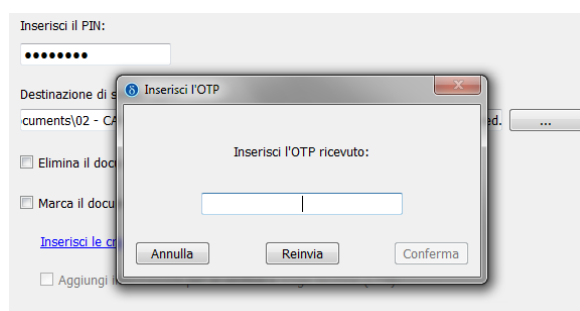
Ma come si firma con la firma remota? Per capirlo riferiamoci alla procedura descritta al paragrafo 3.2.1.

di questo manuale, nel quale si descrive come utilizzare DikeIC per firmare un documento con i certificati caricati su dispositivo. Ripartiamo da questa schermata (vedi pagina.12): il file da firmare è stato appena caricato e ora si chiede di inserire il PIN del certificato.

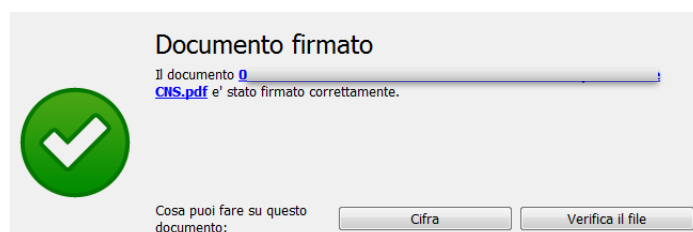


Per firmare con la firma remota è necessario scegliere il certificato associato al software nel menù “**Scegli il certificato**”: naturalmente propedeuticamente a questa fase è necessario aver configurato il proprio account di firma all’interno del software, come spiegato poco sopra.

Inserire il **PIN del certificato di firma remota** e cliccare “**Firma**”, in basso a destra, per procedere.



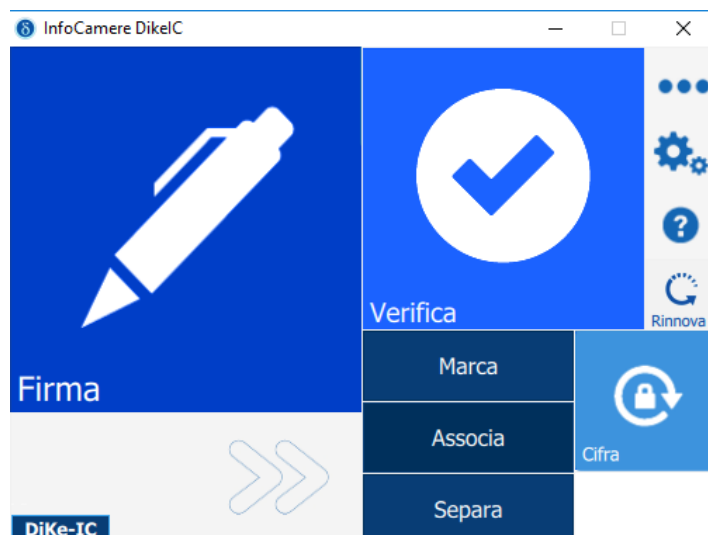
Verrà proposto il pop-up per l’inserimento dell’OTP contestualmente ricevuto al cellulare.



Cliccare “**Conferma**” per completare la procedura. DikeIC confermerà l’avvenuta firma con un messaggio.

4 Marca temporale

Se si desidera apporre su uno o più documenti una marca temporale, è necessario passare il cursore del mouse sul riquadro “**Marca**” per accedere alle funzioni di marcatura.

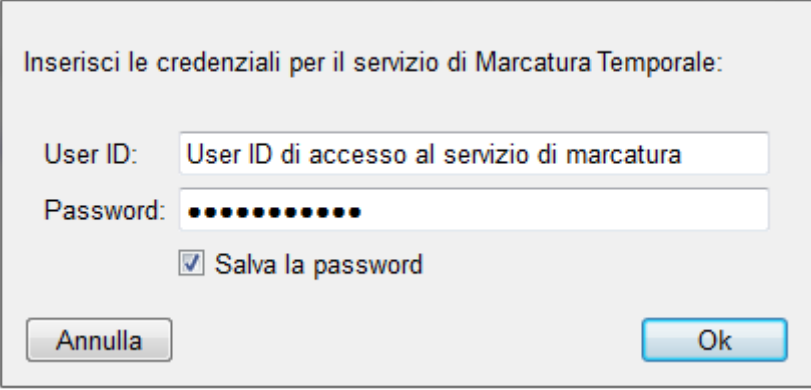


Sono a disposizione le opzioni “**Marca**”, “**Associa**” e “**Separa**” che permettono di selezionare e richiamare all’interno del software rispettivamente:

1. Un file che si vuole **marcare** temporalmente;
2. Un file che si vuole **associare** a una marca temporale precedentemente generata;
3. Un file già marcato da cui si desidera **separare** la marca temporale;

4.1 Marcatura di documenti

Dopo aver cliccato su “**Marca**”, se non sono state **configurate delle credenziali di marcatura** all’interno di DikeIC, il software presenta immediatamente una maschera che consente di farlo:



Inserisci le credenziali per il servizio di Marcatura Temporale:

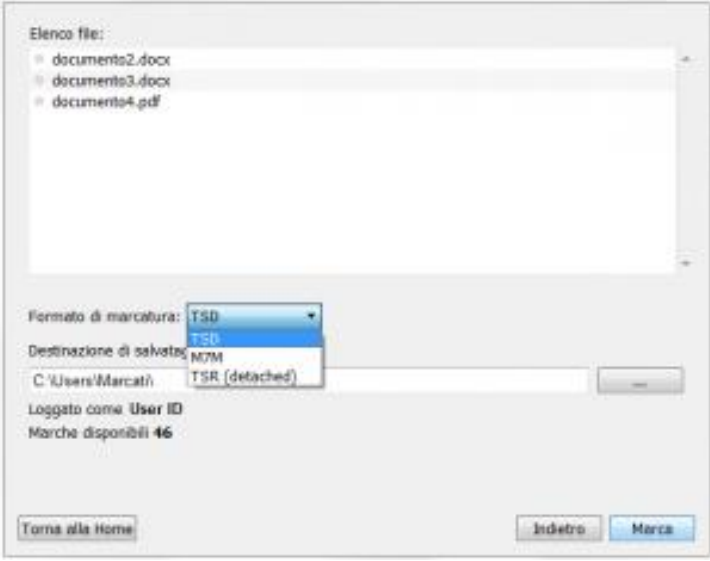
User ID:

Password:

☒ Salva la password

Se delle credenziali sono già state impostate, sarà immediatamente possibile selezionare i file che si vogliono marcare e caricarli sul software. Si ricorda che **è possibile marcare sia un solo documento che un gruppo di documenti**: in questo secondo caso, tutti i file da marcare contemporaneamente devono essere presenti nella stessa cartella.

L'immagine qui di seguito è quanto appare dopo la selezione di tre file da firmare.



Elenco file:

- documento2.docx
- documento3.docx
- documento4.pdf

Formato di marcatura:

Destinazione di salvataggio:

C:\Users\Marcat\

Loggato come: User ID

Marche disponibili: 46

Dopo aver identificato il formato di marcatura desiderato e aver definito dove salvare i file marcati, si può procedere con un clic sul pulsante **“Marca”**.

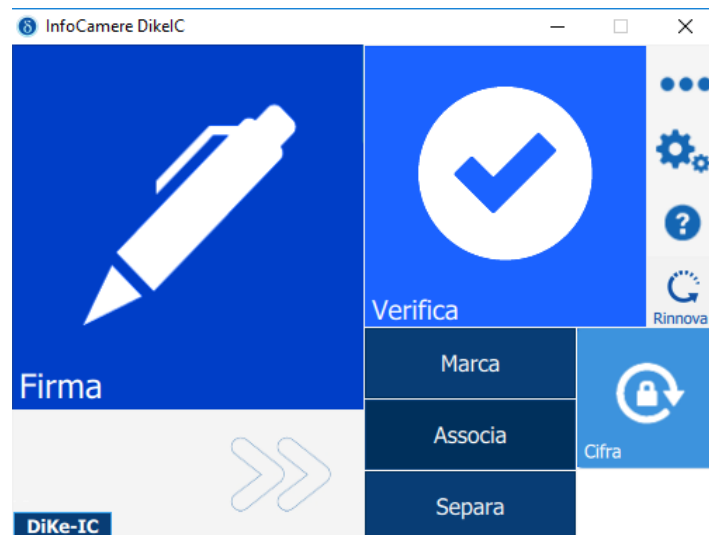
A operazione eseguita, DikeIC ne comunica l'esito con un messaggio a video.



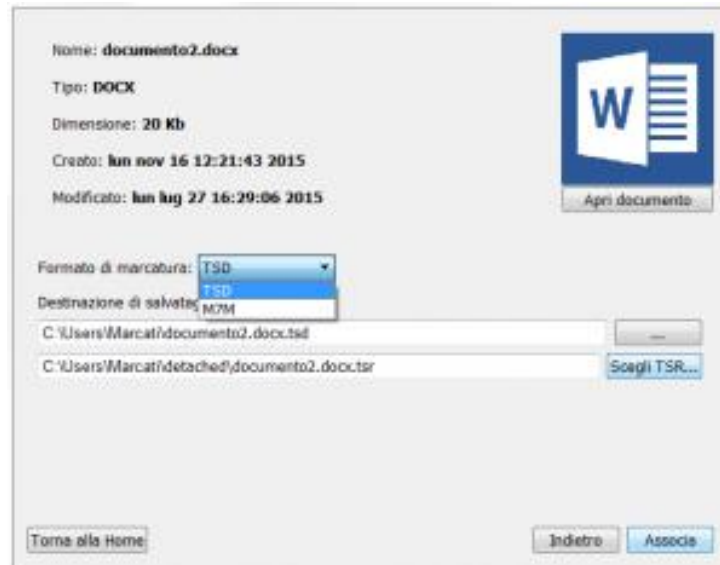
Cliccare “Torna alla home” per concludere la sessione.

4.2 Associazione marche a documenti

DiKeIC permette di associare ad un documento una marca temporale precedentemente prodotta in modalità detached (ovvero presente nel PC singolarmente, non associata ad alcun documento). A questo fine è necessario innanzitutto cliccare su “**Associa**”, nell’home page.



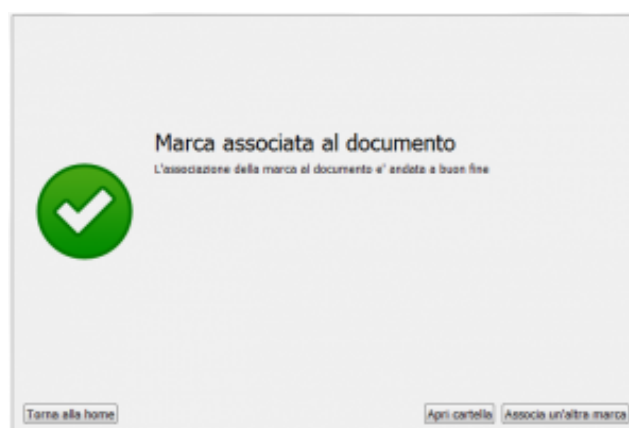
Dopo aver selezionato il documento a cui associare la marca, DikeIC ne presenta gli estremi (tipo, dimensione, ecc.) e il pulsante “**Apri documento**”, che permette di visualizzarlo, come si vede nell’immagine qui di seguito.



Come mostrato nel menù **“Formato di marcatura”** il documento marcato potrà assumere l’estensione .tsd o .m7m.

E’ inoltre necessario scegliere dove salvare il documento firmato (**“Destinazione di salvataggio”**): DikeIC propone il salvataggio del nuovo file nella medesima cartella in cui si trovano il file originale. Se si desidera cambiare questa impostazione predefinita, basta cliccare sul pulsante coi tre puntini e scegliere dove generare il file marcato.

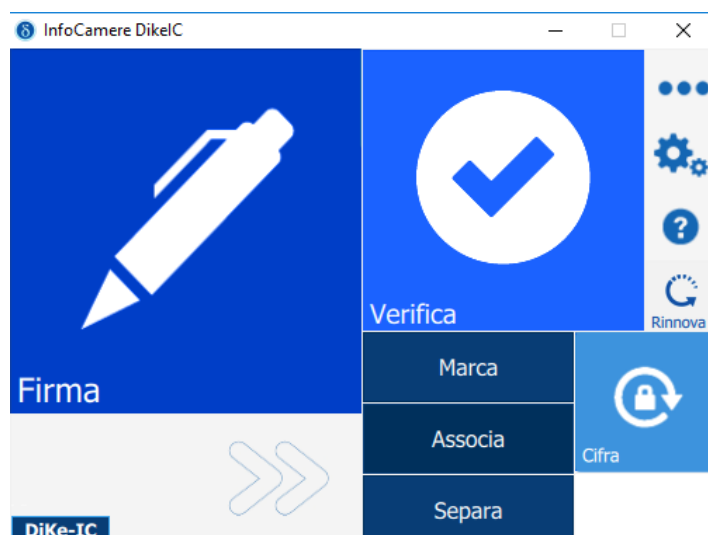
Nella stessa finestra c’è la possibilità di selezionare la marca temporale generata a suo tempo per il documento utilizzando il pulsante **“Scegli TSR”**. Un clic sul pulsante **“Associa”** conclude il processo; DikeIC confermerà l’avvenuta associazione con un messaggio di conferma a video.



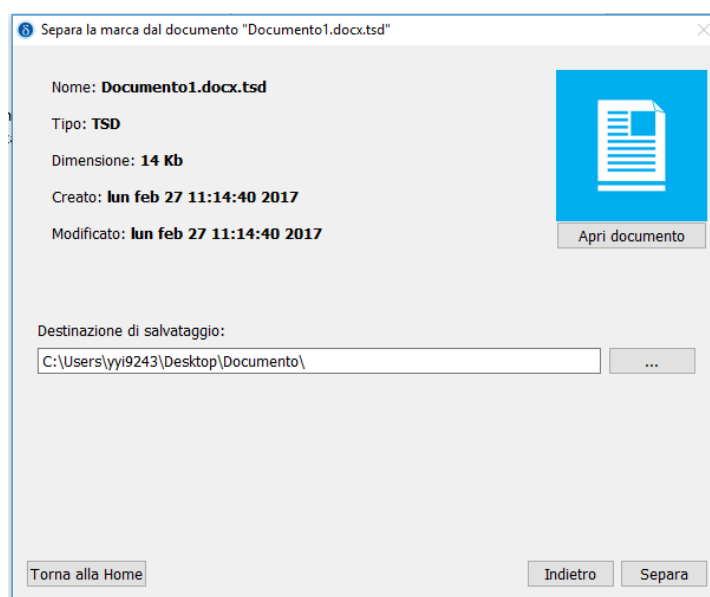
Cliccare **“Torna alla home”** per concludere la sessione.

4.3 Separazione marche da documenti

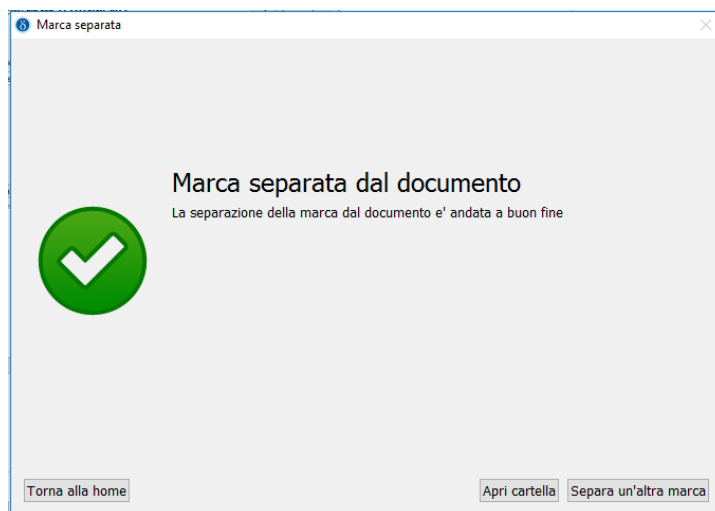
Dike IC permette di separare la marca temporale da un documento marcato. A questo fine si procede cliccando su **“Separa”** nell’home page



Dopo aver selezionato il documento da cui separare la marca, DikeIC ne presenta gli estremi (tipo, dimensione, ecc.) e il pulsante **“Apri documento”**, che permette di visualizzarlo.

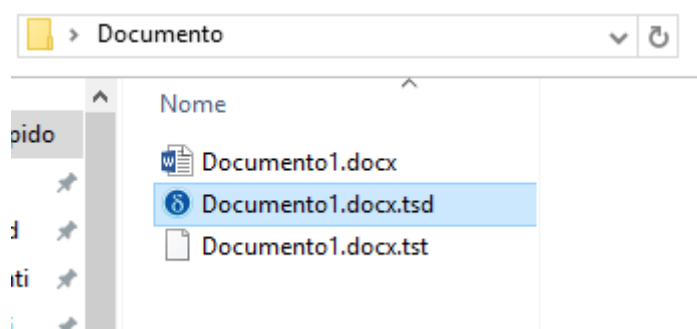


Per procedere alla separazione della marca si deve cliccare sul pulsante **“Separa”**, in basso a destra. Eseguita la separazione, verrà visualizzato il messaggio di conferma.



Nella cartella dov'è salvato il file originale, si noterà che ora i file sono tre:

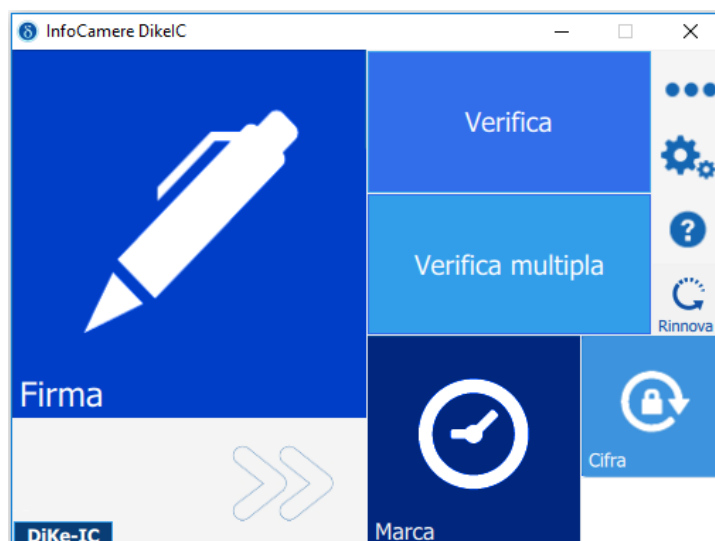
- Il file marcato originale;
- La marca separata (in formato 'tsd')
- Il documento da cui la marca è stata separata (in formato 'tst' o 'tsr')



5 Verifica

DikeIC, oltre alla firma e alla marcatura di documenti, permette anche la loro verifica.

Passando il mouse sul riquadro **“Verifica”**, nell’home page è possibile accedere all’elenco delle funzioni di verifica.



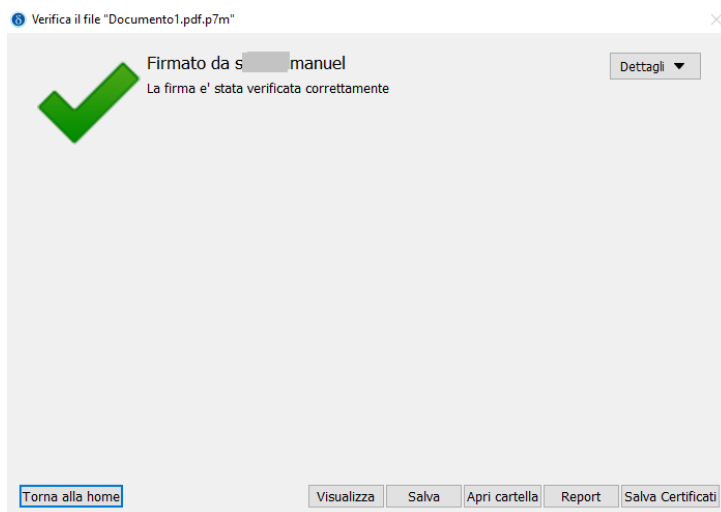
Le opzioni possibili sono:

1. **“Verifica”**: ovvero la possibilità di verificare la validità di un singolo file firmato digitalmente e/o marcato temporalmente;
2. **“Verifica multipla”**: ovvero la possibilità di verificare simultaneamente la validità di un gruppo di file firmati digitalmente e/o marcati temporalmente. In questo caso i file da verificare devono obbligatoriamente essere presenti nella stessa cartella. La verifica multipla funziona anche con file firmati con modalità di firma differenti.

Per verificare un solo file, si clicca su **“Verifica”** nell’home page, si sceglie il file firmato da verificare e lo si carica sul software. In breve verrà visualizzato il risultato dell’operazione. Nella maschera di verifica sono presenti le seguenti funzioni, selezionabili mediante il relativo pulsante:

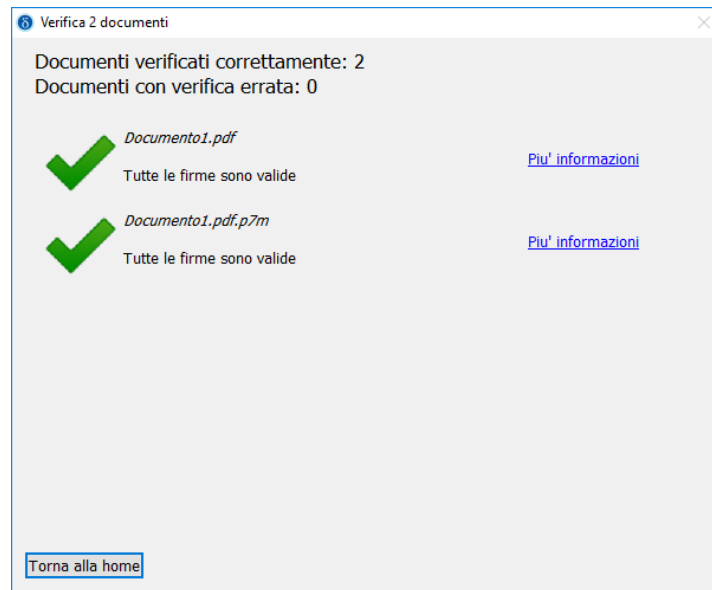
- **“Dettagli”**: permette di mostrare i dati relativi a ciascun firmatario, alla relativa firma ed al certificato utilizzato, permettendo anche il salvataggio del certificato;
- **“Visualizza”**: permette di visualizzare il documento originale;
- **“Salva”**: permette di salvare il file originale;
- **“Apri cartella”**: permette di aprire la cartella dove si trova il file firmato;

- **“Report”**: permette di visualizzare e stampare un report relativo alla verifica e al suo esito;
- **“Salva certificati”**: permette di salvare i certificati dei firmatari;



Si noti che se si sta verificando un file firmato con **firma pdf**, nella sezione **“Dettagli”** saranno visibili anche i **parametri opzionali** (motivo e luogo della firma, e indirizzo e-mail) che il firmatario ha impostato all’atto della firma e che sono caratteristici della firma PAdES (si veda par. 3.2.2). In maniera simile, se si sta verificando un file firmato con **firma XML** nella sezione **“Dettagli”** saranno visibili **la data e l’ora della firma**, a condizione che il firmatario abbia scelto di inserire questi dati (si veda par. 3.2.3).

Per verificare invece più file, si clicca su **“Verifica multipla”** nella home page, si scelgono i file firmati da verificare, che devono tutti essere presenti nella medesima cartella, e li si carica sul software. Verrà visualizzato l’elenco dei file firmati con il risultato della verifica. Cliccando su **“Più informazioni”** accanto ad ogni file, sarà possibile accedere ai dettagli della firma di ognuno dei documenti verificati.



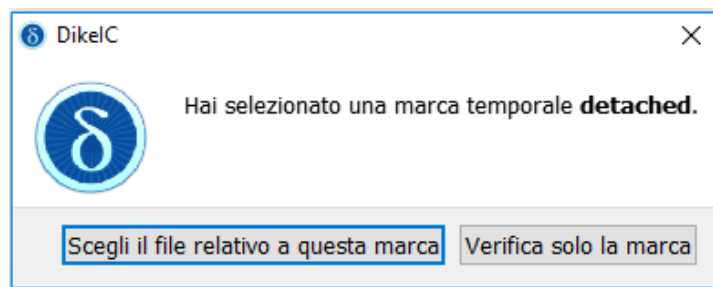
DikeIC è in grado anche di **verificare la marca temporale** apposta ad un documento, sia esso solamente marcato o anche firmato. Nel primo caso, ovvero in occasione della verifica di un file marcato ma non firmato, la maschera di verifica mostrerà l'esito relativo alla sola marca.



Nel secondo caso, ovvero in occasione della verifica di un file che, oltre ad essere marcato, sia anche firmato, la maschera di verifica mostrerà sia l'esito relativo alla marca che quello relativo alla firma.



DikeIC permette di verificare anche i documenti caratterizzati da una marca temporale apposta in modalità detached (documento con estensione '.tsr' o 'tst'), dando modo di eseguire la verifica della sola marca temporale o di associarla al documento informatico cui era stata apposta e passare successivamente alla verifica.



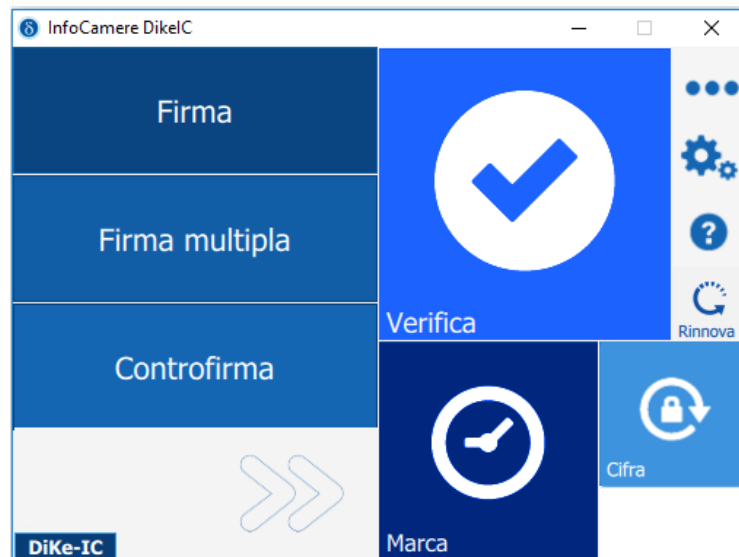
Se si sceglie di cliccare su “**Scegli il file relativo a questa marca**”, prima della verifica apparirà il file system del PC da cui si potrà scegliere il file da associare alla marca. Se si clicca su “**Verifica solo la marca**” verrà visualizzato immediatamente il risultato della verifica.



6 Controfirma

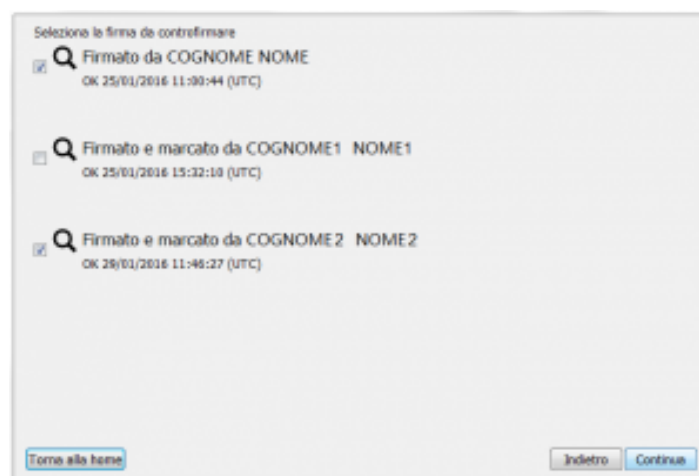
Se è necessario creare una sequenza di firme digitali legate ad un documento e di tenere traccia della sequenza e della gerarchia delle firme apposte, si può utilizzare la funzione **“Controfirma”** di DiKeIC.

Passando il mouse sul riquadro **“Firma”** è possibile accedere alla funzione di controfirma.



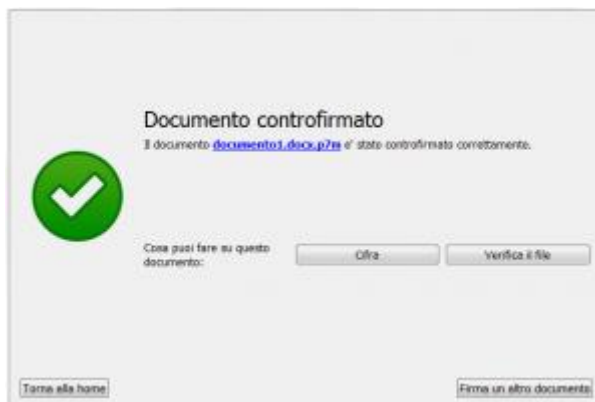
E' possibile applicare la controfirma ad un documento firmato o ad un documento firmato e marcato purché a standard CAdES, che si presenta cioè con estensione P7M.

DikeIC esegue la verifica delle firme e delle eventuali marche temporali apposte al documento. Successivamente, permette di selezionare le firme da controfirmare.



Per firmare è necessario proseguire in modo analogo al caso di firma CAdES di un singolo documento.

Al termine del processo di firma del documento, DikeIC confermerà l'avvenuta controfirma con un messaggio a video.

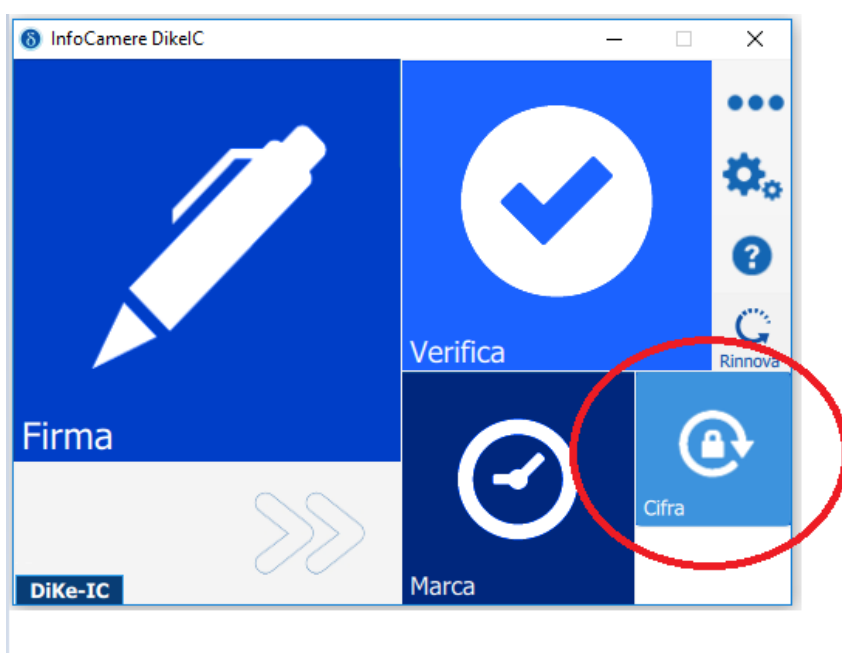


7 Come cifrare e decifrare un file

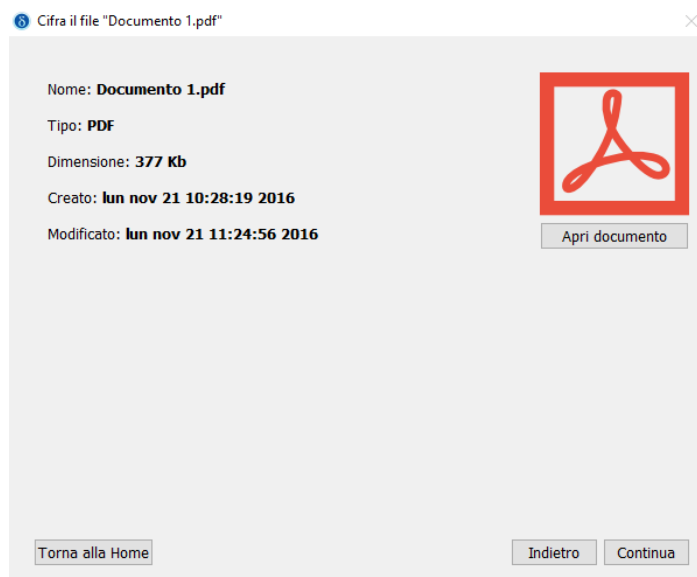
Con DikeIC è possibile **cifrare file e decifrare file cifrati**: è un modo questo per poter spedire in sicurezza dei documenti, visto che solo il destinatario, cui solo sarà stata comunicata la chiave di decifratura, sarà in grado di decifrarli e leggerli.

7.1 Cifrare un file

Per poter **cifrare un file** è necessario accedere dalla home page del programma alla funzione dedicata. Cliccando su “**Cifra**” appariranno le opzioni “**Cifra**” e “**Decifra**”.

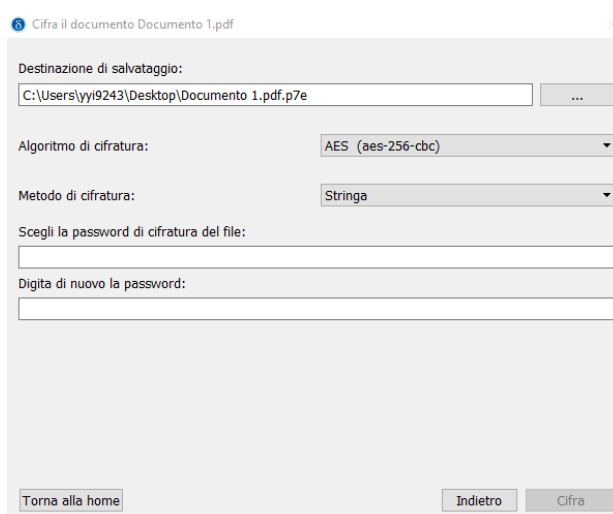


Cliccando “Cifra” si verrà subito invitati a scegliere il file che si vuole cifrare: basta individuare il file desiderato e cliccare su di esso per **selezionarlo**. Non appena fatto ciò, si apre una finestra che riporta alcuni dati relativi al documento prescelto: nome, tipo, dimensione, data di creazione e data dell’ultima modifica. E’ inoltre possibile aprire il file e visualizzarlo: una possibilità in più per assicurarsi di aver selezionato il documento esatto.

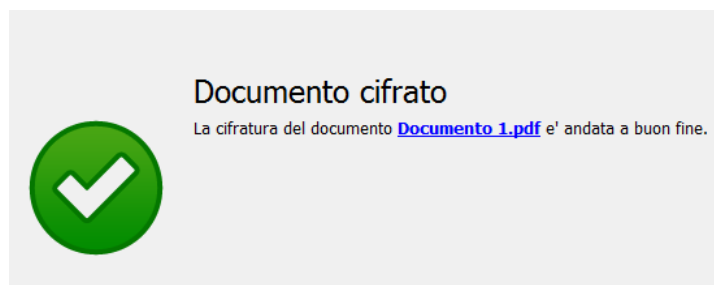


Cliccando sul **"Continua"** si passa alla fase successiva: una nuova finestra permette di stabilire:

- **l'algoritmo di cifratura:** da scegliere tra "AES", "3DES" e "Blowfish" (modificare quello proposto solo in caso di specifica necessità);
- **il metodo di cifratura:** da scegliere tra "Stringa", "Certificato su Smart Card", "Certificato su File P12" e "Certificato su File" (al momento è disponibile solo il primo metodo);
- **la password di cifratura:** ovvero *la password* che permetterà a chi riceve il file cifrato di aprirlo. La password è necessaria solo se si utilizza il metodo "Stringa", mentre, nel caso di cifratura con certificato, sarà *la chiave pubblica dello stesso certificato (selezionabile sul pc) ad essere utilizzata per l'apposizione della firma*.



Cliccando su “**Cifra**” si avvia la cifratura, terminata la quale sarà prodotto un messaggio a video con l’esito dell’operazione.



7.2 Decifrare un file

Per decifrare un documento si procede in maniera del tutto analoga. Cliccando su “**Decifra**” sull’home page, è possibile selezionare il file cifrato che si vuole decifrare. Si ricorda che il file cifrato assumerà l’ulteriore estensione “**p7e**”. Una volta selezionato il file appare questa finestra:

Inserendo due volte la **password di decifratura**, che dovrà essere stata comunicata da chi ha cifrato il file, e cliccando su “**Decifra**” si avvierà la decifratura, terminata la quale sarà prodotto un messaggio a video con l’esito dell’operazione.

