

Difesa D'Ufficio

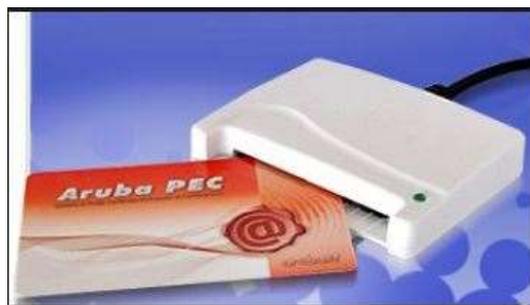
Accesso e gestione elenco nazionale

Torino - Aula magna Pala Giustizia - 11 maggio 2016

Dispositivi di firma digitale e CNS

Dott. Paolo Lorenzin

Cos'è un dispositivo di firma digitale?



A cosa serve il dispositivo di firma digitale e CNS?

1. Firmare digitalmente qualunque documento (file) informatico, nel caso specifico firmare digitalmente la domanda o i documenti richiesti per l'ammissione alle difese d'ufficio
2. Poter accedere in modo "sicuro" ad una serie di servizi telematici, nel caso specifico al programma del CNF delle difese d'ufficio

Entrambe le funzionalità sopra indicate si concretizzano, in sintesi, immettendo il PIN della chiavetta (solitamente un numero di 8 cifre personalizzabile a piacere) fornitoci all'acquisto della stessa

Tali dispositivi sono denominati solitamente «chiavette»

Certificati digitali

Ogni chiavetta contiene (solitamente) al suo interno due certificati digitali:

- ❑ **Certificato di identificazione/autenticazione**
 - ❑ Serve per l'accesso ai servizi telematici
- ❑ **Certificato di firma digitale**
 - ❑ Serve per la sottoscrizione dei documenti informatici

Il certificati digitali sono l'equivalente elettronico di un documento d'identità (come il passaporto o la carta d'identità) e identificano in maniera digitale una persona fisica. Sono emessi da un'apposita Autorità di certificazione (Certification Authority - CA) riconosciuta secondo standard internazionali, la quale garantisce la validità delle informazioni riportate nei certificati.

Come i documenti d'identità cartacei, anche il certificati digitali hanno una **validità temporale** al di fuori della quale risulteranno scaduti e quindi inusabili.

“Chiavetta”

- ❑ È rilasciata alle persone fisiche e l'acquisto non è delegabile
- ❑ Va rinnovata alla scadenza (come un qualunque documento d'identità)
- ❑ Acquistabile on-line o direttamente presso i rivenditori
- ❑ Si può avere più di una chiavetta per persona
- ❑ Se viene smarrita/sottratta occorre presentare denuncia
 - ❑ Anche presso la società che ci ha venduto la chiavetta
- ❑ Acquistabile anche solo con uno dei due certificati

Modelli di "chiavette"

ARUBA KEY	TOKEN	SMART CARD
 <p>VALIDITÀ 3 ANNI</p> <p>MEMORIA 2GB</p>	 <p>VALIDITÀ 3 ANNI</p>	 <p>VALIDITÀ 3 ANNI</p>
		
<p>Vantaggi</p> <ul style="list-style-type: none">• Sicurezza totale• Software preinstallato• Utilizzabile su qualsiasi computer• Backup memoria interna	<p>Vantaggi</p> <ul style="list-style-type: none">• Sicurezza totale• Utilizzabile su qualsiasi computer	<p>Vantaggi</p> <ul style="list-style-type: none">• Sicurezza totale• Utilizzabile su qualsiasi computer

La prima volta che uso il dispositivo su un nuovo pc devo ripetere la procedura di installazione del dispositivo stesso

A cosa serve il certificato di identificazione?

La Carta Nazionale dei Servizi (CNS) è lo strumento che consente l'identificazione certa dell'Utente (Titolare del Certificato) in rete ai servizi online ed ai siti web della Pubblica Amministrazione, come ad esempio i servizi consultabili sul sito dell'Agenzia Delle Entrate (fisconline/entratel), del Registro Imprese, INPS, ex- Inpdap, Equitalia ecc. La CNS è oggi sempre più richiesta sia dai cittadini che dalle aziende e per alcune categorie professionali, come avvocati, geometri, architetti ecc.. è diventato uno strumento necessario per autenticarsi ai propri punti di accesso telematici (vedi processo civile telematico) o scambiare informazioni con le PA. Il Certificato CNS viene rilasciato su supporto Smart/SIM Card unitamente al certificato di Firma Digitale. (*)

(*) <https://www.pec.it/CosaFirmaDigitale.aspx>

A cosa serve il certificato di identificazione nello specifico?

Ad accedere ai servizi offerti dall'Ordine ai propri iscritti:

Punto di Accesso

- 335 Telematico
- Fattura Elettronica
- Torino facile
-

Ma serve anche per accedere a portali istituzionali :

- **Programma del CNF delle difese d'ufficio**
- Portale (Ministeriale) dei Servizi Telematici.
- INPS
- Agenzia delle Entrate (fisconline/entratel)
- Equitalia
- Servizi medici ASL
- ...

A cosa serve il certificato di sottoscrizione

- ❑ La firma digitale è l'equivalente informatico di una firma autografa apposta su carta ed ha il suo stesso valore legale. La sua funzione è quella di garantire autenticità, integrità e validità di un documento assicurandone la provenienza e garantendone l'inalterabilità dello stesso, attribuendo ai documenti valore ex. Art. 2702 C.C. .
 - ❑ il destinatario può verificare l'identità del mittente (autenticità);
 - ❑ il mittente non può disconoscere un documento da lui firmato (non ripudio);
 - ❑ il destinatario non può modificare un documento firmato da qualcun altro (integrità).
- ❑ Si basa su un algoritmo a doppia chiave, quella privata contenuta all'interno della chiavetta (protetta dal pin) e usata per firmare digitalmente un documento, e una pubblica "nota a tutti" e usata per verificare la firma apposta sui documenti.

Firmare digitalmente un documento

- Per sottoscrivere digitalmente un documento informatico servono:
 - "*chiavetta*" con certificato di firma non scaduto
 - **un software** (ArubaSign, Dike... sono gratuiti)
- 2 tipi di firma:
 - Formato: "p7m/busta crittografica" CADES
 - **Ai documenti firmati verrà aggiunta l'estensione "p7m"**
 - Formato: "signed/firma pdf" PAdES – solo per documenti in pdf
 - Firma grafica
 - Firma non grafica

Validità temporale della firma digitale

I certificati di firma hanno una durata di almeno 3/4 anni, alla scadenza degli stessi se non rinnovati, non si potrà più apporre firmi digitali su documenti informatici. Tali certificati scadono come un qualunque altro documento in nostro possesso (patente, passaporto...);

Come dare validità temporale ai documenti Informatici?

Associandogli un'attestazione temporale :

- con una Marca temporale
- con una PEC

Procedura di firma con il software ArubaSign

Formato CADES-p7m

ISTANZA ROSSI

Il sig. Rossi Mario nato a

.....

.....

Documento che vogliamo
firmare:
Es. Istanza rossi.pdf



Esito della procedura di Firma istanza rossi.pdf.p7m

ISTANZA ROSSI

Il sig. Rossi Mario nato a

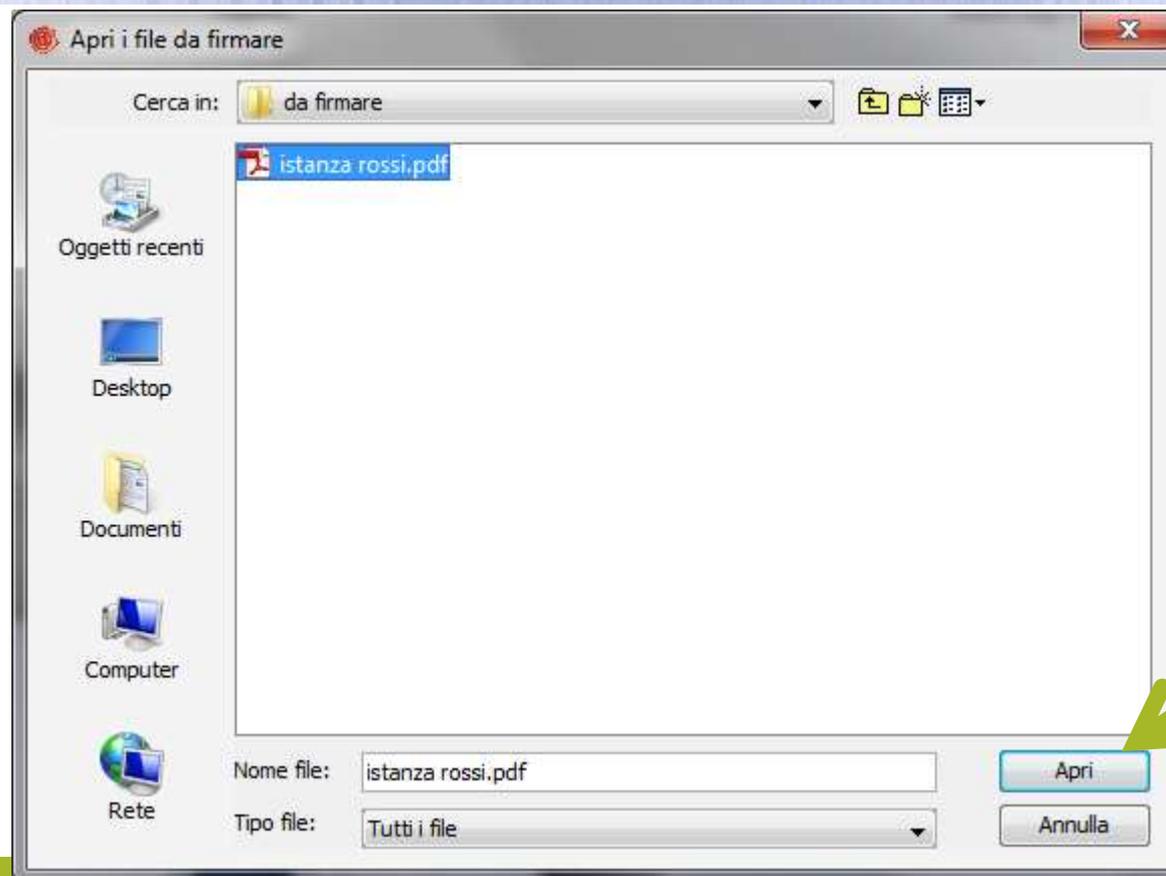
Sul documento non compare
nessun segno grafico
riconducibile al firmatario

The screenshot shows a software interface for document verification. At the top, a green checkmark icon is next to the text "Verifica il tuo documento". Below this, a status bar indicates "Livello 1 (istanza rossi.pdf.p7m) - Tutte le firme Risultano Valide". A list of signatories is shown, with "PAOLO LORENZO LORENZINI" highlighted in a blue box. On the right side, there is a vertical toolbar with several icons, and a red arrow points to the "Apri Contenuto" button. At the bottom, a "Verifica Firmatario" section provides detailed verification results:

- ✓ **La Firma è Integra**
La Firma è in formato Busta Cades
Data-ora di firma dichiarata dal firmatario :08/10/2013 12:21:14
- ✓ **Il certificato è attendibile**
Verifica alla data odierna
- ✓ **Il certificato ha validità legale**
Il certificato è conforme alla direttiva europea 1999/93/EC.
Il certificato è conservato dalla CA per almeno 20 anni.
La chiave privata associata al certificato è memorizzata in un

Procedura di firma con ArubaSign

Formato CADES-p7m



Procedura di firma con ArubaSign Formato P7m - CADES

Firma il tuo documento

Seleziona il Certificato

 PAOLO LORENZO LORENZIN Dettagli

Inserisci Pin

.....

Salva in:

C:\Users\lorenzin\Desktop\da firmare\istanza rossi.pdf.p7m ...

Tipo Busta

Busta Crittografica P7M (CADES)

Richiedi Timestamps

Formato .P7M (con documento firmato e marcato digitalm...)

Indietro Avanti

Procedura di firma con ArubaSign

Formato CADES-P7m

 Firma il tuo documento

Si sta firmando con un certificato a validità legale.
E' necessario esaminare il file prima di poter continuare.

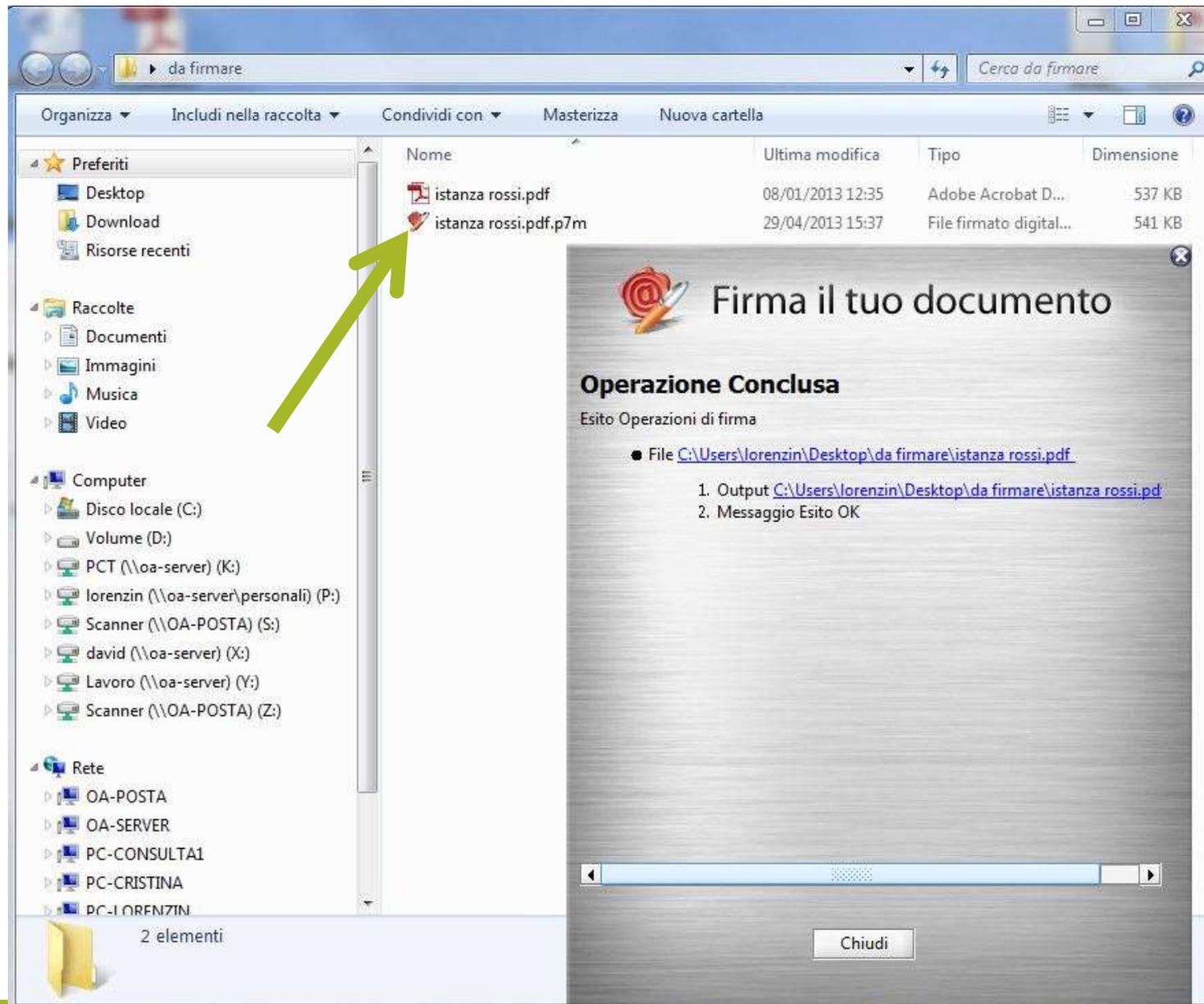
Apri Documento

Dichiaro di aver preso visione del documento, di sottoscriverne il contenuto e di essere consapevole della validità legale della firma apposta.

Indietro Avanti

Procedura di firma con ArubaSign

Formato CADES-P7m



Verifica Firma

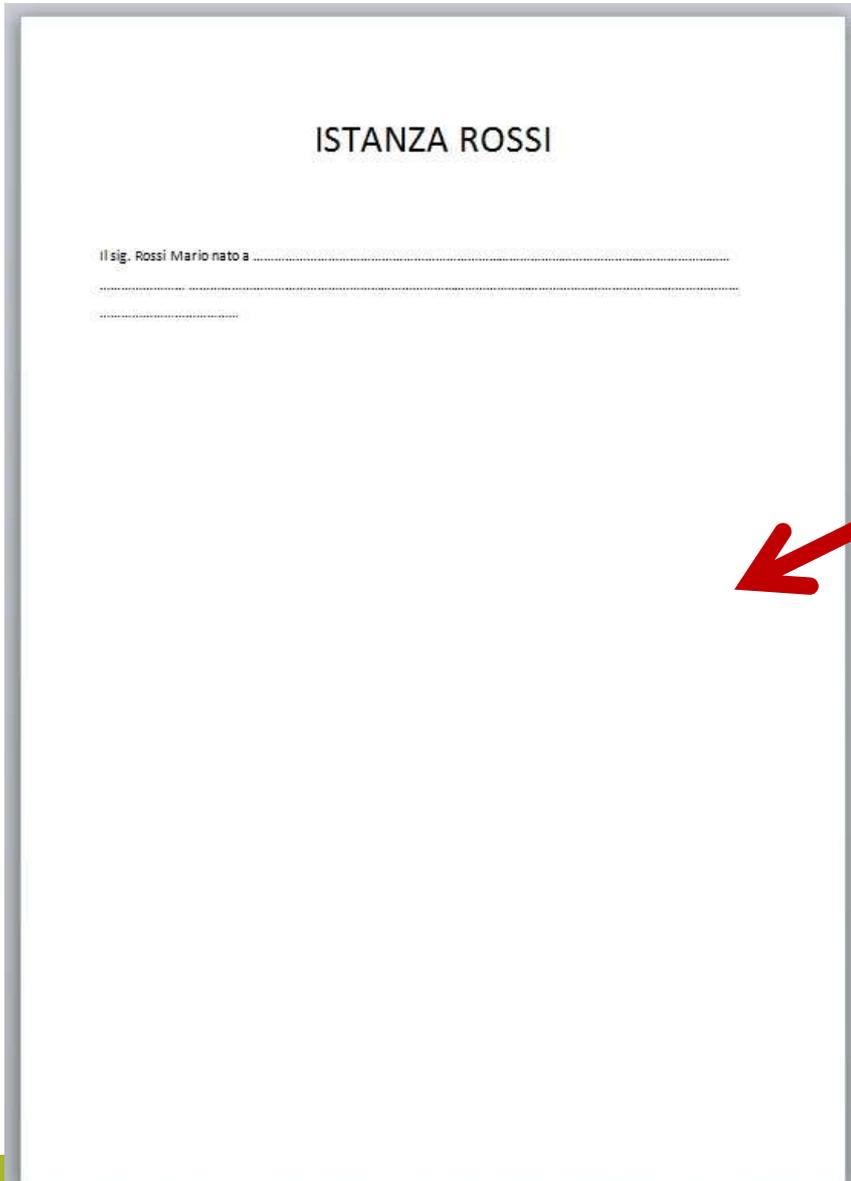
Formato CADES-P7m

The screenshot displays a software window titled "Verifica il tuo documento" (Verify your document). The main area shows the verification results for "Livello 1 (istanza rossi.pdf.p7m) - Tutte le firme Risultano Valide" (Level 1 (instance rossi.pdf.p7m) - All signatures are Valid). A signature by "PAOLO LORENZO LORENZINI" is listed. On the right side, there is a vertical toolbar with icons for document operations, and a file name "istanza rossi.pdf.p7m" is visible. A green arrow points from the toolbar area towards the right. Below the main area, a "Verifica Firmatario" (Verify Signatory) section provides detailed status:

- ✓ **La Firma è Integra**
La Firma è in formato Busta Cades
Data ora di firma dichiarata dal firmatario: 08/10/2012 12:21:14
- ✓ **Il certificato è attendibile**
- ✓ **Il certificato ha validità legale**
Il certificato è conforme alla direttiva europea 1999/93/EC.
Il certificato è conservato dalla CA per almeno 20 anni.
La chiave privata associata al certificato è memorizzata in un

A second green arrow points from the right towards the "Il certificato è attendibile" line.

Visualizzazione del documento firmato istanza rossi.pdf.p7m



Sul documento non compare
nessun segno grafico
riconducibile al firmatario



Procedura di firma con ArubaSign Formato Signed – PADES

Firma il tuo documento

Seleziona il Certificato

PAOLO LORENZO LORENZIN Dettagli

Inserisci Pin

.....

Salva in:

C:\Users\lorenzin\Desktop\istanza rossi\istanza rossi.pdf ...

Tipo Busta

Aggiungi la firma al PDF ←

Richiedi Timestamps

Formato .P7M (con documento firmato e marcato digitalm...)

Firma Grafica ←

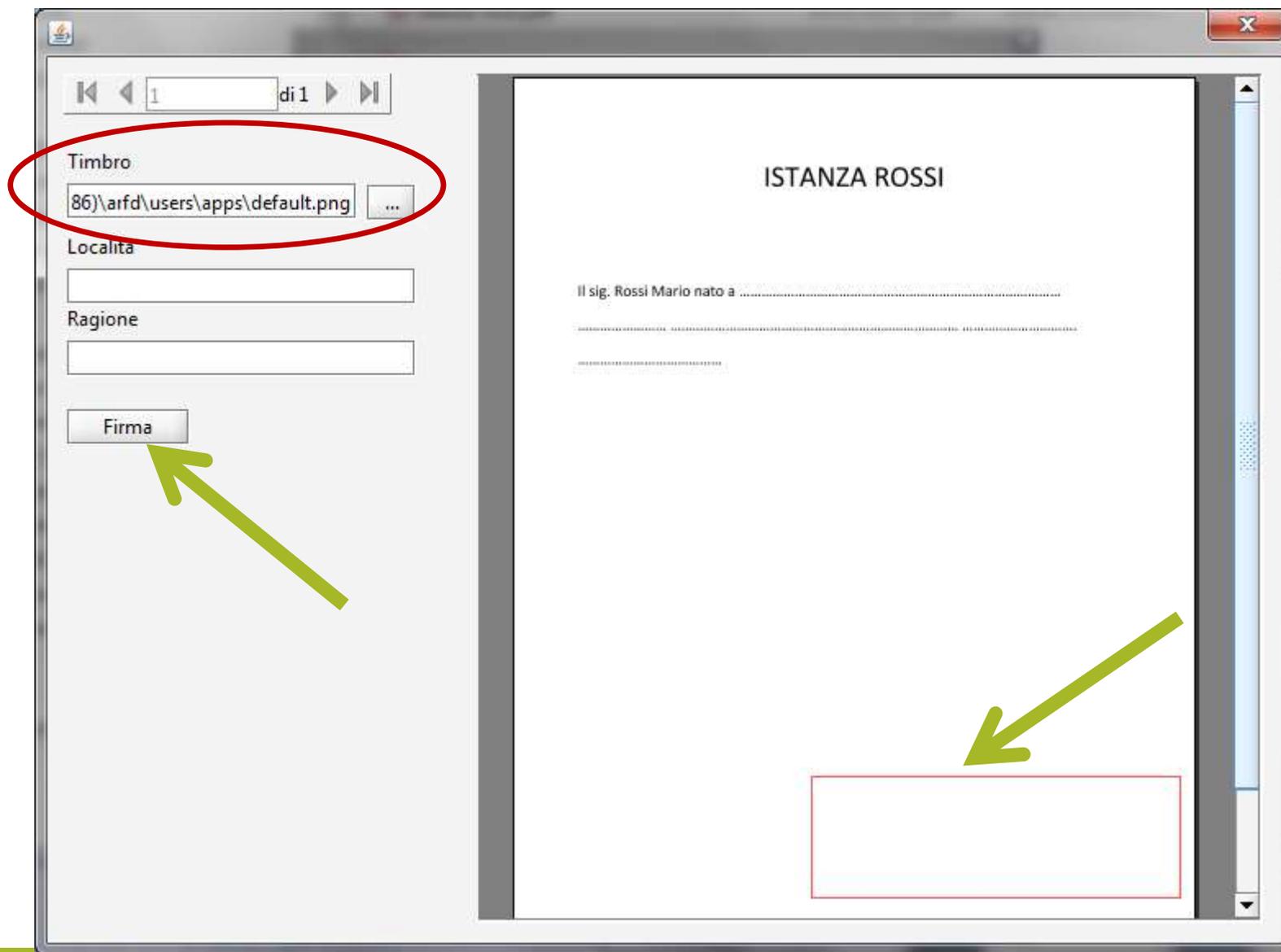
Firma Invisibile

PaperToken

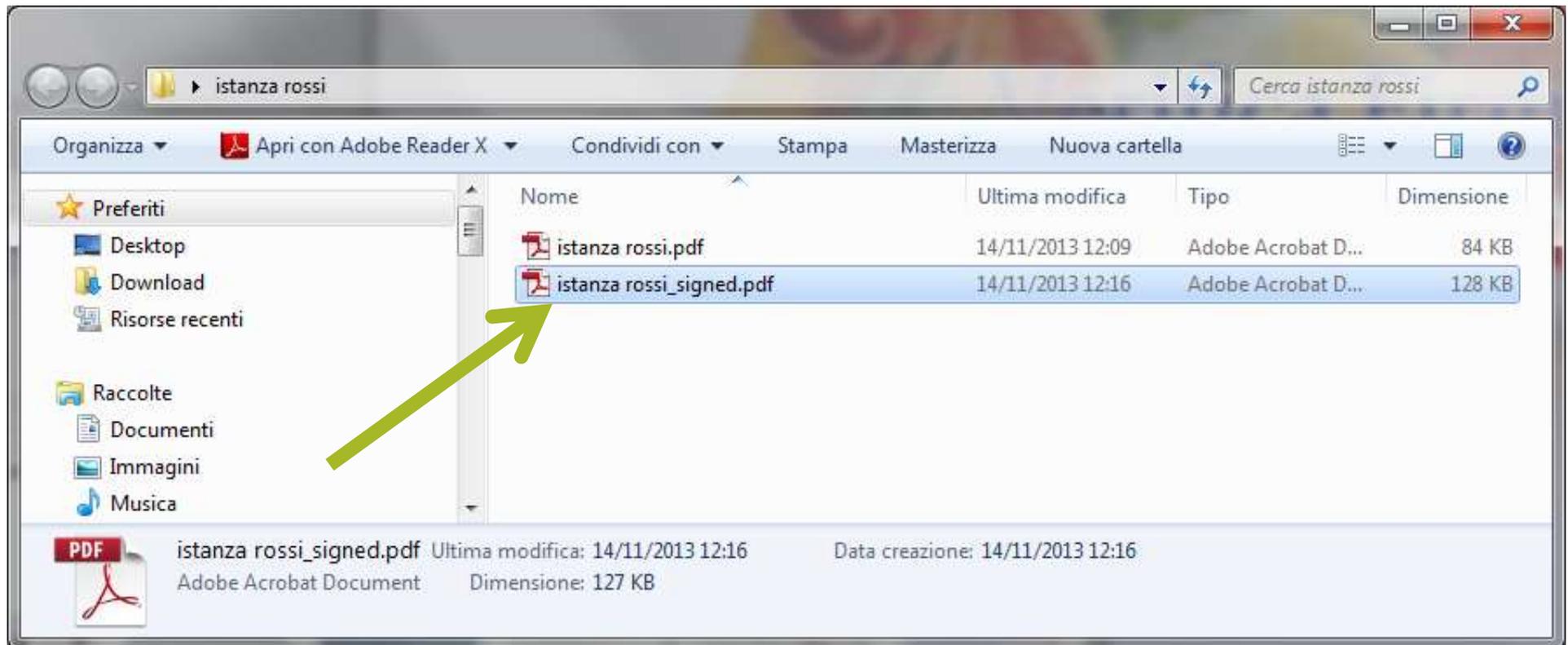
Indietro Avanti

Procedura di firma con ArubaSign

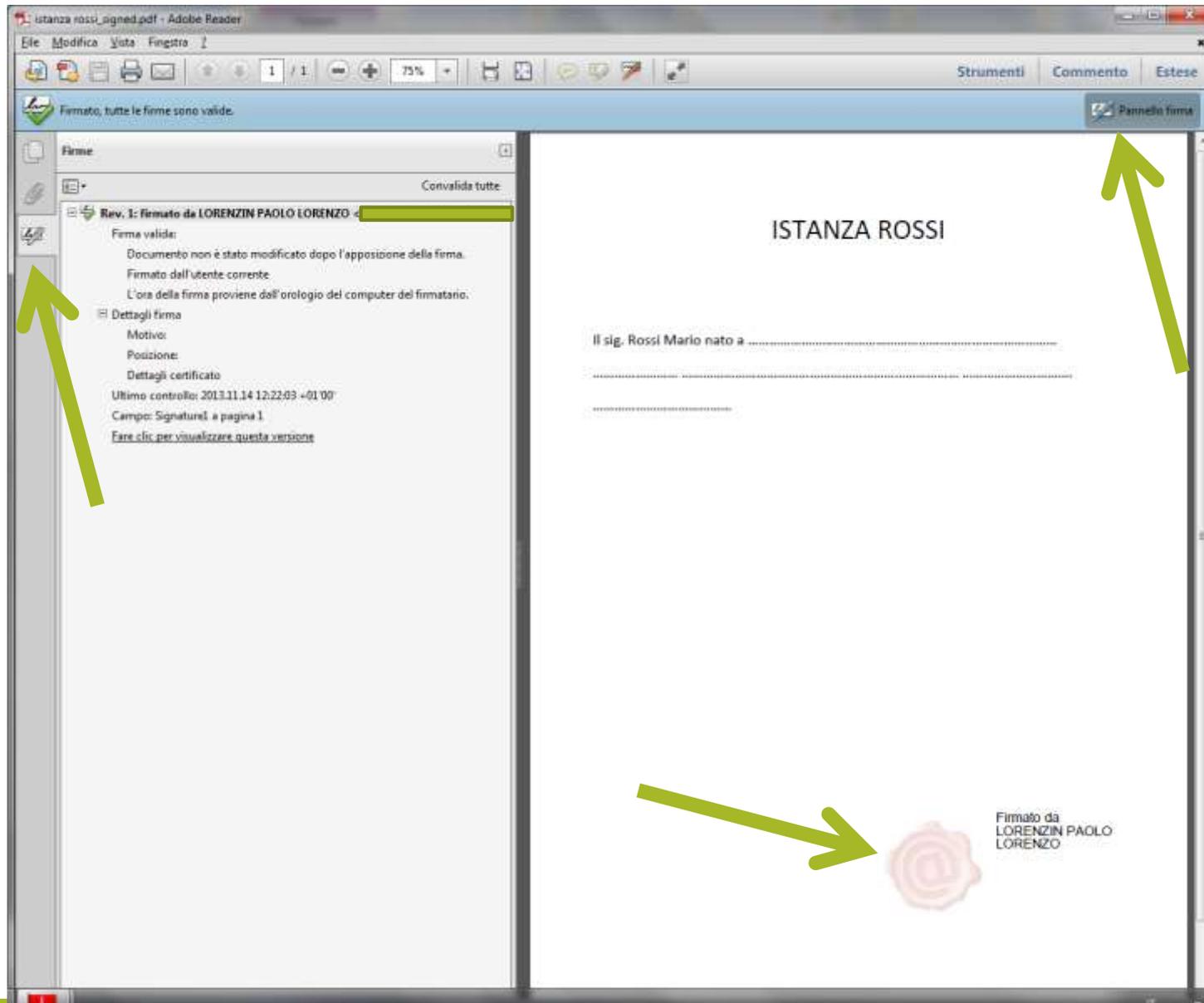
Formato PADES



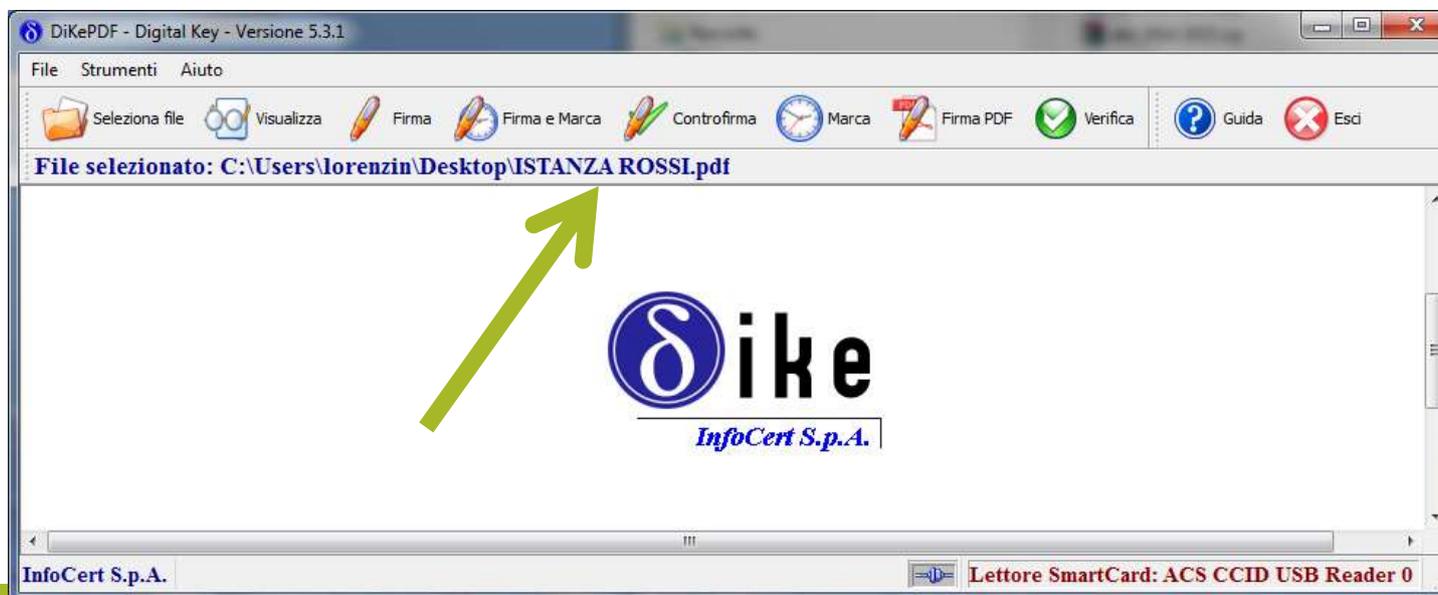
Verifica Firma Formato PADES



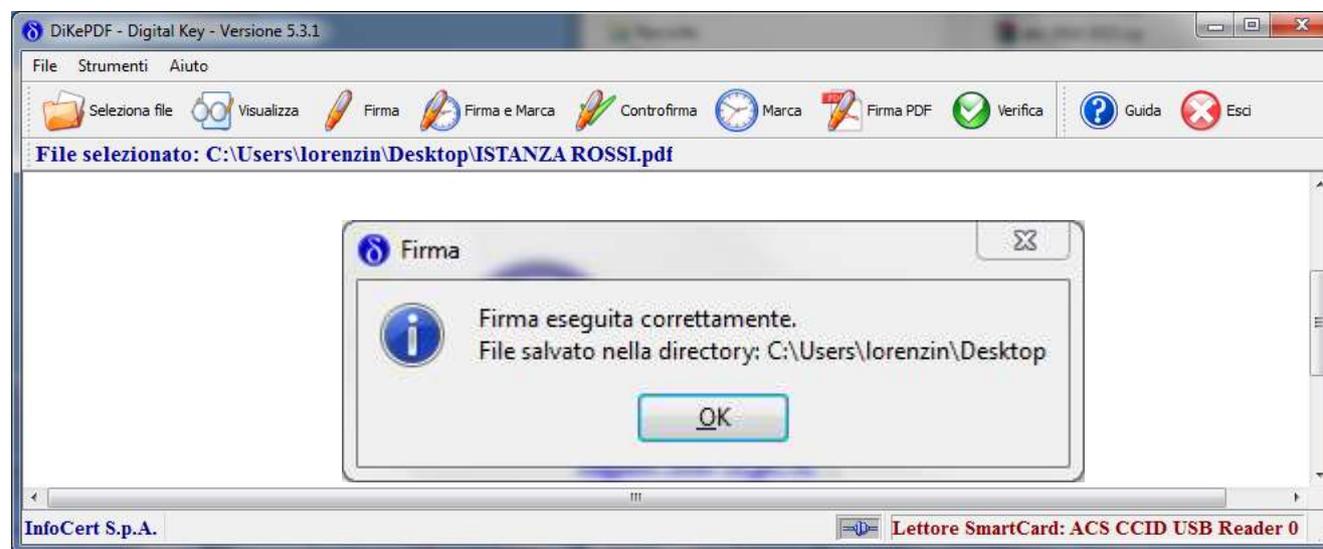
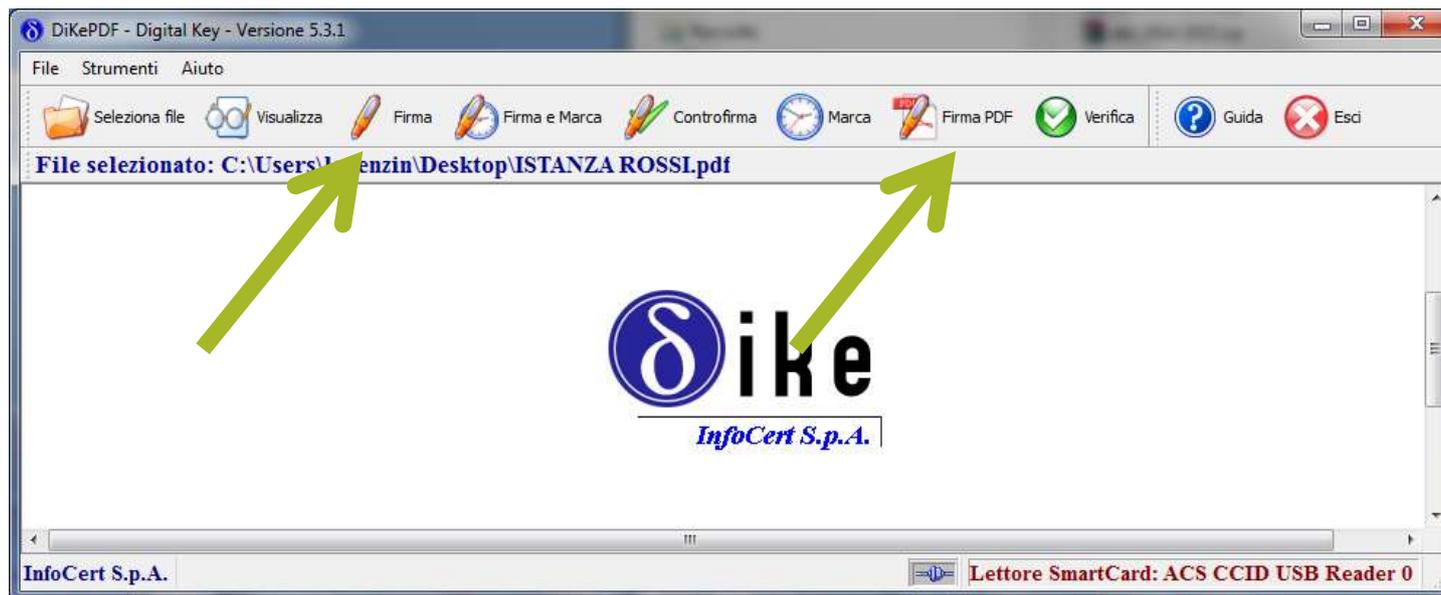
Verifica Firma Formato PADES



Procedura di firma con DikePDF



Procedura di firma con DikePDF





Presentazione preparata dal Dott. Paolo Lorenzin per il Consiglio dell'Ordine degli Avvocati di Torino

(www.ordineavvocatitorino.it/)

Rilasciata con licenza Creative Commons (www.creativecommons.org)
attribuzione - condividi allo stesso modo 3.0 Italia (CC BY-SA 3.0 IT)
<https://creativecommons.org/licenses/by-sa/3.0/it/>