Gli strumenti necessari al PcT

Firma Digitale, PEC e Marca Temporale

Il Processo Civile Telematico

Una serie di servizi telematici sicuri per:

Gli strumenti IT necessari

- Posta elettronica certificata (PEC)
- Firma Digitale

Firma elettronica nel CAD

Nome	Definizione	Esempi
Firma Elettronica	L'insieme dei dati in forma elettronica, logicamente connessi ad altri dati elettronici, utilizzati come metodo di identificazione informatica	Username e password PIN
Firma Elettronica Avanzata	Firma Elettronica + Identificazione del firmatario + Controllo esclusivo del firmatario sul dispositivo di firma	Firma grafometrica Smart card Token USB
Firma Elettronica Qualificata	Firma Elettronica Avanzata + Dispositivo sicuro + Certificato qualificato	Smart card qualificata Token USB qualificato
Firma Digitale	Firma Elettronica Qualificata + Algoritmo di firma basato su un sistema di chiavi asimmetriche, una pubblica e una privata	Smart card qualificata Token USB qualificato

Firma Autografa e Firma Digitale

Componente segreta

Saper disegnare la firma

Possedere la Smart card

LESSICO TECNICO

La componente segreta è detta **chiave privata,** può essere ospitata per esempio in una smart card o in un token USB

Firma Autografa e Firma Digitale

La chiave privata

- Si trova nel chip della smart card
- Non può essere letta (e quindi clonata) in alcun modo
- Nessuno la conosce realmente, neppure chi produce la Smart card

APPROFONDIMENTO TECNICO

Come è possibile eseguire la firma se non è possibile accedere alla chiave privata?

Le operazioni avvengono all'interno del chip, si accede solo ai risultati.

Firma Autografa e Firma Digitale

Identità

Nome e cognome del firmatario

La firma digitale contiene un'identità.

- » Nome cognome.
- » Codice fiscale.

Esito Verifica	Firmatario	Cod. Fiscale
Firma CADES OK	PAOLO PRANDINI	PRNPLA64M03F205W

LESSICO TECNICO
L'identità del firmatario è contenuta nel **certificato di firma** o **chiave pubblica.**
La firma digitale garantisce **autenticità.**

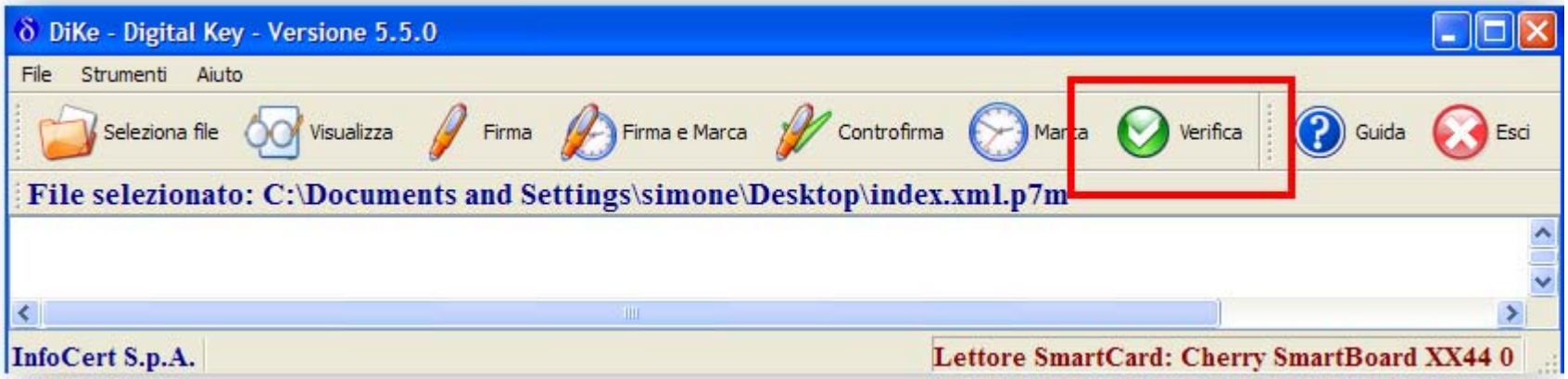
Firma Autografa e Firma Digitale

Verifica della firma

Riconosco la corretta geometria della firma

Eseguo un calcolo matematico

» Es. La prova del nove



Firma Autografa e Firma Digitale

Falsificazione della firma

Semplice

- Mai falsificato una giustifica a scuola?

Impossibile

» Senza essere scoperti

Firma Autografa e Firma Digitale

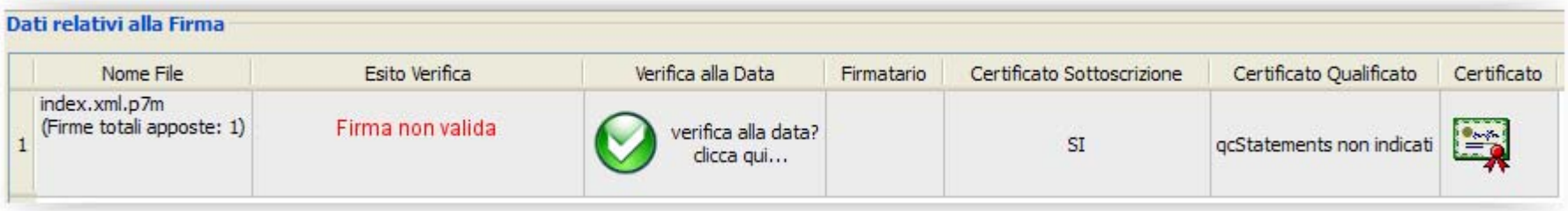
Rilevazione del falso

Difficile

- Serve un perito calligrafico

Semplice

» Basta eseguire un calcolo matematico



Dati relativi alla Firma

	Nome File	Esito Verifica	Verifica alla Data	Firmatario	Certificato Sottoscrizione	Certificato Qualificato	Certificato
1	index.xml.p7m (Firme totali apposte: 1)	Firma non valida	verifica alla data? clicca qui...		SI	qcStatements non indicati	

Firma Autografa e Firma Digitale

Una delega in bianco

È possibile

Non è possibile

La firma è invalidata da una qualsiasi modifica

- del documento firmato
- dell'identità del firmatario

LESSICO TECNICO
La firma digitale garantisce le proprietà di **integrità** e **non ripudio**

Non ripudio

- Solo l’intestatario della firma digitale può eseguire la firma
- Nessuno può clonare la smart card, nemmeno chi l’ha prodotta
- **Non posso disconoscere la paternità di un documento firmato**
- Conservare la Smart card in un luogo sicuro
- Attenzione alla firma remota!

Ripudio in sede di giudizio

Nome	Ripudiabile in sede di giudizio
Firma Elettronica	Non riconoscimento
Firma Elettronica Avanzata	Non riconoscimento
Firma Elettronica Qualificata	Querela di falso
Firma Digitale	Querela di falso

Enti certificatori accreditati

Chi garantisce l'identità del firmatario?

Nessuno

L'ente che rilascia il certificato di firma

Mi devo **fidare** dell'ente certificatore

Esiste un elenco di certificatori accreditati

http://www.agid.gov.it/identita-digitali/firme-elettroniche/certificatori-attivi

Enti certificatori accreditati

In che modo l'ente garantisce l'identità?

Firma digitalmente il certificato di firma.

LESSICO TECNICO
Si compone una **catena di certificati.**

L'ente certificatore è detto **Certification Autority,** abbreviato **CA**

Il certificato di firma

- Ha una data di scadenza
- Ha una data di inizio validità

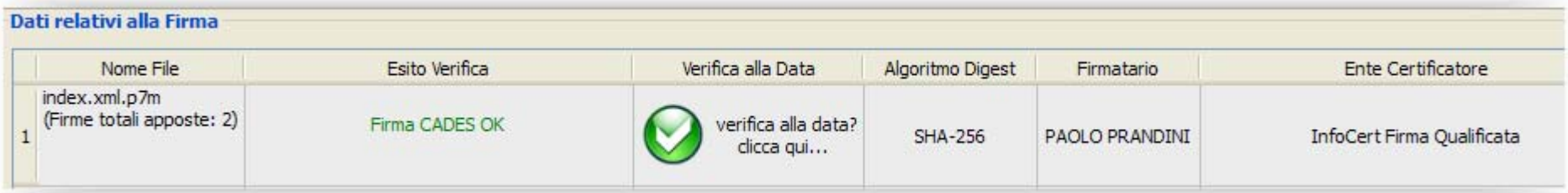
Per essere valido (ad una certa data)

- Non deve essere scaduto
- Deve essere valida la firma della CA
- Non deve essere scaduto il certificato della CA

Valore probatorio

Una firma digitale è valida se:

- È tecnicamente corretta
- Il certificato non è scaduto (Anche della CA)
- Il certificato è rilasciato da un ente accreditato



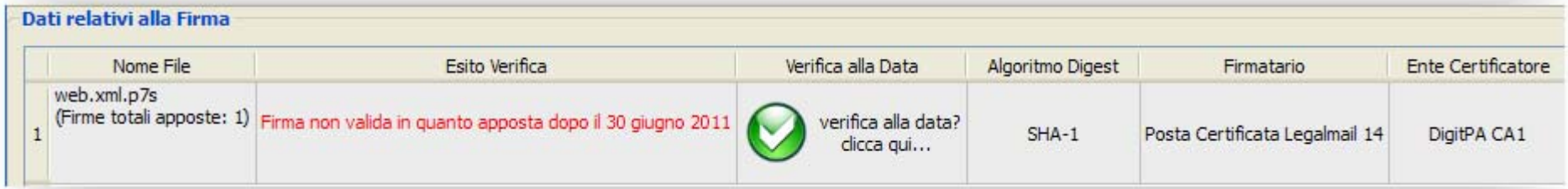
Dati relativi alla Firma

	Nome File	Esito Verifica	Verifica alla Data	Algoritmo Digest	Firmatario	Ente Certificatore
1	index.xml.p7m (Firme totali apposte: 2)	Firma CADES OK	verifica alla data? clicca qui...	SHA-256	PAOLO PRANDINI	InfoCert Firma Qualificata

Valore probatorio

Una firma digitale è valida se:

- Usa gli algoritmi giusti
  - DPCM 22 febbraio 2013



Dati relativi alla Firma

	Nome File	Esito Verifica	Verifica alla Data	Algoritmo Digest	Firmatario	Ente Certificatore
1	web.xml.p7s (Firme totali apposte: 1)	Firma non valida in quanto apposta dopo il 30 giugno 2011	verifica alla data? clicca qui...	SHA-1	Posta Certificata Legalmail 14	DigitPA CA1

LESSICO TECNICO

Si utilizza **SHA-256** come algoritmo di HASH (a sostituzione di SHA-1) e **RSA** con chiave privata di almeno **1024 bit** come algoritmo di cifratura.

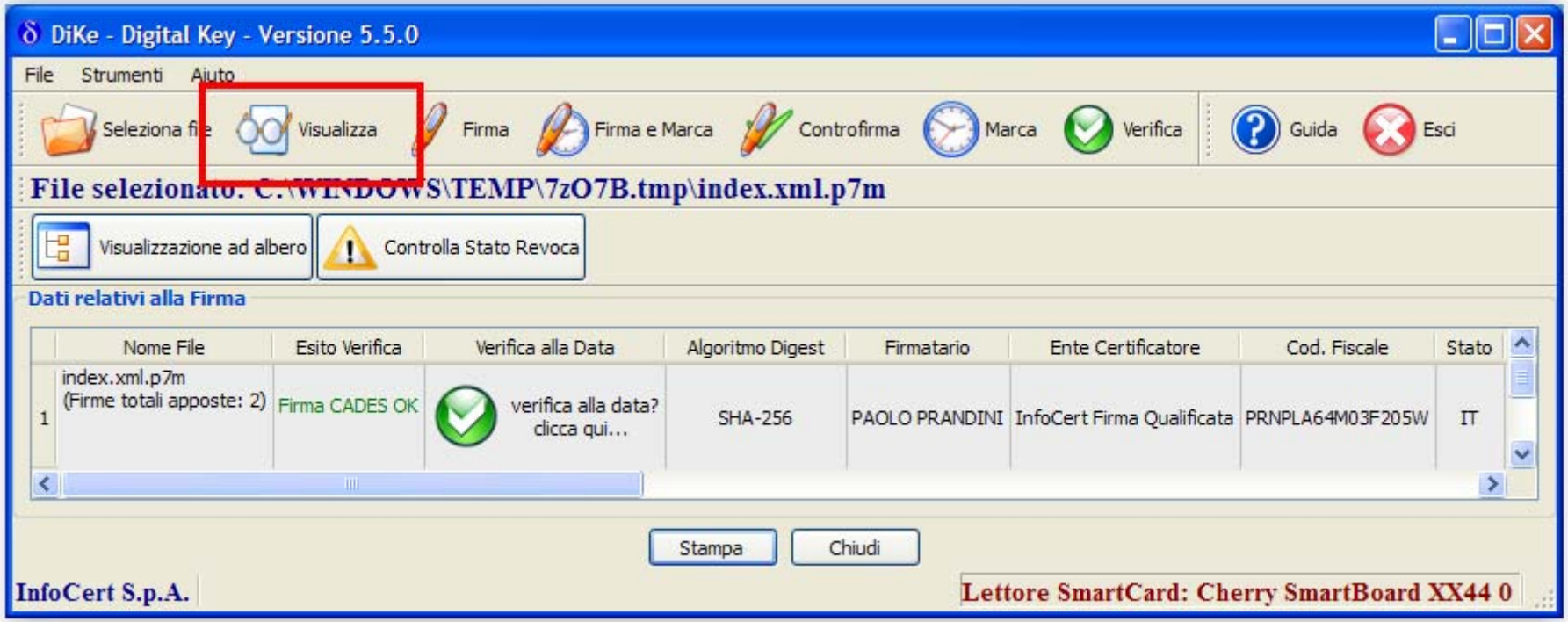
File firmati digitalmente

- P7M
  - È un contenitore, che può ospitare un qualsiasi file (Detto anche busta crittografica)
  - Serve un programma apposito in grado di leggere la busta ed aprirla per estrarre il file
  - Esempio:

    documento.pdf.p7m

LESSICO TECNICO
Il formato di firma utilizzato per produrre file p7m è **CAdES-BES**

File firmati digitalmente

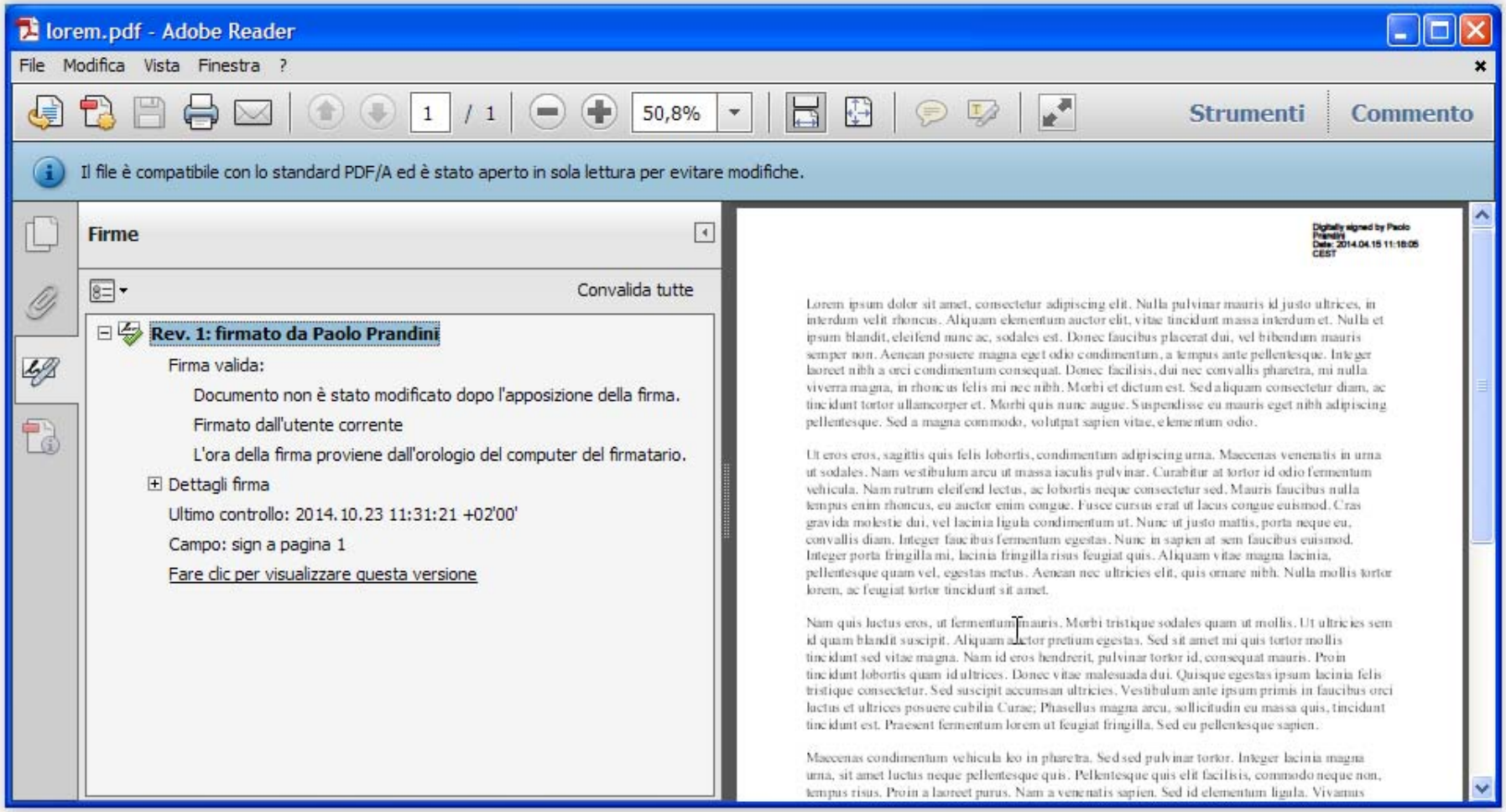


File firmati digitalmente

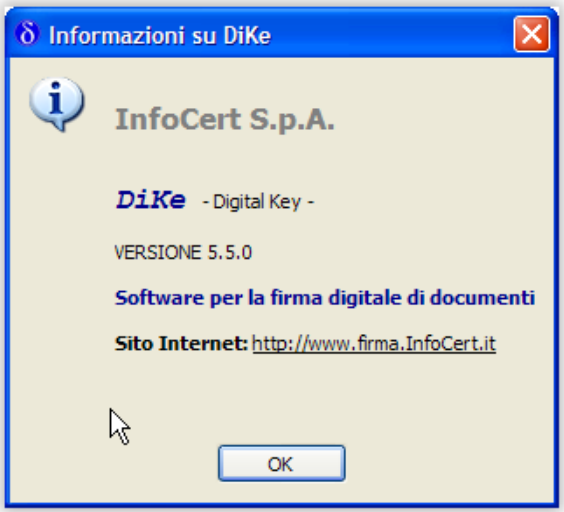
- PDF
  - Il formato PDF supporta nativamente la firma digitale.
  - La firma è inserita direttamente all'interno del PDF
  - Un qualsiasi lettore PDF (Adobe Acrobat Reader) è in grado di aprire il file

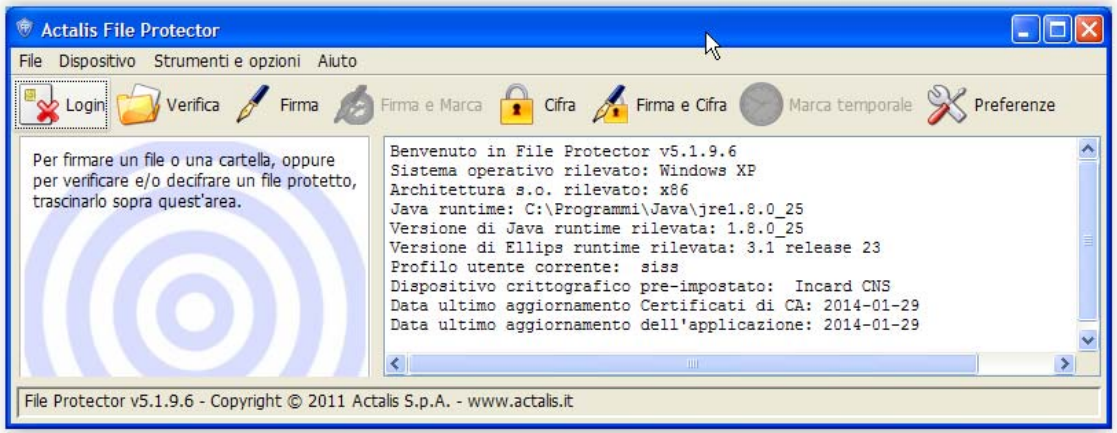
LESSICO TECNICO
Il formato di firma utilizzato per produrre file PDF firmati è **PAdES-BES**

File firmati digitalmente



Programmi per la firma





PEC Posta Elettronica Certificata

Esempio della raccomandata

Attori

Mittente

Mittente

Destinatario

Destinatario

Ufficio postale mittente

Gestore PEC mittente

Ufficio postale destinatario

Gestore PEC destinatario

Esempio della raccomandata

Mittente invia un messaggio

Ufficio postale mittente rilascia una ricevuta

Mittente invia una PEC

Gestore PEC mittente ritorna una ricevuta

Esempio della raccomandata

Ufficio postale dest. riceve un messaggio

Ufficio postale dest. consegna il messaggio

Destinatario rilascia una ricevuta

Gestore PEC dest. riceve un messaggio

Gestore PEC dest. consegna il messaggio

Gestore PEC dest. rilascia una ricevuta

PEC e Firma elettronica avanzata

- Il gestore PEC mittente applica la sua firma elettronica avanzata al messaggio.
- Il gestore PEC destinatario verifica l'integrità della firma.
- Anche le ricevute sono firmate elettronicamente dai gestori.

Importanza della Firma Elettronica

- Una e-mail tradizionale non ha alcun valore probatorio!
- La notifica di lettura di una e-mail tradizionale non ha alcun valore probatorio!

POSSONO ESSERE FALSIFICATE

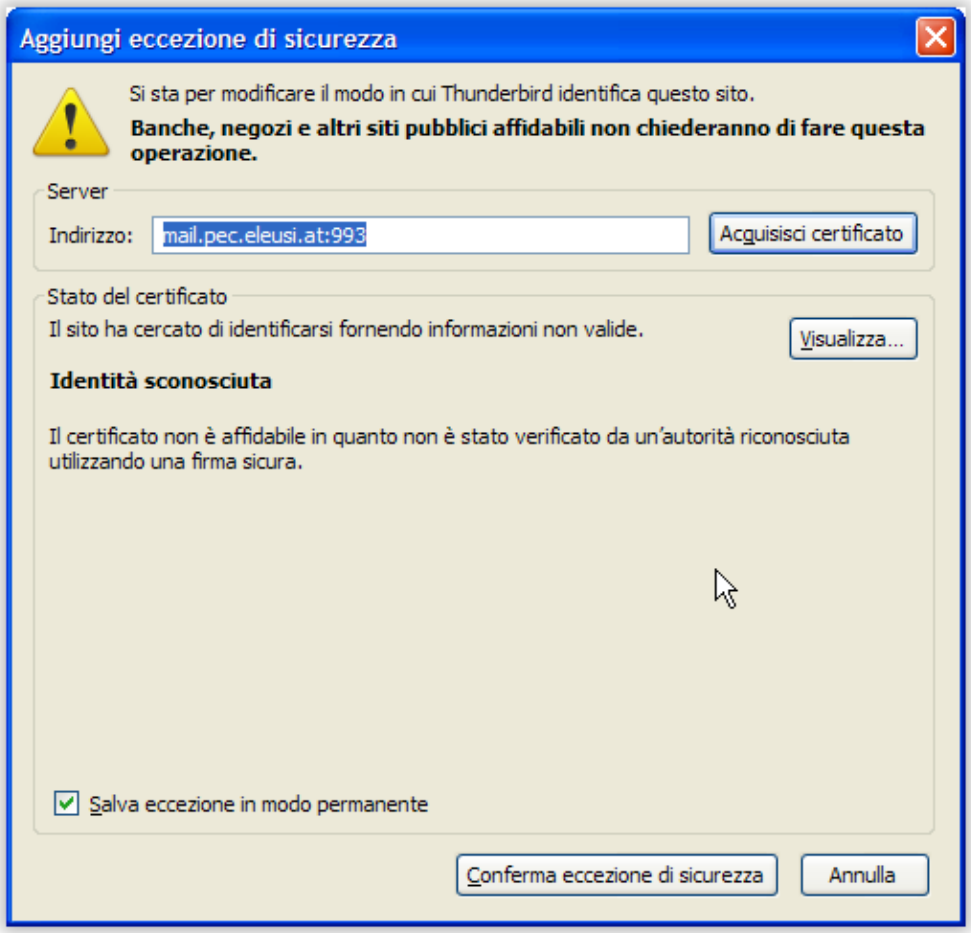
Importanza della Firma Elettronica

- Un messaggio PEC non può essere falsificato
- Una ricevuta PEC non può essere falsificata

Perché non può essere falsificata

LA FIRMA ELETTRONICA

Don’t worry


Aggiungi eccezione di sicurezza
Si sta per modificare il modo in cui Thunderbird identifica questo sito.
Banche, negozi e altri siti pubblici affidabili non chiederanno di fare questa operazione.
Server
Indirizzo:
mail.pec.eleusi.at:993
Acquisisci certificato
Stato del certificato
Il sito ha cercato di identificarsi fornendo informazioni non valide.
Visualizza...
Identità sconosciuta
Il certificato non è affidabile in quanto non è stato verificato da un'autorità riconosciuta utilizzando una firma sicura.
Salva eccezione in modo permanente
Conferma eccezione di sicurezza
Annulla

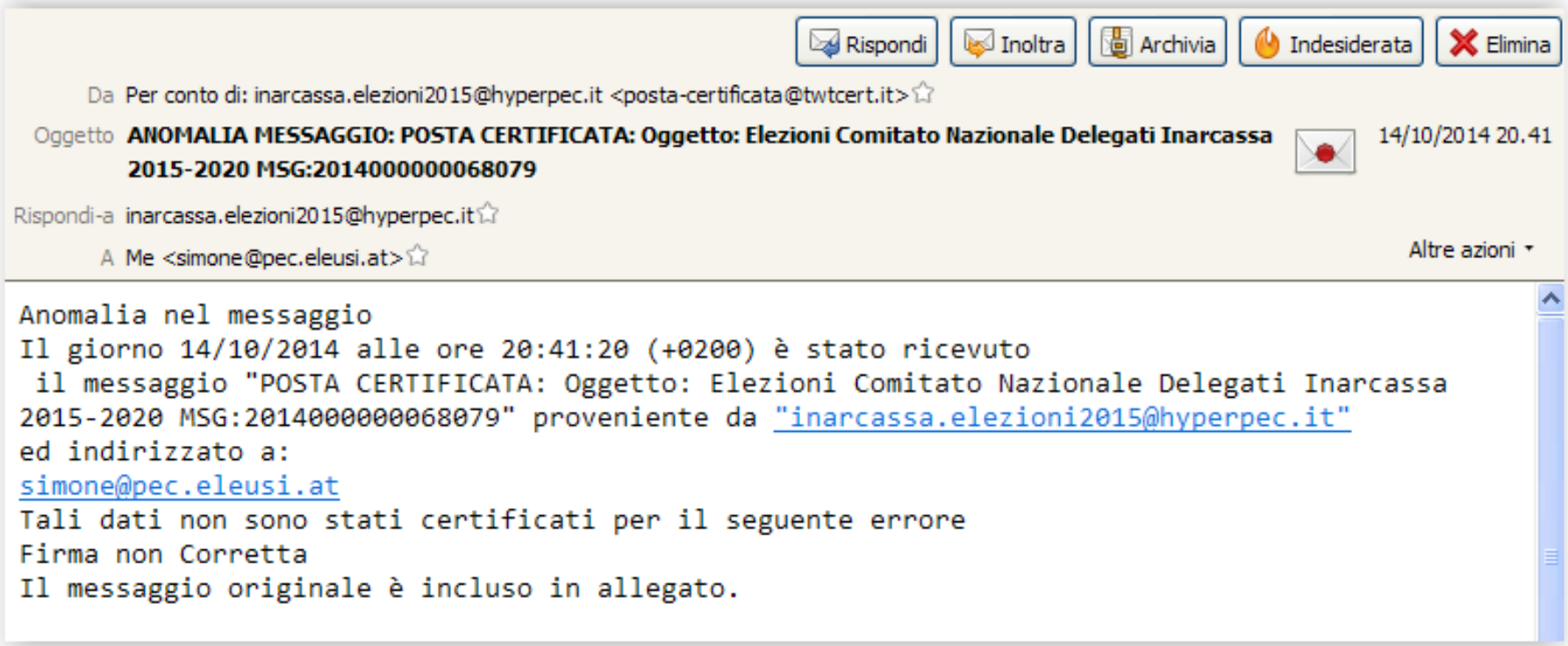
Don’t worry

- Il certificato di firma del gestore non è qualificato
- Devo confermare manualmente la mia fiducia in esso

La PEC è comunque valida?

SÌ, è sufficiente che la firma digitale sia **ELETTRONICA AVANZATA**

Un esempio da non imitare…



CEC-PAC

- **C**omunicazione **E**lettronica **C**ertificata tra la **P**ubblica **A**mministrazione e il **C**ittadino

- È una tipologia di Posta Certificata gratuita per il cittadino (Es: *mio_nome@postacertificata.gov.it)*
- Consente di dialogare esclusivamente con la Pubblica Amministrazione
- La CEC-PAC non è sufficiente al fine di rispettare l'obbligo di dotarsi di una casella PEC introdotto per società, professionisti e Pubbliche Amministrazioni.

Dove reperire gli indirizzi PEC

- **Re**gistro **G**enerale **Ind**irizzi **E**lettronici
- Consultabile all'indirizzo pst.giustizia.it

- Indice delle Pubbliche Amministrazioni
- Consultabile all'indirizzo www.indicepa.gov.it

- INI-PEC www.inipec.gov.it/
- Mette a disposizione indirizzi di professionisti e imprese

Marca Temporale

- Esempio del Timbro Postale
- Attesta l'integrità del documento ad un certo istante di tempo.

Marca sulla Firma OK Data Marca: 15/07/2014 09.06.05 (UTC Time)		SHA-256	Time Stamp Server	Servizio di Certificazione per la Marcatura Temporale

Facciamo un esempio

Voglio dimostrare che il documento contratto.pdf.p7m il giorno 15/07/2014 esisteva e conteneva le clausole 1,2,3 e 4

Dati relativi alla Firma

	Nome File	Esito Verifica	Verifica alla Data	Algoritmo Digest	Firmatario	Ente Certificatore
1	contratto.pdf.p7m (Firme totali apposte: 2)	Marca sulla Firma OK Data Marca: 15/07/2014 07.24.29 (UTC Time)		SHA-256	Time Stamp Server	Servizio di Certificazione per la Marcatura Temporale

Prova informatica inconfutabile

Marca Temporale

Chi mi assicura che la data non sia stata falsificata?

Mi devo fidare di chi ha eseguito la marca temporale.

Servono degli enti fidati

Timestamp Authority

Chi esegue la marca temporale?

- Un ente fidato.
- Non è l'utente!

- Una TSA (TimeStamp Authority).
- La TSA è un ente certificato.

File marcati temporalmente

- P7M
  - È la busta crittografica
  - Può contenere anche una marca

Dati relativi alla Firma

	Nome File	Esito Verifica	Verifica alla Data	Algoritmo Digest	Firmatario	Ente Certificatore
1	index.xml.p7m (Firme totali apposte: 2)	Firma CADES OK	verifica alla data? clicca qui...	SHA-256	PAOLO PRANDINI	InfoCert Firma Qualificata
2		Marca sulla Firma OK Data Marca: 15/07/2014 09.06.05 (UTC Time)		SHA-256	Time Stamp Server	Servizio di Certificazione per la Marcatura Temporale

File marcati temporalmente

- M7M
  - Concettualmente è simile al formato P7M
  - Tecnicamente no…

Dati relativi alla Firma

	Nome File	Esito Verifica	Verifica alla Data	Algoritmo Digest	Firmatario	Ente Certificatore
1	index.xml.p7m (Firme totali apposte: 2)	Firma CADES OK	verifica alla data? clicca qui…	SHA-256	PAOLO PRANDINI	InfoCert Firma Qualificata
2		Marca sulla Firma OK Data Marca: 15/07/2014 09.06.05 (UTC Time)		SHA-256	Time Stamp Server	Servizio di Certificazione per la Marcatura Temporale

File marcati temporalmente

- PDF
  - Il formato PDF supporta nativamente la marca temporale
  - La Marca è inserita direttamente nel file PDF

LESSICO TECNICO
Il formato di firma utilizzato per produrre file PDF firmati e marcati è **PAdES-T**

Gli Strumenti necessari al PcT

Grazie per l'attenzione!