



# LA FIRMA DIGITALE

1 dicembre 2017



*Miriam Colantonio*



- ✓ ~~Modulo 1 - Dematerializzazione dei processi amministrativi~~
- ✓ Modulo 2 - Firma elettronica (1/12/2017);
- ✓ Modulo 3 - Posta elettronica certificata (4/12/2017);
- ✓ Modulo 4 - Protocollo informatico (11/12/2017).

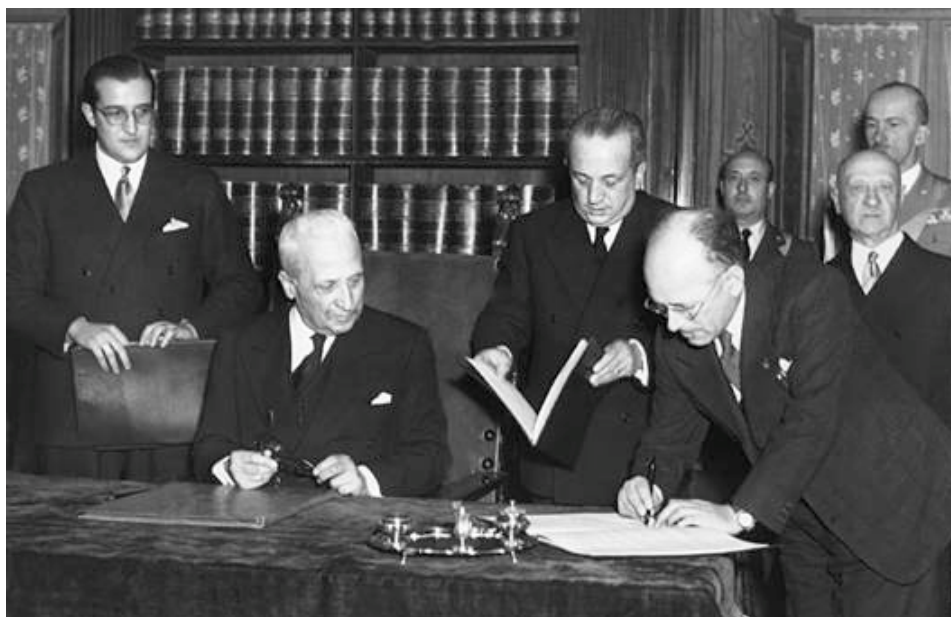
## I flussi di ieri e di oggi



Se dopo oltre dieci anni di firme e documenti informatici siamo qui...evidentemente c'è (almeno) un problema...

Si è pensato più al "come" che al "perché"

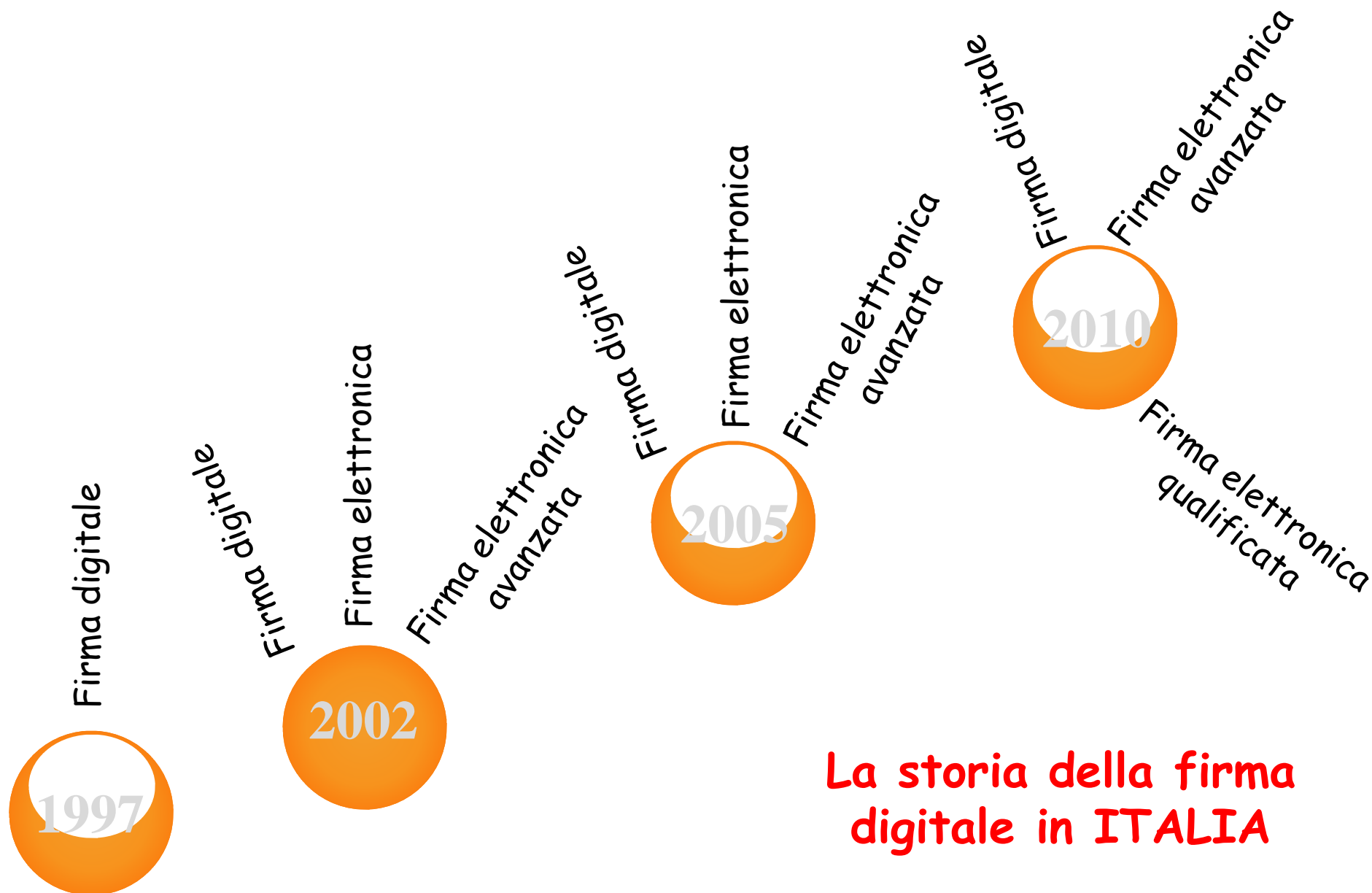
# La firma autografa



## Quadro Normativo

- Legge n.59/97: Doc. cartaceo  $\longleftrightarrow$  Doc. informatico
- D.P.R. 513/97: Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici.
- D.P.C.M 8/2/99: Regole tecniche sulla materia.
- Circolare AIPA n.22 del 22/07/1999: Modalità di iscrizione all'albo dei Certificatori
- Circolare AIPA n.24 del 19/06/2000: Linee guida sull'interoperabilità dei Certificatori

- T.U. 28/12/2000 n.445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- D.lgs 23/01/2002, n.10 e D.P.R. 137 7/04/2003 Recepimento della direttiva 1999/93/CE;
- D.P.C.M. 13/01/04 Nuove regole tecniche;
- D.P.R. 68/2005 Regolamento recante disposizioni per l'utilizzo della Posta Elettronica Certificata



**La storia della firma  
digitale in ITALIA**



## Firme elettroniche e strumenti

Firma  
Elettronica



Firma  
Elettronica  
Avanzata



Firma  
Elettronica  
Qualificata



Firma  
Digitale



## Art. 21. - CAD

(Valore probatorio del documento informatico sottoscritto)



Tipologia	Definizione	Valore probatorio	Tecnologia	Esempi
<b>Firma Elettronica</b>	Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica	Efficacia probatoria valutabile dal giudice caso per caso	Neutra	PIN, firma biometrica, UserID e Password
<b>Firma Elettronica Avanzata</b>	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati	Efficacia probatoria della scrittura privata integra la forma scritta <i>ad substantiam</i> tranne che per i contratti immobiliari	Neutra	Firma grafometrica su tablet, PEC verso la PA.
<b>Firma Elettronica Qualificata</b>	Particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma	Efficacia probatoria della scrittura privata integra la forma scritta <i>ad substantiam</i>	Non neutra, certificato qualificato e dispositivo sicuro	Smart-card, token USB
<b>Firma Elettronica Digitale</b>	Particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico	Efficacia probatoria della scrittura privata integra la forma scritta <i>ad substantiam</i>	Non neutra, certificato qualificato chiavi asimmetriche e dispositivo sicuro	Smart-card, token USB, MicroSD, Firma remota

**La firma digitale**, è definita dall'articolo 1 comma 1 lettera b) del D.P.R. 513/97 come *“il risultato della procedura informatica (validazione) basata su un sistema di **chiavi** asimmetriche a coppia, una **pubblica** e una **privata**, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica rispettivamente di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici”*.

Quindi:

- la **firma digitale** è un particolare tipo di firma elettronica basata su un certificato qualificato e su una coppia di chiavi pubblica e privata che associate al documento informatico attestano con certezza

l'integrità

l'autenticità

la validità,

la veridicità

la paternità dello stesso.



## Chiave privata

deve essere conosciuta solo dal titolare e viene utilizzata per apporre la firma sul documento, è custodita all'interno di una smart card(=carta munita di un chip elettronico) e protetta da un codice segreto che conosce solo lui (PIN =personal identification number).

## Chiave pubblica



Anch'essa associata al titolare, è contenuta in «un certificato digitale» custodito all'interno di una smart card e viene utilizzata per verificare che la firma digitale apposta sul documento informatico provenga dal titolare della coppia di chiavi.

## Certificato digitale di sottoscrizione

La definizione a livello europeo è la seguente: "un attestato digitale che collega un dispositivo di verifica della firma ad una data persona ne conferma l'identità

..... è un **documento d'identità** nel mondo digitale nel quale viene dichiarata la corrispondenza tra un soggetto (persona fisica/giuridica) e la propria chiave e consente la firma digitale.



Nel certificato compare:

- nome del titolare
- codice fiscale
- validità temporale
- ente certificatore
- ecc.

Il certificato di autenticazione è un file rilasciato dall'Ente Certificatore che permette di:

- Firmare la propria posta elettronica
- Connessione sicura con un sito web (SSL3)
- Autenticazione ai siti web per identificazione (Ex user/pwd)
- Autenticazione Microsoft SmartLogon
- CNS (Autenticazione ai servizi web della Pubblica Amm.)



# Azioni preliminari del processo di firma

1. Registrazione dell'utente presso un'autorità di certificazione (quest'ultima garantisce la correttezza e l'inviolabilità dell'associazione tra la chiave pubblica ed il titolare) – AGID= Agenzia per l'Italia Digitale link dove si possono trovare gli Enti certificazione <http://www.agid.gov.it/certificatori-firma-digitale-accreditati-italia>;
2. Generazione di una coppia di chiavi pubblica-privata
3. Certificazione della chiave pubblica.
4. Registrazione e pubblicazione della chiave pubblica

## Durante la validità

- L'utente può firmare documenti con la propria chiave privata fino alla scadenza del certificato
- La validità della chiave può essere revocata in ogni momento a seguito di compromissione (anche solo sospettata) della chiave privata

# Durata della certificazione

Primo rilascio: dal momento di verifica dell'autenticità della persona

Rinnovo: dipende dall'ente di certificazione

IL CERTIFICATO PUO' ESSERE REVOCATO ED EQUIVALE AD  
UNA NORMALE SCADENZA

QUANDO UN CERTIFICATO SCADE TUTTI I DOCUMENTI  
FIRMATI **SUCCESSIVAMENTE** CON QUEL CERTIFICATO  
NON HANNO PIU' ALCUNA VALIDITA'

# Strumenti



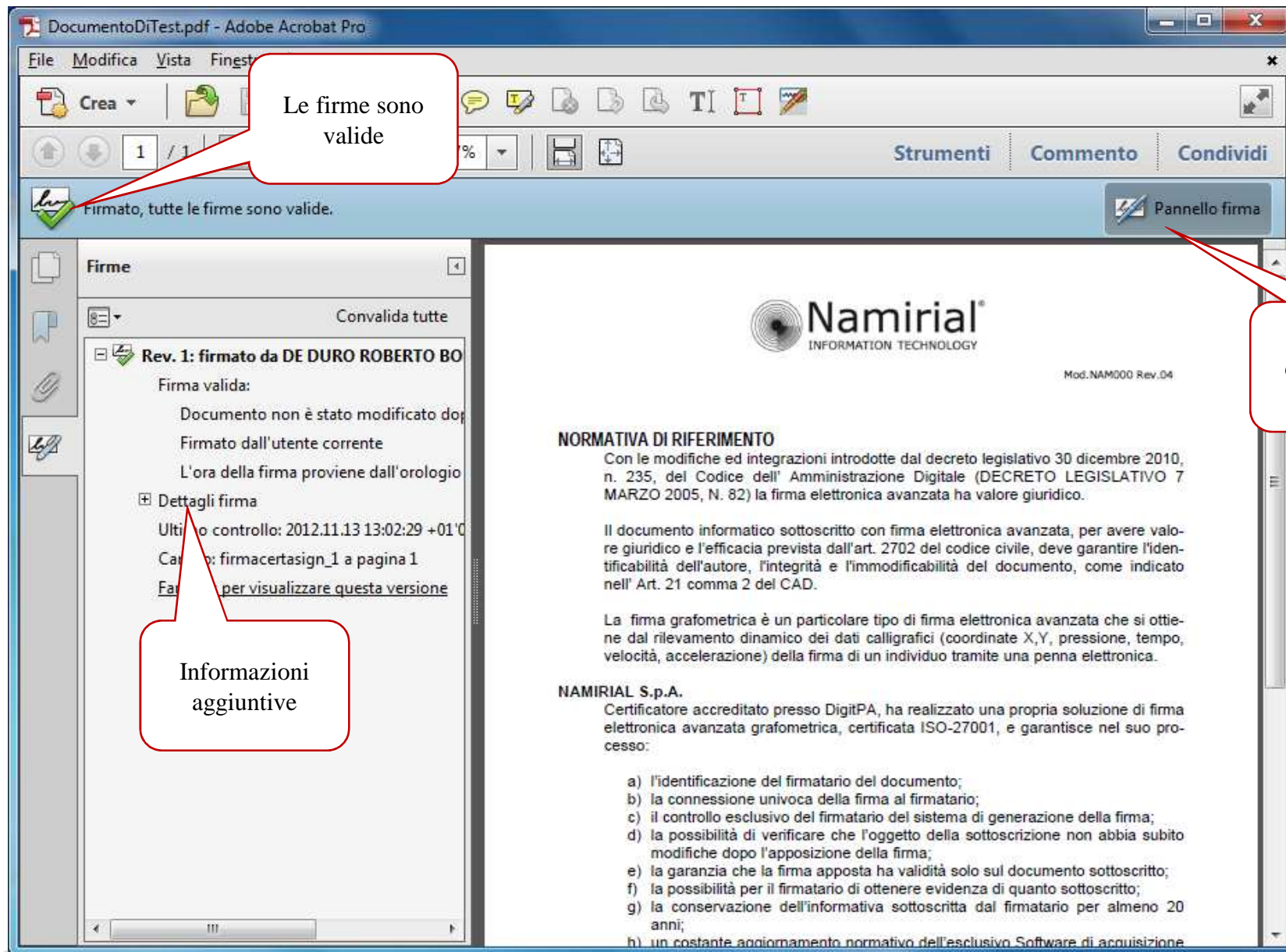
**Business key**

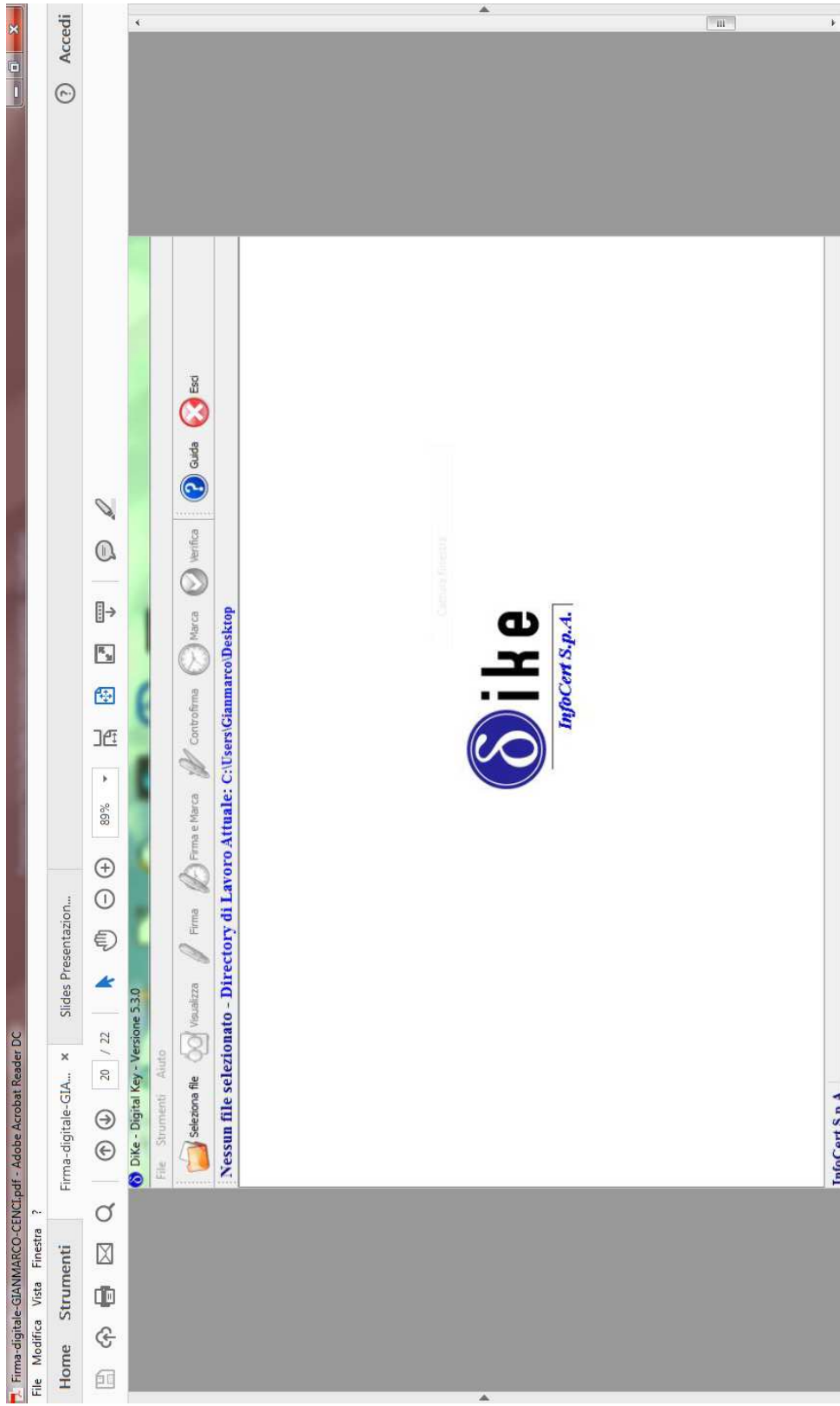


**Smart card +lettore**

## Modalità di firma dei documenti:

CADES estensione **.pdf.p7m**: Il file si firma e si legge con i SW di firma (DiKe, File Protector,...);





Verifica il file "

verbale\_chiusura\_negoziazione\_...

✕

✓

Firmato da [REDACTED]

La firma e' stata verificata correttamente

Dettagli ▾

⚠

Firma di [REDACTED]

**Verifica della firma alla data odierna: (07/10/2017)**

Firma valida : **Certificato del Firmatario scaduto**

[Verifica la firma alla data di apposizione](#)

Dettagli ▾

✓

Firmato da GIUSEPPE VITRANI

La firma e' stata verificata correttamente

Dettagli ▾

Torna alla home

Visualizza

Salva

Apri cartella

Report

Salva Certificati



# Cosa si può fare con la firma digitale???

La legge consente, mediante l'utilizzo della firma digitale di:

- di sottoscrivere un documento informatico;
- di verificare (quale destinatario) l'identità del firmatario;
- di avere la certezza circa la provenienza, l'integrità e la segretezza del documento;
- di archiviare qualsiasi tipo di documento su supporto informatico con pieno valore legale;
- di tenere in forma informatica con pieno valore legale i libri sociali e le scritture contabili obbligatorie per legge;
- di rendere impossibile il ripudio della paternità di un documento

Le possibili applicazioni della firma digitale sono:

- comunicazioni ufficiali con le amministrazioni pubbliche;
- risposte a bandi/gare pubbliche;
- moduli di richiesta di vario tipo;
- dichiarazioni fiscali e d'altro tipo;
- trasmissioni di documenti legali;
- rapporti contrattuali su reti aperte (Internet);
  - fornitura elettronica di beni e servizi;
- transazioni finanziarie;
- identificazione e autorizzazione;
- gestione di attività in gruppi e sistemi chiusi o a partecipazione controllata;
  - gruppi di lavoro e di ricerca;
  - transazioni personali.



**Grazie per l'attenzione!!!**