Namirial® INFORMATION TECHNOLOGY

nei s.p.a.

Roberto De Duro – r.deduro@hotmail.it

# FIRMA DIGITALE

# POSTA ELETTRONICA CERTIFICATA

Udine – Gorizia - Trieste

27 novembre 2012

# La storia della firma digitale in ITALIA

1997

**Decreto del Presidente della Repubblica 10 novembre 1997, n. 513**

1999

Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche.

2002

**DECRETO LEGISLATIVO 23 gennaio 2002, n.10**

2005

**DECRETO LEGISLATIVO 7 marzo 2005, n. 82 Codice dell'amministrazione digitale.**

2010

**DECRETO LEGISLATIVO30 dicembre 2010, n. 235, Codice dell'amministrazione digitale. Modifiche ed integrazioni introdotte**

## 1997

per **firma digitale,** 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;

## 2002

"**Firma digitale**" è un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare 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;

## 2005

"**firma digitale**" un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare 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;

## 2010

"**firma digitale**" un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare 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;

# Come sono cambiate le definizioni di firma

| 1997 | 2002 | 2005 | 2010 |
| --- | --- | --- | --- |
| - | "**firma elettronica**" l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica; | "**firma elettronica**" l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica; | "**firma elettronica**" l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica; |

## Come sono cambiate le definizioni di firma

1997 2002 2005 2010

-

"**firma elettronica avanzata**" la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;

"**firma elettronica avanzata**" 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;

## Come sono cambiate le definizioni di firma

1997

2002

2005

2010

**"firma elettronica qualificata"** firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica;

**"firma elettronica qualificata"** un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;

## Come sono cambiate le definizioni di firma

Art. 21. - CAD

(Valore probatorio del documento informatico sottoscritto)

1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
2. **Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale**, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, **ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.**
3. Salvo quanto previsto dall'articolo 25, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale.

**Codice Civile**

**art. 2702**

La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l' ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta.

## Firma digitale

file

Smart Card
SCD

## Firma elettronica qualificata

Smart Card
* SSCD

Token


Micro SD

HSM

## Firma elettronica avanzata


OTP

Firma
Biometrica

Riconosciment
o biometrico
facciale

Riconoscimento
impronta

*** SSCD** massimo profilo di protezione riconosciuto UE


Per generare una firma digitale è necessario utilizzare una **coppia di chiavi digitali asimmetriche**, attribuite in maniera univoca ad un soggetto, detto **titolare** della coppia di chiavi:

- **la chiave privata**, destinata ad essere conosciuta solo dal titolare, è utilizzata per la generazione della firma digitale da apporre al documento;
- **la chiave da rendere pubblica** viene utilizzata per verificare l'autenticità della firma.

Caratteristica di tale metodo, detto **crittografia a doppia chiave**, è che, una volta firmato il documento con la chiave privata, la firma può essere verificata con successo esclusivamente con la corrispondente chiave pubblica.

La **sicurezza** è garantita dall'impossibilità di ricostruire la chiave privata (segreta) a partire da quella pubblica, anche se le due chiavi sono univocamente collegate.

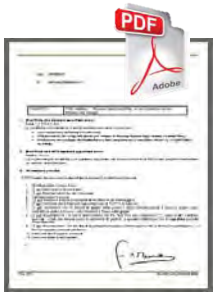
## CAdES
(CMS Advanced Electronic Signature)

La busta crittografica destinata a contenere il documento informatico sottoscritto deve essere conforme, modalità denominata **CAdES – BES**.

Qualsiasi files DOC, XLS, EXE, Ecc.

Estensione file **.p7m**

## PAdES
(PDF Advanced Electronic Signature)



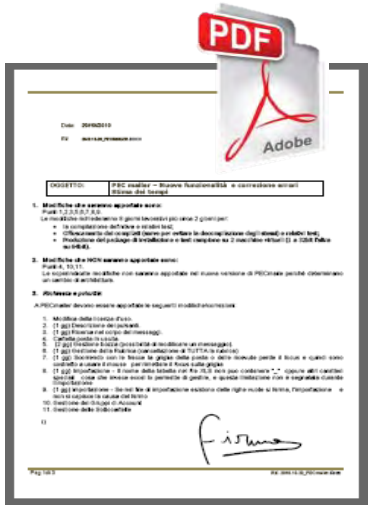

solo files PDF

Estensione file **.pdf**

## XAdES
(XML Advanced Electronic Signature)

XAdES (versione 1.4.1) e ETSI TS 102 904 (versione 1.1.1) , modalità XAdES-BES, XAdES-T, XAdES-A

Estensione file **.xml**

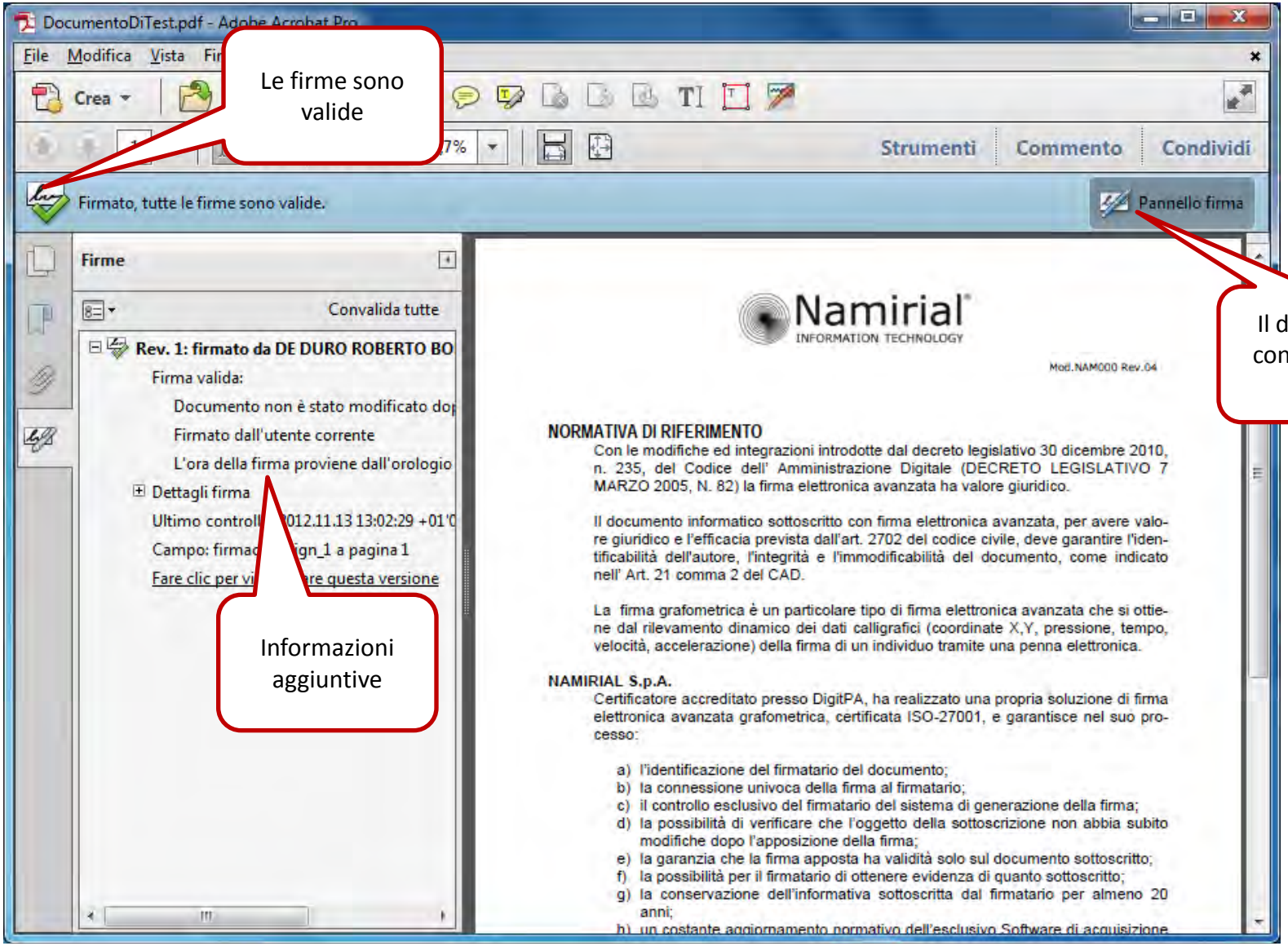


# Come funziona – firma qualificata

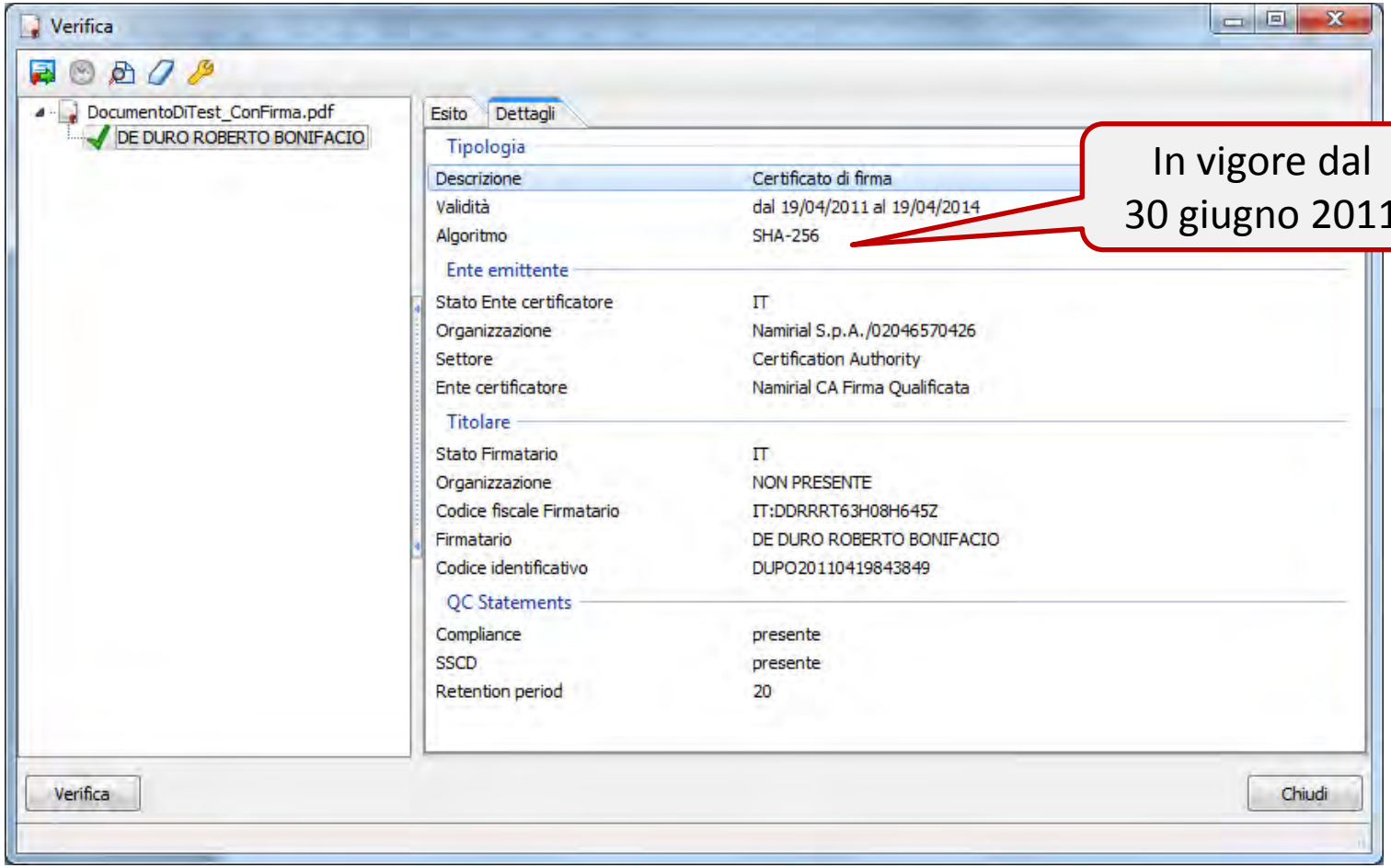
nei s.p.a.

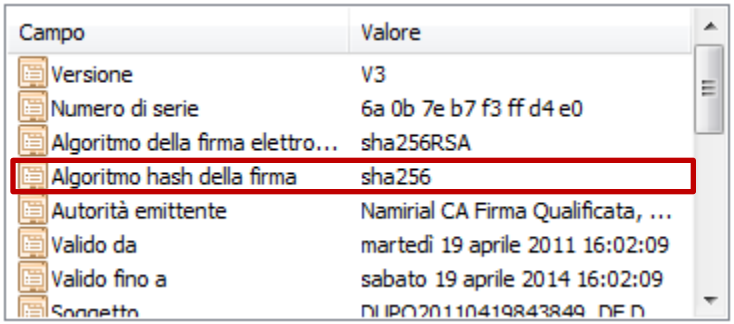
Namirial
INFORMATION TECHNOLOGY

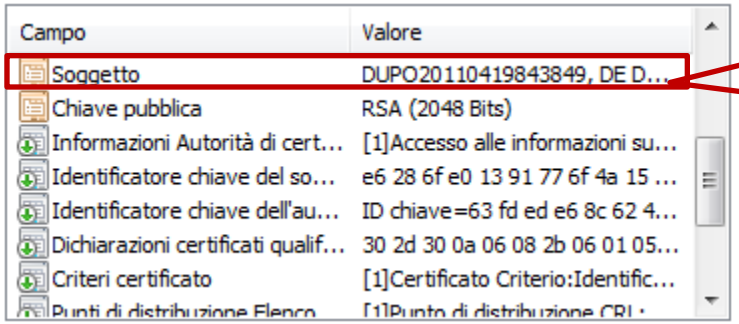
# Come verificare un documento firmato


DocumentoDiTest.pdf - Adobe Acrobat Pro
File Modifica Vista
Crea
Strumenti Commento Condividi
Firmato, tutte le firme sono valide.
Pannello firma
Le firme sono valide
Il documento contiene delle firme
Informazioni aggiuntive
Firme
Convalida tutte
Rev. 1: firmato da DE DURO ROBERTO BO
Firma valida:
Documento non è stato modificato dop
Firmato dall'utente corrente
L'ora della firma proviene dall'orologio
Dettagli firma
Ultimo controll 012.11.13 13:02:29 +01'0
Campo: firmac ign_1 a pagina 1
Fare clic per vi re questa versione
Namirial
INFORMATION TECHNOLOGY
Mod.NAM000 Rev.04
NORMATIVA DI RIFERIMENTO
Con le modifiche ed integrazioni introdotte dal decreto legislativo 30 dicembre 2010, n. 235, del Codice dell' Amministrazione Digitale (DECRETO LEGISLATIVO 7 MARZO 2005, N. 82) la firma elettronica avanzata ha valore giuridico.
Il documento informatico sottoscritto con firma elettronica avanzata, per avere valore giuridico e l'efficacia prevista dall'art. 2702 del codice civile, deve garantire l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, come indicato nell' Art. 21 comma 2 del CAD.
La firma grafometrica è un particolare tipo di firma elettronica avanzata che si ottiene dal rilevamento dinamico dei dati calligrafici (coordinate X,Y, pressione, tempo, velocità, accelerazione) della firma di un individuo tramite una penna elettronica.
NAMIRIAL S.p.A.
Certificatore accreditato presso DigitPA, ha realizzato una propria soluzione di firma elettronica avanzata grafometrica, certificata ISO-27001, e garantisce nel suo processo:
a) l'identificazione del firmatario del documento;
b) la connessione univoca della firma al firmatario;
c) il controllo esclusivo del firmatario del sistema di generazione della firma;
d) la possibilità di verificare che l'oggetto della sottoscrizione non abbia subito modifiche dopo l'apposizione della firma;
e) la garanzia che la firma apposta ha validità solo sul documento sottoscritto;
f) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
g) la conservazione dell'informativa sottoscritta dal firmatario per almeno 20 anni;
h) un costante aggiornamento normativo dell'esclusivo Software di acquisizione

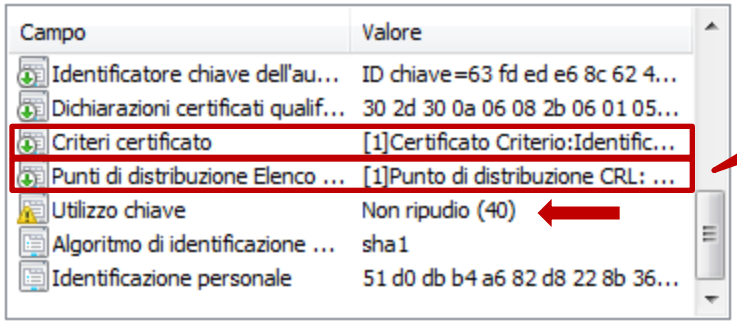
http://www.firmacerta.it/ Prodotti → Software


Verifica
DocumentoDiTest_ConFirma.pdf
DE DURO ROBERTO BONIFACIO
Esito
Dettagli
Tipologia
Descrizione
Certificato di firma
Validità
dal 19/04/2011 al 19/04/2014
Algoritmo
SHA-256
Ente emittente
Stato Ente certificatore
IT
Organizzazione
Namirial S.p.A./02046570426
Settore
Certification Authority
Ente certificatore
Namirial CA Firma Qualificata
Titolare
Stato Firmatario
IT
Organizzazione
NON PRESENTE
Codice fiscale Firmatario
IT:DDRRRT63H08H645Z
Firmatario
DE DURO ROBERTO BONIFACIO
Codice identificativo
DUPO20110419843849
QC Statements
Compliance
presente
SSCD
presente
Retention period
20
Verifica
Chiudi
In vigore dal
30 giugno 2011




dnQualifier = DUPO20110419843849
CN = DE DURO ROBERTO BONIFACIO
SERIALNUMBER = IT:DDRRRT63H08H645Z
G = ROBERTO BONIFACIO
SN = DE DURO
O = NON PRESENTE
C = IT




[1]Criterio certificato:
Identificatore criterio=1.3.6.1.4.1.36203.1.1.2
[1,1]Informazioni sulla definizione del criterio:
ID definizione criterio=CPS
Definizione:
http://www.firmacerta.it/manuali-MO/

[1]Punto di distribuzione CRL
Nome punto distribuzione:
Nome completo:
URL=http://crl.firmacerta.it/FirmaCertaQualificata1.crl

# Leggere il certificato

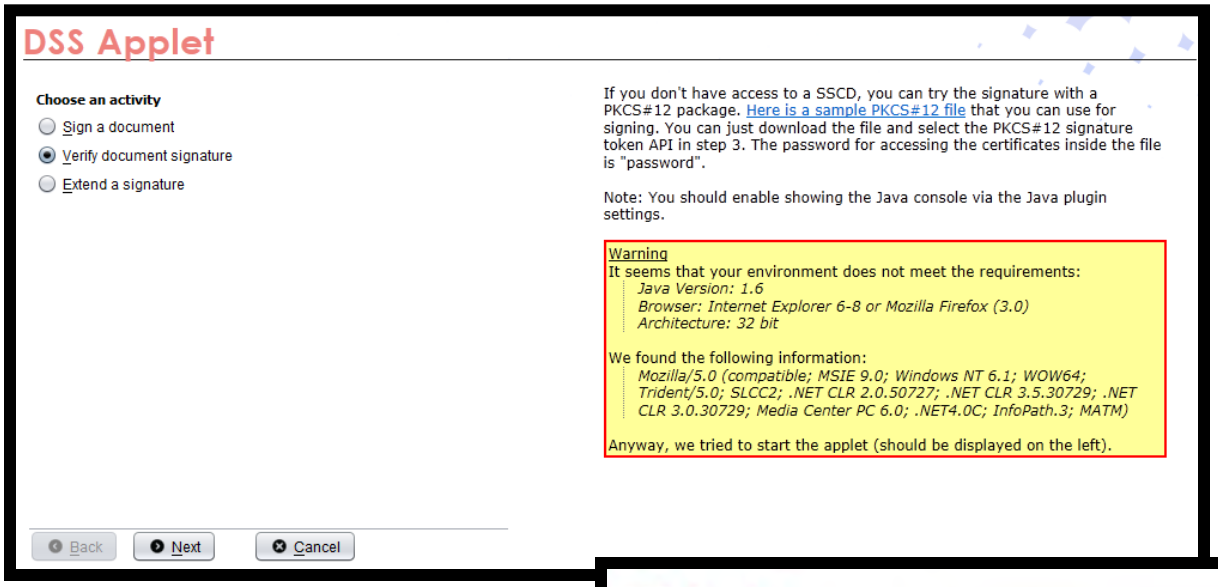
nei s.p.a. Namirial INFORMATION TECHNOLOGY

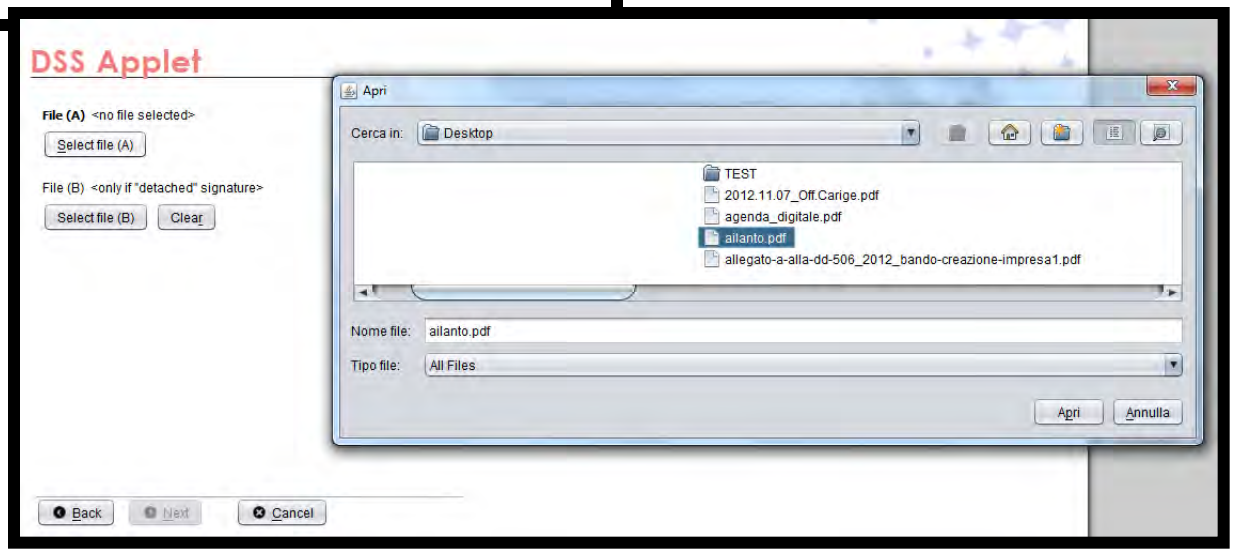
http://www.digitpa.gov.it/categoria/argomenti3/firma-digitale


## Verifica firme digitali di altri Stati dell'UE

Questa applicazione, che consente la verifica di firme digitali basate su **certificati emessi dai certificatori autorizzati nei diversi Stati membri dell'Unione Europea**, è stato promosso e sostenuto dalla Commissione Europea nell'ambito delle iniziative **dell'Agenda Digitale** per agevolare il libero scambio e il mutuo riconoscimento dei documenti informatici sottoscritti con firma digitale in Europa. Per essere utilizzata, è necessario che Digital Signature Service sia installata su un server web.

URL: http://dss.digitpa.gov.it/dss-webapp/signature.jsp

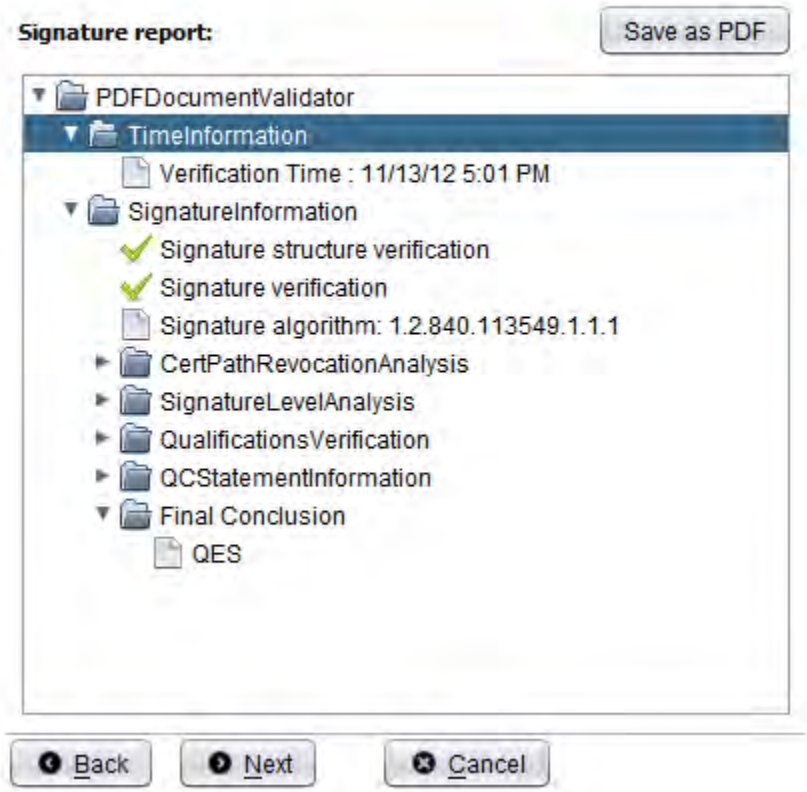



# Come verificare una firma

nei s.p.a. Namirial INFORMATION TECHNOLOGY

# DSS Applet


Signature report:
Save as PDF
PDFDocumentValidator
TimeInformation
Verification Time : 11/13/12 5:01 PM
SignatureInformation
Signature structure verification
Signature verification
Signature algorithm: 1.2.840.113549.1.1.1
CertPathRevocationAnalysis
SignatureLevelAnalysis
QualificationsVerification
QCStatementInformation
Final Conclusion
QES
Back
Next
Cancel

La marca temporale è il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo (data ed ora) certo.

Il servizio di Marcatura Temporale è erogato solo da Certification Authority accreditate presso l'Agenzia per l'Italia Digitale.

**I formati delle marche:**

CAdES-T (marca associata alla firma)
TSD (marca associata al documento)
TSR (marca inserita in un file separato)
TST (marca inserita in un file separato)
PDF (marca associata al PDF)

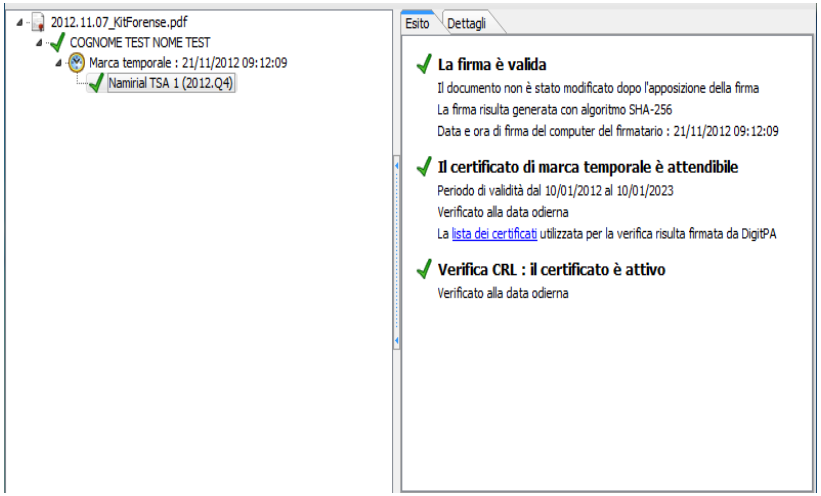
Art. 48

(*Informazioni contenute nella marca temporale)*

**1. Una marca temporale contiene almeno le seguenti informazioni:**

a) identificativo dell'emittente;
b) numero di serie della marca temporale;
c) algoritmo di sottoscrizione della marca temporale;
d) certificato relativo alla chiave utilizzata per la verifica della marca temporale;
e) riferimento temporale della generazione della marca temporale;
f) identificativo della funzione di hash utilizzata per generare l'impronta dell'evidenza
informatica sottoposta a validazione temporale;
g) valore dell'impronta dell'evidenza informatica.

# Verificare la marca:




# POSTA ELETTRONICA CERTIFICATA

# RACCOMANDATA CON RICEVUTA DI RITORNO

Il decreto legge **185 del 29 novembre 2008** stabilisce l'obbligo, per le società di capitali, per le società di persone e per i professionisti iscritti in albi o elenchi e le pubbliche amministrazioni, di dotarsi di una casella di posta elettronica certificata (PEC):

- per le **società di nuova costituzione** la PEC e' immediatamente obbligatoria e deve essere richiesta alla costituzione della società (la mancata comunicazione dell'indirizzo PEC determina la sospensione del procedimento di iscrizione al Registro Imprese);

- per le **società già costituite al 29/11/2008** la PEC deve essere richiesta entro e non oltre il 29/11/2011 e deve essere comunicata al Registro Imprese competente;

- per i **professionisti** (avvocati, ingegneri, architetti, consulenti del lavoro, dottori commercialisti ed esperti contabili, ecc...) diviene obbligatoria dal **29/11/2009** e va comunicata all'ordine o collegio di appartenenza;

- per le **amministrazioni pubbliche** che non vi avessero ancora provveduto ai sensi dell'art. 47, comma 3, lettera a), del Codice dell'Amministrazione digitale (CAD) devono istituire una casella di posta certificata per ciascun registro di protocollo e ne danno comunicazione al DigitPA (ex CNIPA).

# Che cos'è la PEC?

La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica (che utilizza i protocolli standard della posta elettronica tradizionale) nel quale al mittente viene fornita, in formato elettronico, la prova legale dell'invio e della consegna di documenti informatici.

# A cosa serve?

Alla trasmissione di messaggi, che possono contenere qualsiasi tipologia di informazione ed allegato, di cui si vuole avere la certezza della consegna. La PEC è nata per sostituire, attraverso i moderni mezzi di comunicazione, la Raccomandata postale con ricevuta di ritorno, o raccomandata AR.

Così come avviene per la raccomandata AR, al mittente viene inviata una ricevuta che attesta la consegna al destinatario del proprio messaggio.

**Semplicità**: il servizio PEC si usa come la normale posta elettronica sia tramite programma cliente (es. Outlook Express), sia tramite web mail, sia tramite gestionale documentale.

**Valore legale**: a differenza della tradizionale posta elettronica, alla PEC è riconosciuto pieno valore legale e le ricevute possono essere usate come prove dell'invio, della ricezione ed anche del contenuto del messaggio inviato. Le principali informazioni riguardanti la trasmissione e la consegna vengono conservate per 30 mesi dal gestore e sono anch'esse opponibili a terzi.

**No virus e spam**: l'identificazione certa del mittente di ogni messaggio ricevuto ed il fatto che non si possano ricevere messaggi non certificati, rendono il servizio PEC pressoché immune dallo spam.

**Risparmio**: confrontando i costi di una casella PEC con quello di strumenti quali fax e raccomandate è evidente il risparmio che si può ottenere non solo in termini economici, ma anche di tempo.

**Costo fisso**: il prezzo annuale di una casella PEC non prevede costi aggiuntivi in base all'utilizzo.

**Scopo della PEC**

- Dare certezza al processo di inoltro
- Dare valenza legale alla posta elettronica
- Sostituire integralmente il servizio di posta tradizionale raccomandata

**Strumenti di garanzia della PEC**

- Utilizzo della firma elettronica per garantire l'integrità del messaggio
- Scambio di ricevute firmate dai gestori
- Tenuta di log immodificabili delle attività svolte
- Riferimento e marca temporale
- Sincronizzazione degli orologi

**Vantaggi**

- Riduzione dei tempi di consegna
- Gestione dei documenti e dei flussi documentali più efficiente
- Riduzione dei costi (carta, affrancature, personale, etc..)

Art. 45.
(Valore giuridico della trasmissione)

1. I documenti trasmessi da chiunque ad una **pubblica amministrazione con qualsiasi mezzo** telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.
2. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

Art. 61.
(Soluzioni di firma elettronica avanzata )

1. L'invio tramite posta elettronica certificata di cui all'art. 65, comma 1, lettera c-bis) del codice, effettuato richiedendo la ricevuta completa di cui all'art. 1, comma 1, lettera i) del Decreto 2 novembre 2005 recante "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata", costituisce, nei confronti della pubblica amministrazione, firma elettronica avanzata del messaggio spedito ai sensi delle presenti regole tecniche.

| periodo | domini | caselle | messaggi |
|---|---|---|---|
| 1° bimestre 2009 (Gennaio-Febbraio) | 29.477 | 342.291 | 28.326.443 |
| 1° bimestre 2010 (Gennaio-Febbraio) | 79.060 | 1.463.662 | 40.284.331 |
| 1° bimestre 2011 (Gennaio-Febbraio) | 115.995 | 2.340.848 | 52.818.441 |
| 1° bimestre 2012 (Gennaio-Febbraio) | 185.136 | 44.931.44 | 64.442.252 |