

# Firma e timbro digitale nei processi di autenticazione

14 FEBBRAIO.  
ORE 14.00 -16.00.  
SALA MEETING 1

# Agenda

- Introduzione
- Il timbro d
- Il Tim
- L

come strumento e tecnica di operativita dell'ingegnere

**Andrea Quargnali – SYSDATA Italia**  
**Responsabile Commerciale - Area Manager FVG**  
**[andrea.quarniali@sysdata.it](mailto:andrea.quarniali@sysdata.it)**

# **Il Timbro Digitale**

## **Una soluzione tecnologica per l'autenticazione di documenti stampati**

*Sandro Fontana Secure Edge Srl  
Chief Technology Officer  
CISSP, 27001 L.A. , CISM, CISA  
sfontana@Secure-edge.com*



**UDINE FIERE – 14/17 febbraio 2008**  
**Padiglione 2 stand 2B3.8**

# Scenario

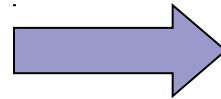
- Deliberazione CNIPA n. 11 del 19/02/2004  
(Conservazione sostitutiva dei documenti informatici)
- D.L. 20 febbraio 2004 n. 52  
(Istituzione fatturazione elettronica)
- D.Lgs 82/2005  
(Codice Amministrazione Digitale)
- Decreto legislativo 4 aprile 2006, n. 159 (integrazione al Codice dell'Amministrazione Digitale)
- 20/02/2007 Direttiva Min.Nicolais su informatizzazione uffici pubblici („dare forte accelerazione all'informatizzazione degli uffici pubblici e dare piena attuazione al codice dell'amministrazione digitale”..)

# Alcuni Dati

*(Fonte: Ministero Innovazione e Tecnologie)*

- 35 mln di certificati prodotti ogni anno dalla P.A.
- Costo per i cittadini 13.5 Euro per ogni certificato

Grazie alle nuove  
tecnologie  
possibile risparmio



400 mln di  
Euro

# L'esigenza

La parola d'ordine diventa: dematerializzare.

Significa evitare, quando possibile, la generazione di stampe, favorendo lo scambio di documentazione tramite Internet (email, web, ...) , sfruttando i nuovi concetti legali di documento elettronico e di firma digitale.

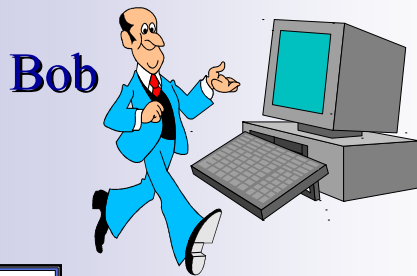
L'eliminazione del supporto fisico (la carta) è tecnicamente possibile:

in alcuni processi in modo totale, in altri —come quelli che coinvolgono attori esterni (es. Cittadini, PMI)— in modo parziale.



# ATTENZIONE:

Il documento elettronico è verificabile  
nella sua integrità ed autenticità finché è elettronico  
..... ma quando il documento viene stampato? .....



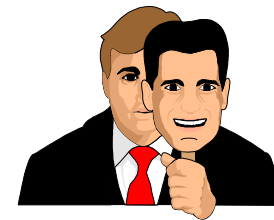
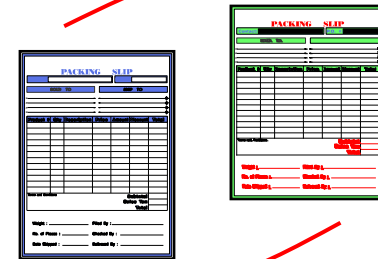
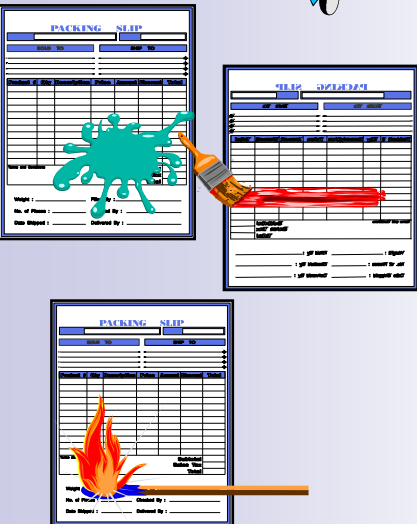
Londra dicembre 1964  
Caro Babbo Natale,  
questo anno sono stato molto  
buono. Sono riuscito a spiare  
tutte le riunioni del Consiglio  
ed a registrare tutto lo suo  
parole. Inoltre ho distribuito  
informazioni false e fuorvianti  
a tutti i governi alleati. Ti prego  
di portarmi una nuova  
maschera per la codifica dei  
miei messaggi; ho paura che  
quella che uso ora non sia  
tanto valida; potrebbero  
scoprirmi!  
Tuo John Profumo



Charlie

Quando il documento viene stampato la  
firma digitale non è più rappresentata!

Con la stampa,  
l'autenticità, l'integrità e non ripudio  
SONO PERSI PER SEMPRE!





# La carta come necessità

Molti sono i casi,  
tra Pubblica Amministrazione e Cittadini,  
dove i documenti attraversano più passaggi sulla carta

- ☑ Leggi e regolamenti
- ☑ Interoperabilità
- ☑ Fruibilità
- ☑ Comodità

L'esigenza rimane quella di proteggerli  
durante tutto il ciclo di vita,  
elettronico e cartaceo



# Garantire

l'inalterabilità, l'autenticità e la riservatezza  
di un documento elettronico è oggi possibile  
tramite l'uso della crittografia.  
(cifratura e firma digitale)

La crittografia risponde in pieno a queste necessità,  
ma solo nell'universo elettronico.

**Come trasferire  
l'autenticità del documento elettronico firmato  
digitalmente sul supporto cartaceo  
per renderlo infalsificabile ?**

# CNIPA

<http://www.cnipa.gov.it>

**Soluzioni tecnologiche per l'autenticazione di documenti stampati 2.0.pdf**

*versione 2.0 18 dicembre 2006*

*Francesco Grasso - CNIPA*

*Gaetano Santucci - CNIPA*

# estratto dallo studio CNIPA

[...] Nell'ambito della Pubblica Amministrazione, e nel rapporto tra questa e i suoi utenti (cittadini e imprese) esistono tuttora numerose situazioni in cui documenti dei quali occorre garantire l'autenticità possono attraversare, nel corso del loro ciclo di vita, uno o più passaggi attraverso la carta.

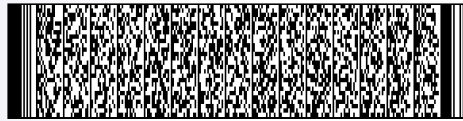
Esiste senz'altro l'esigenza di proteggere tali documenti in tutte le fasi del loro ciclo di vita, indipendentemente dal supporto – elettronico o cartaceo – utilizzato. Questa indipendenza potrebbe essere possibile se si stampassero, contestualmente al contenuto del documento, le informazioni necessarie a controllarne l'autenticità già presenti nel documento stesso, ad esempio: – una rappresentazione alternativa e non alterabile del contenuto del documento; – la certificazione della fonte che ha emesso il documento.

Nel proseguo del documento, indicheremo convenzionalmente la stampa di tutte o parte di queste informazioni con il termine “timbro digitale”.

Per timbro digitale si può intendere quindi una rappresentazione convenzionale di informazioni contenute nel documento elettronico (tutte o parte di esse), stampabile, riconoscibile con strumenti elettronici, ottenuta utilizzando una codifica grafica definita. [...]

# Tecnologia per il Timbro Digitale /1

Lo studio del CNIPA  
ha analizzato diversi codici bidimensionali ed alcuni casi d'uso.



PDF417



QR-Code

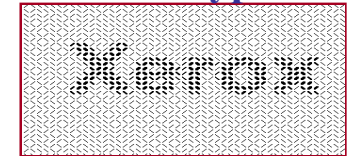


DataMatrix

Tuttavia, questi codici sono di formato fisso  
e non possono contenere più di 1.000..1.300 byte di informazione.

Il DataGlyphs della Xerox  
è un codice a dimensione variabile.

DataGlyphs



... ma la sua densità è di soli 69byte/cm<sup>2</sup> (450/inch<sup>2</sup>)

# Tecnologia per il Timbro Digitale <sup>12</sup>

Il rispetto delle norme legali sulla firma digitale, implica un quantitativo importante di dati.

Sia l'attuale formato di firma PKCS#7, o il più recente XML Signature occupano, solo per le strutture dati, circa 2.5Kbyte.

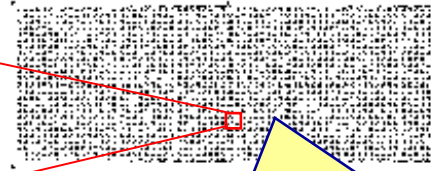
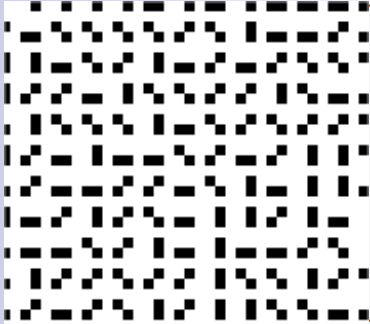
Nessun codice bidimensionale di vecchia generazione ha la capacità di contenere i dati necessari ad una firma a norma di legge.

Questa è la ragione per cui è stato implementato un codice specifico per questa tematica:

il codice 2D-Plus<sup>TM</sup>

# Il codice 2D-Plus™

(Symbol)

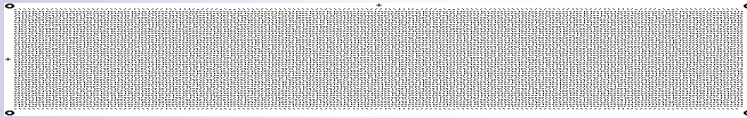


- Capacità di 580byte/cm<sup>2</sup> (3.750 byte/inch<sup>2</sup>)
- Forma quadrangolare dinamica (modificabile)
- Progettato per contenere dati in forma binaria: testo, immagini, biometria (impronte, digitali retina) ma anche audio, video
- codice a correzione di errore Reed-Solomon: dal 5% al 50%
- non necessita di apparecchiature speciali per la stampa e la lettura

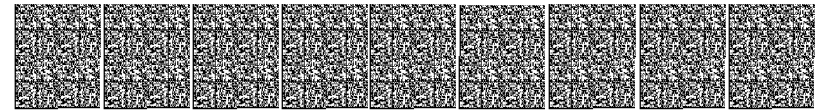
## 2D-Plus™ Vs DatMatrix

Il benchmark si basa su un' area utile posta alla base di un foglio A4 pari a 190mm x 20mm, un processo di stampa a 300 dpi ed un processo di scansione a 600dpi.

Su queste basi sono stati usati i codici bidimensionali in questo modo:



Il codice 2D-Plus ha semplicemente occupato lo spazio a sua disposizione, con un codice di errore pari al 20% (per poter essere equivalente all'ECC-200 del DataMatrix)



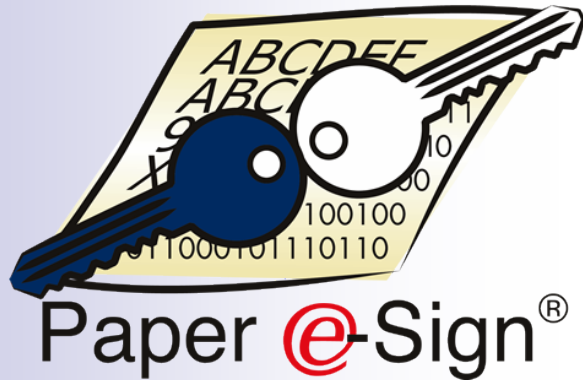
Ottimizzando lo spazio disponibile è stato possibile inserire 9 codici Data Matrix versione ECC-200, adatta per dati binari, da 144x144 pixel.



## 2D-Plus™ Vs DatMatrix Risultati

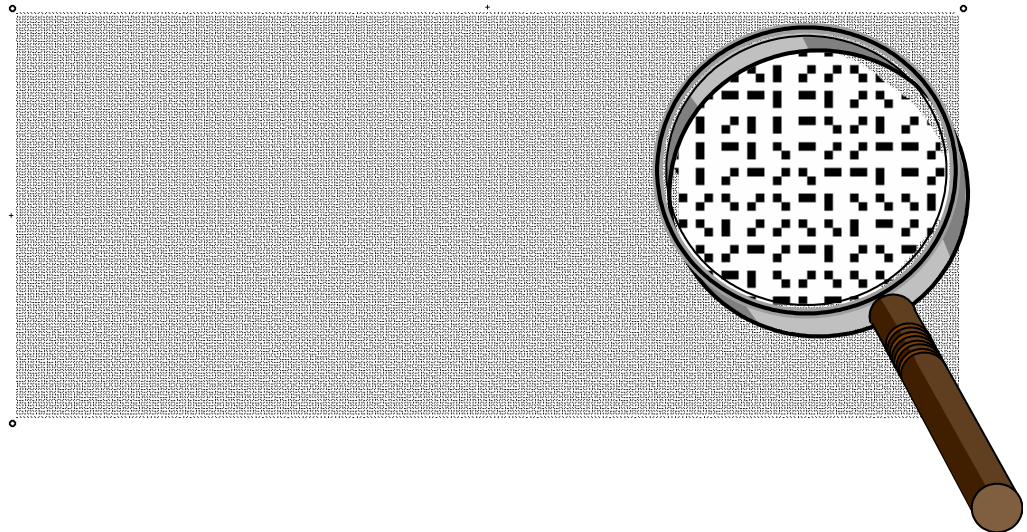
	<b>DataMatrix</b>	<b>2D-Plus™</b>
Capacità utile nello spazio a disposizione	9.000 byte	13.100 byte [+45%]
Tempo di decodifica complessivo	8.5 s	6.3 s [+25%]
Velocità di decodifica	1.059 byte/s	2.079 byte/s [+96%]
Tempo di codifica di 9'000 byte	325 ms	52 ms [+84%]
Velocità di codifica di 9'000 byte	3 codifiche/s	19 codifiche/s [+633%]

# Il Timbro Digitale



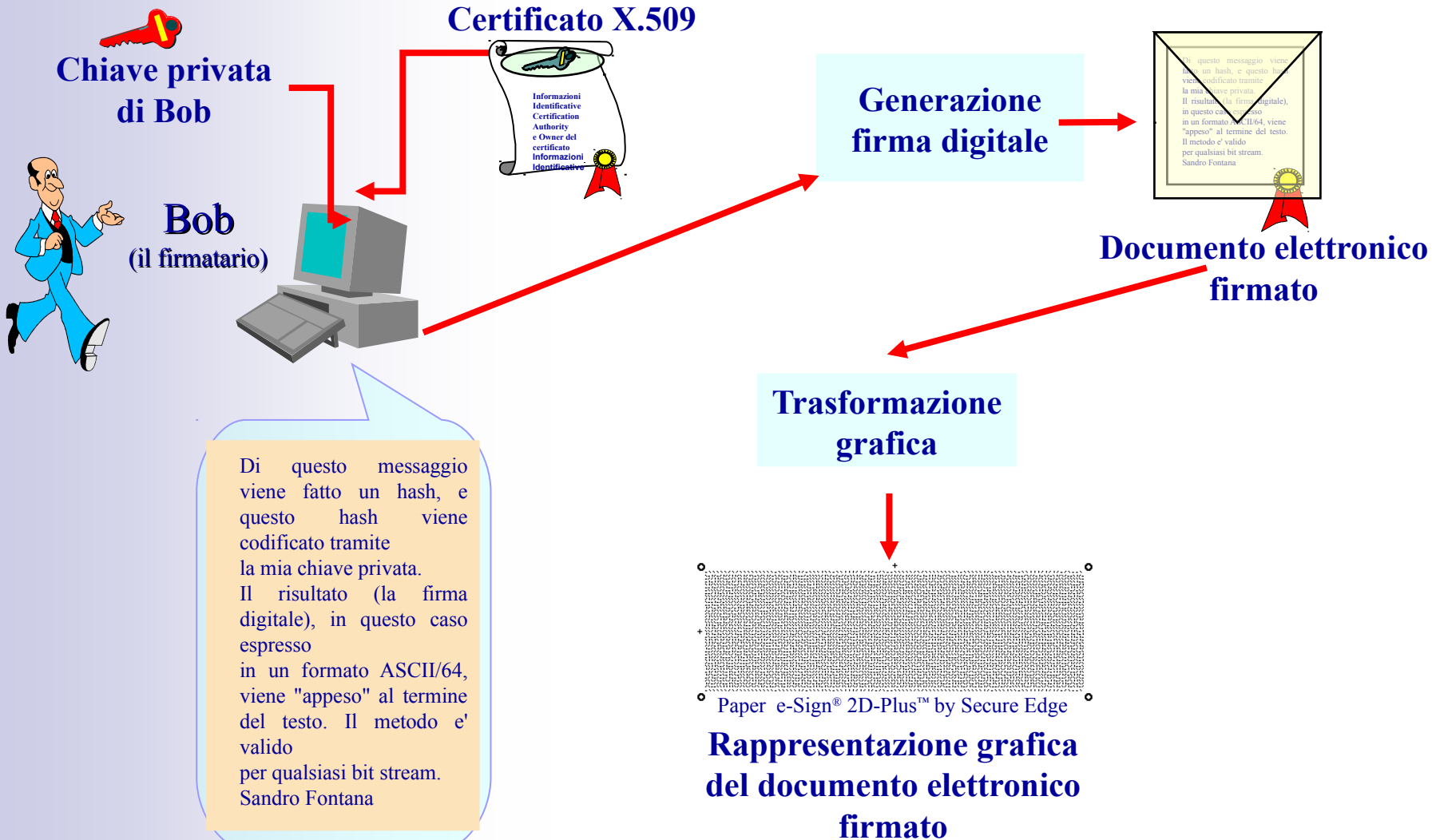
## La firma digitale su carta

**2D-Plus™**  
Codice ad alta densità



# Paper e-Sign® (PeS)

La firma digitale su carta



# Paper e-Sign<sup>®</sup> (PeS) / 2D-Plus<sup>™</sup>

All'interno del codice viene inserito il documento completo, firmato digitalmente nella forma legale di un pacchetto PKCS#7.

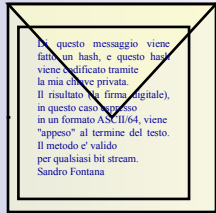
In questa modalità il Timbro Digitale è il vero documento prodotto, mentre la sua rappresentazione testuale è solo una comoda versione leggibile, senza alcuna validità legale.

Questo punto è molto importante rispetto al quadro normativo:  
la soluzione Paper e-Sign<sup>®</sup> 2D-Plus<sup>™</sup>  
permette di trasportare su carta dati firmati secondo  
un formato legale (PKCS#7),  
allo stesso modo di quanto si farà utilizzando un CD o un nastro di back-up.

Il processo Paper e-Sign<sup>®</sup> è nato nel marzo 2001 al fine di trasportare la firma digitale al documento cartaceo, quale volano per la diffusione di progetti di PKI.

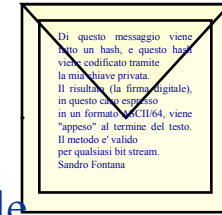
# Il processo

**Dati elettronici  
firmati digitalmente**



Il documento elettronico firmato viene trasformato in un codice grafico bidimensionale capace di contenere, **unico al mondo**, l'intero documento e la sua firma digitale!

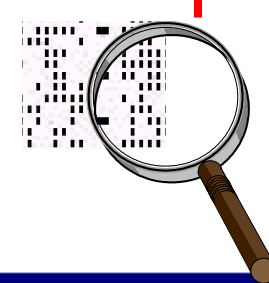
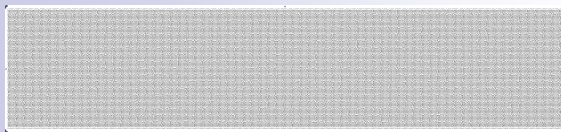
**Dati elettronici  
firmati digitalmente**



Trasformazione grafica

Acquisizione immagine

Verifica firma Digitale e Decodifica Grafica

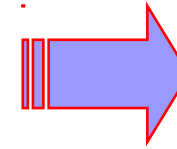
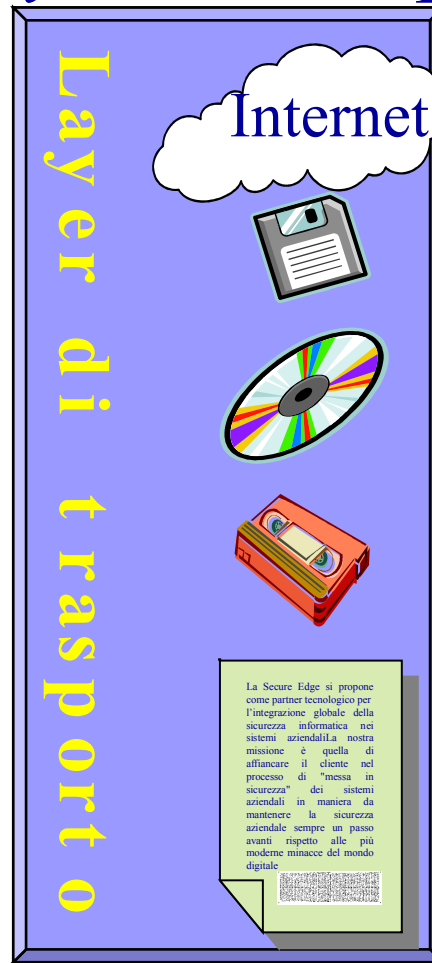
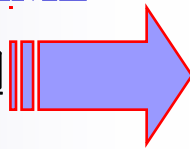


Stampa

# Con PeS 2D-Plus, la carta è un *layer* di trasporto sicuro



Dati firmati digitalmente  
PKCS#7,  
PDF, XML



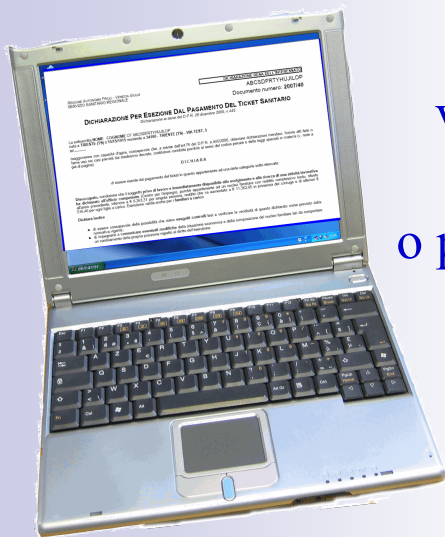
Dati firmati digitalmente  
PKCS#7,  
PDF, XML

# Verifica

La verifica di un Timbro Digitale 2D-Plus,  
è facilmente realizzabile utilizzando l'apposito software  
distribuibile gratuitamente.

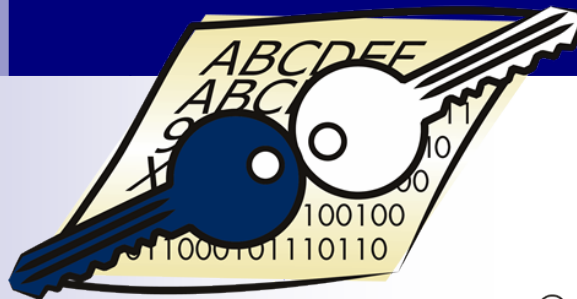
Il software acquisisce, da scanner piano,  
l'immagine del Timbro Digitale.

A partire da questa immagine  
viene ricostruito il file dati in formato PKCS#7  
che può essere verificato o direttamente  
o per mezzo uno dei software forniti gratuitamente  
dai Certificatori Accreditati dal CNIPA.

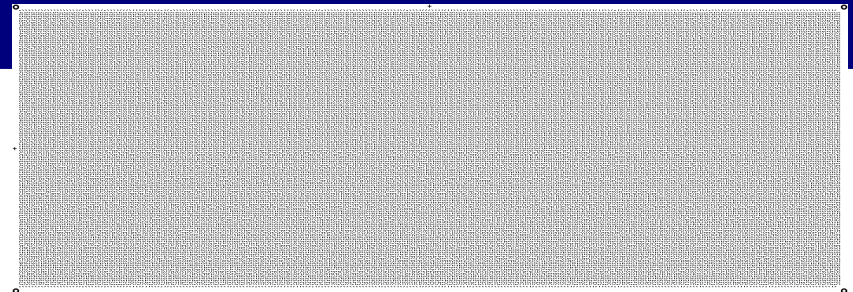




## I Vantaggi



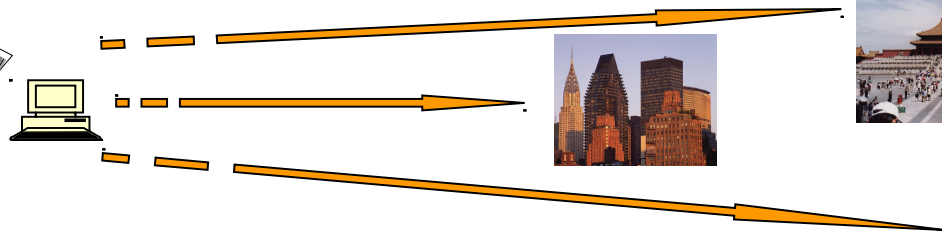
Paper **@**Sign<sup>®</sup>



**2D-Plus<sup>™</sup>**



## Distribuzione Remota



I Cittadini possono stampare documenti **AUTENTICI!**

## Integrazione e Valorizzazione Carta Speciale

Stampabile da  
qualsiasi  
stampante

Integrazione e  
valorizzazione  
carta speciale:

Filigrana, Ultravioletti,  
inserimenti metallici RFID

Nessun  
tipo di  
gestione

## Privacy

### Clinica Salus

Paziente: AZ-2779-BBY-201

Informazioni  
Sensibili:

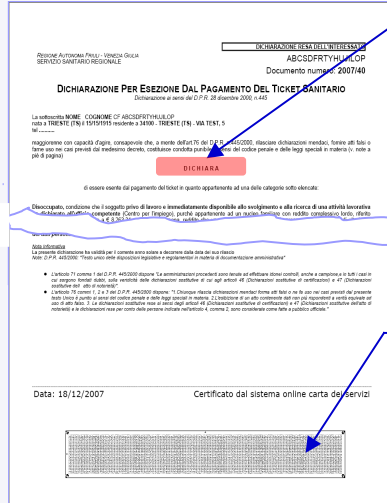
accesso ristretto  
al solo personale  
medico



Il testo in chiaro  
presenta solo dati  
non sensibili

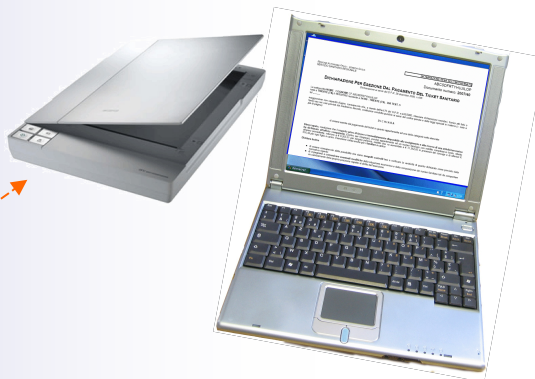
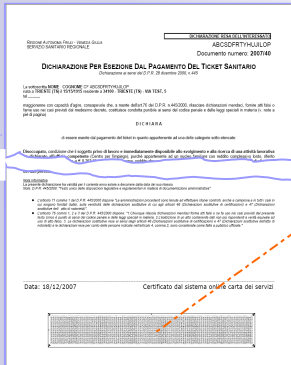
I dati sensibili sono  
contenuti nel Codice  
Grafico (eventualmente  
cifrati)

# Antifalsificazione e Verifica



Protezione antifalsificazione: qualsiasi variazione del testo non potrà essere inserita nel Codice Grafico

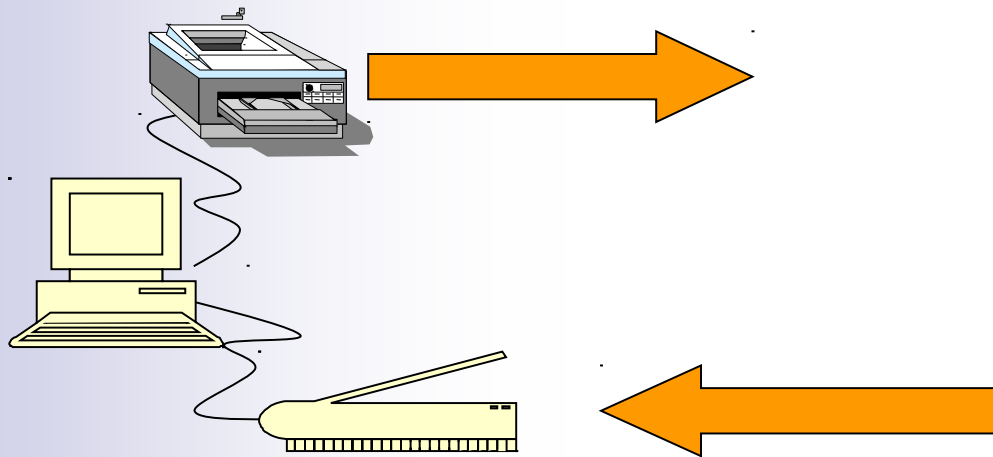
Verifica off line: il controllo dei dati e della firma non necessitano di essere on line



È sufficiente inserire il documento in un qualsiasi scanner, ed un software appositamente predisposto, acquisirà il Timbro Digitale e dopo aver verificato l'attendibilità della firma digitale, restituirà il documento contenuto al suo interno.

# Verifica di Autenticità

# Riacquisizione dati in formato elettronico



**DICHIARAZIONE SUI DATI DELL'INTERESSATO**

Regione Autonoma Friuli - Venezia Giulia  
SERVIZIO SANITARIO REGIONALE

ABCSDFRTYHUJLOP  
Documento numero: 2007/40

**DICHIARAZIONE PER ESECUZIONE DEL PAGAMENTO DEL TICKET SANITARIO**  
Dichiarazione ai sensi del D.P.R. 28 dicembre 2000, n. 445

La sottoscritto **NOME COGNOME CF ABCSDFRTYHUJLOP**  
nata a **TREVIETI (TV) - 520191919** residente a **MARNO - TREVIETI (TV) - VIA TESTI, 5**  
MI .....  
maggiorente con capacità d'agire, consapevole che, ai sensi dell'art.76 del D.P.R. n.445/2000, rilasciare dichiarazioni mendaci, fornire atti falsi o  
falsare uno o più dati previsti dal medesimo decreto, costituisce condotta punibile ai sensi del codice penale e delle leggi speciali in materia (v. note a  
più di pagina)

**DICHIARA**

di essere esente dal pagamento del ticket in quanto appartenente ad una delle categorie sotto elencate:

**Disoccupato, condizione che il soggetto privo di lavoro è immediatamente disponibile allo svolgimento e alla ricerca di una attività lavorativa  
dichiarato all'ufficio competente (Centro per l'impiego), purché appartenente ad un nucleo familiare con reddito complessivo lordo, riferito  
alla persona, inferiore a € 2.303,14.**

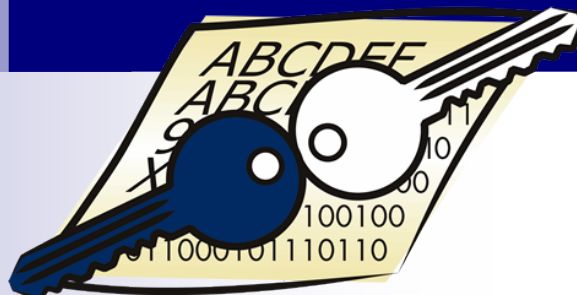
**Nota Informative**  
La presente dichiarazione ha validità per il corrente anno solare e decorre dalla data del suo rilascio.  
Atto: D.P.R. n.445/2000: "Tutti i nuovi dati obbligatoriamente registrati in materia di documentazione amministrativa"

- L'articolo 76 comma 1 del D.P.R. n.445/2000 dispone: "Le amministrazioni provvedono prima anche ad effettuare idonei controlli, anche a campione, su tutti i casi in cui vengono forniti i dati, sulla veridicità delle dichiarazioni assunte e su ogni altro dato (dichiarazioni sostitutive di certificazioni) e di (dichiarazioni sostitutive di atti di notorietà)".
- L'articolo 76 comma 1, 2 e 3 del D.P.R. n.445/2000 dispone: "1) Chiunque rilascia dichiarazioni mendaci, fornisce atti falsi o ne fa uso nel caso previsto dal presente articolo, è punito con la reclusione prevista in una delle leggi speciali in materia. 2) L'adempimento di cui è oggetto del presente articolo è assolvibile in modo alternativo al uso di atti basati. 3. Le dichiarazioni sostitutive sono ai sensi degli articoli 46 (dichiarazioni sostitutive di certificazioni) e 47 (dichiarazioni sostitutive dell'atto di notorietà) e le dichiarazioni non per conto delle persone indicate nell'articolo 4, comma 2, sono considerate come false e punibili a pubblico ufficiale".

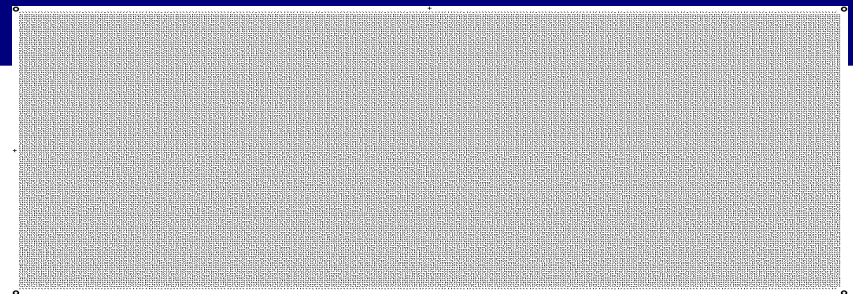
Data: 18/12/2007      Certificato dal sistema online carta dei servizi

Un grande vantaggio deriva infine dall'automatica disponibilità dei dati in forma elettronica con certezza della loro autenticità ed integrità: non più costi dovuti ai processi di data entry, al tempo impiegato ed agli errori introdotti.

## Applicazioni in esercizio



Paper @-Sign®



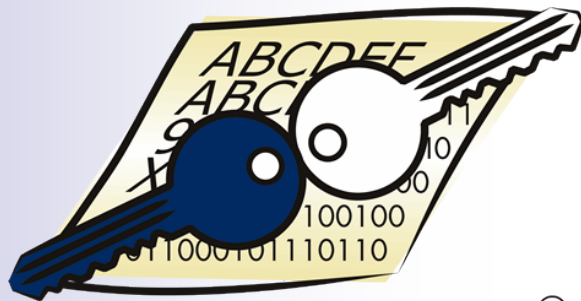
2D-Plus™

<p><b>AICA</b></p>	<p>Anticontraffazione Patente d'Informatica  <i>(300.000 Patenti rilasciate ad oggi)</i></p>
<p><b>SOGEI per AAMS</b></p>	<p>Anticontraffazione “Nulla Osta  apparecchiature da intrattenimento comma 7”</p>
<p><b>ACI INFORMATICA</b></p>	<p>Anticontraffazione:  1) Certificato di Proprietà Auto  <i>(sperimentazione)</i>  2) Visure On Line <i>(prossimo rilascio)</i></p>
<p><b>Vigili del Fuoco (Min. Interno)</b></p>	<p>Rilascio delle Certificazioni Antincendio con  il Timbro Digitale</p>
<p><b>Regione  Friuli Venezia Giulia – INSIEL  Partner: Sysdata Italia Spa</b></p>	<p>Rilascio Esenzioni Sanitarie On Line</p>
<p><b>Postecom  Gruppo Poste Italiane</b></p>	<p>Integrazione 2D-Plus™ Word Add-In con il  Kit di Firma digitale di Postecom  <i>Fornitura di 10.000 Licenze Client</i></p>

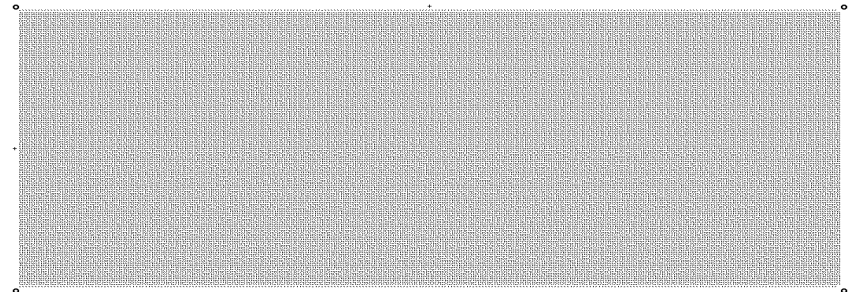
**DEMO**



**UDINE FIERE – 14/17 febbraio 2008**  
**Padiglione 2 stand 2B3.8**



Paper @-Sign®



**2D-Plus™**

*is* **InnovAction**