Dubbi e opportunità nella firma elettronica avanzata

PAVIA – Collegio Ghislieri

17 novembre 2011

Lo scenario di riferimento

- **Il 25 gennaio 2011 è entrato in vigore il decreto legislativo 30 dicembre 2011, n. 235 che ha modificato il codice dell'amministrazione digitale – CAD (DLgs 7 marzo 2005, n. 82).**
- **Tali modifiche sono significative e hanno impatti sul valore legale del documento informatico, sulla sua conservazione digitale e in generale sul suo ciclo di vita.**
- **Il nuovo impianto normativo segue la linea politica del Governo che ritiene la dematerializzazione cruciale per l'efficienza della pubblica amministrazione ma anche del Paese.**
- **Il CAD si coordina con la riforma della pubblica amministrazione considerando l'innovazione con un circolo virtuoso basato su regole, tempi di attuazione certi e sanzioni per le inadempienze.**
- **Molte delle previsioni del CAD dovranno attendere l'emanazione di decreti tecnici, linee guide o altri documenti di supporto.**

Firme elettroniche: definizioni (1/2)

- **Numerose le nuovi definizioni “ai fini del presente codice”.**
- **Autenticazione del documento informatico; definizione introdotta al fine di eliminare ambiguità con il classico termine autenticazione utilizzato per l’accesso ai servizi in rete (tipicamente: autenticazione forte).**
- **Copia per immagine su supporto informatico di documento analogico.**
- **Copia informatica di documento informatico (Es.: passaggio tra un .doc a un .pdf).**
- **Duplicato informatico (la creazione di una ulteriore istanza di un file).**

Firme elettroniche: definizioni (2/2)

- **Documento analogico complementare al documento informatico.**
- **Firma elettronica avanzata; dalla Direttiva 1999/93/CE.**
- **Firma digitale; per un evidente errore non è più presente il dispositivo sicuro per la creazione della firma.**
- **Firma elettronica qualificata.**
- **Le tre firme sono connesse a “matrioska” rispetto al precedente ordinamento che le considerava a “catena”.**
- **Identificazione informatica (invece che autenticazione informatica).**

In dettaglio - 1

- **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”.*

- **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”.*

In dettaglio - 2

- **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”.*

- **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”.*

Le firme elettroniche

- **La nuova definizione di firma elettronica avanzata è cruciale in quanto stabilisce per essa una nuova efficacia pari a quella prevista dal 2702 del codice civile.**
- **A livello europeo si parla di AdES (Advanced Electronic Signature).**
- **Essa consente l'identificazione del firmatario del documento con connessione univoca ad esso.**
- **Viene creata con mezzi sui quali il firmatario può conservare un controllo esclusivo.**
- **Sono rilevabili le modifiche successive al documento informatico.**

La firma elettronica avanzata

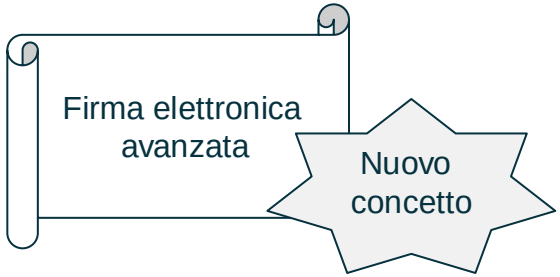
- **I dati per la creazione della firma sono univocamente assegnati a un titolare.**
- **Devono garantire l'identificabilità del titolare.**
  - **Non è obbligatoria la presenza di un certificato digitale.**
- **Deve essere gestito il controllo esclusivo di un «dispositivo» perché è stabilito che "*l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria*".**
- **Per garantire l'integrità si può continuare ad applicare gli standard CADES (estensione dei file .p7m), XADES e PADES (formato PDF) (già presenti nelle vigenti regole tecniche).**

La firma grafometrica

- **E' basata sulle caratteristiche comportamentali del titolare (ritmo, pressione, velocità, accelerazione, movimento, etc.) che firma con uno stilo elettronico su una tavoletta grafica ad alta sensibilità.**
- **Di per sé rappresenta una firma elettronica. Adeguatamente connessa ad un sistema documentale può divenire una firma elettronica avanzata.**
- **Se utilizzata "a sportello" soddisfa anche i requisiti di identificazione del titolare richiesti per la firma elettronica avanzata.**
- **Nei prodotti di mercato viene reso disponibile uno strumento di tipo forense per l'analisi grafologica della sottoscrizione. In tal modo nulla cambia in caso di contestazione della sottoscrizione.**
- **Ma è il sottoscrittore a dover dimostrare di non aver firmato secondo il principio dell'inversione dell'onere della prova.**

Il testo vigente del CAD introduce rilevanti modifiche al quadro normativo

Evidenze del legislatore



- Con le modifiche introdotte al C.A.D. (Dgl 30 Dic 2010) sono state recepite le direttive UE in merito alla firma elettronica avanzata
- Alla “firma elettronica avanzata” è stata conferita **la massima validità giuridica** (*)
- Tale firma deve essere frutto di un processo di calcolo attivato tramite un dispositivo **riconducibile al titolare della firma**
- Vengono pertanto a **cessare** i requisiti **sul dispositivo sicuro** e **sul certificato qualificato**

Conseguenze pratiche

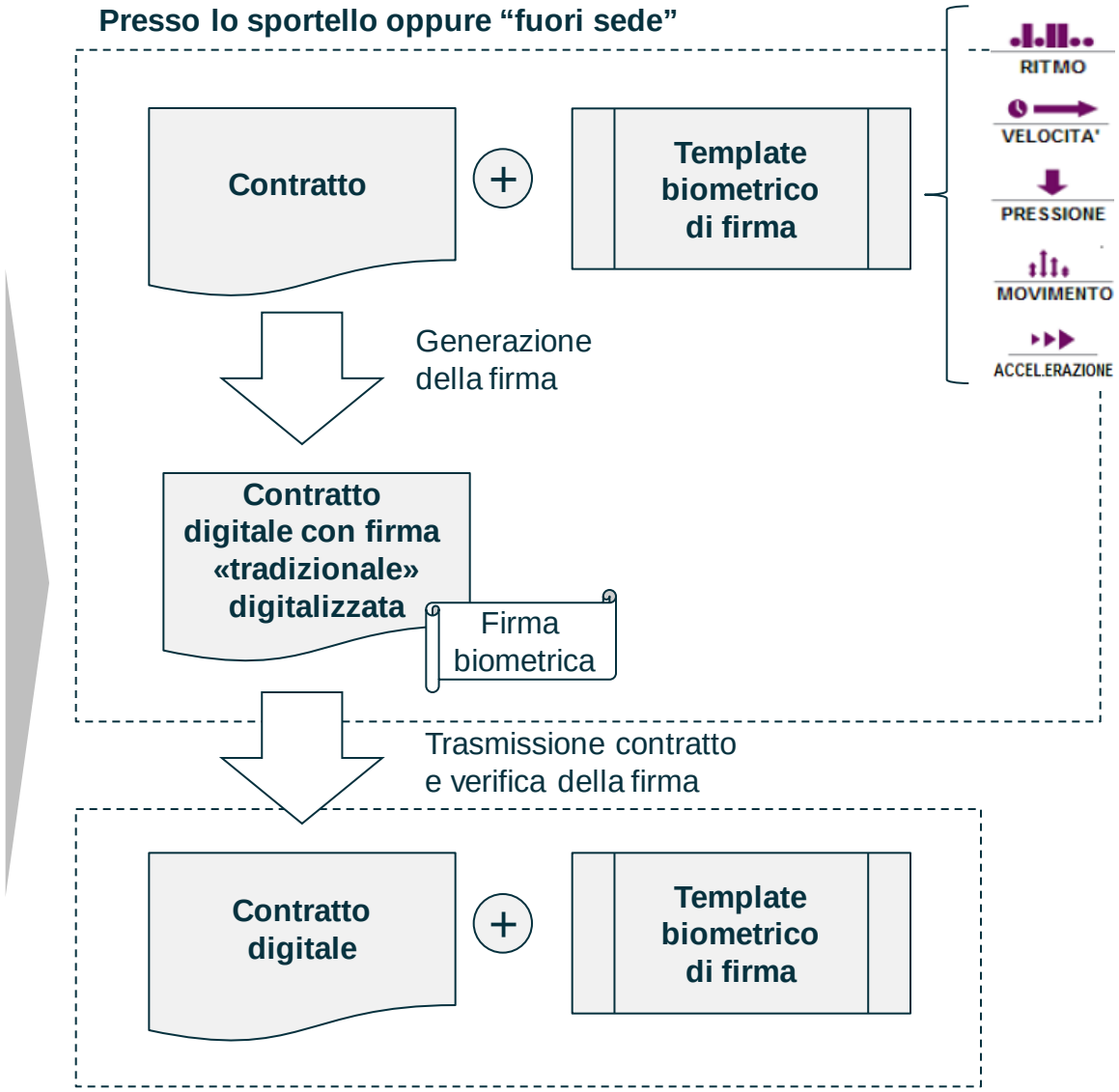
- E’ possibile produrre una firma legalmente valida anche usando le **tavolette di firma**
- Le tavolette e gli algoritmi di calcolo devono garantire i formati di firma elettronica avanzata previsti dagli **standard tecnologici UE** (CAdES, XAdES, PAdES)
- I dettagli saranno chiariti con la **pubblicazione delle Regole Tecniche**

(*) Art.2702 del codice civile

La firma biometrica è una firma elettronica avanzata

Caratteristiche

- La firma biometrica è un **processo di calcolo,** legalmente equiparato ad una **firma elettronica avanzata.**
- Si basa sulle caratteristiche grafometriche rilevate **dal tratto a penna** per generare il documento firmato.
- Per elaborare tali caratteristiche (template biometrico), sono usati **specifici devices** – le tavolette di firma - e **software ad-hoc**.
- I parametri biometrici sono allegati al contratto, che **contiene in calce** anche la **firma "tradizionale" a penna** digitalizzata.
- **La validazione** della firma avviene **direttamente in digitale,** confrontando i parametrici biometrici della firma con il profilo della firma "depositato" (in analogia ai cartellini firma "tradizionali")



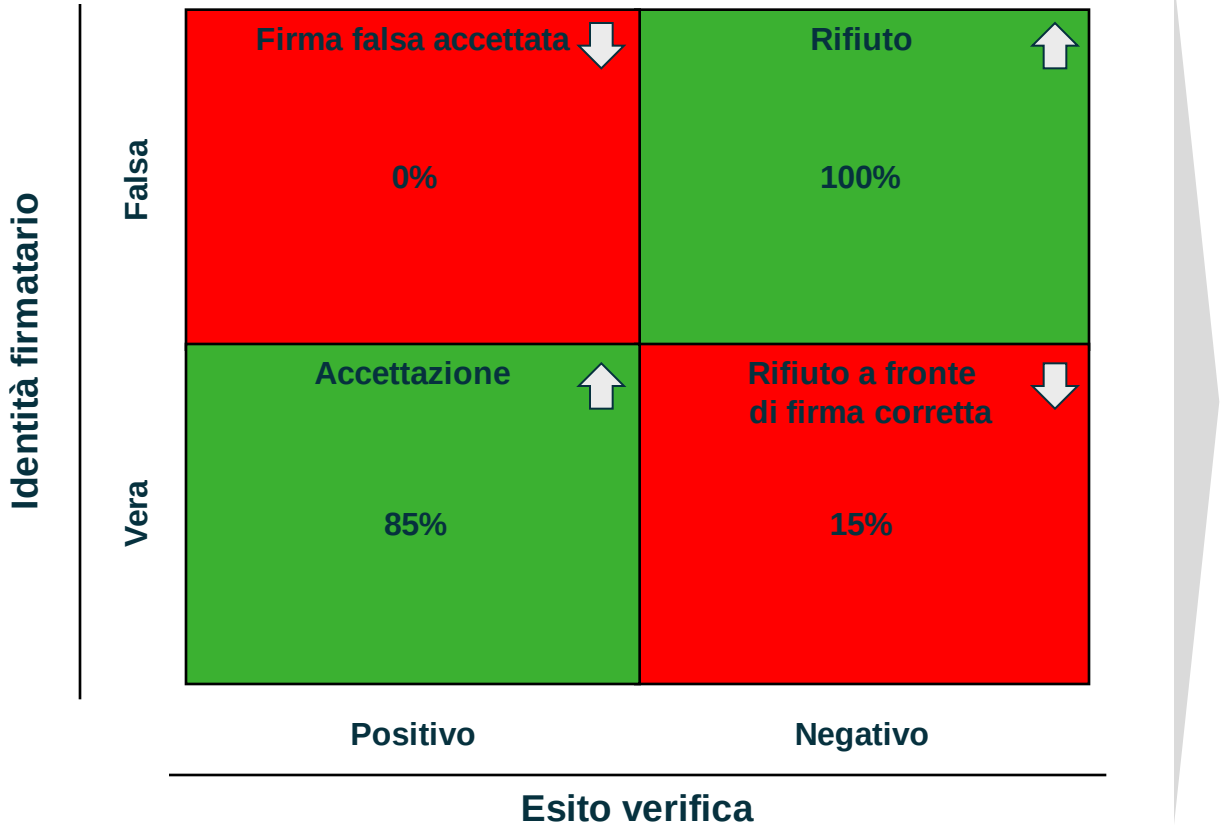
Caratteristiche dei dispositivi di firma

- I device utilizzati per l'apposizione di firme grafometriche sono **dispositivi hardware dotati di tecnologia touch** in grado di rilevare i principali parametri della firma dell'utente
- E' possibile distinguere **due macro categorie** di devices

Dispositivi	Caratteristiche	Parametri rilevati
Tablet dedicati 	• Dispositivi hardware (tablet) dedicati dotati di tecnologia touch • Postazioni fisse o portatili • Connettività verso pc via USB • Associati a speciali penne per l'apposizione delle firme • Massima accuratezza nella rilevazione dei parametri • Possibilità di impiego per enrollment (prima registrazione parametri di firma) e verifica • Costo tra i 50 e i 250 euro in funzione delle caratteristiche del display (b/n vs colori, risoluzione, ecc.)	• Pressione • Velocità • Ritmo • Accelerazione • Movimenti aerei
Dispositivi mobili 	• Dispositivi mobili dotati di tecnologia touch (es. iPad) • Utilizzo non limitato alla sola apposizione di firme • Connettività verso pc e alla rete • Accuratezza dei parametri rilevati minore rispetto ai device dedicati	• Velocità • Ritmo • Accelerazione • Movimenti aerei

L'impossibilità di rilevare la coordinata pressione tramite dispositivi mobili ne riduce il livello di confidenza

Grado di affidabilità del processo di verifica della firma grafometrica



- I produttori di tecnologie **non dichiarano** espressamente il **grado di affidabilità** delle proprie soluzioni
- Indicano in generale **un target** raggiungibile con opportuno tuning in fase di enrollment e autenticazione (**variazione dei livelli di confidenza**)
- La presenza di obiettivi contrastanti obbliga a considerare un **compromesso ottimale** tra sicurezza e usabilità del processo di firma

Sicurezza massima (+) ← **Vincoli nei processi di enrollment e verifica** → (-) **Usabilità massima**

Obiettivo: minimizzare Obiettivo: massimizzare

ESEMPLIFICATIVA

Architettura applicativa per la firma biometrica

Tavoletta di firma

- La firma autografa viene raccolta allo sportello tramite la tavoletta (*), che ne estrae i **5 parametri caratteristici**
- Tali parametri (**template biometrico**) sono trasmessi all'applicazione di firma *su connessione cifrata*

Front end di firma

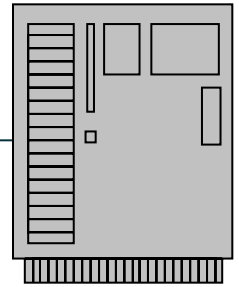
Documento digitale + template biometrico

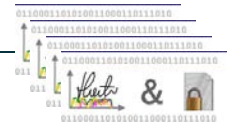
- L'applicazione (integrata nel workflow documentale **) allega il **template biometrico di firma del cliente** al contratto e lo inoltra al server centrale per la verifica di autenticità
- La firma appare sul documento come una normale firma autografa

Back-end di autenticazione

- Riceve il documento con il template biometrico
- Verifica l'autenticità della firma (ed eventualmente inserisce la marcatura temporale.

Back end di gestione dei «cartellini biometrici di firma»





- Gestisce il repository dei «**cartellini» delle firme biometriche**
- Gestisce l'enrolment del cartellino del cliente, nella fase iniziale di registrazione del template biometrico di firma (*)

Questa soluzione può essere **integrata** con un servizio di **firma digitale remota**. Lo sblocco del certificato digitale del cliente viene attivato a fronte dell'esito positivo dell'autenticazione della firma biometrica

(*) In fase di creazione del «cartellino firma biometrica», viene normalmente richiesto al titolare di eseguire più firme, in modo tale da avere un campione di dati biometrici stabile

(**) Adobe ha sviluppato uno specifico plugin di Live Cycle

Firma grafometrica – Cenni tecnici 1/2

- La biometria della firma è basata su ritmo, velocità, pressione, accelerazione e movimento della firma manuale apposta su una tavoletta elettronica (TABLET, PAD).

- In maggiore dettaglio:

  - La velocità di scrittura.
  - La pressione esercitata.
  - L'angolo di inclinazione della penna.
  - L'accelerazione del movimento.
  - Il numero di volte che la penna viene sollevata.

- Se utilizzata a sportello in presenza di un impiegato o all'interno di un'organizzazione i requisiti stabiliti per la firma elettronica avanzata sono soddisfatti.

- Naturalmente è anche necessario essere integrati in un adeguato sistema di gestione documentale. La FEA è sempre un processo informatico.

Firma grafometrica – Cenni tecnici 2/2

- La firma grafometrica è perfettamente integrabile nelle più diffuse piattaforme di gestione documentale.
- E’ possibile effettuare firme multiple sui documenti informatici integrando il workflow documentale con il tool di firma.
- Il vantaggio della dematerializzazione “a sportello” è immediatamente percettibile perché il documento nasce digitale, con piena validità legale e con un’accettazione molto elevata da parte dell’utente.
- E’ opportuno che all’utente vengano illustrati i parametri di sicurezza del sistema.

Un esempio + un tablet

Un esempio di tecnologia

Hardware

Software con analista grafologico

La FEA nella bozza di regole tecniche - 1

- Si fa riferimento al testo prodotto da DigitPA e diramato al Garante per la protezione dei dati personali e alla Conferenza Unificata.

- Alla FEA sono dedicati i nuovi articoli dal 55 al 61 tutti contenuti nel Titolo V dello schema di decreto.

- Nessuna soluzione di FEA può essere soggetta a vincoli preventivi comprese le autorizzazioni.

- Nell'articolo 55, comma 2 una banca può essere il soggetto di cui alla lettera a); un "*system integrator*" quello di cui alla lettera b). Oneri e responsabilità sono specifici per la categoria individuata.

La FEA nella bozza di regole tecniche - 2

- **Le soluzioni di FEA devono garantire:**

  – l'identificazione del firmatario del documento;
  – la connessione univoca al firmatario;
  – il controllo esclusivo del firmatario sul sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma;
  –la possibilità di verificare che l'oggetto della sottoscrizione non abbia subito modifiche dopo l'apposizione della firma;
  –la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
  –l'individuazione del soggetto "erogante";
  –l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, i fatti, o dati nello stesso rappresentati.

La FEA nella bozza di regole tecniche - 3

- **Il soggetto erogante deve:**
  - identificare in modo certo l'utente, informarlo in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di un dichiarazione di accettazione delle condizioni del servizio da parte dell'utente.
  - conservare per almeno vent'anni la dichiarazione di accettazione e ogni altra informazione atta a dimostrare l'ottemperanza ai requisiti di FEA garantendone la disponibilità, integrità, leggibilità e autenticità.
  - Fornire liberamente e gratuitamente copia della dichiarazione precedente e delle eventuali altre informazioni al firmatario se richieste da quest'ultimo.

La FEA nella bozza di regole tecniche - 4

- rendere note le modalità con cui effettuare la richiesta appena descritta pubblicandole anche sul proprio sito internet.
- rendere note le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto, pubblicandole anche sul proprio sito internet.
- consentire l'uso della firma elettronica qualificata e della firma digitale, ove applicabile, in alternativa alla firma elettronica avanzata per i procedimenti per i quali è previsto l'uso della FEA.
- assicurare la disponibilità di un servizio di revoca relativo alla firma elettronica avanzata, ove applicabile, e un servizio di assistenza. Il presente comma non si applica alle soluzioni di PEC (Posta Elettronica Certificata) e CIE/CNS (Carta d'Identità Elettronica/Carta Nazionale dei Servizi).

La FEA nella bozza di regole tecniche - 5

- Il soggetto “erogante” deve poter rispondere di eventuali danni derivanti dall’attività svolta per almeno 500.000 euro.
- Ci si può assicurare e i soggetti interessati sono informati anche tramite il sito internet su come ottemperare all’opzione.
- Altre regole sono per la pubblica amministrazione e per i fruitori di prestazioni sanitarie.
- Ulteriori altre regole riguardano il fornitore della soluzione quindi tipicamente il “*system integrator*”.

La FEA nella bozza di regole tecniche - 6

- La FEA realizzata in conformità con le disposizioni delle presenti regole tecniche, è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto «erogante».

- Sono sicuramente soluzioni di FEA la trasmissione di PEC con richiesta di ricevuta completa in conformità alle vigenti regole tecniche di settore e l'uso della CIE e della CNS.

- La CIE e la CNS sono utilizzabili dalle pubbliche amministrazioni.

- Non è chiaro nello schema di decreto, ma quanto appena detto non sembra escludere soggetti privati sul tema CIE/CNS.

La FEA e la privacy - 1

- Qualora si voglia utilizzare per la FEA la firma grafometrica è doveroso valutare le implicazioni in materia di ottemperanza alla 196/2003 (Privacy).

- Questo perché la firma grafometrica utilizza dati biometrici.

- Considerate le posizioni storiche del Garante Privacy in materia di trattamento dei dati biometrici se ne deduce un atteggiamento prudente sul tema.

- Deve essere valutato l'art. 17 della 196/2003 rispetto al tema della verifica preliminare (prior checking).

La FEA e la privacy - 2

- Il soggetto “eroganete” può valutare dopo le considerazioni organizzative se nel trattamento dei dati si presentano rischi specifici per i diritti e le libertà fondamentali dell’interessato.

- In tal caso la verifica preliminare è obbligatoria.

- In generale questi rischi non ci sono, ma può essere opportuno e di adeguata cautela per il soggetto “erogante” valutare se effettuare la verifica preliminare.
  Comunque nessun soggetto, oggi, vi ha fatto ricorso accettando i rischi relativi.

- Questioni di sicurezza attinenti all’articolo 25 dell’allegato B della 196/2003 sono a carico del “*system integrator*” in stretta successione all’individuazione della soluzione tecnologica.

Contatti

Giovanni Manca
e-mail:
mncgnn59@gmail.com