

## Workshop: “Telemedicina e Sanità elettronica: facciamo il punto !“

### Il ruolo della sicurezza delle informazioni nella Sanità elettronica

**Corrado Giustozzi**  
*Security Evangelist – Capgemini Italia*  
*Responsabile Data Security SIT*  
*Società Italiana Telemedicina e sanità elettronica*

**Roma, 24 giugno 2010**  
**Palazzo dei Congressi all'Eur**

# Chi sono



- “Security evangelist” e consulente di sicurezza delle informazioni... da tempi non sospetti (1986):
- docente di “Informatica forense” (sicurezza delle informazioni e criminalità informatica) all’Università dell’Aquila
- membro del Comitato Scientifico della Unità di Analisi sul Crimine Informatico (UACI) della Polizia Postale e delle Comunicazioni
- membro del Permanent Stakeholder’s Group dell’Agenzia Europea per la Sicurezza delle Reti e delle Informazioni (ENISA)
- responsabile Data Security della SIT



# Il bene supremo della società



- La nostra è la “società dell’informazione”
- L’informazione “tradizionale” è:
  - materiale e coincidente col suo supporto fisico
  - facilmente proteggibile con mezzi fisici
- L’informazione “moderna” è:
  - immateriale e svincolata dal suo supporto fisico
  - difficilmente proteggibile con metodi tradizionali
- L’informazione digitale può facilmente essere:
  - intercettata, copiata, trasportata, spostata, diffusa
  - modificata, contraffatta, falsificata, alterata
  - distrutta

# La sanità “smaterializzata”



- La smaterializzazione delle attività crea valore:
  - superamento delle barriere geografiche e sociali
  - rapporti più efficaci con i propri assistiti
  - rapporti più efficienti verso le altre strutture preposte
- Ma introduce anche nuovi rischi...:
  - frodi e truffe
  - intrusioni telematiche, sabotaggi, attacchi vandalici
  - violazione, divulgazione o abuso di dati sensibili
- ...e nuovi problemi:
  - complessità nella gestione del “documento non-materiale”
  - costo, complessità, difficoltà di uso delle nuove tecnologie
  - valore legale ed interoperabilità delle soluzioni tecniche

# Di cosa stiamo parlando?

---



- Medicina telematica non è più solo “consulto”
- In medicina telematica vigono ormai le stesse esigenze delle aziende tradizionali:
  - dirigenti “mobili” sul territorio che devono rimanere in contatto col sistema informativo aziendale
  - clienti remoti cui bisogna fornire servizi interattivi
  - scambio di documenti digitali verso i partner, i clienti, i fornitori
- I problemi di sicurezza sono i medesimi, ma aggravati dalla sensibilità dei dati trattati:
  - rischio di divulgazione illecita (violazione della privacy)
  - rischio di alterazione o modifica (truffa)
  - rischio di perdita, sottrazione, cancellazione
  - problematiche (anche legali) di autenticazione e responsabilità

# Quale sicurezza per l'e-health?



- Il ruolo della sicurezza delle informazioni è sempre almeno duplice:
  - prevenire o mitigare azioni indesiderabili, naturali o dolose:
    - incidenti, disastri, errori, sabotaggi, truffe, attacchi, ...
  - fornire garanzie a supporto di azioni desiderate:
    - certezza dell'accaduto, integrità, responsabilità anche legale...
- Nel caso della sanità elettronica ciò si declina in:
  - protezione delle informazioni sanitarie:
    - tutela della riservatezza, integrità, disponibilità del dato medico
  - attribuzione di certezze (anche legali) agli atti medici:
    - autenticazione ed autorizzazione dei soggetti e dei sistemi
    - audit: chi ha fatto cosa (e anche come, quando, dove, perché)
    - valore legale al documento informatico formato e trasmesso

# Piccola parentesi lessicale



- Il termine “autenticazione”, comunemente usato nel linguaggio tecnico, è doppiamente ambiguo
- Problema terminologico:
  - giuridicamente l'**autenticazione** la fa il **notaio**, e si riferisce solo a **documenti** e non a persone!
  - il riconoscimento dell'identità personale, ad esempio da parte di un pubblico ufficiale, si chiama **identificazione**
- Problema semantico:
  - **identificazione**: accertare l'identità di un soggetto
  - **autorizzazione**: accertare il diritto di un *soggetto identificato* ad usufruire di servizi o ad accedere a risorse secondo determinate modalità e con eventuali limiti

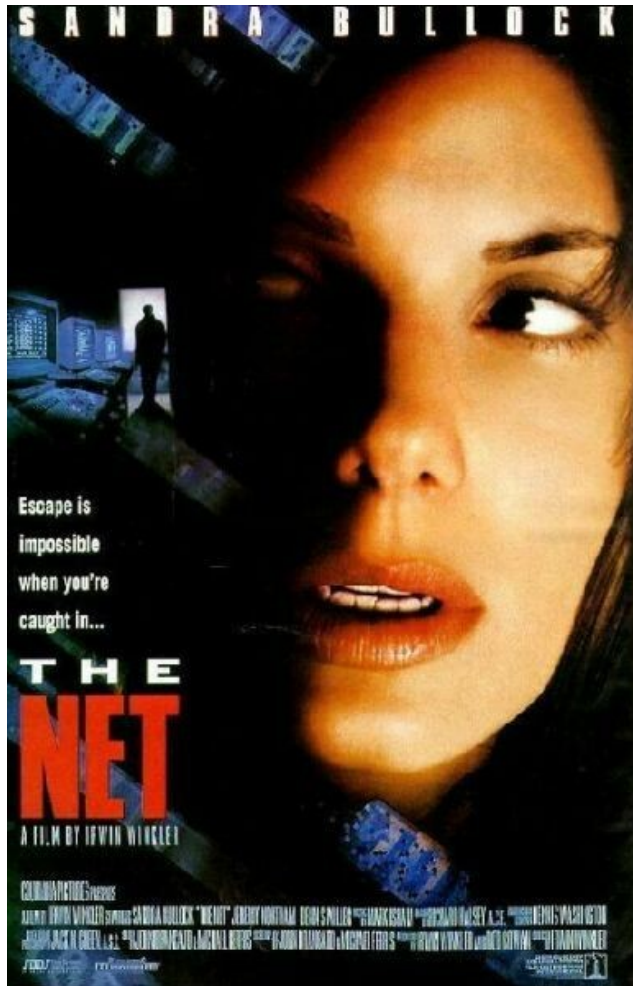
# Il problema dell'identità in Rete

---



- Nel nostro mondo moderno, digitale e sempre più smaterializzato, assume fondamentale importanza la possibilità di *identificare in Rete*, ossia da remoto e senza interventi umani, i soggetti che accedono a servizi telematici
- Il problema solitamente è duplice:
  - il soggetto deve potersi identificare al sistema
  - il soggetto deve poter dimostrare al sistema il proprio *profilo*, ossia l'insieme dei servizi cui ha diritto di accedere assieme alle modalità ed ai limiti per farlo
- La soluzione “ovvia”: un *documento d'identità*:
  - il suo possesso costituisce prova di identità del soggetto
  - riporta e “dimostra” le facoltà o le autorizzazioni del soggetto

# Rischi futuri: il furto di identità



- Per opportunità o obblighi, il *netizen* vive e si esprime sempre più soltanto in Rete
- Anche senza chiamare in causa la fantascienza, la Rete tende a mediare e sostituire i contatti sociali (il che non è sempre un male!...)
- Il problema principale in futuro sarà sempre più il *furto d'identità*
- La dimensione transnazionale della Rete e dei suoi servizi non fa che aggravare i rischi e i problemi...

# Evoluzione del “documento”



- Il documento “classico”:
  - è un *oggetto materiale* che coincide col suo *supporto*
  - è unico e originale, si distingue dalle copie
  - richiede una modifica fisica per l'autentica
- Il documento “moderno”:
  - è un *oggetto immateriale* (contenuto informativo) del tutto indipendente dal tipo di supporto che lo ospita
  - ogni copia è un originale, anche su altro supporto
  - non ammette modifiche fisiche
- Il documento elettronico (definizione legale):
  - “*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*” (ex DPR 513/97 e CodAmmDig)

# Le garanzie necessarie

---



- Da sempre l'uomo ha chiesto ai documenti alcune importanti certezze:
  - autenticità
  - integrità
  - non ripudio
  - confidenzialità
- Per ottenere queste certezze si è sempre fatto ricorso a *modifiche fisiche* al documento:
  - firme, sigilli, timbri, punzoni, filigrane, ologrammi, ...
- ...ma il documento moderno è *immateriale!*
  - come agire in mancanza di un *supporto fisico*?

# I problemi non sono tecnici...

---



- Le soluzioni tecniche esistono da anni:
  - firma digitale per la validazione dei documenti elettronici
  - sistemi di identificazione/autorizzazione “forti” per la validazione dei soggetti umani e l’attribuzione di volontà
  - reti sicure per la trasmissione certa e affidabile
- Tuttavia rimangono ancora molti problemi:
  - complessità e costi delle tecnologie
  - vincoli legali (la legislazione non aiuta...)
  - paradigmi d’interazione sociale superati
- Il caso della firma digitale:
  - dopo 15 anni ancora non decolla!
  - lo strumento ideale (firma “d’infrastruttura”) è formalmente legale ma sostanzialmente quasi impossibile da attuare!

# ...ma organizzativi



- Nella maggior parte dei problemi di sicurezza, la soluzione non è solo tecnica ma soprattutto è **organizzativa**
- In un settore critico come quello della sanità non si può lasciare che ciascuno faccia ciò che vuole: le tematiche più problematiche sono quelle legate alla **interoperabilità di processo** delle soluzioni!
- La sanità è il settore della PA che produce più “certificazioni” e più “firme”, eppure nessuno sembra essersene accorto...
- Occorrerebbe istituire un tavolo interdisciplinare di **addetti ai lavori** per stabilire le *regole del gioco*...

# E la cooperazione in EU?...

---



- Armonizzazione giuridica e legislativa:
  - stesso valore legale ovunque dell'identità digitale
  - stesso valore legale ovunque del documento digitale
  - stesso valore legale ovunque della firma digitale
- Armonizzazione tecnologica:
  - adozione di strumenti comuni o compatibili
  - interoperabilità dei protocolli
- Armonizzazione organizzativa:
  - chi decide gli standard?
  - chi verifica chi?
  - chi garantisce per chi?

# Workshop: “Telemedicina e Sanità elettronica: facciamo il punto !“

**Grazie per l'attenzione**

**Corrado Giustozzi**  
*[corrado.giustozzi@capgemini.com](mailto:corrado.giustozzi@capgemini.com)*  
*[corrado.giustozzi@sanitaelettronica.it](mailto:corrado.giustozzi@sanitaelettronica.it)*

**Roma, 24 giugno 2010**  
**Palazzo dei Congressi all'Eur**