L'*information technology* nella prevenzione e nella sicurezza del dato di laboratorio

M. Pradella[a,b], A. Pastorino[c]

[a]*Laboratorio Analisi Chimico Cliniche, Ospedale Civile, Castelfranco Veneto (TV)*
[b]*CISMEL, Comitato Italiano per la Standardizzazione dei Metodi Ematologici e di Laboratorio, www.cismel.it*
[c]*Presidente Commissione Informatica Medica UNI*

Riassunto

Il prodotto dei laboratori medici come prestazione assistenziale è costituito da informazioni. Gran parte delle garanzie di sicurezza della medicina di laboratorio passa quindi attraverso le tecnologie informatiche. Il sistema informatico deve innanzitutto garantire le misure minime stabilite dall'art. 169 del Codice della Privacy (D.Lvo 196/03), per le quali sono previste sanzioni penali. I requisiti di riservatezza, integrità e disponibilità delle informazioni digitali sono oggetto di diverse norme tecniche. ISO/IEC 17799 descrive come realizzare l'analisi dei rischi per la sicurezza e fornisce una lista di obiettivi di controllo in 11 aree, per un totale di 39 categorie. ISO/DIS 27799 definisce le linee guida per l'interpretazione e la realizzazione delle procedure 17799 nell'informatica sanitaria. ISO/IEC 27001 introduce il concetto di "Sistema per la Gestione della Sicurezza Informatica" e descrive il quadro dei controlli da realizzare. ISO/TR 16142 guida alla selezione delle norme tecniche per la sicurezza. CEN/TS 15260 introduce le tecniche di "risk management" nel contesto dell'informatica sanitaria, in analogia a quanto accade per i dispositivi medici. EN 14484 riguarda il trasferimento internazionale di dati personali. Il sistema di norme ISO 17090 codifica la natura e l'uso dell'infrastruttura di chiave pubblica, ossia della firma digitale. ENV 12924 fornisce gli strumenti per costruire il proprio profilo di rischio e scegliere il livello delle misure opportune di sicurezza. La gestione delle verifiche, degli errori e delle correzioni dei dati di laboratorio invece va ricercata nelle norme della buona pratica professionale, come le checklists del College of American Pathologists, e nelle linee guida per l'utilizzo dei protocolli dei messaggi HL7.

Summary

Information technology in prevention and safety of laboratory data

The product of the medical laboratories as health care activity is information. Therefore, most of safety assurance of laboratory medicine passes through the computer science technologies. The informatic system first of all must guarantee the minimal measures established by art. 169 of the Code of the Privacy (D.Lvo 196/03), for which penal endorsements are previewed. Requirement of confidentiality, integrity and availability of the digital information are object of various technical norms. ISO/IEC 17799 describes how to realize the risk analysis for the emergency and supplies a list of targets of control in 11 areas, for a total of 39 categories. ISO/DIS 27799 defines the guidelines for the interpretation and the realization of 17799 procedures in health care informatics. ISO/IEC 27001 introduces the concept of "Information Security Management Systems" and describes the framework of the controls to realize. ISO/TR 16142 guides to the selection of the standard documents for safety. CEN/TS 15260 introduces the techniques of "risk management" in the context of health care informatics, in analogy to what happens for the medical devices. EN 14484 regards the international transfer of personal data. The system of standard ISO 17090 codifies the nature and the use of the public key infrastructure, that is digital signature. ENV 12924 supplies the instruments to build the profile of risk and to choose the level of the opportune measures of safety. On the other hand, the management of verifications, errors and corrections of the laboratory data must be searched in the standards of good professional practice, like the checklists of the College of American Pathologists, and in the guidelines for using the protocols of messages HL7.

Introduzione

Dai laboratori di analisi mediche si ottengono informazioni. Se vogliamo allestire misure di sicurezza, quindi, dobbiamo prendere in considerazione soprattutto le norme per la sicurezza informatica. Non solo, poiché le informazioni sono quasi sempre oggetti digitali, le procedure di verifica e correzione degli errori utilizzano per forza strumenti informatici.

Le fonti sono diverse: troviamo regole in dispositivi di legge, in documenti europei (CEN, Comitato Europeo per la Normazione) ed internazionali (ISO, Organizzazione Internazionale per gli Standard). Non possiamo però trascurare le linee guida CLSI (Clinical Laboratory Standard Institute) che, pur nascendo in un contesto america-

Ricevuto: 06-07-2006 Pubblicato on-line: 25-09-2006

Corrispondenza a: Dott. Marco Pradella, Laboratorio Analisi Chimico Cliniche e Microbiologia, Ospedale Civile, Via Ospedale, 18, 31033 Castelfranco Veneto (TV). Tel. 0423-732407, fax 0423-732417, e-mail: pradellamarco@yahoo.it

Tabella I. Misure minime obbligatorie secondo il Codice della Privacy (art. 34 e 35; sanzioni all'articolo 169, arresto fino a due anni o ammenda da diecimila a cinquantamila euro).

Con strumenti elettronici	*Senza l'ausilio di strumenti elettronici*
a. autenticazione informatica;	a. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b. adozione di procedure di gestione delle credenziali di autenticazione;	b. previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c. utilizzazione di un sistema di autorizzazione;	c. previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.
d. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;	
e. protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;	
f. adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;	
g. tenuta di un aggiornato documento programmatico sulla sicurezza;	
h. adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.	

no, hanno valenza globale.

Le regole della buona pratica di laboratorio (ad esempio, quelle del College of American Pathologists per l'accreditamento dei laboratori, volontario ed istituzionale) prevedono l'utilizzo dei dispositivi informatici per la verifica dei risultati, la rilevazione degli errori, la correzione e la documentazione.

Il codice della privacy, con sanzioni penali

Il decreto 196/2003, in vigore già dal gennaio 2004, contiene alcune importanti sanzioni penali, poco note ma non per questo trascurabili[1] (Tab. I). Illeciti penali sono puniti agli articoli del capo II del Titolo III (Sanzioni). Reclusione da sei mesi a tre anni per la violazione delle prescrizioni sul trattamento dei dati personali (art. 18, trattamento solo fini istituzionali: art. 19, comunicazione solo fini istituzionali; art. 23, consenso espresso dell'interessato; art. 123, traffico elettronico; art. 126, dati relativi all'ubicazione; art. 130, comunicazioni indesiderate; art. 129, elenchi). Le pene maggiori, da uno a tre anni, sono riservate alle violazioni più gravi (art. 17, diritti e le libertà fondamentali, dignità; art. 20, dati sensibili; art. 21, dati giudiziari; art. 22, dati sensibili e giudiziari, comma 8, diffusione, e comma 11, test psico-attitudinali e diffusione; art. 25, comunicazione e diffusione; art. 26, consenso per dati sensibili; art. 27, dati giudiziari; art. 45, trasferimento altro Stato). La violazione di queste prescrizioni costituisce delitto ed alla pena si aggiunge in ogni caso la pubblicazione della sentenza (art. 172).

Particolarmente interessante per noi è l'articolo 169, Misure di sicurezza: "Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro". Le misure minime dell'articolo 33 o ai sensi dell'articolo 58, comma 3, sono volte ad assicurare un livello minimo di protezione dei dati personali. L'elenco si trova nei successivi art. 34, Trattamenti con strumenti elettronici, e art. 35, Trattamenti senza l'ausilio di strumenti elettronici.

La prescrizione fondamentale si chiama "autenticazione informatica" (Tab. II). In sostanza, non è più legale accedere ai dati personali e sensibili in modo anonimo, senza identificarsi, o con le ben note "login di reparto" o "di qualifica" (password del medico, della caposala, etc..). Ogni atto compiuto nell'area digitale dei dati sensibili richiede una "firma" individuale, qualunque sia la natura dell'atto stesso. Ciò sconvolge molti pregiudizi, e forse qualche aspettativa categoriale, basati in vario modo sul concetto di "firma". La digitalizzazione delle informazioni consente di separare gli atti, per i quali è sempre richiesta una "firma", dai messaggi, per i quali può essere applicata o meno, a seconda del contesto, una autenticazione digitale. Che però riguarda il messaggio, non l'autore degli atti a cui il messaggio stesso si riferisce.

Codice della Privacy, le violazioni amministrative

Se le sanzioni penali del decreto 196/03 sono pesanti, quelle amministrative non sono da meno. L'omessa o inidonea informativa all'interessato (art. 161 ed art. 13) si paga da tremila a trentamila euro, aumentabile fino a novantamila se il contravventore è economicamente forte.

L'informativa consiste nella comunicazione di: *a.* le finalità e le modalità del trattamento cui sono destinati i dati; *b.* la natura obbligatoria o facoltativa del conferimento dei dati; *c.* le conseguenze di un eventuale rifiuto di rispondere; *d.* i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; *e.* i diritti di cui all'articolo 7; *f.* gli estremi identificativi del titolare e del responsabile.

I diritti elencati all'articolo 7 sono quattro.

1. ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. ottenere l'indicazione: *a.* dell'origine dei dati personali; *b.* delle finalità e modalità del trattamento; *c.* della logica

Tabella II. Codice della Privacy (Decreto Legislativo 30 giugno 2003 n. 196): definizioni intorno al concetto di "autenticazione informatica" (art. 4 comma 2).

c. "**autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
d. "**credenziali di autenticazione**", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
e. "**parola chiave**", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
f. "**profilo di autorizzazione**", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
g. "**sistema di autorizzazione**", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; *d.* degli estremi identificativi del titolare, dei responsabili, del rappresentante; *e.* dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza.

3. ottenere: *a.* l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; *b.* la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge.
4. opporsi, in tutto o in parte: *a.* per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; *b.* al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale. Ovvero, ognuno ha diritto al pieno anonimato.

Le direttive per la pubblica amministrazione

E' abitudine di chi lavora in strutture pubbliche ascrivere alla lentezza della catena burocratica la causa delle inadempienze normative e dell'arretratezza rispetto allo stato dell'arte e della tecnologia. Nel nostro caso ciò è un po' più difficile. Il Ministro per l'innovazione e le tecnologie già con la Direttiva del 18 Dicembre 2003 (Linee guida in materia di digitalizzazione dell'amministrazione per l'anno 2004)[2] ha richiamato alla lettera f) (sicurezza delle tecnologie dell'informazione e della comunicazione) la precedente direttiva del marzo 2002, lamentando che gli impegni allora indicati nella (autovalutazione del livello di sicurezza, adeguamento alla "base minima" di sicurezza), non siano ancora compiutamente realizzati. L'ordine perentorio del governo è quindi che le amministrazioni debbano, "*...al più presto, adeguare le propria struttura, almeno, ai livelli di sicurezza minimi richiesti, rivolgendo l'attenzione sia all'ambito organizzativo che alla realizzazione di attività operative...*".

Norme tecniche (Standard) e altre specifiche ISO: TR 16142, DIS 27799

ISO TC 210, che lavora nel campo dei dispositivi medici, si è interessato più volte di sicurezza, danno e rischio, anche per la implicazioni economiche nei riguardi delle aziende che li producono. Negli ultimi anni anche l'ISO TC 215, per l'informatica sanitaria, non ha fatto mancare i suoi contributi. La Tabella III riassume solo quelli più recenti e significativi, mentre nella parte B. sono citati quelli di altri settori ISO sullo stesso tema.

TR 16142 (Guidance on the selection of standards)[3] richiama le informazioni essenziali per recuperare le direttive ISO nel campo della sicurezza dei dispositivi medici. Espone la distinzione tra basic standard (o standard orizzontale: concetti fondamentali, principi e requisiti generali), group standard (o standard semiorizzontale: sicurezza e prestazioni di una famiglia di prodotti simili) e product standard (o standard verticale: sicurezza e prestazioni di un prodotto specifico o di una famiglia compresa nello scopo di un comitato o sottocomitato tecnico). Il numero di documenti citati nel 16142 è molto grande. Come riferimenti generali, ad esempio, riporta ISO Guide 51, Guidelines for the inclusion of safety aspects in standards; ISO Guide 63, Guidance on the development of International Standards in the field of health care technology; ISO Guide 64, Guide for the inclusion of environmental aspects in product standards; IEC 60513, Fundamental aspects of safety standards for medical electrical equipment. Tra i riferimenti più specifici, invece, troviamo ISO 14971 Medical devices - Application of risk management to medical devices; ISO 13485 Medical devices - Quality management systems - Requirements for regulatory purposes; ISO/TR 14969 Medical devices - Quality management systems - Guidance on the application of ISO 13485:2003; ISO 14155 series, Clinical investigations of medical devices for human subjects.

ISO/IEC DIS 27799 (Health Informatics - Security management in health using ISO/IEC 17799)[4] intende guidare per mano all'applicazione in ambito sanitario della norma 17799 per la sicurezza informatica. ISO 17799: 2005 deriva da un documento inglese (BS7799) che ha faticato non poco per essere accolto come norma ISO e tutt'ora lo è solo parzialmente.

ISO 17799[5] enuncia le tre componenti della sicurezza informatica: riservatezza, integrità e disponibilità dell'informazione. Riporta quindi nella prima parte le raccomandazioni per la gestione della sicurezza, descrivendo dieci aree di intervento e sei fasi di analisi. Nella seconda parte, invece, sono contenuti ben 127 "controlli", come indicazioni specifiche per la certificazione della sicurezza.

Il metodo per affrontare i rischi per la sicurezza viene già stabilito dalla serie **ISO 13335** (Guidelines for the management of IT Security) e prevede la netta distinzione tra la fase dell'analisi e quella della gestione. L'analisi può dirsi completa solo se esplora tutte le 10 aree di intervento previste: 1. politica 2. principi organizzativi 3. controllo classificazione patrimonio 4. personale 5. fisica ambientale 6. comunicazioni e operazioni 7. accessi 8. sviluppo manutenzione sistemi 9. gestione continuativa 10. controlli con-

Tabella III. Selezione norme ISO per la sicurezza informatica.

A. sicurezza informatica sanitaria
- ISO TR 16142 Medical devices - Guidance on the selection of standards in support of recognized essential principles of safety and performance of medical devices
- ISO 17090-1: Health Informatics - Public Key Infrastructure - Part 1: Overview of digital certificate services. ISO 17090-2: Health Informatics - Public Key Infrastructure - Part 2: Certificate profile. ISO 17090-3: Health Informatics - Public Key Infrastructure Part 3: Policy management of certification authority.
- ISO 22857 "Health Informatics: Guidelines on data protection to facilitate trans-border flows of personal health information".
- ISO TS 22600-1: Health informatics - privilege management and access control - Part and policy management. ISO TS 22600-2: Health informatics - privilege management and access control - Part models. ISO PDTS 22600-3: Health informatics - privilege management and access control Implementations (under development).
- ISO/TS 21091 Health informatics - directory services for security, communications, and of professionals and patients.
- ISO CD TS 21298 Health informatics - functional and structural roles.
- ISO TR 20514, Health informatics - Electronic health record - Definition, scope and context
- ISO/IEC DIS 27799 Health Informatics - Security management in health using ISO/IEC 17799
- ISO CD TS 25238 Health Informatics : Classification of Safety Risks from Health Software

B. Sicurezza informatica generale
- ISO/IEC 17799:2005, Information technology - Code of practice for information security management
- ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 15408, Information Technology-Security techniques - Evaluation Criteria for IT Security (Parts 1, 2 and 3), 1999.
- ISO/IEC TR 13335-1 Information technology - Guidelines for the management of IT Security - Part 1: Concepts and models for IT security. ISO/IEC TR 13335-2 Information technology - Guidelines for the management of IT Security - Part 2: Managing and Planning IT security. ISO/IEC TR 13335-3 Information technology - Guidelines for the management of IT Security - Part 3: Techniques for management of IT security. ISO/IEC TR 13335-4 Information technology - Guidelines for the management of IT Security - Part 4: Selection of Safeguards. ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security

formità. Lo sviluppo del sistema di sicurezza procede in sei fasi: I scopo II politica III valutazione rischio IV gestione rischio V controlli VI dichiarazioni applicabilità. Per adeguarsi a ISO 9001:2000 si richiama l'esigenza del circolo di qualità (modello Plan Do Check Act. Pianificare: scopo, politica, rischio, opzioni, controlli; attuare: piano trattamento rischi, formazione, gestione operazioni e risorse, gestione incidenti; verificare: monitoraggio, audit, rischio residuo, azioni ed eventi; agire: cambiamenti, azioni correttive preventive, comunicazione risultati).

Alla serie di norme tecniche ISO 17090 (Public Key Infrastructure) come esempio di tecnologia per la sicurezza sarà dedicata una sezione successiva.

Norme tecniche (Standard) e altre specifiche CEN: ENV 12924, TS 15260 e EN 14484

Anche in ambito europeo molto lavoro è stato compiuto intorno alle tematiche della sicurezza informatica (Tab. IV).

ENV 12924: "Security categorisation and protection for healthcare information systems", prodotta dai gruppi III e IV del CEN TC 215, dal 3.6.2005 in corso di revisione, costituisce un esempio paradigmatico di linea guida per affrontare concretamente la gestione dei rischi informatici in sanità[6]. ENV 12924 descrive le attività per la sicurezza come un processo, piuttosto che un'intervento puntuale, che circola in modo ricorsivo dall'analisi dei rischi alla definizione dei requisiti ed all'adeguamento alle direttive. Pone in evidenza gli elementi spesso trascurati di un sistema informativo sanitario, in favore di hardware e software: l'ambiente, ossia la "stanza" del computer, le connessioni, i terminali; le persone, con la loro eterogeneità ed i differenti modi di accesso fisico e logico; la natura dei dati, in cui vanno separate le caratteristiche di riservatezza, integrità e disponibilità. Tramite le risposte a semplici domande relative alla disponibilità (A = availability), alla riservatezza (C = confidentiality) ed alla integrità (I), graduate in non critica-critica oppure non sensibile – sensibile – molto sensibile, si può costruire una griglia di categorie, da I a VI, utile per accedere a diversi pannelli di requisiti generali e specifici, chiamati profili di protezione. Alla definizione delle categorie concorrono l'ambiente fisico (accesso fisico al sistema, presenza di personale di staff, sorveglianza), la connessione fisica alla rete, la connessione logica in un solo dominio e in una sola struttura sanitaria o no.

Obiettivo simile hanno il progetto, presentato recentemente come nuovo argomento (new work item proposal, NWIP, del 7.6.2005) ed il conseguente documento **CEN/TS 15260** Health informatics - Classification of safety risks from health informatics products (approvato il 31.3.2006)[7].

Il progetto CEN parte dalla considerazione che l'informatica appare fuori dallo stretto controllo che viene realizzato per i dispositivi medici, mentre assistiamo alla crescente diffusione di sistemi di supporto alla diagnosi, sotto la pressione di fattori economici (tempo) e legali, e la transizione a pratiche paperless accresce il rischio di corruzione e perdita di dati.

Le indicazioni del *TS 15260* partono dai principi della analisi dei rischi. Ogni rischio ha due dimensioni: la sua probabilità e la gravità delle conseguenze. Per tutt'e due si propone una scala qualitativa in cinque gradi, formando così una matrice di 25 celle, raggruppate a loro volta in cinque classi di rischio. La dimensione di probabilità, che in molti altri casi può essere quantitativa, come frequenza relativa di eventi, nel caso dello strumento informatico, per la scarsità della casistica, deve essere induttivamente qualitativa (Tab. V).

Tabella IV. Selezione documenti CEN per la sicurezza informatica sanitaria.

ENV 12924: Medical Informatics - Security Categorisation and Protection for Healthcare Information System
EN 12251 Health informatics - Secure user identification for health care - Management and security of authentication by passwords
prEN 13608 Health Informatics - Security for Healthcare Communication (SEC-COMM) part 1 Concepts and terminology, part 2 Secure Data Objects, part 3 Secure Data Channels
NWIP "Health informatics- Assuring patient safety of health informatics products"
CEN/TS 15260 Health informatics - Classification of safety risks from health informatics products
EN 14484 Health informatics - International transfer of personal health data covered by the EU data protection directive (July 2003)

Tabella V. Classi di probabilità del rischio informatico secondo CEN/TS 15260.

Categoria di probabilità	*Scopo*
Molto alta	Certo o quasi certo, molto probabile
Alta	Non certo ma molto possibile, ragionevolmente atteso nella maggior parte dei casi
Media	Possibile; non si può escludere che accada
Bassa	Capita, ma non nella maggior parte dei casi
Molto bassa	Trascurabile o quasi trascurabile la possibilità che avvenga

EN 14484 (International transfer of personal health data covered by the EU data protection directive July 2003)[8] costituisce un altro tipico esempio di norma europea. Molti documenti internazionali si riferiscono a questo tema: EU Data Protection Directive "on the protection of individuals with regard to the processing of personal data and free movement of that data" [1]; · OECD "Guidelines on the Protection of Privacy and Trans-border flows of Personal Data" [2]; · OECD "Guidelines for the Security of Information Systems" [3]; · Council of Europe "Convention for the Protection of individuals with regard to Automatic Processing of Personal Data" No. 108 [4]; · "Council of Europe Recommendation R(97)5 on the Protection of Medical Data" [5]; · UN General Assembly "Guidelines for the Regulation of Computerised Personal Data Files" [6]. L'argomento non è quindi sicuramente marginale.

Nella direttiva del governo europeo sulla protezione dei dati una parte (Articolo 17) è dedicata alla sicurezza del trattamento. EN 14484 snocciola ben tredici principi, di cui interessa a noi particolarmente il numero 10, la sicurezza del trattamento dei dati. Per applicare il principio 10 sono descritte ben dodici linee guida. Tre di queste ci interessano direttamente: Guideline Two: encryption during transmission; Guideline Three: proof of data integrity and authentication of origin; Guideline Four: access control and user authentication (Fig. 1).

In sintesi, le direttive prescrivono che il documento contenente dati sanitari venga cifrato durante la trasmissione (*cifrotesto*), ne sia riconoscibile l'autore (*identificazione informatica*) e ne venga ristretto l'accesso in lettura.

Sicurezza dell'autenticazione informatica: ISO 17090 per l'infrastruttura di chiave pubblica

I documenti ISO 17090, votati il 25.1.2006, costituiscono un sistema di tre separate specifiche: Part 1: Quadro generale dei servizi per certificati digitali; Part 2: Profilo dei certificati. Part 3: Gestione delle politiche dell'autorità di certificazione[9].

L'infrastruttura di chiave pubblica è una applicazione del modello di crittografia asimmetrica (Fig. 2). In questo modello, la chiave di decrittazione di un messaggio o di parte del messaggio non è uguale a quella della cifratura, come invece accade nella crittografia asimmetrica. Se una delle due chiavi resta in mano al soggetto che legge il messaggio, si persegue l'obiettivo della segretezza. Se invece resta al soggetto che confeziona il documento-messaggio, si ottiene l'autenticazione digitale.

L'infrastruttura a chiave pubblica (PKI) è tutta l'organizzazione, i dispositivi, le azioni, i controlli, utilizzata nella relazione tra un proprietario di chiave e altre parti, al fine di usare un certificato per un servizio di sicurezza. Comprende una autorità di certificazione, una struttura dei dati del certificato, una politica di certificazione e metodi per validare la pratica di certificazione.

Il certificato di chiave pubblica (PKC) è un oggetto software secondo lo standard X.509 che collega una identità ad una chiave pubblica.

Esistono diversi tipi di certificati: la maggiore suddivisione è tra certificati di chiave pubblica e certificati di attributi. I secondi non contengono una chiave pubblica.

I certificati di chiave pubblica possono essere di autorità di certificazione, di entità finale (end entity) o di collegamento (cross/bridges). Quelli di autorità di certificazione possono essere di tipo radice (root) o subordinati. Quelli di entità finale, che maggiormente ci interessano, possono essere attribuiti a diversi soggetti: individui, organizzazioni, dispositivi, applicazioni o programmi. Gli individui a loro volta possono essere professionisti regolamentati, non regolamentati, fornitori esterni di prestazioni, dipendenti di organizzazioni di supporto, pazienti o consumatori.

Il ventaglio delle possibilità enfatizza lo scopo della infrastruttura di chiave pubblica, ossia quello di autenticare un messaggio-documento collegandolo ad una identità, qualunque sia il tipo di messaggio-documento, professionale o non professionale, individuale o collettivo di organizzazione.

Un esempio di utilizzo del marchio digitale è dato dal **rapporto ISO N266** del 17.4.2002, prodotto da Pekka Ruotsalainen, Finlandia[10]. La gestione delle informazioni

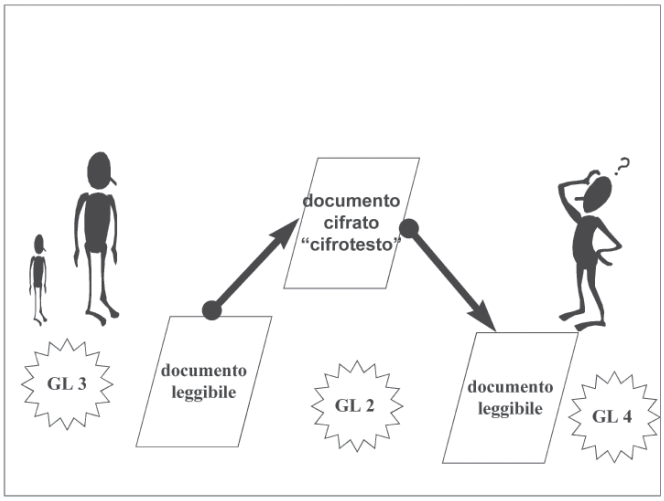

Figura 1. EN 14484:2003 9.10 decimo principio: sicurezza del trattamento.

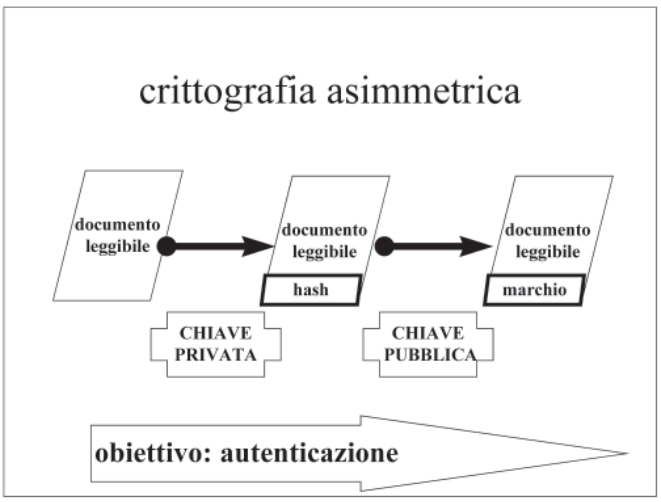

Figura 2. Modello della crittografia asimmetrica per l'autenticazione, alla base della infrastruttura di chiave pubblica della firma digitale.

archiviate, secondo questo rapporto, richiede un marchio digitale, attribuibile all'organizzazione (6.18 Organisational signing). La firma digitale dell'archivio serve per contrassegnare il documento originale, verificarne l'integrità dopo conversioni strutturali, verificare l'autenticità di un estratto parziale, impacchettare una cartella paziente costituita da diverse parti in un contenitore digitale e verificare l'integrità del tutto.

Norme tecniche (Standard) CLSI-NCCLS: AUTO11 e AUTO9

I due documenti CLSI (ex NCCLS) per la sicurezza informatica sono classificati come standard, non linee guida, a significarne l'importanza e la cogenza.

AUTO11, proposto solo nel gennaio di quest'anno, si riferisce alle procedure per la sicurezza informatica dei dispositivi diagnostici in vitro[11].

In AUTO11 si distinguono le responsabilità del fornitore da quelle della struttura sanitaria. I sistemi devono essere costruiti in modo da impedire l'utilizzo non autorizzato dell'applicazione e l'accesso non autorizzato ai dati, mediante una serie di meticolose regole sulla gestione delle password e l'uso delle tecniche di crittografia. Devono altresì essere protetti dagli attacchi del malicious software (virus e simili). E' necessario un sistema di sorveglianza della sicurezza, con rapporti sugli incidenti e verifiche periodiche. E' necessario prevenire la perdita dei dati, con le procedure di backup.

AUTO11 quindi elenca dettagliatamente le attività richieste a fornitori e strutture sanitarie per gli obiettivi identificati.

Il documento CLSI AUTO9, approvato solo nel marzo di quest'anno, è invece dedicato all'accesso remoto via Internet dei dispositivi diagnostici di laboratorio, tema inimmaginabile fino a pochi anni fa[12].

La connessione remota può essere utilizzata per sorvegliare il corretto uso degli strumenti, per raccogliere dati per la teleassistenza e per la gestione elettronica delle scorte.

La sicurezza delle informazioni in questo ambito richiede ancora l'utilizzo delle tecniche di crittografia (compresa la firma digitale del dispositivo), del controllo dell'accesso (password), della registrazione delle operazioni, di tecnologie come firewalls, sistemi anti-intrusione, reti private virtuali (VPN), tecnologie senza fili. Va posta particolare attenzione alla privacy del paziente, garantita in USA dalle norme HIPAA del 1996 ed in Europa dalle direttive 95/46/EC. Anche Giappone, Corea, Singapore e Malesia hanno qualcosa a riguardo. Il Canada possiede una normativa (PHIPA) simile agli altri paesi occidentali. Le operazioni di teleassistenza vanno compiute avendo riguardo alla sicurezza per il paziente e senza interferire con le attività degli operatori sanitari.

Gestione delle verifiche, degli errori e delle correzioni

Il tradizionale ciclo richiesta-risposta è oggi rotto da una serie di fattori. Cambia il flusso delle attività diagnostiche del laboratorio al fine di compensare le discontinuità del sistema sanitario. La buona pratica professionale richiede sia la verifica che la validazione dei risultati degli esami, in base a diversi esempi esposti nelle Checklists del College of American Pathologists. La supervisione, per colmare le discontinuità, può essere asincrona rispetto al flusso dei risultati. La rilevazione e correzione degli errori può avvalersi dei sistemi di automazione informatica (Autoverifica), come indica la linea guida CLSI AUTO10-P. La realizzazione di un meccanismo di autoverifica è un complessa e faticosa, ma consente notevoli vantaggi. Sono disponibili sul mercato sistemi esperti che aiutano notevolmente l'autoverifica ed altri prodotti di middleware. Il documento della risposta di laboratorio può contenere riferimenti alla verifica ed alla validazione, come ad esempio i nomi dei supervisori[13].

Conclusioni

Esercitare l'attività di laboratorio medico implica oggi curarne l'informatizzazione. Informatizzare un laboratorio medico senza il riferimento delle norme tecniche e delle linee guida è come andar per mare senza carte nautiche e senza portolano. Purtroppo, accade spesso proprio così.

E' quindi necessario uno sforzo eccezionale di ogni operatore, ma prima di tutto delle scuole specialistiche e delle

associazioni professionali, per avvicinare tutti i soggetti coinvolti, specialisti, tecnici, medici, stakeholders, amministratori, al concetto di conoscenza e considerazione degli standard, se non proprio di rigoroso rispetto. Il processo dell'accreditamento, su cui tanto si contava, non sembra sufficiente a garantirlo.

Bibliografia

1. Decreto Legislativo 30 giugno 2003 n. 196 (pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003. S. O. n. 123) Codice in materia di protezione dei dati personali.
2. Ministro per l'Innovazione e le Tecnologie. Direttiva del 18 Dicembre 2003: Linee guida in materia di digitalizzazione dell'amministrazione per l'anno 2004. GU n. 28 del 4-2-2004.
3. ISO/TC 210. ISO/DTR 16142 Medical devices - Guidance on the selection of standards in support of recognized essential principles of safety and performance of medical devices. Ginevra: ISO 2004.
4. ISO/TC 215 / SC WG-4. ISO/IEC DIS 27799. Health Informatics - Security management in health using ISO/IEC 17799. Ginevra: ISO 2005.
5. ISO/IEC 17799:2005, Information technology - Code of practice for information security management. Ginevra: ISO 2005.
6. CEN/TC 251/WG III. ENV 12924. Medical Informatics. Security Categorisation and Protection for Healthcare Information Systems. Brussels: CEN 2003.
7. CEN/TC 251. CEN/TS 15260 Health informatics - Classification of safety risks from health informatics products. Brussels: CEN 2006.
8. CEN/TC251. EN 14484 International transfer of personal health data covered by the EU data protection directive July 2003. Brussels: CEN 2003.
9. ISO/TC 215. ISO/DIS 17090 Health informatics - Public key infrastructure - Part 1: Overview of digital certificate services. Part 2: Certificate profile. Part 3: Policy management of certification authority. Ginevra: ISO 2005.
10. ISO/TC 215/WG 4. Health informatics – Security requirements for archiving and backup - Part 1: Archiving of health records. Ginevra: ISO 2001.
11. Clinical and Laboratory Standards Institute (CLSI). IT Security of In Vitro Diagnostic Instruments and Software Systems; Proposed Standard. CLSI document AUTO11-P (ISBN 1-56238-593-3). Clinical and Laboratory Standards Institute, 940 West Valley Road, Suite 1400, Wayne, Pennsylvania 19087-1898 USA, 2006.
12. Clinical and Laboratory Standards Institute (CLSI). Remote Access to Clinical Laboratory Diagnostic Devices via the Internet; Approved Standard. CLSI document AUTO9-A (ISBN 1-56238-599-2). Clinical and Laboratory Standards Institute, 940 West Valley Road, Suite 1400, Wayne, Pennsylvania 19087-1898 USA, 2006.
13. Pradella M. La correzione e la validazione dei risultati. RIMeL / IJLaM 2006; 2:42-9.