

LA PRIVACY IN LABORATORIO: MODALITÀ D'USO
ASL Ospedale di Calligarisone (CT)
venerdì 17 e sabato 18 giugno e ven.16, sab.17, lun. 19 e mar. 20 settembre 2005

Comunicazioni elettroniche sicurezza dei dati e dei sistemi

Marco Pradella
Castelfranco Veneto

sicurezza dei dati e dei sistemi

- sviluppo informatico
- direttive informatiche PA
- standard informatici
- ISO/IEC 27799 - ISO/IEC 17799
- CEN ENV 12924
- fax



LA PRIVACY IN LABORATORIO: MODALITÀ D'USO
ASL Ospedale di Calligarisone (CT)
venerdì 17 e sabato 18 giugno e ven.16, sab.17, lun. 19 e mar. 20 settembre 2005

gestione dei dati e delle applicazioni informatiche e non crittografia, innovazione tecnologica: interoperabilità e infrastrutture

Marco Pradella
Castelfranco Veneto

... per saperne di più ...

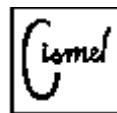


www.LABMEDICO.it

BITMEDICO LABSTATISTICA

LABSITI LABGOVERNO LABLIBRI

LABRISCHIO



www.CISMEL.it

www.SIMEL.it

- gruppo Informatica
- gruppo Risk Management
- news: standard - linee guida



tecnologie della sicurezza informatica in sanità

- percezione e gestione rischi
- fonti degli standard
- dispositivi medici - ISO/DTR 16142
- rischi informatica - prCEN/TS 15260
- dati personali CE - prEN 14484
- chiave pubblica - ISO/DIS 17090



tecnologie della sicurezza informatica in sanità

- percezione e gestione rischi
- fonti degli standard
- dispositivi medici - ISO/DTR 16142
- rischi informatica - prCEN/TS 15260
- dati personali CE - prEN 14484
- chiave pubblica - ISO/DIS 17090



Decisione 814/2005/CE 11 maggio 2005

- da Parlamento e Consiglio Europeo
 - istituzione programma comunitario pluriennale inteso a promuovere un uso più sicuro di internet e delle nuove tecnologie online
 - fenomeni negativi: spamming, pornografia infantile, razzismo
 - investimento: 45 mil € fino al 2008

Decisione 814/2005/CE 11 maggio 2005

- investimento: 45 mil € fino al 2008
 - ripartizione indicativa delle spese
 - lotta ai contenuti illegali: 25-30%
 - contrasto ai contenuti indesiderati (*spam*) e nocivi (*virus*): 10-17%
 - promozione ambiente più sicuro (*forum Safer Internet*): 8-12%
 - sensibilizzazione (*contenuti illegali, indesiderati e nocivi, "se del caso" tutela consumatori, protezione dati, sicurezza reti*): 47-51%

tecnologie della sicurezza informatica in sanità

- percezione e gestione rischi
- fonti degli standard
- dispositivi medici - ISO/DTR 16142
- rischi informatica - prCEN/TS 15260
- dati personali CE - prEN 14484
- chiave pubblica - ISO/DIS 17090

geografia della normazione

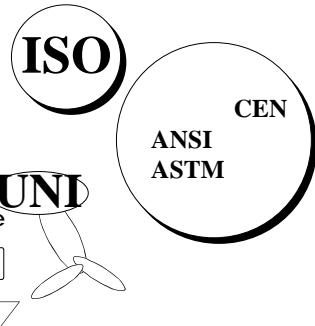
www.ANSI.org

www.ASTM.org

www.ISO.org

www.CENORM.be

www.UNI.com



CEN TC 251

- Working Group I Information Models
- Working Group II Terminology and Knowledge Bases
- Working Group III Security, Safety and Quality
- Working Group IV Technology for Interoperability

ISO o CEN per sicurezza informatica sanitaria

- ISO/TS/17090-1: Health Informatics -- Public Key Infrastructure -- Part 1: Framework and overview
- ISO/TS 17090-2: Health Informatics -- Public Key Infrastructure -- Part 2: Certificate profile
- ISO/TS 17090-3: Health Informatics -- Public Key Infrastructure -- Part 3: Policy management of certification authority.
- ISO/IS ISO/22857 "Health Informatics: Guidelines on data protection to facilitate trans-border flows of personal health information".
- CEN EN 12924: Medical Informatics – Security Categorisation and Protection for Healthcare Information System
- CEN prEN 12251 Health informatics - Secure user identification for health care - Management and security of authentication by passwords

ISO per sicurezza informatica sanitaria - 2

- 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/TS 22600-3: Health informatics – privilege management and access control Implementations (not yet published).
- ISO/TS 21091 Health informatics –directory services for security, communications, and of professionals and patients.
- ISO technical specification 21298 Health informatics – functional and structural roles.
- ISO TR 20514, Health informatics - Electronic health record – Definition, scope and context
- ISO/IEC 27799 Health Informatics: Guideline for security management using ISO/IEC 17799

ISO per sicurezza informatica

- ISO/IEC 17799:2005, Information technology — Code of practice for information security management,
- 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

tecnologie della sicurezza informatica in sanità

- percezione e gestione rischi
- fonti degli standard
- dispositivi medici - ISO/DTR 16142
- rischi informatica - prCEN/TS 15260
- dati personali CE - prEN 14484
- chiave pubblica - ISO/DIS 17090



sicurezza dispositivi medici

ISO © International Organization for Standardization, 2005

– Date: 2005-01-01

– Reference number of document: ISO/DTR 16142

- Committee identification: ISO/TC 210/WG 2
– Secretariat: AAMI (for ANSI)

Medical devices — Guidance on the selection of standards in support of recognized essential principles of safety and performance of medical devices

ISO/DTR 16142 - riferimenti generali

- 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.*

ISO/DTR 16142 - riferimenti specifici

- 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*

tecnologie della sicurezza informatica in sanità

- percezione e gestione rischi
- fonti degli standard
- dispositivi medici - ISO/DTR 16142
- rischi informatica - prCEN/TS 15260
- dati personali CE - prEN 14484
- chiave pubblica - ISO/DIS 17090

NWIP "Health informatics- Assuring patient safety of health informatics products" (CEN/TR)

- da CEN/TC 251/WG III: Health informatics -
Security, Safety and Quality
 - 2005-06-3
 - informatica fuori da controllo per dispositivi medici
 - diffusione sistemi di supporto alla diagnosi,
pressione di fattori economici (tempo) e legali
 - transizione a pratiche *paperless*, rischio di
corruzione e perdita di dati

sicurezza informatica sanitaria: riferimenti generali

- EN 61508-4:2001, *Functional safety of
electrical/electronic/programmable
electronic safety-related systems - Part 4:
Definitions and abbreviations (IEC 61508-
4:1998 + Corrigendum 1999)*
- ISO/IEC Guide 51:1999, *Safety aspects
— Guidelines for their inclusion in
standards*

prCEN/TS 15260: Health informatics - Classification of safety risks from health informatics products (June 2005)

- ...
- **5 Principles of hazard and risk analysis**
- **6 Assignment of a risk class to a health
informatics product**
- **7 The analytical process**
 - Annex B (informative) Examples of assignment of Risk
Classes
 - B.1 Hospital e-prescribing system with decision support
 - B.2 Bar code case note tracking system
 - B.3 Research system for sexually transmitted diseases
 - B.4 Ambulance Service Despatch System
- ...

tecnologie della sicurezza informatica in sanità

- percezione e gestione rischi
- fonti degli standard
- dispositivi medici - ISO/DTR 16142
- rischi informatica - prCEN/TS 15260
- dati personali CE - prEN 14484
- chiave pubblica - ISO/DIS 17090

prEN 14484 - Health informatics - International transfer of personal health data covered by the EU data protection directive (July 2003)

- **5 The European Data Protection
Directive (see annex A)**
 - 5.10 Security of processing (Article 17)
- **9 High Level Security Policy: the
content**
 - 9.10 Principle Ten: security of processing

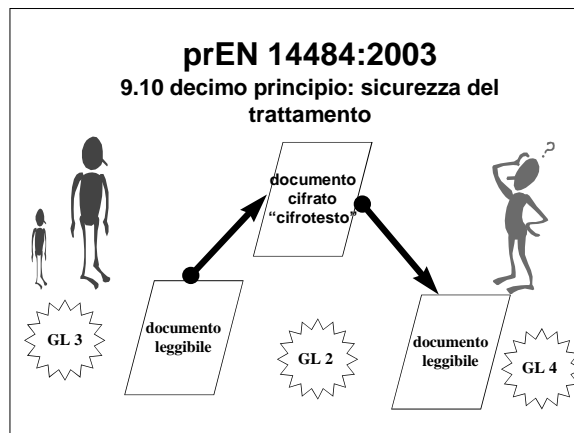
internationally authoritative documents relating to security and data protection:

- 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].

prEN 14484:2003

9.10 Principle Ten: security of processing

- 9.10.3 Principle Ten, Guideline Two: encryption during transmission
- 9.10.4 Principle Ten, Guideline Three: proof of data integrity and authentication of origin
- 9.10.5 Principle Ten, Guideline Four: access control and user authentication



tecnologie della sicurezza informatica in sanità

- percezione e gestione rischi
- fonti degli standard
- dispositivi medici - ISO/DTR 16142
- rischi informatica - CEN/TS 15260
- dati personali CE - prEN 14484
- chiave pubblica - ISO/DIS 17090



DRAFT INTERNATIONAL STANDARD ISO/DIS 17090

- ISO © International Organization for Standardization, 2005
 - ISO/TC 215 Secretariat: ANSI
 - Voting begins on: 2005-08-25
 - Voting terminates on: 2006-01-25

Health informatics — Public key infrastructure —

- Part 1: Overview of digital certificate services
- Part 2: Certificate profile
- Part 3: Policy management of certification authority



DRAFT INTERNATIONAL STANDARD ISO/DIS 17090-1

- ISO © International Organization for Standardization, 2005
 - ISO/TC 215 Secretariat: ANSI
 - Voting begins on: 2005-08-25
 - Voting terminates on: 2006-01-25

Health informatics — Public key infrastructure —

- Part 1: Overview of digital certificate services

crittografia

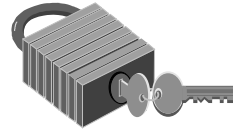
- 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
- A B C D E F G H I L M N O P Q R S T U V Z
- R S T U V Z A B C D E F G H I L M N O P Q
- 6 7 8 9 0 1 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5

– giulio cesare

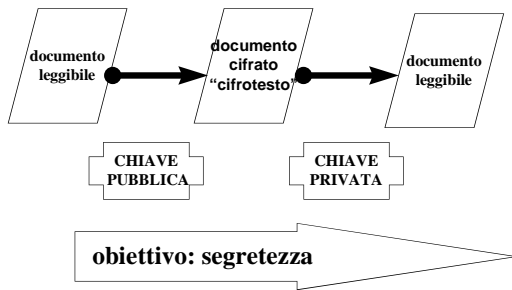
– acodcg tvmlrv

- chiave = 16 oppure AR

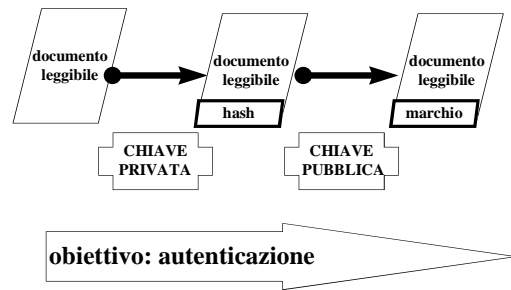
crittografia simmetrica



crittografia asimmetrica



crittografia asimmetrica



ISO/DIS 17090-1: PKI e PKC

- PKI = infrastruttura a chiave pubblica
 - utilizzata in relazioni tra proprietario di chiave e altre parti
- PKC = certificato di chiave pubblica
 - X.509: collega una identità ad una chiave pubblica



DRAFT INTERNATIONAL STANDARD ISO/DIS 17090-2

- ISO © International Organization for Standardization, 2005
 - ISO/TC 215 Secretariat: ANSI
 - Voting begins on: 2005-08-25
 - Voting terminates on: 2006-01-25
- Health informatics — Public key infrastructure —**
 - Part 2: Certificate profile

ISO/DIS 17090-2: contenuti

- profili specifici per la sanità dei certificati digitali basati su International Standard X.509 e IETF/RFC 3280
 - Health Care Certificate Types
 - Public Key Certificates
 - Root CA Certificates
 - Subordinate CA Certificates
 - Cross/ Bridge Certs
 - Attribute Certificates

ISO/DIS 17090-2:

Root CA Certificates
Subordinate CA Certificates

End Entity Certificates

- Individual
 - Regulated Health Professional (Qualified Certificate)
 - Non Regulated Health Care Employee (Qualified Certificate)
 - Patient/Con
 - sumer (Qualified Certificate)
 - Supporting Organization Employee (Qualified Certificate)
- Organization
- Devices
- Application



DRAFT INTERNATIONAL STANDARD ISO/DIS 17090-3

- ISO © International Organization for Standardization, 2005
 - ISO/TC 215 Secretariat: ANSI
 - Voting begins on: 2005-08-25
 - Voting terminates on: 2006-01-25

Health informatics — Public key infrastructure —

- Part 3: Policy management of certification authority

ISO/DIS 17090-3: contenuti

- management issues involved in implementing and using digital certificates in healthcare.
- defines a structure and minimum requirements for certificate policies (CPs) and a structure for associated certification practice statements.
- based on the recommendations of the IETF/RFC 647 *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*
- identifies the principles needed in a healthcare security policy for cross border communication.
- defines the minimum levels of security required, concentrating on the aspects unique to healthcare.

ISO/DIS 17090-3: contenuti

- attività manageriali per introduzione certificati digitali
- definizione struttura e requisiti minimi per certificate policies (CPs) e direttive pratica certificazione
- basato su raccomandazioni IETF/RFC 647 *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*
- identifica principi sicurezza per comunicazioni sanitarie transfrontaliere
- definizione livemmo minimo di sicurezza, per gli aspetti specifici della sanità

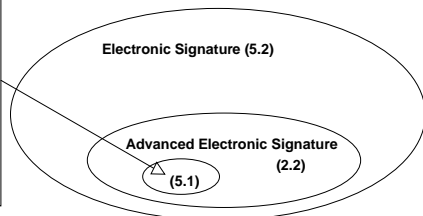
ISO/DIS 17090-3: requisiti CP

- 6 Structure of healthcare CPs and healthcare CPSs
- 7 Minimum requirements for a healthcare CP
 - 7.1 General requirements
 - 7.2 Publication and repository responsibilities
 - 7.3 Identification and authentication
 - 7.4 Certificate life-cycle operational requirements
 - 7.5 Physical controls
 - 7.6 Technical security controls
 - 7.7 Certificate, CRL and OSCP profiles
 - 7.8 Compliance audit
 - 7.9 Other business and legal matters

Il sistema delle firme elettroniche

Qualified Electronic Signature (QES)

QES =
Advanced
Electronic
Signature
(Art. 2.2)
created
with a
SSCD and
provided
with a QC



Direttiva Europea: cos'è una "Electronic Signature"

- ES: dati in formato elettronico attaccati o logicamente associati con altri dati in formato elettronico che ne forniscono un mezzo di autenticazione
- In Italia vedi art. 1 c. 1 lett. cc) del D.P.R. 445/2000.

ATTENZIONE!!!

- „Una firma scannerizzata è una electronic signature(!)
- „Il proprio nome scritto alla fine di un messaggio email è una electronic signature(!)

protezione del documento contro la falsificazione

livello sicurezza	documento cartaceo	documento elettronico
minimo	Codice civile Art. 2712 Riproduzioni meccaniche	idem
intermedio	Codice civile Art. 2702 Efficacia della scrittura privata. Sottoscrizione.	Direttiva 1999/93/CE 13 dicembre 1999 (G.U. delle Comunità europee L. 13 del 13 dicembre 1999), Comma 2 art. 5. <u>Firma elettronica "leggera"</u> .
elevato	Codice civile Art. 2703 Sottoscrizione autenticata	DPCM 13 gennaio 2004. (GU n. 98 del 27 aprile 2004) <u>Firma digitale (elettronica "forte")</u> .



Gestione sicurezza informatica in sanità secondo ISO/IEC 17799

ISO © International Organization for Standardization, 2005

ISO/TC 215/WG 4: Health Informatics/Security

– Secretariat: ANSI, Date: 2005-02-11

ISO/WD 27799

• Health Informatics — Security Management in Health Using ISO/IEC 17799

- Convener of ISO/TC 215/WG 4: Ross Fraser, Sextant Software, Inc.
- Technical secretary of WG 4: Kouichi Kita, Tokyo Institute of Technology



Gestione sicurezza informatica in sanità secondo ISO/IEC 17799

ISO © International Organization for Standardization, 2005

ISO/TC 215/WG 4: Health Informatics/Security

– Secretariat: ANSI, Date: 2005-02-11

ISO/WD 27799

• Health Informatics — Security Management in Health Using ISO/IEC 17799

- Convener of ISO/TC 215/WG 4: Ross Fraser, Sextant Software, Inc.
- Technical secretary of WG 4: Kouichi Kita, Tokyo Institute of Technology

ISO/DTS N266

6 REQUIREMENTS FOR ARCHIVING OF HEALTH RECORDS

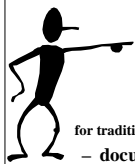
6.1 GENERAL REQUIREMENTS

- 6.2 SECURITY SERVICES
- 6.3 RESPONSIBILITY FOR PRESERVATION OF THE ORIGINAL DOCUMENT
- 6.3.1 TECHNICAL MANAGEMENT OF THE PRESERVATION
 - 6.3.2 PRESERVATION TIME OF DOCUMENTS
 - 6.3.3 ARCHIVING HIERARCHY
 - 6.3.4 NECESSARY PROTECTION AND PRESERVATION FOR A DOCUMENT BASED ON ITS PURPOSE OF USE
- 6.5 DIGITAL PATIENT DOCUMENTS
- 6.6 REFERENCES OF THE USED KNOWLEDGE INFORMATION
- 6.7 NAMING OF ELECTRONIC PATIENT DOCUMENTS
- 6.8 NAME AND REFERENCE SERVICES FOR ELECTRONIC PATIENT DOCUMENTS
- 6.9 METADATA OF ELECTRONIC PATIENT DOCUMENTS
- 6.10 STORAGE OF ELECTRONIC PATIENT DOCUMENTS IN TEXT FORMAT

ISO/DTS N266

6 REQUIREMENTS FOR ARCHIVING OF HEALTH RECORDS

- 6.11 STRUCTURE RECOMMENDATION FOR ELECTRONIC PATIENT DOCUMENTS
- 6.12 CHARACTER SET RECOMMENDATION FOR ELECTRONIC PATIENT DOCUMENTS
- 6.13 CORRECTIONS AND/OR ADDITIONS TO CONTENT OF ELECTRONIC PATIENT DOCUMENTS
- 6.14 STRUCTURAL CONVERSIONS OF ELECTRONIC PATIENT DOCUMENTS
- 6.15 STORAGE MEDIA OF ELECTRONIC PATIENT DOCUMENTS
- 6.16 MANAGING THE ARCHIVAL OF ELECTRONIC PATIENT DOCUMENTS
- 6.17 SIGNATURE OF ELECTRONIC PATIENT DOCUMENTS
- 6.18 ORGANISATIONAL SIGNATURES
- 6.19 ENCRYPTION OF ELECTRONIC PATIENT DOCUMENTS IN TRANSFER AND STORAGE
- 6.20 ACCESS TO ELECTRONIC PATIENT DOCUMENTS

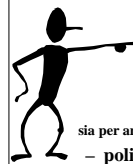


6 Requirements for archiving of health records

6.1 General requirements

for traditional paper archives and for electronic archives

- documented policy and procedures
- stored information understandable for users
- information available
- control over the content information and preservation description information during the entire archiving period.
 - *This can be realised by a migration plan.*
- separate physical ownership of information and conditions for use or transfer of the information
- sufficient control over any modification and use of the stored information.



6 requisiti archivi sanitari

6.1 requisiti generali

sia per archivi tradizionali carta che elettronici

- politica e procedure documentate
- informazioni conservate comprensibili per utenti
- informazioni disponibili
- controllo sul contenuto e conservazione descrizione informazioni durante l'intero periodo.
 - ==> piano di migrazione.
- separazione proprietà fisica e condizioni uso e trasferimento
- controllo su modifiche e utilizzo informazioni archiviate

6.8 Name and reference services for electronic patient documents

- The name of a document does not identify its physical place of storage, but the place of storage can be determined from the name service, which identifies the location of the document (URL address) or the archive or software that contains the document.



6.17 Signature of electronic patient documents

- Electronic patient documents should be signed with an electronic signature. The integrity of the signed data is verified by the signature.
 - A typical signer is a certified health care professional and the signature is a personal one.
 - ...Usually, information about the role of the professional is provided with the signature. The role information may contain both the professional status of the signer (for example specialist doctor) and the job-related dynamic role describing his work task (for example assistant surgeon in Internal Medicine).
- The signature shall contain a time stamp.



6.17 marcatura (“firma”) di documenti elettronici



- . . . documenti . . . integrità
 - di norma personale.
 - . . . di norma collegamento qualifica . . .
- . . . timbro cronologico