Quality labels for e-health

O. Ferrer-Roca, F. Marcano and A. Diaz-Cardama

Abstract: A drug e-prescription demonstrator was created in compliance with existing legislation as well as security and privacy standards. A professional ID-card was built on a high security chip (ISTEC E4 High; EAL-5) with a Hash hardware accelerator for a digital signature placed in a single chip USB token. Commercial software products as well as development kits of the new hardware designed in the project were used to build an authentication, authorisation and electronic signature demonstrator. The degree of legal compliance was evaluated. The tested novel single chip USB token was highly efficient but limited by its 1.1 interface speed (12 Mbit/s). The chip, initialised with a banking-mask, inefficiently managed space for the health-care chain of trust. The public key and privilege management infrastructure was not able to handle health-care attributes in the appropriate extensions. Templates for role-rule privileges were not available and healthcare standards for security and privacy were not found in commercial products. The paper points out the urgent need for an e-health conformance label as well as a quality label for liability and confidence to gain users' trust.

1 Introduction

Commercial healthcare information systems (HC-IS) have a legal responsibility to protect the privacy and personal data of individuals in accordance with the European Convention on Human Rights (1963) (Article 8). Although the US Constitution does not mention the word 'privacy' or the phrase 'protection of privacy', both the European Union (EU) and the USA provide advanced legislation for private electronic data protection [1–3], which is sectored in the USA and global in Europe.

The EU directives are generic statements that are implemented at a country level [4, 5]. As a consequence, country laws have become technologically-driven with three levels of security established: low, medium and high with the latter typically for healthcare data. Hopefully, when all EU countries have achieved the necessary requisites, data exchange between entities will not require bilateral security agreements.

In contrast, the USA's sectored healthcare security laws have been compiled in the HIPAA act (health insurance portability and accountability act) [1, 2]. These guidelines remain neutral on recommendations, being very flexible and adaptable to numerous factors, including the size of an institution, degree of risk and environment. They cover aspects not regulated in the EU (i.e. standard §164.308(a)5 on security awareness and training for all members including managers; standard §164.308(a)1 on risk analysis and risk management and so on). This adaptability and flexibility makes security agreements necessary between entities for information exchange because each one could implement different norms.

The health sector is not always acquainted with the HC-IS software and hardware requirements necessary for compliance and few documents [6–9] and standardised norms [5, 10–12] have been published. Despite this, general norms can be applied; for example, ISO 17799 addresses security standards in the information security world [13, 14] and can be certified with a conformance label called Common Criteria ISO/IEC 15408:1999. Some health organisations use secure infrastructure for addressing the issue (directory services (DSs) based on X.500 and lightweight directory access protocol version 3 (LDAP v3)), while others use certificates, encryption and auditing technologies or hybrid systems that employ DS repositories to centralise the management of user identity and roles [15].

Commercial solutions suitable for accessing complex healthcare data are not easily found. They require a high degree of specialisation in trusted third party services (TTPSs) with 24-hour activity to authenticate, authorise, administer and audit any access or modification of health-related data. Although specified in the ISO/TC251-WG4-DTS 17090 norm [6], it is not possible to find specialised healthcare authorities to identify and electronically allocate licensing, permissions and roles or rules of health workers.

In the EU, the public key infrastructure (PKI) with national registered certification authorities (CAs) as well as independent data protection agencies are already in place. The national laws specify which sensitive data transmitted through public networks have to be ciphered and log-registration audited. Contrary to the health code-of-practice, in which liability is placed on the health-worker's signature, the access/authorisation to carry out a medical act is founded by law merely on personal and univocal ID, and a digital signature is not mandatory.

As stated in the ISO/TC251-WG4-DTS 17090 norm, e-health should have a strong authentication with digital signatures involving credentials using cryptographic techniques with a level of security fixed by law [4, 5]. For PKI, there is an added problem since healthcare authorisation has a limited life-span and access that is based on the user role is very complex. A better solution could be authorisation based on attribute and access-role certificates linked to public key certificates (PKC), but issued by attribute

doi:10.1049/iet-com:20060596

Paper first received 26th October 2006 and in revised form 22nd June 2007

The authors are with the Department of Pathology, Faculty of Medicine, University of La Laguna, Tenerife, Canary Islands 38071, Spain

E-mail: catai@teide.net

authorities and role authorities (AA & RA) within a privilege management infrastructure (PMI) [6, 10, 11]. Private keys for digital signature (electronic ID) [16] should be kept in a highly secure support system or protected store. Smart cards, although widely used, are costly for healthcare since they require a reader at each terminal.

In the work presented here, an e-prescription system with an electronic signature held on a high security and versatile storage device is built and tested. Research was done at eight levels: (1) chip personalisation design, (2) healthcare trusted third party and (3) PKI. Healthcare record integration at the level of (4) authentication, (5) authorisation and (6) e-prescription design, and finally (7) digital signature management checked for (8) speed and functionality. This paper outlines a secure framework and discusses the difficulties involved in achieving legally-compliant high-level security and users' trust because of the absence of entities providing quality and conformance labels.

2 Material and methods

2.1 Simulator

The system architecture is summarised in Fig. 1. The hardware and software components are listed below.

2.1.1 Chip: This was developed under the IST-1999-20323 Smart-USB project, EC 5th framework in a single chip USB token.

Electronics: The USBsec™ microcontroller fulfils the highest security level on USB devices (Information Technology Security Evaluation Criteria (ISTEC) E4 High; ISO/IEC 15408 evaluation assurance level (EAL) 5). The SLE66CUx640P Infineon Technology® chip has a 16 bit CPU, 64 kbytes of ROM and 256 bytes of IRAM with an EEPROM of 32 kbytes. It has an advanced crypto-processor of 1100 bits and 700 bytes of crypto-RAM allowing for streaming cryptography data rates at USB v1.1 speeds. It has a hardware Hash accelerator for the digital signature, compliant with SHA-1 and MD5 that process at a higher speed than the 12 Mbit/s supported by the USB 1.1. It stores private keys and certificates for electronic transactions and carries data encryption.

Operating System: The chip has a TCOS 2.0 operative system (T-TeleSec® Chipcard operating system). Faktum® provides drivers (CT-API) to install a plug-and-play token under W2000 for prototyping.

Initialisation: Faktum® initialises the chip with a modified ISO 7816-4 file structure from T-TeleSec Crypto Nekton 2000™ (NTKS V2.0) (Fig. 2) common to a home banking computer interface (HBCI) application. We determined the space used by the operating system and initialisation mask.

Personalisation: We chose a SafeLayer® KeyOne™ CA application to build a TTP-PKI certificate server able to personalise the chip as a professional health card. We built a subordinate certificate and a registration authority to release user key pairs (public and private keys) and to place physician licensing and specialisation information in the certificates. The physician/supervisor role was placed in the PKC (see Section 3.2.1). We developed a Visual Basic program using Faktum Cryptoseal™-OCX and investigated possible solutions for chip personalisation.

2.1.2 Software: We programmed a Visual Basic v.6.0 application that interacted with the existing EHR distributed data-base. The functions that were built to handle e-prescription included:

Authentication (of user identity-ID) and Authorisation (of roles to access data): We used Faktum Cryptoseal-OCX to manage certificates and electronic signatures inside of the token chip.

Filling up the prescription: Designed to mimic Spanish paper prescription format and to interact with the National Drug Database integrated in the Electronic Health Record (EHR).

Signature and Storage: This was designed to interact with the existing EHR database.

3 Results

3.1 Research on the medical board simulator

3.1.1 Healthcare PKI/PMI: The CA built with SafeLayer® KeyOne™ CA application delivered a PKC

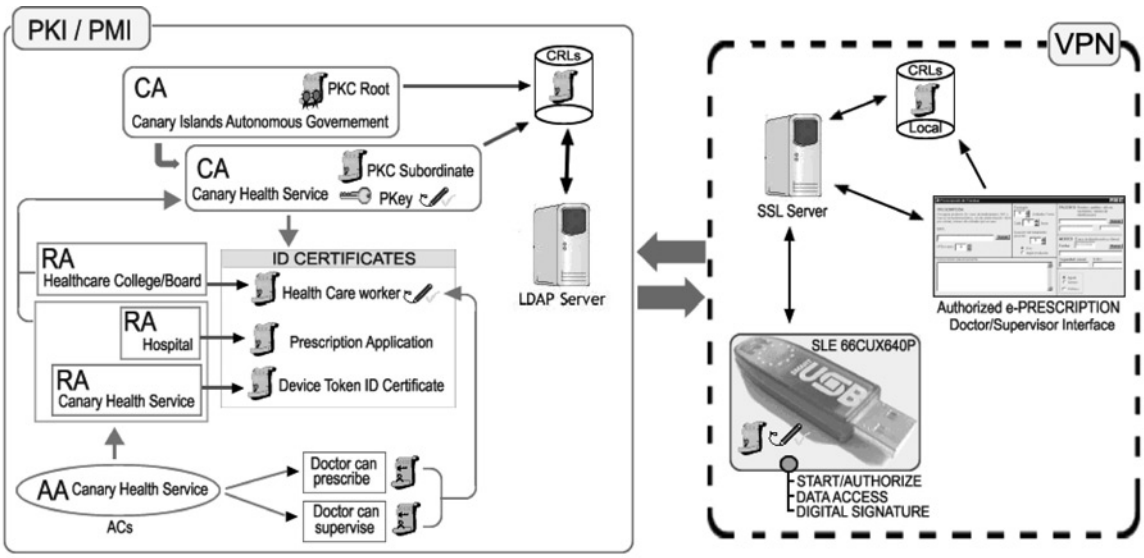

Fig. 1 *Architecture of specialised TTPs on healthcare. On the left, the design of the USBsec™ token in the Smart-USB project can be seen*
CA = Certification Authority; RA = Registration Authority; AA = Attribute Authority; AC = Attribute certificate

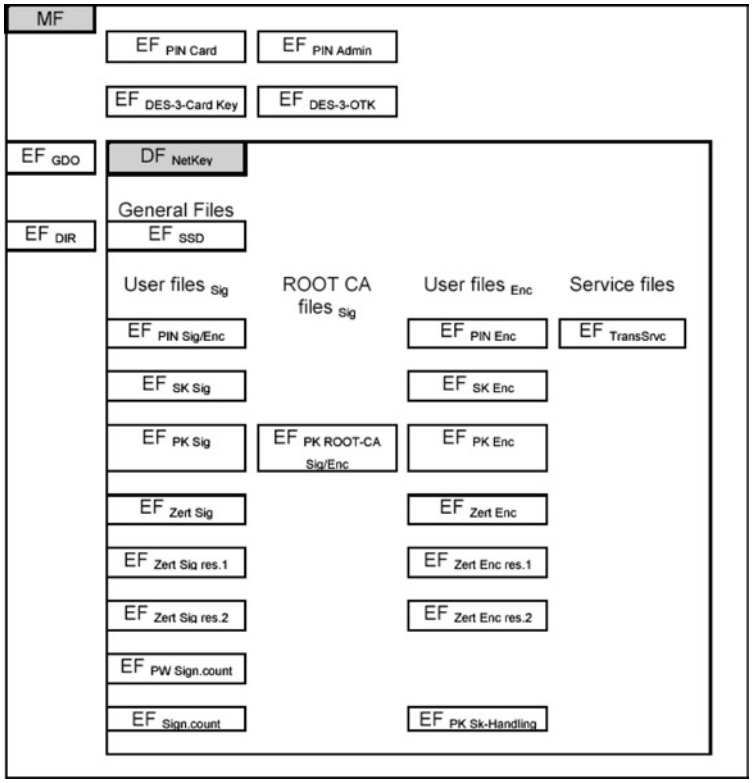

Fig. 2 *Standard TCOS Nekton 2000 structure*

MF = master file; DF = dedicated file; EF = elementary file; GDO = global data *n* = card number; SSD = security service description; SK = secret key; PK = public key

and key pairs. Key pairs were provided as 2 kb PKCS#12 files (public and private software keys) to be imported thereafter into the token chip or PKCS#11 files with key pairs generated inside the chip. Cross-institution/cross-border acceptance policy was included. According to Spanish and EU laws [X.509 public key certificates], PKCs were used as unique identifiers for authentication purposes.

Neither attribute certificate nor access-role certificate templates were available for data access authorisation. Roles, in the form of attributes, were included in PKC extensions (i.e. subject directory attributes), and rules were not considered.

An *ad hoc* certificate revocation list (CRL) was built and uploaded every two hours to a local server for certificate validation purposes.

3.1.2 Chip personalisation: The token was delivered initialised with two non-personalised certificates and a PIN-based access. Our application was designed to simulate a health PKI.

The private key for signing and imported it together with the public certificate into the chip. Since the application was based on Faktum OCX (software development kit (SDK)), only PKCS#12 files could be handled (PKCS#11 generates key pairs inside of the chip, being the only one recognised by law. Faktum-OCX did not provide functions to manage PKCS#11 in the IST-1999-20323 Smart-USB project).

Upward chain of confidence for standard compliance. The chip initialisation process was tested for space to store the whole chain of trust. The operating system and the initialisation mask occupy the ROM and part of the EEPROM. It could only provide enough space for one PKC with a private key and, therefore, the chain of trust could not be incorporated.

3.1.3 Healthcare TTP: Following TC251-WG4-DTS 17090 standard. The commercial solutions that we found and tested showed a very limited or non-existent level of compliance with standards. Specifically: (a) Neither attribute nor role certificate templates were available in any application on the market. (b) The limited chip space left did not allow the storing of device-PKC or the chain of trust. (c) The lack of security because of these limitations made the application and device-PKC unrealistic. Therefore, the functions of the newly built and tested healthcare specialised TTP were limited.

The research on commercial applications, programming and integration of the existing solutions to create a TTP structure required months. Testing was performed in three months.

3.2 Research on the HC-IS management demonstrator

The work included design, implementation and testing for EHR interactions and legal requirements with respect to authentication-authorisation-signature-storage-auditing.

3.2.1 Integrated EHR application: Authentication: The application was built for strong user-authentication. It sent a random number signed with the private key inside the token. The returned Hash was compared with that obtained with the physician's public key. The application before/after assuring user-ID accessed the local updated CRL to check certificate validity.

Authorisation: The application was built to determine whether or not the user (the UI of the token) was authorised to release/supervise the prescription by reading the role PKC attribute extension. Since the Faktum-OCX did not read the Subject Directory Attributes, the information

(as to whether a physician was able to prescribe or a supervisor was able to countersign) had to be placed in an unsuitable field (i.e. the SubjectName-Title). After the user role was recognised, the user certificate validity was checked.

Signature: Upon filling the prescription, the application allowed the physician/supervisor to sign it. By clicking on the signing icon, role and PKC validity were checked. This was followed by a confirmation step, required by law, which carried out a physician's re-authentication and re-authorisation in a user-transparent manner.

Storage: For legal purposes, the application stored the signed e-prescription in the general health-care database together with the physician's public certificate and the chain of trust.

3.2.2 Demonstrator: The trial was built following the architecture summarised in Fig. 1. The demonstrator was successfully implemented with the above-listed restrictions. The application could not be used for real e-prescription, because of the compulsory Spanish laws on data protection [4] and digital signature outlined in this framework could not be implemented with the currently existing solutions. Among the other limitations, there were no recognised certification, registration and role authorities able to certify physician licensing, roles and rules.

Prescription filling: We designed a display that mimics the Spanish paper prescription format (Fig. 3) and allows the selection of medication from the electronic National Drug Database integrated in the EHR. The application imported into the e-prescription patient unique identifiers (PUIs) from the EHR data-base and the physician's administrative data such as medical board number from the certificate-ID stored in the USB-token.

Signature and storage: By clicking on the signature-icon, the application electronically signed the e-prescription. The software stored into the EHR database the prescription together with the physician's public certificate and the chain of trust linked to it. A second icon was built to allow supervisors to review the prescription and counter-sign it, while the application checked for message integrity and carried out the physician's signature validation. The latter was done by checking certificate validity backwards against local CRL and viewing the validity of the chain of trust at the exact time of the signature.

3.2.3 Speed and functionality: The single-chip USB-token did not require specific readers and was easily transported to several computers facilitating multiple access. The application read the token in a transparent manner at least three times (start/data access/sign) in the same session. Data transfer achieved 12 Mbit/s, the maximum rate for full-speed USB 1.1 interfaces.

E-prescription was performed and stored unencrypted as part of the EHR inside a highly secure healthcare virtual private network (HC-VPN).

4 Discussion

The present e-prescription demonstrator is an example of HC-IS where patient privacy and safety are essential premises. The demonstrator faces problems of security and future global data exchange, with respect to EU, Spanish and USA laws. It covers healthcare worker identity standards for cross-border recognition, as well as role certificate creation, delivery and use. The existing barriers enhance the relevance of a nation-based quality label to protect user liability. This label is to assure users and customers that compulsory high security requisites are fulfilled by the commercial solutions when applied to HC-IS. As we have demonstrated, one such commercial solution is the plug-and-play professional card using a versatile device able to carry a healthcare worker's identity and private key, together with attributes or role certificates and the chain of trust. Another solution involves CAs, to provide cross-border/time persistent, legally compliant health workers' digital ID.

The suitability of highly-secure single-chip USB-tokens to carry private key and certificates has been proved. As for less secure two-chip tokens available on the market, the existence of USB ports in all computers reduces costs and eliminates

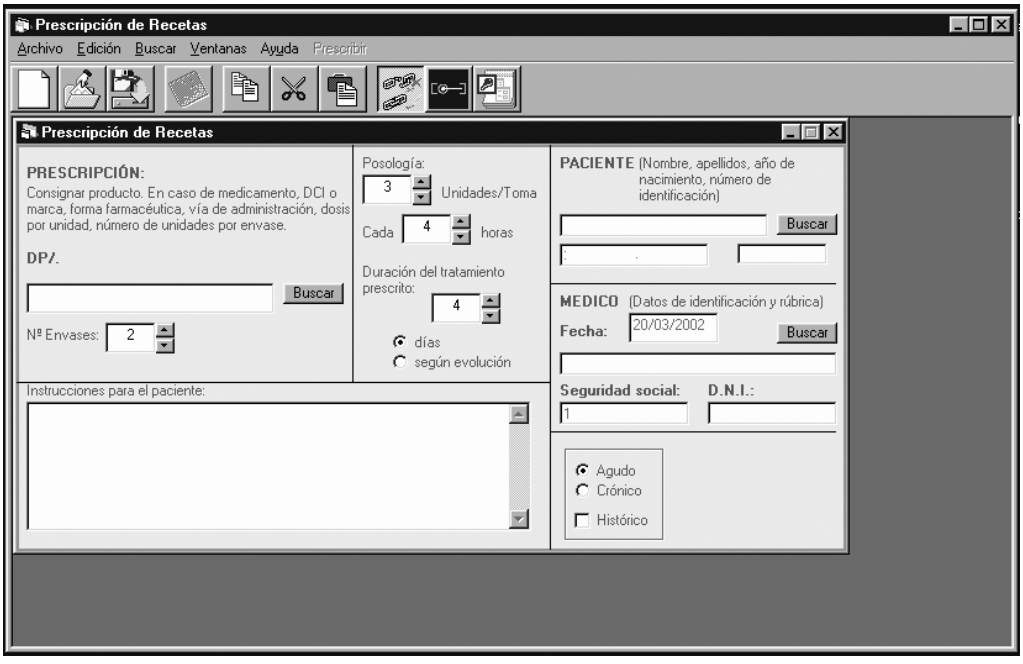

Fig. 3 *E-prescription format following the Spanish paper-based model*

the need for a card reader. Being 'plug-and-play', the authentication/authorisation/certificate checks are facilitated. Its ability to incorporate biometric sensors such as finger-prints in the token-cover is an added value when accessing chip information. Its high-speed hardware performance is only constrained by the maximum speed of the USB port, nowadays a high-speed version 2.0 of 480 Mbit/s, whose real data throughput rate is around 60%.

In Spain as well as other EU countries [5], medical boards have started to implement physician ID-cards (PKI) in conjunction with bank applications on multipurpose smart cards. As we have demonstrated, chip initialisation based on the banking standard did not optimise chip space, although the currently marketed chip has improved the ROM by up to 128 kbyte and EEPROM to 64 kbyte. Chip initialisation requires a structure that optimises memory space for the healthcare certificate hierarchy tree on which to base the chain of trust, plus numerous attribute-role certificates.

Average PKI services address many compulsory security standards [12, 17–21]. Nevertheless, Health-care PKIs (HC-PKI) face additional requirements. These include a high level of assurance-availability-trust, Internet compatibility and evaluation/comparison of certificate policies [6, 22] for the trans-border activities required in federation-based countries (i.e. USA) or nation-based unions (i.e. EU). The ISO/TC-251-WG4 standardisation group has worked extensively on these specifications, but ready-to-use commercial solutions [17, 20, 22] are not compliant as we have demonstrated in this study. National authorities are not competent to handle medical specialist certificates or workers' role allocation. Existing ID-certificates do not have available extensions for physician qualifications and primary roles. No registered attribute certificates or authorities are currently available. No registration authorities are able to confirm qualifications and primary roles of health workers. It seams clear that trust authorities in healthcare should be closed to hospital institutions (for access-role) and to license-registry medical boards (for primary roles) or even located in specific health transaction centres [22] to concentrate specialised healthcare TTPs.

Healthcare electronic data also require time-persistency, since past CRL cannot be checked. For that reason, in any electronic transaction related to a medical act, the worker ID (PKC, attribute or role certificate together with the chain of trust and its validity at the time) should be stored time-stamped (a feature not implemented in our demonstrator). Furthermore, health workers role complexity and short-life of roles compared to average PKC validity (i.e. four years in Spain), demand healthcare specialised attribute authorities to deliver attribute certificates.

Data availability 24 hours a day in healthcare is essential [18]. Stored data cannot be encrypted for a specific user (when a message is encrypted, only the recipient can read it because it is encrypted with his/her public key) and data transactions require highly secure virtual private networks where data are transmitted in an encrypted form. In this context, ID and role access controls ensure privacy, while digital signatures with qualified certificates (QC) verify origin linked to liability (qualified certificates are engineered to identify a person using a high level of assurance in digital signature services for legal recognition, but are difficult to find). Access with a single sign on (SSO) technique that avoids re-authenticating while navigating is, with the exception of devices and applications permanently working, limited in healthcare. Namely:

(*a*) Automatic logoff is essential.
(*b*) Clinical data modifications require digital signature and time-stamping to assure no refutation, integrity and accountability. By law, digital signature permission requires: confirmation, ID and role recognition as well as a valid chain of trust at the moment of signing.
(*c*) To access a specific information level, role checking is demanded (i.e. level of data access is different for physicians or nurses and may change depending on whether they are on duty or not). Any solution must support the principle of the 'least privilege' by which a user is allowed to log into a system with only those roles appropriate for a given occasion, not with all possible roles. For those reasons, SSO was not implemented.

In the flexible and sectored approach of the USA, the electronic healthcare security standard (§164.312(a) 1 access control standard) by-passes the problem by not mentioning terms such as 'role-based-access control' or 'rule-based-access control' and so on; this gives a wider scope and allows any appropriate mechanism. In the EU, models based on hybrid access assume that workers belong to one or several entities (users, roles, permission, teams, contexts and collection of sessions) [11, 23].

It is well known that healthcare software is not subject to the quality control of the medical devices ISO 13485:2003 norm. This represents a risk, even if the software is validated before any clinical use according to 'good automated manufacturing practice' guidelines 0. That validation is mainly focused on patients' and users' health risks and not on standard and/or legal compliance. As demonstrated in this paper, legal compliance with country privacy and security laws is not always apparent in software applications. It is therefore recommended for commercial solutions to carry 'quality labels', preferably certified by government agencies (competent in healthcare), to assure they 'do what they claim' on legal compliance (i.e. assure standardised extensions of the PKC for healthcare, check certificate validity, check identity and roles in every signature, upgrade CRLs regularly, and so on). Similarly, the 'conformance labels' for international standards are relevant even in non-technologically-driven legislation (i.e. USA) if they want to achieve cross-border validation and functionality.

Security issues are essential in medical practice [25, 26]. Unfortunately, faculties of medicine do not offer this training to general practitioners. In our opinion a minimum level of proficiency in this field should be demanded to gain users' trust.

5 Acknowledgments

This work was performed under the auspices of the IST-1999-20323 Smart-USB project whose partners are thanked for their cooperation and support.

6 References

1 Borten, K. (Ed.): 'HIPAA security made simple. Practical advice for compliance' (HCPro Inc., Maryland, 2003, ISBN 1-57839-269-1)
2 HIPAA: Health Insurance Portability and Accountability Act, 1996: US Public Law 141-190, USC 1320d
3 EU Directives: Directive 95/46/EEC about the protection of individuals with regard to the processing of personal data and free movement of data; Directive 99/93/CE of the Parliament and European Council about electronic signature; Directive 200/31/CE on electronic commerce and Directive 98/27/CE on consumer protection
4 Spanish laws: Digital signature RD14/99; Regulations for personal data protection RD949/99; LOPD (organic law on personal data protection) LO15/99; Patient autonomy law and healthcare

information L41/2002; LSSI (law for the services of the information society) and electronic commerce L34/2002
5 van der Haak, M., Wolf, A., Brandner, R., Drings, P., Wannenmacher, M., and Wetter, Th.: 'Data security and protection in cross-institutional electronic patient records', *Int. J. Med. Inf.*, 2003, **70**, pp. 117–130
6 ISO/TC251 WG4: 'Security on health informatics'. Task force of public key certification infrastructure, Draft TS 17090, Parts 1–3, 2001
7 ISO/IEC-15408 'Common criteria for information technology security evaluation', 1999
8 Buckovich, S., Rippen, H., and Rozen, M.: 'Driving toward guiding principles: a goal for privacy, confidentiality, and security of health information', *J. Am. Med. Inf. Assoc.*, 1999, **6**, pp. 122–133
9 Gritzalis, D.: 'A base line security policy for distributed healthcare information systems', *Comp. Secur.*, 1997, **16**, (8), pp. 709–719
10 Mavridis, I., Georgiadis, Ch., Pangalos, G., and Khair, M.: 'Access control based on attribute certificates for medical intranet applications', *J. Med. Internet Res.*, 2001, **3**, (1), e9. Available at: http://www.jmir.org/2001/1/e9. Accessed May 2007
11 Georgiadis, Ch.K., Mavridis, I.K., and Pangalos, G.: 'Healthcare teams over the Internet: programming a certificate-based approach', *Int. J. Med. Inf.*, 2003, **70**, pp. 161–171
12 Spinellis, D., Gritzalis, S., Lliadis, J., Gritzalis, D., and Katsikas, S.: 'Trusted third party services for deploying secure telemedical applications over the WWW', *Comp. Secur.*, 1999, **18**, (7), pp. 627–639
13 ISO 17799: 'Code of practice for information security management and more rigorous X9.79' (ANS X9.79-1'. Part 1: PKI practices and policy framework and web trust (AICPA/CICA WebTrust®)). WebTrust Principles and Criteria for Certificate Authorities, American Institute of Certified Public Accountants Publication, 2000
14 ISO 17799: 'Service and software directory', 2000
15 Johnston, W., Mudumbai, S., and Thompson, M.: 'Authorisation and attribute certificates for widely distributed access control'. IEEE 7th Int. Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'98), Stanford University Press, Stanford, CA, 1998, pp. 340–345
16 Kent, S., and Millet, L.: 'IDs—not that easy. Questions about nationwide identity system' (National Academy Press, Washington, 2002, ISBN: 0-309-08430-X)
17 Schull, H., and Schmidt, V.: 'MedStage: Platform for information and communication in healthcare'. In Hasman, A., Prokosch, H., Blobel, B., Dudeck, J., Gell, G., and Engelbrecht, R. (Eds.): 'Medical infobahn for Europe' (IOS Press, Amsterdam, 2000, vol. 77, Studies in Health Technology and Informatics, ISBN: 978-1-58603-063-62000), pp. 1101–1105
18 Waring, T., and Wainwright, D.: 'Communicating the complexity of computer-integrated operations: an innovative use of process modelling in a north-east hospital trust', *Int. J. Oper. Prod. Man.*, 2002, **22**, (4), pp. 394–411
19 NHS Information Authority. Available at: http://www.nhsia.nhs.uk/security/pages/default.asp. Accessed May 2007
20 Health e-signature authority. Available at: http://www.hesa.com.au. Accessed May 2007
21 Laica, S.: 'Delivering 21st century IT in the NHS', *Brit. J. Healthcare Comp.*, 2002, **19**, (7), pp. 23–26
22 HealtheKey project. Wisekey SA. (World Internet Security key) Wise e-health. Available at: http://www.wisekey.com/press/healthekey.htm. Accessed May 2007
23 Georgiadis, Ch., and Mavridis, K.: 'E-health collaboration technology: a certificate-based approach', in Ferrer-Roca, O. (Ed.): 'CATAI 2004: Quality and Security in e-Health', (CATAI Ed., Tenerife, Spain, 2003, ISBN: 84-6070493-8), pp. 61–66
24 Good automated manufacturing practice (GAMP) guidelines, available at: www.ispe.org/gamp. Accessed May 2007
25 Ferrer-Roca, O., and Sousa-Iudicissa, M. (Eds.): 'Handbook of telemedicine' (IOS Press, Amsterdam, 2nd edn., 1999, vol. 54, Studies in Health Technology and Informatics, ISBN: 90 5199 413 3)
26 Ferrer-Roca, O. (Ed.): 'Telemedicine' (Ed. Medica Panamericana, Madrid, 2001, ISBN: 84-7903-606-0)