DIGITAL CERTIFICATION IN TELERADIOLOGY: A NECESSARY WARNING*

Luiz Felipe Nobre[1], Aldo von Wangenheim[2], Rafael Simon Maia[3], Levi Ferreira[3], Edson Marchiori[4]

Abstract **The increasing worldwide popularization of telemedicine activities has demanded a new approach to the professional practice by physicians and other health professionals. As far as teleradiology is concerned, a remarkable trend has been observed toward the transformation of clinical documents — like radiological studies results, that so far existed as printed films and paper-based reports — into electronic documents available in internal networks of medical clinics and hospitals or through the internet. As a result of this trend, it is necessary to divulge and explain concepts such as digital certification, internet data encryption, sites' reliability, reliability of electronic documents, and digital signature. Even though the baseline principles of these concepts may seem complex for health professionals, they can be effectively understood with no need to wander through labyrinths like the mathematics of asymmetric keys cryptography, or digital data communication protocols. Security and reliability aspects related to internet-based electronic clinical documents are described in the present study, in a straight and practical way, aiming at an informed, safe and soundly grounded interaction between medical users and telemedicine services.**

Keywords: Teleradiology; Safety in information technology.

Resumo *Certificação digital de exames em telerradiologia: um alerta necessário.*
A crescente popularização das atividades de telemedicina em todo o mundo tem exigido de médicos e demais profissionais da saúde novas abordagens em sua prática profissional. No que se refere à telerradiologia, observamos forte tendência à transformação de documentos clínicos — como resultados de exames, que até hoje existiam na forma de filmes impressos e laudos em papel — em documentos eletrônicos, disponibilizados em redes internas de clínicas e hospitais, ou pela internet. Esta tendência torna necessária a divulgação e o esclarecimento de conceitos como a certificação digital, a criptografia de dados na internet, a confiabilidade de *sites*, o documento eletrônico confiável e a assinatura digital. Os princípios básicos desses conceitos, embora por vezes complexos para os profissionais da saúde, podem ser compreendidos de forma efetiva sem que o leitor tenha de mergulhar de cabeça em labirintos como a matemática da criptografia de chaves assimétricas ou os protocolos de comunicação digital de dados. Neste artigo abordaremos de forma direta e com exemplos práticos os aspectos de segurança e confiabilidade de documentos clínicos eletrônicos baseados na internet, com o objetivo de que os usuários médicos possam interagir de forma informada, segura e bem fundamentada com serviços de telerradiologia.

Unitermos: Telerradiologia; Segurança em computação.

INTRODUCTION

An effective information exchange among health professionals may save time and money, provide higher clinical effectiveness, improve the continuity and quality of assistance, as well as facilitate the activities of management in both public and private health systems. New technologies provide an easier access to information that is transformed into the raw materials over which the contemporary society development is based. In this context, telemedicine has been utilized as a relevant tool.

Radiology is one of the medical specialties with highest potential to benefit from telemedicine applications. Activities like distance diagnosis and second medical opinion (respectively telediagnosis and teleconsulting), or even the availability of images and studies reports over the internet has become an increasingly frequent practice in this new reality. Technological platforms allowing these activities have been progressively implemented in the routine of radiological clinics as a part of their information technology infrastructure.

In Brazil, as well as in the rest of the world, an increasing number of radiological clinics and centers have implemented picture archiving and communications systems (PACS) or radiology information systems (RIS). Besides images storage and transmission supported by PACS, RIS also provides storage, manipulation and retrieval of clinical data associated with images. The utilization of these systems offers innumerable advantages for radiologists, assisting physicians and patients. At the

* Study developed as an integral part of Cyclops Project/Laboratory of Telemedicine at Hospital Universitário da Universidade Federal de Santa Catarina (UFSC), Florianópolis, SC, Brazil.

[1] MD, PhD, Professor Assistant of Radiology, Chief for the Department of Radiology, Hospital Universitário da Universidade Federal de Santa Catarina (UFSC), Coordinator for Rede Catarinense de Telemedicina SES/UFSC, Florianópolis, SC, Brazil.

[2] Associate Professor, Department of Information Technology and Statistics, Coordinator for the Cyclops Project, Universidade Federal de Santa Catarina (UFSC), Florianópolis, SC, Brazil.

[3] Fellows Master degree in Computational Sciences, Researchers for the Cyclops Project/Laboratory of Telemedicine at Hospital Universitário, Universidade Federal de Santa Catarina (UFSC), Florianópolis, SC, Brazil.

[4] Titular Professor of Radiology, Universidade Federal Fluminense (UFF), Niterói, RJ, Adjunct Coordinator, Course of Post-graduation in Radiology at Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro, RJ, Brazil.

Mailing address: Prof. Dr. Luiz Felipe Nobre. Rua Constancio Krumel, 1083, Praia Comprida. São José, SC, Brazil, 88103-600. E-mail: luizfelipenobre@gmail.com

Received November 27, 2006. Accepted after revision April 16, 2007.

midterm, a costs reduction is expected, considering the lesser utilization of films and chemicals, and the lower number of studies repetitions either because of technical aspects or for allowing an easier access to previous studies of a determined patient. The integration between these systems over the internet also implies the possibility of an easier exchange of images and tests results, allowing an immediate availability of the option for exchanging clinical reporting services between medical centers, and the creation of telediagnosis centers. Notwithstanding, in the radiological environment, there has been few discussion about a critical question related to this new model: the necessary security for electronic transmission and access to digital images and radiological reports.

We will discuss the relevance of digital certification of electronic documents and files, including digital images and clinical studies reports over the internet, in a brief approach of the most significant technological aspects associated with this matter.

DISCUSSION

Likewise the worldwide developments in the field of radiology in the last few decades, also in Brazil a progressive transformation has been observed, still limited by financial restrictions characteristic of the economic reality in our country. Besides the traditional utilization of originally digital equipment by medical clinics and hospitals, such as sonographs, tomographs and magnetic resonance imaging apparatuses, conventional radiology equipment has been replaced by new models of radiographic equipment which allow the direct or indirect digital images acquisition respectively known as DR and CR. In many cases, radiological images and reports are made available over the internet both for requesting physicians and patients[(1)]. From the information security and confidentiality point of view, it is essential that these imaging studies and clinical reports meet the technical and legal requirements to be considered as reliable electronic documents.

In the last few years, the increase in the traffic of sensitive data over the internet has given room for an increase in the number of electronic frauds, from 2004 to 2005, of something like 579%[(2)]. The techniques utilized in some types of frauds also may be utilized to threaten the traffic of sensitive data regarding patients and medical activities over the internet. For the ease of current and future teleradiology users, there is a set of technologies available to prevent the falsification of images and studies results, offering security and guaranteeing the legal validity of electronic medical documents. Figure 1 demonstrates the division of these security tools into three groups with different actions and characteristics as follows: safe access, electronic signature, and timestamping, constituting what could be called “security tripod of teleradiology” (STT).

What is a reliable electronic document?

Likewise traditional documents that, to be considered as valid, must be complete and with no erasure, be duly dated and signed, so should be electronic documents. Each of the groups of technologies shown on Figure 1 operates with a set of characteristics or attributes required for the production of an electronically reliable document, with legal value according to the Brazilian regulations. In the digital world, besides confidentiality and secrecy provided by a safe access to the internet by means of data encryption, there are some aspects that must be guaranteed to assure that a determined electronic document is reliable, timely generated by a safe source, and that has not been changed. These security requirements, legally accepted as unquestionable, are described as follows:

– **Authenticity:** From the Portuguese language dictionary (Aurélio), “authentic – something known to be genuine”. In a conventional document, the authentication is provided by a recognized signature. On the other hand, an electronic document is considered as authentic, provided it has been digitally signed, by means of a valid digital certificate.

– **Integrity:** “Integral, intact, complete”. This is the evidence that a determined document has by no means been changed. A conventional document cannot present any amendment or adulteration.

– **Irrefutability** (or nonrepudiation): “something that cannot be denied or shown to be incorrect; evident, irrefutable, incontestable”.

– **Tempestivity** (or non-retroactiveness): Possibility of proving that an electronic event has occurred at a specific moment in time.

The discussion about currently available tools guaranteeing the security of internet-based electronic documents exchange will be initiated by the question of secret medical data transmission using cryptography, allowing a straightforward development of the concept of digital certification which is essential in the application of the STT.

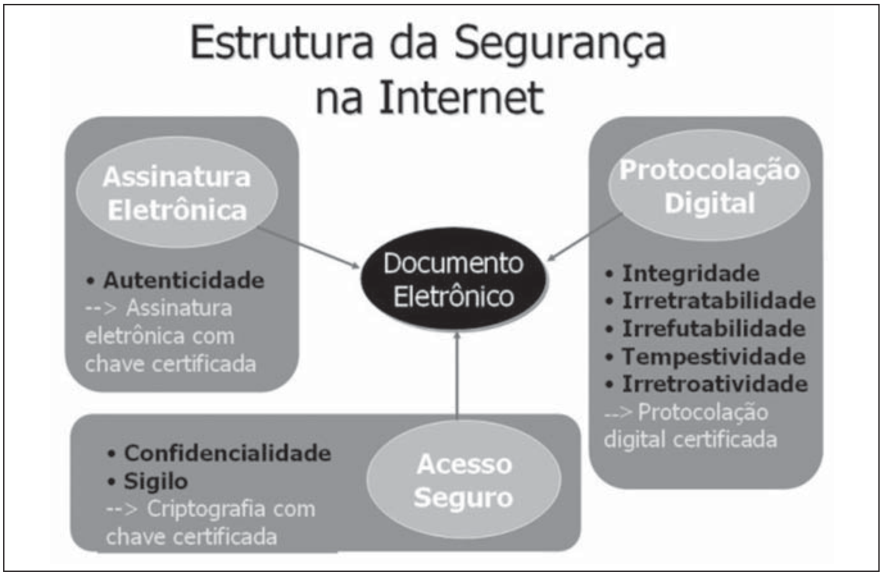


Figure 1. Security technologies for the provision and exchange of electronic documents over the internet, based on the tripod: safe access, digital timestamping and electronic signature.

What is cryptography?

From the Greek *kryptós* "hidden" and the verb *gráphein* "write" – cryptography is the practice and study of rewriting a text hiding information. Also, in information technology, cryptography is related to the utilization of techniques allowing writing in ciphers and codes making the message incomprehensible. When words in a message are transposed or replaced according to a predetermined code, this process is called *encoding*. When a mathematical method is utilized to change the message, this process is known as *ciphering*. The ciphering process is based on a mathematical rule for replacement of letters by numbers in a way that in a message ciphered with different numbers, different results will be obtained. This number is called *key*, and the higher the number, the higher is the ciphering security. This process is aimed at ensuring that only the addressee can read an electronic message, by means of an inverse process, the *deciphering*. When both ciphering and deciphering are performed with a sole password or key, the process is called symmetrical cryptography (Figure 2). The disadvantage of this process is that it is necessary to stipulate a key to be utilized in agreement with the person who will send us a ciphered message, and, in this process, this key may be intercepted. The asymmetrical cryptography, or public key cryptography, is based on a different concept, with a mathematically related key pair called private key and public key. These keys are constituted of very large numbers. Documents or messages encrypted with one key may only be decrypted by using the other half of the key pair. The private key is held and known only by the sender of the electronic document. On the other hand, the public key, as the term already indicates, is widely known and normally is available in the internet.

How does one make information available on internet while guaranteeing its confidentiality?

Asymmetrical cryptography allows a safe and flexible exchange of confidential data on the internet. A cryptographic protocol called SSL/TLS (secure socket layer/transport layer security) provides a secure access, guaranteeing the confidentiality and secret in the transference of data, whether regarding a banking transaction or a patient. When a confidential webpage is accessed, this type of secure encapsulating process is established between the computer and the server of the bank or telemedicine service. For this purpose, the computer browser utilizes a specific public/private key pair different from those utilized by other browsers in other computers. Once the internet connection is established, the computer and the remote server will exchange their public keys, allowing a personalized encryption of the messages or data that they send to each other. As an additional security measure to ensure the public key sender identity, avoiding interception by hackers pretending to be a telemedicine provider, the server must send not only its public key, but an identifiable digital certificate.

What is a digital certificate?

A digital certificate is an electronic file containing personal information about its ownership. Also it is the proof of a cryptographic key ownership. In this certificate, a trusted third party called certification authority testifies the authenticity of the attached public or private key, confirming the identity of the certificate issuer. Besides the public key, a digital certificate includes data from the subject such as name, e-mail, CPF, and the name of the digital certificate issuer, as well as the public key hash digitally signed by the certification authority. In practice, it works like a virtual identity card authenticated by a trusted entity guaranteeing a safe counterpart identification in a transaction over a computer network (Figure 3). Several companies and government agencies issue digital certificates in the Brazilian market. ICP Brasil[3] is the sole certification authority for this country, linked to Instituto Nacional de Tecnologia da Informação, attached to the Presidency of the Republic. The Brazilian PKI (public key infrastructure) or ICP Brasil is comprised of a chain of certification authorities including a root certification authority, certification authorities and register authorities, and also a policy management authority (management committee). This committee comprised of government and civil society representatives, is responsible for defining a set of regulations and standards for digital certification based on international public standards.

How can one know if a site is reliable?

A safe website offers encrypted access by means of a digital certificate authenticated by a trusted certification authority. The following sequence of examples demonstrates how to differentiate between re-

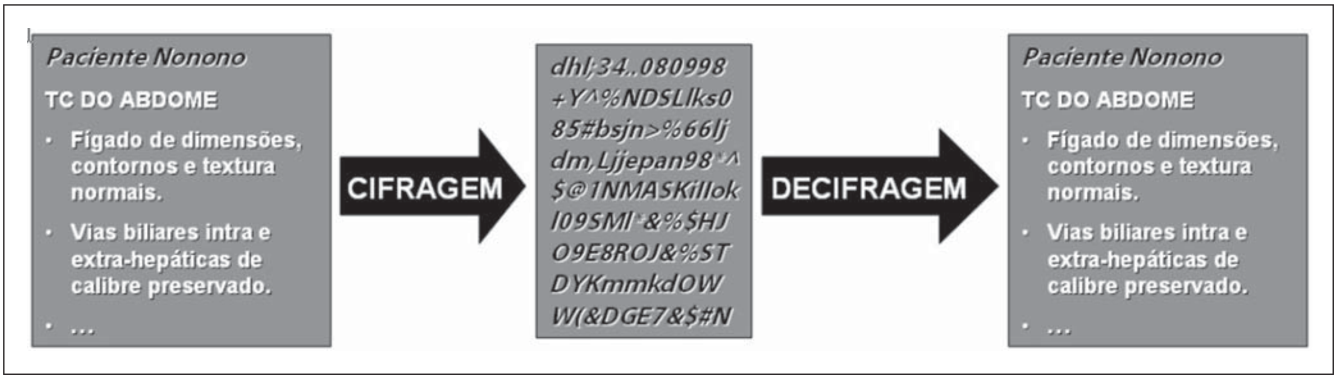

Paciente Nonono
TC DO ABDOME
• Fígado de dimensões, contornos e textura normais.
• Vias biliares intra e extra-hepáticas de calibre preservado.
• ...
CIFRAGEM
dhl;34..080998
+Y^%NDSLlks0
85#bsjn>%66lj
dm,Ljjepan98*^
$@1NMASKillok
l09SMl*&%$HJ
O9E8ROJ&%ST
DYKmmkdOW
W(&DGE7&$#N
DECIFRAGEM
Paciente Nonono
TC DO ABDOME
• Fígado de dimensões, contornos e textura normais.
• Vias biliares intra e extra-hepáticas de calibre preservado.
• ...

Figure 2. Symmetric-key cryptography: the ciphertext of a clinical report is transmitted over the internet. A same digital "key" is utilized both by the sender and the recipient for encryption and decryption of the document content.

liable and invalid digital certificates: Figures 4, 5 and 6 show examples based on the Portuguese version of a free internet browser, Mozilla Firefox®, running in Microsoft Windows®, Linux®, and many other operational systems. Other quite popular browsers such as Microsoft Internet Explorer® or Netscape®, also present very similar digital certificates.

A safe connection is always represented by a padlock icon on the bottom of the browser page (Figure 4). All of the browsers allow accessing information of this connection. By clicking on the padlock icon, one may access the connection certificate. Another option is through the menu "Tools > Internet options" at the top of the browser window. Independently from the option utilized, a window showing the data of the encrypted connection will be opened, specifying, among other information, if the browser could check the digital certificate authenticity, confirming the reliability of the site. Details about both this certificate and the issuer certification authority can be accessed by clicking on the appropriate menu. On Figure 5, Mozilla Firefox® windows showing information about the certificate (a) and about the certificate authentication chain up to the root certification authority (b). This authentication chain is the key issue concerning the digital certificate validity. All the entities involved are certificated by their immediately superior authority constituting a *trust network*. The digital certificate will not be valid if any entity in this chain is not reliable. As far as telemedicine projects are concerned, the Conselho Federal de Medicina – CFM (Federal Council of Medicine) determinates that ICP Brasil is in the root of the confidence chain, and accounts for medical websites security.

For evaluating the reliability of a certification authority, the browser refers to an internal, regularly updated list. This list is shown on Figure 6(a), and may be accessed through the browser's "Internet options" menu. If a browser cannot find a reference for any certification authority in a confidence chain, a window is opened [Figure 6(b)] asking a manual acceptance, or not, of the encrypted connection, and asking whether the issuer certification authority is reliable or not. If this certificate is permanently accepted, the issuer certification authority will be included in the list of reliable certification authorities, and the browser will automatically accept the digital certificate next time this site is visited. Sometimes, the list of certification authorities may be out-of-date, and this manual acceptance may be required. Notwithstanding, care should be taken in these cases.

What is electronic signature?

The electronic signature utilizes the same cryptography mechanism with a digitally certificated key. When a document is electronically signed, a summary of this document is generated by a predefined method called unidirectional hash. This document also will be immediately encrypted with a duly certified private key. This hash function is called unidirectional, considering the impossibility of reversion of this process to retrieve the original message, that is, a hash code can be generated from this message, but this message cannot be retrieved with the hash code.

A digitally signed document may be decrypted with a public key. Also one can see that this document has been signed with a reliable key certified by a certification authority that, in this case plays the role of a "digital notary" in the process of signature authentication. This represents an additional advantage: the technique allows not only checking the document authenticity, but also establishing a "logical immutability" of these data, since any alteration would invalidate the digital signature.

However, it is necessary to differentiate the electronic or digital signature from the digitized signature. A digitized signature is a handwritten signature reproduced by a scanner, generating an image file that can be easily attached to a document. It does not guarantee the electronic document authorship and integrity, considering the lack of an unequivocal association between the subscriber and the digitized text, since it

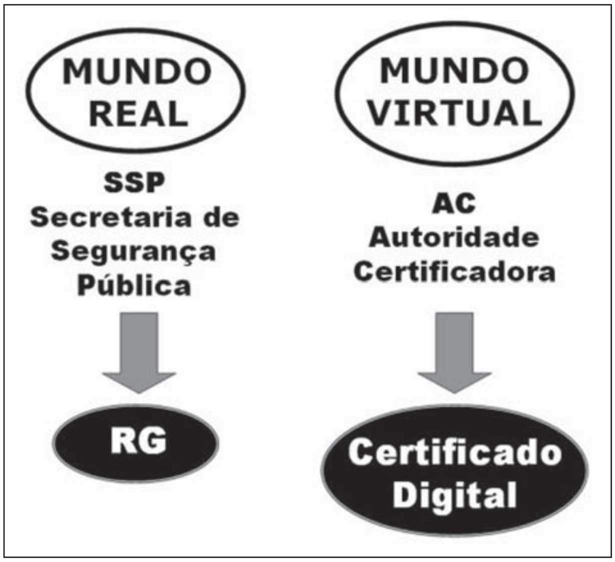
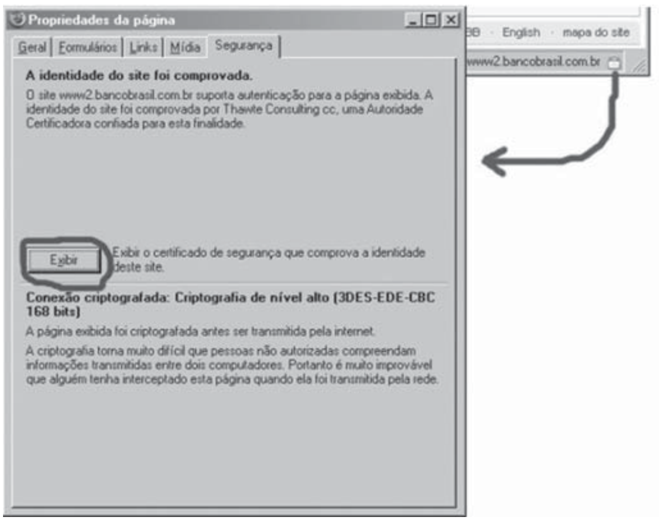


Figure 3. Correspondence between the secure identification of a document in the virtual and real worlds.



A identidade do site foi comprovada.

O site www2.bancobrasil.com.br suporta autenticação para a página exibida. A identidade do site foi comprovada por Thawte Consulting cc, uma Autoridade Certificadora confiada para esta finalidade.

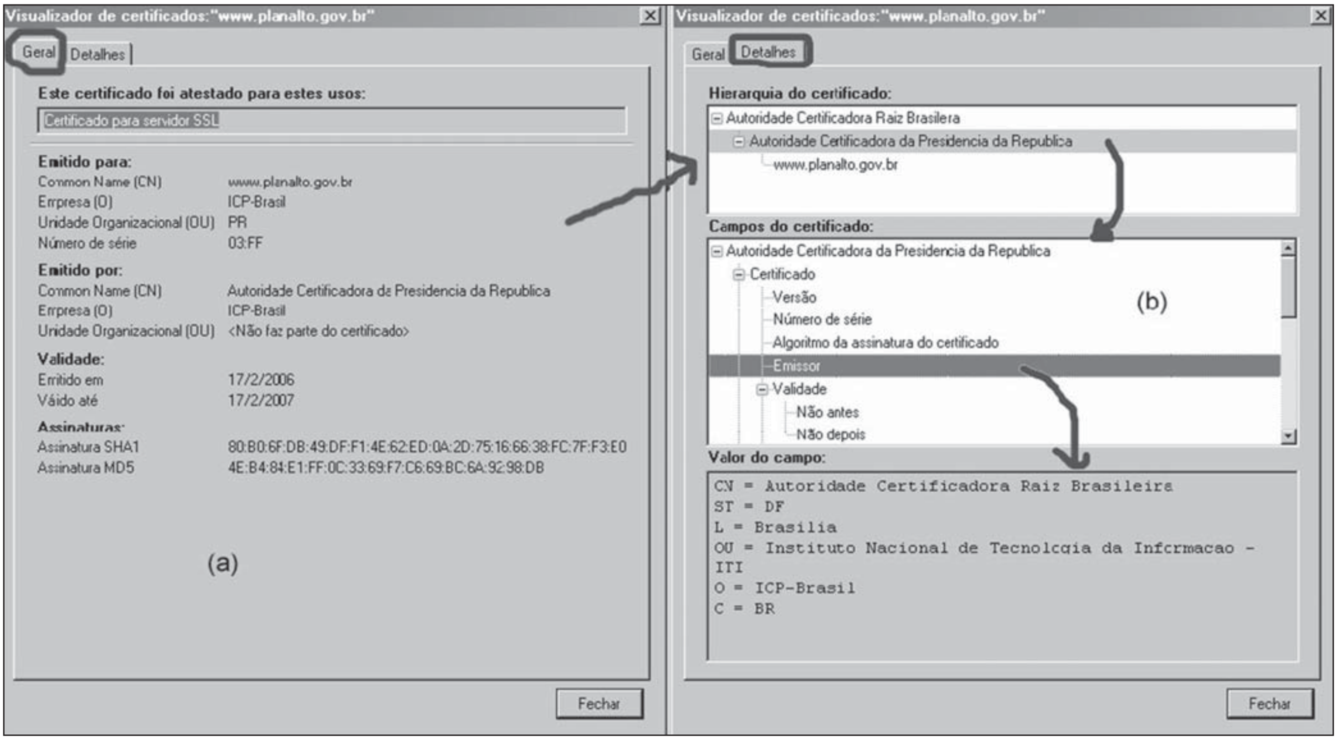
Exibir o certificado de segurança que comprova a identidade deste site.

Conexão criptografada: Criptografia de nível alto (3DES-EDE-CBC 168 bits)

A página exibida foi criptografada antes ser transmitida pela internet.

A criptografia torna muito difícil que pessoas não autorizadas compreendam informações transmitidas entre dois computadores. Portanto é muito improvável que alguém tenha interceptado esta página quando ela foi transmitida pela rede.

Figure 4. Properties of a secure webpage.


Visualizador de certificados:"www.planalto.gov.br"
Geral
Detalhes
(a)
Visualizador de certificados:"www.planalto.gov.br"
Geral
Detalhes
(b)
Fechar
Fechar

Este certificado foi atestado para estes usos:

Certificado para servidor SSL

Emitido para:

Common Name (CN)	www.planalto.gov.br
Empresa (O)	ICP-Brasil
Unidade Organizacional (OU)	PR
Número de série	03:FF

Emitido por:

Common Name (CN)	Autoridade Certificadora da Presidencia da Republica
Empresa (O)	ICP-Brasil
Unidade Organizacional (OU)	<Não faz parte do certificado>

Validade:

Emitido em	17/2/2006
Váido até	17/2/2007

Assinaturas:

Assinatura SHA1	80:B0:6F:DB:49:DF:F1:4E:62:ED:0A:2D:75:16:66:38:FC:7F:F3:E0
Assinatura MD5	4E:B4:84:E1:FF:0C:33:69:F7:C6:69:BC:6A:92:98:DB

Hierarquia do certificado:

```
⊟ Autoridade Certificadora Raiz Brasilera
  ⊟ Autoridade Certificadora da Presidencia da Republica
      └www.planalto.gov.br
```

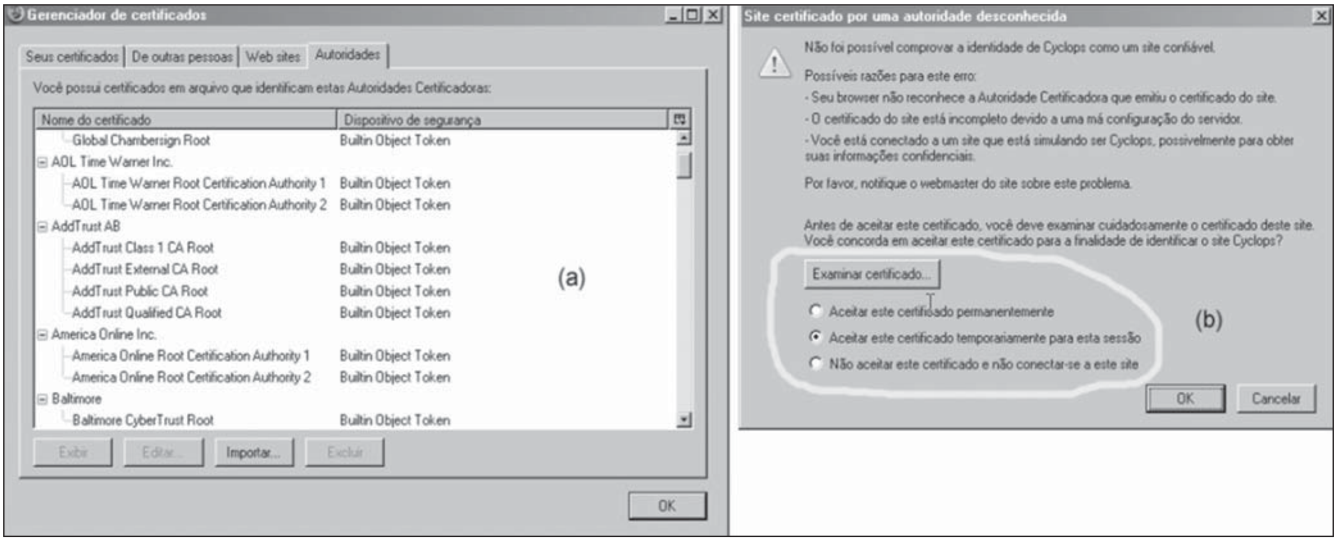
Campos do certificado:

```
⊟ Autoridade Certificadora da Presidencia da Republica
  ⊟ Certificado
      ├Versão
      ├Número de série
      ├Algoritmo da assinatura do certificado
      ├Emissor
      ⊟ Validade
          ├Não antes
          └Não depois
```

Valor do campo:

```
CN = Autoridade Certificadora Raiz Brasileira
ST = DF
L = Brasilia
OU = Instituto Nacional de Tecnolcgia da Infcrmacao -
ITI
O = ICP-Brasil
C = BR
```

Figure 5. Lay-out of a digital certificate of Palácio do Planalto (Brazilian government headquarters), showing (a) data and purposes of the certificate, and, on top, (b) the certification chain.



Você possui certificados em arquivo que identificam estas Autoridades Certificadoras:

Nome do certificado	Dispositivo de segurança
Global Chambersign Root	Builtin Object Token
⊟ AOL Time Warner Inc.	
AOL Time Warner Root Certification Authority 1	Builtin Object Token
AOL Time Warner Root Certification Authority 2	Builtin Object Token
⊟ AddTrust AB	
AddTrust Class 1 CA Root	Builtin Object Token
AddTrust External CA Root	Builtin Object Token
AddTrust Public CA Root	Builtin Object Token
AddTrust Qualified CA Root	Builtin Object Token
⊟ America Online Inc.	
America Online Root Certification Authority 1	Builtin Object Token
America Online Root Certification Authority 2	Builtin Object Token
⊟ Baltimore	
Baltimore CyberTrust Root	Builtin Object Token

Não foi possível comprovar a identidade de Cyclops como um site confiável.

Possíveis razões para este erro:
- Seu browser não reconhece a Autoridade Certificadora que emitiu o certificado do site.
- O certificado do site está incompleto devido a uma má configuração do servidor.
- Você está conectado a um site que está simulando ser Cyclops, possivelmente para obter suas informações confidenciais.

Por favor, notifique o webmaster do site sobre este problema.

Antes de aceitar este certificado, você deve examinar cuidadosamente o certificado deste site. Você concorda em aceitar este certificado para a finalidade de identificar o site Cyclops?

○ Aceitar este certificado permanentemente
● Aceitar este certificado temporariamente para esta sessão
○ Não aceitar este certificado e não conectar-se a este site

Figure 6. (a) List of trusted certification authorities know in the browser and (b) window for inclusion or rejection of a digital certificate issued by an unknown certification authority that could not be checked.

can be easily copied and inserted into another document.

As previously discussed, non-certified and digitally-signed electronic documents present a potential risk for alteration and easy falsification. However, it is important to note that a digital signature does not make the electronic document secret, because it is not ciphered. The confidentiality of an electronic document only can be safeguarded by the encryption of the message with the receiver's public key, because only the receiver's private key can decrypt its contents. The signature on a digital document is made with a personal code included in the private key. With this code, a document can be ciphered to be deciphered only with the respective public key, so identifying its subscriber. When the owner of a digital key produces a document digitally signing it, this document is encrypted and sent with his/her public key, and only can accessed by means of this public key. Security and reliability can be added to any electronic document (contracts, clinical reports, power of attorneys, projects, etc.) by this process. Signing an electronic document with a digital identity corresponds to attribute authenticity and logical integrity to this document. However, it is important to note that, with the techniques already described does not cover the timelines of a document. This is the next topic to be discussed.

The private key for digital signature may be stored in its owner's computer or in handheld hardware such as smart cards or tokens. The access to the information is made by means of a personal password defined by the owner determining a second level of security. The smart card is similar to a magnetic card, requiring a reading device for data transfer. On the other hand, the token is similar to a small key and requires a USB input device, usually available on computers CPU (Figure 7). Unfortunately, even with the utilization of a digital signature system, theft or loss of the device where the private key is stored still may occur, affecting the data security as well as the theft of a physical key may affect the security of a home or business.

Besides these ciphering, or cryptography, digital certification and signature technologies, timing information on electronic documents must be required for several reasons, for example, to prove that a document was signed before a digital certificate revocation, compromising of a private key, or even before a correlated procedure. An example applicable to teleradiology is the relevance of guaranteeing that a determined clinical report was issued **before** a surgery whose planning was based on information included in this report.

A way to safely guarantee tempestivity of an electronic document is utilizing a time stamping authority (TSA). A TSA is a server involved in the process of securely keeping track of the creation and modification time in electronic transactions, providing means to check the integrity of an electronic document, from the moment it was timestamped. TSA includes a computational platform, a digital identity (a public/private key pair, for example), a hardware safe module (HSM) — inviolable memory where these keys are stored — and a software for the necessary interaction. The TSA synchronizes local clocks with the national time standards (Observatório Nacional) by means of a *network time protocol* (NTP). Based on this information, the electronic document is signed with the private key of the TSA. This signed hash with the time stamp is sent back to the requester as a receipt. However, a copy of this receipt is stored in the TSA data bank guaranteeing:

– Privacy: access to a summary of the document, not to the original document.

– Integrity: the TSA digital signature and data integrity can be checked in the receipt.

– Non-repudiation: the receipt proves the existence of the document and respective timestamp. Not even the owner is able to repudiate its existence, nor the time stamping authority can deny the time stamping act.

– Reliability: sealed time stamping equipment, in compliance with physical security standards and auditable logic.

– Easy communication and storage: Only the document summary is utilized.

Which are the consequences of these technologies for teleradiology?

In practice, specifically approaching teleradiology, these several tools become essential for guaranteeing the security and reliability of clinical reports electronically available on the internet. Images, whether separately or in conjunction, as well as the respective clinical report, may be digitally signed and timestamped, so assuring the origin of these documents in a certain period of time, besides their integrity between the moments of their sending and receipt. The digital timestamping by means of a TSA is the sole way to guarantee this type of security for electronic documents [(4)].

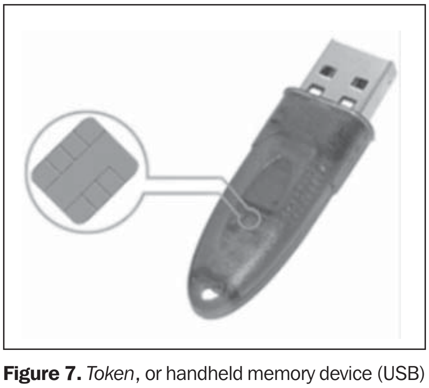


Figure 7. *Token*, or handheld memory device (USB) utilized for cryptographic key storage.

However, as far as specifically teleradiology is concerned, only a CFM resolution (nº 1643/2002), defines the requirements for safe storage, access and transmission of medical data[(5)]. In a careful review of this resolution, one can found that the article 2 requires a safe cryptography channel between the internet provider and the user's browser for medical data transfer in telemedicine. This safe transference must be performed through this cryptographic channel, utilizing the SSL (secure sockets layer) protocol and a cryptographic key provided and authenticated by the state certification authority. In truth, there is no requirement regarding any type of electronic documents certification, timestamping, or even digital signature. However, it is important to note that the same resolution, at its article 4, establishes that "the assistance to patients is a professional responsibility of their assisting physicians. The other professionals involved are solidarily and proportionally liable for any eventual damage to the patients". A question still remains as to whether the assisting physician involved in non-timestamped telediagnosis and second-opinion activities will be confident in taking over integral responsibility for a clinical report provided at distance by a radiologist, knowing that there is no guarantee that this report has not been digitally corrupted. In the State of São Paulo, the Cremesp resolution nº 97/2001 also deals with telemedicine-related subjects and, in some sections, more specifically with teleradiology activities[(6)]. The item 5 regarding transmission of diagnostic tests results over the internet establishes: "...an increasingly frequent procedure is the transmission of diagnostic images and tests results (radiographs, blood tests, urine tests, etc.) over the internet. Aiming at avoiding unintended data disclosure or privacy invasion, those who are involved in data transmission must adopt additional technical precautionary measures such as utilization of cryptography and special servers invulnerable to unauthorized access". Also this resolution is limited to a restricted and confidential access to diagnostic results by means of passwords and encrypted transmission by email, leaving an “open door” for digital fraud involving non-timestamped documents.

CONCLUSION

Telediagnosis and second-opinion activities are becoming more and more frequent practices in teleradiology as a result of new technologies associated with the scarcity of specialized professionals both in remote regions of the country and worldwide. Likewise, the electronic availability of radiological studies results represents a viable and interesting alternative for adding value to the medical assistance for requesting physicians and patients, and for costs reduction purposes. However, as a function of the vulnerability observed in the circulation of information and data over the internet, a series of data security concepts must be taken into consideration in the implementation of telemedicine projects, particularly regarding privacy, probity and temporality of electronically available information.

A guarantee must be given to ensure medical information integrity, the probity of its source, as well as the timeliness of its generation, transmission, manipulation and storage. Digital signature and certification, as well as certification authorities are part of this context. All medical image or procedure records involved in telemedicine activities must be digitally signed and certified. With these procedures, the source probity, content security and tempestivity will be guaranteed for electronic storage, transmission and availability of medical images and reports over internal and external computer networks. All and every access to a medical document only should be possible through the identification of its source by means of the public/private keys mechanism, so any attempt of violation would be detected because of the disagreement with the respective digital certificate.

It is essential that the mentioned concepts regarding electronic security are discussed by an increasing number of peer radiologists who must be aware of the potential difficulties resulting from an inappropriate utilization of non-certificated systems of teleradiology.

REFERENCES

1. Azevedo-Marques PM, Caritá EC, Benedicto AA, Sanches PR. Integração RIS/PACS no Hospital das Clínicas de Ribeirão Preto: uma solução baseada em “web”. Radiol Bras 2005;38:37–43.
2. Instituto Nacional de Tecnologia da Informação. [Acessado em: 12/5/2006]. Disponível em: http: //iti.br/twiki/bin/view/Main/CertFaqs
3. ICP Brasil: Infra-estrutura de chaves públicas brasileira. [Acessado em: 12/5/2006]. Disponível em: http://www.icpbrasil.gov.br
4. Certificados digitais – tire suas dúvidas. BRy tecnologia. [Acessado em: 12/5/2006]. Disponível em: http://www.bry.com.br/cursos/certificados.asp
5. Resolução CFM nº 1.643/2002. [Acessado em: 12/5/2006]. Disponível em: http://www.portalmedico.org.br/resolucoes/cfm/20021643_2002.htm
6. Resolução Cremesp nº 97, de 20 de fevereiro de 2001. [Acessado em: 12/5/2006]. Disponível em: http://www.portalmedico.org.br/resolucoes/CRMSP/resolucoes/2001/97_2001.htm