Digital Signatures Schemes: An Integrative Literature Review of Asymmetric Cryptography Usage as a Technical Method for Authenticity and Nonrepudiation on Remote Medical Reports for PACS

Natanael de Freitas Neto[1], Málaque Abdalla Nunes Freitas[2], Marcel da Câmara Ribeiro Dantas[3], Ricardo Alessandro de Medeiros Valentim[4]

[1]Laboratory of Technological Innovation in Health (LAIS) – Science and Technology Department – Federal University of Rio Grande do Norte (UFRN)

[2]Biotechnology School – Institute of Tropical Pathology and Public Health – Federal University of Goiás

[3]Laboratory of Technological Innovation in Health (LAIS) – Digital Metropole Institute – Federal University of Rio Grande do Norte (UFRN)

[4]Laboratory of Technological Innovation in Health (LAIS) – Biomedical Engineering Department – Federal University of Rio Grande do Norte (UFRN)

natanaelfneto@lais.huol.ufrn.br, malaqueabdalla@ufg.edu.br, mribeirodantas@lais.huol.ufrn.br, ricardovalentim@lais.huol.ufrn.br

Abstract. *Paper documents are being replace in different areas every day and, for any activity that requires authenticity, these new digital forms need to assure the same guaranties as the physical document does, i.e., authorship, authenticity, chronological evidence and integrity. In this article we shall analyze a viable use of available technologies to solve this evidenced issue. In medical reports for image exams, the use of a Picture Archive Communications System (PACS) allow the medical reports to be emitted remotely but it alone does not guarantee any of the security measurements for non-repudiation. The results presented in this article were obtained from an Integrative Literature Review and make evidence that the digital signatures model, based on asymmetric cryptography, could help solve this issue if a solution implementation does not change the installed DICOM/PACS environment and if it makes possible for an easy emitter check without the possibility of repudiation, within the local legislation.*

Resumo. *Os documentos em papel estão sendo substituídos em diferentes áreas todos os dias e, para qualquer atividade que exija autenticidade, essas novas formas digitais precisam assegurar as mesmas garantias que o documento físico, isto é, autoria, autenticidade, evidências cronológicas e integridade. Neste artigo é analisada uma viável utilização das tecnologias disponíveis a fim de solucionar-se o evidenciado problema. Em laudos médicos para exames de imagem, o uso de um Sistema de Comunicações de Arquivo de Imagem (PACS) permite que os laudos médicos sejam emitidos de forma remota, mas, por si só, não garantem nenhuma medida de segurança*

para não-repúdio. Os resultados apresentados neste artigo foram obtidos a partir de uma Revisão Integrativa de Literatura a evidenciam que o modelo de assinaturas digitais, baseados em criptografia assimétrica, poderia ajudar a resolver esta dificuldade, caso a implementação de uma solução não alterasse o ambiente DICOM/PACS já instalado e possibilitasse uma verificação do emissor facilmente, sem a possibilidade de repúdio, dentro da legislação local.

1. Introduction

The last decades have been marked by an explosion in the use of computer science as means to reduce paper consumption, increase productivity and automate processes. In the field of medical reports is no different and as a result, the flow of documents associated with the activity began to migrate from physical to the digital medium. However, replacing paper documents with electronic ones for any area requires them to offer equivalent guarantees, i.e., authorship, authenticity, chronological evidence (ADAMS, CAIN, et al., 2001) and integrity (WERLANG, 2014). Added to these, in the case of medical reports, there are still functional requirements for guaranteeing restricted access to the information and for the linkage between medical exam and its report.

These guarantees can be ensured in an electronic environment if the associated use of digital signatures with the DICOM[1] protocol (DICOM STANDARD, 2018) could be done. Information systems usually are the easiest and securest ways to associate data and they impact on the quality of management and user satisfaction. Different technological solutions adapted to health are being used, enabling the development of systems to support decision making. Brazilian public hospitals already attend a variety of exams through a Picture Archive and Communication Systems – PACS, allowing remote access to medical exams.

Due to the decades of PACS as being a standard medical archiving system, there are an enormous number of exams available and remotely accessible, which opens the possibility that, through the application of computational tools, several solutions can be developed for the also numerous difficulties present in the public health, such as the lack of and equal distribution of physicians by inhabitants in different regions.

2. Data Structure of Medical Images File Format Attributes

The Brazilian public hospitals that have medical equipment unsure a huge diversity of types of exams, already standardized, via DICOM protocol, by NEMA[2] (DICOM PS3.3 2017d - Information Object Definitions [Patients], topic C.7.3.1.1.1 Modality, 2017).

The available system structure for archiving the exams image media, PACS, and the standardized protocol for the association of data to the medical image, DICOM,

[1] DICOM is an acronym for Digital Imaging and Communications in Medicine. The first standard covering point-to-point image communication was ACR-NEMA 300, released in 1985. The specified image transmission used a dedicated 16-bit parallel interface (DICOM STANDARD, 2018),

[2] NEMA is an acronym for the National Electrical Manufacturers Association. The association has about 350 electrical and medical imaging equipment manufacturers, founded in 1926 and based in Rosslyn, Virginia (NEMA, 2017).

allows a cheap and secure development environment for new features in these models. Thus, to add the nonrepudiation capability of signed data into the DICOM image format, which is based on the ACR-NEMA specification (ACR-NEMA, 1989) and adds a file head and several private pre-defined available tags (BIDGOOD and HORII, 1992), a standardized procedure must be followed.

The common structure to add any custom data in DICOM formatted files is done by file attributes called tags that should be developed in such a way to prevent conflicts with the private elements documented by any device manufacturer in the DICOM Conformance Statement.

A usual DICOM tag is composed of a two-byte group, as *g* for a bit, and a two-byte element, as *e* for a bit:

$$(gggg, eeee)$$

The NEMA Private Data Element documentation (DICOM PS3.5 2013 - Data Structures and Encoding, topic C.7.8 Private Data Element [Data Set], 2017) set four rules to avoid conflicts with private data elements that can be resumed as:

1. Private Creator Data Elements numbered $(gggg, 0010 - 00FF)$, where $gggg$ *i*s an odd number, shall be used to reserve a block of elements with group number $gggg$ for use by an individual implementer. The implementer shall insert an identification code in the first unassigned element in this series to reserve a block of private elements (DICOM PS3.5 2013 - Data Structures and Encoding, topic C.7.8.1 Private Data Element Tags [Data Set], 2017).
2. Private creator data element $(gggg, eeee)$ identifies the implementer, until Private Creator Data Element $(gggg, FFFF)$ identifies the implementer reserving elements $(gggg, FF00 - 00FF)$ (DICOM PS3.5 2013 - Data Structures and Encoding, topic C.7.8.1 Private Data Element Tags [Data Set], 2017).
3. Encoders of Private Data Elements shall be able to dynamically assign private data to any unreserved blocks within the Private group and specify this assignment through the blocks corresponding Private Creator Data Elements (DICOM PS3.5 2013 - Data Structures and Encoding, topic C.7.8.1 Private Data Element Tags [Data Set], 2017).
4. Elements with the tags $(0001, eeee)$, $(0003, eeee)$, $(0005, eeee)$ and $(0007, eeee)$ shall not be used (DICOM PS3.5 2013 - Data Structures and Encoding, topic C.7.8.1 Private Data Element Tags [Data Set], 2017).

These tags are a resourceful way to add new content, such as medical reports and its mechanisms of validation, authentication, security and nonrepudiation, to the available PACS structure in any common medical facility, through the private group unreserved blocks of the DICOM protocol. Then, to satisfy that these security attributes can be not just added but verified afterwards, a digital signature scheme is the best development practice to be adopted.

3. Digital Signatures Schemes

Signatures are used as proof of authorship and authenticity for centuries, where individuals record their names in documents and messages. To incorporate these attributes to a digital document it is necessary a mechanism that has both technical and legal validity of guaranteeing the non-repudiation of documents after been signed.

The major process used in the modern communication for authenticity and validation is asymmetric cryptography. It is used from credit cards, securing that only the card owner can buy with its card to cryptocurrencies, helping manage all virtual wallets trades and its owners' identities. All possible due to public key distribution.

Key distribution was a major problem for secure communications until November 1976, when Whitfield Diffie and Martin Hellman invented the public key cryptography in their article "New Directions in Cryptography" (DIFFIE and HELLMAN, 1976), and in particular the digital signature scheme (LYSYANSKAYA, 2002). With the use of one of these schemes, a sender is able to send a signed message simply by applying a secret key to the message, that is, by encrypting it. When the recipient receives the message, it is possible to verify the signature by applying in the encrypted message a second, publicly accessible, key (BATTEN, 2012).

In digital signature schemes, each user has an identity, represented by his public key, that is, a sequence of bits available to all (LYSYANSKAYA, 2002). These schemes exist if, and only if, there are unidirectional transformations (ROMPEL, 1990). Asymmetric cryptography consists precisely of a one-way transformation, through a pair of computationally efficient and non-viable functions for inversion (LYSYANSKAYA, 2002).

For a couple of functions:

$$\mathrm{E_k(M)} \rightarrow \mathrm{m}$$

$$D_k(m) \rightarrow M$$

The major M represents the plain text message as the minor m represents the ciphertext. These equations represent easily computable functions for a given key k. At the same time, it is not computationally feasible to obtain k, even under M or m. It is not an easy task to obtain even one of the messages, possessing the other, without also possessing the value of k (DIFFIE; DIFFIE; HELLMAN, 1976; RIVEST; SHAMIR; ADLEMAN, 1978).

The first digital signature scheme was constructed by Rivest, Shamir and Adleman in the document that also proposed the first public key cryptography system (RIVEST, SHAMIR and ADLEMAN, 1978). Their signature scheme is based on an assumption they introduced, called "the RSA assumption".

The mathematical process for the public key cryptography method consists of:

$$m = E(M) = M^e * \ mod\ n$$

$$M = D(m) = m^d * \ mod\ n$$

Where *M* represents the plaintext message in ciphertext, *n* is the product of two prime numbers ($n = p * q$), and it is a number between 3 and *n*-1, and *e* must also be prime relating to *p*-1 and to *q*-1, and *d* shall be calculated by the expression:

$$M = D(m) = m^d * \ mod\ n$$

Thus, the private key is given by *n* and *d*, and the public key is given by *n* and *e*. The RSA assumption states that: even with a value of *e* close to or equal to 3, the transformation can be considered unidirectional, being that having the result of numerous factors, *n*, and the message encrypted *m*, is still computationally infeasible to obtains a pair *M* and *e* whose message *m* is equal to $M^e * mod\ n$ (RIVEST; SHAMIR; ADLEMAN, 1978).

For the time being, the RSA assumption is given as a standard cryptographic assumption (LYSYANSKAYA, 2002).

4. Objectives

In this article we shall analyze a viable use of available technologies to solve the issue of not having a trusted mechanism, associated with the DICOM file format, that reliably guarantees a non-repudiation attribute for data registered in Private Data Elements of DICOM format file.

These methods might allow the remote issuance of medical reports for exams images to be incorporated into the range of functionalities already present for the DICOM protocol and its archiving systems.

The advance in the security, authentication and authorship of data insertion on DICOM files could allow the responsibility for the data to be ascribe to its emitter with a technical and legal non-repudiation attribute and remove the possibility that technicians, physicians, medical residents and other professionals that might have access to the database or the DICOM files to access or edit its data without previous given permission.

5. Methodology

Brazilian Public Health Policy Administrative Rule No. 2564/2011, redefines the National Telehealth Network Program (BRAZILIAN MINISTRY OF HEALTH, 2011). Thus, it is possible for physicians in regions with high rates of professionals per inhabitant to remotely send reports through the internet for medical image exam of users of the public health systems (patients) in regions where these same professionals are scarce.

To highlight the relevant studies and technologies on the subject, the Integrative Literature Review was the method used, establishing criteria for inclusion and exclusion of studies and technologies; search in literature; categorization; evaluation of the studies and technologies included in the integrative review; interpretation of results; presentation of the review and synthesis of the knowledge acquired.

The time scale for the research adopted was from date of the first digital signature scheme ever proposed, in 1978 (RIVEST; SHAMIR; ADLEMAN, 1978), to the present days (2018). The overall criteria to include studies and technologies were:

- Addressing the issues of security of the data involved;
- Exclusive use of open sourced technologies;
- Easy retrieval of the content after been secured;
- Implementation of a digital signatures scheme does not interfere with the existing PACS/DICOM structured;

To obtain a trustworthy result and different opinions and experiences about involved technologies and knowledge, six main articles database were considered of great value to the involved areas, these databases are:

- *DSpace@MIT: MIT Open Access Articles;*
- *Harvard Dash: Digital Access to Scholarship at Harvard;*
- *Elsevier Scopus database;*
- *Google Scholar repository;*
- *IEEE Xplore Digital Library*
- *CAPES Periodical repository.*

Also, the guiding question for the review was the implantation of new information and communication technologies in the context of medical reports, in agreement with the medical image systems, i.e., Picture Archive and Communication Systems – PACS.

6. Results and Conclusions

Among the articles covered in this integrative review, the main studies and technologies found refer to the use of cryptography methods. There are basically two categories of encryption depending on the type of security keys that is used to encrypt and decrypt the data. These are the symmetric and asymmetric encryption techniques (THAKUR and KUMAR, 2011).

Mostly, the evidence in literature shows the use of asymmetric cryptography mechanisms as the reliable technique to protect communication, restrict information access and to generate and verify secure digital signatures (RIVEST; SHAMIR; ADLEMAN, 1978; LYSYANSKAYA, 2002; THAKUR and KUMAR, 2011, WERLANG, F. C., 2014). This happen as symmetric cryptographic methods has a problem, no matter how strong they are, each pair that is going to exchange messages would need a pair of keys and as the number of pairs increases, the number of required pairs of keys would increase indefinitely (KAPOOR, PANDYA and S. SHERIF, 2011).

Also, a mechanism would be required to manage and distribute the secret keys for each of the points that may be in geographically difficult locations to access, as well as on unsafe routes for traffic, such as public internet access. Problems not evidenced on asymmetric cryptographic method (RIVEST, R. L. 1990; LYSYANSKAYA, 2002).

In software development, topics commonly associate with a PACS environment, the use of private groups is vastly adopted as a source of solving local issues which the standardized protocol often cannot.

These results lead to the conclusion that information systems represent a major impact on the quality of public health system users (patients) management, care and

satisfaction and, even when observed in different stages of implementation, the development of health-adapted information technology solutions has gradually been used and allows the development of methods for comparing practices, exchanging information, supporting systems for decision-making and facilitating access to education processes.

In the case of a system for remote medical reports emitter validation, the benefit occurs both for areas with low concentration of professionals per inhabitants with a relatively cheap solution for professionals who will have an increase in the supply of work without the need to move to other regions, which are often professionally unattractive.

7. Future Work

Many future works could be done by implementing digital signatures schemes into DICOM formatted files. One of then is incorporated on the National Telehealth Network Program, which is the national platform that will enable public health physician to retrieve DICOM files, view its exam image, emit the report and digitally sign it. All the process running on a supply and demand workflow.

The accumulation of publicly accessible digital information, such as anonymized DICOM files, allows institutions and companies to use the database for development of algorithms for artificial intelligence and machine learning as advanced mechanisms of decision-making for medical diagnosis.

With a large amount of image exam data, properly anonymized, and related medical reports, machine leaning techniques and different intelligent algorithms could be used to find correlations, allowing algorithms for prediction on possible diseases to be used in the exams, helping physicians to better precise the diagnostic, enable an earlier treatment start for the health system user (patient) and reduce the possibility of treatment sequels.

References

ACR-NEMA Committee. Digital imaging and communications. ACR-NEMA standards publication No. 300-1988. Washington, DC: National Electrical Manufacturers Association, 1989; iii.

ADAMS, C. et al. Internet X.509 Public Key Infrastructure Time-Stamp. [S.l.]. 2001.

BATTEN, L. M. Public Key Cryptography: Applications and Attacks. Melbourne: IEEE Press, 2012. p. 2-131.

BIDGOOD, W. D. Jr; HORII, S. C. Introduction to the ACR-NEMA DICOM Standard; DOI: 10.1148/radiographics.12.2.1561424; Radiographics; p. 345-355; March 1992.

BRAZILIAN MINISTRY OF HEALTH, Minister's Cabinet. Administrative Rule No. 2.546. October 27, 2011.

DICOM STANDARD. Digital Imaging and Communication in Medicine. History. DICOM Standard 2018. Available at: < https://www.dicomstandard.org/history/>

DIFFIE, W.; HELLMAN, M. New Directions in Cryptography, v. T-22, n. 6, p. 644-654, November 1976.

NEMA. DICOM PS3.3 2017d - Information Object Definitions [Patients], topic C.7.3.1.1.1 Modality. [S.l.]. 2017. Available at: <http://dicom.nema.org/medical/dicom/2017d/output/chtml/part03/sect_7.3.html >

NEMA. DICOM PS3.5 2013 - Data Structures and Encoding [Data Set], chapter 5, topic C.7.8 Private Data Element, 2017. Available at: <http://dicom.nema.org/dicom/2013/output/chtml/part05/sect_7.8.html>

NEMA. DICOM PS3.5 2013 - Data Structures and Encoding [Data Set], chapter 5, topic C.7.8.1 Private Data Element Tags, 2017. Available at: <http://dicom.nema.org/dicom/2013/output/chtml/part05/sect_7.8.html#sect_7.8.1>

DIFFIE, W.; DIFFIE, W.; HELLMAN, M. E. New Directions in Cryptography. IEEE Transactions on Information Theory, v. 22, n. 6, p. 644–654, 1976.

LYSYANSKAYA, A. Signature Schemes and Applications to Cryptographic Protocol Design. [S.l.]: Massachusetts Institute of Technology, 2002.

NEMA. About the National Electrical Manufacturers Association. [S.l.]. 2017.

RIVEST, R. L. Cryptology. In: LEEUWEN, J. V. Handbook of Theoretical Computer Science. Cambridge: Elsevier, 1990. p. 717-755. Available at: <http://people.csail.mit.edu/rivest/Rivest-Cryptography.pdf>.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Programming Techniques, 21, n. 2, February 1978. p. 120-126. MIT Laboratory for Computer Science and Department of Mathematics.

ROMPEL, J. One-way functions are necessary and sufficient for secure, Baltimore, 1990. p. 387-394.

WERLANG, F. C. *Assinatura Digital com Reconhecimento de Firma: um modelo de assinatura digital centrado no usuário*. Florianópolis. 2014.