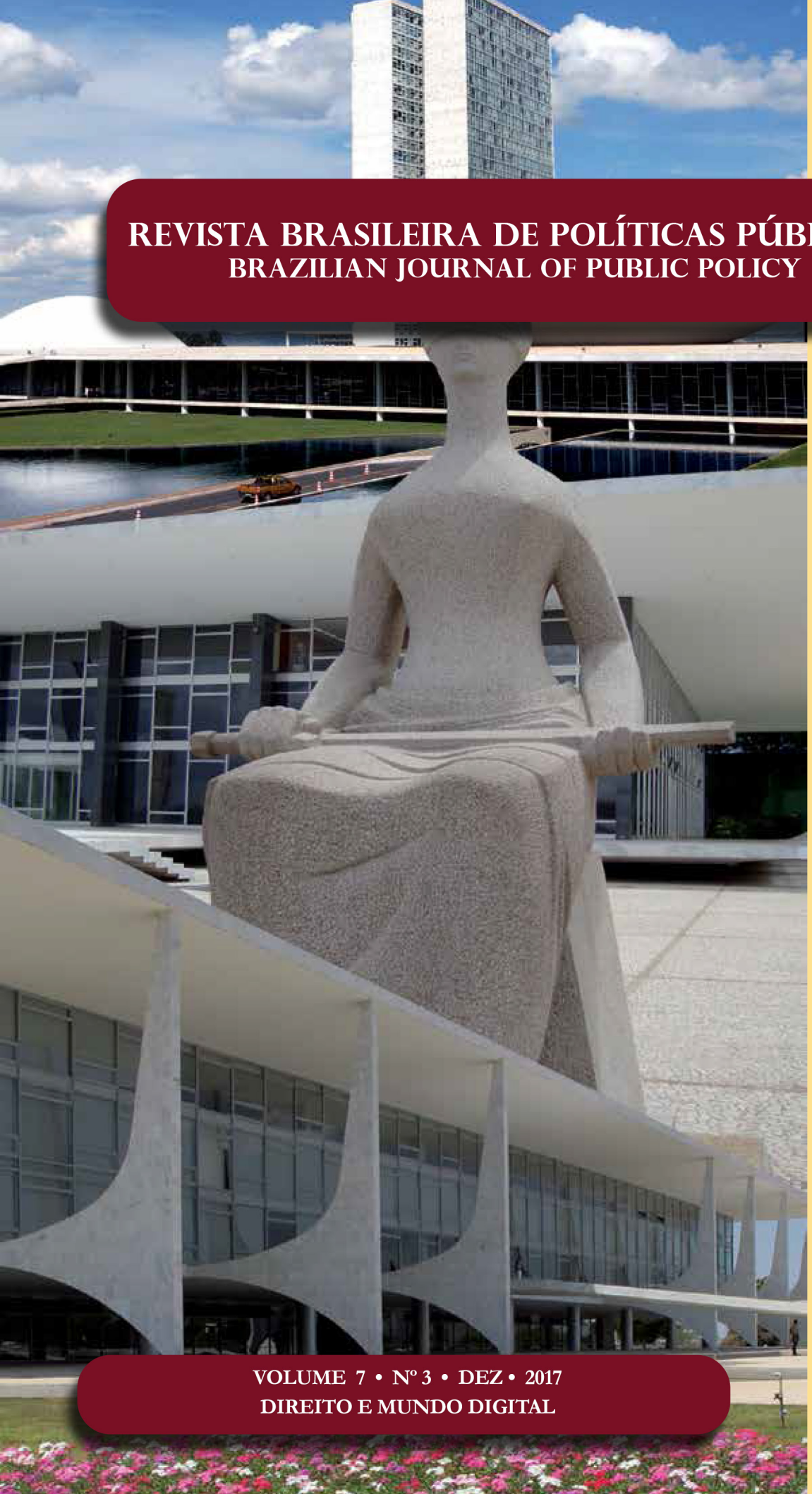

UniCEUB
ISSN 2236-1677

REVISTA BRASILEIRA DE POLÍTICAS PÚBLICAS
BRAZILIAN JOURNAL OF PUBLIC POLICY

Fostering e-government in Brazil: a case study of digital certification adoption

Promovendo o governo eletrônico no Brasil: um estudo de caso sobre a adoção da certificação digital

Lamartine Vieira Braga

VOLUME 7 • Nº 3 • DEZ • 2017
DIREITO E MUNDO DIGITAL

Sumário

doi: 10.5102/rbpp.v7i3.4866

Fostering e-government in Brazil: a case study of digital certification adoption*

Promovendo o governo eletrônico no Brasil: um estudo de caso sobre a adoção da certificação digital

Lamartine Vieira Braga**

Abstract

In the rise of the new Information and Communication Technologies (ICT), governments worldwide as well companies go through a transition, trying to adapt themselves to the Knowledge Society demands. Such innovative technologies enable the improvement of relations between society and their governments, and between companies and their partners, providing improvements in quality and efficiency of public and private sectors. At the same time that these interfaces provide unprecedented opportunities, the growth of the digital universe reveals threats regarding the vulnerability of electronic information. The digital certificate may be the answer that governments and businesses need to operate in this new environment of uncertainty. This article aims to present a current overview of the technology involved in digital certification and a list of the most important applications currently available in Brazil. Therefore, it starts with a series of concepts related with the beginning of encryption, explains the specific aspects of certification and digital signature, and discusses the organizational and legal aspects of the Infrastructure for the Brazilian Public Key Infrastructure. Finally, we present the main applications of this technology in Brazil at this moment. The conclusion we reach is that there is great potential for the use of digital certification in the country that can be the basis for the safe development of electronic government and commerce within confidence and tranquillity to their users.

Keywords: Electronic Government. Electronic Commerce. Public Key Infrastructure. Digital Certification. Encryption. Brazil.

Resumo

Na emergência das novas Tecnologias de Informação e Comunicação (TIC), os governos de todo o mundo, bem como as empresas, passam por uma transição, tentando se adaptar às demandas da Sociedade do Conhecimento. Tais tecnologias inovadoras permitem a melhoria das relações entre a sociedade e seus governos e entre empresas e seus parceiros, proporcionando melhorias na qualidade e na eficiência dos setores público e privado. Ao mesmo tempo em que essas interfaces oferecem oportunidades sem precedentes, o crescimento do universo digital revela ameaças relacionadas

* Recebido em 20/10/2017
Aprovado em 12/12/2017

** Doutor em Administração pela Universidade de Brasília/University of Edinburgh Business School. Professor Colaborador da Fundação Getúlio Vargas (FGV Management). Email: lamartine.braga@gmail.com

à vulnerabilidade da informação eletrônica. O certificado digital pode ser a resposta que os governos e as empresas precisam a fim de operar neste novo ambiente de incerteza. Este artigo tem como objetivo apresentar uma visão geral atual da tecnologia envolvida na certificação digital e uma lista das aplicações mais importantes atualmente disponíveis no Brasil. Portanto, ele se inicia com uma série de conceitos relacionados com o prelúdio da criptografia, explica os aspectos específicos da certificação e assinatura digitais e discute os aspectos organizacionais e legais da Infraestrutura de Chaves Públicas Brasileira. Por fim, são apresentadas as principais aplicações desta tecnologia no Brasil neste momento. A conclusão a que se chega é que há um grande potencial para o uso da certificação digital no país que pode ser a base para o desenvolvimento seguro do governo e comércio eletrônicos com confiança e tranquilidade para seus usuários.

Palavras-chave: Governo eletrônico. Comércio eletrônico. Infraestrutura de chaves públicas. Certificação digital. Criptografia. Brasil.

1. Introduction

The emergence of the Knowledge Society is a profound change in the state organization and on business. It is a global phenomenon, a major source for potential transformation of the social and economic activities, whose structures and dynamics inevitably will be, to some extent, affected by the information infrastructure available.

Although the importance of information for organizations is universally accepted, what makes it especially significant today is its digital nature. Approximately 92% of the information generated in the world today is created in digital format. It is estimated that by 2020 there will be over 5,200 gigabytes for every person on the planet, making a total of 40,000 exabytes (or 40 trillion gigabytes). The International Data Corporation – IDC (2012) suggests that the virtual world will double in size every two years until 2020.

This scenario, while it opens up various opportunities, imposes new challenges related to the vulnerability of transmitting sensitive data on a secure way.[1] The three main problems faced by users of the internet are integrity, authentication, and non-repudiation. Cryptography holds the most promise as a solution to these problems and the public key cryptography (PKI) in particular appears to be best suited to fulfill these requirements.[2]

Developed based on the public-key encryption technique, the PKI creates, stores and manages digital certificates which map public keys to owners. It consists of a certificate authority (CA) that both issues and verifies the digital certificates, a registration authority that verifies the identity of users requesting information from the CA, and a central directory which securely stores keys.[3]

The purpose of this article is to present an overview of applications of digital certification in Brazil, both in the public sector and in the private sector, as well the technology that covers such processes. Therefore, this paper is organized as follows: besides this introductory section, the second section presents the theory on the symmetric and asymmetric encryption. The third section discusses the procedures evolved in the digital signature. The fourth section explains the concepts of the digital certificates. The fifth section explains the operation of a public key infrastructure, from the organizational, legal and technological perspective. The sixth section shows the main applications of digital certification in Brazil, including those used by public and private organizations. Finally, the seventh section presents the conclusions of the article.

1 BELDAD, A.; JONG, M.; STEEHOUDER, M. 'I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions'. *Computers in Human Behavior*, v. 27, n. 6, p. 2233-2242, 2011.

2 LAIH, C.; JEN, S.; LU, C. 'Long-term confidentiality of PKI'. *Communications of the ACM*, v. 55, n. 1, p. 91-95, 2012.

3 ZHANG, J.; HU, N.; RAJA, M. K. 'Digital certificate management: Optimal pricing and CRL releasing strategies'. *Decision Support Systems*, v. 58, n. 1, p. 74-78, 2014.

2. Symmetric and asymmetric encryption

Back to ancient times, man tries to hide its secrets to win wars and to defend commercial interests. The earliest record is from a rudimentary encryption from the time of the Pharaoh Amenemhet in Egypt around the year 1900 BC.[4] As one of the best known examples in history, it reports the roman Julius Caesar use of a very simple technique, that is, a simple replacement of alphabet characters with the intention to confuse someone who eventually intercept the messages.[5]

Today, the need to protect electronic information, ensuring safety of transactions and privacy of the users has taken encryption to evolve and be present in various activities of daily life, from the most mundane to the most complex. With the advent of computers, rather than shuffling and replace letters of the alphabet, as in traditional techniques, we started to work with binary digits. Encryption incorporated intricate Mathematics' algorithms in its processes, taking it to speeding process and to a level of complexity never imagined before.

The act of cipher, encrypt, and encode corresponds to the "data transformation process or information to an unintelligible form using a cryptographic algorithm and a cryptographic key". The data cannot be recovered without using the reverse process of deciphering "or" the process of data conversation unreadable code to prevent unauthorized persons having access to information. According the Brazilian Infrastructure for Public Key - ICP (2007), "the reverse procedure, i.e., decipher, decode or decrypt is the "process that transforms previously encrypted and unintelligible data back to its readable form". Thus, it is the distinction between the cipher text (encrypted data) and the clear text, or simple (since it was not encrypted or that was deciphered).

Computed encryption algorithms are often complex mathematical operations or just bit manipulations.[6] There are two competing factors to consider when choosing an algorithm: speed and resistance to attacks.[7] What is needed is also a key, that is, a mathematical value (number or set of alphanumeric characters) which is fed with the algorithm to start its operation. Every key has a size expressed in bits.[8]

If an encrypted message suffers interception, it is necessary to determine both the key and the mathematical operations of the algorithm in order to get the clear text. Algorithm operations are mathematically deterministic; can be complex, but they are not random. The keys provide the random factor that algorithms do not possess and lining of difficulty attempts to deduct the original data from the encrypted data.[9]

Additionally, the question of the keys is of importance, because any given data can be decoded by trying to employ all possible keys, which is called brute force attack. In these cases, the time required to break a cipher is directly proportional to key size; higher, stronger security. The 128-bit size is considered safe, taking into account the current processing capacity of computers.[10] Another factor that must be taken into consideration is that the longer the key, the lower the velocity of an algorithm.[11] Although various algorithms are widely known in the public domain, the keys must remain confidential.[12]

Symmetric encryption uses the same key, secret, to encode and decode information. By this method it

4 KAHN, D. *The codebreakers:* the comprehensive history of secret communication from ancient times to the internet. New York: Scribner, 1996.

5 SINGH, S. *The code book:* the science of secrecy from ancient Egypt to quantum cryptography. New York: Anchor Books, 1999.

6 BURNETT, S.; PAINE, S. *RSA Security's Official Guide to Cryptography*. Berkeley: Osborne/*McGraw-Hill*, 2002.

7 ATREYA, M. et al. *Digital Signatures*. Berkeley: McGraw-Hill, 2002.

8 FEGHHI, J.; WILLIAMS, P. *Digital certificates:* applied internet security. New Jersey: Addison Wesley, 1999.

9 ATREYA, M. et al. *Digital Signatures*. Berkeley: McGraw-Hill, 2002.

10 CHOUDHURY, S., BHATNAGAR, K., and HAQUE, W. (2002) Public key infrastructure: implementation and design. New York: M&T Books, 2002.

11 BURNETT, S. and PAINE, S. (2002) RSA Security's Official Guide to Cryptography. Berkeley: Osborne/McGraw-Hill, 2002.

12 ADAMS, C.; LLOYD, S. *Understanding PKI:* concepts, standards, and deployment considerations. 2nd. New Jersey: Addison Wesley, 2003.

is possible to confidentiality, authenticity and data integrity.[13] This key must be kept secret to ensure confidentiality of information. Several algorithms have been developed based on the concept of symmetric key cryptography.

A conceptualization of some of the requirements relating to information security[14] are: (i) Confidentiality, that is, the ability to access data only by authorized persons, even in shared environments; (ii) Integrity is the guarantee of accurately and completely information, from source to destination without any modifications; (iii) Authenticity is the ability to verify the identity of a user, confirming that the information is in fact originating from the alleged origin.

Having been explained their applications; information security can be defined as the preservation of confidentiality, integrity and availability. Additionally, authenticity, accountability, non-repudiation and reliability can also be involved.[15]

While symmetric encryption exhibits a number of desirable features such as high speediness, there are some drawbacks, such as: the need to exchange the secret key; difficulties to start a secure communication between previously unknown parties; and difficulties of scale (a community of n users requires $n^2/2$ unique secret keys).[16]

In order to address security issues relating to key distribution, one must use another modality of encryption, called asymmetric or public key. This method uses a pair of different keys instead of only one secret key. The first, known as private, is always kept secret by its holder; it is not transferred to anyone, and is safely stored. The public key, in turn, is accessible and can be freely shared with anyone.[17] His invention was attributed to Whitfield Diffie and Martin Hellman in 1975, although there are rumors that their concepts had been previously discovered.[18]

The relationship among the key pair is mathematical; the knowledge of one of them does not allow the deduction of another. This means that a key can be made public without reducing its security, provided that the other remains secret. The safety of this technology is based on the fact that, currently, it is computationally infeasible to derive the private key from the public key. Theoretically, the private key can always be deduced, but the time required regarding the today's computational capacity makes the procedure unviable.[19]

Encryption of public key allows us to encrypt messages with the public key that can only be decrypted with the corresponding private key. This enables secure electronic communications without the problem of key distribution. This technique also allows encrypting messages with the private key that can only be decrypted with the corresponding public key, a mechanism used in digital signatures.[20]

Virtually all public key algorithms are based on one of the following mathematic techniques: factorization of integers; calculation of discrete logarithms and calculation of discrete logarithms of elliptic curves.[21]

Asymmetric encryption has the disadvantage of being a slow process compared to the symmetrical method; this difference may be 100 to 1,000 times.[22] For this reason, instead of encrypting the entire text with the private key, launches the feature to encode representative data, which is a summary of the message,

13 FEGHHI, J.; WILLIAMS, P. *Digital certificates:* applied internet security. New Jersey: Addison Wesley, 1999.
14 STALLINGS, W. *Data and computer communications*. 8th New Jersey: Pearson Prentice Hall, 2007.
15 BRAZILIAN ASSOCIATION OF TECHNICAL STANDARDS. *NBR ISO/IEC 17799:* código de prática para a gestão da segurança da informação. 2nd. Rio de Janeiro: ABNT, 2005.
16 ADAMS, C.; LLOYD, S. *Understanding PKI:* concepts, standards, and deployment considerations. 2nd. New Jersey: Addison Wesley, 2003.
17 CHOUDHURY, S.; BHATNAGAR, K.; HAQUE, W. *Public key infrastructure:* implementation and design. New York: M&T Books, 2002.
18 FEGHHI, J.; WILLIAMS, P. *Digital certificates:* applied internet security. New Jersey: Addison Wesley, 1999.
19 ADAMS, C.; LLOYD, S. *Understanding PKI:* concepts, standards, and deployment considerations. 2nd. New Jersey: Addison Wesley, 2003.
20 ATREYA, M. et al. *Digital Signatures*. Berkeley: McGraw-Hill, 2002.
21 FEGHHI, J.; WILLIAMS, P. *Digital certificates:* applied internet security. New Jersey: Addison Wesley, 1999.
22 FEGHHI, J.; WILLIAMS, P. *Digital certificates:* applied internet security. New Jersey: Addison Wesley, 1999.

known in English as *hash* or *digest*.[23]

A summary algorithm works a message within a variable-length and produces a result of fixed size. It takes three properties to ensure its cryptographic security. First, may not be feasible to determine the original message from the summary. In other words, the direction of the message to your resume is a one--way function and cannot be reversed. Second, it may not be possible to find an arbitrary message that has a desired abstract in particular. Third, it must be computationally infeasible to find two messages that have this summary. Furthermore, a well-designed algorithm shows a path, randomly assigned, to the message and any kind of change, even of just one bit of the original message results in an entirely new summary with no correlation with the previous one.[24]

When the last property described above is violated, it does the so called collision, a situation in which two messages produce the same summary. Although the amount of possible messages is almost infinite, the same does not occur with the number of summaries.[25]

The *hash* function does not provide confidentiality and do not involve the use of a secret key to generate the summary. They are well suited for authentication and to ensure data integrity. They can also be used for the purpose of compressing data, and is particularly useful when a large message has to be digitally signed.[26]

Although it is possible to use asymmetric algorithms to encrypt information using the public key, and then decrypt it, using the corresponding private key, usually this process is very slow. Thus, often one opts for a procedure that combines two techniques described previously. Data is encrypted using a symmetric key randomly generated; then this key is encrypted by the public key of the message recipient. When the message recipient gets the message, the following process goes on: deciphering the symmetric key through its private key; and the use of the symmetric key to decrypt the data.[27]

The combined techniques of encryption are widely used. Some notable examples can be cited: SSH (Secure Shell), used to establish a secure communication between a client and a server; PGP (Pretty Good Privacy), used to exchange messages and, above all, SSL (Secure Sockets Layer) cryptographic protocol used by browsers and web servers to establish a safe communication channel for services such as email and browsing pages.[28]

3. Digital Signature

One of the services offered by public key cryptography is the digital signature. That is characterized for being analogous to hand written signatures made on paper, once a single entity can sign some data that are then capable of being read by several other entities which are able to verify its authenticity. This process is safer than conventional signatures given the capacity of today's computers, a fraud is not feasible.

According to Silva[29], digital signature is a value that can only be generated by the document issuer incorporated in the body of this and verified by the receiver through a specific process; in addition, it satisfies

23 BURNETT, S.; PAINE, S. *RSA Security's Official Guide to Cryptography*. Berkeley: Osborne/*McGraw-Hill*, 2002.
24 FEGHHI, J.; WILLIAMS, P. *Digital certificates:* applied internet security. New Jersey: Addison Wesley, 1999.
25 BURNETT, S.; PAINE, S. *RSA Security's Official Guide to Cryptography*. Berkeley: Osborne/*McGraw-Hill*, 2002.
26 ATREYA, M. et al. *Digital Signatures*. Berkeley: McGraw-Hill, 2002; CHOUDHURY, S.; BHATNAGAR, K.; HAQUE, W. *Public key infrastructure:* implementation and design. New York: M&T Books, 2002.
27 ADAMS, C.; LLOYD, S. *Understanding PKI:* concepts, standards, and deployment considerations. 2nd. New Jersey: Addison Wesley, 2003.
28 CHOUDHURY, S., BHATNAGAR, K., and HAQUE, W. Public key infrastructure: implementation and design. New York: M&T Books, 2002.
29 SILVA, L. S. da. *Public key infrastructure – PKI:* conheça a infraestrutura de chaves públicas e a certificação digital. São Paulo: Novatec, 2004.

all five criteria of the role of signatures (i) cannot be counterfeited, since only the sender knows his private key; (ii) is true because when the receiver verifies the signature with the public key of the issuer, he knows that only the latter was able to encode (sign) the document or message; (iii) is not reusable because it was generated based on a summary of the original message and cannot be transferred to other documents; (iv) is unchanged, since any change in the original will produce a different summary of the received one, so neither signature nor the document are more valid; and (v) cannot be rejected, since the receiver does not need emitter help to verify your signature.

When a message is signed, it is explicitly related to the single emitter. Moreover, a public key should be potentially available to all entities to verify its authenticity.[30]

Both digital signatures provide authentication of origin, and the resulting non-repudiation[31], as regarding the data integrity[32], they may also be used as a means of providing confidential to electronic information.[33]

Authentication services, or identification, establish the validity of a transmission, or of a message, and its origin. The goal is to enable the recipient of the message to determine its origin. The integrity services, in turn, deal with changes of accidental or unauthorized information, which includes insertion and subtraction of data. To ensure integrity, a system must be able to detect unauthorized changes. The purpose is to enable the recipient to verify if that information did not change. In turn, the services of non-repudiation prevent an individual refuse to perform certain actions previously made. Your task is to ensure to the message recipient the certainty of the identity of the issuer. Finally, the confidentiality services restrict access to sensitive information to only individuals' previously authorized.[34]

Authentication services, or identification, establish the validity of a transmission, or a message, and its origin. The goal is to enable the recipient of the message to determine its origin. The integrity services, in turn, deal with changes of accidental or unauthorized information, which includes insertion and subtraction of data. To ensure integrity, a system must be able to detect unauthorized changes. The purpose is to enable the recipient to verify if the information did not change. On the other hand, the services of non-repudiation prevent an individual to refuse to perform certain actions previously done. The purpose is to ensure to the message recipient the certainty of the issuer' identity. Finally, the confidentiality services restrict access to sensitive information only to previously authorized individuals.[35]

A digital signature can be generated using the private key of the issuer, encrypting the message in full or summary value; its result is attached to the original message and sent to addressee. In the case of encrypting the whole message, the digital signature, in this case, also provides to data confidentiality. To check the authenticity of the signature, the recipient decrypts the content with the public key of the sender and makes the comparison with the original message. If the signature is not validated, it is false or there may have been a change in the content of the original message. A digital signature can be checked as well the author, date and time, if a time stamp issued, as will be explained later.[36]

It should be noted that each piece of data has its own signature, that is, each signature is unique to the signed data and the keys used. If a person signs two different messages with the same key, signatures are different. Likewise, two persons with different keys sign the same message creating different signatures.[37]

30 ADAMS, C.; LLOYD, S. *Understanding PKI:* concepts, standards, and deployment considerations. 2nd. New Jersey: Addison Wesley, 2003.

31 BURNETT, S.; PAINE, S. *RSA Security's Official Guide to Cryptography*. Berkeley: Osborne/*McGraw-Hill*, 2002.

32 ADAMS, C.; LLOYD, S. *Understanding PKI:* concepts, standards, and deployment considerations. 2nd. New Jersey: Addison Wesley, 2003.

33 ATREYA, M. et al. *Digital Signatures*. Berkeley: McGraw-Hill, 2002.

34 ATREYA, M. et al. *Digital Signatures*. Berkeley: McGraw-Hill, 2002.

35 ATREYA, M. et al. *Digital Signatures*. Berkeley: McGraw-Hill, 2002.

36 CHOUDHURY, S.; BHATNAGAR, K.; HAQUE, W. *Public key infrastructure:* implementation and design. New York: M&T Books, 2002.

37 BURNETT, S.; PAINE, S. *RSA Security's Official Guide to Cryptography*. Berkeley: Osborne/*McGraw-Hill*, 2002.

4. Digital Certificate

Traditional certificates are designed to establish and document characteristics belonging to a specific individual, be it an identification number (i.e., social security number, driver's license number), a level of achievement (i.e., college degree, license to practice a profession), or membership status (i.e., company ID, trade union card). The digital certificate extends this concept into the electronic world, identifying and linking the certificate holder to a public encryption key that is subsequently used as a means of identification.[38]

As noted earlier, one of the fundamental principles of asymmetric cryptography is the possibility to freely distribute the public key to the entities that make use of security services. However, this provision should be associated to protect its integrity, preventing undue alterations. In addition, mechanisms to ensure its integrity are not sufficient to establish a relationship between a public key to a particular entity.[39]

Digital certificates are a vital component in the PKI infrastructure (shown further) as they act as digital passports by binding the user's digital signature to their public key.[40]

Only the user holds their private key. The user's computer generates the public and private key pair. The public key is then sent to the Certificate Authority (CA) where it is verified and a digital certificate is issued. This certificate is then sent back to the user and stored. Copies of this certificate can then accompany transactions from which the certified public key is available. The fact that a cryptographically weak password is a security issue that needs careful consideration.[41]

Digital certificates support the asymmetric encryption, because they contain the public key of the entity identified in the certificate, correlating it to a particular individual.

Digital certificate is a set of tamper-proof data that certifies the association of a cryptographic key pair to a final user. To provide this association, a set of trusted third parties confirms their identity. Such third party, called certificate authorities, issue certificates for the user with his name, his public key and other identifying information. After being digitally signed by the respective Certification Authority, the certificates can be transferred and stored.[42]

Digital certification is a process of recognition of an electronic media activity characterized by establishing a unique relationship, transferable license of a cryptography key to an individual, business, or machine application. This recognition is inserted into a digital certificate by a Certification Authority.[43]

A digital certificate is characterized by having a life cycle that begins with a request and ends within an expired data or its repeal. In addition, it follows a hierarchy. The certificate is issued and signed by a Certification Authority occupying higher position.

The most common type of digital certificate is X.509, a specification for the binary file format.[44] The International Telecommunication Union was responsible for the specification of this standard in 1988 and its format became known as version 1.[45] Later in 1993, version 2 was released, with the incorporation of two

38 GERDES, J. H.; KALVENES, J.; HUANG, C. 'Multi-dimensional credentialing using veiled certificates: Protecting privacy in the face of regulatory reporting requirements'. *Computers & Security*, v. 28, n. 5, p. 248-259, 2009.

39 ADAMS, C.; LLOYD, S. *Understanding PKI:* concepts, standards, and deployment considerations. 2nd. New Jersey: Addison Wesley, 2003.

40 HUNT, R. 'Technological infrastructure for PKI and digital certification'. *Computer Communications*, v. 24, n. 14, p. 1460-1471, 2001.

41 LI, H.; WU, C. 'Study on the application of digital certificates in the protection of network information security and data integrity'. *Journal of Networks*, v. 8, n. 11, p. 2592-2598, 2013.

42 BURNETT, S.; PAINE, S. *RSA Security's Official Guide to Cryptography*. Berkeley: Osborne/*McGraw-Hill*, 2002.

43 INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. *Glossário ICP - Brasil. Versão 1.2*. Brasília: ICP, 2007.

44 HARN, L.; REN, J. 'Generalized digital certificate for user authentication and key establishment for secure communications'. *IEEE Transactions on Wireless Communications*, v. 10, n. 7, p. 2372-2379, 2011.

45 ORTEGA, M.; SÁNCHEZ, S. 'University authentication system based on java card and digital X.509 certificate'. *International*

unique ID fields. In 1997, version 3 was released with the addition of an extension field.[46]

Digital certificates are structured with standardized information in the following format according the standard X.509[47]: (i) *Version* differentiates the successive versions of the script (1, 2 or 3, currently); (ii) S*erial Number* contains a unique identification number of each certificate, generated by the Certification Authority; (iii) *Algorithm Identification Signature* has a code indicating the algorithm used to sign the certificate; (iv) N*ame of the issuer* identifies the Certificate Authority that signed the certificate; (v*) Validity* tells the definition of the certificate validity period, with date and time; (vi) S*ubject name* identifies the final entity to which the certificate relates; (vii) *Information on the subject's public key*, as the value of the public key of the certificate holder and the algorithm identifier; (viii) *Emitter unique identifier* contains a unique identifier; and (ix) *Extensions* with additional information.

5. Public Key Infrastructure - PKI

Public key cryptography was conceived in 1976 by Diffie and Hellman.[48] Later, Rivest *et al* designed the RSA Cryptosystem, the first public key system.[49] Each public key cryptosystem has its own technical features, however they all share the property that given an encryption key it is computationally infeasible to determine the decryption key and vice versa.

The principle objectives of developing a PKI is to enable secure, conventional, and efficient acquistion of public keys. A PKI enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.[50]

According to Hunt[51], PKI is a system for publishing the public keys used in public key cryptography. PKI provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the three principal security functions: integrity, authentication and non-repudiation.

A PKI is a combination of hardware and software products, policies and procedures. It provides the basic security required to carry out e-business so that users who do not know each other or are widely distributed can communicate securely through a chain of trust. A PKI consists of: (i) Security Policy; (ii) Certificate Authority (CA); (iii) Registration Authority (RA); (iv) Certificate Repository and Distribution System; and (v) PKI-enabled Applications.

Registration authorities generally have the following functions (described some of the described functions do not apply to Brazilian model, as will be explained in the next section)[52]: (i) Accept and verify the registration information on new registrars; (ii) Generate keys in favor of end users; (iii) Accept and authorize requests to a backup and a key recovery; (iv) Accept and authorize requests for certificate revocation; and

Journal of Computer Science Issues, v. 9, n. 4, p. 23-29, 2012.

46 TOMA, C. 'Security issues of the digital certificates within public key infrastructures'. *Informatica Economică*, v. 13, n. 1, p. 16-28, 2009.

47 MING, Z. 'Secure digital certificate design based on the public key cryptography algorithm'. *Telkomnika*, v. 11, n. 12, p. 7366-7372, 2013.

48 DIFFIE, W.; HELLMAN, M. E. 'New directions in cryptography'. *IEEE Transactions on Information Theory*, v. 22, n. 6, p. 644-654, 1976.

49 RIVEST, R.; SHAMIR, A.; ADLEMAN, L. 'A method for obtaining digital signatures and public key cryptosystems'. *Communications of the ACM*, v. 21, n. 2, p. 120-126, 1978.

50 SHARMA, A.; GOYAT, N.; SAROHA, V. 'Public-Key Infrastructure (PKI)'. *International Journal of Advanced Research in Computer Engineering & Technology*, v. 2, n. 7, p. 2307-2310, 2013.

51 HUNT, R. 'Technological infrastructure for PKI and digital certification'. *Computer Communications*, v. 24, n. 14, p. 1460-1471, 2001.

52 BURNETT, S.; PAINE, S. *RSA Security's Official Guide to Cryptography*. Berkeley: Osborne/*McGraw-Hill*, 2002.

(v) Deploying or retrieving hardware devices.

The weakest link within the PKI framework is the storage and security of the private key which, if exposed, allows other parties to both decrypt messages and to transmit fraudulently signed messages; and if lost, prevents the original owner from de-coding incoming messages and historic signed materials. A solution is therefore needed to prevent keys from functioning for anyone but the valid owner, even if they are lost or stolen.[53]

The Brazilian Infrastructure for Public Key - ICP was created in 2001 and defines itself as a set of techniques, architecture, organization, practices and procedures carried out by the Brazilian government and private organizations that support together the implementation and the operation of a certification system. Aims to establish the technical foundations and methodologies for a digital certification system based on public key cryptography, to ensure authenticity, integrity and legal validity of documents in electronic form of the support applications and of the enabled applications using digital certificates, as well as conducting secure electronic transactions[54].

The National Institute of Information Technology - ITI, federal agency under the Civil House of the Presidency is the Certificate Authority Root of ICP, that is, the first authorization of the certificate chain, executor of Certificate Policy and technical and operational standards approved by the Administrative Committee of ICP. The certification authorities, registration authorities and support service providers make up the hierarchy of the ICP. The ITI certificate is self-signed and can be checked through specific mechanisms and procedures, without ties with this.

There is a chain of certification authorities, that is, an existing hierarchical interconnection between the different participating entities of ICP. Currently, there are eight first-level certification authorities: Federal Savings Bank; VeriSign; Official Press of the State of São Paulo; Judiciary; Presidency of the Republic; Serasa; Serpro and IRS. Digital certificates also follow a hierarchical series of certificates signed by successive certificate authorities.

The Administrative Committee of ICP is the managing authority policies and responsible, among other thing for establishing policy and certification standards and monitor the activities of Root Certification Authority.

It is to the ITI to launch, forward, distribute, and revoke and manage the certificates of certification authorities to immediately subsequent level; manage the list of certificates issued, withdraw it and the do and perform activities of inspection and audit of certification authorities, registration authorities and support service providers enabled in ICP, in accordance with the guidelines and technical standards established by Administrative Committee of ICP and perform other duties as assigned by the management authority policies.

Certifying Authority is the entity subject to the hierarchy of the ICP responsible for issuing, distributing, renew, revoke and manage digital certificates. It does the lists of repealed certificates - LRC and keeps the records of its operations, always obeying the practice defined in the Declaration Certification Practice - DPC. Its plays an essential role exercising the responsibility to verify that the certificate holder has the private key corresponding to the public key that is part of the certificate. Creates and digitally signs the certificate of the subscriber, where the certificate issued by the Certification Authority is the statement of the identity of the holder, which has a single pair of keys (public / private). In the hierarchy of public certification services, the certification authorities are subject to the higher hierarchical level entity.

Registration Authority is responsible for the interface between the user and their Authority Certification,

53 BROMBY, M. 'Identification, trust and privacy: How biometrics can aid certification of digital signatures'. *International Review of Law, Computers & Technology*, v. 24, n. 1, p. 133-141, 2010.

54 INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. *Glossário ICP - Brasil. Versão 1.2*. Brasília: ICP, 2007.

which keeps hierarchical bonds. Aims to receipt, to do to the validation, the routing issuing requests or revocation of digital certificates to certifications and the identification authorities, in person, of their applicants. It is its responsibility to keep records of their operations. Can be physically located in a certification authority or be a remote registry entity.

The Time Stamp Authority - ACT is the entity in which the user timestamp services (ie, subscribers and third parties) trust to issue timestamps. The Entity of Time Audit - EAT performs authentication activity and timing Time Stamp Servers - SCT, installed in the ACT. In the structure of time stamp of the ICP, the EAT is the National Observatory.

6. Current Applications of digital certification in Brazil

Broadly, digital certification provides the following requirements relating to security-information, described in the previous section: confidentiality; authenticity and data integrity. These features may be present alone or together in a number of possible applications, as shown in sequence.

e-CPF is an electronic version of CPF - Registration of Individuals. In addition to identifying with security-individuals, the e-CPF ensures reliability, privacy, integrity and inviolability of messages and various types of transactions via the Internet. Besides, the digital certification has legal validity for use as hand written signatures, indicating that their owner agrees with the signed document.

As of July 2008, the micro and small businesses, opting or not for the tax National Simple regime, can use digital certification in order to reduce bureaucracy and simplify processes procedures, as well to reducing costs in the medium term. The e-CPF Simple variation of e-CPF, is exclusively responsible for the micro holder and small business. It consists of a certification valid for one year, issued in specific cryptographic hardware. It allows quick access to the National Simple Portal for issuing the Simple Collection Document - DAS, only with the inclusion of private password of digital certification.

The e-CNPJ functions as a digital version of CNPJ - National Register of Legal Entities. It also ensures the authenticity and integrity in communication companies. There are two types of e-CNPJ, A3 and A1. The e-CNPJ type A3 offers greater security, since its certificate is generated, stored and processed in the smart card or token, which remains inviolable and unique. Only the holder of the password, created at the time of validation, can use the private key. This digital certificate is valid for three years. The e-CNPJ type A1 is generated and stored in the user's computer, the use of smart cards or tokens is unnecessary. The data can be protected by a password created by the user. Only with this password it can be accessed, moved and copied the private key. The validity of this certificate is 1 year, counted from their date of issue.

The e-CAC stands for Virtual Taxpayer Service Center, is a typical example of application of a digital certification to electronic government. In this area, are available all the services of the Federal Revenue of Brazil and the National Treasury Attorney that can be made through the Internet.

The Federal Revenue of Brazil adopted the digital certificate for the services protected by tax secrecy which allow tax payers to be served through its website, ensuring privacy and inviolability.

With this guarantee, the taxpayer and businesses can have access to the following services: (i) Delivery declarations of personal income tax and corporate; (ii) Recovery of historical statements and copies of payments; (iii) Correction of payments made, as well as installment of trading; (iv) Consultation and regularization of taxpayer situation -individuals and companies with e-CPF legal guardian; (v) Transactions on the Integrated Foreign Trade System - Siscomex; (vi) Electronic Installment online of individual and corporate debts; (vii) Electronic Scheduling of individuals and companies treatment by the CCC counter to resolve disputes.

The Public Digital Bookkeeping System (SPED) was established in 2007 and is in a further step in the computerization of the relationship between tax authorities and taxpayers. In general, it promote the modernization of the systematic compliance with the accessory obligations, transmitted by taxpayers to the tax administrations and regulatory agencies, using digital certification for signing electronic documents. This system is the instrument that unifies the activities of receipt, validation, storage and authentication of books and documents that comprise the commercial and fiscal bookkeeping of entrepreneurs and business companies, through a single, computerized flow of information.

The SPED consists of three major subprojects: Digital Bookkeeping, Digital Tax Bookkeeping and Electronic Invoice - National Environment. In practice, is an integrated initiative of the tax administrations in the three spheres of government, federal, state and city level (municipal). This systematic allows the effective participation of taxpayers in the definition of service means the accessory tax obligations required by law to contribute to enhance these mechanisms and check to these instruments greater social legitimacy, establishing a new type of relation, based on mutual transparency, with positive effects for the whole society.

The Electronic Invoice (NF-e) can be regarded as an only digital existence document issued and stored electronically in order to document for tax purposes, an operation of movement or the provision of services that occurred between the parties. Its legal validity is guaranteed by the digital signature of the sender (guarantee of authorship and integrity) and the receipt by the tax authorities of the electronic document before the triggering event.

In simple terms, the issuing company NF generates an electronic file containing the tax information of commercial operation, which must be digitally signed in order to ensure data integrity and the issuer's ownership. This electronic file corresponding to the NF-e, will then be transmitted over the Internet to the office of the taxpayer's jurisdiction farm that will make a file pre-validation and return it to a receipt protocol (use permit), without it cannot have the transit of the cargo. The NF-e will also be transmitted to the IRS, which will be national repository of all NF-e issued (National Environment) and in the case of interstate operation for the operation from the State Farm secretarial and Superintendent Zone Franca de Manaus (Suframa) in case of goods destined for areas encouraged. The financial departments and the IRS (National Environment), make available consultation through the Internet to the recipient and other stakeholders legitimate, holding the access key of the electronic document.

The adoption of NF-e brings a number of benefits to all involved in a business transaction, among which are: reducing printing costs and purchase of paper (reduction of paper consumption, with positive impact on the environment) ; reduction of dispatch of the tax document costs; reducing storage costs of tax documents; reducing truck stop time in Border Tax Offices; elimination of typing invoices on receipt of goods; delivery logistics planning for early receipt of information of NF-*e*; reduction of bookkeeping errors in typing invoices; encouraging e-commerce and the use of new technologies; improvement in the process of fiscal control, enabling a better exchange and share of information between tax authorities; cost reduction in the control process of the captured invoices for supervision of goods in transit; reduction of tax evasion and increased tax collection.

National Simple (FPEM) is the system of applications developed for the representatives of the farm and finance secretaries of the States and Municipalities Participation Fund of the States and MUNICIPALITES (FPEM) to access the National Simple database. The representative of the State or the Municipality at to the fund called "representative in FPEM" is the "master user". From the representative "users-certifiers" are accredited who may allow other "users". Thus, creating a systemic chain of accreditation at the National Simple database.

According to the Steering Committee of the National Simple, representatives of states and municipalities throughout Brazil must have personal digital certificate (e-CPF type A1 or A3), to access the taxpayers database of the National Simple.

The justification for the access to this database has to be done by digital certification is the need to ensure the security of information electronically transmitted by the Internet is to ensure the protection taxpayers secrecy.

Starting on April 2002, financial institutions have been conducting secure transactions with the implementation of the Brazilian Payment System (SPB). Which is responsible for managing the process of clearing and settling payments electronically, linking financial certified institutions by the Central Bank of Brazil. Electronic message for fund transferring, transiting exclusively through the National Financial System Network - RSFN, are standardized and observe specific safety procedures (digital certificates of ICP) to authenticate and verify the identity of participants in all the operations performed.

The Criminal Court of Appeals of the State of São Paulo - TACrim held in August 2007, through its 11th Chamber of Trials, the first digital trial session, in which the physical processes have been replaced by digital files with digital signature. Armed with a laptop computer, judges brought their votes already scanned for the session, containing all the information necessary for the trials of processes. In the future, the intention is to make the TACrim fully computerized, with petitions and other documents in the file, at both first and second instances, transformed into digital files and accessible through any computer via the logical network to be implemented in the Court. This system reduces the bureaucracy, when significantly reducing the processing of cases before the Court meeting, eliminating the use of paper during the sessions, reducing costs and shortening the time length of the trials.

The project e-Jus proposes is linking computers at meetings rooms and allow for online reporting of all legal procedures during a trial, streamlining the work of the sessions, providing resources to the judges in the preparation, monitoring and trial judgments. In the e-Jus, the judgments of proposals are stored in the system in judgment format. After the trial of a case, the judge and the prosecutor can connect to computer their digital identity card, enter the password and register their signature electronically during the judgment session. This operation eliminates the need to manually sign the document, and at the same time eliminates any judgment step of drafting. At the session on cable, digitally judgments signed go directly to the publication stage.

The cases whose judgments are digitally signed are retained in the office of the class and do not come back to the office. The judgment is printed by the Registry and joined by the Court. Soon after made the gathered, the process is referred to the publication stage. The digitally signed judgments are, then, available for consultation on the Internet two days after the session. The release of trial certificates by the secretariat, however, follows the traditional rite.

In order to further streamline at the adjudication and create easy access, save time and cost to jurisdictional, the Labor Court offers the Integrated Filing and Flow Electronic Documents of the Labor Court (e-DOC). The system allows the electro-single shipping documents relating to proceedings before the Labor Courts, regional labor courts and the Superior Labor Court, via the Internet, without the need for subsequent submission of original documents. *e*-DOC is scheduled for physical personal use of digital certificate, refusing access to a legal entity.

On May 24, 2007, it was launched the Electronic Petitioning Service (e-PET) by the Superior Court of Justice - STJ. The system is optional, but its use expedites adjudication and facilitates access to the court. After sending, the system generates a report that can be printed by the user, with date and time of transmission, lawyer's name, party and identification of files transmitted. To use e-PET, the professional must have the digital certificate, be accredited in the Supreme Court of the system and have the necessary software and hardware on his computer. The new system allows electronic submission of initial and incidental petitions, and its progress can be followed online by accredited user without the need for petitions written on paper.

The Electronic Management System of Private Security (GESP) was developed to speed the request, with the use of digital certification, operating authorization procedures, review and acquisition of weapons,

ammunition and fitting equipment of private security companies to the Department of Federal police. To use the service, each company must have a digital certificate e-CNPJ type A1 or A3 issued by a certificate authority linked to ICP, which can be used by both the matrix and by its subsidiaries. In this way, companies at the time of transmission of any process will have to sign it using their digital certificate. Thus, there is a guarantee that all information submitted will be accessible only by the Federal Police. On the other hand, the Federal Police will be assured that the information submitted is really coming from that company, including legal validity. Furthermore, GESP provides operational advantages such as reduced process time, on-line monitoring of the procedure and standardized procedures.

The Official Press of the State was established as Certificate Authority Official at the São Paulo State, having as the preferred Registration Authority the Nossa Caixa Bank. This partnership provides technical confidence, legal and operational required under the ICP for the promotion of e-government in the state. Every day, the contents of the Official Press Gazette of the State of São Paulo is published in full at the Internet for those with digital certification, including the Executive notebooks, Legislative, Judiciary, Business, Trade Board and the Official Gazette of the City of São Paulo. In the case of the Official Gazette - DOU, digital certification is used in processing and electronic signature of official documents, by Ministers and the President of the Republic, for publication in the Official Gazette. In addition, the website of the National Press, which brings the Gazette and the Journal of Justice, is also certified, enabling users to verify the authenticity of information published in the electronic version of the Official Gazette. These certified digital publications facilitate access to information and guarantee the authenticity of the documents consulted. Through the digital certificate, the user has the option to use the digital signature, allowing the exchange of documents, authentication, confidentiality and integrity of content. The documents that travel electronically, to have legal recognition, no longer need to be converted to paper and signed. Moreover, this service provides the elimination of the physical distance, prevents fraud, and enables a greater number of electronic services to be carried out with absolute certainty.

The Program University for All (PROUNI) is a program created by the federal government in January 2005. It aims to give full and partial scholarships to low-income students in undergraduate and specific sequential training in private higher education institutions, offering in return, exemption from certain taxes to those institutions that adhere to the program. Access to PROUNI System - SISPROUNI is held today, exclusively with the use of digital certificates issued under the ICP. Therefore, should be use educational institutions certificates (legal entity certificate of type A1 or A3 ICP) and PROUNI Coordinators and their representatives (individual certificate of type A1 or A3 ICP).

In addition to ensuring security to the information registered in SISPROUNI, the use of digital certification enables the digital signature record in all documents issued, which eliminates sending these by post, and the notarization of the signatories ensuring its legal validity.

Social Connectivity is an example of an electronic channel relationship between the Caixa Economica Federal - CEF, an agent operator agent of the Service Time Guarantee Fund - FGTS, and the business and accounting firms. Social Connectivity allows the transmission of the Enterprise System of FGTS Collection and the Social Security Information – SEFIP, which requires the digital certification that the business company uses it. The accounting firms that perform gatherings and provide information to the FGTS and the National Institute of Social Security (INSS) on behalf of its customers can also use the Social Connectivity for this purpose. All is needed is that the client generates at the Internet, an electronic power of attorney. If case one must exchange his counter, just have to withdraw the previous electronic proxy and checked it to the new counter, all over the internet and without complications. This channel allows to simplify the gathering of FGTS process, with greater flexibility and convenience; reducing operational costs; increasing the security of transactions, reducing the occurrence of inconsistencies and the need for future adjustments and improving the protection of business against irregularities.

In 2002, was established in Brazil a new type of bidding called trading, seeking to increase competitive-

ness and agility in public procurement, with transparency to society, less bureaucratic procedures and cost reduction. Later, in 2005, became mandatory the use of electronic trading for the purchase of common goods and services, except in cases of proven impossibility to be justified by the competent authority. It is currently the main type of contract performed by the Federal Government. The criers and expense of officers, participants of the operation system, must necessarily make use of digital certificate type A3. The application of this tool has a number of advantages such as increased efficiency, via automation of administrative systems and processes, and assurance of safety to acts performed. In addition, it supports the market, generating competition among suppliers, allowing even the participation of medium and small companies in tenders promoted by the government, doing to the fact of prescient the physical presence of their representatives as established previously in the way of traditional contracting.

The Environmental Sanitation Technology Company of the State Secretariat of Environment of the State of São Paulo - CETESB started to adopt Simplified Licensing System (SILIS), based on digital certification, where low potential developments polluter can by Internet, get their environmental license through a simplified procedure, such as Preliminary License; Installation License and Operating License in on single document. In addition, the SILIS can also be used for the renewal of the Operating License. All actions involved in this procedure are triggered without user need to attend the Environmental Agencies CETESB, providing greater comfort.

The National Institute of Industrial Property - INPI is pursuing a process of computerization to achieve a "paperless INPI." Thus, is was launched the Electronic System for Management of Industrial Property (*e*-INPI), an electronic system for service request, for example for, trademark applications over the Internet, through an electronic form with digital certification. With this mechanism, the INPI aims to reduce the deadline for grant of brands by 80%. This system, in addition to streamline processes and provide greater security for transactions, make it easier for users, without the need for physical presence and greater convenience; provides reduction of costs, economy of paper, and significantly decrease of mistakes in the filling out of paper forms.

In 2004, the Superintendence of Private Insurance - SUSEP regulated digital signatures in electronic documents relating to insurance operations, capitalization and complementary pension. The objective was to standardize and especially signal to the market that there is a modern and effective tool on use. The electronic policy replaces the documents that are sent annually to policyholders and brokers for each closed contract, so there is no need to collect and guard roles for periods ranging from 5 to 20 years. Electronic proceeding with digital certification, promote the rationalization and streamlining of processes, using a secure technology that prevents problems such as fakes and misplacement of documents. In addition, this system provides added convenience to the user and reduction of costs for the broker and the insurer, with consequent environmental preservation.

The Financier of Studies and Projects - FINEP is adopting digital certificates of ICP in a new project called Zero Interest, that is to stimulate the innovative capacity of micro and small Brazilian companies in the commercial aspects, processes, products or services. One of the main features of this project is that most of the negotiations are done by digital means, for example, the submission of proposals that goes through a form available on the site FINEP, and the signing of contracts, providing a drastic reduction of bureaucracy. Applying companies must prove that they have a computerized system able to handle digital certification and electronic signatures following all the standards of ICP.

The Per Diem and Air Fare Tickets Concession System (SCDP) is a computerized system, accessed via the Web, which includes the concession activities, registration, monitoring, management and control of daily flights resulting from trips taken in the interests of the administration in the country or abroad, by public servants of the Federal Government. It is currently in operation in 36 units on ministries, municipalities, foundations and agencies, summing up about 100 institutional users throughout the country. Since 2004, when it was deployed, the SCDP promotes electronic processing of documents using digital certificates of

type A3. By December 31, 2008, its membership became mandatory. Because the SCDP enable requests made at the Internet, there is a reduction of the time of ticketing and improvement in service conditions and consultation of users.

7. Conclusion

At the moment of the current transition towards the Knowledge Society, governments and business companies efforts to adapt to a new paradigm resulting from the globalization of markets and the recent technological revolution, which results in instability and insecurity environment. In this context, ICT present interesting solutions for both the public sector and the private sector.

For the public sector, ICT provides a new interaction interface with society, creating possibilities for a more effective participation in political processes and the provision of better quality public services such as greater transparency and efficiency to the state apparatus.

For the private sector, ICT provides a significant reduction of costs by decreasing bureaucratic processes, bringing efficiency gains and agility to business and greater convenience to its customers.

All the long list of possible applications of ICT opens up a large amount of opportunities, but also imposes obstacles with regard to the need for protection of electronic information.

In this context, digital certification is an alternative, with respect to the security of information, referring to its main applications, authenticity, confidentiality and data integrity and additionally legal validity of electronic documents. It's either that, in practice, as it turns out a great spread of this technology in Brazil and there are excellent prospects for the use in other areas of public and private sector. The continuity of this spread will result, in an information security platform that will be the basis for the safe development of electronic commerce and government, supported in the strengthening of the level of confidence of its members.

References

ADAMS, C.; LLOYD, S. *Understanding PKI:* concepts, standards, and deployment considerations. 2nd. New Jersey: Addison Wesley, 2003.

ATREYA, M. et al. *Digital Signatures*. Berkeley: McGraw-Hill, 2002.

BELDAD, A.; JONG, M.; STEEHOUDER, M. 'I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions'. *Computers in Human Behavior*, v. 27, n. 6, p. 2233-2242, 2011.

BRAZILIAN ASSOCIATION OF TECHNICAL STANDARDS. *NBR ISO/IEC 17799:* código de prática para a gestão da segurança da informação. 2nd. Rio de Janeiro: ABNT, 2005.

BROMBY, M. 'Identification, trust and privacy: How biometrics can aid certification of digital signatures'. *International Review of Law, Computers & Technology*, v. 24, n. 1, p. 133-141, 2010.

BURNETT, S.; PAINE, S. *RSA Security's Official Guide to Cryptography*. Berkeley: Osborne/*McGraw-Hill*, 2002.

CHOUDHURY, S.; BHATNAGAR, K.; HAQUE, W. *Public key infrastructure:* implementation and design. New York: M&T Books, 2002.

DIFFIE, W.; HELLMAN, M. E. 'New directions in cryptography'. *IEEE Transactions on Information Theory*,

v. 22, n. 6, p. 644-654, 1976.

FEGHHI, J.; WILLIAMS, P. *Digital certificates:* applied internet security. New Jersey: Addison Wesley, 1999.

GERDES, J. H.; KALVENES, J.; HUANG, C. 'Multi-dimensional credentialing using veiled certificates: Protecting privacy in the face of regulatory reporting requirements'. *Computers & Security*, v. 28, n. 5, p. 248-259, 2009.

HARN, L.; REN, J. 'Generalized digital certificate for user authentication and key establishment for secure communications'. *IEEE Transactions on Wireless Communications*, v. 10, n. 7, p. 2372-2379, 2011.

HUNT, R. 'Technological infrastructure for PKI and digital certification'. *Computer Communications*, v. 24, n. 14, p. 1460-1471, 2001.

INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. *Glossário ICP - Brasil. Versão 1.2*. Brasília: ICP, 2007.

INTERNATIONAL DATA CORPORATION. *The Digital Universe in 2020:* Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East. IDC White Paper. Framingham: IDC, 2012.

KAHN, D. *The codebreakers:* the comprehensive history of secret communication from ancient times to the internet. New York: Scribner, 1996.

LAIH, C.; JEN, S.; LU, C. 'Long-term confidentiality of PKI'. *Communications of the ACM*, v. 55, n. 1, p. 91-95, 2012.

LI, H.; WU, C. 'Study on the application of digital certificates in the protection of network information security and data integrity'. *Journal of Networks*, v. 8, n. 11, p. 2592-2598, 2013.

MING, Z. 'Secure digital certificate design based on the public key cryptography algorithm'. *Telkomnika*, v. 11, n. 12, p. 7366-7372, 2013.

ORTEGA, M.; SÁNCHEZ, S. 'University authentication system based on java card and digital X.509 certificate'. *International Journal of Computer Science Issues*, v. 9, n. 4, p. 23-29, 2012.

RIVEST, R.; SHAMIR, A.; ADLEMAN, L. 'A method for obtaining digital signatures and public key cryptosystems'. *Communications of the ACM*, v. 21, n. 2, p. 120-126, 1978.

SHARMA, A.; GOYAT, N.; SAROHA, V. 'Public-Key Infrastructure (PKI)'. *International Journal of Advanced Research in Computer Engineering & Technology*, v. 2, n. 7, p. 2307-2310, 2013.

SILVA, L. S. da. *Public key infrastructure – PKI:* conheça a infraestrutura de chaves públicas e a certificação digital. São Paulo: Novatec, 2004.

SINGH, S. *The code book:* the science of secrecy from ancient Egypt to quantum cryptography. New York: Anchor Books, 1999.

STALLINGS, W. *Data and computer communications.* 8th New Jersey: Pearson Prentice Hall, 2007.

TOMA, C. 'Security issues of the digital certificates within public key infrastructures'. *Informatica Economică*, v. 13, n. 1, p. 16-28, 2009.

ZHANG, J.; HU, N.; RAJA, M. K. 'Digital certificate management: Optimal pricing and CRL releasing strategies'. *Decision Support Systems*, v. 58, n. 1, p. 74-78, 2014.

Para publicar na revista Brasileira de Políticas Públicas, acesse o endereço eletrônico www.rbpp.uniceub.br
Observe as normas de publicação, para facilitar e agilizar o trabalho de edição.