COMPARAÇÃO ENTRE OS PRODUTOS E SERVIÇOS OFERECIDOS PELAS AUTORIDADES CERTIFICADORAS

COMPARISON AMONG PRODUCTS AND SERVICES PROVIDED BY CAS

Wagner Junqueira de Araújo[1]
Yasmin Brito de Lemos Vieira[2]

RESUMO
Com a utilização dos documentos em formato digital, foi necessário desenvolver tecnologias que garantissem a autenticação e o sigilo destes. Uma das tecnologias que habilitam tais características nos documentos digitais é a certificação digital que, por sua vez, é oferecida pelas autoridades certificadoras (ACs). Esta comunicação descreve resultado de pesquisa que teve como objetivo identificar e comparar os produtos e serviços oferecidos por diferentes autoridades certificadoras distribuídas pelo mundo. Descreve as estruturas das Autoridades Certificadoras (ACs) e seu papel no processo de certificação digital, como a responsável pela emissão dos certificados e as Autoridades de Registro que verificam a autenticidade das informações contidas no certificado. Apresenta os tipos de ACs e quais as principais Autoridades Certificadoras do Brasil, credenciadas pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Trata-se de uma pesquisa qualitativa, que utilizou a análise documental como método para coleta e análise de conteúdo para tabulação e análise. A amostra foi composta por quarenta e quatro ACs, distribuídas em doze países. Como resultado, são apresentados dois quadros, que indicam os produtos de certificação digital prestados pelas ACs no Brasil e pelas internacionais. Faz uma descrição dos produtos e serviços por elas oferecidos, e o detalhamento e a aplicação de cada um. Verificou-se que os produtos e serviços oferecidos são similares entre as ACs mundo a fora e no Brasil, as diferenças estão nos certificados emitidos para finalidades específicas, como os que foram criados para atender serviços como o e-CPF, e-CNPJ, Conectividade Social, etc.

PALAVRAS-CHAVE: Gestão da segurança da informação. Autoridade certificadora. Certificado digital. Serviços de certificação digital.

ABSTRACT
With the use of digital documents, it was necessary to develop technologies that would guarantee the authentication and the confidentiality of these. One technology that enables such features in digital documents are the digital certification that, in turn, offered by certification authorities (CAs). This paper describes results of research that aimed to identify and compare the products and services offered by different certificate authorities distributed around the world. Describes the structures of Certification Authorities (CAs) and its role in digital certification process, as responsible for the issuance of licenses and registration authorities that verify the authenticity of the information contained in the certificate. Presents the types of CAs and what are the mains Certification Authorities in Brazil, accredited by the Brazilian Public Key Infrastructure (PKI-Brazil). A qualitative study used the document analysis as a method for collection and content analysis for tabulation and analysis. The sample consisted of forty-four ACs, distributed in twelve countries. As a result, there are two tables, which show the digital certification of products provided by CAs in Brazil and international. Makes a description of products and services offered by them, and the detailing and the application of each. Was verified that the products and services offered are similar among CAs outside and inside, the differences are the certificates issued for specific purposes, such as those created in Brazil to attend services with e-CPF, e-CNPJ, Social Connectivity, etc.

Keywords: Security Information Management. Certification Authority. Digital certificate. Digital certification services.

[1] Professor do Programa de Pós-graduação em Ciência da Informação - PPGCI-UFPB. Professor Adjunto - III do Departamento de Ciência da Informação da Universidade Federal da Paraíba - UFPB. E-mail: wagnerjunqueira.araujo@gmail.com
[2] Graduanda em arquivologia. E-mail: yasminblemos@gmail.com
Recebido em: 20/11/2014 - **Aceito em:** 19/04/2015

1. INTRODUÇÃO

Com a atualização da tecnologia da informação e com o surgimento da *Internet* passamos a receber e produzir informações com agilidade, rapidez e eficácia. Podemos efetuar compras *on-line* de forma segura, acessar contas e fazer transações bancárias sem sair de casa, dentre outros serviços.

Pensando nisso, a substituição do documento físico (papel) pelo documento digital tem sido cada vez mais recorrente em empresas privadas e/ou públicas. Segundo o Dicionário Brasileiro de Terminologia Arquivística (2005, p. 75), "documento eletrônico é um gênero documental formado por documentos que são acessíveis apenas por meio de equipamentos eletrônicos". Já os documentos digitais "são unidades de registro de informações codificados em dígitos binários e acessíveis somente por um sistema computacional". (ARQUIVO NACIONAL, 2005, p. 75).

De acordo com Corrêa e Dorneles (2013, p. 4):

> A aplicação da certificação digital sobre informações registradas em suportes digitais visam garantir a autenticidade, confidencialidade e integridade das mesmas diante de sua reconhecida instabilidade. Para tanto, é necessário o estabelecimento de políticas públicas, diretrizes, programas e projetos específicos, legislação, metodologias, normas, padrões e protocolos que minimizem os efeitos da fragilidade e da obsolescência de *hardware*, *software* e formatos e que assegurem, ao longo do tempo, a autenticidade, a confidencialidade, a integridade, o acesso contínuo e o uso pleno da informação certificada digitalmente a todos os segmentos da sociedade.

A certificação digital usa a tecnologia assimétrica de chave pública e particular que permite cifrar e decifrar documentos, além de possibilitar a assinatura e validação destas através dos pares de chaves gerados pela Autoridade Certificadora. (ARAÚJO; VIEIRA, 2012, p. 294).

> Um certificado de chave pública, normalmente denominado certificado, é uma declaração assinada digitalmente que estabelece uma ligação do valor de uma chave pública com a identidade da pessoa, o dispositivo ou o serviço que contém a chave particular correspondente. (MICROSOFT, [200?]).

Os certificados digitais são arquivos digitais formados por um conjunto de dados de identificação de um indivíduo ou entidade. Eles estão destinados a interligar, de forma única e segura, a relação entre a chave privada (ou particular) e a chave pública do indivíduo ou entidade. A estrutura e o modo de operação das autoridades certificados e dos certificados digitais são reguladas pelas determinações técnicas do *Internet Engineering Task Force (IETF)* conforme o padrão X509v3 sendo sua última atualização descrita na RFC 6818 (*Request for Comments*). (IETF, 2013).

O objetivo deste trabalho foi identificar e comparar os catálogos de produtos e serviços oferecidos por diferentes autoridades certificadoras distribuídas pelo mundo. Cabe ao profissional da informação, especialmente aos arquivistas, entender e dominar os

procedimentos, ferramentas e atores envolvidos no processo de certificação digital, pois a validade, integridade, autenticidade, não repúdio e preservação dos documentos digitais estão relacionados diretamente com tais tecnologias e atividades intimamente ligadas a este tipo de profissional. O resultado deste trabalho vem auxiliar na construção de um referencial sobre o tema para Ciência da Informação no Brasil, uma vez que existem apenas dois artigos indexados pela BRAPCI que abordam os certificados digitais e a assinatura digital identificados até a conclusão deste trabalho, e nenhum trata especificamente sobre as Autoridades Certificadoras. Nos encontros de 2010 até 2014 do Enancib nenhum trabalho sobre o tema foi apresentado no GT 8 que trata das tecnologias de informação sob a ótica da CI.

2. CERTIFICAÇÃO DIGITAL

A certificação digital é uma tecnologia que busca garantir a segurança das informações trocadas em relações eletrônicas, identificando ao receptor da informação quem é o emissor. Segundo Freitas e Veronese (2005), este sistema assegura basicamente a autenticidade, a confidencialidade, a integridade e o não repúdio da informação.

Já os certificados digitais são arquivos digitais formados por um conjunto de dados de identificação da entidade e do emissor, o valor da chave pública da entidade, o período de validade (indica a quantidade de tempo em que o certificado é considerado válido) e a assinatura digital do emissor (AC), que atesta a validade do vínculo entre a chave pública da entidade e as informações de identificação da entidade. Eles estão destinados a interligar, de forma única e segura, a relação entre a chave pública e a chave privada.

> O papel de certificados digitais está crescendo rapidamente em computadores individuais e redes e em toda a Internet. Embora certificados possam ser usados com pouca ou nenhuma intervenção do usuário, pode ser importante examinar e entender o conteúdo de certificados, além de gerenciar o seu uso. (MICROSOFT, [200?]).

Possuem diferentes aplicações, podem ser usados para identificar uma pessoa, um sistema ou um equipamento, utilizados para assinatura digital individual ou em série, podem ser empregados para criptografar documentos, mensagens ou dados transmitidos pela Internet. Contudo para emissão de um certificado é necessário um infraestrutura de chaves publicas ICP, que pode ser composta por uma AC Raiz e ACs intermediárias.

Devido à existência de vários modelos de infraestrutura de chaves públicas (ICPs) pelo mundo, os navegadores de *Internet* trazem instalados automaticamente certificados de Autoridades Certificadoras Raízes que eles consideram confiáveis. É dado um alerta quando o usuário acessa um determinado site, que não tenha instalado um certificado assinado por uma Autoridade Certificadora (AC) confiável, para que o usuário tenha a opção de instalar da AC emissora os certificados necessários, antes de estabelecer uma conexão. As Autoridades Certificadoras são responsáveis pela emissão e assinatura dos certificados.

3. AUTORIDADE CERTIFICADORA (AC)

A Autoridade Certificadora pode ser considerada como o componente mais importante de uma Infraestrutura de Chaves Públicas (ICP ou, em inglês, *Public Key Infrastructures* – PKI). Segundo Monteiro e Mignoni (2007, p. 17):

> As autoridades certificadoras são entidades de confiança, que emitem certificados digitais para outras entidades, empresas, indivíduos, que precisam se identificar e garantir suas operações no mundo digital. Cada Certificado Digital emitido é certificado e garantido pela AC responsável pela sua emissão.

A autoridade certificadora fornece os pares de chaves utilizados tanto para a assinatura digital como para a criptografia. Também fornece os certificados digitais, que identificam quem você é para as outras pessoas, além de evitar o repúdio. (GANDINI; SALOMÃO; JACOB, 2001). Uma AC pode prestar diferentes serviços, como por exemplo: o serviço de gerenciamento de chaves, a autenticação de data e a divulgação da Lista de Certificados Revogados. Chang et al.(2007, 351, tradução nossa) indicam que no ambiente de rede, as atividades de e-governo e comércio eletrônico são dependentes dos documentos e das assinaturas digitais como uma de suas fundações para segurança da comunicação eletrônica e para transações. Por isso,

> [...] vários navegadores *web* são pré-configurados para confiar em autoridades certificadoras bem conhecidas, isto é, tais navegadores já vêm com os certificados de autoridades como a VeriSign, Thawte, dentre outras. (MARTINS, 2001, p. 6).

Todas as autoridades precisam ter um certificado que comprove sua identidade que pode ser emitido por outra AC confiável, ou produzida por ela mesma, no caso da AC Raiz.

As ACs atuam em conjunto com as Autoridades de Registro (AR) que têm a função, verificar os dados de identificação fornecidos pelos requisitantes dos certificados a fim de garantir a veracidade destas informações. As ARs recebem, conferem e registram as informações cedidas pelo requerente em um banco de dados. Comprovada a veracidade das informações, a AR solicita que a AC gere, assine e emita o certificado digital.

3.1 Tipos de Autoridades Certificadoras

As ACs seguem uma hierarquia dentro da infraestrutura de chaves públicas. Existem dois tipos de Autoridades Certificadoras: as Autoridades Certificadoras Raiz e as Autoridades Certificadoras Intermediárias, conhecidas também por Autoridades Certificadoras Subordinadas.

As Autoridades Certificadoras Raiz estão no topo da cadeia de Autoridades Certificadoras. Elas são usadas na emissão de certificados para outras autoridades de certificação subordinadas e são autoassinadas. São também o elemento da mais alta confiança da cadeia. Se uma AC Raiz ou seu certificado for comprometido ou emitir um certificado para uma entidade não autorizada, toda a estrutura ficará vulnerável.

As Autoridades Certificadoras Intermediárias estão sempre subordinadas à AC Raiz. É a AC Raiz quem aprova os procedimentos de certificação de sua AC subordinada. A AC Intermediária é responsável pela emissão de certificados para usuários finais. As ACs intermediárias também podem emitir certificados para outras autoridades de certificação mais subordinadas.

No Brasil, podemos encontrar estes dois tipos de Autoridades Certificadoras. O Instituto Brasileiro de Tecnologia da Informação (ITI – Brasil) é um exemplo de mantenedor de AC Raiz, e a Certisign uma AC Intermediária.

3.2 Autoridades Certificadoras Brasileiras

De acordo com a Medida Provisória nº 2.200-2, de 24 de agosto de 2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil e transforma o Instituto Nacional de Tecnologia da Informação em autarquia, no seu Art. 5º, compete à AC Raiz

> [...] emitir, expedir, distribuir, revogar e gerenciar os certificados das ACs de nível imediatamente subsequente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das ACs e das ARs e dos prestadores de serviço habilitados na ICP [...].

A Medida Provisória proíbe a AC Raiz de emitir certificados diretamente ao usuário final, e designa esta tarefa às ACs intermediárias que têm a função de

> "[...] emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações." (BRASIL, 2001).

O Brasil possui uma infraestrutura pública, mantida pelo Instituto Nacional de Tecnologia da Informação (ITI) – que segue regras de funcionamento estabelecidas pelo Comitê Gestor da ICP-Brasil. Como o Brasil adotou um modelo de certificação com raiz única, o ITI, além de atuar como mantenedor da Autoridade Certificadora Raiz, também é o responsável pela manutenção dos processos de credenciamento de ACs subordinadas à ICP-Brasil. Compete ainda ao ITI estimular e desenvolver projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital, inclusão digital e à popularização da certificação digital ICP-Brasil. (ITI, 200?).

Para manter o controle sobre as ACs credenciadas, são realizadas auditorias pela AC Raiz, antes do início de suas atividades e, depois do credenciamento, uma vez por ano, para verificar se as exigências das normas da ICP-Brasil e da legislação estão sendo integralmente cumpridas.

Em sua página *web,* o ITI apresenta informações sobre os certificados digitais (o que são, como adquirir) e sobre a estrutura da ICP-Brasil e seu funcionamento. O ITI também disponibiliza organogramas com a estrutura completa ou resumida (1º e 2º níveis) e uma relação com descrição sobre as ACs de 1º nível, juntamente com a apresentação da sua estrutura. São elas:

- **SERPRO – Serviço Federal de Processamento de Dados:** A primeira AC de 1º nível a ser credenciada pela ICP-Brasil. Trabalha com prestação de serviços em Tecnologia da Informação e Comunicações para o setor público. É considerada uma das maiores organizações públicas de TI no mundo.
- **Caixa Econômica Federal:** É a única instituição financeira credenciada como AC na ICP-Brasil.
- **Serasa Experian:** É uma AC do setor privado que fornece a segurança dos certificados digitais para quase todos os grupos financeiros participantes do Sistema de Pagamentos Brasileiro (SPB).
- **Receita Federal do Brasil:** Disponibiliza serviços para facilitar e simplificar o cumprimento espontâneo das obrigações tributárias para os que possuem certificados digitais ICP-Brasil.
- **Certisign:** Pertencente ao grupo Symantec (antiga VeriSign). Fornece a ferramenta tecnológica e desenvolve soluções para uso exclusivo com certificados digitais ICP-Brasil.
- **Imprensa Oficial do Estado de São Paulo:** É a Autoridade Certificadora Oficial do Governo do Estado de São Paulo. Oferece produtos e serviços de certificação digital para os poderes executivo, legislativo e judiciário, incluindo todas as esferas da administração pública, nos âmbitos estadual e municipal.
- **AC JUS:** A AC-JUS é a primeira AC no mundo criada e mantida pelo poder judiciário, pensando no desenvolvimento de aplicações para comunicação e troca de documentos, viabilizando o Processo Judicial Eletrônico (PJ-e).
- **AC PR:** Criada por iniciativa da Casa Civil, essa tem como objetivo emitir e gerir certificados digitais das autoridades da Presidência da República, ministros de estado, secretários-executivos e assessores jurídicos que se relacionem com a PR.
- **Casa da Moeda do Brasil:** Empresa pública responsável pela produção do meio circulante brasileiro e de outros produtos de segurança, tais como passaportes com *chips* e selos fiscais.
- **Valid Certificadora Digital:** Além da emissão dos certificados, a Valid oferece serviços de tecnologia para infraestrutura de chaves públicas, consultoria e suporte em processos e atividades de apoio a Autoridades de Registro.
- **Soluti Certificação Digital: A**tuava como Autoridade de Registro (AR) e em 2012 tornou-se AC vinculada à ICP-Brasil.
- **AC DigitalSign:** É uma empresa portuguesa que tornou-se uma AC através da DigitalSign Certificadora, pertencente ao grupo DigitalSign Portugal, AET Europe e Thomas Greg & Sons.
- **AC Boa Vista:** É a unidade de negócios de certificação digital da Boa Vista Serviços – administradora do Serviço Central de Proteção ao Crédito (SCPC) – que oferece

soluções para a tomada de decisões sustentáveis de crédito e gestão de negócios. (ITI, 200?).

4. APLICAÇÕES DOS CERTIFICADOS DIGITAIS OFERECIDOS PELAS ACs

As Autoridades Certificadoras podem oferecer diversos produtos ou serviços de certificação digital, cada um com uma utilidade diferente, como listado a seguir.

- Certificado SSL - De acordo com a VeriSign, há nos servidores e navegadores *Web* um protocolo SSL (*Secure Sockets Layer*) que auxilia os usuários a proteger seus dados por meio de um canal criptografado, durante a transferência, para as comunicações privadas pela *Internet* pública.

> Todo certificado SSL emitido para uma entidade verificada pela CA é emitido para um servidor e domínio de *site* específicos (endereço do *site*). Quando uma pessoa usa o navegador para ir até um endereço de um *site* com um certificado SSL, uma conexão segura (saudação) é estabelecida entre o navegador e o servidor. As informações são solicitadas do servidor, que se tornam então visíveis ao usuário em sua janela do navegador. Você notará alterações indicando que uma sessão segura foi iniciada, por exemplo, uma marca de confiança será exibida. (SYMANTEC, 2012, p. 4).

- Infraestrutura de Chave Pública (ICP) Corporativo - Utilizada por empresas que precisam de segurança de alto nível para operar aplicações de negócios através da *Internet*. É possível obter essa segurança através de certificados fornecidos por uma infraestrutura de chave pública (ICP), que protege aplicativos empresariais que exigem o mais alto nível de segurança, como por exemplo: a forma de assinatura digital, mensagens instantâneas da empresa, e comércio eletrônico, *firewalls*, redes virtuais privadas (VPNs), diretórios entre outros.

> Sua finalidade é gerenciar chaves e certificados, ajudando uma organização a estabelecer e manter um ambiente de rede confiável. A PKI permite o uso de criptografia e serviços de assinatura digital através de uma ampla variedade de aplicações. (ENTRUST, 200?).

- Assinatura Digital de Documentos - A assinatura digital é um elemento de credibilidade que autentica o documento eletrônico, identificando seu assinante e comprovando que o documento não tenha sido alterado a partir da sua assinatura.

> Assim como assinar na forma manuscrita garante a autenticidade, do mesmo modo quando aplicada a um documento a assinatura digital permite a verificação de sua integridade e estabelece uma imutabilidade lógica do conteúdo do documento. (ARAÚJO, VIEIRA. 2012, p. 295).

© Rev. Digit.Bibliotecon. Cienc. Inf. | Campinas, SP | v.13 | n.2 | p.366-385 | maio/ago. 2015 | ISSN 1678-765X

- Assinatura Eletrônica Automatizada de Documento - Esta solução tem praticamente as mesmas características da Assinatura Digital. A diferença é que ela permite que o usuário assine uma grande quantidade de documentos automaticamente.

- Assinatura de Código - Atualmente não há garantia de que um código de *software* publicado na *Internet* não foi alterado ao ser transferido. Normalmente os navegadores *web* exibem uma mensagem de aviso alertando no caso de existirem possíveis perigos nos *downloads* de aplicativos, mas não eles não conferem autenticidade e a integridade do código. Assim,

> A assinatura de código é o processo de assinatura digital de arquivos executáveis e *scripts* para confirmar a identidade do autor de *software* e garante que o código não tenha sido alterado ou corrompido desde que foi assinado. A AC Raiz é responsável por confirmar a identidade dos assinantes e vincular sua chave pública para um certificado de assinatura de código. (ENTRUST, 2013, p 4. Tradução nossa).

- Assinatura de Correio Eletrônico - Esta aplicação permite que o usurário proteja informações pessoais, sensíveis e valiosas, assinando digitalmente e criptografando mensagens de correio eletrônico (*e-mails*) através de um ID. Assim, o destinatário terá a confirmação da proveniência da mensagem e de que a sua privacidade foi mantida durante a transmissão.

> A encriptação de uma mensagem de correio eletrônico [...] protege a privacidade da mensagem convertendo-a de texto simples legível num arquivo de encriptação. Apenas o destinatário que tem a chave privada correspondente à chave pública utilizada para encriptar a mensagem poderá descodificar a mensagem para leitura. Qualquer destinatário sem a chave privada correspondente verá texto incompreensível. (MICROSOFT, 200?).

- Assinatura Eletrônica Móvel - É uma aplicação "tudo em um" portátil, que se apresenta no formato de um dispositivo USB, um *Token* criptográfico, que não necessita de instalação de *softwares*, ou de configurações. Este dispositivo atua sem deixar rastros ou algum registro do que está sendo feito no computador. Ele contém: certificado digital reconhecido; aplicação para assinatura eletrônica, para assinar documentos eletronicamente; navegador de *Internet*; aplicativo de *e-mail* com a funcionalidade de assinatura e criptografia; aplicativo de criptografia para armazenar e transportar com segurança documentos pessoais e confidenciais. (Camerfirma, [200?]. Tradução nossa.).

- *TimeStamp* - Sua tradução quer dizer "carimbo/selo de tempo". É um serviço que tem a função de provar a data e hora de uma operação ou uma determinada transação como compra ou venda, por exemplo. Serve ainda para comprovar que não foram feitas alterações nos dados a partir da data de referência. O relógio do computador é ajustado, aferido e controlado de acordo com os algoritmos de seleção e sincronização de um sistema que calcula o tempo com precisão, certificado por uma AC. Assim, o momento exato em que um documento é produzido e/ou assinado fica garantido. A

utilização do Carimbo de Tempo no Brasil tem validade legal incontestável apenas se for emitido por uma Autoridade de Carimbo de Tempo (ACT) credenciada pelo ITI.

- Cartão de Identificação Digital - É uma mídia criptográfica de armazenagem de certificados digitais e pares de chaves criptográficas. Seu formato é o de um *smartcard* (cartão inteligente), similar a um cartão de crédito e possui dois códigos de segurança que são gravados internamente, similar aos *chips* de algumas operadoras de telefonia – o PIN e o PUK. Ele é utilizado para autenticação do titular e assinaturas digitais em ambiente eletrônico. (Certisign, [200?].).

- Certificados para dispositivos móveis - Neste caso os certificados digitais são implantados em dispositivos móveis para conceder e garantir o acesso a redes de *e-mails* corporativos e para proteger identidades e transações móveis. É baseado em serviços de nuvem de uma AC. Sendo assim, as corporações não precisam implementar ou gerenciar uma AC: elas têm acesso direto às plataformas pelos dispositivos móveis.

> A solução otimiza o gerenciamento e entrega de certificados de dispositivo, que podem ser entregues diretamente aos dispositivos móveis sem a necessidade de *software*. Isso tudo é realizado através de uma interface fácil de usar que pode ser acessada a qualquer hora e de qualquer lugar. Essa abordagem reduz os custos, aumenta a eficiência e simplifica a configuração e implantação. (ENTRUST, [200?]. Tradução nossa).

Para atender a demanda específica do mercado Brasileiro, Autoridades de Certificação no Brasil desenvolveram diferentes especificidades em seus certificados.

- Acesso Remoto - É um serviço exclusivo do Serviço Federal de Processamento de Dados – SERPRO, que permite aos clientes e usuários o acesso remoto à *Intranet* do Serpro no Brasil ou fora dele, através da *Internet*, de forma segura. Para acessar tal serviço, é necessário que o usuário possua um Certificado Digital do tipo A1 (válido por um ano) ou do tipo A3 (válido por três anos) credenciado pela ICP-Brasil. (SERPRO, [200?]).

- Certificados para Mercado Financeiro Brasileiro - Existem variados tipos de certificados para o mercado financeiro, como por exemplo: CCS, SPB, CIP, COMPE. Todos foram desenvolvidos para autenticar, homologar e garantir a segurança no acesso e nas transações realizadas eletronicamente entre as instituições financeiras e o Banco Central ou a Secretaria do Tesouro Nacional.

- Conectividade Social ICP - Este serviço substitui o antigo Conectividade Social, que antes era um *software* instalado no computador, emitido em disquete. Com o novo Conectividade Social ICP basta acessar a página na *Internet*, de posse do certificado digital ICP, para envio de arquivos e recebimento de relatórios, transmitir os arquivos do FGTS, como também acessar o aplicativo *web* "Conexão Segura", utilizado para

fazer a comunicação de afastamento do empregado, entre outras tarefas. (CAIXA, 2011).

- e-CPF - É o documento eletrônico de identidade (versão eletrônica do CPF) emitido por Autoridade Certificadora credenciada junto à Autoridade Certificadora Raiz da ICP-Brasil e habilitada pela Autoridade Certificadora da Receita Federal do Brasil (AC-RFB), que garante a autenticidade, integridade, privacidade e inviolabilidade dos emissores e destinatários e dos documentos e dados por eles emitidos nas transações eletrônicas de pessoa física. Existem dois tipos de e-CPF: o A1, que é gerado e armazenado diretamente no computador do titular com um ano de validade; e o A3, que é armazenado em mídia criptográfica, ou seja, um *token* ou cartão inteligente, de acordo com as normas da ICP-Brasil, válido por um ou três anos.

- e-CNPJ - Da mesma forma do e-CPF, o e-CNPJ é um documento eletrônico em forma de certificado digital. Ele garante que a comunicação entre pessoa jurídica e a RFB seja segura, autêntica e íntegra.

> Através dele é possível realizar consultas e atualizar os cadastros de contribuinte pessoa jurídica, obter certidões da Receita Federal, cadastrar procurações e acompanhar processos tributários através da *Internet* sem a necessidade de ir até um posto de atendimento. (SOLUTI, [200?]).

O e-CNPJ também pode ser encontrado nos tipos A1 e A3, igualmente ao e-CPF.

- e-NF - A Nota Fiscal Eletrônica (e-NF) é a versão eletrônica do documento Nota Fiscal, que registra uma transferência de propriedade sobre um bem ou uma atividade comercial prestada por uma empresa e uma pessoa física ou outra empresa. Sua validade jurídica se dá pela assinatura digital do remetente através de um certificado digital ICP-Brasil. Com este serviço, é possível acompanhar em tempo real as operações comerciais realizadas pelo Fisco. Encontrada nos tipos A1 e A3. (CERTISIGN, [200?]).

- GED - O serviço de Gestão Eletrônica de Documentos – GED oferecido pela Imprensa Oficial do Estado de São Paulo trabalha com métodos baseados nos conceitos do *Business Process Management* – BPM. É realizada a captura de documentos, a indexação de arquivos eletrônicos, aplicação de *software* de Reconhecimento Óptico de Caracteres – OCR, e consultoria em digitalização.

5. DESENVOLVIMENTO E METOGOLOGIA

A amostra foi composta pelos documentos publicados nos *sites* de quarenta e quatro ACs, sendo treze no Brasil e trinta e um no exterior. A lista das ACs internacionais foi obtida junto aos navegadores WEB (Gloogle Chome, Mozila Firefox, IE e Safari). Para a relação das CAs brasileiras foi consultado o site do ITI. Os documentos foram consultados entre outubro de 2013 e março de 2014.

Neste projeto, utilizamos a análise de conteúdo como metodologia para tabular e analisar os resultados obtidos. Bardin (1979) define a análise de conteúdo como:

> Um conjunto de técnicas de análise das comunicações visando obter, por procedimentos, sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) destas mensagens. (BARDIN, 1979, p. 42).

Existem diferentes fases da análise de conteúdo que, segundo Bardin (1979), se organizam em três polos cronológicos. São elas:

- a pré-análise – fase de organização e escolha dos documentos a serem analisados;
- a exploração/análise do material – é a fase, longa e cansativa, da análise propriamente dita;
- e o tratamento dos resultados, a inferência e a interpretação – fase onde os resultados da análise são tratados quantitativamente, mas sem excluir a interpretação qualitativa, para que sejam significativos e válidos.

5.1 Etapas de realização do projeto

O desenvolvimento do projeto foi realizado durante o período de 10 meses. Nos primeiros dois meses, foi desenvolvida revisão de literatura sobre Segurança da Informação e Certificação Digital, para construir as bases conceituais para execução do projeto.

Pré-análise:

Durante cinco meses, realizamos uma busca das Autoridades Certificadoras Raiz nos navegadores Chrome, Internet Explorer, Safari e o Mozilla Firefox. Foi identificado as ACs juntamente com seu caminho de certificação, e mapeado os produtos e serviços de certificação oferecidos por cada uma delas. Indicando o que cada um proporciona ao cliente permitindo montar assim, um quadro como o modelo de negócio, relacionando os produtos/serviços oferecidos às ACs. A consulta aos produtos e serviços de cada AC Raiz foi realizada através da *Internet*, por meio do buscador *Google* utilizando o nome das ACs como termo para a busca. Assim, encontrou-se a *homepage* das ACs Raiz permitindo analisar os seus produtos e serviços.

Exploração e análise do material:

Foi realizada a leitura, tradução e classificação do material. O material analisado foi composto por páginas *web*, portfólios de produtos e artigos. A maior parte do material foi colhida em páginas *web* das ACs, onde encontramos portfólios de produtos e aplicações, como por exemplo: Assinatura de Códigos, Certificados SLL e Conectividade Social, respectivamente das ACs Entrust, Symantec e Caixa. Como a maioria das ACs são estrangeiras, foi necessária a utilização de aplicativos de tradução *on-line*. Nos últimos três

meses, produzimos documentos para a interpretação dos dados coletados, citados acima que foram organizados nos quadros 1 e 2.

© Rev. Digit.Bibliotecon. Cienc. Inf. | Campinas, SP | v.13 | n.2 | p.366-385 | maio/ago. 2015 | ISSN 1678-765X

QUADRO 1 – Relação das Autoridades Certificadoras Raiz brasileiras, regulamentadas pelo ITI e pela ICP-Brasil, e os produtos e serviços por elas oferecidos.

AC	Certificado Digital	Acesso Remoto	Certificado de Assinatura de Código	Certificados para Mercado Financeiro	Certificado para Servidor Web (SSL)	e-CPF	e-CNPJ	e-NF	GED	Correio Eletrônico Confiável	Assinatura Digital de Documentos	Conectividade Social ICP
Caixa	X											X
SERPRO	X	X	X									
Serasa Experian	X		X	X	X			X				
Receita Federal do Brasil						X	X					
Imprensa Oficial - SP					X	X	X		X	X		
AC JUS	X		X		X							
AC PR	X		X									
Casa da Moeda do Brasil	X		X									
Certisign			X	X	X	X	X	X		X	X	
Valid C.D.				X	X	X	X	X			X	X
Soluti C.D.	X					X	X	X			X	
Digitalsign					X	X	X	X			X	x
AC Boa Vista					X	X	X	X				x

Fonte: Dados da pesquisa (2014).

QUADRO 2: Relação das Autoridades Certificadoras Raiz e os produtos e serviços por elas oferecidos.

Nome da AC Raiz/ serviço prestado	Certificado SSL	Assinatura de Correio Eletrônico	Time Stamp	Cartão de Identificação	Certificados para dispositivos móveis	Assinatura Digital	Assinatura Eletrônica Automatizada de Documento	Assinatura Eletrônica Móvel	PKI Corporativo	Assinatura de Código
Camerfirma	X		X				X	X		
Actalis	X		X			X		X		
Affirm Trust	X									
Agencia Catalana de Certificacion	X									
AS Sertifitseerimiskeskus	X		X			X				
A-Trust	X	X		X		X		X		
CertSign	X	X	X			X	X			
Buypass	X			X			X		X	
Certinomis	X	X	X						X	
Comodo	X	X								
ComSign	X					X				
Dhimyotis	X		X	X		X				

DigiCert	X					X			X	X
Digital Signature Trust	X					X			X	
Disig a.s.	X				X			X		
EBG Bilisim Teknolojileri ve Hismetleri A.S.	X		X	X		X		X		
Elektronik Bilgi Guvenligi	X		X			X	X			X
Entrust	X	X		X		X		X	X	X
GeoTrust	X	X				X				X
GlobalSign	X					X				X
Go Daddy	X									X
GTE CyberTrust Global Root	X	X	X			X			X	
Hellenic Academic And Research Institutions Root	X									
Starfield Root Certificate Authority	X									
STARTCOM CERTIFICATION AUTHORITY	X					X		X		
THAWTE PREMIUM SERVER CA	X									X
TURKTTRUST ELETRONIK SERTIFIKA HIZMET	X		X			X		X	X	X
VERISIGN	X	X				X			X	X

Fonte: dados da pesquisa (2014).

Verificou-se que os produtos e serviços oferecidos pelas ACs nacionais e internacionais são similares, as diferenças foram verificadas nos certificados emitidos para finalidades específicas, como os criados no Brasil para atender o sistema nacional de Nota Fiscal eletrônica, o e-CPF, e-CNPJ, etc.

4. CONSIDERAÇÕES FINAIS

São poucos os estudos acadêmicos publicados sobre este tema no Brasil e no exterior. Estudos como os desenvolvidos por Bos (1996), Chang et at. (2007) e Yu et al.(2012) abordam os fatores para adoção no uso dos certificados digitais em aplicações na área de saúde, como a assinatura digital em prontuários médicos. O texto de Bos (1996, p.158), por ser dos anos 90, ainda discute a necessidade de um aporte legal para validação das assinaturas digitais.

A questão legal da adoção da certificação digital e de suas aplicações no Brasil foram amplamente discutidas no início dos anos 2000, logo após a edição da MP 2.200-2. Contudo com a criação da AC-Jus, e a crescente utilização dos certificados digitais nos processos do judiciário, o debate sobre a legalidade ou não da utilização dos certificados digitais foi minimizado.

Neste trabalho foram analisadas ACs de diversos países: Estados Unidos, França, Espanha, Eslováquia, Estônia, Áustria, Noruega, Alemanha, Israel, Turquia, Grécia e África do Sul. Foi constatado que o serviço mais popular foi ode emissão do Certificado SSL, onde trinta e duas, ou seja, todas as ACs estrangeiras e cinco das treze ACs brasileiras oferecem esse tipo de certificado. O que era esperado, pois este tipo de certificado é utilizado pelos sites e portais para criptografia de dados nas relações de comercio eletrônico, acesso a bancos via Web, acesso seguro a servidores de correio eletrônico, entre outros serviços populares na Internet.

Já os mais específicos foram os de GED, oferecido apenas pela AC brasileira da Imprensa Oficial do Estado de São Paulo, e o certificado para dispositivos móveis oferecido pela Disig. Contudo deve-se observar este último, pois com o crescimento na utilização de dispositivos moveis é possível que outras ACs venham oferecer este produto. Os resultados desta pesquisa apresentam um quadro dos serviços e produtos oferecidos pelas ACs no período em que esta foi desenvolvida, e é de se esperar que este quadro se altere conforme as necessidades do mercado for se modificando.

Neste contexto é importante que os profissionais de informação, especialmente os arquivistas atuantes no Brasil, conheçam a legislação e entendam quais são os procedimentos, ferramentas e atores envolvidos no processo de certificação digital, e a diferença entre as Autoridades Certificadoras e Autoridades de Registro. Além de desenvolver os saberes que possibilitem escolher o certificado ideal para cada caso permitindo que este possa discernir e contratar tais serviços corretamente, pois os documentos digitais precisam ser preservados,

validados, mantidos íntegros e autênticos, e isso está diretamente relacionado com tais tecnologias.

Este estudo mostra que a oferta dos certificados digitais pelas ACs acontece devido a demanda do mercado usuário dessa tecnologia, não necessariamente pela tecnologia utilizada na emissão ou por esse tipo de certificado ou aquele ser melhor ou mais acessível.

Essa afirmação pode ser evidenciada na oferta dos certificados do tipo e-CPF e e-CNPJ que são exclusivos de uso no Brasil, e ofertados pela maiorias das ACs nacionais. Uma vez que são regulamentados pelas instruções normativas da Receita Federal do Brasil (RFB), e permitem as mesmas aplicações de uso que os oferecidos pelos certificados emitidos por ACs estrangeiras, pois sua estrutura é a mesma regulamentada pela RFC 6818, no entanto traz informações adicionais como por exemplo o CPF o titular, no caso do e-CPF. O mesmo ocorre para os certificados emitidos para os advogados e suas interações eletrônicas com diferentes instâncias do poder judiciário.

Os resultados obtidos permitem ainda inferir que o Brasil se encontra na vanguarda, quando se tratada utilização desta tecnologia, esse fato pode ser verificado quando se analisa as especificidades dos produtos de certificação digital que são oferecidos pelas ACs credenciadas junto à ICP-Brasil.

É fato que os profissionais arquivistas irão cada vez mais encontrar documentos que existirão apenas no meio digital, ou seja: serão criados, processados e são descartados digitalmente, e assim como os documentos em suporte físico, os documentos digitais também necessitam de gestão e preservação eficientes, que podem ser realizadas através de diferentes *softwares*. A autenticidade desses documentos precisa estar de acordo com os procedimentos de gestão arquivística. Contudo, sabemos que a tecnologia pode se tornar obsoleta no decorrer do tempo e isso pode fazer com que a validade e a autenticidade de um documento assinado digitalmente sejam perdidas com a atualização ou a substituição dos *softwares* e *hardwares*. Para fazer frente a estes desafios os profissionais da informação devem conhecer e acompanhar cada uma das tecnologias apresentadas neste artigo, ou correm o risco de se tornarem obsoletos tão rapidamente como tantas tecnologias já criadas e descontinuadas.

REFERÊNCIAS

ARAÚJO, Francisco de Assis Noberto Galdino de; CRUZ, José Manuel Magalhães; SBROGLIO, Suzilaine. **Autoridades de Certificação**: importância e necessidade para uma infraestrutura de chave pública (PKI). Faculdade de Engenharia da Universidade do Porto. 2011. 23 p. Disponível em: <http://paginas.fe.up.pt/~jmcruz/seginf/seginf.1112/trabs-als/final/G3-T1.certif-auth.final.pdf>. Acesso em: 5 maio 2014.

ARAÚJO, Wagner Junqueira de; VIEIRA, Renato Melo. Assinatura de documentos eletrônicos utilizando certificados digitais. **Biblionline**, João Pessoa, v. 8, n. esp., p. 290-302, set. 2012.

ARQUIVO NACIONAL. **Dicionário brasileiro de terminologia arquivística**. Rio de Janeiro: Arquivo Nacional, 2005. 232p.; 30cm. – Publicações Técnicas; nº 51

BARDIN, Laurence. **Análise de conteúdo.** Lisboa: Edições 70, 1979.

BOS, J. J. Digital signatures and the electronic health records: providing legal and security guarantees. **International journal of bio-medical computing**, v. 42, n. 1, p. 157-163, 1996

BRASIL. INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **ICP-Brasil**: Estrutura. Disponível em: <http://www.iti.gov.br/icp-brasil/estrutura>. Acesso em: 5 maio 2014.

BRASIL. **Medida Provisória nº 2.200-2**, de 24 de Agosto de 2001. Disponível em: <http://www.iti.gov.br/images/icp-brasil/legislacao/Medida%20Provisoria/MEDIDA_PROVIS_RIA_2_200_2_D.pdf> Acesso em: 5 maio 2014

CAIXA. **Conectividade Social ICP**: Guia de orientações ao usuário. v. 1.4. 2011. Disponível em: < http://www.caixa.gov.br/fgts/conectividade_social_ICP.asp> Acesso em: 22 ago 2014

CAMERFIRMA. Businesswear. [200?]. Disponível em: <http://www.camerfirma.com/en/productos/businesswear/> Acesso em: 19 ago 2014

CHANG, I.-Chiu et al. Factors affecting the adoption of electronic signature: Executives' perspective of hospital information department. **Decision Support Systems**, v. 44, n. 1, p. 350-359, 2007.

CERTISIGN. NF-e. [200?]. Disponível em: < http://www.certisign.com.br/certificado-digital/para-empresa/nfe>. Acesso em 22 ago 2014

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais**. 2012. Disponível em: <http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm>. Acesso em: 22 ago 2014

CORRÊA, Renato Fernandes; DORNELES, Sânderson Lopes. Gestão de documentos digitais em aplicações de certificação digital. **Informação Arquivística**, Rio de Janeiro, v. 2, n. 2, p. 3-31, jul./dez., 2013. Disponível em: <http://www.aaerj.org.br/ojs/index.php/informacaoarquivistica/article/view/28>. Acesso em: 31 jul 2014.

ENTRUST. **Entrust IdentityGuard Cloud Services Device Certificates**. [200?]. Disponível em: <http://entrust.wpengine.netdna-cdn.com/wp-content/uploads/2013/05/DS_Entrust-IDGCS_DeviceCerts_web_Jan2014.pdf> Acesso em: 15 ago 2014

ENTRUST. **What is Code Signing?** The ins and outs of how code signing works and why it's necessary. 2013. Disponível em: < http://entrust.wpengine.netdna-cdn.com/wp-content/uploads/2013/10/WP_CodeSigning_Oct2013.pdf>. Acesso em: 15 ago 2014

FREITAS, Christiana Soares de; VERONESE, Alexandre. Segredo e democracia: certificação digital e *software* livre. **Informática Pública**, Belo Horizonte, v. 8, n. 2, p. 09-26, maio, 2007. Disponível em: <http://www.ip.pbh.gov.br/ANO8_N2_PDF/artigo-segredo-e-democracia.pdf>. Acesso em: 4 ago 2014

GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva; JACOB, Cristiane. **A segurança dos documentos digitais**. [S.l.: s.n.], 2001. 19 p. Disponível em: <http://egov.ufsc.br/portal/sites/default/files/anexos/27250-27260-1-PB.pdf>. Acesso em: 4 maio 2014.

IETF. INTERNET ENGINEERING TASK FORCE. Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. **Request for Comments: 6818**. Janeiro de 2013. Disponível em: <https://tools.ietf.org/html/rfc6818>. Acesso em: 27 de maio de 2015.

MARQUES, Francisco das Chagas Fontenele; CASTRO, Isaac de Sousa; VERAS, Jaclason Machado. **Certificação digital**: tecnologia indispensável na segurança das transações eletrônicas. Disponível em: <http://www.enucomp.com.br/2012/conteudos/artigos/certificacaoDigital.pdf>. Acesso em 5 maio 2014.

MARTINS, Alessandro. **Autoridade Certificadora para Acesso Seguro**. Universidade Federal do Rio de Janeiro – UFRJ: [s.n.], 2001. 17 p. Disponível em: <http://www.lockabit.coppe.ufrj.br/sites/lockabit.coppe.ufrj.br/files/publicacoes/lockabit/ca.pdf>. Acesso em: 4 maio 2014.

MICROSOFT. **Encriptar mensagens de correio electrónico**. [200?]. Disponível em: < http://office.microsoft.com/pt-pt/outlook-help/encriptar-mensagens-de-correio-electronico-HP010355559.aspx?CTT=5&origin=HP010355563> Acesso em: 19 ago 2014

MICROSOFT. **Tipos de autoridades de certificação**. [S.l.: s.n.], [200?]. Disponível em: <http://technet.microsoft.com/pt-br/library/cc740257(v=ws.10).aspx>. Acesso em: 5 maio 2014.

MONTEIRO, Emiliano S., MIGNONI, Maria Eloisa. **Certificados Digitais**: Conceitos e Práticas. Rio de Janeiro: Brasport, 2007. 218 p.

RICHARDSON, Roberto Jarry. Pesquisa Social: métodos e técnicas. 3. ed. São Paulo: Atlas, 1999. p. 334.

SERPRO. SAR. **Descrição do Serviço**. [200?]. Disponível em: < https://www.serpro.gov.br/gestao-corporativa/servicos/sar-descricao-do-servico> Acesso em: 22 ago 2014

SINGH, Simon. **O livro dos códigos**: a ciência do sigilo o do antigo Egito à criptografia quântica. Rio de Janeiro: Record, 2001.

SOLUTI. **Para sua empresa**. [200?]. Disponível em: < http://site.solutinet.com.br/2014/menu/para-sua-empresa.html>. Acesso em: 22 ago 2014

SYMANTEC. **Informe oficial**: guia de certificados SSL para iniciantes. [S.l.: s.n.], 2012. Disponível em: <https://forms.symantec.com/websurveys/servlet/ActionMultiplexer?Action_ID=ACT2000&WSD_mode=3&WSD_surveyInfoID=1833&toc=TA48R-1833-01-04&brand=01&country=04&cid=1994A5EA8FE2665A>. Acesso em: 15 ago 2014

YU, Yao-Chang; HUANG, To-Yeh; HOU, Ting-Wei. Forward secure digital signature for electronic medical records. **Journal of medical systems**, v. 36, n. 2, p. 399-406, 2012.

Como citar este documento:

ARAÚJO, Wagner Junqueira de; VIEIRA, Yasmin Brito de Lemos. Comparação entre produtos e serviços oferecidos pelas Autoridades Certificadoras.. **Revista Digital de Biblioteconomia e Ciência da Informação**, Campinas, SP, v. 13, n. 2, p. 366-385, maio/ago. 2015. ISSN 1678-765X. Disponível em: <http://periodicos.bc.unicamp.br/ojs/index.php/rdbci/article/view/2120>. Acesso em: 31 maio 2015.