Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

SÉRGIO MOTA DA SILVA JÚNIOR

CERTIFICAÇÃO DIGITAL
A IMPORTÂNCIA PARA ÓRGÃO PÚBLICO

Brasília
2013

SÉRGIO MOTA DA SILVA JÚNIOR

CERTIFICAÇÃO DIGITAL
A IMPORTÂNCIA PARA ÓRGÃO PÚBLICO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Rede de Computadores com Ênfase em Segurança.

Orientador: Prof. Rafael Sarres de Almeida

Brasília
2013

SÉRGIO MOTA DA SILVA JÚNIOR

CERTIFICAÇÃO DIGITAL
A IMPORTÂNCIA PARA ÓRGÃO PÚBLICO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Rede de Computadores com Ênfase em Segurança.

Orientador: Prof. Rafael Sarres de Almeida

Brasília, 09 de abril de 2013.

Banca Examinadora

_____

Prof. ,

_____

Prof. Gilson Ciarallo

Deus, a ti dedico a conclusão dessa etapa, toda honra e glória a ti.

AGRADECIMENTOS

Agradeço a minha esposa, Raquel, que me incentivou a fazer, continuar e concluir essa etapa da minha vida, ela que por vezes me dizia para já ir escrevendo o trabalho de conclusão de curso e sempre me deu apoio.
Agradeço também a minha filha, Rafaela, que apesar de ser apenas um bebê me faz querer ir mais além por ela, para dar o melhor a ela e querer o melhor para ela; filha, obrigado pelos seus sorrisos e incentivos.

Em especial a Deus por ter me dado oportunidades e ajuda para chegar até aqui e vencer mais essa etapa da minha vida.

RESUMO

O presente trabalho visa apresentar um estudo sobre a importância do certificado digital para uma empresa pública apresentando uma breve explicação do que é certificado digital, Autoridades Certificadoras, AC-Raiz, o cenário da empresa, uma breve apresentação do projeto, os problemas encontrados na execução e gerência da emissão dos certificados digitais para os empregados, além de sugerir mudanças e de que forma lidar com uma possível renovação dos certificados. Para tanto será feito um estudo no método e critérios que foram utilizados para emissão dos certificados, no próprio certificado (atributos), erros cometidos durante a execução do projeto e sugestões de elaboração de documentos como o que consta no apêndice, também que ela adote boas práticas do PMBOK e da IN 04/2010 para caso queira renovar os certificados digitais tenha um projeto bem estruturado e documentado e, por conseguinte responder ao problema que atualmente se encontra na empresa: **Quais formas para lidar com uma renovação dos certificados são as melhores?**

Palavras-chave: Certificado digital. Empresa pública. ICP-Brasil.

ABSTRACT

This work aims to present a study about the importance of digital certificate to public enterprise, showing in brief what a digital certificate is, Certification Authorities, Root Certification Authorities, scenario enterprise, and a short project presentation, the problems to be found in the execution and issuance digital certificates management to employees, beyond suggesting changes and the way to deal whit a possible certificates renewing. So it is going to be done a study over the method and criteria used to certificate issuing, in the certificate itself (attributes), errors made while project execution besides suggestions about documents elaboration like the one included in the appendix, also that it adopts PMBOK good practices and from IN 04/2010 in order to renew the digital certificates it has got a well structured project and recorded documentation, and as a consequence answer the question found in the enterprise: **Which are ways to deal with a renewal certificates are the best?**

Key words: Digital certificate. Public enterprise. ICP-Brasil.

LISTA DE ABREVIATURAS E SIGLAS

AC - Autoridade Certificadora

AC-Raiz - Autoridade Certificadora Raiz

AR - Autoridade de Registro

CG - Comitê Gestor da ICP-Brasil

CRM-DF – Conselho Regional de Medicina do Distrito Federal

ECC – Criptografia de Curvas Elípticas

ICP- Infraestrutura de Chaves públicas

ICP-Brasil - Infraestrutura de Chaves públicas Brasileira

ITI- Instituto de Tecnologia da Informação

OAB – Ordem dos Advogados do Brasil

RG – Registro Geral

RH – Recursos Humanos

RSA – Rivest, Shamir e Adleman

SSP – Secretaria de Segurança Pública

UNICEUB – Centro Universitário de Brasília

SUMÁRIO

INTRODUÇÃO

A certificação digital, hoje, pode ser considerada uma das maneiras mais seguras de se garantir que algo disponível em meio digital seja de fato de quem a reivindica ou possa a reivindicar, já que o certificado garante que conteúdo de mensagens ou textos, seu autor e data sejam confirmados por meio de técnicas e processos que proporcionam segurança à comunicação e transações eletrônicas segundo o Professor Luiz Gustavo Cordeiro da Silva (CASAGRANDE, 2011, p.13).

Desse modo, o presente trabalho apresenta e analisa um cenário em que foi usada a certificação digital com a intenção de se garantir a segurança de informações.

A empresa citada no trabalho existe e faz parte da administração pública indireta do governo federal, porém, devido a problemas burocráticos o nome foi omitido.

Atualmente a empresa por meio de contrato firmado com uma Autoridade Certificadora emitiu certo número de certificados para seus usuários internos, mas como não houve divulgação e informação de como usar e sua importância, a grande maioria não os utilizam.

Pouquíssimos utilizam o total de recursos disponível pelo certificado, alguns acabam simplesmente por utilizá-lo para assinar e-mails e outros, como já mencionado anteriormente, nunca sequer utilizaram.

Mediante ao exposto, os objetivos do trabalho são:

- Demonstrar a importância e relevância da certificação digital para o Governo Federal;
- Destacar a importância da certificação digital para a empresa;
- Apresentar e analisar a implantação do certificado digital;
- Apresentar formas de gerenciamento de certificados.

Para alcançar os objetivos, procedeu-se da seguinte maneira: pesquisas de artigos, trabalhos acadêmicos, periódicos públicos, entrevista com funcionários

que participaram do projeto e emissão dos certificados e qualquer meio que aborde sobre o tema certificado digital como alguns sites do próprio governo federal.

Desse modo, espera-se demonstrar a importância de um certificado digital e aprofundar no processo de implantação de certificação digital da empresa.

O presente trabalho foi então estruturado em 3 capítulos.

No primeiro capítulo, é apresentado a ICP-Brasil, tecnologias usadas, o certificado digital, assinatura digital, garantias e validade jurídica, autoridade certificadora e como obtê-lo.

O segundo capítulo proporciona a apresentação da empresa e o cenário em que foi concebido o projeto, ainda apresenta o critério adotado para aquisição e distribuição do certificado digital, além de problemas enfrentados pela equipe.

Já no terceiro capítulo é apresentado sugestões de melhorias levantadas no capítulo anterior; é dada uma ênfase especial a um problema considerado grave pelo observador e como tratar os demais pela empresa pública.

Por fim, é feita a conclusão para o presente trabalho e algumas considerações são apresentas caso a empresa pública queira dar continuidade ao projeto de certificação digital.

1 ICP-BRASIL, TECNOLOGIA E CERTIFICAÇÃO DIGITAL

Com o surgimento da internet e o crescente volume de dados sendo gerados e transitados pela rede houve a necessidade também de certificá-los, de garantir a um indivíduo e/ou entidade que suas informações são verdadeiras e seguras.

Desse modo, em 2001 criou-se a ICP-Brasil uma autarquia federal ligada à Casa Civil da Presidência da República, responsável por manter a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, sendo a primeira autoridade da cadeia de certificação - AC Raiz.

> Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. (BRASIL, 2001)

A ICP-Brasil é uma infraestrutura composta de *hardware*, *software*, pessoas, políticas e procedimentos para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais. A partir dela os primeiros certificados foram gerados bem como permissão para novas Autoridades Certificadoras – AC.

1.1 Tecnologia – Criptografia

Segundo o site Dicionário Informal, (www.dicionarioinformal.com.br/criptografia), criptografia é uma palavra de origem grega, ***kryptós*** (escondido) e ***gráphein*** (escrita), que significa escrever secretamente.

A criptografia é uma maneira de esconder informações de uma terceira pessoa, fazendo com que ela tenha um grande trabalho para acessar a informação quando ela não tem permissão para tal.

> Dentre as diversas tentativas de definir criptografia de maneira precisa, pode-se dizer de um modo simples, que **criptografia é a ciência de fazer com que o custo de adquirir uma informação de maneira imprópria**

> **seja maior que o custo obtido com a informação**. (SILVA apud CASAGRANDE, 2011, p.21)

Contudo, esse custo pode diminuir caso a pessoa interessada em obter a informação tenha um poder computacional grande. Para evitar que tal pessoa use desse poder que gerencia a informação deverá então aumentar o tamanho da chave usada para criptografar e descriptografar.

> Chave é um valor numérico para cifrar e decifrar um texto. A segurança de um criptossistema pode então ser mensurado baseado no tamanho do espaço de chaves e no poder computacional atualmente disponível. (SILVA apud CASAGRANDE, 2011, p.21)

Atualmente há dois tipos de tecnologia de geração de chaves: chave simétrica e chave assimétrica. Para a chave simétrica há apenas uma chave que faz as duas operações, cifrar e decifrar, esta deve estar em poder apenas das partes que farão a troca de informações.

Já para a chave assimétrica, conhecida também como chave pública, há uma chave pública de conhecimento geral que cifra a informação, porém, para decifrar a informação há somente outra chave, chave privada, que fica em poder de quem de fato pode ler a informação.

Sabendo da chave pública não se consegue chegar à chave privada correspondente, porém se relacionam por meio de algum dos algoritmos existentes. Hoje em dia, há algoritmos que são considerados os mais seguros e práticos para se trabalhar, segundo o Professor Rezende do Departamento de Ciência da Computação - CIC da UNB, 2012.

1.2 Tecnologia - Hash

É uma função em que dada um valor na entrada é fácil calcular o valor da saída, porém, dado o valor da saída é improvável calcular e chegar ao valor da entrada.

O Professor Barros do curso de Pós-Graduação, Redes de Computadores, do UNICEUB cita como exemplo claro a quebra de um prato e o resultado do seu novo estado.

> A quebra de um prato é um bom exemplo de função unidirecional. É fácil quebrar um prato em um milhão de pedaços, entretanto não é fácil juntar todos os pequenos pedaços de forma a formar novamente o prato original (BARROS, 2012, p.12)

Isso porque a função *hash* é uma operação matemática que ao receber certo valor (Ex: 35 bytes) na entrada transforma-o em um novo valor e normalmente menor na saída (Ex: 15 bytes), esse novo valor é o *hash*.

Na resolução nº 62 de 2009 o CG da ICP-Brasil informam algumas definições para que se entenda melhor o documento, entre elas está a seguinte definição para função *hash.*

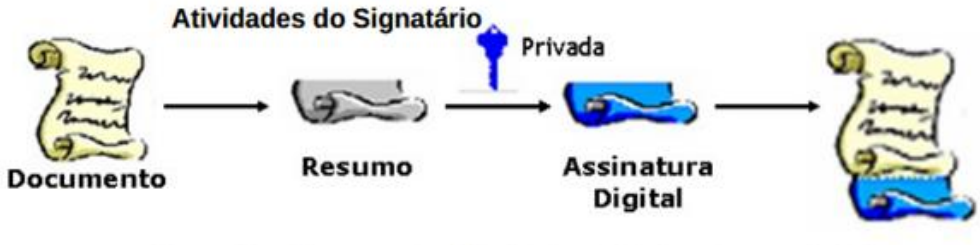
> 3.13 Função hash - uma transformação matemática que faz o mapeamento de uma sequencia de bits de tamanho arbitrário para uma sequencia de bits de tamanho fixo menor conhecido como resultado hash ou resumo criptográfico de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash (resistência à colisão) e que o processo reverso também não seja realizável (dado um resultado hash, não é possível recuperar a mensagem que o gerou) (ITI, 2009)

O uso da função hash é bastante utilizado em assinaturas digitais, já que para uma sequência de bits analisado de uma informação é gerado um valor único e caso essa informação seja modificada um novo valor será gerado.

A assinatura digital se dá quando uma das partes gera um hash do documento (resumo criptográfico) e com sua chave privada criptografa esse resumo, gerando então a assinatura digital.

Posteriormente ele associa ao documento, do qual foi gerado resumo criptográfico (hash) a assinatura para que possa ser validado pelo receptor. Abaixo a figura exemplifica essa operação.

Figura 1 - Assinatura Digital.



Fonte: Certificação Digital - CASAGRANDE

1.3 Certificado Digital

"Na prática, o certificado digital funciona como uma carteira de identidade virtual..." (ITI, 2012).

"É uma técnica de criptografia de informações em geral, que permite que identifique corretamente qualquer pessoa física ou entidade jurídica..." (CARUSO; STEFFEN, 2006, p. 184).

Essas afirmações são concepções claras e objetivas do que venha a ser a certificação digital.

Uma identidade virtual que identifica de maneira segura seu autor e caso ele queira fazer alguma transação e/ou se identificar de maneira segura utiliza o certificado para tal fim, por meio de operações matemáticas/lógicas, consegue fazer todo o processo de maneira segura garantindo a integridade dos dados.

> Os certificados digitais são utilizados para confirmação da identidade na Internet, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifragem de chaves de sessão, assinatura de documentos com verificação da integridade de suas informações, cifragem de documentos, bases de dados, mensagens e outras informações eletrônicas (CARUSO; STEFFEN, 2006, p. 184)

Essa identidade virtual é gerada e assinada por uma AC considerada de confiança pelos envolvidos, como uma secretaria de segurança pública – SSP que gera um registro civil – RG e nos associa a um número único e exclusivo; a AC também nos associa a um certificado único e exclusivo.

Em um certificado digital emitido pela AC constarão algumas informações que podem identificar uma pessoa, uma máquina ou ainda uma instituição. Entre essas informações do titular constam: nome, CPF, *e*-mail, um par de chaves (pública e privada), nome e assinatura da AC que emitiu.

Essas informações dão a certeza a quem recebe um documento a identidade de quem o produziu, a certeza de estar se relacionado com a pessoa desejada. A AC acaba por agir como um cartório dando fé aos documentos, valida juridicamente.

Já as chaves tem um papel importante, são utilizadas para fazer assinatura digital, criptografia dos dados que poderão trafegar por um meio digital e desse modo garantir o não repúdio, confidencialidade, integridade e autenticidade como se verá a seguir.

1.3.1 Assinatura Digital

Para Caruso e Steffen no livro Segurança em Informática e de Informações a assinatura digital de qualquer conteúdo eletrônico por uma pessoa garante a autenticidade da origem deste (CARUSO; STEFFEN, 2006, p. 184).

Para tal, o certificado digital faz uso de algum algoritmo (RSA, Diffie-Hellman ElGamal, DSA) para gerar um hash. O emissor utiliza sua chave privada para criptografar o hash, nesse momento é gerada a assinatura que é enviada juntamente com o documento para o recepto..

Figura 2 - Geração da Assinatura Digital

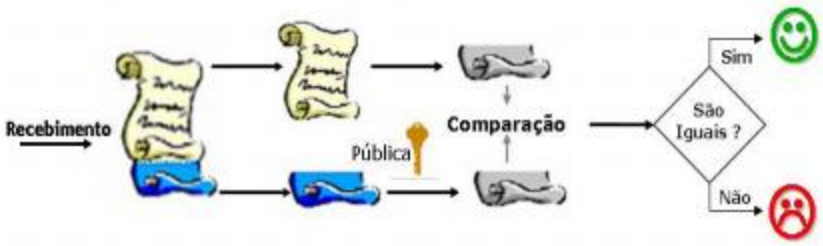
Fonte:Certificação Digital - CASAGRANDE

Quando o receptor recebe o documento assinado ele gera um novo *hash,* utilizando o mesmo algoritmo que o emissor usou, do documento e compara com o *hash* gerado após descriptografar a assinatura utilizando sua chave pública.

Se o *hash* atual e o original tiverem o mesmo valor o documento não foi alterado, caso contrário o documento foi adulterado ou o par de chaves utilizadas não eram relacionadas.

Assim garante-se a integridade do documento, a autenticidade, a confidencialidade e o não repúdio.

Figura 3 - Checagem da Assinatura



Fonte:Certificação Digital - CASAGRANDE

1.3.2 Garantias e Validade Jurídica

A garantia e a validade jurídica para um documento, que não se dê no meio eletrônico, é o fato de alguém atestar sua veracidade, ou seja, um cartório atestar que o documento é verdadeiro ou que da fé ao mesmo por meio de checagem do original e a pessoa que o apresenta.

Já para um documento em meio eletrônico se dá por meio do certificado digital emitido por uma AC que acabam por fazer o papel do cartório.

> Para a prevenção deste tipo de situação, surgiu a certificação digital. Seu funcionamento pode ser comparado a de um serviço notarial efetuado pelo tabelião. Fundamenta-se na existência de uma autoridade certificadora [responsável pela emissão do certificado digital] que possui registrado, em sua base de informações, a chave pública [usada para decifrar a mensagem – criptoanálise] do emissor do documento. Através de mecanismos próprios, a autoridade certificadora pode identificar como original o documento do emissor e, a partir desta comprovação, certificar, com uma assinatura digital própria, a autenticidade do documento eletrônico. (VOLPI; MARLON, *apud* RESENDE, 2009, p., 117).

Conforme abordado pela Profª Dilma A. Resende, mesmo usando certificado digital emitido por uma AC confiável há ainda a possibilidade de termos fraudes, alguém falsificar um certificado digital, ou a AC ser atacada e emitir certificados com finalidades criminais.

Nesses casos a pessoa fica sujeita a responder criminalmente como se tivesse cometido falsificação, adulteração de informações e documentos na forma de papel (física) para obter vantagens.

Além disso, a responsabilidade maior é da AC conforme a Profª Dilma relata.

> "É notório que as fraudes podem ocorrem tanto no mundo físico quanto no digital, e esse problema é inerente ao ser humano... Importante lembrar que a falsificação de uma certidão digital tem as mesmas consequências jurídicas que a falsificação de uma certidão de papel (física). (RESENDE, 2009, p.117).

No caso da empresa pública mencionada nesse trabalho o uso do certificado digital teria papel fundamental para validar, autenticar e certificar petições eletrônicas elaboradas pela equipe de advogados da empresa.

1.4 Autoridade Certificadora – AC

Mas o que é uma Autoridade Certificadora?

AC é uma entidade responsável por emitir, distribuir, revogar, gerenciar certificados, além disso, disponibilizar uma lista com certificados revogados e manter sob sua guarda informações de registros.

A ITI em sua página na internet (O que é certificado Digital?) informa que uma AC é considerada a terceira parte de confiança que acaba por relacionar as chaves com o respectivo dono, pois, por meio dela é que são obtidos os certificados.

Além disso, uma AC pode, segundo Casagrande, assinar digitalmente um certificado usando sua chave privada mediante a uma solicitação e checagem de informações do solicitador, assim o mesmo terá uma credencial confiável para ser usada em uma infraestrutura de chave pública (CASAGRANDE, 2011, p.14).

No caso da ICP-Brasil ela é a AC-Raiz que é a responsável por emitir certificados as outras ACs, com isso executa políticas e normas emitidas pelo Comitê Gestor “...compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu.” (ITI, 2012).

Entidades públicas e privadas podem vir a se tornar uma AC. Elas se submetem a AC-Raiz atuando conforme as normas e políticas geradas pelo Comitê Gestor.

A empresa citada no trabalho não é uma AC vinculada a AC-Raiz e muito menos uma AC Autônoma, desse modo, não gera seus certificados. Contudo, à época houve um estudo de viabilidade da mesma vir a ser tornar uma.

Chegou-se a conclusão que apesar de atender aos critérios para credenciamento de AC divulgados pela ITI no documento **Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil** (ITI, 2012) a empresa não tinha estrutura física para atender aos requisitos de geração, gerenciamento e guarda das informações e certificados digitais.

O custo para montar o parque tecnológico (equipamentos, tecnologia de geração, treinamento, manutenção e etc), gerenciamento e guarda (segurança física) e posteriormente gerar para seus funcionários ficaria muito à cima do que simplesmente adquirir diretamente de uma AC credenciada a ICP-Brasil.

Ademais, não seria possível a empresa se tornar uma AC Autônoma, porque, como um dos objetivos do certificado digital era o uso em petições e processos jurídicos os mesmos precisavam ter a confiança de um certificado digital emitido por uma AC da hierarquia ICP-Brasil.

1.5 Obtendo um Certificado Digital

Para obter um certificado digital deve se escolher uma AC cadastrada na AC-Raiz. A hierarquia das ACs encontra-se em: http://www.iti.gov.br/images/icp-brasil/estrutura/atualiza%C3%A7%C3%A3o15/Estrutura_completa.pdf.

Posteriormente, escolher dentro da AC qual é o tipo de certificado que vai requerer; A1 (validade de um ano e armazenado no computador), A3 (validade de cinco anos e armazenado em cartão e/ou *token*) são os mais comercializados para pessoas jurídica e física.

As ACs mais conhecidas são: AC Serpro, AC Caixa Econômica Federal, AC Serasa Experian, AC Receita Federal do Brasil, AC Certisign, AC JUS entre outras.

A ICP presta mais informações dessas e outras ACs, o seguinte link http://www.iti.gov.br/index.php/icp-brasil/estrutura é possível consultá-los.

Há também a possibilidade de obter o certificado por meio de uma Autoridade de Registro (AR) que é uma entidade vinculada a uma AC que simplesmente encaminham as solicitações de certificados após fazerem a identificação e registro de usuários.

2 CENÁRIO DA EMPRESA

2.1 Metodologia

Para a obtenção das informações foi feita entrevista junto aos funcionários que ainda trabalham na área e participaram do projeto. Não houve a possibilidade de se estudar e pesquisar uma documentação que tivesse se aprofundado em relatar todo o projeto.

As entrevistas foram agendas com os funcionários separadamente, não houve necessidade deles responderem a um questionário pronto, apenas as perguntas que iam surgindo conforme iam relatando.

2.2 Cenário à época

O objetivo e justificativa da aquisição dos certificados digitais à época foram os de atender a dois aplicativos eletrônicos. Um que trabalharia com gerenciamento de identidade e controle de acesso e outro com gestão de documentos jurídicos.

Paralelamente a isso, visava dar a possibilidade de agilizar a disponibilidade dos documentos com autenticidade, irretratabilidade e respaldo jurídico exigido junto a órgãos e entidades da administração direta e indireta que seriam gerados pela ferramenta de gestão de documentos jurídicos.

Já para a ferramenta de gerenciamento de identidade e controle de acesso, seria o de possibilitar aos empregados que efetuassem a autenticação em suas estações de trabalho de maneira mais rápida e segura, contudo não é o que ocorre hoje.

Nos documentos analisados não há outros motivos como: venda de certificados para terceiros, certificação de equipamentos internos ou processos, assinatura de documentos criptografados e etc. Ações e procedimentos atendidos por um certificado digital e que dariam respaldo ainda maior na justificativa de aquisição.

Posto isso, pois, há uma ressalva na justificativa de que a aquisição atende a um dos objetivos do plano estratégico de tecnologia da informação da empresa, **garantir a segurança da informação: promover a segurança da informação.**

Mas tal objetivo não está sendo atendido na integra, a não ser por alguns e-mails que são assinados. É importante salientar que há pessoas na área de segurança que não dispõe de certificado digital.

Em entrevistas com um empregado ele ressalta que, à época, como havia o projeto de aquisição da ferramenta de gerenciamento de identidade e controle de acesso foi posto no escopo deste projeto uma referência ao uso de certificado digital, justificando dessa maneira por outro projeto a aquisição dos certificados.

Foi encontrado uma justificativa para o treinamento dos funcionários que iriam fazer o gerenciamento dos certificados digitais, um treinamento oficial oferecido pela empresa fornecedora dos certificados que oferecia o conhecimento aos participantes para avaliar, criar, implementar e gerenciar os certificados digitais que seriam usados pela empresa pública.

Atualmente há um funcionário que participou do treinamento ligado ao projeto de certificação digital.

2.2.1 Ferramenta de Gerenciamento de Identidade

Como dito anteriormente, uma das duas justificativas era que o certificado digital atendesse à ferramenta de gerenciamento de identidade.

No projeto de aquisição, um dos requisitos a ser atendido era que a ferramenta deveria suportar autenticação utilizando certificado digital X.509. Os projetos idealizados dessa maneira justificaram a aquisição um do outro.

Ao longo dos projetos verificou-se que os atributos do certificado digital escolhidos como obrigatórios não atendiam aos atributos necessários para se fazer a autenticação pela ferramenta.

Somado a isso, verificou-se que o desenvolvimento de parte da ferramenta de gerenciamento de identidade e acesso foi feita de maneira errada. A ferramenta fazia o controle de identidade e acesso via *Active Directory* da *Microsoft,* sem haver “ativado” também via certificação digital.

A empresa contratada não foi informada ao longo do projeto que a ferramenta de fato iria trabalhar com os certificados para autenticar os usuários quando fossem fazer *login* nas estações de trabalho.

Quando a mesma fez a análise dos atributos utilizados pela ferramenta verificou-se que ela trabalhava com um atributo imutável e obrigatório (CPF) e que no certificado não havia nenhum que atendesse a esse requisito. No certificado, além de nome e outras informações que podiam mudar, estava o e-mail do usuário utilizado na empresa como obrigatório.

As soluções propostas seriam: a revogação dos certificados, até então emitidos, emitir novos certificados com o campo CPF como obrigatório para atender a ferramenta e adequá-la para trabalhar com o certificado digital em relação a autenticação e controle de acesso.

Essas soluções foram descartadas pela gerência da área com a justificativa que demandaria tempo e custos. Não atentou para o fato de que mais tarde poderia responder a uma auditoria pelo descumprimento de atender aos objetivos do projeto, o que ocorreu.

Infelizmente não foi possível ter acesso aos documentos de questionamento e resposta para os objetivos não atendidos do projeto.

2.3 Aquisição

Em 2009 por meio de Adesão à Ata de Registro a empresa pública deu início ao projeto para certificar digitalmente seus empregados. A empresa privada ganhadora começou em 2010 a emitir os certificados.

A empresa ganhadora teve que fornecer os certificados do tipo A1, A3 e *tokens,* estes foram entregues aos empregados que se achavam em um dos critérios criados pela empresa.

Foram gerados e entregues mais de 10 mil certificados e *tokens*.

2.4 Critério Utilizado na Distribuição

Nas análises dos documentos disponibilizados são relatadas de forma simples a quantidade de certificados que seriam emitidos:

- 2500 certificados e tokens para empregados de função de confiança que utilizavam a ferramenta de gestão de documentos jurídicos;
- 1000 certificados e tokens para empregados que iriam assinar e-mails;
- 6000 certificados e tokens para empregados novos (novos contratados);e
- 500 certificados e tokens para contingência em casos de perda e revogação.

Nessa etapa abre-se um parêntese para uma brusca mudança, a geração de 30 (trinta) certificados do tipo A1 para equipamentos servidores da empresa. Não há relato do motivo dessa nova aquisição.

Com base no exposto acima, verificou-se que foi montado um cronograma com datas e locais a serem visitados para coleta de dados, emissão e entrega dos certificados e tokens.

Contudo, nas entrevistas com os empregados que participaram nas coletas de dados, emissão e entrega de certificados e tokens informaram que não havia um critério de quem seriam essas pessoas de confiança e quem seriam esses demais empregados a receber.

Para eles não houve nenhuma análise de quem, de fato estando em cargo de confiança, deveria ter o certificado, visto que, uma das entregas era para um empregado (em cargo de confiança) que morava a mais de 200km do local de entrega tomando conta de uma antena de transmissão.

Em outros casos tiveram que voltar por diversas vezes ou para emitir ou apenas entregar os certificados.

Um dos entrevistados informou que, apensar de ter o certificado, não o utiliza em nada, nem assinando e-mails.

b

2.5 Problemas de Gerenciamento e Entrega

Durante a emissão dos *tokens,* as pessoas que estavam à frente dessa tarefa tiveram alguns problemas que são expostos a seguir. Espera-se com isso que sirvam de base para não serem repetidos por pessoa e/ou entidade.

Além disso, as sugestões serão dadas com base nesses problemas relatados para que não venham a ser repetir, são eles:

Quadro 1 - Problemas e Impactos

NÚMERO	PROBLEMA	IMPACTO
1º	Ausência de Infraestrutura solicitada	1. Impacto no processo de envio de documentos e recebimento das aprovações; 2. Dificuldade em acessar equipamentos; 3. Comprometimento em impressão de documento; 4. Comprometimento no envio de documentação; 5. Parada do serviço e/ou impossibilidade de execução.
2º	Ausência de quem receberá o certificado na data/hora determinado	1. Demora na entrega do certificado; 2. A não emissão do certificado.
3º	Preenchimento incorreto de formulário, dificuldade de entender informações ou a não realização do cadastro para compra do certificado	1. Retrabalho de preenchimento e/ou entender preenchimento junto ao solicitante; 2. Demora em fazer cadastro e solicitar compra de certificado; 3. Demora na geração de certificado.
4º	Não fazer registro de modo correto das emissões e entrega dos certificados	1. Incerteza da quantidade de certificados emitidos; 2. Incerteza de quem recebeu os certificados; 3. Falta de prova material/documental caso seja feita uma auditoria; 4. Problemas com pagamento junto a AC.
5º	Emissão de certificado para empregados que não precisam	1. Gasto desnecessário com emissão; 2. Gasto desnecessário com envio de equipe para emissão entrega coleta e checagem de documentos; 3. Falta de critério para emissão.

6º	Envio de várias equipes em datas diferentes para entrega, emissão, coleta e checagem de documentos no mesmo local	1. Gasto desnecessário no envio de equipes para o mesmo local em datas diferentes; 2. Demora na conclusão de emissão para uma localidade.
7º	Não definir de modo correto os campos	1. Problemas de uso com ferramentas que façam uso do certificado digital; 2. Revogação de certificado digital para adequação; 3. Emissão de novo certificado com os campos corretos.

Fonte: Autoria própria

Esses problemas foram os citados pela equipe que trabalhou à frente na emissão, entrega de certificados, coleta e checagem de documentos dos empregados da empresa pública.

Juntamente a esses destacamos um problema que é considerado gravíssimo e relatado por eles, a falta de documentação comprovando a entrega dos certificados emitidos para os empregados.

Um dos entrevistados informou que, por própria teve a iniciativa em gerar 3 (três) vias de recebimento/entrega do certificado, onde:

- Uma via ficava com o empregado que recebeu o certificado;
- Uma via com a empresa ganhadora que emite o certificado;e
- Uma via com a empresa pública para controle pessoal.

Contudo essa iniciativa não pode impedir que em meados do final de 2011 uma equipe de auditores internos da empresa questionasse os valores pagos e a quantidade emitida de certificados, já que a empresa fornecedora alegava ter emitido certificados e ainda não ter recebido.

3 SUGESTÕES DE MELHORIAS

As sugestões tendem a ajudar e auxiliar a empresa pública citada no trabalho, a outros órgãos da administração direta e indireta, pessoas que visam fazer uso de certificado digital e a quem queira obter experiências e sugestões para projeto parecido.

Entenda essas sugestões como uma maneira de se evitar erros cometidos por essa empresa pública e seus gestores. Esteja livre para utilizar, moldar, transformar as sugestões e o documento que consta no apêndice.

3.1 Falta de Comprovante de Entrega

Como foi abordado no final do capítulo 2, começarei com o problema de não documentar os certificados entregues.

É sugerido que seja elaborado um documento e que seja impresso em pelo menos 3 (três) vias para controle da entrega do certificado.

Neste documento deve constar no mínimo: nome de quem recebe o certificado, nome de quem entrega o certificado, data, local e hora da entrega, especificidade do uso do certificado (em que se pode usá-lo), *checkbox*: **entregue, recusado, pendente** e campo para observações do *checkbox* e demais que possam ser acrescidas ao documento.

Este observador montou um modelo que serve de base e pode ser alterado, adequado ou usado por quem se interessar por este trabalho. O modelo se encontra no **Apêndice A**.

3.2 Planejamento para aquisição

Recomenda-se que a empresa, juntamente com sua equipe, faça um planejamento e estudo de viabilidade na aquisição de novos certificados digitais usando para tal metodologia e boas práticas disponíveis no mercado, tais como:

PMBOK para gerenciar o projeto, Instrução Normativa 04 de para aquisição de soluções de TI, ITIL para entrega de serviço e até desenvolver e adequá-las a seu cenário, COBIT para controle de processos de TI, BSC – planejamento e estratégia de gestão entre outros.

3.3 Demais problemas

Para os problemas apontados na tabela 1 – Relação de Problemas seguem as sugestões de melhoras:

1. **Ausência de Infraestrutura solicitada:** sugere-se, caso não eleve o custo para empresa, *kits* de equipamentos leves para a equipe (notebook, modem 3G/Discagem, impressora e scanner portáteis). Caso não seja possível os equipamentos solicitados devem estar montados, checados e testados.
2. **Ausência de quem receberá o certificado na data/hora determinado:** Sugere-se que seja relatada no documento de entrega/recebimento de certificado digital a ausência de empregado na data e local. Sugere-se que caso empregado a qualquer momento venha requerer o seu certificado seja lhe cobrado um valor. Casos excepcionais deverão ser analisados. Nos casos da administração pública direta e indireta, sugere-se que, o servidor/empregado deverá responder processo administrativo e arque com os gastos para adquirir e buscar seu cerificado digital.
3. **Preenchimento incorreto de formulário, dificuldade de entender informações ou a não realização do cadastro para compra do certificado:** Sugere-se que haja uma pessoa responsável por checar e conferir documentos e preenchimento de formulários. Sugere-se que se tenha um número de contato telefônico para auxílio e/ou sejam confeccionados materiais explicativos e sejam entregues aos interessados antes dos mesmos retornarem com os documentos para entregarem e

receberem os certificados. Sugere-se que sejam divulgados como preencher formulários e quais documentos apresentar de forma ampla por meio impresso, digital (site, blog, fóruns etc), e palestras.

4. **Não fazer registro de modo correto das emissões e entrega dos certificados:** Sugere-se que equipe seja bem treinada no ambiente de coleta, emissão e checagem de informações e certificados digitais. Sugere-se a entrega de vias para o interessado no certificado digital e a coleta de assinatura nas vias que ficarão com a empresa emissora e com o emissor. Sugere-se que ao final do trabalho seja conferida a quantidade de certificados emitidos pela empresa com as vias assinadas, como forma de checagem certeza de entrega (modelo APENDÊNCIE A). Sugere-se que tais documentos sejam arquivos.
5. **Emissão de certificado para empregados que não precisam:** Sugere-se critérios mais rigorosos para emissão de certificados. Sugere-se que em caso de lista com nomes sejam checados e qual é a real função exercida pela pessoa. Sugere-se que seja bem acordo entre as áreas requisitantes com seus representantes e a área de emissão de certificados digitais. Sugere-se nesse caso o apoio da alta diretoria, RH, equipe de certificados digitais para informarem custos, benefícios, trabalhos desenvolvidos e interessados.
6. **Envio de várias equipes em datas diferentes para entrega, emissão, coleta e checagem de documentos no mesmo local:** Sugere-se elaboração de cronogramas em cima do que ficar acordado em relação às pessoas que irão receber os certificados digitais. Sugere-se que seja checado se as pessoas estarão no local para receber certificados digitais caso haja necessidade do envio de equipe. Sugere-se que o número de pessoas na equipe aumente nos casos em que o número de interessados for alto, montar uma força tarefa.
7. **Não definir de modo correto os campos:** Sugere-se que as áreas interessadas no certificado digital deixem claro em que será usado o certificado digital e dessa forma definir quais campos

> (atributos) devem ser utilizados como preferencial para transações, consultas e qualquer outra ferramenta que faça uso de certificado digital. Sugere-se que sejam utilizados campos com informações que não são voláteis. Ex: CPF, CNPJ, data de nascimento, registro funcional.

Ainda sugere-se, no caso da administração pública direta e indireta, que a elaboração do projeto de certificação digital siga algumas normas e melhores práticas, tais como:

A Instrução Normativa nº 04 de 2010 diz como proceder para contratação de serviços de TI. Elaboração de equipes que irão escrever termos, analisar ferramentas, justificativa de eficiência, eficácia e economia, justificativa de retorno de benefícios, analisar financeiramente a ferramenta e outros passos estão relatados nesse documento disponível pelo Ministério do Planejamento, Orçamento e Gestão (BRASIL,2010).

É sugerido ainda que seja adotado algum método de boas práticas para gestão de projeto como o PMBOK, que orientarão de que modo o projeto pode ser tocado, visto que, se tornar uma AC, AR, PSS ou simplesmente solicitar certificados requer tempo e responsabilidade no trato de informações de terceiros.

Ainda para os órgãos da administração pública direta e indireta sugere-se que a equipe que estará à frente do projeto documente muito bem desde o princípio; no caso envolvendo as trocas de e-mails com fornecedores, relatórios de prova de conceito referente a softwares, relatórios de equipamento físicos, emissões de certificados de treinamento, documentos referenciados pela IN 04/2010, histórico e justificativas para aquisição do certificado digital, emissões e etc.

Essa sugestão pode ser acatada por uma empresa não governamental para dar maior controle e seriedade ao seu projeto, no caso de alguns órgãos públicos essas informações são mantidas em pastas, documentos. Nada impede de estarem em forma digital armazenadas em CDs, DVDs ou servidores.

É importante informar que a elaboração, guarda, descarte de documentos e informações referentes a emissão, revogação e qualquer outras de certificados digitais também seguem um padrão dito pela ICP-Brasil.

3.4 Sugestões para a empresa pública

Para a empresa pública, além do abordado nos itens anteriores, é sugerido que caso a empresa opte pela emissão de novos certificados use a IN 04/2010 para geração dos documentos que servirão de base e justificativa para a contratação e adote as boas práticas do PMBOK para gerir esse novo projeto.

Sugere-se que seja aberta nova pasta e nela sejam postas todas as informações e documentos, tais como: análise de demanda, termo de abertura, cenário da empresa, análise de risco, estratégia de contratação, plano de sustentação para contratação, análise de viabilidade, caderno técnico, e-mails, atas de reunião, edital de contratação, contrato firmado com empresa ganhadora e etc.

Essas informações e documentos poderão ser utilizados para responder a novos questionamentos da equipe de auditoria e também a questionamentos do Tribunal de Contas da União – TCU.

Ainda sugere-se que seja revisado o critério de emissão de certificados digitais para os atuais detentores, que o escopo seja diminuído fazendo com que emissões desnecessárias sejam evitadas. Além disso, verificar junto ao RH se empregados ainda trabalham na empresa e junto aos responsáveis pelas áreas o que eles realmente fazem, qual a função desempenhada, que papel e grau de importância têm para a empresa.

Sugere-se que caso a empresa opte por novas emissões estude a possibilidade de não enviar equipe aos locais, mas dar treinamento para 02 (duas) pessoas da localidade fazerem a coleta, checagem, emissão e entrega dos certificados digitais. Se possível verificar a possibilidade de cada localidade se tornar uma AR vinculada a empresa ganhadora responsável pela emissão dos certificados visto que os locais não são muitos e podem ser divididos por regionais.

Não é recomendado, no cenário atual e para o objetivo de autenticação do projeto, que todos os funcionários da empresa tenham certificados digitais, visto que a ferramenta de gerenciamento de identidade e controle de acesso não está utilizando o certificado como forma de autenticação.

Não é recomendado à empresa que se torne uma autoridade autônoma, visto que os empregados da área jurídica trabalham com processos que requerem confirmação de uma autoridade confiável para os processos. Nesse caso, uma autoridade autônoma não é submetida a AC-Raiz ou a outra vinculada a ela.

CONCLUSÃO

É notório que a certificação digital vem desempenhando papel de extrema importância a cada dia.

Ações que antes demandavam tempo, pilhas e pilhas de papéis devido à burocracia, filas quase intermináveis para se obter informações ou entregar documentos comprovando quem você é quem diz ser tendem a ficar no passado.

O uso de certificado digital em transações bancárias, troca de e-mail, assinatura de documentos criptografados ou não, transações cibernéticas como o site Comprasnet, entrega de impostos já é um começo que facilita em muito a vida do cidadão.

Contudo, no caso da empresa pública mencionada no trabalho, ela restringiu-se ao uso em processos jurídicos e assinatura de e-mail por parte de alguns empregados. Demonstra dessa maneira, um desconhecimento do real potencial do certificado digital e as reais possibilidades de seu uso.

Caso os certificados venham a se restringir apenas ao uso com os processos jurídicos a empresa pode fazer parceria com a OAB que já entregam aos seus profissionais carteiras de identificação contendo certificação digital. Quanto aos demais empregados utilizarem o certificado para assinar e-mails a empresa deveria rever a real necessidade.

Entretanto, a empresa poderia traçar e explorar novos objetivos antes não visados, tais como:

- Ser uma autoridade certificadora;
- Vender serviço de certificação digital para seus clientes;
- Explorar o certificado digital junto a outras ferramentas;
- Usar o certificado digital como forma de validar o acesso as estações;
- Usar o certificado digital como forma de validar o acesso a rede quanto ao uso de equipamentos móveis;
- Aumentar o uso do certificado digital para documentos;
- Usar o certificado digital como chave para acesso a VPN;e

- Explorar o uso do certificado digital junto as aplicações web da empresa.

Essas são algumas possibilidades que podem ser exploradas tanto pela empresa como por outra entidade ou pessoa que queira adotar a emissão de certificados digitais e não sabe por onde começar ou tenha dúvidas em que pode ser usado.

A venda de serviço já é algo real e presente em muitas empresas e no caso da área de TI da empresa mencionada no trabalho é uma forma dela começar novo projeto e poder se sustentar. Além do lucro da venda dos certificados, terá receita para investir em outros projetos da própria área.

Essa é uma demonstração de verba pública bem aplicada e gestão pública bem organizada, eficaz e eficiente.

REFERÊNCIAS

BARROS, Eduardo Gomes de. **Criptografia**. Material Didático disponível aos alunos do curso de Pós-Graduação Lato Sensu Rede de Computadores com Ênfase em Segurança. Brasília, 2012;

BRASIL, **Medida Provisória nº 2.200-2/01**. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. 2001. Disponível em: <http://www2.camara.leg.br/legin/fed/medpro/2001/medidaprovisoria-2200-2-24-agosto-2001-391394-publicacaooriginal-1-pe.html>. Acesso em 25 nov 2012;

CARUSO, Carlos A. A.; STEFFEN, Flávio D. **Segurança em Informática e de Informações**. 3ª ed. Rev. e Ampl. – São Paulo: Editora SENAC, 2006. P. 183-189;

CASAGRANDE, Airton Ruberval. **Certificação digital**. Trabalho de Conclusão de Curso (Especialização) – Universidade Tecnológica Federal do Paraná, Curitiba, 2011. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/handle/1/392>. Acesso em: 17 dez. 2012;

ITI - Instituto Nacional de Tecnologia da Informação. **O que é Certificação Digital?**. 2012.Disponível em: <http://www.iti.gov.br/index.php/certificacao-digital/o-que-e>. Acesso em: 25 nov. 2012;

ITI - Instituto Nacional de Tecnologia da Informação. **RESOLUÇÃO Nº 62, 09 de Janeiro de 2009,** 2009. Disponível em: <http://www.iti.gov.br/images/icp-brasil/legislacao/Resolucoes/Resolucao_62.pdf>. Acesso em 20 dez 2012;

RESENDE, Dilma A. Revista Jurídica UNIGRAN. **Certificado Digital**. Mato Grosso do Sul; v. 11, p. 111-122, 2009. Disponível em: < http://www.unigran.br/revistas/juridica/ed_anteriores/22/artigos/artigo09.pdf>. Acesso em: 04 jan. 2013;

REZENDE, Pedro A. D. **Algoritmos Criptográficos de Chave Pública**. Universidade de Brasília – UNB – IE – Ciência da Computação: Segurança de Dados, Brasília, 2012. Disponível em: <http://www.cic.unb.br/docentes/pedro/segdados_files/CriptSegC.pdf>. Acesso em: 18 dez. 2012;

APÊNDICE A – Modelo de Controle de Entrega de Certificado Digital

Termo de Recebimento/Entrega – Certificado Digital

Brasília, 29 de agosto de 2012.

Eu, _____ empregado público da Empresa XXXXX, detentor do RG XX.XXX.XXX-X, sob a matrícula XX.XXX-XX. Declaro para os devidos fins de comprovação ter recebido meu certificado digital na presente data e local.

Eu, _____ empregado público da Empresa XXXXX, detentor do RG XX.XXX.XXX-X, sob a matrícula YY.YYY-YY. Declaro para os devidos fins de comprovação ter entregado ao empregado a cima relacionado o certificado digital na presente data e local.

Certificado Digital foi/está:

- ☐ Entregue
- ☐ Recusado
- ☐ Pendente

Observações:

Estar ciente quanto ao uso:

1. Será usado para assinatura de e-mail, documentos de qualquer natureza (petições, atas de reunião, termos de abertura e etc), acesso ao *site* da Receita Federal, transações eletrônicas e autenticação na estação de trabalho;
2. Terá mesma importância de documentos assinados de forma manuscrita;
3. Não passar, emprestar, dar, conceder e/ou divulgar senha de uso do certificado;
4. Não passar, emprestar, dar, conceder e/ou compartilhar o certificado digital;
5. Torna-se responsável por qualquer documento assinado por seu certificado digital, podendo responder nos termos da lei;
6. Caso perca, entrar em contato com Fulano da Silva pelo ramal 7711 para revogação do certificado digital e procedimentos para adquirir outro certificado.

(Beltrano das Condocas – Matrícula XX.XXX-XX)

(Fulano da Silva – Matrícula YY.YYY-YY)