UNIVERSIDADE FEDERAL DE MINAS GERAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA
CURSO DE ESPECIALIZAÇÃO EM AUTOMAÇÃO INDUSTRIAL

CERTIFICAÇÃO DIGITAL

Natália Vartuli Cordeiro e Silva

Monografia submetida à Banca Examinadora designada pela Comissão Coordenadora do Curso de Especialização em Automação Industrial, como parte dos requisitos necessários à obtenção do Certificado de Especialista em Automação Industrial.

Orientador: Prof. Luciano de Errico

Belo Horizonte
Fevereiro, 2011

Dedico este trabalho aos meus pais, pelas lições de vida e amor, ao meu irmão por sempre estar ao meu lado e ao meu noivo Cristiano, pela paciência, compreensão e incentivo.

Resumo

O cenário tecnológico atual exige formas de garantia de autenticidade, confiabilidade e integridade nas transações por meio eletrônico, sem a presença física das partes envolvidas. Para esse objetivo foi criado o Certificado Digital, que equivale a uma carteira de identidade virtual e permite a identificação de uma pessoa no meio digital/eletrônico, quando do envio de uma mensagem ou em uma transação pela *Internet* que necessite de validade legal.

Este trabalho tem por objetivo introduzir o assunto de Certificação Digital, apresentando seus principais requisitos e os problemas de segurança no desenvolvimento de sistemas e documentos eletrônicos confiáveis.

Palavras chave: Certificado Digital, Criptografia, Chave Pública.

Lista de Abreviaturas, Siglas, Acrônimos e Glossário

AC - Autoridade Certificadora
AR – Autoridade de Registro
ICP - Infra-estrutura de Chaves Públicas
DES - *Data Encryption Standard*
PKCS – *Public Key Cryptography Standards*
ITU-T - *International Telecommunication Union – Telecommunication Standartization Sector*
IEC - *International Electrotechncal Comission*
MD5 – *Message Digest 5*
DSS – *Digital Signature Standard*
PRODEMG - Companhia de Tecnologia da Informação do Estado de Minas Gerais
CN - *Common Name*
XML - *eXtensible Markup Language*
SGSI – Sistema de Gestão de Segurança da Informação
SSH – *Secure Shell*
SSL – *Secure Socket Layer*
OU – *Organization Unit*

Sumário

1. INTRODUÇÃO

A *Internet* e os computadores são hoje utilizados para o processamento de dados, troca de mensagens e documentos entre empresas.

A informação eletrônica, através da troca de mensagens e documentos na *Internet*, hoje é tratada e aceita de forma natural nas diversas relações entre empresas. No entanto, estas transações eletrônicas necessitam de mecanismos de segurança capazes de garantir autenticidade, confiabilidade e integridade das informações eletrônicas, o que foi intensificado quando passou a existir uma legislação imputando validade legal à sua utilização. A Certificação Digital é a tecnologia que provê estes mecanismos.

Para se estabelecer um ambiente de certificação digital é preciso ter uma autoridade confiável, que ateste e emita os certificados. Uma ICP (Infra-estrutura de Chaves Públicas) é um órgão, uma iniciativa privada ou pública, que tem como objetivo manter uma estrutura de emissão de chaves públicas, baseando-se no princípio da terceira parte confiável, oferecendo uma medição de acreditação e confiança em transações entre partes que utilizam certificados digitais. A principal função da ICP é definir um conjunto de técnicas, práticas e procedimentos a serem adotados pelas entidades a fim de estabelecer um sistema de certificação digital baseado em chave pública. A ICP do Brasil, definida pela Medida Provisória n.º 2.200-2, de 24 de agosto de 2001, é denominada ICP – Brasil [4]. Já as Autoridades Certificadoras (AC) são entidades de confiança, que emitem certificados digitais para outras entidades, empresas, indivíduos, que precisam se identificar e garantir as suas operações no mundo digital. Cada certificado digital emitido é certificado e garantido pela AC responsável pela sua emissão, que recebe e autentica a solicitação de certificado, emite e cancela digitalmente o certificado e gerencia os certificados emitidos [5].

Com a certificação digital é possível utilizar a Internet como meio de comunicação alternativo para a disponibilização de diversos serviços com uma maior agilidade, facilidade de acesso e substancial redução de custos. A tecnologia da certificação digital foi desenvolvida graças aos avanços da criptografia nos últimos 30 anos. Ela pode ser usada, por exemplo [4]:

- Garantida de sigilo e privacidade de *sites* – Em um *site* "seguro", o computador recebe o certificado contendo a chave pública, criptografando todas as informações de envio para o *site*, fazendo com que apenas o servidor possa compreender o real significado da informação.

- Controle de acesso a aplicativos – O *software* pode solicitar ao usuário que apresente um certificado digital em vez de digitar a permissão de acesso com o nome do usuário e senha, assim o usuário não coloca em perigo a aplicação por falta de cuidado no uso e na armazenagem da senha.
- Assinaturas de formulários – Os usuários poderão assinar eletronicamente os formulários preenchidos pela *web*, da mesma maneira que fariam pessoalmente em um balcão de atendimento.
- Garantia de sigilo e privacidade de *e-mail* – Pode-se selar a correspondência em um "envelope digital criptográfico", certificando-se de que apenas o destinatário será capaz de compreender seu conteúdo.
- Identificação de remetente – Não existirão mais dúvidas sobre a origem de uma mensagem, pois será possível comprovar a identidade do emissor.
- Assinatura de mensagem e impossibilidade de repúdio – As mensagens de correio eletrônico ou qualquer documento digital passam a valer como documento assinado, com validade jurídica, dispensando o uso do papel. O serviço de não repúdio impede que uma parte envolvida na comunicação venha a negar a sua participação em qualquer momento da comunicação.

Neste trabalho é focado o tema do Certificado Digital, documento eletrônico que contém o nome, um número público exclusivo denominado chave pública e muitos outros dados que mostram quem somos para as pessoas e para os sistemas de informação. No Capítulo 2 é apresentado um breve estudo sobre a certificação digital e as estruturas mínimas necessárias para a prática da mesma. No Capítulo 3 é apresentado um estudo de caso, que mostra como o certificado digital pode ser utilizado. No Capítulo 4 vem a conclusão do trabalho.

2. SEGURANÇA DA INFORMAÇÃO

Nos dias de hoje, as empresas dependem cada vez mais dos sistemas de informação e da *Internet* para fazer negócios, não podendo se dar ao luxo de sofrer interrupções em suas operações. Um incidente de segurança pode impactar direta e negativamente as receitas de uma corporação, a confiança de seus clientes e o relacionamento com sua rede de parceiros e fornecedores [6].

A segurança da informação refere-se à proteção das informações de determinadas empresas ou pessoas. Na sociedade em que vivemos, seu papel é fundamental, por isso foram criados alguns atributos básicos: confidencialidade, integridade e disponibilidade. A segurança da informação busca reduzir erros, fraudes, roubos e diversos problemas que comprometam os atributos básicos.

Mais do que processos de trabalho bem definidos, profissionais conscientes e capacitados, a segurança da informação requer ferramentas especificas para a implementação das regras contidas nas políticas de segurança [6]. As recomendações de segurança são encontradas em controles físicos e lógicos. Estas recomendações podem ser encontradas em um arsenal de ferramentas, os principais são a identidade, defesa contra ameaças e criptografia, conforme ilustrado na Figura 01.

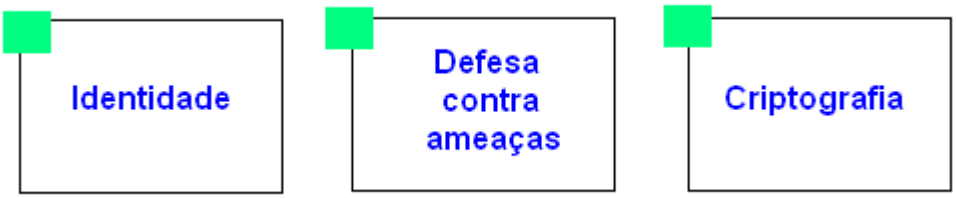

FIGURA 01: Gestão da segurança da Informação.

A gestão de identidade são ferramentas que permitem a correta identificação de um usuário para lhe conferir acesso de acordo com seu perfil [6]. Estas ferramentas podem ser:

- Identificação/Autenticação: Permitem identificar unicamente um usuário e verificar a autenticidade da sua identidade através de mecanismos variados, como por exemplo, senhas pré-definidas, certificados digitais, biometria ou dispositivos portáteis (*tokens, smart cards*).

- Autorização/Controle de Acesso: Possibilitam especificar as ações permitidas e níveis de privilégio diferenciados para cada usuário através do estabelecimento de políticas de uso.
- *Public Key Infrastructure/Certification Authority*: Realizam a geração e gestão de chaves e certificados digitais que conferem autenticidade aos usuários ou à informação. Outra aplicação dessa categoria de ferramentas é o fornecimento de chaves para suportar soluções de criptografia.

Existem diversas soluções atuando na defesa contra ameaças, de forma preventiva ou corretiva [6]. Alguns exemplos de defesa são:

- Proteção do perímetro: Permitem definir uma fronteira, lógica ou física, em torno de um conjunto de ativos de informação e implementar as medidas necessárias para evitar a troca de informação não autorizada através de perímetro.
- Detecção de anomalias e intrusão: Realizam o monitoramento de redes, plataformas e aplicações visando à detecção de atividades não autorizadas, ataques, mau uso e outras anomalias de origem interna ou externa.
- Proteção contra infecção: Garantem que os sistemas e os recursos de informação neles contidos não sejam contaminados.
- Identificação de vulnerabilidades: Ferramentas utilizadas pelos profissionais de segurança para identificar vulnerabilidade nos sistemas existentes.
- *Backup*: Permitem o backup, de forma autorizada, de informações contidas em estações de trabalho e servidores.

A criptografia das informações são mecanismos que garantem a confidencialidade da informação em diversas camadas, através da aplicação de algoritmos de criptografia [6]. Estes temas serão aprofundados mais adiante.

2.1. Criptografia

Chave é um valor matemático que determina como uma mensagem de texto pleno é criptografada para produzir um texto cifrado, e sua posse é requerida para descriptografar o texto cifrado e recuperar a mensagem original. Uma chave tem um correspondente tamanho, que consiste no número de bits (ou em alguns casos bytes) necessários para armazenar a chave. O espaço de chaves de uma chave é a coleção de todos os valores matemáticos que têm

o mesmo tamanho desta chave. Em geral uma chave de tamanho n bits gera um espaço de chaves de 2n valores distintos [4].

A criptografia é uma ciência que usa a matemática (em forma de algoritmos) para ocultar dados (embaralhar informações). Sua lógica é muito simples, o transmissor aplica uma função e criptografa a mensagem original em texto simples, a mensagem resultante em texto cifrado é envida pela rede, e o receptor aplica uma função reversa (chamada de descriptografia) para recuperar o texto simples original. O processo de criptografia/descriptografia geralmente depende de uma chave secreta compartilhada entre o transmissor e receptor. Quando é usada uma combinação adequada de uma chave e um algoritmo de criptografia, é suficientemente difícil para um intruso desvendar o texto cifrado, e o transmissor e o receptor podem estar certos de que sua comunicação é segura [1].

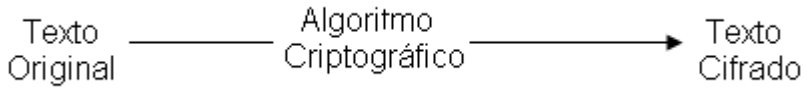

FIGURA 02: Criptografia.

A criptografia é utilizada para garantir a privacidade, mas este não é o único serviço que ela oferece. Ela também pode ser utilizada para garantir a autenticação e integridade do serviço.

Os algoritmos de criptografia são apenas blocos de montagem para a construção de um sistema seguro. A Figura 03 mostra a classificação da segurança de rede.

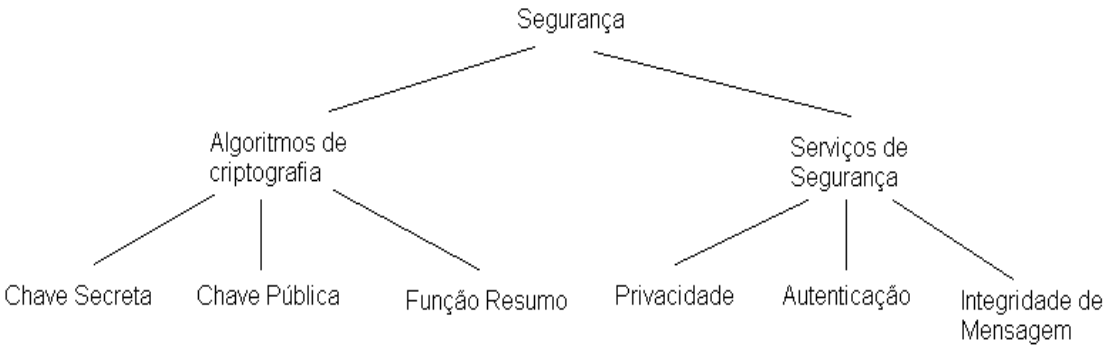

FIGURA 03: Classificação de segurança da rede.

O requisito básico para um algoritmo de criptografia é que ele seja capaz de transformar o texto simples em texto cifrado de modo que apenas o destinatário desejado – o possuidor da

chave de descriptografia – possa recuperar o texto simples. Isso significa basicamente que o método de criptografia deve ser seguro contra ataques de pessoas que não possuem a chave. Como um ponto inicial, devemos considerar que o próprio algoritmo de criptografia é conhecido e que somente a chave se mantém secreta. O motivo para essa suposição é que, se você depender de um algoritmo sendo mantido em secreto, então terá de abandoná-lo quando achar que ele não é mais secreto. Isso significa potencialmente mudanças freqüentes do algoritmo, o que é problemático, pois é necessário muito trabalho para desenvolver um novo algoritmo. Além disso, uma das melhores maneiras de saber que um algoritmo é eficiente é usá-lo por muito tempo – se ninguém o violar, ele provavelmente é seguro. Assim, existe o risco considerável ao se implementar um novo algoritmo. Portanto, nosso primeiro requisito é que o segredo da chave, e não o algoritmo em si seja a única coisa necessária para garantir a privacidade dos dados [1]. Existem duas classes de algoritmos baseados em chaves: os simétricos e os assimétricos.

2.1.1. Criptografia Simétrica (Chave Secreta)

A Criptografia Simétrica foi a primeira forma conhecida para cifrar/ocultar dados sigilosos.

Os algoritmos simétricos são baseados em chaves privadas. Assim, o emissor cifra a mensagem e o receptor a decifra. Para as duas operações é utilizada a mesma chave, gerada por um algoritmo simétrico. Assim, a operação matemática é idêntica no cifrar e no decifrar. Esta chave é compartilhada pelo remetente e destinatário. A mensagem original (chamada de texto simples) é transformada em um texto cifrado. O destinatário, por sua vez realiza a transformação reversa, do texto cifrado para o texto simples. A força de um algoritmo de criptografia simétrico reside tão somente no tamanho da chave utilizada [2].

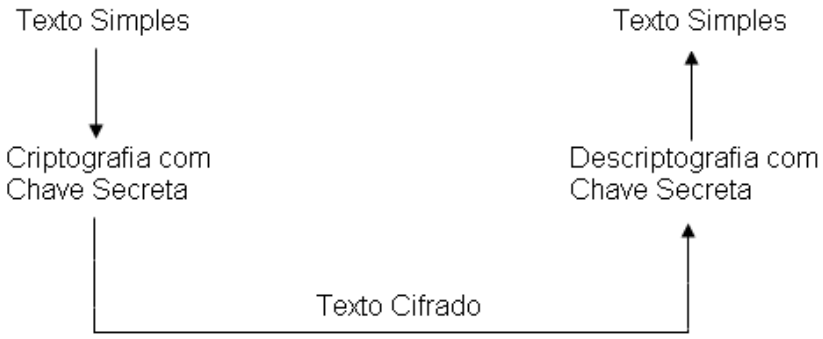

FIGURA 04: Criptografia de chave secreta.

O grande problema do sistema de chaves simétricas reside no compartilhamento de chaves. Pode-se imaginar a dificuldade de manter relações sigilosas dentro de uma empresa, por exemplo. Se existirem tantas chaves quantos funcionários, a gestão delas será uma tarefa complexa no cotidiano dos empregados. Da mesma forma, existirão muitas possibilidades de perda e de vazamento das chaves, na medida em que elas forem compartilhadas entre os vários funcionários. Se elas tiverem que ser trocadas sempre, a possibilidade de perda dos dados aumenta, pois sem uma chave, não se abre a mensagem cifrada. Se a chave for única para a empresa toda, seu vazamento significará exposição total. Em algum momento terá que haver intercâmbio da chave entre emissor e receptor. Se ela for interceptada por um terceiro, toda a comunicação é comprometida. Ainda, este terceiro poderá intervir como se fosse tanto o emissor quanto o receptor. Este problema se relaciona profundamente com o ambiente das novas tecnologias da informação, quando se verifica o largo uso de redes abertas. A criptografia simétrica ainda possui utilidade. Ela é aceitável para uma comunicação única, onde a chave pode ser descartada depois do uso. Ela serve também para comunicações com baixo risco de vazamento. Mas ela possui desvantagens quando aplicada em comunicação contínua. Ela também não permite o sistema de assinatura eletrônica, com autoridades de certificação porque não há como manter uma chave pública para comparação. Por conta destes problemas é que a criptografia simétrica se afirmou como um sistema não confiável [3].

Na criptografia simétrica, o algoritmo mais conhecido e padrão por muitos anos foi o DES. O DES criptografa um bloco de 64 *bits* de texto simples usando uma chave de 64 *bits*. A chave, na realidade, contém apenas 56 *bits* utilizáveis – o último bit de cada um dos 8 *bytes* na chave é um bit de paridade para esse *byte*.

Uma técnica, utilizada no DES, é tornar o algoritmo tão complicado que praticamente nenhuma estrutura do texto simples permaneça no texto cifrado. Isso deixa o atacante sem opção alem de procurar exaustivamente no espaço de chaves possíveis. Isso pode se tornar inviável com a escolha de um espaço de chaves adequadamente grande e tornando a operação de verificação de uma chave razoavelmente dispendiosa. O DES agora está se tornando pouco seguro com base nisso [1].

2.1.2. Criptografia Assimétrica (Chave Pública)

A criptografia assimétrica consiste na utilização de duas chaves (Privada e Pública), uma para cifrar e outra para decifrar. A partir do algoritmo são geradas duas chaves, que formam um

par único. Uma delas será pública e ficará disponível para o uso geral. A outra será privada, mantida pelo titular. A técnica permitiu o aparecimento de um meio mais seguro para a cifração de informações e, principalmente, para a montagem de sistemas de certificação digital (infra-estruturas de chaves públicas), que gerem as chaves públicas em repositórios abertos, bem como emitem as chaves privadas e são passíveis de auditoria e controle técnico. A função nova é a produção de assinaturas eletrônicas, passíveis de conferência. Com esta função é resolvido o dilema do compartilhamento de chaves pelos canais de comunicação inseguros. Deste modo, ela tornou-se um meio central para a segurança nos tempos atuais da *Internet*. Em resumo, existem duas funções técnicas, que têm importante uso com a criptografia assimétrica: a cifração de conteúdos de mensagens (sigilo) e a utilização de certificados digitais, como garantia das assinaturas digitais. Os certificados, que permitem as assinaturas, são gerados com chaves criptográficas [3].

Somente o destinatário que possui a chave privada conseguirá desfazer a operação de cifragem, ou seja, decifrar e recuperar as informações originais, dessa forma é garantido o sigilo, conforme demonstrado na Figura 05.

FIGURA 05: Criptografia de chave pública.

No processo de autenticação, as chaves são aplicadas no sentido inverso ao da confidencialidade. O autor de um documento utiliza sua chave privada para cifrá-lo de modo a garantir a autoria em um documento ou a identificação em uma transação. Esse resultado só é obtido porque a chave privada é conhecida exclusivamente por seu proprietário.

Na criptografia Assimétrica, o algoritmo mais conhecido é o RSA. Ele foi o primeiro algoritmo assimétrico desenvolvido. Seus criadores foram Ron Rivest, Adi Shamir e Leonard Adleman, que em 1976 o utilizaram com sucesso tanto para cifrar dados como para

Assinatura Digital, implementando os conceitos apresentados por *Diffie e Helman* um ano antes. O RSA é certamente o algoritmo mais popular, sendo baseado na dificuldade em fatorar dois números primos grandes [5].

Os ataques ao RSA podem ocorrer por força bruta, onde o invasor tenta decifrar a chave. Para proteger-se, o tamanho da chave deverá ser aumentado e o tempo de ataque de temporarização, baseado no tempo gasto para efetuar o cálculo do algoritmo, com o intuito de obter o tamanho dos fatores utilizados. O principal ataque sofrido pela RSA foi a tentativa de desfatorar os números primos [5].

RSA é um algoritmo muito diferente, não apenas porque envolve chaves diferentes para criptografia (chave pública) e descriptografia (chave privada), mas também porque é baseado na teoria numérica. De fato, o aspecto essencial do RSA se reduz a como essas duas chaves são selecionadas. O ato de criptografar ou descriptografar uma mensagem é expresso como uma função simples, embora essa função exija enorme poder computacional. Em particular, RSA normalmente usa um tamanho de chave de 1.024 bits, tornando muito mais dispendioso de calcular do que DES [1].

2.1.3. Função Resumo (HASH)

A assinatura digital obtida com o uso da criptografia assimétrica, ou de chave pública não pode ser empregada de forma isolada. Sua utilização, como componente de assinaturas digitais, é necessária em virtude da lentidão dos algoritmos assimétricos, ou seja, na prática é inviável utilizar puramente algoritmos de chave pública pra assinaturas digitais, principalmente quando se deseja assinar grandes mensagens, que podem levar preciosos minutos ou mesmo horas para serem integralmente criptografadas com a chave privada de alguém [7].

A função resumo funciona como o seu próprio nome diz como um resumo é semelhante ao dígito verificador do CPF, ou seja, qualquer número do CPF que for alterado irá acarretar mudanças no dígito. A função resumo recebe como entrada uma mensagem de qualquer tamanho e produz um resumo de tamanho fixo, que representa o conteúdo da mensagem. O tamanho da saída varia de acordo com o algoritmo usado. O propósito de uma função resumo é produzir uma “impressão digital” da mensagem [5]. O resultado que a função resumo gera garante a integridade da mensagem.

Um algoritmo de resumo precisa ter três propriedades para ser seguro no sentido de criptografia [4]:

- Primeiramente, precisa ser inviável computacionalmente reencontrar a mensagem de entrada baseada apenas em seu resumo.
- Não deve ser possível achar uma mensagem particular que tenha um resumo específico.
- E, por último, não ser computacionalmente viável achar duas mensagens distintas com o mesmo resumo.

Funções resumo são funções de caminho único, ou seja, elas só possuem um sentido. Com o resultado gerado por uma Função Resumo é possível garantir a integridade de uma mensagem, pois o resumo gerado no destino por uma Função Resumo terá que ser igual ao resumo gerado na origem. O algoritmo mais utilizado no momento é o MD5. O MD5 é um algoritmo para ser utilizado no padrão DSS. A função desse algoritmo é gerar um resumo de uma mensagem de tamanho fixo, que seja único e inviolável.

O MD5 opera sobre uma mensagem de 512 *bits* de cada vez, de modo que a primeira etapa é preencher a mensagem para um múltiplo de 512 *bits*. Matematicamente os algoritmos MD5 costumam ter mais em comum com DES do que com RSA. Ou seja, eles não têm uma base matemática formal, mas contam com a complexidade do algoritmo para produzir uma saída aleatória, de modo que os requisitos esboçados anteriormente sejam atendidos [1].

2.2. Autenticação

A autenticação provê a garantia de que as entidades envolvidas em uma transação são quem elas dizem ser. Estas entidades podem ser pessoas ou dispositivos. Uma autenticação pode ser feita considerando os seguintes fatores [5]:

- Algo que você sabe: A autenticação é realizada através de alguma coisa que você especifica de seu conhecimento sobre o individuo. Este fator conhecido poderá ser uma senha, um nome ou um número de identificação pessoal.
- Algo que você tem: A entidade será identificada através da posse de alguma coisa física, um objeto que possua a chave privada armazenada.
- Algo que você é: A entidade utiliza alguma medida biométrica.
- Quando: a data e a hora da autenticação podem ser conhecidas e verificadas.

- Onde você está: A posição geográfica do individuo é levada em consideração no momento em que é realizada a autenticação.
- Presença de testemunha: A presença de uma ou mais testemunhas é necessária para a realização da autenticação.

O serviço de autenticação é especialmente importante para a operação de segurança de um sistema. Um sistema, em geral, contém uma fase inicial de autenticação antes de estabelecer comunicação com uma entidade. A identidade da entidade então é usada para estabelecer os privilégios de acesso. Durante o protocolo de autenticação, duas partes usualmente concordam em tornar sua mensagem em uma comunicação em segredo [4].

2.2.1. Protocolo de Autenticação

Antes que dois participantes provavelmente estabeleçam um canal seguro entre eles – ou seja, usem um algoritmo como DES para criptografar as mensagens que eles trocam –, eles geralmente desejarão saber se o outro participante é quem ele afirma ser. Esse é o problema da autenticação [1].

Existem vários protocolos de autenticação, os mais utilizados são:

- *Handshake* de Três Vias Simples: Um protocolo de autenticação simples é possível quando os dois participantes que querem autenticar um ao outro – pense neles como um cliente e um servidor – já compartilham uma chave secreta. Essa situação é semelhante a um usuário (cliente) tendo uma conta em um sistema de computador (servidor), onde tanto o cliente quanto o servidor conhecem a senha para a conta [1].
- Terceiro Confiável: Um cenário mais provável é que os dois participantes não saibam nada um sobre o outro, mas confiam em um terceiro. Esse terceiro às vezes é chamado de servidor de autenticação, e ele usa um protocolo para ajudar os dois participantes a autenticarem um ao outro. [1]
- Autenticação de Chave Pública: Este protocolo utiliza a criptografia de chave pública. Este protocolo é útil, pois não são necessários que os dois lados compartilhem uma chave secreta, eles precisam só conhecer a chave pública do outro lado.

2.3. Padrões de Criptografia de Chave Pública

A empresa RSA *Security*, em cooperação com desenvolvedores, definiu uma série de Padrões para o uso da criptografia de Chaves Públicas. Eles são denominados PKCS, com a finalidade

de desenvolver aplicações seguras, baseadas na criptografia de Chave Pública. Atualmente, existem padrões já definidos, que vêm sendo amplamente implementados e referenciados em experiências disponíveis pelo mundo. A grande maioria das aplicações que utilizam serviços de criptografia usufrui destes padrões [5].

Os Padrões PKCS #7 e PKCS #10 são dois destes padrões que são largamente utilizados em infra-estrutura de Chaves Públicas.

O padrão PKCS #7 descreve a sintaxe geral, sendo utilizado para a transferência de dados assinados ou cifrados. Ele também permite o encapsulamento de uma mensagem, assinada ou cifrada, dentro de uma nova mensagem, com o que uma mensagem pode ser cifrada e depois assinada.

O PKCS #10 é o padrão que descreve a sintaxe de requisições de certificados. Uma requisição é formada pela identificação do requisitante ou nome distinto e uma Chave Pública, juntamente com outros atributos opcionais. Também faz parte desta requisição um identificador do algoritmo da assinatura e a Assinatura Digital da informação da requisição do certificado. Todo o conjunto de dados é assinado digitalmente pela entidade que está requerendo a Certificação. Requisições para certificados são enviadas para ACs, que as transformam em certificados digitais. Após criado o Certificado Digital, a AC (Autoridade Certificadora) o envia para o requisitante. As duas razões para incluir um conjunto de atributos na requisição de um certificado são: fornecer informações sobre a entidade requisitante, o que possibilitará à entidade requisitar a Revogação do certificado; e permitir o acréscimo de atributos no certificado X.509 [5].

2.4. Certificado Digital

Um certificado digital ou identidade digital é um arquivo digital de computador que, como os demais documentos tradicionais de identificação, além dos dados do indivíduo ou entidade, possuem também uma chave pública do assinante [5].

Baseada na infra-estrutura de chaves públicas, ou seja, utilizando o par de chave pública e privada, a certificação digital possibilita agregar os seguintes requisitos de segurança:

- Autenticidade – Garantia da autoria de um documento.
- Privacidade – Garantia de que nenhuma pessoa não-autorizada terá acesso ao conteúdo.

- Integridade – Garantia de que a informação não será violada.
- Não-repúdio – Garantia da impossibilidade de negar a autoria.

2.4.1. Ciclo de Vida

Os certificados digitais apresentam um ciclo de vida, é necessário possuir um prazo de validade devido à evolução dos dispositivos de processamento. Este ciclo é composto por sete itens que executam todo o processo da Certificação, desde a solicitação até o encerramento das atividades do certificado. A figura 06 ilustra o ciclo de vida dos mesmos [5].

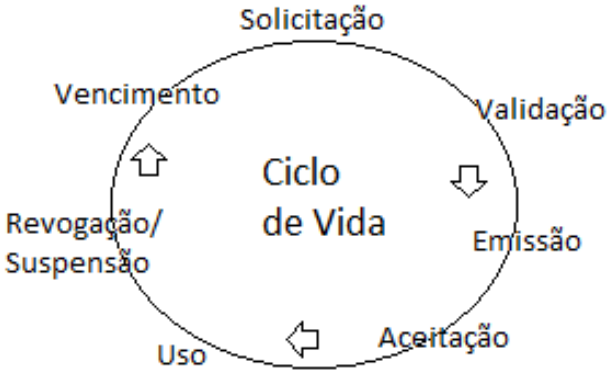

FIGURA 06: Ciclo de Vida do Certificado.

- Solicitação de Certificados: Os procedimentos para a solicitação incluem exigências referentes à geração, proteção do par de chaves e lista de informações necessárias para cada classe de certificado, preenchimento de uma solicitação e seu envio à AC pertinente, anexando a Chave Pública.
- Validação de Certificados: A validação consiste basicamente em verificar se a solicitação preenche os pré-requisitos para a emissão do certificado. Caso as validações sejam aprovadas será emitido o certificado, mas se a solicitação for rejeitada, ou seja, as informações da solicitação não sejam verdadeiras ou houver indícios de irregularidades na solicitação, a aprovação da mesma não poderá ocorrer, havendo a rejeição.
- Emissão de Certificados: A emissão de um certificado ocorrerá após a AC receber uma solicitação aprovada pela AR.

- Aceitação de Certificados: Quando o certificado é aceito, o assinante deverá garantir a integridade de sua Chave Privada, a veracidade de suas informações e o certificado será de uso exclusivo para a sua finalidade.
- Uso de Certificados: A garantia de que os certificados estão sendo utilizados corretamente é realizada pela conferência da Assinatura Digital.
- Suspensão / Revogação de Certificados: A Suspensão e/ou Revogação pode ocorrer por vários motivos, seguem alguns: comprometimento, perda, roubo, modificações e etc.
- Vencimento do Certificado: A AC deve emitir uma notificação aos assinantes sobre o vencimento do certificado.

2.4.2. Estrutura Hierárquica de Certificação Digital

Um documento oficial de identificação, como por exemplo, o RG, é expedido pela SSP (Secretaria de Segurança Pública), atestando que você realmente é. No mundo digital, o processo não muda. Na Figura 07 é apresentada a hierarquia existente na expedição de RG e a geração de um certificado.

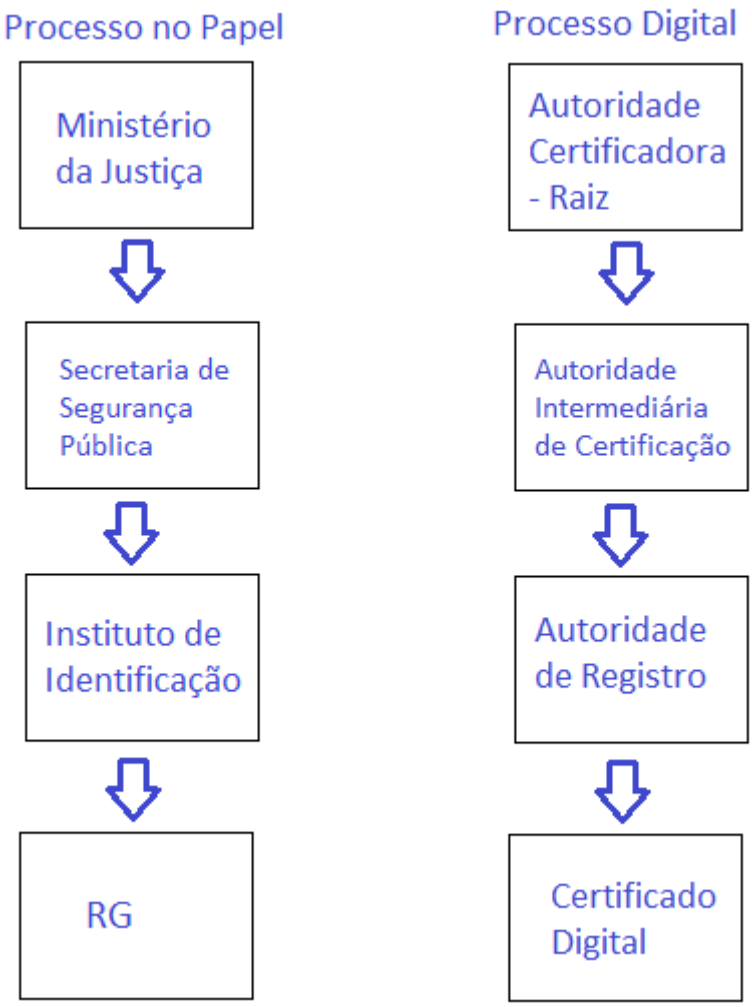

FIGURA 07: Estrutura hierárquica da cadeia de certificação digital.

O certificado digital é uma estrutura de dados, dentro quais estão no mínimo as seguintes informações:

- Nome da pessoa ou entidade a quem foi emitido o certificado.
- Chave pública e sua validade.
- Número de série.
- Nome da AC (Autoridade Certificadora) que emitiu o certificado.
- Assinatura digital da AC.
- Extensão.

Embora existam vários tipos de certificados em uso, o mais utilizado é o X.509. O formato X.509 é um padrão de formato de certificado criado pela ITU-T e ISO/IEC, primeiramente publicado em 1988.

O conteúdo do certificado varia de acordo com o sistema da AC (Autoridade Certificadora). O conteúdo e as limitações do certificado são a fonte para o risco estratégico assumido pela AC. Um certificado-padrão identifica o assinante e a entidade emissora AC. Quanto mais curta a vida de um certificado, menor será o risco assumido pela AC que o emitiu. A segurança do certificado passa por vulnerabilidades físicas e lógicas que extrapolam o software utilizado para gerar a assinatura digital. Quanto mais tempo esse software estiver em uso, maiores serão as chances de ele ser corrompido ou de que alguém consiga um acesso não autorizado [7].

A Figura 08 ilustra o formato de certificado X.509. Um certificado X.509 abrange um conjunto de campos pré-definidos e zero ou mais campos de extensão. A tabela contém as descrições dos campos ilustrados na figura 08.

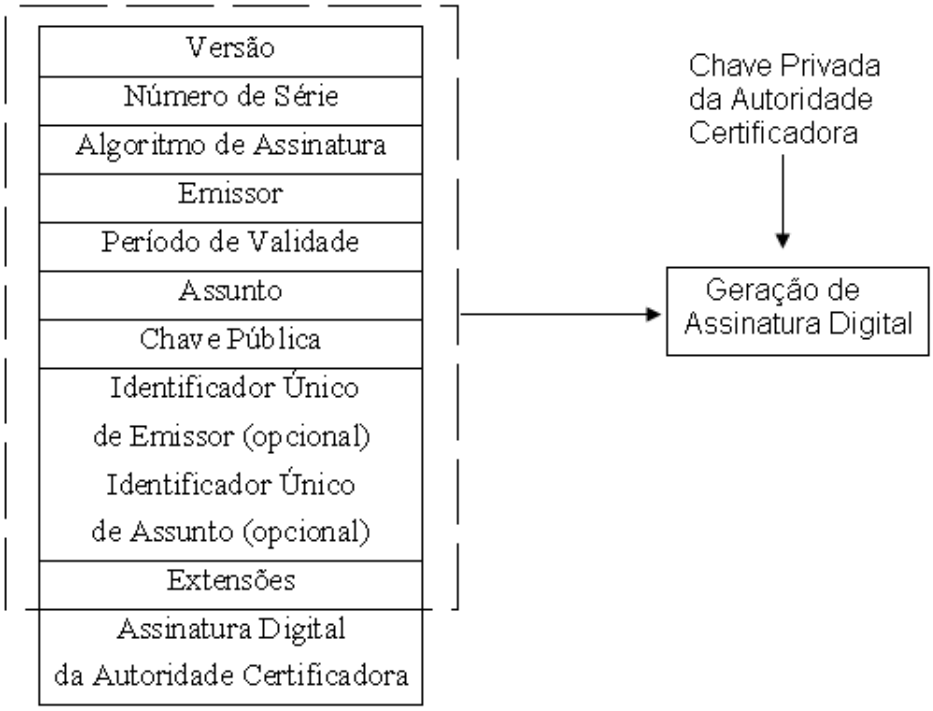

FIGURA 08: Certificado digital no padrão X.509.

As extensões advindas do formato X.509 proporcionam uma maneira de associar informações adicionais para uma entidade, chave pública, autoridade certificadora ou qualquer outra informação contida do certificado. Estas extensões proporcionam também a possibilidade de organizações e empresas definirem seus próprios campos de extensões e codificar informações específicas às suas necessidades.

Nome do Campo	**Descrição**
Versão	Número da versão X.509 do certificado.
Número de série	Identificador único do certificado e representado por um inteiro. Não deve haver mais de um certificado emitido com o mesmo número de série por uma mesma autoridade certificadora.
Algoritmo de Assinatura	Identificador do algoritmo usado para assinatura do certificado pela autoridade certificadora.
Emissor	Nome da autoridade certificadora que produziu e assinou o certificado.
Período de Validade	Intervalo de tempo de duração que determina quando um certificado deve ser considerado válido pelas aplicações.
Assunto	Identifica o dono da chave pública do certificado. O assunto deve ser único para cada assunto no certificado emitido por uma autoridade certificadora.
Chave Pública	Contém o valor da chave pública do certificado junto com informações de algoritmos com o qual a chave deve ser usada.
Identificador Único de Emissor (opcional)	Campo opcional para permitir o reuso de um emissor com o tempo.
Identificador Único de Assunto (opcional)	Campo opcional para permitir o reuso de um assunto com o tempo.
Extensões	Campo complementares com informações adicionais personalizadas.

TABELA 01: Descrição dos campos de um certificado no formato X.509.

2.5. Assinatura Digital

Assinatura Digital é um conjunto de dados usados para garantir a integridade à autenticidade de uma determinada mensagem. O autor da mensagem usa sua chave de assinatura para assinar a mensagem e enviá-la junto com a assinatura digital para um destinatário. O destinatário recebe a mensagem e usa uma chave de verificação para verificar a origem da mensagem e garantir que ela não foi modificada enquanto estava em trânsito [4].

As chaves de assinatura e verificação são distintas, garantindo que o destinatário possa somente verificar a assinatura, mas não será capaz de forjá-la. Devido ao fato de não ser computacionalmente viável forjar uma assinatura sem a posse da chave de assinatura, o autor não pode repudiar o fato que assinou uma mensagem [4].

Essa não é nenhuma comunicação segura, mas o objetivo da assinatura digital não é proteger a informação, e, sim, garantir que ela provém da entidade que a enviou, ou seja, qualquer pessoa pode descriptografar a assinatura digital do emissor, uma vez que somente é necessária sua chave pública, para descobrir o resumo da mensagem original. Por outro lado, ninguém mais tem a chave privada do emissor, ou seja, ninguém mais poderia ter codificado isso, e dessa forma, autentica-se a origem da mensagem [7].

Esta é a idéia central da assinatura digital: só o emissor conhece sua chave privada, logo somente ele pode codificar a mensagem. Todo mundo conhece a chave pública do emissor, assim qualquer um pode decifrar a mensagem. Codificando a mensagem com a chave privada dele, o emissor está efetivamente assinando a mensagem. Ele está fazendo algo com a mensagem que somente ele pode executar. Além disso, visto que o resumo só pode ser cifrado ao utilizar a chave privada do emissor, uma terceira entidade, que não conhece essa chave privada, não poderá modificá-la, pois não terá como gerar um resumo cifrado correspondente à mensagem alterada. Desse modo, com a assinatura digital e a presença de um resumo válido, há uma garantia da integridade da origem da mensagem [7].

3. ESTUDO DE CASO

3.1. Empresa

Atuando desde 1992 no segmento financeiro, a *ZetraSoft* mantém com seus clientes uma constante relação de parceria e interação. Com sede em Belo Horizonte, a *ZetraSoft* desenvolve projetos de *e-Business* desde 1998, e hoje conta com uma equipe capacitada explorando todas as potencialidades da *web* [9].

O *eConsig* – Sistema Digital de Consignações foi desenvolvido para revolucionar o processo operacional de consignações. Utiliza a tecnologia da *internet* proporcionando operações de consignações *on-line*, de forma segura e ágil, aos seus usuários (consignantes, consignatárias e funcionários/servidores). Atende empresas privadas e órgãos públicos [9].

Os responsáveis pelos convênios e os funcionários da empresa são os gestores. A função do gestor é planejar, organizar, comandar, coordenar e controlar o sistema.

3.1.1. E-CPF

O *e-CPF* é a versão eletrônica do CPF, que garante a autenticidade e a integridade nas transações eletrônicas de pessoas físicas.

O *e-CPF* (ePass2000) que é utilizado pela *ZetraSoft* é o A3 e a AC é a PRODEMGE. O certificado digital A3 oferece maior segurança, pois seus dados são gerados, armazenados e processados em *token*, permanecendo assim invioláveis e únicos, uma vez que a chave privada é gerada dentro do dispositivo e não pode ser exportada. Somente o detentor da senha de acesso pode fazer utilização da chave privada. Por estar contido em um dispositivo como *token*, terá a possibilidade de ser transportado e utilizado em qualquer computador.

Para utilização do certificado digital do tipo A3 são necessários dois itens, a senha e o *token*. Dessa forma, mesmo que um programa malicioso capture a senha, não será possível a utilização do certificado, pois a chave privada está contida dentro do dispositivo.

Para solicitar o certificado do tipo A3 é necessário apresentar as seguintes documentações na validação presencial com a Autoridade Certificadora:

- CPF e Cédula de Identidade válida. Pode ser um dos documentos: Carteira de Habilitação, RG, Carteira Funcional, Carteira Profissional ou Passaporte;

- Foto 3x4 colorida e recente;
- Comprovante de residência em nome do titular do certificado;
- Termo de Titularidade (esse termo é enviado por e-mail cadastrado na solicitação eletrônica.);
- Comprovante de pagamento do boleto bancário. O custo para possuir um certificado digital (*e-CPF* A3) durante 1 ano é de R$ 100,00.

A empresa decidiu pela utilização do certificado do tipo A3, pois o par de chaves é gerado em *hardware* específico, isto é, em um *token*, que não permite a exportação ou qualquer outro tipo de reprodução ou cópia da chave privada. Também no certificado tipo A3 a chave pública será enviada para a AC (Autoridade Certificadora) junto com a solicitação de emissão do certificado, enquanto a chave privada ficará armazenada no *token*, impedindo tentativas de acesso de terceiros.

3.2. Implementação da Segurança da Informação

O *eConsig* controla descontos consignados, ou seja, descontos no contra-cheque do servidor ou funcionário. Temos o controle das margens e dos descontos de todos servidores dos convênios que trabalhamos, como por exemplo, Marinha do Brasil, Comando da Aeronáutica, Prefeitura de São Paulo, Governo do Mato Grosso do Sul entre outros. A segurança das informações é obtida a partir da implementação de conjuntos de controles adequados à empresa. Definir, alcançar, manter e melhorar a segurança da informação pode ser atividades essenciais para assegurar a competitividade, o lucro, o atendimento aos requisitos e a imagem da organização junto ao mercado.

Como dito anteriormente a segurança da informação é importante para os negócios, tanto do setor público como do setor privado, e para proteger as infra-estruturas críticas. Em ambos os setores, sua função é viabilizar os negócios como o governo eletrônico (*e-gov*) ou o comércio eletrônico (*e-business*), e evitar ou reduzir os riscos relevantes. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso [8]. O sistema da empresa e a rede de computadores ficavam expostos a vários tipos de ameaças como fraudes, espionagens e sabotagens. Com a implantação e utilização do certificado digital os riscos diminuíram. Atualmente somente usuários cadastrados e com o *e-CPF* podem acessar o sistema como gestor. A segurança das informações ainda está em fase de testes, mas já está melhorando a confiabilidade dos sistemas.

Para acessar é necessário que o *token* seja validado pelo site. Ele é identificado assim que é acessado o *eConsig* através do endereço eletrônico. È necessário que seja informado o usuário, senha e o código *captcha,* conforme Figura 09.

FIGURA 09: Tela de *login* do sistema *eConsig*.

Quando é criado o usuário do gestor é cadastrado o CPF, e é assim que é validado o *e-CPF*. Quando o usuário loga no sistema é verificado se o CPF cadastrado nos dados do usuário são os mesmos que o *token* está emitindo.

FIGURA 10: Tela de cadastro de usuário do sistema eConsig.

Após a digitação dos dados na tela de *login*, o sistema valida o *e-CPF* do usuário.

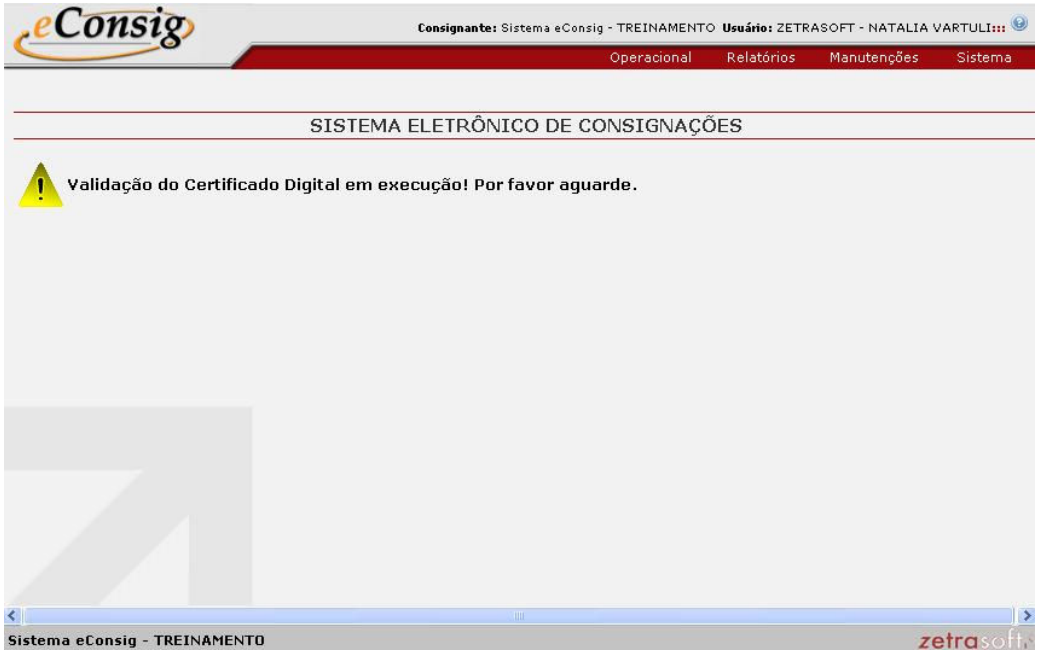

FIGURA 11: Tela da validação do certificado do sistema eConsig.

Toda a validação é feita através de um *XML* criado para capturar os campos necessários que são emitidos pelo *token*. De início o sistema estava preparado somente para validar o certificado digital utilizado pelos funcionarios da *ZetraSoft*. Após a utilização do certificado por 3 meses os clientes começaram a adotar a utilização do certificado para acessar o sistema. Como o *eConsig* estava preparado para validar somente o certificado *e-CPF* do tipo A3 e os clientes utilizam outros certificados, viu-se a necessidade de criar um XML que valide todos os tipos de certificados utilizados pelos clientes. Com isso foi implementado o XML da Figura 12.

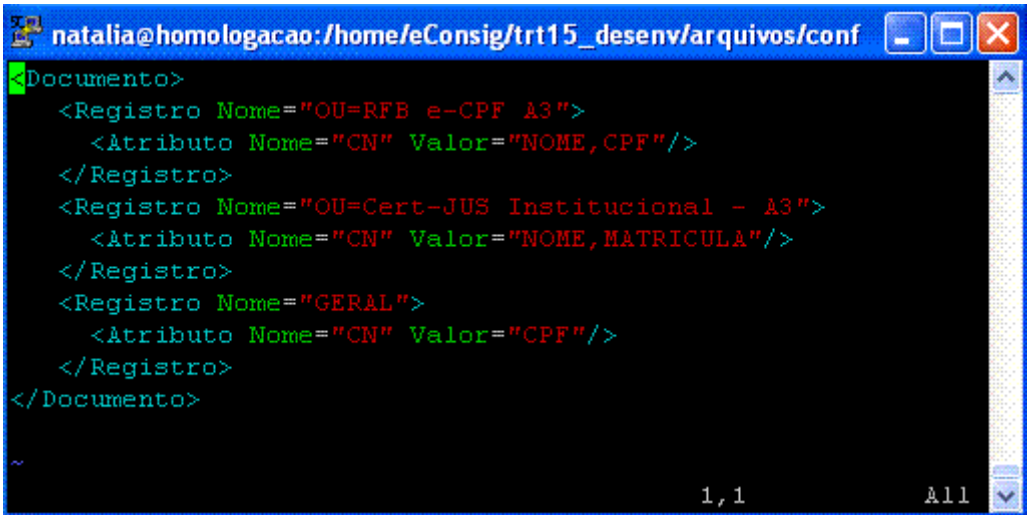

FIGURA 12: Tela da validação do certificado do sistema eConsig.

A ideia é que cada <Registro> represente um formato válido para o certificado. Por exemplo,

```
<Registro Nome="OU=Cert-JUS Institucional - A3">
  <Atributo Nome="CN" Valor="NOME,MATRICULA"/>
</Registro>.
```

Neste caso, o *eConsig* procura no certificado pelo "OU=" e se for "Cert-JUS Institucional - A3" ele irá validar o campo CN (*Common Name*) e considerar que as informações contidas no *token* são Nome e Matricula. No XML criado deverá conter todos os tipos possíveis dos certificados a serem usados.

O CN é composto do nome da pessoa física, com cumprimento máximo de 52 caracteres. O *Organization Unit* (OU) é um campo de preenchimento livre, normalmente contém o nome da Autoridade de Registro responsável pela aprovação do certificado.

A validação de certificado digital do *eConsig*, quando está no modo padrão, busca o campo CN do certificado e obtém dele o valor do CPF do usuário. Nos CPF dos funcionários da *ZetraSoft* , o CN é da seguinte forma:

Certificado Digital: **CN=NATALIA VARTULI CORDEIRO E SILVA:** [redacted], OU=Autenticado por PRODEMGE RFB, OU=(EM BRANCO), OU=RFB e-CPF A3, OU=Secretaria da Receita Federal do Brasil - RFB, O=ICP-Brasil, C=BR

, ou seja, Nome:CPF.

Para adequar os sistemas da empresa foi necessário contratar uma empresa para treinamentos sobre certificação digital e disponibilizar uma equipe de funcionários para implementação e testes. A *ZetraSoft* está se preparando para seguir a Norma Brasileira ABNT NBR ISO/IEC 27001:2006. Esta norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados e tamanho da estrutura da organização.

O ponto de partida para a segurança da informação já foi tomado pela empresa:

- Proteção dos dados e privacidade de informações pessoais;
- Proteção dos registros organizacionais;
- Direitos de propriedade intelectual;
- Documento da política de segurança da informação;
- Atribuição de responsabilidades para segurança da informação;
- Conscientização, educação e treinamento em segurança da informação;
- Processamento correto nas aplicações;
- Gestão de vulnerabilidades técnicas;
- Gestão de continuidade do negócio;
- Gestão de incidentes de segurança da informação e melhorias.

A grande dificuldade da utilização do certificado é quando são contratados novos funcionários, existe um tempo de espera entre a compra e o envio do certificado. Neste espaço de tempo de uma semana o funcionário não tem acesso aos sistemas.

Para garantir ainda mais segurança no acesso ao *eConsig* foram criadas as jaulas. Elas servem para limitar o acesso dos usuários a algumas funcionalidades, o usuário que estiver utilizando a jaula é incapaz de enxergar qualquer coisa fora de sua cadeia. Cada jaula foi criada conforme necessidades de cada setor, levantou-se quais funcionalidades cada setor necessitava e foi avaliado se realmente estas funcionalidades eram necessárias. Depois de vários testes definiram-se quais funcionalidades cada jaula teria. De início vários funcionários fizeram reclamações sobre o acesso restrito, mas este acesso restrito é necessário para garantir confiabilidade do sistema.

Apesar de algumas dificuldades na implementação da certificação digital, suas vantagens são indiscutíveis. O aumento da segurança no controle de acesso utilizando a autenticação do usuário, aumento da confiabilidade dos *logs* de acesso, processos tornaram-se menos burocráticos, a mensagem enviada com certificação tem o *status* e a validade de um documento propriamente dito.

4. CONCLUSÃO

O Certificado Digital é um documento eletrônico que permite a identificação das pessoas de modo seguro em transações realizadas utilizando mídias ou redes digitais. Esse documento eletrônico é gerado e assinado por uma terceira parte, uma AC (Autoridade Certificadora), que segue as regras emitidas pelo Comitê Gestor da ICP-Brasil (Infra-estrutura de Chaves Públicas – Brasil). Este trabalho apresentou os principais conceitos sobre certificação digital, além de discutir um estudo de caso de implementação da mesma.

Utilizando o estudo de caso realizado como base de discussão, algumas considerações importantes podem ser feitas com relação ao uso da certificação digital.

Ao utilizar certificação digital, a empresa deve buscar a certificação ISO. Os benefícios de certificação da norma ISO geram qualidade para os clientes e garantia de satisfação, que é o resultado da obtenção de serviços e produtos que seguem procedimentos rigorosos, tornando a empresa referência no mercado de crédito consignado.

Alem da utilização do certificado, a empresa deve garantir outros tipos de segurança das informações. Para acesso ao sistema via SSL um certificado deve possuir criptografia de 128 *bits* com algoritmo DES, o que dificulta a quebra do código cifrado. Para chaves de 128 *bits*, teremos 2^{128} combinações possíveis, o que torna a busca exaustiva pela chave correta.

O acesso aos servidores deve ser via SSH. A grande vantagem do SSH é a ênfase na segurança, pois um servidor SSH bem configurado é virtualmente impenetrável. Ele utiliza um conjunto de técnicas de criptografia para assegurar que apenas as pessoas autorizadas tenham acesso ao servidor. O SSH utiliza chaves assimétricas para fazer a autenticação. Assim, quando se conecta a um servidor SSH, o PC e o servidor trocam as chaves públicas, permitindo que um envie informações para o outro de forma segura.

Para garantir o controle de acesso dos usuários uma possibilidade são as jaulas (*JAIL Linux*). Para a sua criação devem ser levantados os comandos e aplicativos utilizados pelos funcionários de cada setor, gerando a padronização dos scripts de apoio e suas pastas de alocação física nos servidores. Após o levantamento são criados ambientes “jaulas” por equipe/papel, homologados por um colaborador de perfil correspondente e colocados em produção.

Ainda assim uma grande preocupação de uma empresa seria se os dados dos sistemas fossem corrompidos. Para tal deve ser criada uma política de *backup* padrão pelo Comitê de Segurança, com base em requisitos contratuais. Em servidores sob responsabilidade do cliente, a política é executada no devido parque tecnológico e utiliza os recursos do próprio cliente. Em servidores de hospedagem da *ZetraSoft*, no caso estudado, a política é executada por uma empresa contratada e os riscos foram transferidos para eles com base contratual.

A maior dificuldade na implementação da certificação digital é a adequação dos sistemas já utilizados ao uso dos certificados. No estudo de caso analisado, com a criação do XML de validação do certificado, inicialmente foi pensado que todos utilizariam o certificado *e-CPF*. Porém, com o grande número de sistemas que a *ZetraSoft* controla, vários gestores já possuíam outro tipo de certificado, como por exemplo, Cert-Jus Institucional, muito utilizado pelo poder judiciário. Foi necessário adequar o XML para validar todo tipo de certificado e criar soluções paralelas, para suprir a necessidade dos novos funcionários enquanto o *e-CPF* não ficava pronto.

Outra desvantagem é a instalação do certificado e a segurança da chave privada da Autoridade Certificadora. É necessário instalar o *token* ou os leitores de cartão em caso de *smart card*, as cadeias de certificação e diversos outros programas que para um usuário pode-se tornar um processo complicado, podendo levar à insatisfação do produto. Já a chave privada de uma Autoridade Certificadora pode ser comprometida, e todos os certificados emitidos por ela deverão ser revogados, e não serão mais confiáveis.

Apesar das dificuldades de implementação e resistência dos funcionários fica claro que o certificado digital é uma boa opção para complementar os requisitos de segurança da informação. As principais vantagens com a utilização do certificado digital são a segurança e confiança, mas a cada dia o mercado encontra novas vantagens e usos para esta tecnologia.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Peterson, Larry L., Davie, Bruce S. Redes de Computadores – Uma abordagem de Sistemas. Editora Campus, 3ª Edição, 2004.

[2] AUTRET, T.; BELLEFIN, L.; OBLE-LAFFAIRE, M. Sécuriser ses échanges életroniques avec une PKI: solutions techniques et aspects juridiques. Paris: Eyrolles, 2002.

[3] Veronese, Alexandre. A Política de Certificação Digital: Processos Eletrônicos e a Informatização Judiciária. Disponível em http://www.conpedi.org/manaus/arquivos/anais/bh/alexandre_veronese.pdf. Acessado em 19 de outubro de 2009.

[4] Silva, Luiz Gustavo C.; Silva, Paulo Caetano; Batista, Eduardo Mazza; Homolka, Herbert Otto; Júnior, Ivanildo José de Sousa Aquino; Lima, Marcelo Ferreira. Certificação Digital – Conceitos e Aplicações: Modelos Brasileiro e Australiano. Editora Ciência Moderna, 2008

[5] Monteiro, Emiliano S., Mignoni, Maria Eloísa. Certificados Digitais – Conceitos e Práticas. Editora Brasport, 2007.

[6] Zapater, Marcio, Suzuki, Rodrigo: Segurança da Informação. Um diferencial determinante na competitividade das corporações. Disponível em http://www.promon.com.br/portugues/noticias/download/Seguranca_4Web.pdf. Acessado em 06 de maio de 2010.

[7] Silva, Lino Sarno da: *Public Key Infrastructure* – PKI. Conheça a Infra-Estrutura de Chaves Públicas e a Certificação Digital. Editora NOVATEC, 2004.

[8] ABNT, Associação Brasileira de Normas Técnicas: Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação. ABNT, 2005.

[9] www.zetrasoft.com.br. Acessado em 08 de novembro de 2010.