A SEGURANÇA DA CERTIFICAÇÃO DIGITAL

Lucas Carvalho Assunção[1]

Lucas.c.assuncao@gmail.com

Wagner Cardoso[2]

Wagner.cardoso@uniube.br

RESUMO

Este trabalho foi desenvolvido para apresentar ao leitor a Certificação Digital, mostrando em uma linguagem mais tecnológica os conceitos e detalhes da segurança contidas no certificado digital. O mundo virtual está em constante evolução e traz consigo a necessidade de algo que garanta segurança e tranquilidade aos dados e informações dos usuários da atualidade. A criptografia, que é a segurança da certificação digital, tem como função e principal objetivo proteger informações que são transmitidas entre os usuários no meio virtual. A criptografia existe em outras formas, mas trabalha sempre no mesmo objetivo, que é proteger informações. Por meio de exemplos de uso, detalhes do funcionamento e modelos de criptografia, o trabalho utiliza uma linha de raciocínio buscando interagir o leitor dessa nova realidade e provando a efetividade da ferramenta despertar o interesse em utilizar o certificado em aplicações virtuais.

Palavras Chave: Criptografia, Segurança, Digital, Proteção

ABSTRACT

This work was developed to show to the reader the Digital Certification, presenting the concepts and details of security using a technical language. The virtual world is constantly evolving and brings with it the need for something that guarantees safety and tranquility to users in relation to their data and information. Encryption, which is the digital certification's form of security, has as its main objective and purpose to protect information that is transmitted between users in the virtual environment. It exists in other ways, but always works with the same goal, which is to protect information. Using examples of use, details of operation and cryptographic models, the work uses a line of objective reasoning, seeking the reader's interaction with this new reality and proving the effectiveness of the tool by arousing interest in the use of the certificate in virtual applications.

Keywords: Cryptography, Security, Digital, Protection

[1] Graduando em Engenharia de Computação na Universidade de Uberaba

[2] Orientador e Professor de Engenharia na Universidade de Uberaba

1. INTRODUÇÃO

Buscando apresentar ao leitor o mundo da certificação digital, o conteúdo deste trabalho foi exposto de maneira clara e detalhada, para garantir o entendimento do que realmente é a certificação digital, incluindo a sua importância, segurança e aplicações. O objetivo principal deste projeto é apresentar a segurança da certificação digital, suas aplicações e mostra que a segurança proposta é realmente eficaz, e finalizar despertando o interesse em utilizar essa segurança diariamente cada vez mais.

Como complemento a este objetivo e também confirmação de que a tecnologia é robusta, mostrar que a segurança utilizada no certificado digital já está em uso pelo usuário sem que ele saiba. Diante da falta de conhecimento sobre a certificação digital por parte da sociedade e seus usuários, o objetivo especifico que motivou a criação deste trabalho foi de apresentar detalhes e aprofundar no tema de segurança da certificação digital, para a usabilidade no dia a dia desses usuários. É realmente importante conhecer as tecnologias disponíveis ao seu alcance, e mais importante que conhecer, é compreender sobre essa tecnologia, utilizando de exemplos práticos.

Será apresentado conceitos, detalhes e posteriormente aplicações de uma maneira que faça com que o leitor, ao compreender a certificação digital, consiga relacionar o uso dela às situações de seu cotidiano. Para atingir esse nível, é preciso falar sobre a realidade dos dias antes do certificado, que ainda continuam em uso, para ter um comparativo do antes e o depois do uso da certificação, como documento de identificação digital.

No Brasil, a Carteira de Identidade, ou RG como é conhecido, é o principal documento de identificação que um brasileiro possui a partir dos primeiros anos de vida, além da certidão de nascimento e também do Cadastro de Pessoa Fisica - CPF. Este documento possui informações de seu portador que são utilizadas única e exclusivamente para identificá-lo. O RG contém nome completo e data de nascimento do portador, a digital de um de seus polegares, o local de nascimento além de dados referentes ao registro da certidão de nascimento no cartório.

Atualmente, uma pessoa, ao chegar em um estabelecimento, órgão público ou privado, faz uso de seu documento pessoal, para se apresentar e até mesmo provar sua identidade. Por exemplo, a Maria Aparecida Pereira consegue provar, em um cartório, que é realmente Maria Aparecida Pereira, apresentando pessoalmente seu RG. O mesmo vale para identificação de empresas que são representadas por pessoas físicas, onde, a pessoa física deverá apresentar documentos de identificação da empresa, os seus documentos pessoais e também documentos que lhe conferem o direito de representar, como uma pessoa física, aquela pessoa jurídica.

Já no meio digital a forma mais simples de uma pessoa ou empresa garantir e provar sua identidade uma vez que não está junto à pessoa solicitante, é apresentar o seu certificado digital. Através de uma tecnologia de criptografia, utilizada juntamente com senhas de uso pessoal, uma empresa ou cidadão consegue provar sua identidade virtualmente.

Além do uso como documento de identificação, o início do uso diário de transferências de informações e dados sigilosos, além de outros processos, fez-se necessário a criação de um método que garantisse a segurança dessas informações desde sua criação, transmissão até a leitura. Mas os usuários que a utilizam deveriam se perguntar, se realmente é seguro o uso da certificação digital, o que poderá melhorar em seu dia a dia e ,mais ainda, se é oportuno o uso da certificação digital em sua realidade.

2. A CERTIFICAÇÃO DIGITAL

Procedimentos burocráticos, como por exemplo abertura ou fechamento de empresa, cálculos e transmissões de registros trabalhistas, acesso a contas bancarias, dentre outros procedimentos que até então eram realizados de forma física e pessoalmente, pois era necessária a identificação do responsável e sua assinatura, passaram a ser executados também de forma digital, por meio de sites ou sistemas na web. O acesso e a identificação do responsável pela execução dos procedimentos, são realizados através do certificado digital emitido para aquela pessoa ou empresa, através de um órgão autorizado. (ITI[3], 2012, p.1)

> O ano de 2006 poderá entrar para a história, como aquele em que a certificação digital decolou no Brasil. O uso desta tecnologia de forma massificada ainda levará alguns anos para se tornar realidade, mas hoje os certificados digitais já fazem parte do dia-a-dia de muitos brasileiros, de funcionários e correntistas de bancos a médicos e advogados. (ITI, 2012, p. 1)

No momento da emissão de um certificado digital em uma AR (Autoridade de Registro) ou AC (Autoridade Certificadora) no Brasil, o cidadão deve apresentar documentos originais que comprove sua identidade. Até 2015, juntamente com documentos, e a conferencia da originalidade e validade desses documentos, o cidadão era obrigado a assinar, semelhantemente ao documento apresentado os documentos para à emissão de seu certificado. Para evitar fraudes na emissão e aumentar a segurança, a partir de 2016, o ITI determinou que toda e qualquer emissão de certificado deverá conter também as digitais dos dedos de uma das

[3] Instituto de Tecnologia da Informação.

mãos do cidadão e foto 3x4 registrada no momento da entrega desses documentos. (ITI, 2016, p. 2-3).

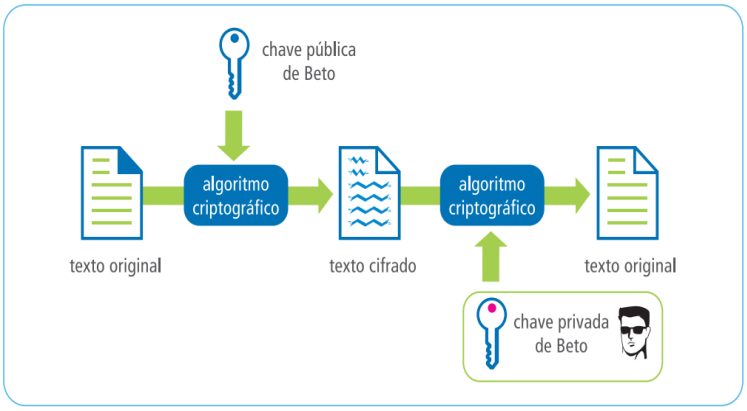
Com isso, uma vez emitido, o certificado digital poderá ser utilizado como chave na identificação de seu portador em diversas situações, como no exemplo citado anteriormente, acessar sua conta bancaria via web, pois nele estão contidas informações que permitem identificar o cidadão no meio virtual.

O certificado digital, segundo ARISP[4] ([21-?] - p.2), prove autenticidade, confidencialidade e integridade às informações que são inseridas em transações eletrônicas. Ele utiliza um sistema de criptografia para garantir a segurança da informação.

2.1 A segurança da certificação digital

A segurança do certificado digital existe graças a criptografia e é dividida em duas modalidades: Criptografia Simétrica e a de Chave Pública. A criptografia simétrica atua por meio do processo de **cifragem** e **decifragem** do conteúdo em uma comunicação. O processo de cifragem consiste simplesmente no embaralhamento da informação transmitida, impedindo assim, que caso a informação seja desviada a mesma não seja visualizada e interpretada; posteriormente a decifragem atua no processo inverso, organizando e apresentando de forma legível o conteúdo da mensagem em sua forma original. O processo foi esquematizado na imagem acima. (OFICIO ELETRONICO, 2016, p.4).

Figura 1 - Chaves Públicas e Privadas



Fonte: www.oficioeletronico.com.br

[4] Associação dos Registradores Imobiliários de São Paulo

Já a chave pública é o um número, ou chave, utilizada no acesso ao algoritmo utilizado no processo de cifragem e decifragem dessa mensagem. Ou seja, quando uma mensagem é criptografada, é utilizado um algoritmo para realizar a cifragem, ou criptografia, da informação contida nessa mensagem, e para que esse algoritmo seja acessado é necessário ter essa chave. Essas chaves públicas podem ser disponibilizadas na internet, através de diretórios públicos específicos. Cada cidadão ou empresa que tem um certificado digital, possui uma chave pública.

Por outro lado, existe a chave privada, que é o certificado digital propriamente dito. A chave privada garante a autenticidade como destinatário exclusivo de uma mensagem. Uma vez que a chave privada utilizada para acessar o algoritmo de decifragem, pertence ao real destinatário da mensagem, ou seja, portador da chave pública utilizada na cifragem, o mesmo terá acesso completo e ininterrupto ao conteúdo da mensagem. (SOTERO, 2003, p.9)

Como apresentado na figura acima, o emitente utiliza a chave pública do destinatário, como chave de acesso ao algoritmo de cifragem, para que assim, apenas o destinatário, de posse de sua chave privada, consiga acessar o algoritmo e decifrar a mensagem.

O algoritmo é a peça chave da segurança da certificação digital, pois o certificado lhe garante acesso ao algoritmo que fará a cifragem ou decifragem da mensagem. Algoritmos de cifragem podem ser desenvolvido como qualquer outro algoritmo, utilizando qualquer linguagem. É claro que um algoritmo desenvolvido de forma orientada e com tratativas de segurança e também que utiliza uma linguagem mais bem estruturada executará a cifragem ou decifragem de forma mais segura. O que pode e sempre influencia na qualidade do algoritmo é a metodologia utilizada, ou modo de cifragem. No anexo I, ao final deste trabalho o leitor poderá conhecer um algoritmo de cifragem.

3. A CRIPTOGRAFIA

De maneira resumida pode se dizer que a criptografia é uma forma de proteger uma informação através da codificação, ou embaralhamento dessa informação. Segundo a ARISP (2017), “a palavra criptografia tem origem grega e significa ‘*a arte de escrever em código’* ”. Inicialmente a criptografia de informações era muito utilizada na transmissão de informações pelo exército e pela marinha em momentos de guerra. Com o passar dos anos, o uso da criptografia, como forma de segurança à uma determinada informação, foi absorvendo novas formas de informações, novos meios de transmissão e também novas forma de criação dessa criptografia.

Tudo na criptografia depende diretamente do algoritmo de codificação. O algoritmo de codificação, é a principal e mais importante ferramenta na criptografia de uma informação. O algoritmo é responsável pelo processo de tradução da mensagem inicial em uma mensagem cifrada, cujo o processo inverso também deve ser feito utilizando esse algoritmo.

Para Burnett e Paine (2002, p. 11) “A tradução dessa mensagem para uma linguagem “desconhecida” é chamada de cifras de substituição, pois consiste em trocar uma letra do alfabeto por outra. O processo inverso, é chamada de cifras de transposição”, que traduz a mensagem cifrada para a mensagem original, utilizando do mesmo mecanismo de tradução para reverter a mensagem cifrada, ou seja, a substituição de uma letra por outra. Veja na figura 2 abaixo, um exemplo de cifra de substituição, chamado monoalfabetica, onde o mesmo cria uma relação para regulamentar que uma determinada letra do alfabeto, no texto cifrado será representado por outra letra do mesmo alfabeto.

Figura 2 – Esquematização da Cifra de Substituição

Fonte: https://capivararex.wordpress.com/2016/01/31/cifra-de-substituicao-em-linguagem-c

Após buscas, outro tipo de cifra de substituição muito encontrado é a cifra de Júlio Cesar, que consistia simplesmente em deslocar o alfabeto substituto 3 posições, ou mais, em relação ao alfabeto original. Por exemplo, originalmente a letra “A”, seria substituída por “D”, por estar 3 posições a sua frente no alfabeto original. Veja um exemplo na tabela 1 abaixo.

Tabela 1 – Exemplo de Cifragem de Júlio César.

Palavra Original:	A	M	O	R
Três posições seguintes:	B.C.D	N.O.P	P.Q.R	S.T.U
Palavra Cifrada	D	P	R	U

Fonte: Acervo do Autor, 2017

O fato de ser um processo que exige muito poder computacional para leitura e tradução da informação e também de fácil quebra por meio da detecção das vogais, colaborou para o desuso da metodologia de Julio Cesar.

Portanto, entende-se que a cifragem é responsável pela criação de uma mensagem ilegível a partir da mensagem original. A criptografia é a forma de proteger o código que interpreta essa codificação e realiza a cifragem ou decifragem da mensagem

3.1 A criptografia da certificação digital

Para proteção da codificação ou criptografia de uma mensagem existem dois métodos ou técnicas para criptografia. São dois métodos considerados modernos, pois suas técnicas, que possuem diferenças e melhorias entre elas, são utilizadas até os dias de hoje. Esses métodos são chamados de Criptografia Simétrica e Assimétrica.

Inicialmente, para a criptografia simétrica foi criado o padrão DES – Padrão de Ciframento de Dados (*Data Encryption Standart*). O sistema contava com uma chave de acesso ao código composta por 56 bits, sendo capaz de processar blocos de texto de 64 bits cada vez. Porém esse modelo tornou-se inseguro com o aumento do poder computacional. O modelo DES foi melhorado triplicando o poder da chave para 168 bits, porém ainda assim não foi suficiente. A partir disso, foi criado o padrão AES – Padrão Avançado de Ciframento (*Advanced Encryption Standart*). A diferença se encontra no tamanho da chave utilizada, que pode conter de 128 a 256 bits atuando em blocos de 128 bits de dados para cada análise (BARBOSA, *et al*, 2003).

O outro método de criptografia de acesso ao código de cifragem é a criptografia assimétrica. A segurança da criptografia da certificação digital utiliza esse padrão, pois é composta pela chave pública e chave privada. Daí a ideia de assimetria, diferença entre as chaves. O código de cifragem e de decifragem de uma informação criptografada usando o certificado digital, somente é acessado por uma chave autorizada. No processo de cifragem, ou criptografia de uma mensagem, é utilizada a chave pública de uma pessoa ou empresa. O processo inverso, ou seja, a decifragem, somente é possível acontecer se o destinatário daquela mensagem possuir uma chave privada compatível com a chave pública que foi utilizada na cifragem da mensagem. (Burnett e Paine, 2002)

3.1.1 Comparativo criptografia simétrica e assimétrica.

Como já foi visto anteriormente, ambos os métodos de criptografia são bastantes seguros e utilizados até os dias de hoje. O que os diferenciam, de modo simplificado, é que a criptografia assimétrica, utiliza a diferença entre as duas chaves para dobrar sua força de segurança. Isso se dá pelo fato que para que a mensagem seja interpretada, é necessária ter sempre as duas chaves. O que não ocorre no método simétrico, pois conta com uma única chave de acesso à mensagem. Claro que pela segurança e poder de criptografia fornecida, graças aos 128 bits da chave, é realmente muito eficiente, mas proporciona a facilidade de ter que quebrar apenas uma única chave para ter acesso à mensagem. Ou seja, para quebrar a criptografia de acesso ao código de cifragem, o invasor deverá quebrar uma única criptografia na simétrica, enquanto na criptografia assimétrica o trabalho é dobrado. Como é a criptografia utilizada nos certificados digitais, pode se considerar uma segurança segura para uma mensagem ou documento (BARBOSA, *et al*, 2003).

3.2 Criptografia Assimétrica

3.2.1 Definição

Assimetria resume a ideia de contrário à igualdade. Essa contrariedade à igualdade, ou diferença, entre as chaves foi desenvolvida com o objetivo de ser criada a chave privada e a chave pública. Apesar de diferentes, ambas as chaves possuem uma ligação entre si através de uma ligação matemática. (CASAGRANDE, 2011, p. 21)

3.2.2 Segurança

A chave pública é composta por algumas informações únicas da chave publica que se relacionam a outras informações da chave privada também unicas. Essas informações são relacionamentos matemáticos que partem de resultados de contas matemáticas, como a fatoração de um número. O resultado de uma fatoração de um numero da chave privada pode estar presente em uma parte da chave pública, por exemplo. (CASAGRANDE,, 2011, p. 21)

Para que uma mensagem seja decriptografada é necessário que o agente possua a chave privada relacionada à chave pública que foi utilizada no momento da criptografia da mensagem. No momento da decriptação da mensagem é feita uma validação, ou conferencia para que, se

essas informações se relacionarem, a mensagem possa ser acessada. Um exemplo real dessas informações utilizadas na comparação entre chaves é o número de série de cada uma das chaves, o que por sua vez possui uma relação matemática.

A chave pública, como o próprio nome já diz, é acessível por qualquer pessoa. Isso garante que a mensagem pode ser criptografada, para que assim, seja encaminhada ao seu destinatário. O local de armazenamento dessas chaves públicas é fornecido por uma Autoridade Certificadora (AC). No momento da emissão de um certificado é gerado a chave privada (que é entregue ao usuário) e a chave pública (que é armazenada no diretório público da AC). No momento de uma encriptação de uma mensagem, o emissor utiliza a chave pulica do destinatário para criptografar a mensagem.

Após o recebimento dessa mensagem ainda criptografada, o usuário deverá apresentar sua chave privada, para que após a conferencia de relacionamento entre as chaves a mensagem seja convertida ao seu estado original e disponibilizada para leitura.

Definitivamente, a segurança de todo o processo de criptografia assimétrica é focada na proteção da chave privada, garantindo que ninguém tenha acesso à mesma, pois de posse dela é possível acessar a mensagem original.

3.2.3 Aplicação

A segurança da certificação digital, criptografia assimétrica, é utilizada na transmissão de mensagens (vídeos, áudios, fotos e texto) no maior aplicativo de conversas instantâneas, para dispositivos móveis do mundo, o Whatts App.

Segundo Rohr, Araújo e Gomes (2016, p.1), “em cinco de abril de 2016, o whatts app anunciou a todos os poucos mais de 600 milhões, de usuários, que as mensagens transmitidas através do aplicativo possuiriam a segurança da criptografia chamada de “ponta a ponta”. Essa criptografia tem o funcionamento da criptografia assimétrica, pois todos os usuários do whatts app possuem uma chave privada e uma chave pública, e elas são usadas para criptografar uma mensagem no ato do envio, para que possa ser decriptografada pelo destinatário desejado, utilizando a sua chave privada, que com já foi detalhado anteriormente, tem relação direta com a chave pública. O armazenamento da chave pública nesse caso, fica por conta da empresa regente do aplicativo.

O termo ponta a ponta, nomeia de forma subliminar cada usuário como sendo um a “ponta” de uma conversa. Faça uma analogia utilizando uma tubulação. Essa tubulação é o meio de transferência das mensagens (internet), onde em cada ponta se encontra um usuário. A

criptografia nesse caso é a tubulação em si, pois garante que ninguém tenha acesso à informação que ali transita, se não tiver acesso à tubulação. Esse “acesso” são os grupos.

4. TIPOS DE CERTIFICADOS DIGITAIS.

4.1. Certificado tipo A1.

Um certificado do tipo A1 pode ser utilizado tanto por uma pessoa física (CPF) ou uma empresa (CNPJ). Em ambos os casos o certificado A1 é emitido no próprio computador do usuário. O processo de emissão é simples e pode ser realizado apenas pelo seu titular ou representante, no caso de CNPJ, no computador onde será utilizado. Ele tem validade de 1 ano, que começa a contar a partir do momento de sua emissão.

A emissão somente acontece após a validação, que é a conferencia das documentações que são apresentadas à uma AR (Autoridade Certificadora). Durante a validação é impresso e entregue um código de emissão A1 pela autoridade responsável da validação. Após a finalização da validação, a AC (Autoridade Certificadora) vinculada à AR, enviará um código de emissão A2. De posse do código 1 e 2, o usuário poderá realizar a emissão.

No momento da emissão é solicitada a criação de uma senha, que deverá ser digitada em cada uso desse certificado. Uma vez emitido o certificado torna-se um arquivo, e esse arquivo poderá ser instalado no computador que o usuário necessitar. Lembrando que no momento da instalação ou utilização o mesmo deverá sempre digitar a senha, pois é essa senha que permite acesso ao algoritmo de criptografia do certificado, permitindo assim consequentemente, o acesso a determinado sistema, ou documento, garantindo a confidencialidade da informação apenas à quem é destinada.

O arquivo criado no momento da emissão do certificado A1 é a chave privada do certificado daquele usuário (ITI, 2012). A baixa segurança desse tipo de certificado se dá pelo fato de a chave privada ser um simples arquivo que poderá ser armazenado, copiado, enviado ou transferido de um computador para outro. Isso abre uma porta para a insegurança, pois visto que a senha é apenas um PIN de 4 a 6 dígitos, descobrir essa senha, ou quebrar a segurança da chave é mais fácil.

4.2. Certificado tipo A3

O certificado do tipo A3 com relação a emissão segue os mesmos padrões do tipo A1, com a opção de ser emitido no ato da validação pela Autoridade de Registro responsável pela validação. Agora, com relação a segurança, o A3 é realmente o diferencial, pois no momento da emissão é criado uma chave pública, esta será armazenada em diretório online, criado e disponibilizado pela certificadora, e a emissão da chave privada, que acontece dentro de um dispositivo físico, como ilustrado na figura 3 abaixo, que pode ser um Smartcard ou até mesmo um token. (ITI, 2013)

Figura 3 - Leitora USB / Token USB / Smartcard Criptográfico

Fonte: Revista Digital nº 8 – Instituto Nacional de Tecnologia da Informação – 2013

O token é semelhante à um pendrive, que utiliza apenas a conexão USB, já o Smartcard necessita de uma leitora para conectar-se ao computador.

4.2.1. Smartcard

O Smart Card é um dispositivo físico que armazena informações pessoais do usuário, bem como informações pertinentes à chave privada que ele representa, incluindo dados do certificado como data de emissão, serial, emissor, etc. O Smart Card, é semelhante ao cartão de credito ou debito, utilizado pelos bancos hoje em dia. Na verdade, a analogia da utilização à aplicação do smart card, é a mesma do cartão de debito para com o certificado digital. O smart

card possui um microchip com um microcontrolador integrado para processamento e armazenamento das informações.

> Segundo Matos (2017, p. 3) “A capacidade de um smart card é definida pelo seu circuito integrado. Tipicamente, um circuito integrado consiste de um microprocessador, memória apenas de leitura ROM /RAM não estática e uma EEPROM que manterá seu estado quando a alimentação for removida.”.

A comunicação dos smart cards é limitada a 9600 bits por segundo e segue o protocolo de comunicação ISO 7816/3;

4.2.1.1. Token

O Token é também um dispositivo físico para armazenamento do certificado e de informações dos usuários, assim como o smart card, mas o que o diferencia do smart card é asua segurança e sua capacidade. Enquanto o smart card possui capacidade de até 128 Kbits, o token consegue armazenar até 72KBytes. Ou seja, se 128 Kbits são 16 KBytes, o token tem capacidade de armazenamento de quase 5 vezes mais que o smart card.

Além disso, a chave criptográfica do token pode chegar a 2048 bits. Isso garante ao usuário gravar uma senha de acesso alfanumérica, onde a tentativa de quebra da chave para acesso ao algoritmo de criptografia é bem mais complicada do que no smart card. A chave criptografia do token é do tipo SHA. (Digital Security do Brasil, 2016)

4.2.1.2. Secure Hash Algorithm - SHA

SHA significa algoritmo de hash seguro (*secure hash algotithm). Hash* é um algoritmo matemático responsável pela transformação de um bloco de dados (no caso a chave criptográfica) em uma serie de caracteres de comprimento fixo. Uma tradução análoga ao algoritmo de criptografia presente nos certificados digitais. (CASTELLÓ e VAZ, [21-?])

Resumindo, SHA é um resumo de algoritmo criptografado que permite acesso ao algoritmo que criptografa uma informação, no momento do uso da chave privada de um certificado digital.

4.3. Certificado tipo SSL

SSL (Secure Socket Layer) significa em uma tradução tecnóloga à ambiente de conexão segura. O SSL é utilizado internamente na comunicação entre o navegador utilizado

pelo usuário para acessar um site qualquer, e o servidor onde está armazenado esse site. A comunicação funciona da seguinte forma; ao acessar um site com esse tipo de segurança, o navegador solicita ao servidor de armazenamento do site o seu certificado SSL, ao receber a solicitação, o servidor por sua vez o enviará, e nesse momento o navegador realizará a verificação e conferencia da identidade desse certificado. Uma vez confirmada a identidade e autenticidade do certificado, o navegador ira liberar a comunicação entre usuário e site. Toda e qualquer informação que é transmitida entre usuário e site, passa por um processo de criptografia, para que assim a informação que é enviada do usuário para o servidor, ou vice-versa, levará com ela a garantia de que a informação enviada chegou e sempre chegará sem nenhuma intervenção ou interferência (BARBOSA, *et al*, 2003).

O uso do certificado SSL é muito comum nos dias de hoje, principalmente em sites de lojas virtuais e-commerce (sites de compras e vendas), pois como são realizadas transferências de informações sigilosas (dados pessoais, bancários, dados de cartões, etc.) essa segurança fornecida pelo certificado SSL garante a tranquilidade ao usuário de que suas informações estarão sempre seguras e causa um destaque para o site, pois mostra que o mesmo se preocupa com a segurança da informação e a tranquilidade de seus usuários.

5. APLICAÇÕES

O certificado digital, graças à sua segurança permite o uso em diversas atividades no dia a dia de empresas e cidadãos. Muitas das maneiras de utilização do certificado não são de conhecimento da sociedade. A facilidade proposta com o certificado, somado com a segurança que ele proporciona ao usuário, são motivos de sobra para que qualquer um que tenha uma conta em um banco ou até mesmo uma empresa utilize o certificado, mas não é o que acontece. O certificado existe e vêm crescendo com o passar do tempo, mas sua utilização apesar de estar em constante evolução ainda está consideravelmente abaixo do possível. Talvez essa diferença se dá pelo custo empregado na aquisição.

5.1. Certificado Digital Pessoa Física

Como já comentado anteriormente, hoje qualquer cidadão pode ter o seu próprio certificado digital. O custo pode oscilar entre as Autoridades Certificadoras, mas a aplicação é a mesma, pois a estrutura desse certificado é regulamentada pela ICP (Infraestrutura de Chaves Públicas Brasileira). Cada tipo de certificado tem a sua aplicação, e também a sua restrição.

5.1.1.1. Procuração

Existem ações obrigatórias que algumas pessoas devem executar junto à RFB (Receita Federal do Brasil). Uma dessas ações é acesso ao e-CAC (Centro Virtual de Atendimento ao Contribuinte) onde lá são executadas a transferência e declaração de valores e impostos pagos pelo contribuinte, por exemplo. Em casos específicos, uma pessoa física, pode designar o poder de transmissão e declaração dessas informações para a RFB, a outra pessoa física. Essa procuração é eletrônica, tem validade definida, de uso restrito no site e é irrecusável. Porém, como já informado, para elaborar essa procuração o emitente deve possuir um certificado digital, pois assim a RFB fará a verificação de sua identidade e designará o poder destinado a outra pessoa física. É importante destacar que esse procurador mencionado deve também possuir certificado digital em seu CPF.

5.1.1.2. Assinatura Digital

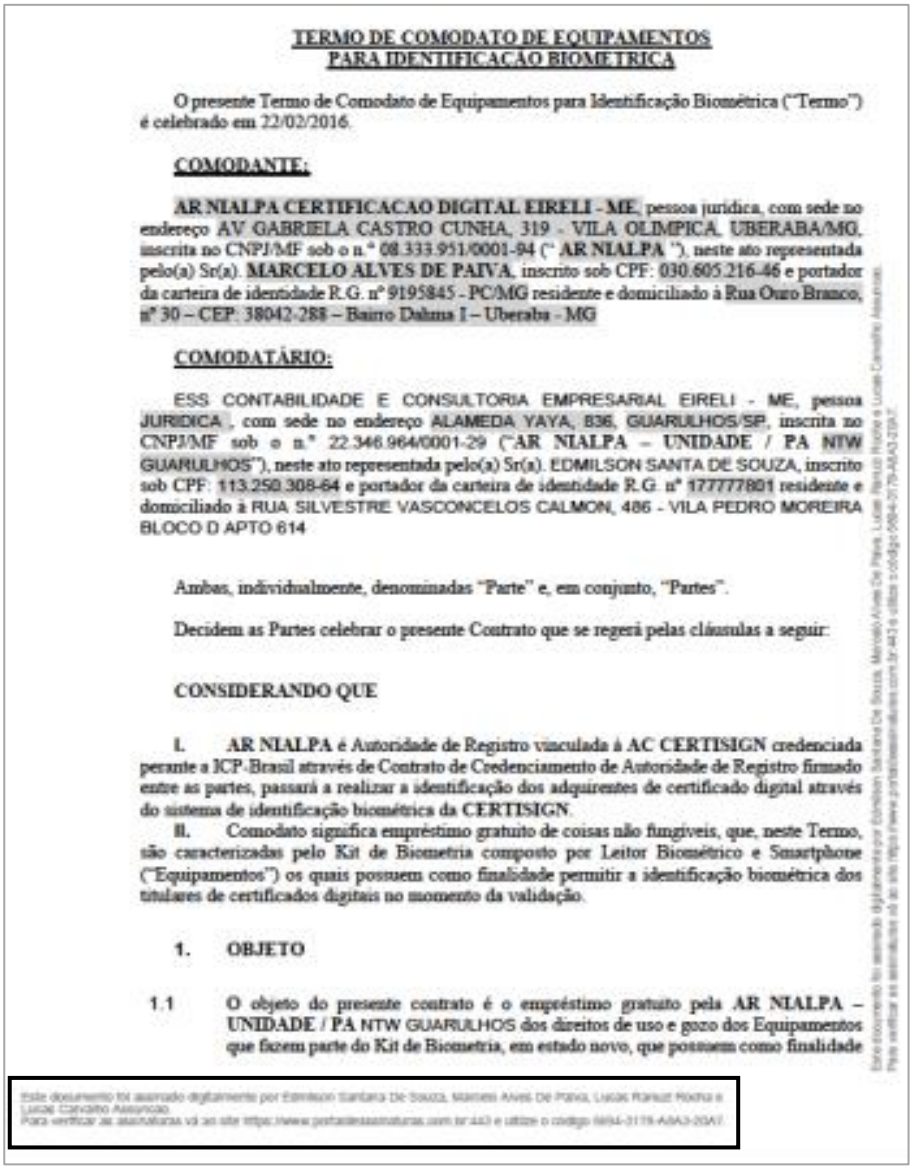
A assinatura digital, como o próprio nome diz, consiste em assinar determinado documento de forma digital. O processo utiliza exclusivamente o certificado e-CPF A3, pois se faz necessário o uso de chave pública e privada com a segurança SHA. O processo constitui basicamente em assinar um documento e encaminhar ele para alguém ou alguma empresa. Após assinado o documento ganha informações que poderão e deverão ser utilizadas pelo destinatário para conferencia e validação da informação, para garantir a autenticidade daquele documento.

Toda mensagem no momento de sua encriptação passa por um processo de resumo, esse processo é chamado de HASH. O Hash faz com que esse resumo (que é parte da mensagem original) seja criptografado juntamente à chave. A verificação ou confirmação da veracidade da assinatura, consiste em comparara o hash da mensagem e o resumo que acompanha a chave pública do emitente. Como o resumo acompanha a chave, após a decriptação é realizada a comparação entre o resumo enviado e o resumo encriptado. A igualdade entre os resumos garante que a mensagem não foi modificada.

Um programa gratuito que pode ser utilizado para assinar e validar a assinatura de um documento é o Adobe Acrobat Reader. Mas existem portais online onde qualquer usuário pode assinar e armazenar aquele documento assinado.

A figura 4 apresenta uma página de um documento qualquer assinado digitalmente através de um portal (online) de assinaturas digitais. No destaque [5] da figura 4, percebe-se que é grafado no documento (parte inferior e lateral direita) uma informação mencionando quem assinou aquele documento, um link e um código de verificação para que caso o destinatário desse documento não seja uma das pessoas envolvidas nas assinaturas, possa conferir o documento afim de validar a sua integridade. A informação comentada foi transcrita no rodapé deste página.

Figura. 4 – Fragmento de um documento assinado digitalmente.



TERMO DE COMODATO DE EQUIPAMENTOS PARA IDENTIFICAÇÃO BIOMETRICA

O presente Termo de Comodato de Equipamentos para Identificação Biométrica ("Termo") é celebrado em 22/02/2016.

COMODANTE:

AR NIALPA CERTIFICACAO DIGITAL EIRELI - ME, pessoa jurídica, com sede no endereço AV GABRIELA CASTRO CUNHA, 319 - VILA OLIMPICA, UBERABA/MG, inscrita no CNPJ/MF sob o n.º 08.333.951/0001-94 (" **AR NIALPA** "), neste ato representada pelo(a) Sr(a). **MARCELO ALVES DE PAIVA**, inscrito sob CPF: 030.605.216-46 e portador da carteira de identidade R.G. nº 9195845 - PC/MG residente e domiciliado à Rua Ouro Branco, nº 30 – CEP: 38042-288 – Bairro Dalma I – Uberaba - MG

COMODATÁRIO:

ESS CONTABILIDADE E CONSULTORIA EMPRESARIAL EIRELI - ME, pessoa JURIDICA , com sede no endereço ALAMEDA YAYA, 836, GUARULHOS/SP, inscrita no CNPJ/MF sob o n.º 22.346.964/0001-29 ("**AR NIALPA – UNIDADE / PA NTW GUARULHOS**"), neste ato representada pelo(a) Sr(a). EDMILSON SANTA DE SOUZA, inscrito sob CPF: 113.250.308-64 e portador da carteira de identidade R.G. nº 177777801 residente e domiciliado à RUA SILVESTRE VASCONCELOS CALMON, 486 - VILA PEDRO MOREIRA BLOCO D APTO 614

Ambas, individualmente, denominadas "Parte" e, em conjunto, "Partes".

Decidem as Partes celebrar o presente Contrato que se regerá pelas cláusulas a seguir:

CONSIDERANDO QUE

I. **AR NIALPA** é Autoridade de Registro vinculada à **AC CERTISIGN** credenciada perante a ICP-Brasil através de Contrato de Credenciamento de Autoridade de Registro firmado entre as partes, passará a realizar a identificação dos adquirentes de certificado digital através do sistema de identificação biométrica da **CERTISIGN**.

II. Comodato significa empréstimo gratuito de coisas não fungíveis, que, neste Termo, são caracterizadas pelo Kit de Biometria composto por Leitor Biométrico e Smartphone ("Equipamentos") os quais possuem como finalidade permitir a identificação biométrica dos titulares de certificados digitais no momento da validação.

1. **OBJETO**

1.1 O objeto do presente contrato é o empréstimo gratuito pela **AR NIALPA – UNIDADE / PA NTW GUARULHOS** dos direitos de uso e gozo dos Equipamentos que fizem parte do Kit de Biometria, em estado novo, que possuem como finalidade

Este documento foi assinado digitalmente por Edmilson Santana De Souza, Marcelo Alves De Paiva, Lucas Ranuzi Rocha e Lucas Carvalho Assunção.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5694-3178-A8A3-20A7.

Fonte: Acervo do Autor, 2016

[5] "Este documento foi assinado digitalmente por Edmilson Santana de Souza, Marcelo Alves de Paiva, Lucas Ranuzi Rocha e Lucas Carvalho Assunção.
Para verificar as assinaturas vá ao site: https://www.portaldeassinaturas.com.br:443 e utilize o código: 5694-3178-A8A3-20A7"

No momento que entra no sistema e valida a informação, o usuário consegue baixar o arquivo e no final dele para conferencia é entregue um formulário confirmando que o documento foi assinado pelas pessoas citadas (incluindo o CPF dos responsáveis), bem como o HASH, que é a informação criada a partir do documento e transmitida juntamente com o mesmo para conferencia das chaves privadas de cada um dos assinantes. Esse documento de confirmação está apresentado na figura 5.

Imagine uma situação em que um empresário decide vender um imóvel de sua empresa, assim, elabora um contrato de compra e venda. Esse contrato é assinado de forma digital e encaminhado para o comprador. O comprador, por sua vez, pode abrir aquele PDF assinado no Acrobat e o programa lhe dirá se aquele documento está assinado, por quem e , inclusive, se a assinatura ainda é válida (o que acontece apenas se o documento não foi modificado). Em um portal o documento assinado ganha impressão de informações na lateral que possibilitam a validação da assinatura, como exemplificado na figura abaixo, o documento ganha um código de verificação. O destinatário entra no portal (que é online e público) digita o código de identificação e o código de verificação daquele documento assinado, como na figura 5 abaixo. Se todas as informações apresentadas estiverem de acordo, o destinatário conseguira inclusive visualizar o documento diretamente no portal, e assim confirmar mais uma vez que o documento apresentado é o documento original sem nenhuma intervenção não autorizada.

Figura 5 – Comprovante de validação de conferencia de assinaturas.

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Portal de Assinaturas Certisign. Para verificar as assinaturas clique no link: https://www.portaldeassinaturas.com.br/Verificar/5694-3178-A8A3-20A7 ou vá até o site https://www.portaldeassinaturas.com.br:443 e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: 5694-3178-A8A3-20A7

Hash do Documento
F0760A23340BBE2AC901D84CE9FA6473A6EC2AD8A23EDC68037C6CAA85F7ED48

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 27/05/2017 é(são) :

- Lucas Carvalho Assuncao (Testemunha) - 076.573.456-75 em 29/02/2016 17:10 UTC-03:00
  Tipo: Certificado Digital
- Lucas Ranuzi Rocha (Testemunha) - 095.410.816-73 em 29/02/2016 17:13 UTC-03:00
  Tipo: Certificado Digital
- Edmilson Santana De Souza (Parte) - 113.250.308-64 em 01/03/2016 11:18 UTC-03:00
  Tipo: Certificado Digital
- Marcelo Alves De Paiva (Parte) - 030.605.216-46 em 07/03/2016 19:09 UTC-03:00
  Tipo: Certificado Digital

Fonte: Acervo do Autor, 2016

Figura 6 – Tela de verificação de assinaturas.

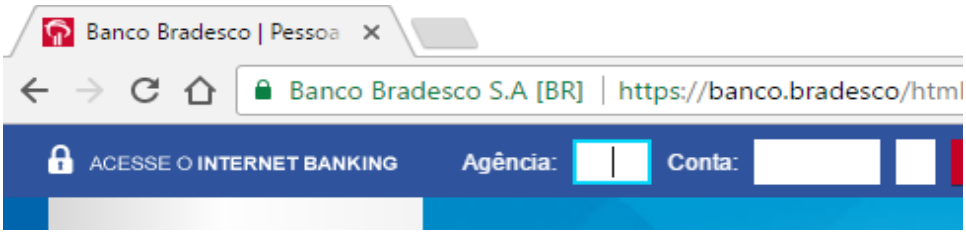
Fonte: https://www.portaldeassinaturas.com.br/VerificadorAssinaturas/Index

5.1.1.3. Internet Banking

O uso de sistemas bancários online (internet banking) hoje em dia é cada constante. Uma forma de aumentar a garantia de acesso restrito a uma determinada conta seja exclusivamente do seu titular, alguns bancos possuem a alternativa de acesso à sua conta por meio do certificado digital. Essa forma de login é cadastrada através de um acesso convencional (usuário e senha cadastrado) para que uma vez dentro da conta, o usuário vai até o painel de configurações e cadastra o seu certificado digital para conectar-se à sua conta. No próximo login, o usuário irá selecionar o acesso mediante certificado digital e neste momento será solicitada a senha do certificado, podendo assim, confirmar a identidade do titular da conta a ser acessada, através dos dados do titular contidos dentro do certificado digital. O detalhe primordial dessa aplicação é que o único certificado digital que pode ser utilizado é o certificado do tipo A3, por possuir um nível de segurança avançado.

O site de um internet banking, assim como outros sites de e-commerce que possuem a segurança da certificação digital (SSL) inserida em seu funcionamento, é identificada pelo usuário através de um cadeado verde ao lado do link, como é apresentado na figura 6 abaixo.

Figura 7 – Visualizaçao do simbolo de segurança no navegador.



Fonte: Acervo do Autor, 2017

Por isso, ao acessar um site, verifique a segurança do mesmo e caso encontre esse "sinal" de segurança, fique tranquilo, ali existe a certificação digital. Na maioria dos casos, os sites que apresentam esse tipo de segurança proporcionam funções de envio e recebimento de informações. Confirmando assim, um dos principais objetivos da segurança da certificação.

6. CONSIDERAÇÕES FINAIS

Todo o estudo e fundamentação para a elaboração desse trabalho, foi motivado pela percepção de que muitos usuários não conhecem a certificação digital, não sabem que a têm e muito menos que a usam. Já no final espera-se que tenha sido proveitoso conhecer sobre a certificação digital, com ênfase em sua segurança, pois sabendo de sua eficácia é possível implementar essa segurança nas atividades do dia a dia.

A metodologia de estudo e busca pela informação concreta e confiável, se deu através da leitura de diversos artigos, sites, revistas e até mesmo livros que falam sobre a certificação digital, focada na segurança utilizada.

Como mencionado no início do trabalho o uso dessa proteção virtual ainda é pequeno no contexto virtual mundial. E, visando difundir o conhecimento sobre a certificação digital, especificações, bem como suas aplicações este trabalho apresentou algumas das formas de certificação digital para que ainda o leitor possa confiar na utilização e aplicar em algum possível negócio, ou fazer uso em suas aplicações virtuais diárias.

Compreendendo a segurança da certificação digital e suas aplicações, as ações no mundo virtual serão realizadas com mais segurança e tranquilidade graças ao uso da certificação digital. Diante disso, conclui-se que o certificado digital é uma ferramenta de grande utilidade e forte impacto na segurança de sites e sistemas. E de forma satisfatória, pode se afirmar e definir o papel deste trabalho como uma fonte de conteúdo e conhecimento sobre algo que hoje pode e deve ser aplicado ao mundo virtual, a Segurança da Certificação Digital.

7. ANEXOS

Anexo 1 – Exemplo de Algoritmo de Cifragem:

```
public class EncriptaDecriptaRSA {

public static final String ALGORITHM = "RSA";

// Local da chave privada no sistema de arquivos.
public static final String PATH_CHAVE_PRIVADA =
"C:/keys/private.key";

// Local da chave pública no sistema de arquivos.
public static final String PATH_CHAVE_PUBLICA =
"C:/keys/public.key";

public static void geraChave() {
  try {
    final KeyPairGenerator keyGen =
KeyPairGenerator.getInstance(ALGORITHM);
    keyGen.initialize(1024);
    final KeyPair key = keyGen.generateKeyPair();

    File chavePrivadaFile = new File(PATH_CHAVE_PRIVADA);
    File chavePublicaFile = new File(PATH_CHAVE_PUBLICA);

    // Cria os arquivos para armazenar a chave Privada e a chave Publica
    if (chavePrivadaFile.getParentFile() != null) {
      chavePrivadaFile.getParentFile().mkdirs();
    }

    chavePrivadaFile.createNewFile();

    if (chavePublicaFile.getParentFile() != null) {
      chavePublicaFile.getParentFile().mkdirs();
    }

    chavePublicaFile.createNewFile();

    // Salva a Chave Pública no arquivo
    ObjectOutputStream chavePublicaOS = new ObjectOutputStream(
        new FileOutputStream(chavePublicaFile));
    chavePublicaOS.writeObject(key.getPublic());
    chavePublicaOS.close(); // Salva a Chave Privada no arquivo
    ObjectOutputStream chavePrivadaOS = new ObjectOutputStream(
        new FileOutputStream(chavePrivadaFile));
    chavePrivadaOS.writeObject(key.getPrivate());
    chavePrivadaOS.close();
  } catch (Exception e) {
    e.printStackTrace();
  }
}

public static boolean verificaSeExisteChavesNoSO() {

  File chavePrivada = new File(PATH_CHAVE_PRIVADA);
  File chavePublica = new File(PATH_CHAVE_PUBLICA);

  if (chavePrivada.exists() && chavePublica.exists()) {
    return true;
  }
  return false;
}

// Criptografa o texto puro usando chave pública.
public static byte[] criptografa(String texto, PublicKey chave) {
  byte[] cipherText = null;

  try {
    final Cipher cipher = Cipher.getInstance(ALGORITHM);
    // Criptografa o texto puro usando a chave Pública
    cipher.init(Cipher.ENCRYPT_MODE, chave);
    cipherText = cipher.doFinal(texto.getBytes());
  } catch (Exception e) {
    e.printStackTrace();
  }

  return cipherText;
}

// Decriptografa o texto puro usando chave privada.

public static String decriptografa(byte[] texto, PrivateKey chave) {
  byte[] dectyptedText = null;

  try {
    final Cipher cipher = Cipher.getInstance(ALGORITHM);
    // Decriptografa o texto puro usando a chave Privada
    cipher.init(Cipher.DECRYPT_MODE, chave);
    dectyptedText = cipher.doFinal(texto);

  } catch (Exception ex) {
    ex.printStackTrace();
  }

  return new String(dectyptedText);
}

// Testa o Algoritmo
public static void main(String[] args) {

  try {

    // Verifica se já existe um par de chaves, caso contrário gera-se as
chaves..
    if (!verificaSeExisteChavesNoSO()) {
     // Método responsável por gerar um par de chaves usando o algoritmo
RSA e
     // armazena as chaves nos seus respectivos arquivos.
      geraChave();
    }

    final String msgOriginal = "Exemplo de mensagem";
    ObjectInputStream inputStream = null;

    inputStream = new ObjectInputStream(new
FileInputStream(PATH_CHAVE_PUBLICA));
    final PublicKey chavePublica = (PublicKey) inputStream.readObject();
    final byte[] textoCriptografado = criptografa(msgOriginal,
chavePublica);

    inputStream = new ObjectInputStream(new
FileInputStream(PATH_CHAVE_PRIVADA));
    final PrivateKey chavePrivada = (PrivateKey)
inputStream.readObject();
    final String textoPuro = decriptografa(textoCriptografado,
chavePrivada);

    System.out.println("Mensagem Original: " + msgOriginal);
    System.out.println("Mensagem Criptografada: "
+textoCriptografado.toString());
    System.out.println("Mensagem Decriptografada: " + textoPuro);

  } catch (Exception e) {
    e.printStackTrace();
  }
 }
}
```

Fonte: MEDEIROS [21 - ?]

8. REFERÊNCIAS

ITI, Instituto de Nacional de Tecnologia da Informação - Certificação Digital. 2012. Disponível em <http://www.iti.gov.br/certificacao-digital>. Acesso em: 03 nov. 2016.

ARISP – Associação dos Registradores Imobiliarios de São Paulo – **Assinador Digital.** [21-?]. Disponivel em <http://www.arisp.com.br/>. Acesso em 27 abr. 2017

ELETRÔNICO, Oficio. **Cartilha da Certificação Digital. –** [21-?]. Disponivel em <https://www.oficioeletronico.com.br/>. Acesso em 28 abr. 2017.

SOTERO, Sérgio. **iMasters - Criptografia e Certificação Digital.** 2003**.** Disponível em <https://imasters.com.br/artigo/1209/dotnet/criptografiaecertificacaodigital/?trace=151902 01197&source=single>. Acesso em: 24 abr. 2017.

BURNETT, Steve, *et al.* **Criptografia e Segurança** – o Guia Oficial RSA. Tradução aprovada por RSA PRESS. 3 ed. [2002] - Rio de Janeiro: CAMPUS.

BARBOSA, Luís Alberto de Moraes. *et al*. **RSA** – Criptografia Assimétrica e Assinatura Digital. 2003, 50 p. Trabalho de curso (Especialização em Redes de Computadores) – Universidade Estadual de Campinas, Campinas.
Disponível em <http://www.braghetto.eti.br/files/Trabalho%20Oficial %20Final%20RSA.pdf > Acesso em: 22 dez. 2016.

CASAGRANDE, Airton Ruberval. **Certificação Digital** 2011, 31 p. Trabalho de curso (Especialização em Configurações e Gerenciamento e Servidores e Equipamentos de Redes) Universidade Tecnóloga Federal do Paraná, Curitiba. Disponível em <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/392/3/CT_GESER_1_2011_01.pdf>. Acesso em: 28 abr. 2017.

ROHR, Altieres, *et al.* **Criptografia no Whatsapp:** veja em vídeo como funciona o novo "sigilo"**.** 2016.
Disponível em <http://g1.globo.com/tecnologia/noticia/2016/04/criptografia-no-whatsapp-veja-em-video-como-funciona-novo-sigilo.html>. Acesso em: 12 maio 2017.

MATOS, Conrado Leiras. **Smart Card.** 1997. Disponível em <https://www.gta.ufrj.br/grad/01_2/Smartcard/smartcard.html>. Acesso em: 28 abr. 2017.

BRASIL, Digital Security. **Produtos** [21-?]. Disponível em: <http://www.digitalsecurity.com.br/comprar-token-usb-e_cpf-e_cnpj-para-certificado-digital.aspx>. Acesso em: 28 abr. 2017.

CASTELLÓ, Tiago; VAZ, Verônica. **Assinatura Digital**. [21-?]. Disponível em: <https://www.gta.ufrj.br/grad/07_1/ass-dig/TiposdeCriptografia.html>. Acesso em: 28 abr. 2017.

MEDEIROS, Higor; **Criptografia Assimétrica –** Criptografando e Descriptografando dados em java. [21-?]. Disponível em: <http://www.devmedia.com.br/criptografia-assimetrica-criptogradando-e-descriptografando-dados-em-java/32113>. Acesso em: 10 abr. 2017