ARTIGO

ASSINATURAS DIGITAIS E ARQUIVOLOGIA

Ernesto Carlos Bodê
bode@stj.gov.br

Resumo

O trabalho apresenta a tecnologia que possibilita a implementação do uso de assinaturas digitais em documentos eletrônicos. É apresentada a fundamentação sobre criptografia, algoritmos criptográficos, chaves criptográficas, a infra-estrutura de chaves públicas além do uso de certificados de assinaturas digitais. O conceito de assinatura e seu correspondente eletrônico e digital é abordado, tanto do ponto de vista tecnológico como do ponto de vista sócio cultural e legal. O uso do documento eletrônico, sua autenticidade e conseqüente utilização como documento arquivístico é analisado. Conclui-se o artigo com possíveis conseqüências para os documentos eletrônicos e a arquivologia.

Palavras-chave: criptografia simétrica, criptografia assimétrica, infra-estrutura de chaves públicas, assinatura digital, documento eletrônico, autenticidade, arquivologia.

Digital signatures, record management and archives

Abstract

This article presents the main technology which supports digital signatures within electronic records. We present the fundamentals about cryptographic, cryptographic algorithm, cryptographic keys, public key infrastructure and the correlated certificates. We show the meaning of signature and its correspondent on digital world, also from technology point of view as from cultural and legal ones. The use of electronic records, its authentication and its use as a record is analyzed, as well, possible consequences to record management and archives.

Keywords: symmetric cryptography, asymmetric cryptography, public key infrastructure, digital signature, electronic record, authentication, record management, archival science.

Introdução

Este trabalho abordará o tema das assinaturas digitais e as possíveis relações deste com a arquivologia, especificamente no que tange aos documentos eletrônicos com valor arquivístico. O tema é ainda novo no mundo em geral (algumas décadas), como veremos, e menos maduro ainda nas áreas de estudo e prática com documentos tradicionais ou digitais, como demonstram as propostas, tanto científicas como legislativas.

Para a consecução deste objetivo, efetivaremos uma visão geral sobre as tecnologias que suportam a assinatura digital. Para o uso desta, fazem-se necessárias diversas outras tecnologias. Esta abordagem também possibilitará o entendimento de como se chegou ao conceito da assinatura digital em si, já que não se trata de um produto planejado para uso como tal, mas foi muito mais uma conseqüência de outras tecnologias, aplicadas para a comunicação de informações e documentos. Entre estas tecnologias, destaca-se o uso da criptografia em comunicação de dados e informações.

A compreensão do que é a assinatura digital, do ponto de vista tecnológico, possibilitará uma melhor compreensão do papel dos documentos no âmbito da arquivologia, no que cabe à Gestão Documental e conseqüências para os arquivos permanentes.

Abordaremos também aspectos jurídico/legais, de maneira ampla. Os aspectos legais também são fundamentais para o uso e consolidação de assinaturas digitais em documentos eletrônicos na atualidade.

1- Tecnologias Fundamentais

Para que seja possível compreender o que são assinaturas digitais, um recurso tecnológico que, aliás, é completamente diferente das assinaturas tradicionais, é preciso, também, conhecer outras tecnologias, como a *criptografia* e o uso de *chaves públicas*.

Adiantando-se a possíveis dúvidas, cabe neste ponto, esclarecer que quando falamos em assinaturas digitais, não estamos nos referindo à visualização de uma assinatura tradicional de próprio punho, digitalizada a partir de um scanner ou outro equipamento similar. Isto ficará claro ao longo deste artigo, de qualquer forma, este tipo de assinatura[1] "digital", se é que podemos chamá-la assim, traria uma série de problemas de segurança em função da facilidade com que qualquer pessoa, além daquela que

[1] Alguns autores classificam as assinaturas de próprio punho e digitalizadas como sendo do tipo eletrônicas, que se refere, de maneira geral, a diversas formas de identificação e inclui, entre outras, a biometrica (identificação por rasterização de impressões digitais).

efetivamente fez o modelo original com uma caneta, poderia reproduzir tal imagem digital.

A base para o uso de assinaturas digitais é a **criptografia**. Assim, vamos primeiramente abordar este tema. Criptografia pode ser definida como a *"Arte de escrever em cifra ou em código"* (FERREIRA, 1986, p. 499), "A palavra é de origem grega e formada pelas partes que, em português, significam secreta (*cripto*) e escrita (*grafia*)" (TRAIN, 2005, p. 27), em outras palavras, os procedimentos para embaralhar ou emaranhar as informações a serem transmitidas, de tal maneira que, apenas quem conheça a regra original, pode fazer o processo inverso (note que estamos falando de conhecer a mesma regra (e sua "chave") para criptografar e reverter o processo, o que em determinado momento histórico foi alterado).

O uso de criptografia parece existir desde a própria existência da escrita, "De acordo com Heródoto, foi a arte de escrita secreta que salvou a Grécia de ser conquistada por Xerxes, Rei dos reis, o líder déspota dos persas" (SINGH, 1999, p. 4, tradução nossa). Esta sempre esteve associada ao envio de mensagens importantes, ou seja, comunicação de documentos vitais (freqüentemente envolvendo transações de altos valores ou estratégias militares).

Desde sua invenção, o homem criou muitas maneiras de camuflar o conteúdo real de uma mensagem, como o uso do *scytale* espartano (500 AC),

> O *scytale* é um bastão de madeira ao redor do qual uma tira de couro ou pergaminho era enrolada [...]. O remetente escreve a mensagem no comprimento do *scytale*, desenrola a tira, que então parece carregar letras sem sentido (SINGH, 1999, p.8, tradução nossa).

No entanto, os métodos que envolvem fórmulas matemáticas se mostraram mais eficazes e hoje, a matemática é largamente utilizada.

Algoritmo é a palavra que descreve, no campo matemático, como uma informação é criptografada, assim como a reversão deste processo:

> Processo de cálculo, ou de resolução de um grupo de problemas semelhantes, em que se estipulam, com generalidade e sem restrições, regras formais para obtenção do resultado, ou da solução do problema" (FERREIRA, 1986, p. 84).

Vamos exemplificar utilizando um algoritmo trivial. Suponhamos que uma pessoa queira enviar uma mensagem secreta a um amigo cujo conteúdo é "VOLTE" e adote como regra criptográfica o algoritmo (CC = CM + *shift* à direita(1)), onde "*shift à*

direita(1)" significa deslocar a posição, no alfabeto de nosso vernáculo, em uma posição à direita, assim, "a" seria "b", "f" seria "g", "m" seria "n" o "z" (último caractere faria *shift* para o começo do alfabeto, o "a", *CC* significa Caractere Codificado e *CM* Caractere da Mensagem. No nosso exemplo então, aplicando este algoritmo, "V" vira "X", "O" vira "P", "L" vira "M", "T" vira "U" e "E" vira "F", assim a mensagem original "VOLTE" ficará criptografada em "XPMUF".

O destinatário da mensagem terá que saber qual é o segredo do algoritmo, para desfazer a criptografia, no caso, utilizando um algoritmo reverso que fará um *shift* para a esquerda, em cada caractere. Na prática, os algoritmos de criptografia podem ser bastante complexos, utilizando regras que requerem grande esforço de reversão.

Modernamente, as regras criptográficas são aplicadas para códigos binários digitais, já que no mundo dos computadores, toda informação é armazenada, recuperada e transmitida através de *bits*. As possibilidades de emaranhar as informações serão ainda mais sofisticadas, ainda mais se utilizarmos o poder e velocidade de computadores. E como reforço, a representação binária, por si só, já é uma maneira de criptografar, vejamos porquê. A regra geral é o uso de um grupo de *bits* (geralmente um *byte* = *8 bits*) representando cada número, letra, acento gráfico, pontuação e caracteres especiais como o *@.* Existem tabelas oficiais de codificação binária, a mais conhecida chama-se tabela ASCII[2] (*American Standard Code for Information Interchange*) e pode ser facilmente encontrada nos serviços de busca da *Internet*. Por exemplo, por uma destas tabelas, o caractere *"a"* (há códigos diferentes para maiúsculas e minúsculas) é representado através do **número binário** "01100001".

Independentemente do quão um algoritmo de criptografia possa ser complexo, ou seja, de como os caracteres de uma mensagem podem estar emaranhados, colocados fora de ordem e etc. Sempre precisará existir uma fórmula secreta necessária para reverter o processo criptográfico. Nos contextos históricos iniciais, isto não chegava a ser um problema. Por exemplo, um comandante poderia combinar o segredo com outros generais pessoalmente, e num segundo momento, quando estes recebessem uma mensagem, executariam o processo reverso na mensagem. No entanto, com a intensidade de mensagens enviadas, necessidade de celeridade e longas distâncias percorridas, o uso

[2] A Tabela ASCII (American Standard Code for Information Interchange) é usada pela maior parte da indústria de computadores para a troca de informações.

de equipamentos de telecomunicações tornou-se imprescindível, equipamentos como o telégrafo, rádio, fax, telefone e recentemente a Internet, tornaram-se comuns. O problema com estes equipamentos é que as mensagens podem ser monitoradas e interceptadas. É verdade que um cavaleiro carregando um pergaminho na idade média também poderia sê-lo. No entanto, no mundo das comunicações digitais, possíveis intervenções podem ser extremamente mais eficazes e sutis. Além disto, os governos e grandes corporações montaram equipes de profissionais especializados em decifrar os algoritmos criptográficos. Estes **criptógrafos** passaram a utilizar computadores (na verdade, os primórdios destes) para desvendar segredos de mensagens, sendo um dos mais famosos a máquina alemã *Enigma* (SINGH, 2002, p. 142).

Juntamente aos avanços na potência dos computadores e na área de criptografia (emaranhando e revertendo o processo), desvendar o algoritmo utilizado passou a não ser mais uma missão tão difícil assim, o que compromete a segurança das transmissões e eventuais problemas envolvendo segredos de Estado, grandes negócios e altos valores. Ao mesmo tempo, a utilização de softwares para criptografar e reverter o processo, exige o uso de um algoritmo bem definido e fixo para a elaboração do software correspondente.

Uma das primeiras soluções para este cenário, foi o **algoritmo DES**,

> O *Data Encryption Standard* (DES) tem sido usado largamente nas últimas décadas. O DES foi desenvolvido pela IBM no começo dos anos 70. O *National Bureau of Standards*, agora *National Institute of Standards and Technoloy* (NIST), originalmente solicitou propostas para um padrão de algoritmo criptográfico em 1973. O algoritmo da IBM tornou-se o padrão oficial do governo federal em 1977. (ATREYA, 2002, p. 32, tradução nossa)

Este complexo algoritmo, projetado para emaranhar os bits de uma mensagem, é conhecido publicamente e padronizado e, portanto pode ser implementado em qualquer software, que assim poderá decifrar uma mensagem criptografada. Porém, o que mantém a privacidade e impossibilita que a pessoa errada possa decifrar a mensagem, é a necessidade de um número binário (**chave**), essencial para o processo de reversão do algoritmo DES (como parte do cálculo matemático a ser executado), apenas as pessoas autorizadas que souberem este número poderão reverter o processo, *"O algoritmo é público, e as partes que se comunicam combinam uma chave secreta compartilhada para usar com o algoritmo"* (SCHNEIER, 2001, p. 97). Claro é que, conhecendo o algoritmo DES, qualquer pessoa pode fazer tentativas com *n* números até achar o correto. Embora

isto tome um tempo considerável[3], é possível encontrá-lo. Por questões de segurança, para mitigar a possibilidade de que a chave seja encontrada, as chaves criptográficas precisam ser substituídas periodicamente, o tempo maior ou menor dependerá do tamanho dos bits desta chave e da potência dos computadores no momento.

A necessidade de enviar, além da mensagem criptografada, o segredo do algoritmo criptográfico, sempre foi um grande problema que chamou a atenção dos pesquisadores na área. É paradoxal, há a necessidade de segredo nas comunicações, que exige a criptografia, por outro lado, o remetente desta mensagem continua com outro problema, enviar o segredo da reversão do processo (modernamente, apenas a chave do algoritmo), que também é uma mensagem em si. Com o incremento na freqüência das mensagens, a *distribuição de chaves* se tornou um problema tão sério quanto criptografar em si,

> Acompanhando o crescimento das redes de negócios, conforme mais mensagens eram enviadas, e mais chaves precisavam ser despachadas, os bancos perceberam que o processo de distribuição de chaves tornou-se um pesadelo logístico horrível e os custos proibitivos (SINGH, 1999, p.251, tradução nossa).

O grande problema que se coloca é: para mensagens criptografadas onde há a necessidade de uma chave secreta para reverter o processo criptográfico, como enviar tal chave ? Ressalta-se que o algoritmo criptográfico em si é conhecido por todos. Isto inclusive é desejável, pois por estar sujeito a um número maior de tentativas de encontrarem falhas, ao longo do tempo se o algoritmo resiste, isto prova que se trata de um bom algoritmo. Algumas instituições inclusive oferecem prêmios para quem conseguir encontrar pontos fracos no algoritmo (SINGH, 1999, p. 278).

Vamos exemplificar melhor, o que também conduzirá à solução encontrada para este problema. Na área da matemática, uma função é uma fórmula, através da qual obtêm-se um número (ou números), a partir de um outro (ou outros números). Por exemplo, na função ($x = y^2$), x será igual a 9 quando (e somente quando) y for igual a 3. Como ponderou Simon *"Nós podemos pensar em todas as formas de criptografia por computadores como funções, porque eles transformam um número, a mensagem original, em outro, a mensagem criptografada"* (SINGH, 1999, p. 260, tradução nossa). Vamos novamente utilizar o número binário "01100001", que representa o caractere minúsculo "a", esse número binário em codificação decimal, para simplificar, é igual a "97", assim,

[3] O tempo necessário para um computador encontrar a chave correta, por tentativa e erro, depende da capacidade de processamento destes computadores e da gama de possibilidades numéricas, sobre isto ver (SCHNEIER, 2001, p. 107)

aplicando a função acima, x resultará em "9409", ou seja (97^2). Note que, neste exemplo, conhecendo-se o algoritmo ($x = y^2$) e a mensagem codificada "9409", torna-se fácil encontrar y, pois a função reversa é (y = raiz quadrada de x). Mas, nem todas as funções são reversíveis, algumas geram números, mas não se pode reverter o processo[4], a não ser por tentativa e erro, o que, dependendo do algoritmo e do tamanho dos números pode ser quase impraticável.

Em 1976, a partir do uso de funções não reversíveis e números primos gigantescos, Diffie, Hellman e Merkle anunciaram publicamente um esquema que possibilita o estabelecimento de um número escolhido individualmente entre remetente e destinatário, o qual pode ser utilizado como chave de um esquema criptográfico. Para uma explicação detalhada de como funciona tal esquema veja (SINGH, 1999, p. 265) ou (BENANTAR, 2002, p. 25). Note que não se trata exatamente de uma proposta de criptografia, mas uma solução para estabelecimento do número secreto (chave), o qual pode ser utilizado em um outro algoritmo criptográfico qualquer.

O **esquema Diffie, Hellman e Merkle** para estabelecimento das chaves de comunicação para criptografia resolveu um problema de séculos. Através da comunicação de informações que podem ser interceptadas livremente, é possível definir chaves criptográficas e assim enviar mensagens codificadas.

Apesar de diversos inconvenientes, como o problema do estabelecimento de chaves entre os membros da mensagem criptografada, o que tem de ser feito com ambos os membros da comunicação *on-line* (ATREYA, 2002, p.35), a invenção deste esquema foi um grande passo para o avanço da criptografia, pois resolveu o problema de enviar uma chave criptografada.

O próximo passo seria dado com o desenvolvimento de um **algoritmo assimétrico**[5] para criptografia em oposição aos sistemas simétricos. Estes últimos (todos os algoritmos utilizados até então eram **simétricos**), significam basicamente utilizar a mesma chave tanto na parte do algoritmo correspondente ao emaranhamento da mensagem como na parte que cabe ao processo reverso.

Em agosto de 1977 Ronald Rivest, Adi Shamir e Leonard Adleman, anunciaram o **algoritmo RSA** (as iniciais de seus nomes). Para uma descrição detalhada deste algoritmo, veja (SINGH, 1999, p. 252). O método envolve também o uso de funções não reversíveis

[4] Um exemplo de função não reversível são as funções modulares, para um estudo aprofundado das mesmas e sua relação com criptografia veja o trabalho de Salahoddin Shokranian (SHOKRANIAN, 2005).

e grandes números primos, como no esquema anterior. Em resumo, os indivíduos que precisam trocar informações criptografadas escolhem dois **números primos** (extremamente grandes, algo como n = 3.490.529.510.847.650.949.147.849.619.903.898.133.417.764.638.493.387.843.990.820.577), operações matemáticas serão feitas com estes números (secretamente em cada lado da comunicação), estas operações resultarão em dois números, um deles pode ser livremente conhecido por todos, a chave pública, e outro mantido em segredo, será a chave privada. Ambos compõem o par de chaves criptográficas.

Quando alguém precisar enviar uma mensagem criptografada para algum indivíduo, utilizará o algoritmo RSA (atualmente existem outros algoritmos disponíveis, com o mesmo princípio e alteração nas fórmulas matemáticas) e a **chave pública** do destinatário. Esta mensagem quando criptografada não necessitará da chave pública para reverter o processo (como em algoritmos simétricos), mas sim sua **chave privada**, a qual pode ser utilizada pelo destinatário da mensagem (e somente através desta chave) para desfazer o processo criptográfico, *"As chaves são diferentes, e não é possível calcular uma chave a partir da outra. Ou seja, se você tem a chave de codificação, não pode descobrir qual é a chave de decodificação"* (SCHNEIER, 2001, p. 103)

O uso de criptografia assimétrica (uma chave para criptografar e outra, relacionada à primeira, para reverter o processo) tem sido apontada como uma grande revolução para a área da criptografia e tecnologia das comunicações de uma maneira geral. No entanto, possui restrições, algumas delas são:

Primeiro, assim como os demais sistemas criptográficos computacionais, está sujeito aos ataques de força bruta, ou seja, a possibilidade de encontrar as chaves privadas (números binários) por tentativa e erro, problema que tem sido contornado utilizando-se números primos cada vez maiores, o que conseqüentemente exige mais potência computacional, assim como nos métodos criptográficos anteriores. Isto criou uma disputa entre potência computacional versus tamanho em bits dos algoritmos.

Segundo, criptografar uma mensagem inteira somente usando o algoritmo RSA cria um problema prático, isto toma muito tempo computacional, e até pode inviabilizar o processo, dependendo do tamanho da mensagem. Este problema tem sido resolvido através do uso de um algoritmo simétrico para criptografar a mensagem em si (já quem são bem mais rápidos) e criptografar com o algoritmo RSA somente a chave necessária ao

[5] Os algoritmos simétricos ainda são utilizados, em combinação aos simétricos, o motivo está basicamente relacionado a melhor performance computacional do tipo simétrico.

processo de decifrar o algoritmo da mensagem. Na prática, portanto, o algoritmo RSA coexiste com algoritmos simétricos de cifragem (ATREYA, 2002, p. 47).

Terceiro, como conseqüência direta da própria proposta, o algoritmo RSA exige mecanismos para encontrar, recuperar e confiar nas chaves públicas dos usuários, as quais possibilitarão criptografar mensagens que somente poderão ser decifradas pelos usuários possuidores das correspondentes chaves privadas do processo. Na prática, isto tem sido resolvido com a implementação de Infra-estruturas de Chaves Públicas (ICP), um mesmo país podendo possuir uma única ou várias ICP's. O Brasil já possui uma oficial, a ICP-Brasil[6], convivendo com opções da iniciativa privada.

> A infra-estrutura de chaves públicas permite que as empresas utilizem redes abertas, tais como a Internet, para fazer uma réplica ou até mesmo aperfeiçoar os mecanismos usados para assegurar a segurança no mundo real (SILVA, 2004, p. 27).

Trata-se de um repositório das chaves públicas de usuários (além de pessoas físicas é possível existir chaves públicas para servidores de rede ou organizações) que tomaram a iniciativa de se registrar junto ao órgão responsável pela administração de tal estrutura. Esta é definitivamente dependente da comunicação em rede mundial e, teoricamente, deve permanecer *on-line* ininterruptamente. Entre os objetivos de uma ICP estão, "Segurança na comunicação, carimbo de tempo seguro, não repúdio, gerência de privilégios, recuperação de chaves" (SILVA, 2004, p. 37).

Dentro de uma estrutura de chaves públicas, o conceito de certificado é fundamental, é neste "documento" eletrônico (um arquivo com informações) que estão disponíveis a chave pública do usuário, da entidade responsável pela estrutura de chaves e outras informações como nome do portador do certificado e algoritmos utilizados, sobre o tema ver (SCHNEIER, 2001, p. 226).

2 – Assinaturas e Assinaturas Digitais

No item anterior deste artigo, procuramos abordar e apresentar, de forma bem sintética (indicando possíveis opções para aprofundamento teórico), algumas tecnologias, como a criptografia (simétrica e assimétrica), algoritmos, números binários, chaves criptográficas, Infra-estrutura de Chaves Públicas[7] (ICP) e certificados. Estas tecnologias nos permitirão entender neste ponto, o conceito de Assinaturas Digitais.

---

[6] Ver http://www.iti.gov.br.

[7] O termo corrente em inglês, para efeitos de recuperação de documentos disponíveis nesta língua, é PKI (Public Key Infraestructure).

Como vimos anteriormente, dentro do processo de criptografia assimétrica, através da utilização da *chave pública* de um destinatário, é possível enviar uma mensagem que somente poderá ser decifrada pelo possuidor da correspondente *chave privada.* Trabalha-se, portanto com um par de chaves (pública e privada para cada destinatário registrado na ICP utilizada). Ocorre que este processo pode ser feito ao contrário.

Considere que um usuário utilize sua chave privada para criptografar uma mensagem, e desta maneira, possibilitando que qualquer pessoa, acessando a chave pública deste usuário possa decifrar a mensagem. Neste caso, e sem considerar outras tecnologias[8], o usuário perde a confidencialidade desta mensagem, pois qualquer um poderá decifrar este algoritmo, a chave pública está disponível a todos na ICP. Ocorre, porém, que somente o remetente possuidor da chave privada do par de chaves dentro da estrutura ICP, teria sido capaz de criptografar a mensagem original, o que garante a origem e identidade do emissor[9] da mensagem, sua marca individual, sua assinatura.

Neste ponto, cabe uma revisão do próprio conceito de assinatura, a partir de alguns pontos de vista diferentes.

Uma das definições de dicionário da palavra assinatura é *"nome escrito, firma" ou "marca, desenho ou modelo próprio de alguém"* (FERREIRA, 1986, p. 185), acepção muito próxima do Dicionário Brasileiro de Terminologia Arquivística, note a ênfase para a assinatura autógrafa *"Nome de uma pessoa ou a sua representação,* ***feito de próprio punho*** *sobre um documento para indicar sua autoria ou avalizar seu conteúdo"* (AN, 2005, p. 38, grifo nosso).

No âmbito da análise diplomática[10] uma assinatura faz parte da estrutura de um documento como uma "anotação intelectual" (RONDINELLI, 2002). A assinatura é um dos elementos que podem ser utilizados para a autenticação[11] de um documento.

As assinaturas em si são objetos de discussões jurídicas também, o que é natural, visto que sua presença está diretamente ligada à comprovação de direitos e deveres através dos documentos assinados. E hoje, em função da existência de contratos firmados através da internet, muitas vezes em países diferentes, o conceito jurídico de assinatura tende a se tornar amplo para abarcar todas as possibilidades de manifestação desta, neste sentido, reproduzimos um trecho de Miguel Pupo Correia:

---

[8] Existem alternativas tecnológicas que possibilitam o sigilo também.
[9] Através do certificado correspondente, que relaciona os dados do emissor e sua chave pública.
[10] "Disciplina que tem como objeto o estudo da estrutura forma e da autenticidade dos documentos" (AN, 2005, p. 70).
[11] "Atestação de que um documento é verdadeiro ou de que uma cópia reproduz fielmente o original, de acordo com as normas legais de validação" (AN, 2005, p.39)

> [...] o termo assinatura significa, numa acepção ampla, qualquer ato pelo qual o autor de um documento se identifica e manifesta a sua concordância com o conteúdo declarativo dele constante, isto é, o ato de autenticação pelo próprio autor do documento por ele gerado ou gerado por terceiro e cujo conteúdo este aprova ou aceita. Portanto, a assinatura constitui um sinal ou meio, suscetível de ser usado com exclusividade e aposto a um documento, através do qual o autor deste:
>
> - revela a sua identidade pessoal de forma inequívoca;
> - manifesta a sua vontade de gerar o documento e emitir as declarações de vontade ou conhecimento dele constantes ou ainda, aderir ao seu conteúdo;
> - na medida do possível, procura preservar a integridade do documento, isto é, sua inalterabilidade, máxime quando é objeto de comunicação com outra pessoa.
>
> (CORREIA, apud BLUM, 2001, p.47)

Na atualidade, podemos falar em diversos tipos de assinatura, ou seja, diversas maneiras de comprovar a autoria em um documento. Além das assinaturas autógrafas, pode-se falar em "assinaturas eletrônicas", Fabiano Menke, cita dispositivos biométricos (para leitura de digitais da mão ou íris dos olhos), análise por computador de assinaturas de próprio punho e até identificação por senhas individuais (MENKE, 2005, p. 41). Dentro deste grupo "eletrônico" encontram-se as assinaturas digitais baseadas no uso de chaves criptográficas assimétricas. Na verdade, sempre que se fala em qualquer tipo de processamento por computador, sempre estaremos falando em assinaturas digitais, uma digital humana ou qualquer outra informação, será interpretada pelo computador como um número binário digital, em última instância. No entanto, as assinaturas com a estrutura criptográfica assimétrica, conforme descrito nos parágrafos anteriores, oferecem uma segurança ímpar na atualidade.

A segurança oferecida pelo uso de chaves assimétricas tem se mostrado tão eficaz que, tanto culturalmente como juridicamente, esta técnica deve se equiparar às assinaturas tradicionais:

> Se, até recentemente, a escrita manual era o único meio conhecido de gerar um sinal distintivo único e exclusivo, é evidente que para o Direito não se deixava margem para questionar o que se entendia por 'assinatura'. Na medida em que a evolução da técnica permite uma 'assinatura eletrônica' que possua essas mesmas características, possível se mostra dar-lhe o mesmo significado e eficácia jurídica da assinatura manual (MARCACINI, 2002, p.84)

Foge ao nosso escopo um aprofundamento nos aspectos jurídicos das assinaturas jurídicas, mas cabe notar que, a quantidade atual de leis recentes e projetos de lei em diversas esferas jurídicas, no Brasil e no mundo, demonstram o ambiente ainda um tanto incerto e de debates em torno das assinaturas digitais. De qualquer forma, a capacidade e

necessidade da legislação de um país acompanhar os avanços tecnológicos pode ser bem resumida no parágrafo seguinte:

> Por amor à argumentação, aceitemos a hipótese de que amanhã uma "nova tecnologia" possa ser inventada, para produzir uma assinatura digital sem de modo algum cifrar o arquivo eletrônico. Neste caso, passemos ao argumento jurídico. Não se entende que mal haveria em legislar mais uma vez, para acrescentar no sistema jurídico esta nova possibilidade tecnológica. Esta, aliás, seria a opção mais salutar. (COSTA; MARCACINI, 2004, p. 163)

3 – Os documentos eletrônicos autênticos

O termo Documento Eletrônico refere-se simplesmente a um documento com suporte eletrônico? Certamente que não, trata-se de algo muito mais complexo, que traz uma nova gama de desafios, no caso da arquivologia, desafios estes relacionados principalmente à Gestão Documental (que deve incluir Preservação Documental de documentos eletrônicos). Além de problemas que podem se estender até a própria questão da preservação da memória.

Antes de mais nada, na verdade, nem mesmo existe um suporte eletrônico ou digital (documento digital é outro termo bastante recorrente). Na prática, existem equipamentos, estes eletrônicos, que são imprescindíveis para compreensão do conteúdo (codificado digitalmente) gravado em suportes como a fita magnética (plásticos e substâncias ferro-magnéticas), disquetes (plásticos e substâncias ferro-magnéticas), discos rígidos (metais magnetizáveis), discos ópticos (plásticos, diferentes metais e outras substâncias químicas), *compact discs* (CD´s - plásticos, diferentes metais e outras substâncias químicas) e outros, além das tecnologias que surgirão nos próximos anos.

A Legibilidade por Máquinas (e estas, em geral, necessitando de programas de computador, *softwares*) é uma das características determinantes dos documentos eletrônicos/digitais. Outras características são a "Independência entre suporte e conteúdo", "Codificação Digital" e a "Diversidade de Conteúdos" (BODÊ, 2006).

A característica "Diversidade de Conteúdos", refere-se à riqueza encontrada nos documentos eletrônicos com relação ao que normalmente é classificado como diferentes gêneros documentais, como o gênero textual e iconográfico. Os documentos em suportes tradicionais, encontram-se em pares de suporte e conteúdo, assim, documentos sonoros encontram-se em suportes como o disco vinil e a fita magnética tipo cassete; documentos textuais em suportes como o pergaminho, papiro e papel; documentos fotográficos em papel fotográfico e películas em geral. Os documentos eletrônicos, tornam-se, a partir das últimas décadas, uma confluência para todos estes gêneros. É possível encontrar

documentos eletrônicos (*formatos eletrônicos de arquivo*[12], em termos de estruturação lógica e codificação digital), gravados em um suporte qualquer, com conteúdos textuais, imagens fixas e em movimento, sonoros e outros. Esta diversidade de gêneros, é um dos fatores que, cada vez mais, coloca os documentos eletrônicos no centro das atenções para a gestão documental.

Além disto, os documentos eletrônicos trazem também diversas outras vantagens, como a rápida recuperação num acervo (desde que corretamente descritos e indexados), necessidade de pouco espaço físico para armazenamento, possibilidade de acesso (pelo menos de leitura) por vários usuários ao mesmo tempo e inclusive em localidades geograficamente distintas, além de outras.

No entanto, infelizmente, existem problemas presentes além de vantagens. Um dos mais prementes e que vem tomando espaço de pesquisa é a preservação dos documentos eletrônicos, a este respeito:

> Um formato é freqüentemente controlado como propriedade intelectual de uma entidade comercial, a qual, tipicamente tem grande interesse em esconder o código base. A competição direciona freqüentes mudanças no formato individual, tanto quanto nas empresas que os controlam; as tecnologias da informação também impõem contínuas transformações. Esta combinação de opacidade e mudança significa que não há segurança de que a tecnologia futura irá suportar os formatos de hoje. De fato, o cenário digital de amanhã será repleto de objetos grandemente difíceis de preservar, acessar e interpretar. (LeFURGY, 2003, tradução nossa)

A preservação de documentos eletrônicos é um tema vasto para pesquisas e que também está ligado às assinaturas digitais baseadas em criptografia assimétrica. O ponto chave é a própria durabilidade da chave pública e privada (tempo necessário para encontra a privada computacionalmente) e todo o software necessário para o processo de reversão da criptografia. Para longos períodos de preservação, os procedimentos necessários envolverão a migração dos formatos de arquivo utilizados, o que leva à eliminação da codificação criptográfica. Trata-se de um problema ainda sem respostas definitivas. Alguns Arquivos Nacionais que já recebem documentos eletrônicos, como o do Reino Unido (ver www.na.gov.uk) não recebem documentos criptografados.

[12] "No nível mais básico, objetos digitais são seqüências de zeros e uns que representam dados codificados. Diferentes **Formatos de Arquivo** especificam como estes códigos representam o conteúdo intelectual criado por um autor do objeto digital. Um exemplo disto é o formato Microsoft Word. Este formato é uma especificação para armazenamento de dados textuais, bem como informações de formatação. Muitos Formatos de Arquivo são incrivelmente complexos, de maneira que os códigos podem ficam ininteligíveis para um observador humano. Para que este objeto digital tenha sentido, um

Além da questão da preservação por longos períodos, os documentos eletrônicos apresentam um problema igualmente importante, a facilidade de alteração de seu conteúdo, sua integridade, *"Integridade no que se refere a dados, tipicamente se refere a assegurar que a informação somente pode ser modificada por pessoas autorizadas"* (ATREYA, 2002, p.85, tradução nossa). Qualquer documento em suporte tradicional e consagrado como o papel ou papiro pode ter seu conteúdo alterado, no entanto, via de regra, é possível detectar as modificações ou possíveis falsificações. O mesmo não acontece com documentos eletrônicos, as modificações num arquivo eletrônico, as quais, saliente-se, podem ser realizadas com relativa facilidade, não podem ser detectadas.

O processo de criptografar uma mensagem, utilizando-se um método de criptografia assimétrica, que gera uma mensagem que só pode ser decifrada pelo possuidor da chave do destinatário, por si somente, já é um método que garante certa integridade de dados, pois somente os dados originais funcionarão com a chave do destinatário. No entanto, criptografar mensagens longas (às vezes com gigabytes em anexos) é um processo extremamente demorado utilizando-se o método assimétrico de criptografia. A solução tecnológica está relacionada ao uso de algoritmos *Hash*, estes algoritmos resumem uma mensagem, de qualquer tamanho, a um número fixo. Apenas a mensagem com o texto original (isto inclui caracteres, espaços e qualquer outro sinal) gera tal número fixo,

> Funções *hash* são, às vezes, chamadas de funções unidirecionais, por sua característica única, que faz o processo inverso extremamente difícil ou impossível de se alcançar. Algumas pessoas referem-se ao resumo de mensagem (hash) como sendo uma impressão digital dos dados de entrada [...]. Dado o mesmo valor de entrada duas vezes, a função hash deve ser capaz de gerar o mesmo resumo em ambas as vezes. Uma mudança de 1 bit nos dados de entrada resultará num valor bastante diferente de resumo." (ATREYA, 2002, p. 88, tradução nossa)

Na prática, a segurança da integridade dos dados originais é obtida comparando-se um novo resumo hash do texto original assinado pelo remetente com o resumo hash do que foi recebido. Estes dois resumos têm de ser iguais e isto garantirá que o texto original não foi alterado em algum momento.

Existem também outras soluções tecnológicas relacionadas a documentos eletrônicos para seu uso mais eficaz, como a necessidade de sigilo nas comunicações de mensagens eletrônicas, sendo o caso mais comum, o de *e-mail*. Se é certo que as mensagens enviadas em suportes físicos como o papel (cartas, encomendas e etc.)

---

software será necessário para interpretar e exibir [ou renderizar] os dados para o usuário." (UNIVERSITY

também podem ser interceptadas e ter sua confidencialidade comprometida, em relação às mensagens eletrônicas, os documentos em suportes tradicionais exigem um procedimento muito mais complicado para uma efetiva alteração de conteúdo. As mensagens eletrônicas podem ser interceptadas com grande facilidade, durante seu trajeto por redes de computadores, e pior ainda, é praticamente impossível detectar esta intromissão. Neste sentido a indústria desenvolveu diversas saídas tecnológicas que envolvem criptografia e uso de certificados digitais, como o protocolo *"S/MIME (Securo/Multipurpose Internet Mail Extension), PEM (Privacy Enhanced Mail) e o PGP (Pretty Good Privacy)"* (ATREYA, 2002, p 192).

Atente-se para o ponto fundamental de que o uso de assinaturas digitais em documentos eletrônicos não cumpre apenas uma formalidade de autenticidade, como as assinaturas tradicionais. As primeiras, além de estarem tecnologicamente aptas a se equipararem às últimas, vão muito além e se estendem em funcionalidade à própria integridade de um documento eletrônico (e apenas aqueles) assinados com criptografia assimétrica:

> Quando se fala em fazer prova por meio de documento eletrônico, mostra-se necessário, porém, separar o joio do trigo: nem todos os registros eletrônicos podem servir como prova, mas apenas aqueles que estejam assinados mediante o emprego de uma técnica conhecida por criptografia assimétrica ou criptografia de chave pública. O grande problema do uso de registros eletrônicos como prova é o fato de serem alteráveis sem deixar vestígios físicos, não conferindo, assim, a mesma segurança do papel. Entretanto, com o uso da criptografia assimétrica, é possível "assinar" documentos eletrônicos, de modo a identificar o "signatário" e a tornar inalterável o conteúdo do documento "assinado". (COSTA; MARCACINI, 2004, p. 155)

O uso de assinaturas digitais baseadas em criptografia assimétrica oferece a possibilidade tecnológica de nivelar os documentos eletrônicos ao mesmo *status* de documentos em suportes tradicionais, como o papel, no que tange a sua autenticidade, integridade e sigilo, quando se tratar de documentos que exigem tais características[13]. O número de documentos eletrônicos, portanto, que podem alçados ao patamar de documento com valor arquivístico tende a crescer ao longo do tempo. Isto deve ocorrer, na medida em que, além dos fatores técnicos e tecnológicos, estes documentos receberem uma aceitação social e legal.

OF LEEDS, 2003, tradução e grifo nossos)

4 – Conclusão

Os avanços tecnológicos ocorridos nas últimas décadas do século XX, na área da criptografia e informática, possibilitaram o surgimento de métodos bastante seguros para comunicação entre indivíduos, organizações ou entre organizações e indivíduos.

Como produto deste contexto, surge o conceito de assinatura eletrônica, que extrapolou o campo das comunicações e comércio e hoje é aplicável em diferentes áreas[14] onde se utilizam documentos e onde o documento eletrônico vem ganhando espaço e importância.

No seio das organizações nacionais ou transnacionais, públicas e privadas, o documento eletrônico, independentemente do uso de qualquer tipo de assinatura eletrônica ou digital, vem trilhando um caminho de conquista de espaço em função das vantagens que incorpora. O uso de assinaturas digitais, baseadas em chaves públicas e ICP`s confiáveis com respaldo legal pode agregar ainda mais valor e aplicabilidade aos documentos eletrônicos.

A segurança com o uso de assinaturas digitais é um fator que tem provocado cautela para seu uso. Certamente, não podemos ser ingênuos para acreditar numa solução a prova de falhas. Para o uso destas assinaturas, uma grande estrutura de equipamentos, comunicação e legislação são necessárias, a qual envolve pessoas também. As possibilidades de falhas na segurança sempre estarão presentes, portanto. Na verdade, o uso de assinaturas convencionais em papel também não é um método a prova de falsificações e falhas, os anais da justiça e as crônicas policiais que o digam.

Por outro lado, o valor legal de documentos eletrônicos está intimamente ligado a sua autenticidade, a qual está fortemente ligada às assinaturas digitais baseadas em criptografia assimétrica de chave pública. Se o ponto de vista da arquivologia e diplomática a autenticidade de documentos não depende apenas do elemento assinatura, mas de todo um conjunto de elementos que inclui o próprio contexto de produção, tramitação e arquivamento. Do ponto de vista cultural e jurídico, as assinaturas (digitais ou não) ocupam um papel chave.

---

[13] Nem todos os documentos eletrônicos ou mesmo convencionais, necessitam de sigilo, como os documentos de valor histórico e cultural ostensivos, que até mesmo devem ser divulgados para o maior número possível de possíveis interessados.

[14] Na área de documentos eletrônicos jurídicos, por exemplo, ver (GUIMARÃES; NASCIMENTO; NETO, 2005)

As assinaturas digitais e seu uso em documentos eletrônicos, juntamente com todos os pré-requisitos de segurança, potencializam sua equiparação às assinaturas convencionais.

As consequências para a Arquivologia são importantes, tanto no que cabe à Gestão Documental dos documentos não permanentes, como a administração dos acervos Permanentes. Além da preservação de documentos eletrônicos, a presença nas organizações de documentos eletrônicos autênticos e com valor legal, aumenta ainda mais a carga de responsabilidade para sua correta administração.

Conseqüentemente, as atividades relacionadas à classificação, descrição e preservação de documentos eletrônicos, levando-se em consideração as características próprias destes, como os *metadados*, devem ser levadas em consideração no fazer e pensar arquivístico.

Os arquivistas modernos podem e devem acompanhar estes avanços tecnológicos, encontrar e propor as soluções cabíveis a altura do desafio que a sociedade do conhecimento moderno impõe.

REFERÊNCIAS

ARQUIVO NACIONAL (Brasil). **Dicionário brasileiro de terminologia arquivística**. Rio de Janeiro: Arquivo Nacional, 2005.

ATREYA, Mohan, at al. **Digital signatures**. California: McGraw-Hill, RSA Press, 2002.

BENANTAR, Messaoud. **Introduction to the public key infrastructure for the internet**. NJ: Prentice Hall, 2002.

BLUM, Renato M. S. Opice (coord). **Direito eletrônico**: a Internet e os tribunais. Bauru: Edipro, 2001.

BODÊ, Ernesto C. **Formatos de arquivo e a preservação de documentos digitais**. Comunicação livre apresentada no XIV Congresso Brasileiro de Arquivologia, Rio de Janeiro, 2006.

COSTA, Marcos da; MARCACINI, Tavares R. **Direito em bits**. São Paulo: Fiuza Editores, 2004.

FERREIRA, Aurélio B. de Holanda. **Novo dicionário da língua portuguesa**. 2. ed. Rio de Janeiro: Nova Fronteira, 1986.

LeFURGY, William G. PDF/A: Developing a file format for long-term preservation. **RLG News**, NY, v. 7, n. 6, 2003. Disponível em: http://www.rlg.org. Acesso em: 10 novembro 2005.

MARCACINI, A. T. Rosa. **Direito e informática**: uma abordagem jurídica sobre a criptografia. Rio de Janeiro: Forense, 2002.

MENKE, Fabiano. **Assinatura eletrônica**: aspectos jurídicos no direito brasileiro. São Paulo: Editora Revistas dos Tribunais, 2005.

RONDINELLI, Rosely Curi. **Gerenciamento arquivístico de documentos eletrônicos**: uma abordagem teórica da diplomática arquivística contemporânea. Rio de Janeiro: FGV, 2002.

SCHNEIER, Bruce. **Segurança.com**: segredos e mentiras sobre a proteção na vida digital. Rio de Janeiro: Campus, 2001.

SHOKRANIAN, Salahodin. **Criptografia para iniciantes**. Brasília: Editora Universidade de Brasília, 2005.

SILVA, Lino Sarlo da. **Public key infrastructure – pki**: conheça a infra-estrutura de chaves públicas e a certificação digital. São Paulo: Novatec, 2004.

SINGH, Simon. **The code book**: the evolution of secrecy from Mary Queen of Scots to quantum cryptography. New York: Anchor Books, 1999.

TRAIN, Sheila. **Certificação digital**: conceitos básicos e aplicações. São Paulo: Imprensa Oficial, 2005.

UNIVERSITY OF LEEDS. Survey and assessement of sources of information on file formats and software documentation. Final Report.