ASSINATURA DIGITAL

1. INTRODUÇÃO

Uma assinatura eletrônica permite que um documento seja assinado por meio eletrônico, e isso pode ser feito mediante senha, biometria, reconhecimento da retina e muitas outras formas, incluindo a assinatura digital. A assinatura digital é um tipo de assinatura eletrônica e seu entendimento envolve o estudo de um conjunto de recursos, termos e conceitos, como: chaves públicas e privadas, criptografia, modelos matemáticos, autoridade registradora (conhecida também como autoridade de registro) e autoridade certificadora.

Após estudo aprofundado desses recursos, termos e conceitos, pode-se compreender as etapas do processo de assinatura eletrônica de documentos e transações por meio da assinatura digital. Além disso, também é importante o entendimento do funcionamento da validação da autenticidade das assinaturas digitais realizadas por organizações, pessoas ou equipamentos.

O primeiro passo para conseguir utilizar uma assinatura digital é o requerimento do certificado digital, emitido por uma autoridade certificadora, o qual pode ser utilizado para assinar eletronicamente (digitalmente) diversos tipos de documentos. O processo para emissão de um certificado digital passa pelas seguintes etapas:

1) O requerente envia seus dados para uma autoridade registradora.
2) A autoridade registradora confere todos os dados do solicitante.
3) Com os dados validados, a autoridade registradora solicita a emissão do certificado digital para uma autoridade certificadora.

4) Após esse processo, é gerado um certificado digital que permite que documentos e transações sejam autenticados e validados eletronicamente, tendo valor equivalente ao da assinatura de próprio punho.

2. CRIPTOGRAFIA, CHAVES SIMÉTRICAS E CHAVES ASSIMÉTRICAS

A criptografia de dados pode ser feita utilizando mecanismos de chave simétrica ou assimétrica:

- **Criptografia de chave simétrica**: utiliza uma única chave compartilhada para codificação e decodificação. Dessa forma, é necessário que o emissor e o receptor de uma mensagem tenham essa chave compartilhada. Um exemplo de algoritmo utilizado no processo de chave simétrica é o DES (CERT.BR, 2021; CASTELLÓ; VAZ, 2021 [a]).
- **Criptografia de chaves assimétricas**: utiliza duas chaves diferentes, uma privada e uma pública, para realizar a codificação e decodificação. Um exemplo de algoritmo utilizado no processo de chave assimétrica é o RSA (CERT.BR, 2021; CASTELLÓ; VAZ, 2021 [a]). Na assinatura digital, é utilizada criptografia de chaves assimétricas, ficando as chaves privada e pública em *tokens* ou *smartcard* (CERT.BR, 2021; CASTELLÓ; VAZ, 2021 [a]).

3. ASSINATURA DIGITAL

A assinatura digital é feita utilizando um *hash*, como, por exemplo, o MD5 ou o SHA-256. O *hash* utilizado faz um resumo da mensagem sempre com um tamanho fixo. Na assinatura digital, o *hash* é criptografado com a chave privada. Com a finalidade de verificar a validade da assinatura, o receptor descriptografa a mensagem com a chave pública e compara o *hash* recebido com o *hash* original da assinatura. Caso sejam iguais,

a assinatura é válida (CERT.BR, 2021; CASTELLÓ; VAZ, 2021 [b]). Veja nos esquemas a seguir o processo de assinatura digital e validação da assinatura digital.

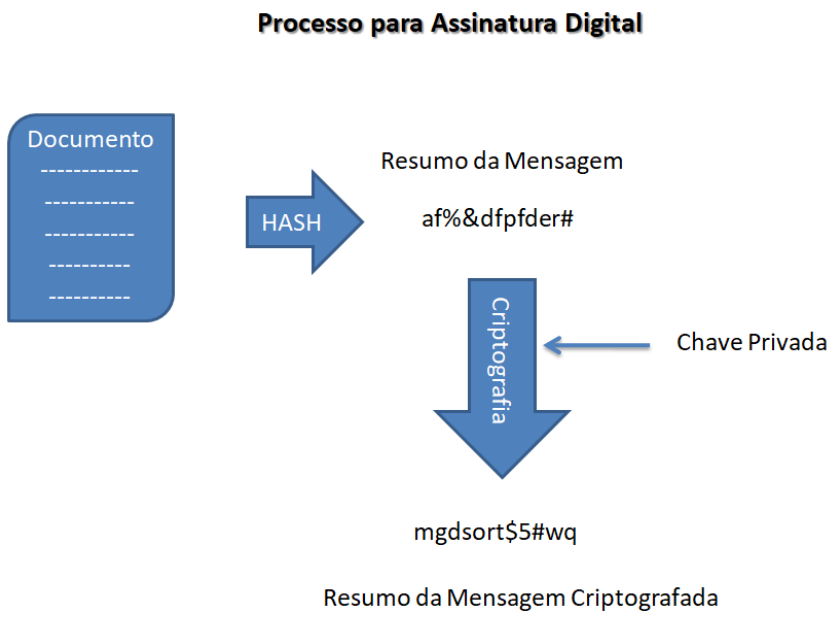

Figura 1 – Processo para assinatura digital. Fonte: Elaborada pelo autor (2021).

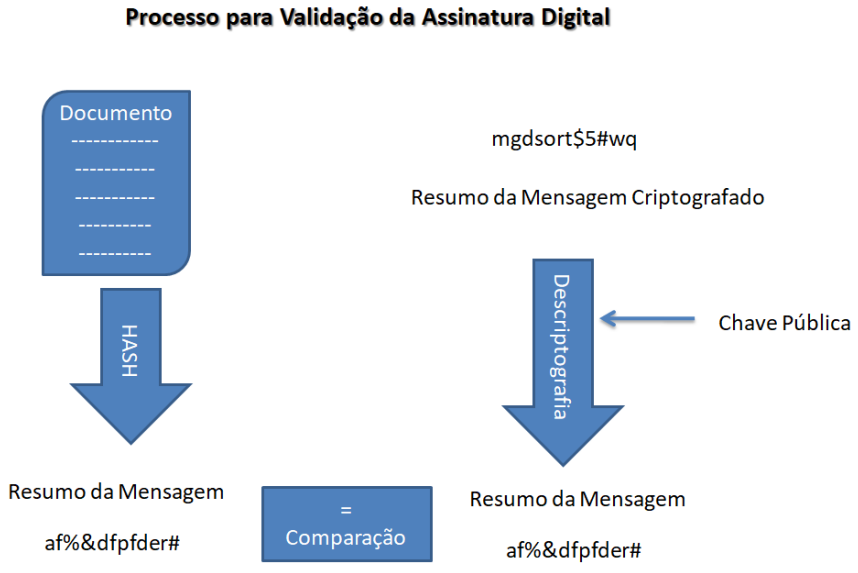

Figura 2 – Processo para validação da assinatura digital. Fonte: Elaborada pelo autor (2021).

4. CERTIFICADO DIGITAL

Um certificado digital emitido por autoridade certificadora contém a chave pública e os dados de uma organização, pessoa ou equipamento, por exemplo. Dessa forma, o certificado funciona como a identificação destes e fornece os dados e a chave pública para validação da assinatura digital (CERT.BR, 2021; CASTELLÓ; VAZ, 2021 [b]).

Além do certificado digital emitido por uma autoridade certificadora, também é possível a criação de um certificado autoassinado gerado por uma organização. O problema desse certificado é que, como ele não é registrado em uma autoridade certificadora, geralmente, em alguns navegadores, aparece a exibição de uma mensagem de erro relacionada com problemas na autenticidade, o que faz com que muitos usuários desistam de utilizar uma aplicação, por exemplo.

REFERÊNCIAS BIBLIOGRÁFICAS

CASTELLÓ, Thiago; VAZ, Verônica [a]. Assinatura digital: possibilidades de fraude. **UFRJ**, [*s. d.*]. Disponível em: https://www.gta.ufrj.br/grad/07_1/ass-dig/PossibilidadesdeFraude.html. Acesso em: 19 mar. 2021.

CASTELLÓ, Thiago; VAZ, Verônica [b]. Assinatura digital: funcionamento da assinatura digital. **UFRJ**, [*s. d.*]. Disponível em: https://www.gta.ufrj.br/grad/07_1/ass-dig/ComocriarumaAssinaturaDigital.html. Acesso em: 19 mar. 2021.

CERT.BR. Cartilha de segurança para internet: criptografia. **CERT.br**, 2017. Disponível em: https://cartilha.cert.br/criptografia/. Acesso em: 19 mar. 2021.