ASSINATURA DIGITAL II

Com a evolução tecnológica e a adoção do digital para praticamente todas as áreas na sociedade, tanto pessoais quanto profissionais, as pessoas utilizam cada dia mais a internet para a realização de diferentes operações virtuais, inclusive transações financeiras. No entanto, a internet em si não é segura o bastante e, por isso, cabe a sistemas e usuários a adição de segurança extra em suas operações, sendo a assinatura digital uma das mais importantes.

A assinatura digital pode ser definida como uma forma de conferir segurança, autenticidade e integridade a documentos eletrônicos. A partir dela é possível provar a veracidade das informações em documentos digitais (BARRETO *et al*., 2018)

Um documento assinado digitalmente tem a mesma validade que documentos assinados em cartório, podendo ser usada para a validação de diversos tipos de documentos e operações virtuais, uma vez que garante que a mensagem recebida foi realmente enviada por quem alega ter enviado. Para que essa segurança seja tão eficiente, Nakamura e Geus (2007) afirmam que uma assinatura digital deve ter as seguintes características:

- Autenticidade: o destinatário pode confirmar que a assinatura da mensagem foi emitida pelo remetente.
- Integridade: a assinatura digital garante que o conteúdo não foi alterado desde que foi assinado digitalmente.
- Irretratabilidade: a assinatura digital ajuda a comprovar a origem do conteúdo assinado para todas as partes, de modo que o remetente não possa negar a origem da mensagem.

Isso ocorre porque a assinatura digital utiliza criptografia e certificado digital vinculados em todos os documentos assinados, ou seja, tem um certificado e uma chave privada que é exclusiva do titular, e tal certificado digital é assinado por uma autoridade certificadora, garantindo a sua confiança.

A infraestrutura de chaves públicas brasileiras (ICP-Brasil) define regras e fiscaliza as autoridades certificadoras. Ela é responsável por configurar um sistema de serviços, políticas e recursos, que dão suporte para a utilização de criptografia de chave pública, permitindo que as partes envolvidas em uma transação digital sejam autenticadas. Dessa forma, a ICP-Brasil oferece ferramentas de gerenciamento de certificados digitais e chaves públicas, criando uma cadeia hierárquica de confiança, possibilitando a emissão dos certificados para que o remetente do documento assinado digitalmente seja identificado.

Barreto *et al*. (2018) apresentam o processo de emissão de certificado digital, conforme a Figura 1.

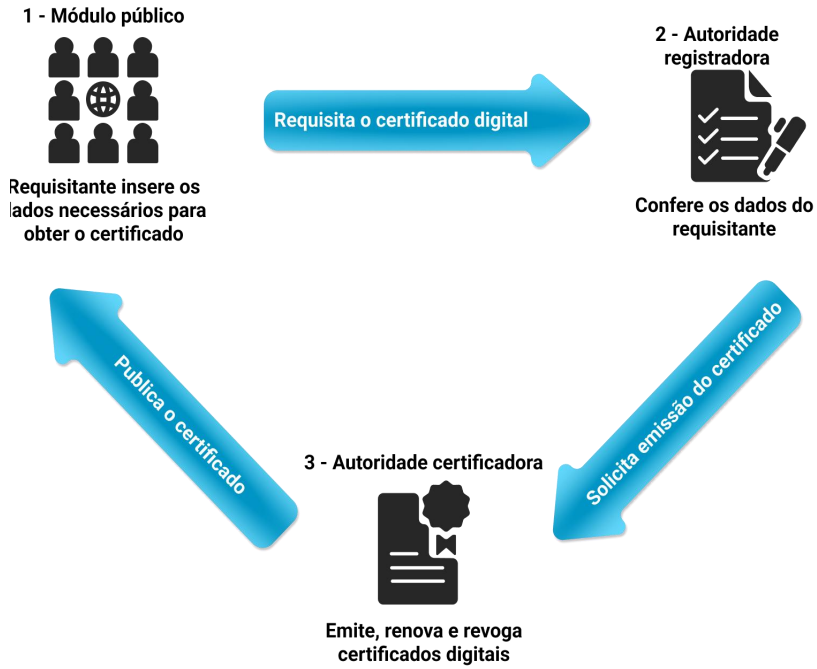

Figura 1 - Processo de emissão de certificado digital. Fonte: Barreto *et al*. (2018).

- Módulo público: portal de serviços em que o usuário solicita ou instala o certificado digital.
- Autoridade certificadora (AC): entidade responsável por emitir, gerar, renovar e revogar certificados digitais. Além disso, distribui chaves públicas e mantém as regras de publicação dos certificados.
- Autoridade de registro (AR): entidade responsável por estabelecer a interface entre a autoridade certificadora e o usuário. Ademais, verifica as informações do usuário e envia a requisição do certificado para a AC.

Em suma, a assinatura digital é a ferramenta mais avançada e confiável para garantir a segurança de transações efetuadas via internet.

REFERÊNCIAS BIBLIOGRÁFICAS

BARRETO, J. S. *et al*. **Fundamentos de segurança da informação**. Porto Alegre: Sagah, 2018.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.