ANTONIO MARCOS DA SILVA PIRES

RENATO DROZDEK JUNIOR

RODRIGO FERREIRA DOS ANJOS

SAMANTHA SOARES HEIL

Assinatura digital é um método de autenticação de informação digital que substitui a assinatura física, e elimina a necessidade de uma versão papel do documento assinado.

Com o avanço da tecnologia, houve a necessidade de criar uma assinatura digital (*PKI – Public Key Infrastructure* – “Infraestrutura de Chave Pública”), para gerar documentos digitais com validade legal, e equivale a uma assinatura de próprio punho. Essa tecnologia utiliza criptografia e vincula o certificado digital ao documento eletrônico assinado, portanto, garante a segurança e autenticidade do documento em questão. Com esse novo conceito, as empresas e departamentos eliminam processos manuais, remessas físicas de documentos, reconhecimentos de firmas e reduz custos simplificando e agilizando processos.

Criptografia consiste em uma função que transforma uma mensagem legível em outra ilegível para transmissão. Existe também a criptografia assimétrica onde as chaves usadas para criptografar e descriptografar são diferentes. Similar ao processo de assinatura, porém neste caso os papeis das chaves se invertem.

A criptografia de chave pública é usada para “assinar” informações digitais. Estas informações são usadas em Certificados Digitais para assegurar a autenticidade de pessoas, usuários e serviços. A chave pública é usada para descriptografar uma mensagem criptografada por uma chave privada, isso porque a chave privada gera um *hash* e anexa na mensagem a ser enviada, e somente o portado da chave pública correspondente consegue ler o texto recebido.

Para garantir a segurança das informações seguras passadas pelo usuário, como senhas por exemplo, usa-se o método *hash* que basicamente consiste em receber a informação, guardá-la de modo criptografado, ou seja, você insere sua senha ela é codificada e se torna irreversível e segura.