DESENVOLVIMENTO DE AUTORIDADE CERTIFICADORA DE BAIXO CUSTO

Apresentado no
10° Congresso de Inovação, Ciência e Tecnologia do IFSP ou no 4º Congresso de Pós-Graduação do IFSP
27 e 28 de novembro de 2019- Sorocaba-SP, Brasil

RESUMO: A partir da introdução do modelo da criptografia assimétrica em meados da década de 70, surge a possibilidade de utilizá-la também para assinaturas digitais utilizando os pares de chaves públicas e privadas. A chave pública nesse contexto é utilizada por todos os usuários que validam a assinatura de alguém. Já a chave privada é utilizada pelo usuário para assinar algo. Com o desenvolvimento de um protótipo do algoritmo RSA foi possível realizar o comparativo entre o RSA e o AES, evidenciando que o RSA é um algoritmo mais lento para a funcionalidade de cifragem, porém destaca-se no âmbito da assinatura digital. Neste contexto, as autoridades certificadoras possuem a responsabilidade de assinar e distribuir de forma segura os certificados digitais, que contam com o mesmo valor jurídico das assinaturas físicas. O projeto busca desenvolver uma autoridade certificadora utilizando o *software open source* EJBCA. Os certificados serão disponibilizados para toda comunidade do Instituto Federal de São Paulo - Campus Campinas, através de uma interface web que também será desenvolvida no projeto.

PALAVRAS-CHAVE: criptografia; rsa; aes; assinatura digital; certificado digital; chave pública/privada.

LOW COST CERTIFICATING AUTHORITY DEVELOPMENT

ABSTRACT: From the introduction of the asymmetric cryptography model in the mid-1970s, it is possible to use it for digital signatures using public and private key pairs. The public key in this context is used by all users who validate someone's signature. The private key is used by the user to sign something. With the development of a prototype of the RSA algorithm, it was possible to compare RSA with AES, showing that RSA is a slower algorithm for encryption functionality but stands out in the digital signature. Certifiers have a responsibility to securely sign and distribute digital certificates, which have the same legal value as physical signatures. In this sense, the project seeks to develop a certification authority using the open source EJBCA software. The certificates will be made available to the entire community of the Instituto Federal de São Paulo - Campus Campinas, through a web interface that will also be developed in the project.

KEYWORDS: encryption; rsa; aes; digital signature; digital certificate; public/private key.

INTRODUÇÃO

A criptografia assimétrica trouxe um novo paradigma através da introdução de modelos matemáticos. Estes modelos, têm como característica a utilização de duas chaves denominadas pública e privada, diferentemente dos algoritmos simétricos, onde apenas uma chave é utilizada. A chave pública é disponibilizada para todos os usuários que irão cifrar algo para o dono dessa chave. A novidade deste tipo de criptografia é a possibilidade de utilizá-la para assinaturas digitais. Essas assinaturas são criadas pela chave privada de um usuário (de forma sigilosa) e verificada por qualquer pessoa que tenha sua chave pública. As assinaturas digitais, têm substituído os papéis

fisicamente assinados oferecendo o mesmo valor jurídico em diversos cenários. Além disso, elas oferecem uma maior dificuldade para falsificações e proporcionam economia de recursos naturais. As autoridades certificadoras são responsáveis pela emissão dos certificados digitais, e possui como principal função garantir que uma determinada chave é realmente de propriedade de uma pessoa, além de realizar a gerência do certificado, principalmente em relação ao tempo de validade ou revogação do mesmo. Os certificados são documentos digitais que contém a chave pública, associada a uma chave privada, e um prazo de validade, informando sua expiração para os usuários. A autoridade certificadora garante que o certificado foi emitido por ela, pois ela assina o mesmo digitalmente com sua própria chave privada. A chave pública de uma autoridade confiável é amplamente divulgada e aceita como válida pelos usuários e sistemas computacionais. Entendendo a importância das assinaturas digitais, o projeto propõe o desenvolvimento de uma autoridade certificadora de baixo custo utilizando softwares de código aberto para a criação da autoridade certificadora e da interface web, distribuindo gratuitamente os certificados e economizando os recursos demandados com as assinaturas físicas (papel, tinta, etc.)

MATERIAL E MÉTODOS

Analisando o estado da arte dos atuais métodos de criptografia, é imensurável a relevância dos sistemas criptográficos assimétricos de chave pública, como por exemplo, o RSA. Este algoritmo foi proposto na década de 1970 por três matemáticos (Rivest, Shamir e Adleman), e até os dias atuais é um dos principais sistemas que garantem de fato a segurança dos usuários no contexto das cifras assimétricas e assinaturas digitais. Neste contexto, foi desenvolvido um protótipo simplificado do algoritmo de criptografia RSA, com as funcionalidades de geração de pares de chaves (pública/privada) e de cifrar/decifrar textos simples.

O protótipo foi desenvolvido em Linguagem de programação C e segue o modelo proposto na figura 1. Nesta figura a entrada de um texto em claro representado pela letra A é cifrado usando a chave pública do usuário B, conforme mostrado na letra E. Este texto é então encaminhado de forma segura por um canal de comunicação sujeito a ataques (texto cifrado: $E(PU_B, M)$). Ao chegar no seu destino (usuário B), o texto cifrado é então decifrado com a chave privada de B, como pode ser visto na letra D. Por fim, o usuário B tem o texto em claro e pode ver suas informações.

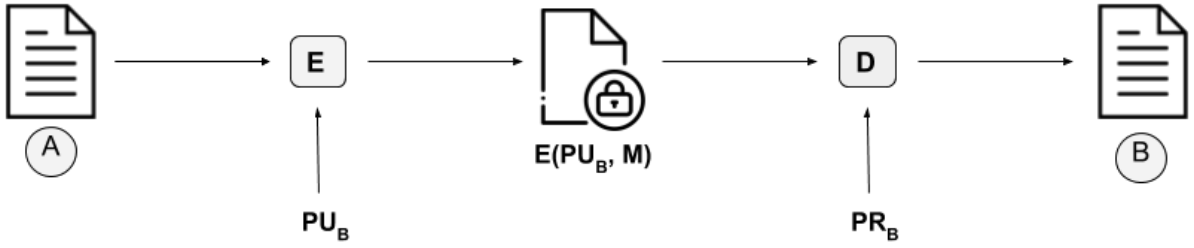

FIGURA 1. Arquitetura básica do algoritmo RSA desenvolvido.

Para evolução deste cenário de testes com o RSA, pretende-se implementar uma autoridade certificadora utilizando o software EJBCA. Este software é amplamente utilizado por diversas autoridades públicas e privadas para geração de certificados comerciais. Além disso, pretende-se criar uma interface web que seja integrada com o EJBCA através de *web services*. Esta interface será desenvolvida de forma responsiva e funcional para diversos *web browsers*. Além disso, a interface irá permitir que usuários de outras áreas possam criar facilmente os certificados e revogá-los quando necessário. A arquitetura simplificada do projeto pode ser verificada na figura 2.

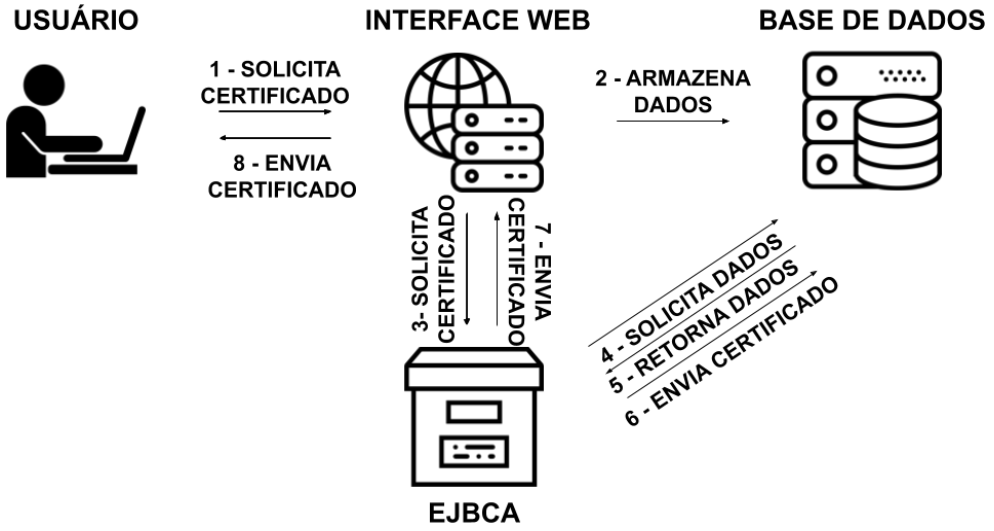

FIGURA 2. Arquitetura básica do projeto.

Nesta arquitetura o usuário interage apenas com a interface web, onde seus dados ficarão armazenados em uma base de dados segura para futuros acessos. A interface por sua vez, é responsável por se comunicar através dos *web services* com a autoridade certificadora (EJBCA). Ela enviará todos os dados necessários para que o certificado possa ser criado, e receberá um certificado válido e assinado pela autoridade.

As autoridades certificadoras são organizadas de forma hierárquica onde autoridades de primeiro nível são responsáveis por assinar outras de níveis mais baixos. No Brasil toda hierarquia de autoridades é administrada pela infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, essa hierarquia é dividida em quatro classe: autoridade certificadora Raiz, autoridade certificadora primária, autoridade certificadora secundária e autoridade de registro.

Em meio a estas sub-hierarquias é encontrada a rede de autoridade certificadoras do ICPEDU, uma autoridade certificadora que disponibiliza às instituições/vinculadas à Rede Nacional de Pesquisa - RNP a distribuição de certificados digitais gratuitos. Nesta hierarquia existe a autoridade certificadora ICPEDU sendo a raiz e outras três autoridade certificadoras, sendo elas: duas autoridade certificadoras da Universidade Federal de Santa Catarina e outra da Universidade Estadual de Campinas (UNICAMP). Através desta análise, busca-se que a autoridade certificadora proposta neste trabalho seja garantida (através de uma assinatura) pelo ICPEDU, o que traria maior confiabilidade para a autoridade proposta neste trabalho. .

RESULTADOS E DISCUSSÃO

Notou-se através da implementação do RSA que o texto mesmo que simples e pequeno é totalmente irreconhecível quando está criptografado com a chave pública do usuário. Desta forma, mostrou-se que o algoritmo RSA ainda pode ser utilizado com segurança desde que o tamanho da chave seja adequado aos padrões atuais, pois o poder computacional tem aumentado significativamente o que pode trazer impactos negativos as cifras assimétricas e principalmente ao RSA. Além disso, temos como resultado comparativo que o RSA é um algoritmo mais lento que as cifras simétricas baseadas em substituições e permutações como o AES, por exemplo. Isto mostra o porquê de o RSA e as cifras assimétricas em geral serem utilizadas apenas para troca de chaves simétricas quando utilizado como algoritmo de criptografia. Seu uso mais intenso é portanto, restringido às assinaturas digitais. Neste contexto, o que de fato o protocolo assina é um resumo criptográfico da mensagem original. Este resumo é obtido a partir da saída de uma função hash segura. Normalmente utiliza-se SHA (secure hash algorithm) com no mínimo 256 bits de saída.

Utilizar um hash seguro garante que o RSA irá assinar poucos bits independente do tamanho da mensagem de entrada. Além disso, caso a mensagem seja alterada por um atacante na rede, a mesma será detectada pelo receptor, pois o hash será completamente diferente daquele que foi assinado pelo remetente. Esta última propriedade é uma característica das funções hash, onde uma pequena mudança nos bits da entrada (mesmo que seja alterado apenas um bit) provoca uma grande mudança no resumo de saída do hash.

CONCLUSÕES

O algoritmo RSA é fundamental no contexto da criptografia assimétrica, pois foi o primeiro esquema a ser utilizado em larga escala desde sua criação. O algoritmo é utilizado no âmbito da cifragem de pequenos textos (como a cifragem de chaves de sessões) e, principalmente, nas assinaturas digitais tendo em vista o seu sistema de chaves públicas e privadas. Para garantir que uma assinatura é de fato da pessoa que assina é necessário que uma autoridade certificadora confiável forneça essa garantia. Por isso o papel de uma autoridade é fundamental para que o ecossistema de assinaturas digitais possa existir em grande escala e com segurança aceitável.

AGRADECIMENTOS

Ao Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - IFSP / Amarais - Campus Campinas

REFERÊNCIAS

BRASIL. ICP-Brasil. Disponível em: <https://www.iti.gov.br/icp-brasil>. Acesso em: 15 jun. 2019.

PrimeKey Solutions AB. EJBCA: The Open Source CA. Disponível em: <https://www.ejbca.org>. Acesso em: 18 jun. 2019.

Stallings, William Criptografia e segurança de redes: princípios e práticas / William Stallings; tradução Daniel Vieira; revisão técnica Paulo Sérgio Licciardi Messeder Barreto, Rafael Misoczki. – 6. ed. – São Paulo: Pearson Education do Brasil, 2015

Rede Nacional de Pesquisa - RNP. ICPEdu.. Disponível em: <https://www.rnp.br/servicos/servicos-avancados/icpedu>. Acesso em: 20 jun. 2019.