PROPOSTA DE PACOTE PARA USO DE CERTIFICADOS DIGITAIS EM APLICAÇÕES LARAVEL

AMARAL, Augusto Araújo[1]; PEREIRA JUNIOR, Manoel[2]

[1]Estudante do curso de Ciência da Computação do Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais (IFMG) – *Campus* Formiga. E-mail: augusto.amaral.araujo@gmail.com
[2]Professor orientador do IFMG - *Campus* Formiga. E-mail: manoel.pereira@ifmg.edu.br

Resumo: A tecnologia está progredindo para nos permitir cada vez mais realizar tarefas de forma prática. Junto com esse progresso surge a necessidade da segurança da informação. Uma solução para esta necessidade é o Certificado Digital, que pode ser utilizado para assegurar a autenticidade, integridade, não repúdio e validade jurídica das informações trafegadas na rede. Este resumo expandido apresenta o desenvolvimento do protótipo de um pacote Laravel para o uso de certificados digitais em aplicações *web Laravel* utilizando a biblioteca PHP OpenSSL. No estágio atual do desenvolvimento do pacote é possível utilizar o certificado A1 para autenticar um usuário e gerar assinaturas para documentos digitais.

Palavras-chave: Certificação digital. Assinatura digital. Certificado digital.

1 INTRODUÇÃO

Com o avanço tecnológico das últimas décadas, vários dos conceitos e processos que antes eram consolidados estão sendo revolucionados devido à maior facilidade de acesso à informação. Podemos citar como exemplo os aplicativos de bancos que permitem que transações bancárias sejam efetuadas pelo celular. Contudo, junto com o avanço tecnológico surge uma demanda para garantir a segurança da informação.

A criptografia é uma das tecnologias de maior êxito aplicada para esconder as informações e garantir segurança nas transações on-line. Inventada em 1976 por Diffie e Hellman (1976), a criptografia de chaves públicas, também conhecida como criptografia assimétrica, introduziu o conceito da assinatura digital em documentos eletrônicos. Essa técnica utiliza um sistema de duas chaves distintas. Uma chave do par é pública e pode ser divulgada, e a outra é privada, que deve ser conhecida somente pelo seu proprietário. Se cifrar a mensagem com a chave privada ela somente será decifrada pela chave pública e vice-versa.

Em 1978, logo após a invenção da criptografia assimétrica, os certificados digitais surgiram como um mecanismo confiável para o armazenamento de chaves públicas. O certificado digital é um arquivo eletrônico que atua como uma identidade virtual para uma pessoa física ou jurídica. Assinar um documento eletrônico digitalmente consiste basicamente em associar um certificado digital ao documento que está sendo assinado.

A assinatura eletrônica é definida por Stallings como "[...] mecanismo de autenticação que permite ao criador de uma mensagem anexar um código que atue como uma assinatura" (STALLINGS, 2008). Tal assinatura possui validade legal de acordo com a Medida Provisória 2.200-2, que determina que qualquer documento digital tem validade legal se for certificado pela ICP-Brasil (a ICP oficial brasileira) e garante autenticidade, integridade e irretratabilidade. No Brasil os certificados A1 e A3 são os mais comuns.

O Certificado A1 é um arquivo gerado por *software* que possui uma chave de 1024 *bits* e pode ser acessado por *login* e senha, geralmente fica instalado em um computador da empresa e apresenta menor custo. Devido a automatização do processo, a senha geralmente só é utilizada caso seja necessária a remoção do certificado de um computador para outro, possibilitando assim maior sigilo, pois as senhas não precisem ser conhecidas por todos os usuários. Como o certificado A1 se trata de um arquivo, ele pode ser utilizado simultaneamente por mais de um dispositivo.

O Certificado A3 é baseado em *hardware*, seja em *token* (USB) ou cartão com leitor específico em conformidade com a legislação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Possui uma chave de 2048 *bits*, destaca-se como uma vantagem a mobilidade e, por ser gerado em um token ou cartão, o certificado pode ser levado e instalado em qualquer computador. Para utilizar o certificado do tipo A3 é necessário usar a senha em cada uso, como consequência todos os usuários deverão saber a senha para que possam utilizá-lo. Como o certificado A3 é baseado em hardware, ele pode ser utilizado somente em um dispositivo por vez.

Esse trabalho tem como objetivo propor um pacote que realize a autenticação e assinatura digital utilizando um certificado digital do tipo A1 em aplicações *web* com o *framework* Laravel.

2 MATERIAIS E MÉTODOS

A linguagem definida para o desenvolvimento do projeto foi a utilizada pelo *Framework* Laravel: o PHP. "O PHP (um acrônimo recursivo para PHP: Hypertext Preprocessor) é uma linguagem de *script open source* de uso geral, muito utilizada, e especialmente adequada para o desenvolvimento web e que pode ser embutida dentro do HTML" (THE PHP GROUP, 2019). Dentre suas vantagens, destaca-se o suporte nativo a bibliotecas de criptografia e certificado.

Para assinar e checar os arquivos, foi utilizada a biblioteca OpenSSL (PHP OPEN SSL, 2019). Esta extensão do PHP tem como objetivo efetuar a criptografia e descriptografia simétrica e assimétrica, PBKDF2, PKCS7, PKCS12, X509 e outras operações de criptografia.

O Framework Laravel na sua versão 5.8 foi o escolhido no desenvolvimento do projeto. Laravel é um framework PHP open-source criado por Taylor B. Otwell, com o objetivo de facilitar o desenvolvimento de aplicações web. Dentre suas principais funcionalidades se destacam: *Template Engine*, Suporte a arquitetura MVC, Modularização em pacotes, Eloquent ORM e Artisan.

PHPStorm foi o ambiente de desenvolvimento integrado (IDE) utilizado. Desenvolvido pela JetBrains, o PHPStorm facilita o desenvolvimento da aplicação, com recursos como *Code Sniffer*, Suporte a SQL, PHPDoc e *code completion*.

O Apache versão 2.0 foi utilizado como o servidor da aplicação onde foram realizados os testes. Para que seja possível exportar o certificado digital do cliente, o servidor deve estar com o protocolo *HTTPS* habilitado. Como o objetivo era somente testar o pacote, foi gerado um certificado auto assinado, dessa forma não foi necessário obter um certificado digital SSL de uma empresa/autoridade certificadora. Requisitar o certificado digital de um cliente é responsabilidade do servidor e não da aplicação (APACHE, 2019). Para contornar alguns problemas de usabilidade e tornar essa comunicação mais transparente ao usuário, a aplicação e o pacote foram divididos em dois domínios diferentes, sendo o domínio principal utilizado pela aplicação e o subdomínio pelo pacote desenvolvido. As rotas do pacote foram registradas no subdomínio. O subdomínio requisitava o certificado do cliente, permitindo que o pacote tenha acesso ao certificado exportado pelo servidor. Por meio da sessão compartilhada, o pacote desenvolvido fornece o acesso ao certificado para a aplicação principal.

3 RESULTADOS E DISCUSSÃO

O trabalho foi divido em duas principais fases: estudo sobre a aplicabilidade da certificação digital em sistemas web e desenvolvimento de um protótipo de um pacote que facilite a integração da certificação digital para o *framework* Laravel. No estudo foi constatado que é possível integrar a certificação digital utilizando apenas o suporte nativo dos navegadores e servidores. Apesar dos navegadores ainda possuírem alguns problemas de usabilidade e limitações relacionados a certificação digital, é possível chegar a um resultado satisfatório. O próximo passo para o desenvolvimento foi definir um fluxo de comunicação entre a aplicação principal e o pacote Laravel. A Figura 1 demonstra o fluxo desenvolvido.

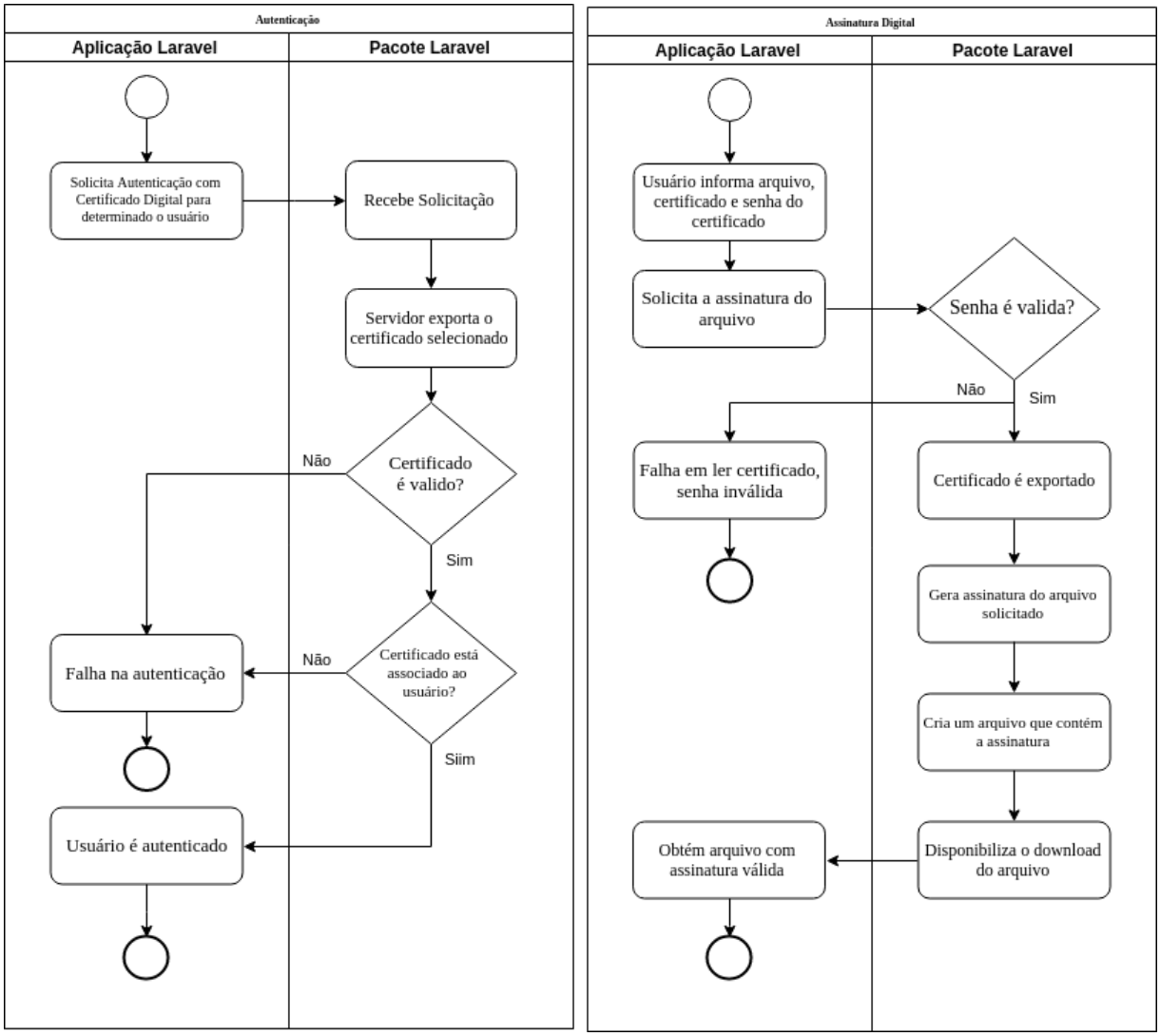

Figura 1: Fluxograma - Autenticação e Assinatura Digital

O pacote apresentou o funcionamento correto em testes realizados com uma aplicação Laravel simples que gerenciava usuários, autenticando o usuário quando solicitado e gerando assinaturas válidas para arquivos.

4 CONCLUSÃO

Como dito na seção 3, foi demonstrado, por meio de uma aplicação Laravel que o pacote desenvolvido neste trabalho respondeu de forma satisfatória aos testes realizados. Foi possível implementar a autenticação de um usuário através do certificado digital, bem como a assinatura digital de arquivos. A estratégia escolhida no trabalho não depende de nenhum *software* instalado no cliente, facilitando a distribuição, pois todas as operações são realizadas no servidor.

Nas próximas etapas do trabalho serão feitos ajustes no código e será desenvolvida toda a documentação do pacote contendo instruções de uso, configuração, funcionalidades e exemplos. Ao término do desenvolvimento o protótipo será disponibilizado em um repositório público para que outros desenvolvedores possam fazer uso ou dar suas contribuições.

REFERÊNCIAS

APACHE. **Documentation, Apache.** 2019. Disponível em: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html. Acesso em: ago. 2019.

DIFFIE, W.; HELLMAN M. E. New directions in cryptography. **IEEE Transactions on information Theory,** v. 22, n. 6, p. 644-654, 1976.

PHP OPEN SSL. **Documentation, PHP.** 2019. Disponível em: https://www.php.net/manual/pt_BR/intro.openssl.php. Acesso em: ago. 2019.

STALLINGS, W. **Criptografia e segurança de redes**: princípios e práticas. 4. ed. São Paulo: Prentice Hall, 2008.

THE PHP GROUP. **Documentation, PHP.** 2019. Disponível em: https://www.php.net/manual/pt_BR/intro-whatis.php. Acesso em: ago. 2019.

Como citar este trabalho:
AMARAL, A. A.; PEREIRA JÚNIOR, M. Proposta de arquitetura para uso de certificados digitais em aplicações Laravel. *In*: SEMINÁRIO DE PESQUISA E INOVAÇÃO (SemPI), III., 2019. Formiga. **Anais eletrônicos** [...]. Formiga: IFMG – *Campus* Formiga, 2019. ISSN - 2674-7111.