CENTRO UNIVERSITÁRIO LUTERANO DE PALMAS
Recredenciado pela Portaria Ministerial nº 1.162, de 13/10/16, D.O.U nº 198, de 14/10/2016
ASSOCIAÇÃO EDUCACIONAL LUTERANA DO BRASIL

Antônio Carlos Mota Júnior
Gabriel Fernandes
Glaycow Silveira Silva e Souza
Lucas Ribeiro Reis de Sousa
Raphael Bentes

GRUPO 4: Desenvolvimento de um software de consulta da validade de documentos

Palmas-TO
2017

SUMÁRIO

1. INTRODUÇÃO

Para atender as necessidades do projeto final da disciplina de Segurança de Sistemas, o presente projeto objetiva desenvolver um software que valide assinatura de documentos eletrônicos.

Este software, será integrado com os demais desenvolvidos por outros grupos de alunos da disciplina. Para o funcionamento do sistema proposto, será necessário o funcionamento do sistema1, visto que este irá realizar o gerenciamento de documentos que poderão ser assinados eletronicamente por usuários por meio de um certificado digital.

2 TECNOLOGIAS UTILIZADAS NO PROJETO

2.1 PHP

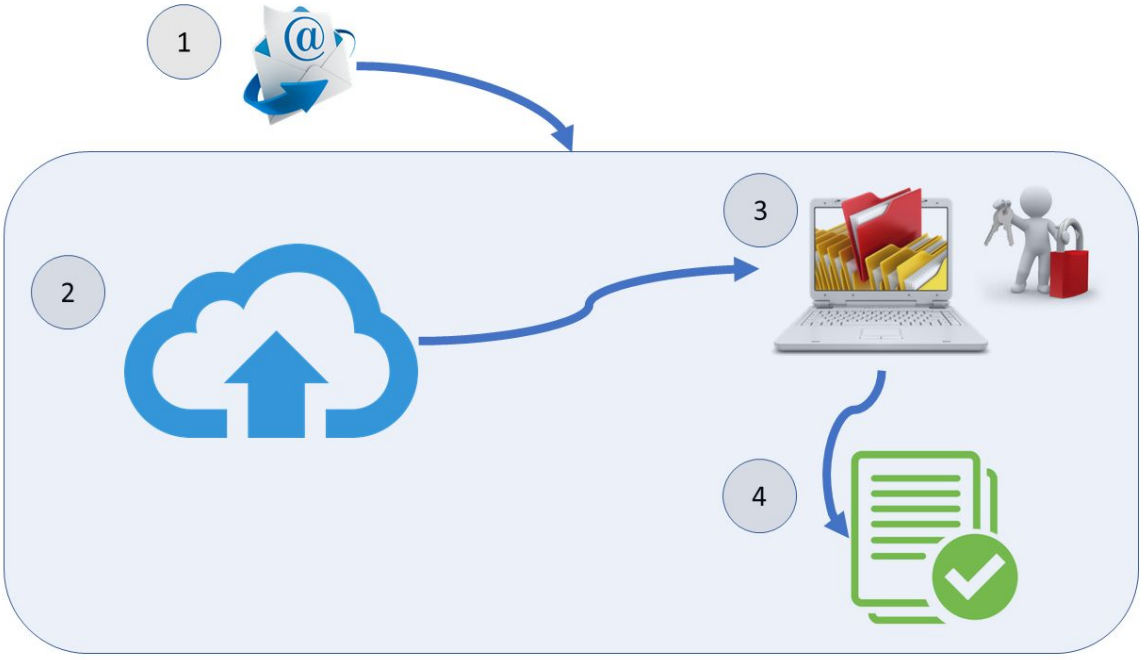
Linguagem de programação bastante utilizada por desenvolvedores Web, usada originalmente para desenvolvimento de aplicações presentes no lado do servidor, capaz de gerar conteúdo dinâmico na World Wide Web. No presente projeto, essa linguagem foi utilizada para construir o sistema web de validação de documentos, posibilitando agregar tecnologías como: HTML5, CSS3, JavaScript para contruir o visual do sistema e também possibilitar o upload e leitura de arquivos.

2.2 OpenSSL

Biblioteca PHP, para criptografia e decodificação simétricas e assimétricas PBKDF2, PKCS7, PKCS12, X509 e outras operações de criptografia, além de fornecer implementação de fluxos FLS. No presente projeto, esta biblioteca pôde fornecer a função de decriptação, utilizando a chave pública do usuário relacionado a determinado documento para validação.

3 DESENVOLVIMENTO

O presente projeto possui a seguinte estrutura:



Conforme apresentado na estrutura acima, para a realizar a consulta de validade de documentos no sistema desenvolvido dentro do projeto final da disciplina de Segurança de Sistemas, é necessário primeiramente receber o documento assinado e os dados encriptados do usuário que assinou o presente documento, via e mail do sistema1 (Sistema responsável pela assinatura de documentos utilizando certificado digital). Em seguida, é necessário realizar o upload desses arquivos recebidos via email, de forma manual, para o presente sistema desenvolvido, para que esse realize o passo 3 apresentado na estrutura (Realizar a validação do documento utilizando a biblioteca OpenSSL para decriptar o arquivo de token, utilizado para descobrir a chave pública do usuário, e assim verificar se este mesmo usuário assinou o documento que foi enviado para a aplicação). Por fim, o sistema apresenta se a validade da assinatura do documento é verdadeira ou falsa, retornando uma mensagem ao usuário.