Certificado Digital Acadêmico na Nuvem

Jean Martina[1], Fernando Pereira[2], Giovani Pieri[3], Roque Bezerra[3], Luis Cordeiro[3], Leonardo Meurer[3], Guilherme Gerônimo[3], Ricardo Custodio[1], Douglas Martins[1], Vinicius Macelai[1]

[1]Laboratório de Segurança em Computação

[2]Coordenadoria de Certificação Digital

[3]Superintendência de Tecnologia da Informação e Telecomunicações
Universidade Federal de Santa Catarina (UFSC)
Campus Universitário - Florianópolis - SC - Brasil

Resumo. *O objetivo desta apresentação é descrever um sistema que está sendo atualmente implementado na Universidade Federal de Santa Catarina para a criação de documentos eletrônicos assinados digitalmente utilizando a Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEDU). Neste sistema adotamos uma estrutura similar à utilizada na infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) a qual faz uso de uma nuvem para armazenamento de certificados e chaves privadas. Nossa solução conta com uma integração junto aos sistemas da UFSC para o armazenamento das chaves em um diretório e a sua consequente disponibilização por um serviço de autenticação LDAP. O uso da chave privada, para fins de assinatura, é feito por uma ferramenta chamada Assinador. Essa ferramenta aceita tanto certificados ICP-Brasil quanto ICPEDU. Os sistemas ainda estão em desenvolvimento e o objetivo desta apresentação é trazer à tona uma discussão sobre documento eletrônico no ambiente educacional e sua viabilidade por meio de sistemas em nuvem.*

1. Introdução

Desde a publicação da medida provisória 2200-2, o Brasil passou a contar com uma infraestrutura que proporcionou ao cidadão brasileiro a possibilidade de assinar documentos eletrônicos com validade jurídica. Desta forma, documentos assinados digitalmente são considerados equivalentes a documentos assinados em papel, com reconhecimento de firma em um cartório. Tal infraestrutura é conhecida como Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) [1].

Paralelamente à ICP-Brasil, a Rede Nacional de Ensino e Pesquisa (RNP) propiciou a criação da Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu) [4]. A ICPEDU oferece à comunidade acadêmica acesso simples e gratuito a certificados digitais para os mais diversos propósitos. Certificados são usados em salas de aula, laboratórios de ensino, equipamentos e sistemas computacionais para a criação de canais seguros de comunicação. Também são usados para assinatura de mensagens e documentos eletrônicos e para autenticação em provedores de serviços com autenticação baseada em certificados digitais. A ICPEDU opera com uma autoridade certificadora raiz e com algumas autoridades certificadoras prestando serviços para os usuários finais. Em especial, podemos citar a autoridade certificadora para usuários finais (*end users*), chamada de certificado P1 ou chamado EduId [3].

Nesta autoridade certificadora, qualquer usuário da federação CAFe (Comunidade Acadêmica Federada [2]) pode solicitar a emissão de um certificado digital, desde que a

sua instituição libere os atributos corretos para a autoridade certificadora P1. Estes certificados têm sua chave privada gerada na máquina do usuário, em software, encapsulados em um arquivo no formato PKCS12. De posse desses certificados, o usuário pode instalá-lo em sua máquina ou na aplicação que desejar, a fim de utilizá-lo para Autenticação e para conferir autenticidade de documentos. De forma geral, o certificado digital emitido por esta autoridade é um certificado de curta duração e descartável, porém apresenta um grande potencial no processo de criação de documentos eletrônicos.

Alguns dos desafios que os usuários encontram ao utilizar este tipo de certificado são: (i) a sua instalação na máquina, antes de qualquer uso; (ii) a sua desinstalação após seu uso, medida necessária para garantir a segurança de todo o processo; e (iii) o procedimento da assinatura de documentos digitais, que, apesar de múltiplas soluções livres estarem disponíveis, tem seu uso restrito para a maioria dos usuários pela dificuldade de sua utilização.

Inicialmente, a dependência da interação do usuário com o processo para garantir a segurança é um problema identificado que restringe a adoção massiva do certificado P1 no ambiente acadêmico. Então iniciamos o desenvolvimento de um processo de integração do certificado ICPEDU com o sistema de autenticação centralizada da UFSC. Criamos, dentro do sistema de gerenciamento de pessoas da UFSC, a funcionalidade de importação e armazenamento cifrado do arquivo PKCS12 na base de dados de autenticação da instituição. Permitindo que o certificado seja utilizado sob demanda, isto possibilita aos usuários conferirem autenticidade a documentos quando necessário.

Por último, para facilitar o procedimento de assinatura dos documentos digitais, nós desenvolvemos um sistema centralizado para a coleta de assinaturas digitais integrando as soluções de certificado em nuvem e soluções baseadas em tokens e arquivos. Este sistema hoje já integra a solução em nuvem disponibilizada pelo SERPRO e é um mecanismo para a busca do certificado digital P1 a partir da base da UFSC.

A fim de testar a viabilidade da solução, foi implementado um pequeno assinador de documentos PDF, o qual se integra com certificados na nuvem tanto da ICP-Brasil quanto da ICPEDU, utilizando este mecanismo de busca da chave na base de dados autoritativa de autenticação. Todo o processo foi feito utilizando entradas padronizadas de esquemas LDAP, seu armazenamento para o serviço se faz através de um sistema de autenticação centralizada, de tokens CAS e Shibboleth.

Este é um processo ainda em desenvolvimento, mas que tem como objetivo maior a criação de um padrão de assinaturas digitais para arquivamento com o uso de carimbos de tempo dentro da ICPEDU. Todo este processo ocorre na UFSC a fim de atender as diretivas do Ministério da Educação que versam a digitalização dos acervos acadêmicos das instituições de ensino superior.

Referências

[1] ITI. ICP-Brasil, Julho 2019. https://www.iti.gov.br/icp-brasil.

[2] RNP. CAFe, Julho 2019. https://www.rnp.br/servicos/servicos-avancados/cafe.

[3] RNP. EduId, Julho 2019. https://p1.icpedu.rnp.br.

[4] RNP. ICPEdu, Julho 2019. https://www.rnp.br/servicos/servicos-avancados/icpedu.