eduID – Certificados Pessoais para a Comunidade Acadêmica Brasileira

Christian Lyra Gomes[1], Luciano Rocha[1], Alex Galhano Robertson[1]

[1]Rede Nacional de Ensino e Pesquisa (RNP)
SAS, Quadra 5, Lote 6, Bloco H, 7º Andar – Brasília - DF
{christian.lyra, luciano.rocha, alex.galhano}@rnp.br

Resumo. *O eduUD é o serviço de certificados digitais para pessoas da RNP, associado à federação de identidade CAFe (Comunidade Acadêmica Federada). Este artigo descreve o trabalho em andamento para a implementação do serviço, bem como a infraestrutura necessária para suportá-lo.*

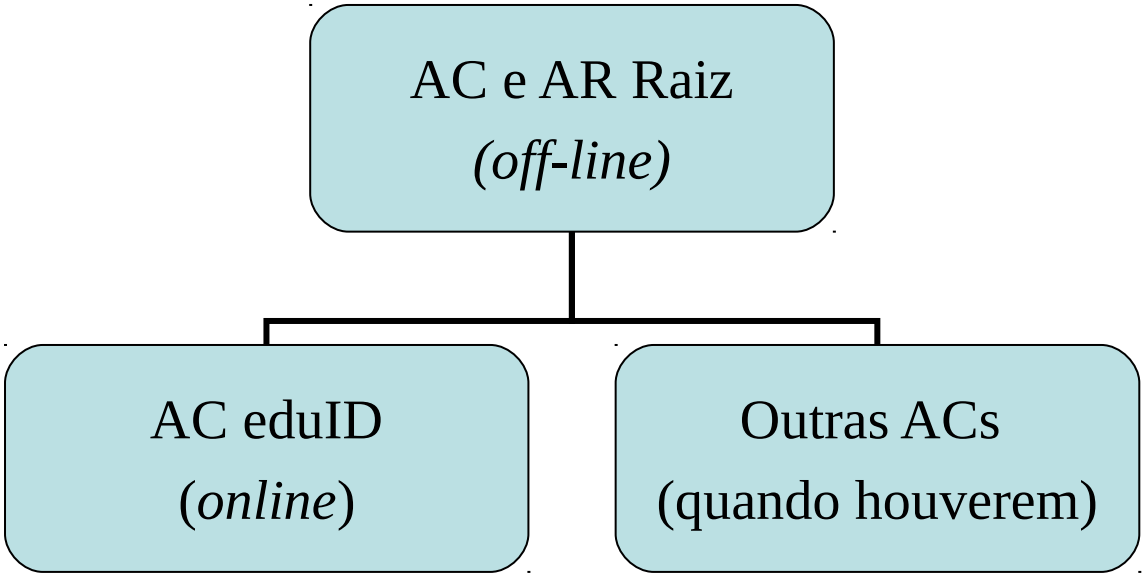
1. Introdução

Os certificados digitais funcionam como uma identidade eletrônica e podem ser utilizados para assinar/autenticar documentos eletrônicos permitindo assim otimizar processos, reduzir custos e eliminar a necessidade de impressão destes documentos. No entanto para fazer a emissão e o controle destes certificados são necessários a utilização de Autoridades Certificadoras e Autoridades de Registro. Em seguida será descrito como os serviços providos pela icpedu e pela CAFe foram utilizados para criar tais estruturas.

1.1. ICPEDU

A Infraestutura de Chaves Públicas para Ensino e Pesquisa (icpedu) é o serviço de certificação digital oferecido pela Rede Nacional de Ensino e Pesquisa (RNP) que provê infraestrutura para a emissão de certificados digitais e chaves de segurança [Rede Nacional de Ensino e Pesquisa, 2019 A]. Originalmente a icpedu previa que a RNP se responsabilizaria pela criação da Autoridade Certificadora Raiz (AC-Raiz) e Autoridade de Registro Raiz (AR-Raiz) e as instituições que aderissem ao serviço criariam suas próprias Autoridades Certificadoras de Serviço/Intermediárias, estas sim responsáveis pela emissão de certificados para os usuários. Como a criação e manutenção de autoridades certificadoras envolvem custos de manutenção e conhecimento e hardware especializado, a estratégia inicial passou a representar uma barreira para adoção do serviço. A partir de 2014 a icpedu iniciou sua primeira grande reestruturação, com o objetivo de tornar o serviço mais acessível e uma das iniciativas desse movimento foi a criação da Autoridade Certificadora eduID.

A RNP continua mantendo as Autoridades Certificadoras Raiz e Autoridade de Registro Raiz da icpedu, que são armazenadas em datacenters seguros, contando com Sala/Rack Cofre e *hardware* criptográficos especializados conhecidos como HSMs, para a guarda das chaves. As autoridades Raiz são mantidas off-line e utilizadas apenas para a criação/ revogação de autoridades intermediárias, como as ACs do eduID.



1.2. CAFe

A Comunidade Acadêmica Federada (CAFe) é um serviço de gestão de identidade, baseada em SAML (Security Assertion Markup Language) e Shibboleth, que reúne instituições de ensino e pesquisa brasileiras através da integração de suas bases de dados. Isso significa que, por meio de uma conta única, o usuário pode acessar, de onde estiver, os serviços de sua própria instituição e os oferecidos pelas outras organizações que participam da federação [Rede Nacional de Ensino e Pesquisa, 2019 B]. Cada instituição é responsável pelo cadastro e manutenção da sua base de usuários. A CAFe pode também prover dados do usuário de maneira segura, como CPF e data de nascimento. Essa característica permitiu que a CAFe exerça a função de uma Autoridade de Registro para o eduID.

1.3. eduID

O eduID é o nome do serviço e da AC intermediária *online* da icpedu que emite os certificados das pessoas. É mantida pela RNP e possibilita que usuários das instituições clientes que estão na CAFe possam emitir certificados digitais pessoais sem intervenção de nenhum funcionário.

Além da infraestrutura de chaves públicas, foi desenvolvido um portal e um programa especial onde o usuário utiliza suas credenciais da CAFe para obter acesso ao sistema de emissão de certificados. A instituição, por meio da café, informa os atributos necessários para a emissão do certificado pessoal: o nome da instituição do usuário, mais o nome completo, a data de nascimento, o CPF e o endereço de email da pessoa.

O portal gera as chaves e a requisição de certificado, que é assinado de maneira online pela AC eduID, de maneira transparente para o usuário. O certificado é criptografado com senha provida pelo usuário e é feito o download para sua máquina, podendo ser instalado automaticamente na hora ou copiado e instalado em outros dispositivos posteriormente.

Essa AC também é mantida em ambiente seguro e utiliza *hardware* criptográfico especializado, o HSM.

No momento, o serviço está funcionado como piloto. Está em estágio de homologação, com expectativa de lançamento até o fim do ano.

4. Expectativas

No momento, o serviço se encontra em estágio de homologação, com expectativa de lançamento até o fim do ano.

Como sua utilização é bastante simples, espera-se que funcione como um facilitador para adoção práticas como a assinatura digital de documentos e processos eletrônicos pelas instituições de ensino e pesquisa nacionais.

7. References

Rede Nacional de Ensino e Pesquisa – Infraestrutura de Chaves Públicas para Ensino e Pesquisa. Disponível em: <https://www.rnp.br/servicos/servicos-avancados/icpedu>. Acesso em 20 de julho de 2019.

Rede Nacional de Ensino e Pesquisa - Serviço Avançado CAFe. Disponível em: <https://www.rnp.br/servicos/servicos-avancados/cafe>. Acesso em 20 de julho de 2019.