Menos Certificação Digital e Mais Identidade Eletrônica: ICPEdu e CAFe em um Assinador Digital Inclusivo

Eduardo Dani Perottoni[1], Bernardo Pandolfi Costa[1], Fernanda Larissa Müller[1], Victor dos Santos Camargo[1], Frederico Schardong[1,2], Wellington Silvano[1], Lucas Mayr[1], Ricardo F. Custódio[1], Luciano Rocha[3], Christian Lyra[3], Reinaldo Matushima[3], Nicole Rieckmann[3]

[1]Laboratório de Segurança em Computação (LabSEC)
Universidade Federal de Santa Catarina (UFSC)

[2]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS)

[3]Rede Nacional de Ensino e Pesquisa (RNP)

Resumo. *Este artigo apresenta a arquitetura e funcionalidades de um assinador digital tecnicamente inclusivo. O assinador utiliza identidades eletrônicas da Comunidade Acadêmica Federada (CAFe) para a emissão de Certificados de Assinatura Única (CertAU) na Infraestrutura de Chaves-Públicas de Educação (ICPEdu). O assinador permite que documentos sejam assinados de forma simples, rápida e segura.*

1. Introdução

A identidade eletrônica é um dos pilares da construção de sistemas seguros. Dentre as diversas maneiras de projetar, implementar e gerenciar identidades eletrônicas, a construção de federações de provedores de identidade, ou *Identity Providers* (IdPs), traz interoperabilidade e acesso a serviços aos usuários de IdPs da federação. A Comunidade Acadêmica Federada (CAFe) é uma implementação desse modelo gerenciada pela Rede Nacional de Ensino e Pesquisa (RNP) desde 2008, e reúne, no momento de escrita deste artigo, mais de 1 milhão de usuários em 380 IdPs de instituições de ensino e pesquisa no Brasil, permitindo o acesso a inúmeros serviços entre usuários de diferentes instituições.

Um dos serviços oferecidos aos membros da CAFe é a emissão de certificados digitais. Esses certificados fazem parte da Infraestrutura de Chaves Públicas (ICP) para Ensino e Pesquisa (ICPEdu) e permitem que os usuários tenham, sem custo, certificados para realizarem autenticação e assinatura digital. Entretanto, apenas 4% dos usuários da CAFe fazem uso deste serviço, apesar da crescente demanda por assinaturas digitais.

Este artigo apresenta um projeto que une CAFe, ICPEdu e Certificado de Assinatura Única (CertAU) para criar um assinador digital onde não é necessário qualquer interação do usuário final com a ICP, efetivamente provendo interações mais simples e significativas no processo de assinatura. O restante do trabalho é organizado da seguinte maneira: a Seção 2 apresenta a infraestrutura da ICPEdu modificada visando a geração de certificados CertAU; a Seção 3 apresenta a arquitetura do assinador, assim como o fluxo de assinatura e uma discussão sobre o processo de assinatura e a Seção 4 conclui o artigo.

O presente trabalho foi realizado com apoio do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS).

2. Mudanças na ICPEdu

ICP é um conjunto de políticas operacionais e de segurança, serviços e protocolos de interoperabilidade que suportam o uso de criptografia de chave pública para gestão de chaves e certificados [Weise 2001]. Uma ICP é tradicionalmente organizada em uma hierarquia de Autoridades Certificadoras (ACs) no formato de árvore, onde as folhas representam certificados de usuários. O certificado digital é um documento eletrônico que associa uma chave pública a uma entidade.

A ICPEdu emite certificados digitais para membros das instituições da CAFe. Porém, o manuseio destes certificados por usuários é trabalhoso, visto que uma alta carga de responsabilidade é atribuída ao usuário. Por exemplo, fica a cargo do usuário fazer a gestão da chave privada de seu certificado, bem como instalar o certificado e sua respectiva chave em sistemas para poder assinar documentos digitalmente.

Considerando essas e outras dificuldades, o Certificado de Assinatura Única (CertAU) propõe a geração de um certificado para cada assinatura digital, eliminando a possibilidade de comprometimento de chave privada [Mayr et al. 2022]. O CertAU é associado ao documento assinado através do cômputo do resumo criptográfico do documento, que é adicionado ao certificado. Os atributos que associam unicamente o usuário e a chave pública no CertAU são obtidos através do IdP do usuário autenticado. Nesse caso, autenticado em um IdP da CAFe. Considerando que: (i) o CertAU só é válido para o documento associado; (ii) os atributos que identificam o usuário no CertAU são obtidos do IdP a cada assinatura; então (iii) a revogação torna-se desnecessária [Mayr et al. 2022]. Porém, para garantir interoperabilidade com sistemas existentes, as ACs CertAUs podem emitir uma Lista de Certificados Revogados (LCR) vazia. Como consequência de não ser revogável e os atributos serem obtidos no momento da assinatura, o CertAU remove a necessidade de adicionar carimbo do tempo no documento assinado e pode ter tempo de vida longo, *e.g.* 100 anos.

Uma nova árvore de certificação, composta de uma AC Raiz e uma AC emissora de CertAUs ambas com validade de 100 anos, foi criada. Adicionalmente, uma Lista de Serviços de Confiança (LSC) [ETSI TS 119 612 2016] foi criada para gerenciar as raízes de confiança da ICPEdu. A Figura 1 ilustra a LSC com as duas ACs raízes e suas respectivas árvores de certificação.

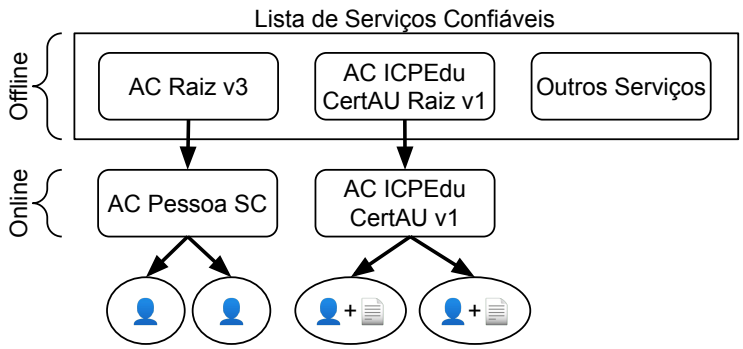

Figura 1. ICPEdu com LSC e duas árvores de certificação: tradicional e CertAU.

3. Assinador Digital

O Assinador Digital é um projeto da RNP que faz uso da árvore de certificação CertAU da ICPEdu. Ele segue a arquitetura de microsserviços. Ou seja, cada serviço é construído para executar uma tarefa específica dentro do contexto da aplicação e pode ser desenvolvido, implantado e escalado de forma independente dos outros serviços, proporcionando flexibilidade e modularidade [Thönes 2015].

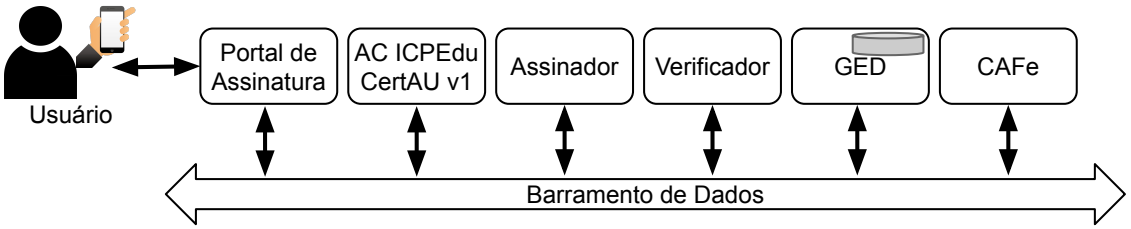

Figura 2. Arquitetura do assinador digital.

O Assinador Digital é constituído pelos seguintes serviços: (i) portal de assinatura é a interface entre o usuário e os demais serviços; (ii) ICP é o serviço que se comunica com ICPEdu para emitir CertAUs; (iii) verificador é responsável pela verificação de documentos assinados; (iv) assinador realiza a assinatura digital em PDFs de acordo com a especificação ISO 32000-2 [ISO 32000-2:2020 2020]; (v) Gerenciamento Eletrônico de Documentos (GED) armazena documentos assinados permitindo diferentes usuários assinarem o mesmo documento sem seu reenvio; e (vi) ID conecta-se a CAFe para autenticar usuários e coletar seus atributos para emissão de CertAU.

O usuário final, ao interagir com o assinador digital através do portal de assinatura, faz uso dos serviços descritos acima. A Figura 3 ilustra em um fluxograma as interações entre usuário, assinador digital, CAFe e ICPEdu para a assinatura de um documento.

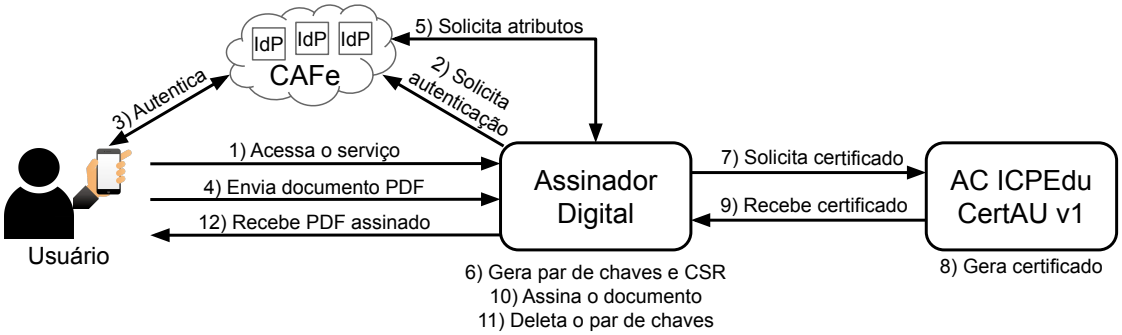

Figura 3. Fluxograma de assinatura.

O usuário acessa, por meio de seu navegador, o assinador digital (passo 1), que solicita sua autenticação, redirecionando-o para a CAFe (passo 2). Após autenticar-se em um dos IdPs da federação (passo 3), o usuário envia o documento que deseja assinar (passo 4). É importante observar que a autenticação (passo 3) obriga o uso de múltiplos fator de autenticação (MFA). Sem a necessidade de intervenção do usuário, o assinador solicita os atributos ao IdP (passo 5), gera um par de chaves assimétricas e constrói o *Certificate Signing Request* (CSR) (passo 6), que é enviado para a AC (passo 7). O CSR contém, além

dos atributos do usuário, o *hash* do documento enviado no passo 4. Recebendo o CSR, a AC emite o certificado CertAU (passo 8), enviado-o como resposta para o assinador (passo 9). Com o certificado que associa o usuário ao documento, o assinador faz a assinatura aplicando as especificações da ISO 32000-2 (passo 10), que engloba adicionar o certificado ao PDF, e então deleta o certificado e o par de chaves gerados no passo 6 (passo 11) e retornando o documento assinado (passo 12).

O CertAU simplifica a ICP ao remover a necessidade de revogação de certificados finais e carimbo do tempo em documento assinados. O CertAU é criado e usado apenas para assinar o documento que o usuário deseja assinar. Consequentemente a experiência do usuário é aprimorada, visto que o mesmo não precisa gerenciar smartcards, chaves, certificados em nuvem, PIN de desbloqueio ou outros artefatos relacionados à certificação digital. O usuário apenas interage com a CAFe para autenticar-se e com o assinador para enviar o documento que deseja assinar e recebê-lo assinado. Essas interações são simples, diretas e não exigem do usuário conhecimento técnico. Nota-se que não há perda de nível de segurança ao utilizar IdP ao invés de smartcards, *i.e.*, na ICP tradicional é necessário ter posse do token criptografico e sua senha, no CertAU é necessário conhecer as credenciais de acesso e ter posse do dispositivo de MFA.

4. Conclusão

No momento da escrita deste artigo a ICPEdu tem 42 mil certificados válidos potencialmente em uso[1], apesar da CAFe ter em torno de 1 milhão de usuários nos IDPs federados. O assinador digital da RNP pode alterar este panorama, permitindo que todos os usuários da CAFe façam uso da assinatura digital. Através da utilização de CertAU na ICPEdu e da federação CAFe, o assinador digital da RNP permite que usuários leigos façam assinatura digital com interações simples e significativas. Ele não exige conhecimento sobre certificação digital, tampouco gestão de artefatos criptográficos e cria assinaturas digitais que valem para toda a vida do usuário empregando certificados com validade de 100 anos.

Referências

ETSI TS 119 612 (2016). Electronic signatures and infrastructures (esi); trusted lists. Standard, European Telecommunications Standards Institute.

ISO 32000-2:2020 (2020). Document management — portable document format — part 2: Pdf 2.0. Standard, International Organization for Standardization.

Mayr, L., Schardong, F., and Custódio, R. (2022). Simplifying electronic document digital signatures. Disponível em: `https://arxiv.org/pdf/2208.03951.pdf`. Acesso em: 24 jul. 2023.

Thönes, J. (2015). Microservices. *IEEE Software*, 32(1):116–116. Disponível em: `https://ieeexplore.ieee.org/abstract/document/7030212`. Acesso em: 27 jul. 2023.

Weise, J. (2001). Public key infrastructure overview. *Sun BluePrints OnLine, August*, pages 1–27.

[1] `https://web.archive.org/web/20230727134153/https://painel.icpedu.rnp.br/public/stats/certificate`