Assin@UFSC:
Uma Solução Centralizada para
Assinatura Digital de Documentos

Resumo. Em 2020, durante a pandemia, a Universidade Federal de Santa Catarina (UFSC) gerou mais de 500.000 documentos assinados digitalmente, o que possibilitou que sua administração operasse 100\% de forma digital. Neste artigo descrevemos a solução desenvolvida para a criação de documentos eletrônicos assinados digitalmente com certificados ICPEdu e ICP-Brasil. Este artigo engloba as questões legais e os processos de criação dos certificados pessoais, assinatura de documentos, validação e integração com outros sistemas. Por fim, são apresentados números referentes à adoção de assinatura digital no contexto da universidade.

Palavras-chave: Documentos eletrônicos; Assinatura Digital; Segurança da Informação.

Eixo temático: Tecnologías y soluciones para el trabajo remoto de los investigadores.

1. Introdução

A Pandemia global da COVID-19 exigiu uma resposta rápida das instituições de ensino. Neste contexto, em um intervalo curto de tempo, a Universidade Federal de Santa Catarina (UFSC) se viu obrigada, assim como demais órgãos e instituições de ensino, a suspender quase todas as atividades presenciais. Tanto as aulas quanto as atividades administrativas passaram a ser desempenhadas de forma remota, forçando a adoção em massa de ferramentas de Tecnologias de Informação e Comunicação. Um dos grandes desafios encontrados durante esse processo foi a questão de como transpor a assinatura de documentos para o mundo digital.

Desde a publicação da medida provisória 2200-2/2001 [1], o Brasil passou a contar com um arcabouço legal que permite pessoas físicas e jurídicas realizarem assinaturas digitais em documentos eletrônicos com validade jurídica. Além disso, a Lei 14.063/2021[2] regulamenta o uso de assinaturas eletrônicas para comunicação entre cidadãos e os entes públicos, incluindo a classificação dos tipos de assinatura e os graus de confiabilidade conferidos em cada caso.

Para todos os efeitos legais, documentos assinados digitalmente são considerados equivalentes a documentos assinados em papel com reconhecimento de firma em um cartório. O pré-requisito para que o documento assinado digital seja considerado válido é que sejam usadas tecnologias de criptografia assimétrica (assinatura digital) com certificado emitidos dentro da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) [3], ou mesmo certificados de outras ICPs, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

A massificação do uso de assinaturas digitais como resposta à necessidade de tratar a assinatura eletrônica de documentos incorre em um problema de custos. Os Certificados ICP-Brasil tem um custo de aquisição na ordem de R$ 250,00 cada, com validade de 3 anos. Em uma instituição universitária do porte da UFSC, cuja comunidade acadêmica tem em torno de 55.000 pessoas, isso geraria um custo na ordem de R$ 13.750.000,00. Além disso, a emissão de um certificado digital ICP-Brasil exige procedimentos de entrega do certificado *in loco* (em Autoridades de Registro), que seria restritivo durante a pandemia.

Paralelamente à ICP-Brasil, a Rede Nacional de Ensino e Pesquisa (RNP) criou a Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu) [4]. A ICPEdu oferece à comunidade acadêmica acesso simples e gratuito a certificados digitais pessoais.

Nesta autoridade certificadora, qualquer usuário da federação CAFe (Comunidade Acadêmica Federada [5]) pode solicitar a emissão de um certificado digital, desde que a sua instituição libere os atributos corretos para a autoridade certificadora da ICPEdu. 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.

Para a massificação do uso de criptografia assimétrica e certificados digitais como solução de larga escala para assinatura de documentos eletrônicos, identificamos uma série de desafios e dificuldades apresentadas pelos usuários durante o processos de assinatura digital adotado na UFSC: (i) dificuldade no entendimento e manipulação de certificados digitais pela comunidade universitária; (ii) o procedimento da assinatura de documentos digitais *in loco* (nas estações de trabalho); (iii) a validação dos documentos já assinados; (iv) a credibilidade e adoção da certificação digital, a fim de eliminar o processo

"imprime/assina/digitaliza" comum na instituição.

Paralelamente, enfrentamos a questão da resistência na adoção da solução pelos usuários. Como sua utilização é facultativa, convencer, estimular e difundir o uso da solução tornou-se um desafio frente aos velhos costumes.

Tecnicamente, identificou-se a necessidade de integrar a solução proposta à sistemas já utilizados na gestão eletrônica de documentos (GED), na medida em que exigiam atualização para se adequarem às novas demandas de trabalho. Por outro lado, deparou-se com o desafio de fazer a integração desses sistemas de forma desacoplada, exigindo o mínimo de refatoração possível.

Assim, com estas questões em mente, as principais contribuições da solução de Assinatura Digital que se encontra em uso na UFSC atualmente: (i) na solução de armazenamento de certificados em nuvem - para retirar do usuário final a responsabilidade pela correta manipulação de certificados digitais; (ii) no sistema web para assinatura de documentos digitais - para simplificar o processo de assinatura; (iii) no serviço de validação de documentos autenticados - para permitir a validação simples de documentos pelos usuários; (iv) na estratégia de integração de sistemas legados, e; (v) no plano de ação administrativo para difundir a assinatura digital e extinguir processos em papel.

O projeto de assinatura digital foi liberado para os usuários no fim de 2019.Em um ano de uso, atingiu a marca de mais de 500.000 documentos eletrônicos assinados digitalmente. Com a pandemia, a UFSC passou a ser 100% digital, e o processo de assinaturas eletrônica é feito integralmente com certificação digital e criptografia assimétrica.

2. ICPEdu: Certificados gratuitos para toda a comunidade universitária

A Infraestrutura de Chaves Públicas para Pesquisa e Ensino (ICPEdu) é um serviço da RNP que corresponde a um esforço para incentivar a criação de certificados digitais e chaves de segurança, aplicados em autenticação, assinatura digital e sigilo, dentro do ambiente das Instituições Federais de Ensino Superior (Ifes), Unidades de Pesquisa (UPs) e demais instituições de ensino. As organizações usuárias da ICPEdu podem emitir gratuitamente seus próprios certificados digitais, que funcionam como assinaturas eletrônicas para pessoas. O usuário obtém um certificado emitido pela instituição, o qual é reconhecido pelos demais membros da rede. A partir do reconhecimento do certificado, ele pode assinar documentos de forma segura e confiável.

A utilização de certificados digitais pelas Ifes e UPs confere credibilidade aos serviços e processos administrativos das instituições, bem como garante a identidade de seu portador. Além disso, permite que processos sejam executados com maior eficiência e agilidade, resultando em economia de tempo e dinheiro.

As soluções técnicas, ferramentas e equipamentos aplicados na implantação da ICPEdu são resultados de estudos iniciados em 2003, desenvolvidos por Grupos de Trabalho (GTs) da RNP. Em 2007, a ICPEdu foi lançada em caráter experimental, envolvendo um pequeno número de instituições. E, após uma fase piloto em 2018, o serviço foi oficalmente lançado para a comunidade em março de 2021 pelo Ministério da Educação.

Os usuários emitem seus próprios certificados digitais pessoais ICPEdu por meio de um portal Web [5], disponibilizado como um serviço através da Comunidade Acadêmica Federada (CAFe). A CAFe é uma solução de gestão de identidade federada, baseada em SAML (Security Assertion Markup Language) e Shibboleth, que reúne instituições de ensino e pesquisas brasileiras através da integração de suas bases de dados. Isso significa que, por meio de uma conta única, dentro da sua própria instituição, o usuário pode acessar,

de onde estiver, os serviços oferecidos pelas outras organizações que participam da CAFe na condição de provedor de serviço.

Para que o portal possa gerar um certificado digital pessoal, a instituição, por meio da café [6], informa os atributos do usuário ao portal: o nome da instituição do usuário, o nome completo, a data de nascimento, o CPF e o endereço de e-mail. O portal então gera as chaves e a requisição de certificado, que é assinado de maneira online pela autoridade certificadora AC Pessoa, de maneira transparente para o usuário. O certificado é criptografado com senha (PIN) provida pelo usuário, e este pode fazer o download e instalar o certificado no sistema local ou em outros dispositivos posteriormente.

Uma característica importante da geração de certificados pessoais ICPEdu é que o par de chaves criptográficas são gerados localmente no dispositivo do usuário, de forma que, por padrão, a chave privada do usuário não é conhecida por nenhum sistema externo. Isso confere uma camada de proteção a uma série de vulnerabilidades de segurança, porém coloca no usuário a responsabilidade de manipular corretamente a única cópia existente do seu certificado.

Outra característica, relacionada à anterior, é que a AC Pessoa somente permite um certificado ativo por usuário, sendo que ao gerar um certificado novo, o certificado antigo é automaticamente revogado. Juntamente com a característica anterior, isso leva a possibilidade de cenários onde um usuário pode ter diversos certificados antigos, revogados, instalados em sistemas e dispositivos diferentes, sendo inclusive utilizados para gerar assinaturas inválidas.

3. Custódia de Certificados na Nuvem

Apesar dos certificados Pessoais da ICPEdu já serem gerados pelo portal [5], é necessário que a solução de assinatura digital Assin@UFSC possa acessar esse artefato de forma ágil e com o mínimo de dificuldade na interação do usuário. Assim, criou-se um módulo de gerenciamento de certificados, onde cada usuário pode guardar seus certificados Pessoais ICPEdu. Esse módulo tem o papel de centralizar o acesso ao certificado digital do usuário, e simplificar a gestão do mesmo.

Para executar o procedimento de criação e armazenamento dos certificados, o usuário: (i) entra no portal de geração de certificados pessoais [5], autenticando-se com suas credenciais da CAFe; (ii) informa uma senha (PIN) para o certificado novo - o certificado anterior é automaticamente revogado; (iii) faz o download do certificado em um formato PKCS#12, protegido pela senha (PIN); (iv) entra no módulo de gestão do certificado em nuvem do Assin@UFSC; (v) visualiza os dados do seu antigo certificado, se houver; e, (vi) realiza o upload do seu certificado novo, que passará a ser utilizado nos procedimentos de assinatura de documentos no Assin@UFSC.

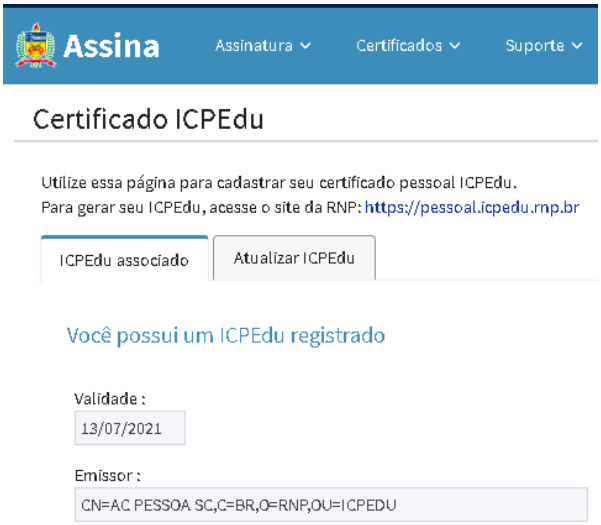

Fig. 1. Interface do módulo de gerencia de certificados na nuvem.

4. Assinando e Validando Documentos

O princípio do Assin@UFSC é facilitar e simplificar o processo de assinatura digital tendo como usuário alvo pessoas sem conhecimento técnico acerca de segurança da informação e gestão de documentos digitais. Assim levantamos os seguintes requisitos a serem atendidos: (i) possibilitar a assinatura em diversos dispositivos (estação de trabalho, celular, tablet, etc.); (ii) dispensar a necessidade de ter o certificado pessoal instalado localmente nos dispositivos para assinatura; (iii) possibilitar múltiplas assinaturas no mesmo documento; (iv) suportar a assinatura de documentos PDF; (v) permitir a validação dos documentos previamente assinados; e (vi) uma representação gráfica das assinaturas (assinatura de conforto);

A interface de validação [7] de documentos recebe arquivos e analisa suas assinaturas, considerando confiáveis certificados pertencentes às cadeias certificadoras da ICPEdu e ICP-Brasil. Um relatório é gerado exibindo ao usuário os dados de cada assinatura (nome, status da assinatura, atributos envolvidos) e os dados do caminho da cadeia certificadora. A Figura 2 exemplifica um relatório da interface do validador.

Fig. 2. Relatório de Validação de Documentos Assinados.

O processo de assinatura idealizado é:

1. o usuário entra em assina.ufsc.br [8];
2. se autentica no sistema de autenticação centralizado, caso ainda não esteja autenticado;
3. clica em "Adicionar Arquivo", seleciona o documento e faz o *upload*;
4. ao visualizar o documento na ferramenta, seleciona a posição onde deseja que fique a sua assinatura;
5. ao clicar em assinar, uma lista de provedores de certificados (ICPEdu, NeoId, etc) é exibido para escolha;
6. o sistema requisita a senha do certificado, assina o documento e exibe o mesmo com a representação gráfica da assinatura.

A Figura 3 exemplifica esta interface com um documento assinado e assinatura no canto direito inferior.

Fig. 3. Interface de Assinatura de Documentos

O sistema do assinador usa uma arquitetura baseada em WebServices, e um front-end implementado usando tecnologias Java EE. A estrutura interna é esquematizada na figura 4. A solução pode ser subdividida em 3 grandes partes:

1. Webservices para manipulação eletrônica de documentos e assinatura eletrônica;
2. Sistema de armazenamento e recuperação de certificados digitais em nuvens;
3. Provedores de assinaturas.

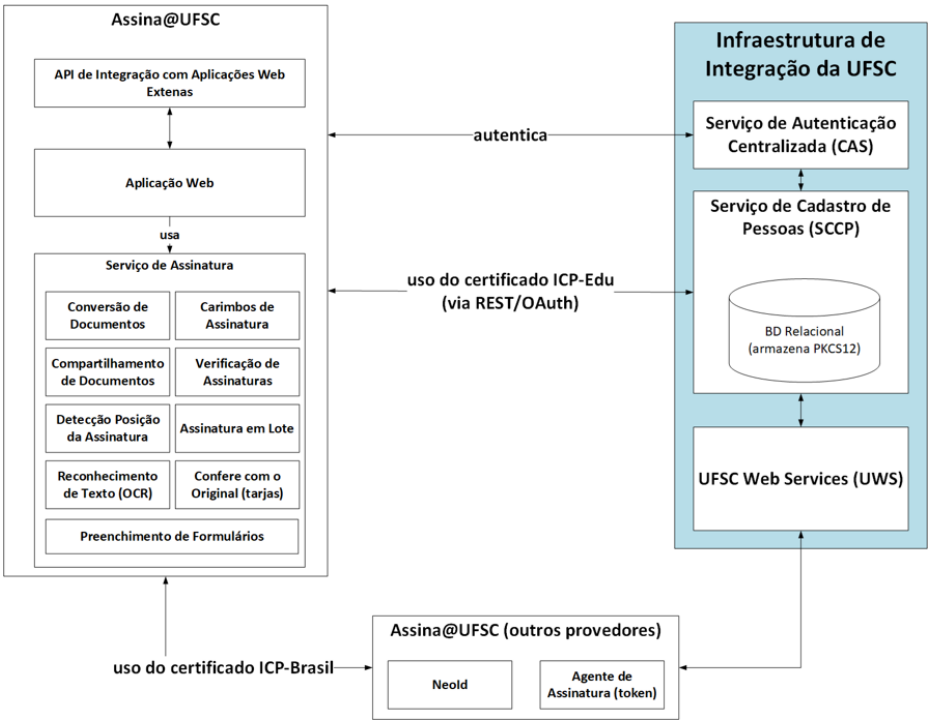

Fig. 4. Representação esquemática da solução Assina UFSC

Os certificados digitais ICPEdu criptografados são armazenados dentro da base autoritativa de usuários da UFSC. Para a recuperação dos certificados digitais dos usuários é obrigatório fazer uso de um Webservice próprio cujo acesso foi autorizado explicitamente pelo usuário por OAuth, implementado pelo sistema de autenticação centralizada da UFSC (CAS). Dessa forma garante-se que para ter acesso ao certificado digital criptografado de um usuário, o usuário teve que dar autorização explicita.

Para realização de uma assinatura, pode-se usar diferentes provedores de assinatura. Atualmente o Assin@UFSC suporta três provedores de certificados:

(1) certificado armazenado na nuvem de certificados do Assin@UFSC;
(2) certificado digital ICP-Brasil armazenado em nuvem emitido pelo Serpro (NeoID);
(3) certificado digital da infraestrutura GOV.Br;
(4) certificado físico instalado na máquina do usuário (token).

Esta decisão arquitetural na separação do webservice de assinatura do provedor de cifra criptográfica permite que o Assin@UFSC não dependa de um fornecedor de equipamentos e soluções criptográficas, permitindo ao usuário e a instituição o livre uso das certificados digitais que ele possui.

No que tange a geração de assinaturas eletrônicas, cada formato de documento possui associada a si um padrão diferente. Por este motivo, decidiu-se na padronização de todos os documentos eletrônicos da UFSC no padrão PDF. Este é um padrão que já estava em uso na universidade, é um padrão aberto normatizado pela ISO 32000-1 e possui suporte nativo para assinatura digital. Dentro dos diferentes padrões de assinatura, foi adotado o padrão adbe.pkcs7.detached [9], que consiste em uma assinatura na Sintaxe de Mensagem Criptográfica (Cryptographic Message Syntax -- CMS -- RFC5652) embarcada em um formulário PDF em um campo PDSignature. Para realização de uma assinatura encaminha-se ao webservice de assinatura digital o PDF a ser assinado, este PDF é então processado e

um Hash Criptográfico SHA-256 do documento é calculado, conforme especificado pela ISO 32000-1. Uma vez calculado o Hash do documento, o pacote CMS em conformidade com a RFC5652 é gerado e um novo Hash 256 do pacote CMS é realizado e uma cifra criptográfica é criada com o algoritmo RSA. Essa cifra criptográfica é incluída no pacote CMS, e finalmente o pacote CMS é anexado ao elemento PDSignature.

O Assin@UFSC e o webservice de assinatura usam uma carimbadora de tempo para prover uma estampilha de tempo confiável na confecção da assinatura digital. Isso traz mais um elemento de confiança as assinaturas digitais, pois impossibilita que um atacante manipule seu relógio local durante a geração da assinatura digital. Além disso, este elemento permite que documentos que tenham sido assinados usando um certificado digital revogado possam ser verificados e permaneçam confiáveis, caso a assinatura tenha ocorrido antes da revogação do certificado.

Para implementação da solução foram adotados os seguintes softwares livres:

- **PDF.js [10]**: Biblioteca javascript responsável pela renderização dos documentos PDFs em navegadores. Devido a uma decisão política feita pelos mantenedores da biblioteca, tivemos que modificá-la para exibir a representação gráfica das assinaturas, que é desabilitada por padrão.
- **PDFBox [11]:** Biblioteca Java usada para embarcar assinaturas digital em documentos PDF, computo de Hashes para assinatura, criação das representações gráficas das assinaturas, preenchimento e manipulação de formulários PDFs.
- **Bouncy Castle [12]:** Biblioteca Java que implementa algoritmos criptográficos necessários para geração da assinatura digital, como por exemplo, a manipulação dos certificados digitais, implementação de funções de hashes criptográficas e o algoritmo de criptografia assimétrica RSA-256.
- **LibreOffice [13]:** Suite opensource usada para conversão automática de documentos para o padrão PDF/A.

Dentro das várias dificuldades técnicas, ressaltamos os seguintes pontos:

- Celulares: Dispositivos móveis demonstraram ser um desafio para seleção da localização das assinaturas. Como a biblioteca PDF.js e navegadores não se comportam homogeneamente entre distintos aparelhos, o ponto selecionado na tela nem sempre era o mesmo interpretado pela biblioteca, causando a representação errada da marca no documento.
- Políticas de Certificado: Apesar de haver uma padronização de políticas de assinaturas para PDF, conhecida como PAdES (normatizada pela ETSI [14]), no Brasil o ITI [15] criou normativas para assinaturas avançadas conhecidas como Padrão Brasileiro de Assinaturas Digitais (PBAD). Infelizmente, diferentemente do PAdES, o PBAD não é nativamente reconhecido pelos principais softwares de verificação de assinaturas digitais (e.g. Adobe), ou seja, documentos assinados no padrão PBAD são considerados inválidos. Portanto, decidimos não implementar padrões de assinatura avançada (nem PAdES, nem PBAD), somente assinatura simples (PKCS7), para evitar confusão devido a refutação de softwares de terceiros que não validam nossos documentos.

5. Mecanismo de integração com sistemas externos

Identificamos que existem uma gama de aplicações e sistemas diferentes que fazem uso ou podem vir a adotar soluções de assinatura digital dentro dos processos administrativos e gerenciais da Universidade.
Portanto, decidiu-se que a solução deve ser agnóstica a processos, mas deve permitir que outras aplicações e sistemas integrem-se a ela.

Para atingir este objetivo foi projetada uma API de integração baseada no protocolo HTTP. Para que um sistema se integre a solução é necessário que ele implemente três URLs:

- **URL de Download** - usada pelo Assin@UFSC para realizar o download do documento PDF que deve ser assinado pelo usuário.
- **URL de Upload** - usada pelo Assin@UFSC para realizar o upload do documento PDF já assinado pelo usuário.
- **URL de Retorno** - usada pelo usuário para retomar a sua atividade no sistema de origem, após o processo de assinatura.

O sistema que deseja se integrar deve redirecionar seu usuário a URL https://assina.ufsc.br/assinatura com as informações listadas acima no GET (variáveis "doc","p" e "redirect"). O Assin@UFSC então:

1. faz o download do documento PDF que deve ser assinado;
2. realiza todo o procedimento de assinatura junto ao usuario
3. faz o upload do documento PDF assinado;
4. redireciona o navegador do usuário de volta à aplicação de origem.

A figura 5 exemplifica a troca de mensagens entre o usuário, o Assin@UFSC e o sistema integrado.

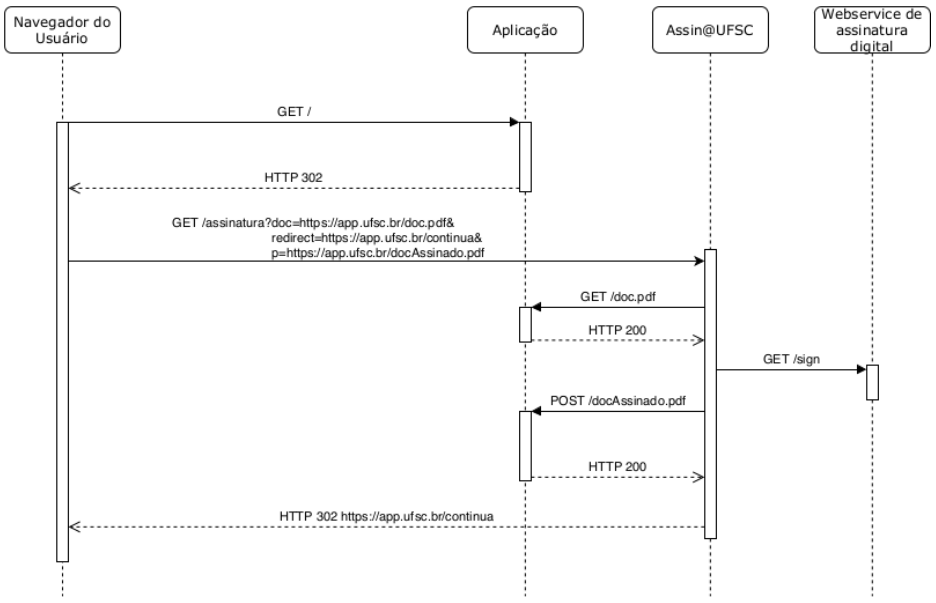

Fig. 5. Sequência de integração do Assina com sistemas externos

6. Reconhecimento da Instituição

Mesmo com a parte técnica funcionando, foi necessária uma ação junto aos usuários para difundir o uso da solução.

O primeiro passo para a difusão do uso da solução foi ter um respaldo político junto a reitoria da Universidade. Foi articulada a assinatura de uma Portaria Normativa 276/2019/GR, de 18 de setembro de 2019 [16], instituindo e disciplinando o uso de Certificação Digital na Universidade Federal de Santa Catarina, dando assim respaldo para o uso da ICPEdu para trâmites internos à UFSC.

Com respaldo político junto a instituição, foi realizada a divulgação da solução em articulação com o Agência de Comunicação da UFSC. Assim como foi produzido material de apoio e tutoriais disponibilizados no site https://e.ufsc.br.

Paralelamente, foi desenvolvido por intermédio da Coordenadoria de Certificação Digital da UFSC um trabalho de conscientização e divulgação nos diferentes setores da Universidade. Busca-se identificar setores que apresentam grande geração de processos ainda em papel para apresentar a alternativa digital baseada em assinaturas digitais.

Todo esse movimento político, e preparação e adequação de documentação para a comunidade acadêmica viabilizou o sucesso da migração da UFSC para operação 100% digital.

7. Considerações Finais

A adoção e implementação de assinaturas digitais é um processo complexo e lento, pois não é puramente técnico: envolve aprendizado e mudança nos hábitos dos usuários.

Com o Assin@UFSC foi possível suplantar diversas dificuldades que a comunidade acadêmica encontrava para adoção da assinatura digital a baixíssimo custo.

Entretanto, na UFSC agora nos deparamos com o desafio de consolidar, divulgar e modificar os processos atualmente existentes, de forma a torná-los 100% digitais e extinguir o papel.

Em 2020, 19.645 pessoas, entre servidores e alunos, utilizaram plataforma de assinaturas Assin@UFSC para gerar 505.461 assinaturas. Além disso, nota-se, conforme figura 6, a aceleração gradual do número de assinaturas a partir de março de 2020, data em que se iniciou o trabalho remoto na UFSC devido a pandemia.

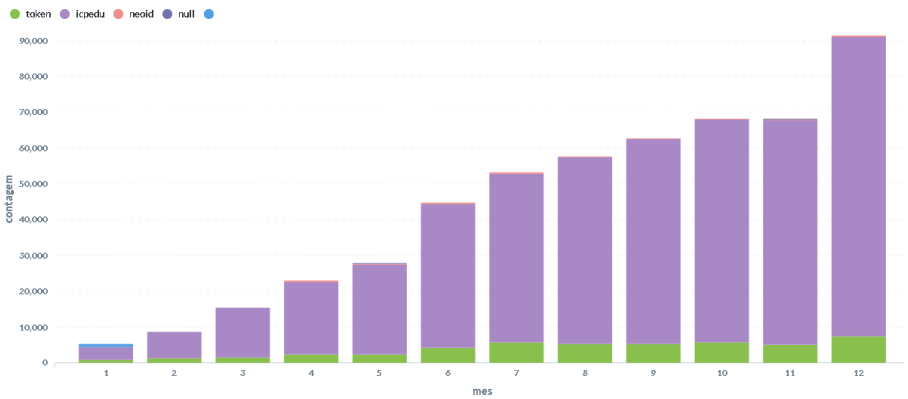

Fig. 6. Número de assinaturas realizadas por mês, e por tipo de certificado

Como trabalho futuro visualizamos:

1. desenvolver um serviço de armazenamento de certificados integrado à CAFe (desvinculado da UFSC), possibilitando qualquer instituição da federação armazenar os certificados pessoais dos seus usuários; e
2. integrar o Assin@UFSC como um serviço da CAFe, permitindo que a federação assine seus documentos na solução.

Agradecimentos

Aos membros da Coordenadoria de Certificação Digital (CCD/UFSC) que difundiram a solução através do desenvolvimento dos documentos, materiais de ensino, treinamentos e suporte a comunidade; do Laboratório de Segurança em Computação (LabSec/UFSC), que germinaram a ideia e nutriram o projeto; e a toda a equipe da SeTIC/UFSC que apoiou e suportou o desenvolvimento do serviço; principalmente aos que investiram seu tempo na concepção, desenvolvimento e execução do projeto: Prof. Ricardo Custódio, Fernando Pereira, Gustavo Zambonin, Douglas Martins, Leonardo Meurer, Bruno Amattos.

Referências

1 Casa Civil. Medida Provisória No 2.200-2, Agosto 2001. http://www.planalto.gov.br/ccivil 03/mpv/antigas 2001/2200-2.htm.

2 Diário Oficial da União. Lei Nº 14.063, Setembro 2020. https://www.in.gov.br/web/dou/-/lei-n-14.063-de-23-de-setembro-de-2020-279185931.

3 ITI. ICP-Brasil, Maio 2021. https://www.iti.gov.br/icp-brasil.

4 RNP. ICPEdu, Maio 2021. https://www.rnp.br/servicos/servicos-avancados/icpedu.

5 RNP. ICPEdu Certificado Pessoal. https://pessoal.icpedu.rnp.br/home.

6 RNP. CAFe, Maio 2021. https://www.rnp.br/servicos/servicos-avancados/cafe.

7 LabSec. Validador de Documentos Assinados, Marc¸o 2021. https://validador.ufsc.br.

8 SeTIC/UFSC. Sistema de Assinatura Digitais, Marc¸o 2021. https://assina.ufsc.br.

9 Adobe. Padrão PKCS7, Março 2021. https://www.adobe.com/devnet-docs/acrobatetk/tools/DigSigDC/standards.html.

10 Mozilla Foundation. Projeto PDF.js, Março 2021. https://mozilla.github.io/pdf.js/.

11 Apache Foundation. Projeto Java PDFBox, Março 2021. https://pdfbox.apache.org/.

12 Projeto Bouncy Castle. Biblioteca de Criptografia, Março 2021. https://www.bouncycastle.org/.

13 The document Foundation. Libre Office, Março 2021. https://www.libreoffice.org/.

14 ETSI. European telecommunications standards institute, Março 2021. https://etsi.org.

15 Casa Civil. Instituto Nacional de Tecnologia da Informaçãao, Março 2021. https://www.iti.gov.br/.

16 UFSC. Portaria Normativa 276/2021/GR, Maio 2021. https://e.ufsc.br.