Usabilidade de Ferramentas para Assinatura Digital de Documentos PDF

Sandro Oliveira[1], **Luciano Vargas**[1], **Rodrigo Mansilha**[1], **Diego Kreutz**[1]

[1] Universidade Federal do Pampa (Unipampa)
{NomeSobrenome}@unipampa.edu.br

Resumo. *Neste trabalho investigamos questões de usabilidade em seis ferramentas que viabilizam assinatura digital de documentos PDF. Como um passo nesta direção, realizamos um estudo empírico com usuários digitalmente proficientes. Os resultados indicam que ainda temos um caminho pela frente quando consideramos usabilidade no contexto de assinaturas digitais.*

1. Introdução

A Lei nº 14.063/2020[1] dispõe sobre uso no Brasil de assinaturas eletrônicas (que diferem de assinaturas de próprio punho, capturadas por caneta digital ou fotocópia) para provimento de garantias quanto à integridade de dados, à autenticidade (ou integridade de fonte) e ao não-repúdio baseado essencialmente em algoritmos criptográficos (e não em análise de padrão de escrita). Conforme essa lei, as assinaturas eletrônicas podem ser classificadas em três níveis crescentes de segurança: simples, avançada e qualificada.

A assinatura eletrônica simples não requer certificado digital – a identificação é baseada exclusivamente em registros internos à entidade que mantém o sistema. Um exemplo popular de sistema de assinatura simples é o SEI[2], que é instanciado por diversos órgãos governamentais, como a Unipampa e o Superior Tribunal de Justiça. Exemplos comerciais de sistemas que oferecem mecanismos para assinatura eletrônica simples são o ClickSign[3] e DocuSign[3]. Exemplos de registros internos mantidos por sistemas de assinatura simples incluem resumos criptográficos dos documentos (para permitir verificação de integridade de dados), links com *tokens* de autenticação via e-mail, data, hora e IP de origem do acesso (para identificar a fonte).

As assinaturas eletrônicas avançadas e qualificadas requerem o emprego de algum tipo de certificado e verificação documental da identidade do usuário. A assinatura eletrônica avançada permite a utilização de certificados digitais emitidos por entidades independentes da ICP-Brasil, como a CertSign[3]. Já a assinatura eletrônica qualificada exige também que o certificado digital seja qualificado como ICP-Brasil[4], isto é, seja emitido por uma autoridade certificadora com raiz na ICP-Brasil. O ICP-Brasil garante que um determinado conjunto de regras técnicas (e.g., dupla verificação documental da identidade do usuário) sejam rigidamente cumpridas, porém implica em maior custo e compromissos administrativos. Exemplos de serviços que oferecem recursos para assinaturas digitais utilizando certificados ICP-Brasil é o Assinador[5] (da plataforma Gov.br).

[1] http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14063.htm
[2] https://www.gov.br/economia/pt-br/acesso-a-informacao/sei
[3] https://www.clicksign.com/, https://docusign.com/, https://www.certisign.com.br
[4] http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm#art10\%A71
[5] https://assinador.iti.br

Na área de segurança computacional, a assinatura qualificada e a assinatura avançada são classificadas como *assinatura digital*, isto é, realizadas através de um certificado digital. Apesar de a assinatura digital oferecer vantagens significativas em relação à assinatura simples (e à assinatura digitalizada), e estar no mercado há mais de 15 anos, sua adoção ainda é restrita[6]. Acreditamos que a adoção da assinatura digital é limitada por diversos fatores sociais incluindo aspectos econômicos, culturais e políticos, e também tecnológicos, como *usabilidade*. De fato, no passado, alguns estudos destacaram questões de usabilidade (e.g., complexidade de gestão), em diferentes níveis e componentes, como limitadores para a ampla adoção de certificados emitidos por ICPs [Lopez et al., 2005, Bühler et al., 2014].

Para dar um exemplo prático de questões de usabilidade, que observamos empiricamente, em 2010 foi implantado o uso de assinatura digital qualificada na Unipampa. Na época, o processo de emissão dos *tokens*, contendo os certificados digitais, era exclusivamente de forma presencial, ou seja, além dos custos de emissão dos certificados, ainda havia a questão de o processo ser presencial. Um segundo aspecto observado durante os anos de implantação e utilização das assinaturas digitais na instituição estava relacionado às questões culturais (e.g., mudança de paradigma do tradicional papel para o digital) e dificuldades técnicas de utilização dos *tokens* (e.g., *drivers* funcionavam apenas no Windows) e ferramentas de assinatura digital, que eram escassas.

Do ponto de vista tecnológico, a usabilidade dos sistemas de emissão de certificados digitais tem melhorado, passando de um processo que exigia procedimentos presenciais para algo integralmente online. No caso do ICPEdu, por exemplo, um usuário da Federação CAFé[7] (*e.g.*, aluno ou servidor de uma universidade) pode acessar o portal ICPEdu e, através de suas credenciais institucionais, gerar o certificado digital em poucos minutos. Isso simplifica o processo e melhora a usabilidade. Entretanto, no caso de certificados ICP-Brasil, apesar de termos evoluído de um processo presencial para um online, ainda há aspectos a serem observados com relação a emissão dos certificados. Atualmente, as autoridades certificadoras oferecem um grande leque de opções de certificados com diferentes atributos técnicos e compromissos de custo/benefício. Sabe-se que a disponibilização excessiva de opções é, em geral, desvantajoso pois a etapa decisória atrasa o processo como um todo, quando não o cancela. Por exemplo, a CertSign[8] oferece atualmente 20 opções de certificados digitais, que podem suscitar dúvidas como: qual é a opção mais segura? Qual opção oferece melhor relação custo/benefício para a minha tarefa? Qual alternativa oferece maior compatibilidade com serviços como a declaração de imposto da Receita Federal?

Algumas entidades certificadoras têm procurado reduzir o número de opções, restringindo certas alternativas à determinados mercados. Por exemplo, a Serasa Experian[9] oferece apenas quatro opções, que são mais simples e mais facilmente diferenciáveis de certificados para os usuários finais que as 20 opções do CertSign. Apesar de aperfeiçoamentos como esses, acreditamos que ainda há um longo caminho a ser percorrido até chegarmos em situação de ampla adoção de assinatura digital.

---

[6] https://blog.qualisign.com.br/wp-content/uploads/2020/08/Revista-Assinatura-Digital-2.a-edicao-2017-v2.pdf

[7] https://www.rnp.br/en/servicos/gestores-de-ti/cafe

[8] https://loja.certisign.com.br

[9] https://serasa.certificadodigital.com.br/

O objetivo geral deste trabalho é *caracterizar preliminarmente fatores tecnológicos que eventualmente possam estar atrasando a expansão da adoção de assinaturas digitais para elencar oportunidades de melhorias rumo à ampla adoção de assinatura digital*. Especificamente, este trabalho apresenta as seguintes contribuições: (a) uma análise comparativa de 6 (seis) ferramentas que permitem a assinatura e verificação de assinaturas; e (b) um estudo baseado em questionário sobre impressões dos usuários sobre o processo de assinatura digital.

O restante deste trabalho está organizado como segue. Na Seção 2 introduzimos a metodologia e os resultados do estudo realizado. Por fim, na Seção 3 apresentamos as considerações finais e perspectivas de trabalhos futuros. É importante destacar também que discussões e dados complementares (e.g., sobre nuvens de certificados e plataformas de assinatura online) podem ser vistas na versão estendida do trabalho [Lemos et al., 2021].

2. Usabilidade de Assinatura Digital Centrada no Usuário

Na sequência, apresentamos um levantamento de dados e discussões acerca de algumas das principais ferramentas que permitem assinaturas digitais centradas no usuário, isto é, onde o certificado digital fica exclusivamente em posse do usuário e não armazenado e gerenciado em uma nuvem, como é o caso do Assinador e do Assina@UFSC, por exemplo (mais detalhes em [Lemos et al., 2021]). Nosso objetivo é identificar questões de usabilidade e limitações técnicas que podem levar a novos *insights* para a construção de um ecossistema de ferramentas mais amigáveis para assinatura digital de documentos PDF.

2.1. Metodologia

A nossa primeira avaliação de usabilidade das ferramentas para assinatura digital de documentos PDF foi dividida em duas etapas. Na primeira etapa, realizamos um estudo exploratório das ferramentas que permitem a realização de assinaturas digitais a partir de certificados ICPEdu.

Com a participação dos co-autores do trabalho e mais de 15 estudantes da disciplina de Tópicos em Segurança de Sistemas e da Informação dos cursos de Ciência da Computação e Engenharia de Software da Unipampa, elencamos 6 (seis) ferramentas voltadas para computador pessoal: Okular, Wondershare PDFElement, Foxit Reader, PDF Xchange, Adobe Acrobat e Libre Office.

Na segunda etapa, organizamos um teste do tipo validação/verificação através de tarefas [Rubin et al., 2011] e uma avaliação participativa [Muller et al., 1997]. A avaliação foi realizada com um grupo de usuários da Unipampa, incluindo alunos dos cursos de Ciência da Computação e Engenharia de Software, analistas e técnicos de tecnologia da informação e auxiliares administrativos da área de tecnologia.

O objetivo da avaliação foi observar questões de usabilidade sobre (a) a geração de certificados digitais ICPEdu Pessoal, (b) a utilização das ferramentas previamente selecionadas para assinatura digital e (c) a verificação das assinaturas digitais. Durante a avaliação, procuramos observar de forma empírica alguns dos princípios de usabilidade [Nielsen, 1994] como: (a) *facilidade de aprendizado* através da observação de quanto tempo e esforço foi necessário para gerar o certificado e assinar digitalmente um documento PDF; (b) *eficiência* na assinatura e na verificação de assinaturas em documentos

PDF; e (c) *satisfação do usuário* observando a experiência de uso, identificando o quão difícil foi gerar e usar o certificado em determinada ferramenta.

Inicialmente, estruturamos a avaliação em 11 perguntas[10] envolvendo duas tarefas, a geração do certificado ICPEdu e a utilização do certificado para assinar um documento. Para cada tarefa, relacionamos diferentes questões para entender a percepção do usuário sobre cada um dos processos. As questões foram aplicadas de forma online e assíncrona, com e-mail de instruções. Para cada participante, foram selecionadas duas ferramentas para avaliação.

Num segundo momento, realizamos uma chamada síncrona com os participantes do questionário, para fazer a analise colaborativa e coletar impressões, obter *feedback* adicional e discutir os resultados. Durante o momento síncrono, também aplicamos o SUS (*System Usability Scale*) [Brooke et al., 1996] por ser um questionário simples, de rápida aplicação, e com boa confiabilidade [Bangor et al., 2008]. O SUS é um instrumento de pesquisa que contém dez questões em escala Linkert[11] que visam medir a usabilidade de produtos, avaliando a satisfação do usuário em relação ao mesmo. Utilizamos a versão em português [Martins et al., 2015] substituindo a palavra produto por sistema, tornando possível uma comparação com os resultado do questionário que aplicamos anteriormente.

2.2. Resultados

Ao total, obtivemos respostas de 18 participantes. A proficiência digital dos respondentes foi alta, com média de 4,5 (de 5) pontos. A maioria dos participantes (79%) afirmou que sabe diferenciar entre assinatura simples e qualificada. Além disso, 90% dos participantes informou que já tinha assinado digitalmente algum documento. *Com base nisso, concluímos que o nível de conhecimento sobre o tema do grupo entrevistado pode ser caracterizado entre intermediário e avançado.*

Na emissão do certificado ICPEdu, primeira tarefa, perguntamos quanto tempo o usuário gastou no processo. Os resultados são apresentados na Figura 1.

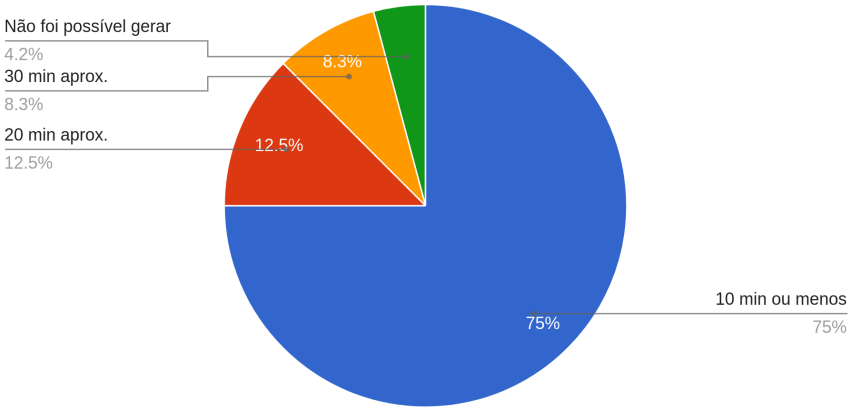

Figura 1. Tempo para criar o certificado

Podemos observar que 75% dos participantes levou 10 minutos ou menos para emitir um certificado ICPEdu. Entretanto, é interessante observar que 25% necessitou

[10] Formulário disponível online em `https://bit.ly/3AoX1ah`.
[11] `https://psycnet.apa.org/record/1933-01885-001`

mais de 10 minutos ou não conseguiu emitir o certificado (e.g., problemas para identificar a instituição ou credenciais). *Acreditamos que esse seja um dado preocupante em termos de usabilidade, especialmente considerando que trata-se de um grupo de pessoas com alta proficiência digital.*

O nível de dificuldade na geração do certificado foi considerado entre fácil a muito fácil pelos entrevistados. Combinado com a análise colaborativa síncrona, realizada após a aplicação do formulário, a maioria dos participantes considerou que o processo de geração do certificado no site do ICPEdu Pessoal[12] não apresenta dificuldades técnicas.

Com relação às ferramentas de assinatura de PDF, os entrevistados informaram que não encontraram dificuldades técnicas na instalação. Entretanto, na segunda tarefa, que consistiu na utilização do certificado para assinar digitalmente um documento PDF, um percentual significativo (43%, como pode ser visto na Figura 2), levou mais de 20 minutos para assinar o documento ou não conseguiu assinar. Corroborando, metade dos respondentes informou que teve que recorrer a manuais das ferramentas para assinar digitalmente o documento. Considerando que os participantes são digitalmente proficientes, podemos inferir que as ferramentas ainda pecam em termos de usabilidade. Usuários leigos, acostumados a aplicativos de dispositivos móveis que não necessitam de manuais, muito provavelmente serão desestimulados a utilizar ferramentas pouco intuitivas como essas. *Acreditamos que as ferramentas ainda precisam evoluir em termos de usabilidade de forma a impulsionar o ecossistema das assinaturas digitais.*

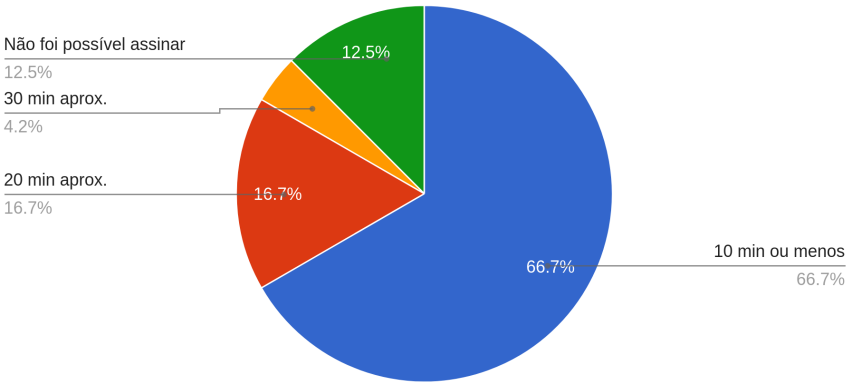

Figura 2. Tempo para assinar o PDF

Para o experimento com SUS, realizado de forma síncrona, tivemos 9 participantes. A mediana para cada uma das dez perguntas ficou em: 4, 3, 3, 1, 2, 2, 2, 3, 3, 2. Isto resulta em um índice SUS de 62,5 (somatório da mediana multiplicado por 2,5). Analisando a mediana dos resultado SUS de cada respondente temos um índice de 57,5. Segundo a classificação de usabilidade sugerida por [Bangor et al., 2009], temos um boa usabilidade para um grupo de usuários digitalmente proficientes, que quando comparada com o resultados do questionário é bastante compatível.

Considerando os participantes da pesquisa, realizamos também um terceiro experimento, utilizando 4 arquivos assinados digitalmente, entre os quais 2 dos arquivos estavam assinados com certificados ICPEdu revogados. Neste experimento observamos que nenhuma das ferramentas auxiliou os participantes a identificar que dois dos documentos

[12] `https://pessoal.icpedu.rnp.br`

estavam assinados com certificados revogados. Para verificar se o certificado ainda é válido, as listas de certificados revogados da raiz ICPEdu deveriam ser carregadas (manual ou automaticamente) pelas ferramentas. *Embora a amostra seja pequena, acreditamos que o resultado seja relevante considerando a importância dessa funcionalidade para o ecossistema de assinaturas eletrônicas avançadas ou qualificadas. Isso indica que há desafios e oportunidades a serem explorados nesse aspecto.*

3. Considerações Finais

Os resultados permitem concluir que ainda há diversas oportunidades de melhoria em ferramentas para assinatura digital de documentos PDF, incluindo Okular, Wondershare PDFElement, Foxit Reader, PDF Xchange, Adobe Acrobat e Libre Office. Com base nos dados levantados, concluímos que nenhuma dessas ferramentas é suficientemente intuitiva a ponto de apresentar uma boa usabilidade para usuários que não sejam digitalmente proficientes.

Ferramentas como a PDF Xchange se destacam das demais, entretanto, são comerciais e funcionam exclusivamente em ambientes Windows. As opções em ambientes Linux são limitadas, como o Okular, cuja versão que suporta assinaturas digitais está disponível, hoje, apenas em algumas distribuições, e o Libre Office utiliza o Draw para assinar digitalmente documentos, isto é, uma ferramenta pouco conhecida. Além disso, a importação dos certificados em ambientes Linux exige (em alguns casos) instalação de software adicional, o que dificulta o processo para usuários digitalmente pouco fluentes.

Como trabalhos futuros vislumbramos: (a) ampliar a quantidade e diversidade do público entrevistado; (b) analisar em profundidade plataformas online como o Assina@UFSC e o Assinador Gov.br; (c) investigar aplicativos para dispositivos móveis, cuja grande maioria informa a finalidade assinatura digital no próprio nome, entretanto, na verdade, oferecem majoritariamente apenas a opção de assinaturas digitalizadas.

Referências

Bangor, A., Kortum, P., and Miller, J. (2009). Determining what individual sus scores mean: Adding an adjective rating scale. *Journal of usability studies*, 4(3):114–123.

Bangor, A., Kortum, P. T., and Miller, J. T. (2008). An empirical evaluation of the system usability scale. *Intl. Journal of Human–Computer Interaction*, 24(6):574–594.

Brooke, J. et al. (1996). SUS-a quick and dirty usability scale. *Usability evaluation in industry*, 189:4–7.

Bühler, G., Entschew, E., and Selhorst, M. (2014). Security versus usability–user-friendly qualified signatures based on German ID cards. In *Securing Electronic Business Processes*, pages 94–105. Springer.

Lemos, S., Vargas, L., Mansilha, R., and Kreutz, D. (2021). Assinatura digital em documentos PDF (versão estendida). `https://arxiv.kreutz.xyz/wrseg2021_assina_PDF_ve1.pdf`.

Lopez, J., Oppliger, R., and Pernul, G. (2005). Why have public key infrastructures failed so far? *Internet Research*.

Martins, A. I., Rosa, A. F., Queirós, A., Silva, A., and Rocha, N. P. (2015). European portuguese validation of the system usability scale (SUS). *Procedia Computer Science*, 67:293–300.

Muller, M. J., Haslwanter, J. H., and Dayton, T. (1997). Participatory practices in the software lifecycle. In *Handbook of human-computer interaction*, pages 255–297. Elsevier.

Nielsen, J. (1994). *Usability engineering*. Morgan Kaufmann.

Rubin, J., Chisnell, D., and Spool, J. (2011). *Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests*. Wiley.