MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO

Tutorial de emissão de certificados pessoais pelo ICPEdu e Assinatura de documentos na UFERSA

Mossoró/2020

Versão 1.0

ADMINISTRAÇÃO

Reitor
Prof. José de Arimatea de Matos

Vice-Reitor
Prof. José Domingues Fontenele Neto

Chefe de Gabinete
Prof. Felipe de Azevedo Silva Ribeiro

Pró-Reitor de Administração
Jorge Luiz de Oliveira Cunha

Pró-Reitora de Assuntos Estudantis
Prof.ª Vânia Christina Nascimento Porto

Pró-Reitor de Extensão e Cultura
Prof. Dr. Sílvio Roberto Fernandes de Araújo

Pró-Reitor de Graduação
Prof. Rodrigo Nogueira de Codes

Pró-Reitor de Pesquisa e Pós-Graduação
Prof. Daniel Valadão Silva

Pró-Reitor de Planejamento
Prof. Álvaro Fabiano Pereira de Macêdo

Pró-Reitora de Gestão de Pessoas
Prof. Alexandre José de Oliveira

Superintendente de Infraestrutura
Cleyton Kleber Dantas Alberto

Superintendente de Tecnologia, da Informação e Comunicação
Marcos Tullyo Campos

Elaboração e manutenção deste documento

Divisão de Segurança da Informação
Kleber Jacinto

Assinado digitalmente por KLEBER JACINTO:96963700400
DN: CN=KLEBER JACINTO: 96963700400, OU=UFERSA - Universidade Federal Rural do Semi-Arido, O=ICPEdu, C=BR
Localização: Mossoró, RN - Brasil
Data: 2020-07-19 01:01:02
Foxit Reader Versão: 9.7.1

Sugestões, reclamações e pedido e informações: DSI@ufersa.edu.br

Sumário

Preâmbulo

O uso de ferramentas computacionais para dar suporte às atividades humanas tornou-se fato cotidiano em especial naquelas atividades que demandam armazenamento e manipulação de dados, inclusive os atos e processos administrativos. As instituições movimentam-se para oficializar/legalizar estas ferramentas e agregá-las à rotina de suas atividades.

No caso da UFERSA, o planejamento e a execução adoção da digitalização de processo e diminuição gradual de documentos físicos vem ocorrendo desde a implantação dos SIGs (SIPAC, SIGAA, SIGRH) há quase 10 anos, onde processos como matrículas, gestão de diários de classe, emissão de memorandos, aquisições e gestão de materiais, pouco a pouco vem saindo das mesas e migrando para as telas. O passo mais ressente é a aprovação da Resolução CONSAD/UFERSA nº 003/2020, de 07/07/2020, que dispõe sobre o processo administrativo eletrônico no âmbito da Universidade Federal Rural do Semi-árido (UFERSA) e estabelece os parâmetros para sua implementação, funcionamento e uso.

Um dos pontos importantes dessa resolução é a possibilidade de aceite de documentos em formatos digitais, desde que se possa identificar de forma inequívoca de quem ou de onde veio o documento. Neste ponto torna-se importante o conceito de assinatura digital ou certificado digital.

A segurança da informação é fundamentada em alguns pilares dentre os mais importantes são a disponibilidade (uma informação deve estar sempre disponível mediante a necessidade de seu uso), a confidencialidade (uma informação deve estar disponível apenas para as pessoas que tem permissão de acesso às mesmas) e a Integridade (é possível definir quem gerou a informação e se ela não foi alterada indevidamente). O uso dos certificados digitais visa atuar nos dois últimos pilares.

Quanto à confidencialidade os certificados digitais podem ser utilizados para proteger documentos, mensagens e comunicações através de diversas técnicas de criptografia, que em palavras simples é a proteção da informação por um embaralhamento de seu conteúdo de forma que a informação se torna ilegível para aqueles que não possuem o certificado.

Quanto à integridade, os certificados possibilitam identificar de forma inequívoca o emissor daquele documento ou mensagem, quando foi gerada a informação e identificar se houve adulteração de seu conteúdo desde o momento em que ele foi criado. Esta última característica tende a ser mais amplamente utilizada e no momento atual de excepcionalidade decorrente da Pandemia do COVID-19, tornou-se ferramenta importante que motivou a SUTIC a buscar uma solução que pudesse permitir seu uso pela instituição à luz da Legalidade e das recentes normas aprovadas.

A solução então foi utilizar a estrutura do projeto ICPEdu (Infraestrutura de Chaves Públicas para Ensino e Pesquisa), projeto criado pela RNP (Rede Nacional de Pesquisa) em 2004 e que se tornou disponível recentemente para as instituições de ensino atendidas pela RNP e tem por finalidade a manutenção de uma infraestrutura de criação de certificados digitais e chaves de segurança dentro do ambiente das Instituições Federais de Ensino Superior (IFES) e Unidades de Pesquisa (UPs).

Mas efetivamente, o que é o certificado digital? É um arquivo que contém dados criptografados e que somente pode ser acessível através de uma senha única, pessoal e intransferível fornecida no ato da criação do certificado. Este arquivo e esta senha devem ser guardados com o máximo de cuidado, pois uma vez perdidos permite que terceiros possam passar-se pelo proprietário do certificado.

No caso do ICPEdu, a RNP faz o papel de mantenedor da infraestrutura e principalmente atua como a Autoridade Certificadora Raiz (AC Raiz), responsável por credenciar as Autoridades Certificadoras Intermediárias (IFES e UPs), que permitem que seus usuários possam emitir seus certificados individuais. Esta relação Pessoa-Instituição-RNP estabelece uma cadeia de confiança na emissão e reconhecimento do certificado, o que permite que estes certificados possam ser usados para assinar documentos digitalmente. Todas as Universidades, Institutos e Unidades de Pesquisa Federais estão aderindo a esta ferramenta, pela confiabilidade, gratuidade e universalidade (os alunos também têm acesso aos certificados).

Uma informação é essencial sobre o ICPEdu é que, até o momento da emissão deste documento, seu reconhecimento é limitado. Isso não implica em fragilidade, não implica em falta de legalidade, não implicada em impossibilidade de uso. Não é um certificado sugerido para toda e qualquer operação, mas que para assinatura de documentos institucionais, dentro do contexto das atividades meio e fim da instituição são totalmente aplicáveis. Ao não ser amplamente reconhecido alguns aplicativos podem emitir mensagens de alertas que avisam quanto ao fato da Certificadora Raiz não ser reconhecida. Esta mensagem é informativa, não uma mensagem de erro. O certificado funcionará perfeitamente apesar dele.

Neste cenário, os certificados ICPEdu podem ser utilizados para assinar documentos. mas que documentos? Em tese qualquer arquivo digital pode ser assinado mas para fins de universalidade e manutenção da integridade o coerente é que seja um formato que aceite a assinatura digital, que seja de difícil adulteração e que possa ser legível em muitos dispositivos, sistemas operacionais, e o formato padrão para estas ações é o PDF (*Portable Document Format*).

Além destas informações prestadas, que obviamente não cobrem todo o assunto, mas serve de introdução ao uso dos certificados, o objetivo maior deste pequeno manual é fornecer de forma simplificada um passo a passo de como gerar os certificados e de como utilizá-los para assinar documentos institucionais.

Além deste tutorial, o próprio ICPEdu possui instruções detalhadas de várias operações possível na própria página do serviço, nas abas “Ajuda” e “Sobre”.

Emissão do ICPEdu - certificado pessoal

1) Acessar o serviço e clicar em umas das três opções destacadas;

https://pessoal.icpedu.rnp.br/home

Figura 01 – Tela inicial padrão do serviço de emissão do ICPEdu

2) Buscar a UFERSA na lista de instituições (pode ser digitada a sigla) e clicar em "Prosseguir";

Figura 02 – Seleção da UFERSA dentre as Instituições

3) Entrar com nome e senha. Estes dados são os mesmos que você usa para acessar os SIGs (SIGAA, SIPAC, SIGRH) e clicar em “Login”. Não é necessário marcar nenhuma outra opção;

Figura 03 – Fornecimento de credenciais para acessar o ICPEdu

4) Conformação de envio de dados privados das bases de dados da UFERSA para o ICPEdu; sugere-se manter as opções padrão e clicar em “Accept”. Clicar em “Reject” significa que você não concorda com o procedimento e o processo será interrompido;

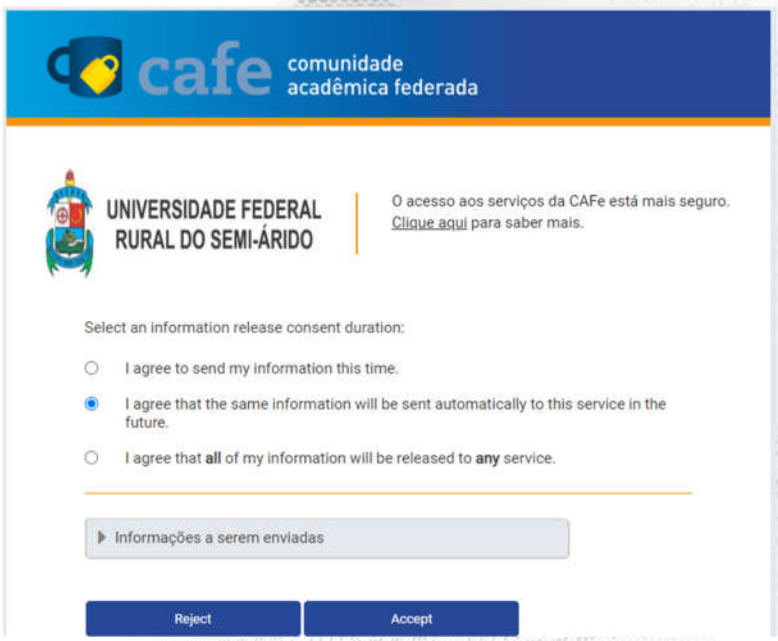

Figura 04 – Confirmação de envio de dados

5) Se tudo foi feito corretamente até aqui, no canto superior direito na página estarão seu nome e a sigla da Instituição. A emissão do certificado inicia-se clicando em “Emitir Certificado Pessoal”;

Figura 05 – Página principal do Serviço

6) A página seguinte pede para que se confirme seus dados pessoais. Caso haja dados incorretos deve-se encaminhar e-mail para dsi@ufersa.edu.br (divisão de Segurança da Informação) informando acerca da inconsistência. A confirmação de concretiza ao clicar em “Confirmar dados”;

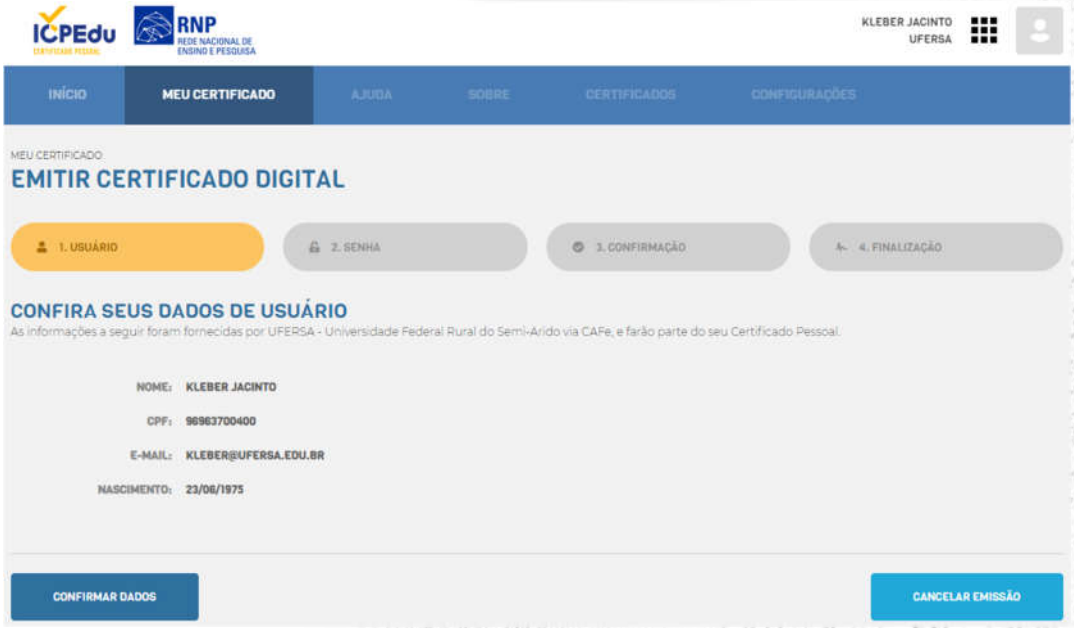

Figura 06 – Confirmação de dados pessoais

7) Neste momento deve ser fornecida uma senha e algo que possa lembrá-lo da senha em caso de esquecimento. Não é possível recuperar a senha em caso de perda, por isso a necessidade do lembrete. Sem a senha o certificado torna-se inutilizável. LEMBRE-SE: Senhas são pessoais e intransferíveis; uso de senhas de terceiros implicam em responsabilização perante as leis vigentes no país (em especial artigos 154-A e 307 do código penal). A senha deve ser confirmada e deve conter no mínimo 8 caracteres, dentre eles pelo menos um número, uma letra maiúscula, uma letra minúscula e um caractere especial, por exemplo: !@#$%¨&*()_+{}][; Evite escrever a senha, seja em papel, seja em e-mail ou outro meio eletrônico. Somente após fornecer senha, repeti-la e incluir o lembrete, a opção “confirmar senha” tornar-se-á disponível.

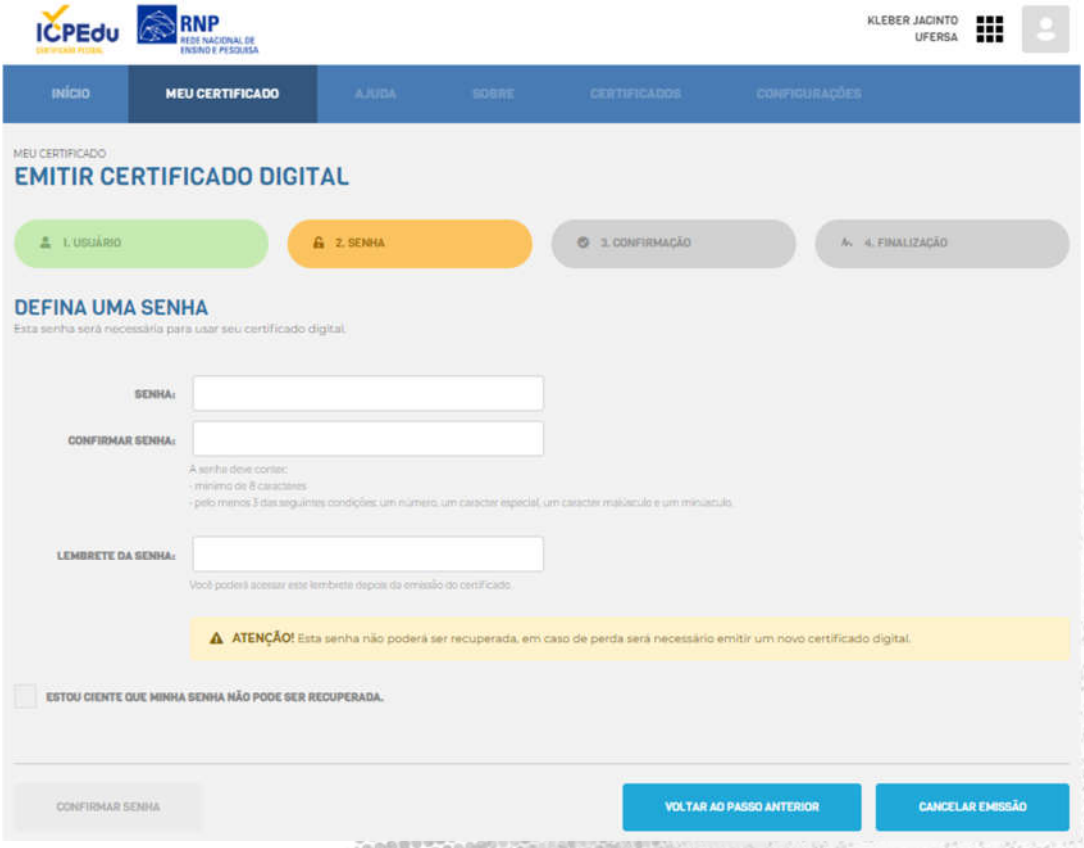

Figura 07 – Fornecimento de senha

8) A página seguinte solicita nova conformação de seus dados e também da instituição clicando em “Emitir Certificado Digital”;

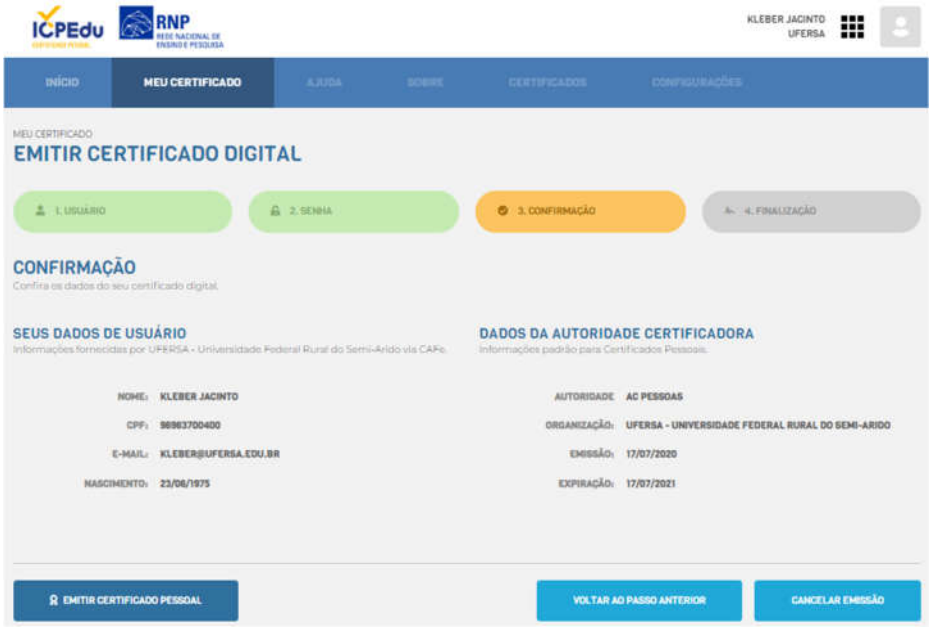

Figura 08 – Confirmação e emissão dos dados

9) Seu certificado foi gerado!!! Você precisa marcar a opção “declaro que guardarei o arquivo do certificado em local seguro” para que a opção “download do certificado digital” esteja disponível. Ao clicar nesta última será baixado um arquivo com o formato “SEU_NOME_SEUCPF-certificate.p12”. Este é o arquivo do seu certificado.

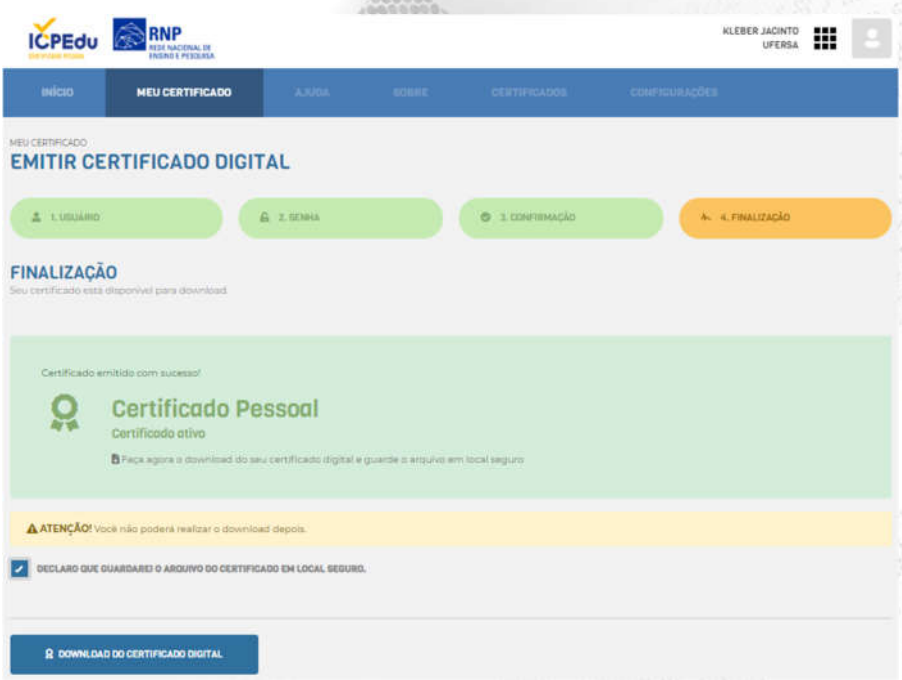

Figura 09 – Download do Certificado

Observações:

1. Se você já emitiu um certificado e tentar emitir um novo receberá um aviso de que já possui um certificado e que o anterior será revogado.

Figura 10 – Aviso de revogação de certificados

2. A revogação de um certificado não invalida os documentos anteriormente assinados com aquele certificado;
3. Perdida a senha não há como recuperá-la um novo certificado deve ser emitido.

Assinatura de Documentos

A Assinatura de Documentos deve ser realizada por software capazes de ler PDFs, existe diversos disponíveis, mas a SUTIC recomendará duas ferramentas, o Acrobat Reader® e o FoxIt Reader®, ambos gratuitos e que permitem o uso do certificado. Eles podem ser encontrados em:

https://get.adobe.com/br/reader/

https://www.foxitsoftware.com/pt-br/downloads/

Este último, possui a vantagem de que também estar acompanhado de uma "impressora virtual" que possibilita a criação de PDF a partir de qualquer aplicativo: basta mandar imprimir com a Impressora do Foxit Reader®. Algumas versões do MS-Office® também possuem a capacidade de "imprimir" seus documentos em formato PDF.

É importantíssimo lembrar que os documentos a serem assinados devem estar em formato PDF

Assinatura com o Acrobat Reader®

1) Abrir o arquivo que se pretende assinar e buscar a Aba Ferramentas:

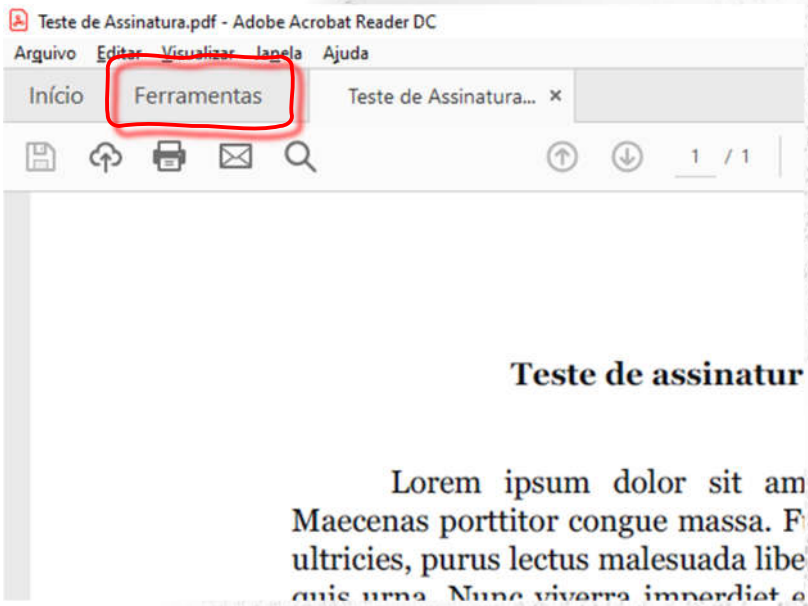

Figura 11 – Abertura do documento e Busca pela aba Ferramentas

2) Na Aba Ferramentas busque a opção Certificados:

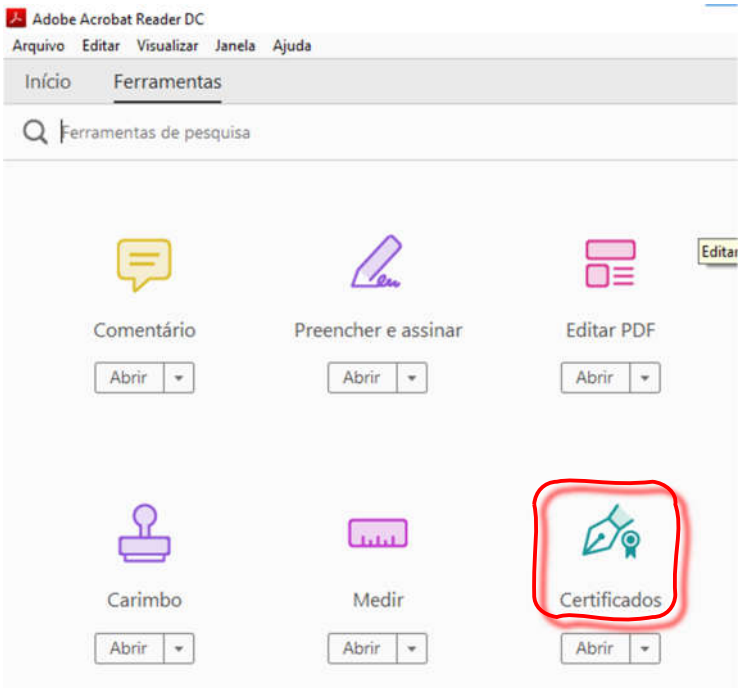

Figura 12 – Escolha da ferramenta “Certificados”

3) Selecionada a ferramenta Certificados, passa a constar na barra de ferramentas um ícone referente aos certificados e na área superior, sobre o texto, a barra de opções da ferramenta certificados

Figura 13 – Detalhes a ferramenta “Certificados” e suas opções

4) Busque a opção “Assinar Digitalmente”.

Figura 13 – Escolha da Opção “Assinar Digitalmente”

5) Você será informado de que deve marcar um retângulo onde será inserida a assinatura. Se esse retângulo for muito pequeno, as informações da assinatura não serão legíveis. Na edição do documento reserve um espaço razoável para a inclusão da assinatura.

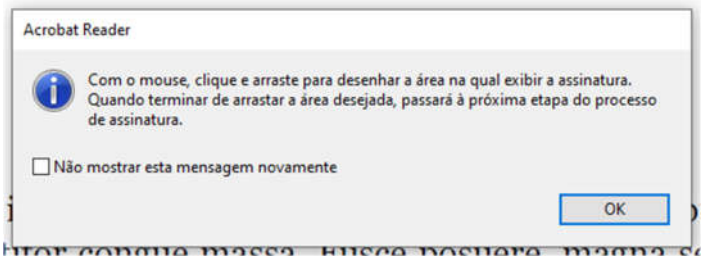

Figura 13 – Caixa de informações sobre a inclusão de retângulo para a assinatura

6) Se for a primeira vez que você vai assinar um documento, o Acrobat Reader vai te convidar a configurar a “ID digital”. Caso contrário você será levado ao passo 10.

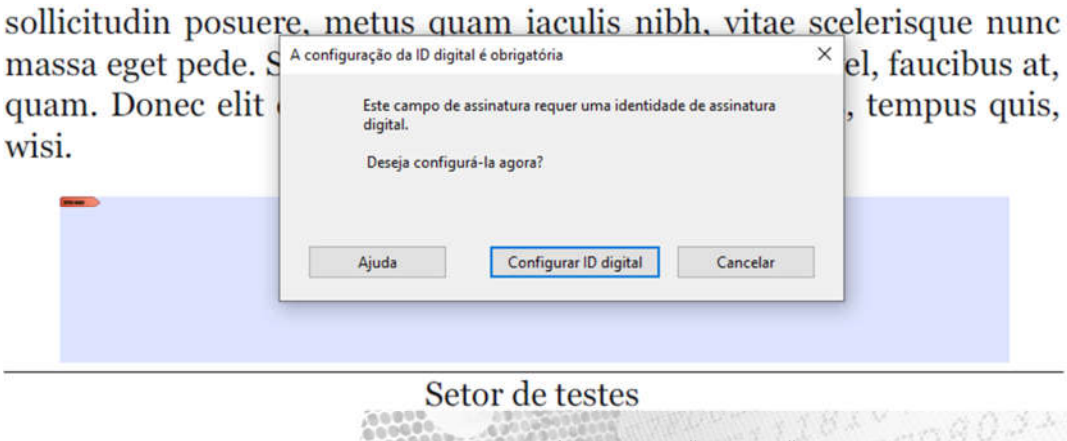

Figura 14 – Alerta para Configuração de “ID digital”

7) Para configurar o ID com certificado você deve selecionar a Segunda opção (Ela não é a opção padrão) e clique em continuar. Por padrão o Acrobat tenta criar uma nova ID, funcionando como Entidade certificadora). Mas como está disponível o arquivo digital, vamos utilizá-lo;

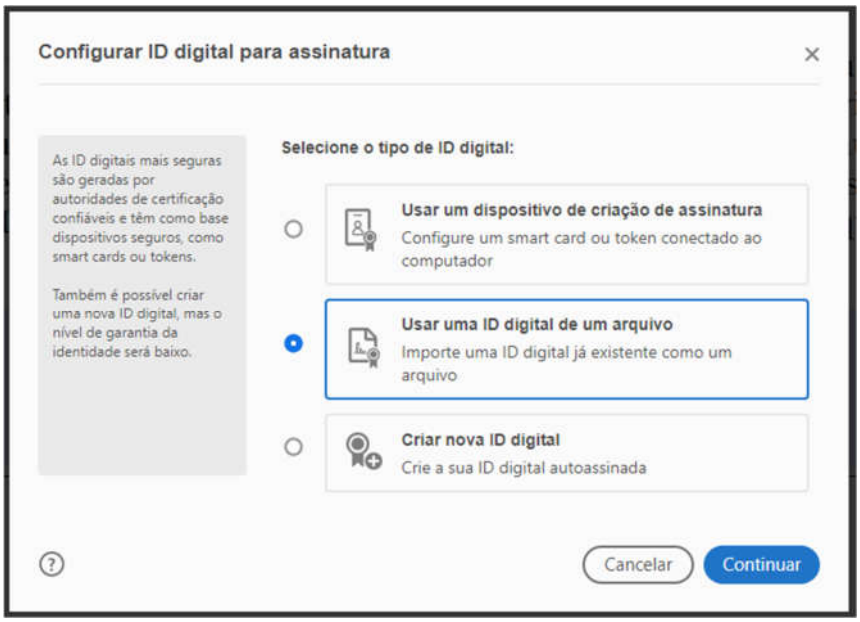

Figura 15 – Opções de criação de ID

8) Use o botão “procurar” para buscar o arquivo p12 que você gerou no ICPEdu e depois insira a mesma senha que você usou para gerar o certificado. Clique em continuar

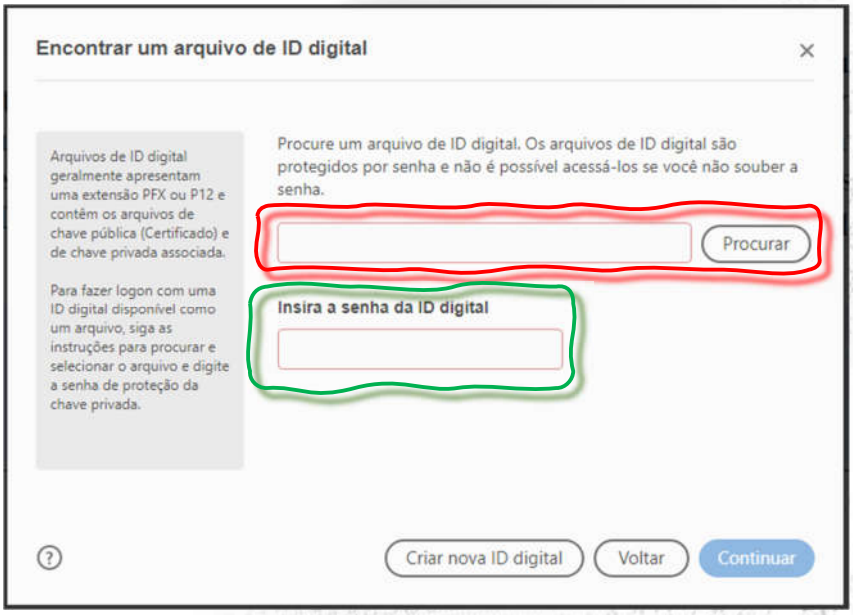

Figura 16 – Seleção do certificado para criação do ID digital

9) O Acrobat informa o sucesso da importação do certificado mostrando os dados pessoais contidos no certificado, os dados do emissões (AC PESSOA SC) e a data de expiração. Clique em continuar.

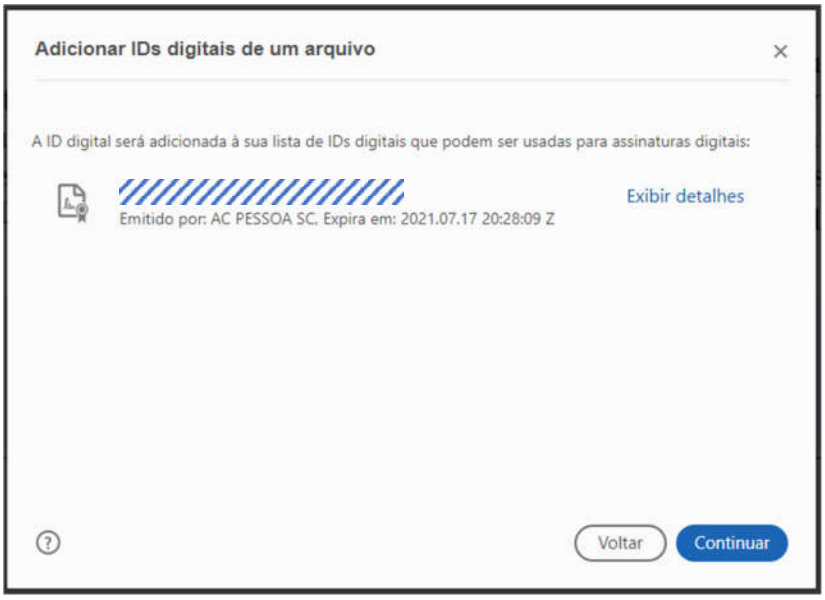

Figura 17 – Detalhes do Certificado que está sendo adicionado

10) Uma vez criada a ID digital, baseada no certificado, você pode selecioná-la para assinar o documento clicando em “continuar”

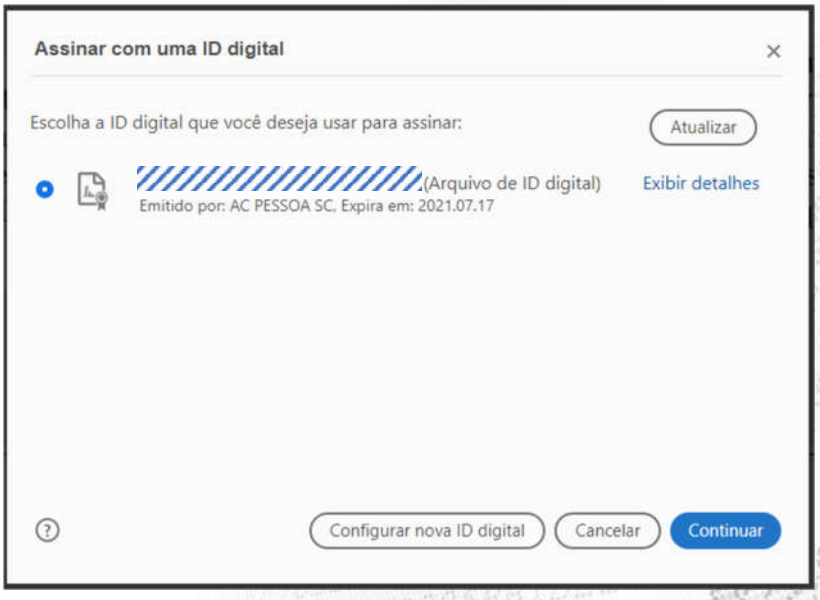

Figura 18 – Detalhes do Certificado que será utilizado para assinar o documento

11) Existem algumas opções de personalização para a assinatura, mas o mais natural é usar o “Texto Padrão”. O botão “assinar” somente estará disponível após a digitação da senha do certificado digital. A Senha SEMPRE será solicitada no ato da assinatura. Uma importante opção é a de “Bloquear o Documento depois de Assinar”. Se esta opção for marcada o arquivo não poderá mais ser alterado. Para documentos que deverão ser assinados por mais de uma pessoa, é importante que apenas a última marque esta opção.

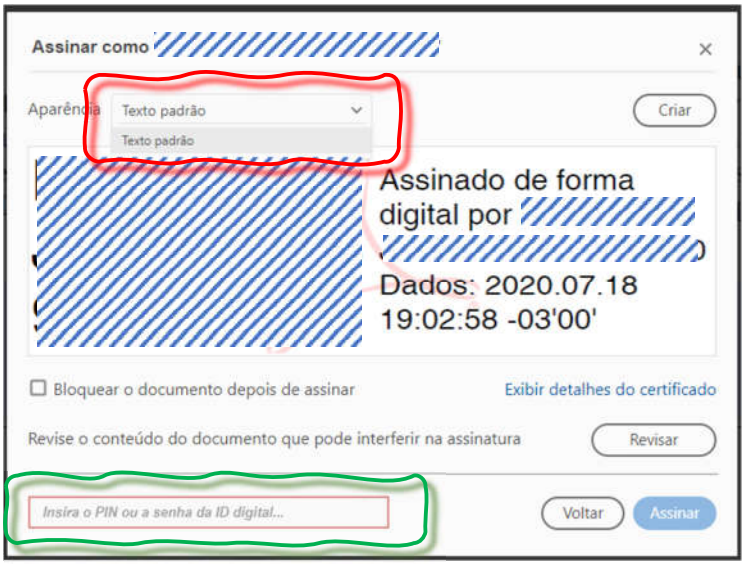

Figura 19 – Detalhes do Certificado que será utilizado para assinar o documento

12) Será pedido para salvar o documento assinado. Uma boa prática é salvar o arquivo com um outro nome (por exemplo, o arquivo original era “declaração.pdf” e o arquivo assinado seria “declaração_assinada.pdf”). Apesar de não ser algo necessário, salvar com outro nome permite identificar de forma inequívoca se o arquivo está ou não assinado e também manter o original por alguma necessidade, por exemplo alterações ou assinatura por mais de uma pessoa. **Uma vez salvo, o documento está assinado.**

13) Uma vez assinado, um aviso pode aparecer. Como dito na sessão introdutória deste tutorial, este aviso não implica em falha na assinatura, mas apenas que a entidade certificadora (o ICPEdu) não é universalmente reconhecida. O simples fato de mostrar o alerta, é uma importante prova de que o arquivo está assinado.

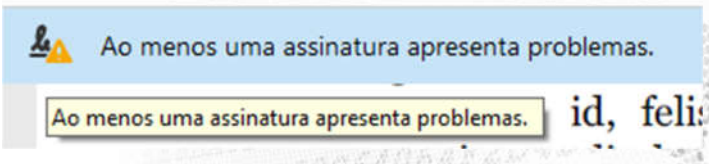

Figura 20 – Alerta de Assinatura

14) Quando o arquivo é aberto por você ou outra pessoa, a mesma mensagem de alerta pode ser exibida. Se for usada a função “Painel de Assinaturas”, será exibida a assinatura

com alerta e os detalhes da assinatura, inclusive a afirmação de que o documento foi ou não alterado após a assinatura e se a data da assinatura é compatível.

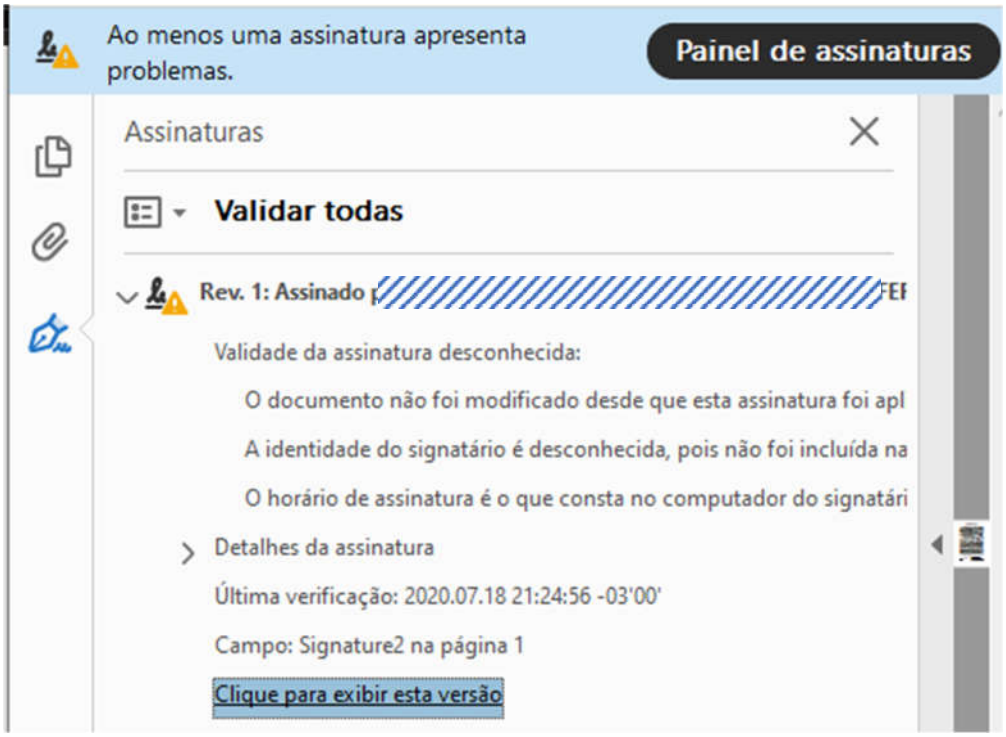

Figura 21 – Detalhes das Assinaturas no documento

Assinando com o FoxIt Reader®

1) Abrir o arquivo que se pretende assinar e buscar a o menu “Proteger”:

2) Se for a primeira vez que você vai assinar um documento, será necessário Configurar seu ID digital clicando na função “IDs Digitais”. Caso contrário siga ao passo 8.

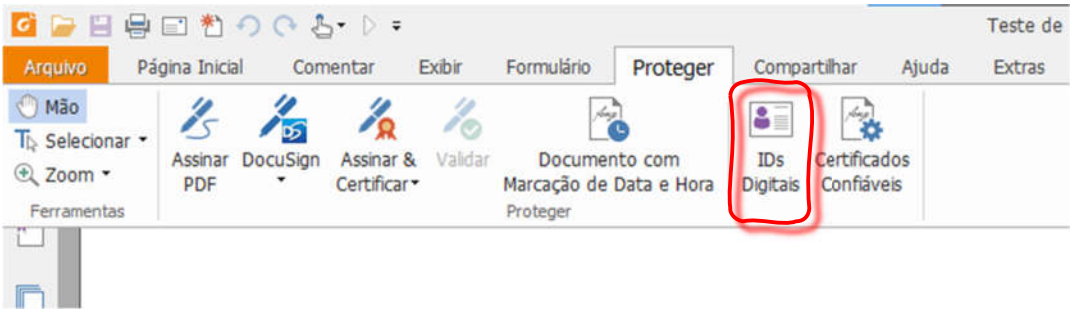

Figura 22 – Menu proteger do Foxit Reader®

3) Você deve selecionar a função “Adicionar ID”, que permitirá a inserção do certificado.

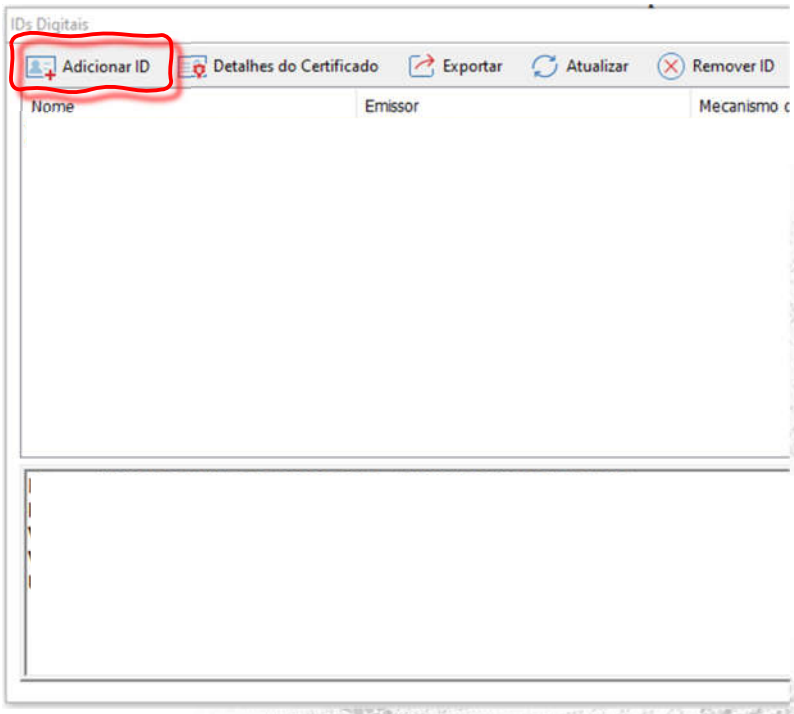

Figura 23 – Tela de gestão de Identidades do aplicativo

4) Para configurar o ID com certificado você deve selecionar a Primeira opção (ela é a opção padrão) e clique em “Próximo”.

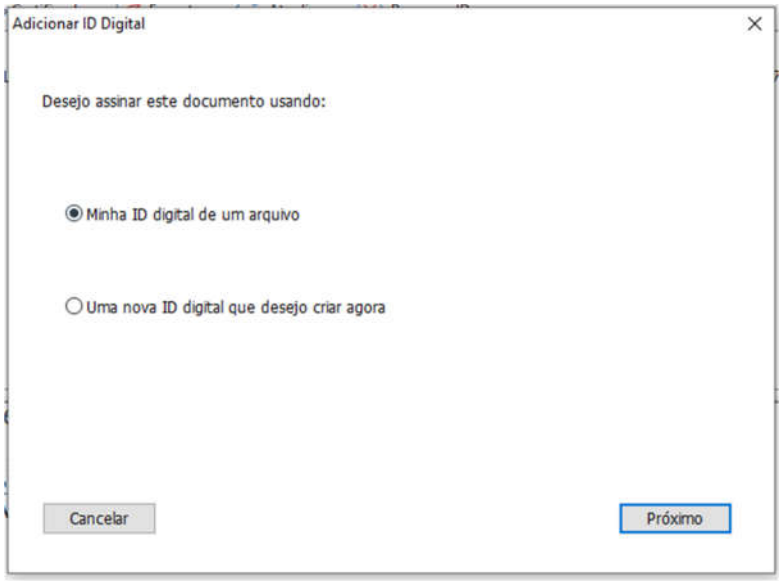

Figura 24 – Painel de seleção de tipo de ID a ser criado

5) Use o botão “procurar” para buscar o arquivo p12 que você gerou no ICPEdu e depois insira a mesma senha que você usou para gerar o certificado. Clique em “Próximo”.

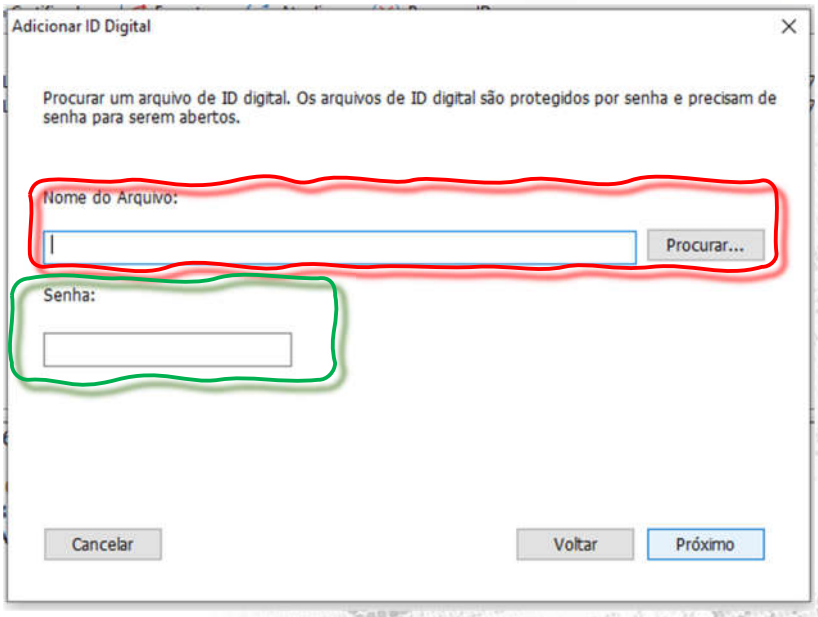

Figura 25 – painel de Escolha de Certificado e inclusão de senha

6) O Foxit informa o sucesso da importação do certificado mostrando os dados pessoais contidos no certificado, os dados do emissões (AC PESSOA SC) e a data de expiração. Clique em continuar.

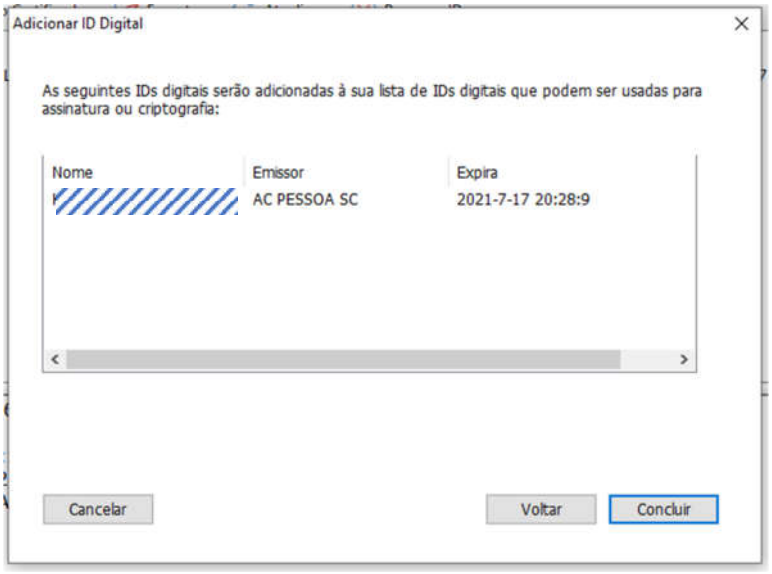

Figura 26 – Confirmação de importação do certificado digital

7) Uma vez criada a ID digital, baseada no certificado, você pode selecioná-la para assinar o documento. Pode fechar esta janela.

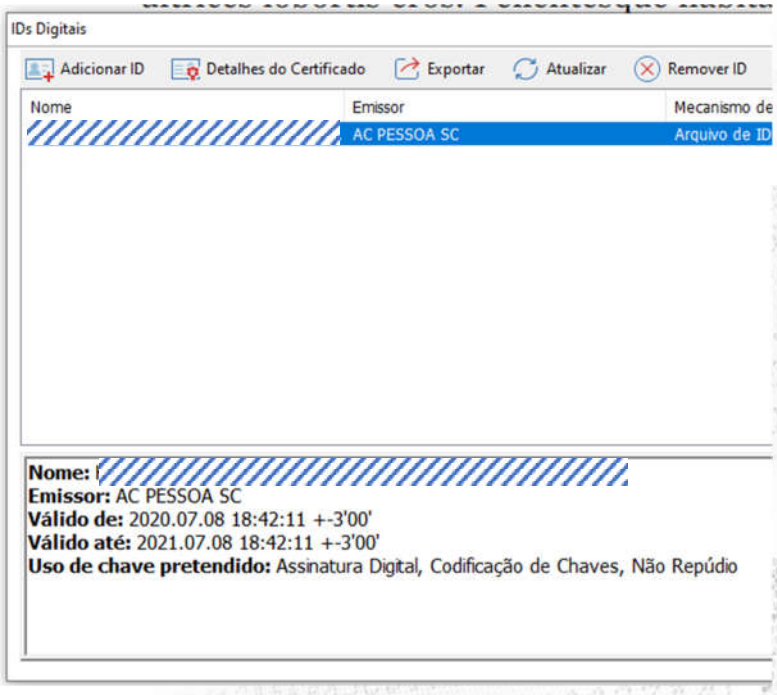

Figura 27 – Painel com Ids disponíveis para assinatura

8) Para assinar o documento vá ao menu “Proteger” e busque a função “Assinar e certificar” e em seguida “Colocar Assinatura”

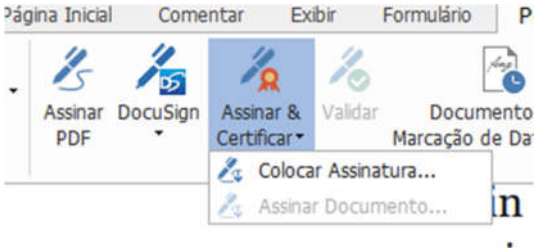

Figura 28 – Detalhe do Menu Proteger com a funcionalidade “Colocar Assinatura”

9) Existem algumas opções de personalização para a assinatura, mas o mais natural é usar o “Estilo Padrão”. O botão “assinar” somente estará disponível após a digitação da senha do certificado digital. A Senha SEMPRE será solicitada no ato da assinatura. Uma importante opção é a de “Bloquear o Documento depois de Assinado”. Se esta opção for marcada o arquivo não poderá mais ser alterado. Para documentos que deverão ser assinados por mais de uma pessoa, é importante que apenas a última marque esta opção.

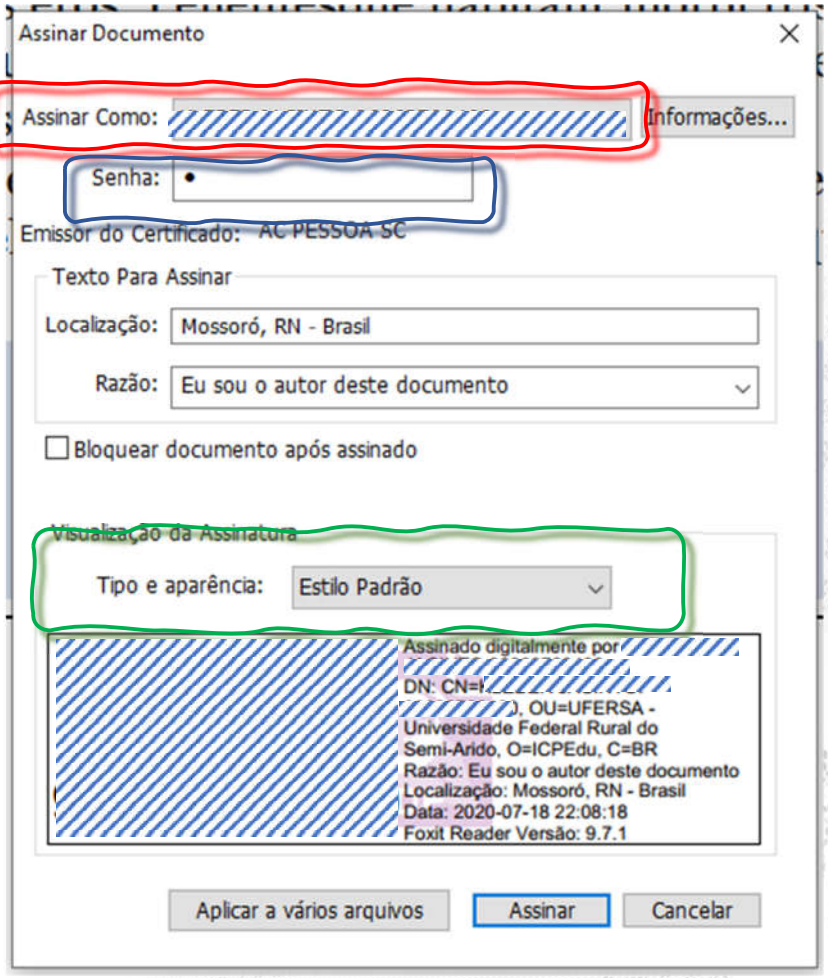

Figura 29 – Painel de inclusão de assinatura

10) Será pedido para salvar o documento assinado. Uma boa prática é salvar o arquivo com um outro nome (por exemplo, o arquivo original era “declaração.pdf” e o arquivo assinado seria “declaração_assinada.pdf”). Apesar de não ser algo necessário, salvar com outro nome permite identificar de forma inequívoca se o arquivo está ou não assinado e também manter o original por alguma necessidade, por exemplo alterações ou assinatura por mais de uma pessoa. **Uma vez salvo, o documento está assinado.**

11) Uma vez assinado, um aviso pode aparecer. Como dito na sessão introdutória deste tutorial, este aviso não implica em falha na assinatura, mas apenas que a entidade certificadora (o ICPEdu) não é universalmente reconhecida. O simples fato de mostrar o alerta, é uma importante prova de que o arquivo está assinado.

12) Quando o arquivo é aberto por você ou outra pessoa, a mesma mensagem de alerta pode ser exibida. Se for usada a função “Painel de Assinatura”, será exibida a assinatura com alerta e os detalhes da assinatura, inclusive a afirmação de que o documento foi ou não alterado após a assinatura e se a data da assinatura é compatível.

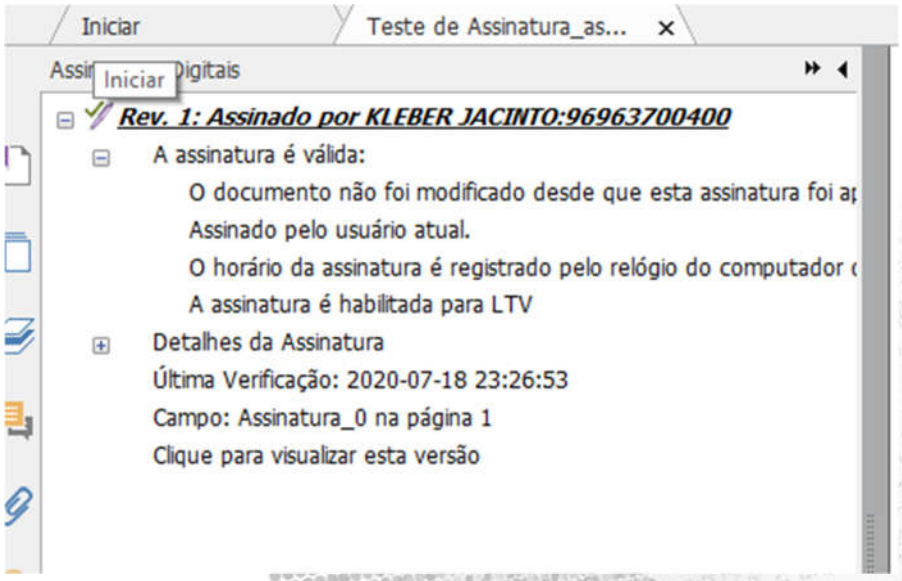

Figura 30 – Painel de Assinaturas digitais do Documento