MUITO IMPORTANTE

1º. Todo o processo de aprovar e instalar o certificado pessoal deve realizar-se numa máquina controlada pelo requerente e a que outros não tenham acesso.

Caso a máquina usada para assinar um documento seja aquela onde se pretende que o mesmo seja naturalmente usado, é conveniente realizar os seguintes passos:

- ***Gerar e transferir o certificado pessoal digital (ponto 1)***
- ***Instalar o certificado com chave privada exportável na máquina de destino. (ponto 7.2 [Windows] ou 18.1 [MAC OS])***
- ***Configurar a aplicação de leitura de PDF's para utilizar o serviço do Cartão de Cidadão que certifique a hora e data da assinatura (ponto 16)***
- ***Guardar o seu certificado num local que se recorde (pode ser numa PenDrive)***

2º. Todo o processo de assinar um documento pessoal em PDF, XLSX. XLS, DOC ou DOCX deve realizar-se numa máquina controlada pelo requerente e a que outros não tenham acesso.

Caso a máquina usada para assinar um documento seja aquela onde se pretende que o mesmo seja naturalmente usado, é necessário e conveniente realizar os seguintes passos:

- ***Abrir o documento onde se pretende colocar a assinatura***
- ***Assinar o documento XLSX, DOCX, XLS ou DOC usando o seu certificado que se encontra instalado na árvore de certificados do Windows (pontos 5, 6, 12 e 13) ou;***
- ***Assinar o documento PDF usando o seu certificado que se encontra instalado na árvore de certificados do Windows (pontos 2, 14 e 15)***
- ***Configurar a aplicação de leitura de PDF's para utilizar o serviço do Cartão do Cidadão que certifique a hora e data da assinatura (ponto 16)***

3º. Todo o processo de assinar um documento pessoal em PDF pode realizar-se numa máquina que seja da confiança do requerente e que não seja da sua exclusiva utilização.

Caso a máquina usada para assinar um documento não seja aquela onde se pretende que o mesmo seja naturalmente usado, é necessário e conveniente realizar os seguintes passos:

- ***Ligar a PenDrive que contém o seu certificado ao computador***
- ***Assinar os documentos utilizando o seu certificado em ficheiro. (ponto 17)***
- ***Configurar a aplicação de leitura de PDF's para utilizar o serviço do Cartão do Cidadão que certifique a hora e data da assinatura (ponto 16)***
- ***Remover a PenDrive que contém o seu certificado, do computador.***

Índice

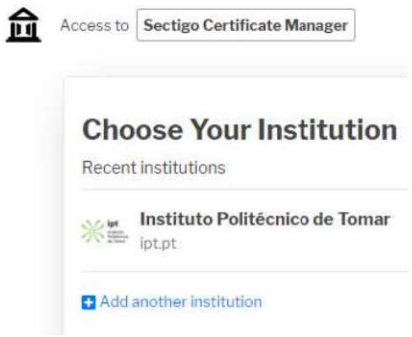
1.Como gerar um certificado digital pessoal na sectigo. 5
2. Usar o certificado no Acrobat Reader DC antes 8
2.1. A Usar o Acrobat Reader DC antes de agosto de 23 8
2.2. A Usar o Acrobat Reader DC na versão 2023.003.10269 ou superior 9
3. Como validar as assinaturas baseadas em certificados quando o Adobe Reader as apresenta como inválidas 10
3.1. Verificação de assinaturas 10
3.2. Inclusão do certificado digital nas assinaturas confiáveis do Acrobat Reader 10
4. Assinar Digitalmente todas as mensagens no Microsoft Outlook 12
5. Assinar digitalmente um documento do Microsoft Word 13
6. Assinar digitalmente um documento do Microsoft Excel 15
7. Transferir certificados do Mozila Firefox para o Microsoft Windows 17
7.1. Exportar o certificado do Mozila Firefox até à versão 68 17
7.2. Importar o certificado para o Windows 19
8. Como transferir o conteúdo do Microsoft Edge para o Internet Explorer 22
9. Verificar a existência do certificado do IPT na árvore do Windows 23
10. Exportar certificado com chave privada da árvore do Microsoft Windows 25
10.1 Exportar certificado com chave privada da árvore do Microsoft Windows anteriores ao windows 10 25
10.2 Exportar certificado com chave privada da árvore do Microsoft Windows 10 ou superior 27
11. Remover certificado com chave privada 30
11.1 Remoção de certificado no Windows 30
11.2 Remoção de certificado no Mozila Firefox 31
12. Assinar digitalmente um documento no Microsoft Word 2003 32
13. Assinar digitalmente um documento no Microsoft Excel 2003 33
14. Usar o certificado no Foxit 34
14.1. Configurar o foxit para verificar as assinaturas de forma automática 34
14.2. Assinar documentos 35
15. Usar o certificado no Acrobat Reader 11 36
15.1 Assinar Documentos 36
16. Usar servidor de Time Stamp (Marcar o documento com data e hora) 37
16.1. No Adobe Acrobat Reader 37
16.2. No FoxIT Reader 39
16.3. No Acrobat Reader 11 40

17. Assinar Documentos PDF tendo o certificado numa PenDrive 42
17.1 Acrobat reader DC 42
17.2 FoxIT reader 43
17.3 Acrobat Reader 11 45
18. Gerar e transferir o certificado digital pessoal em MACOS 47
18.1. Instalar o certificado no Porta Chaves 47
18.2. Exportar o Certificado do Porta Chaves com chave privada 47

Página Intencionalmente deixada em branco

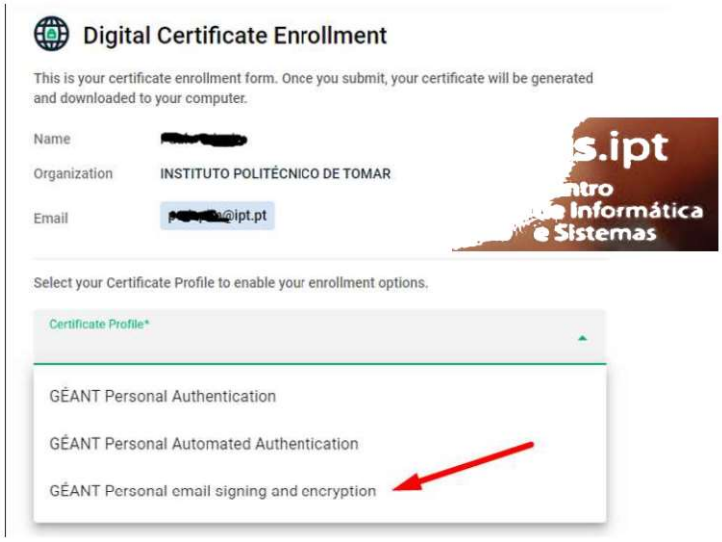
1.COMO GERAR UM CERTIFICADO DIGITAL PESSOAL NA SECTIGO.

Deve aceder a https://cert-manager.com/customer/fccn/idp/clientgeant, e escolher 'Instituto Politécnico de tomar' e usar as suas credenciais para aceder.



Os seus dados que se encontram **pré-preenchidos (*)** não podem ser alterados.

No 'Certificate Profile' deve escolher 'GÉANT Personal email signing and encryption'

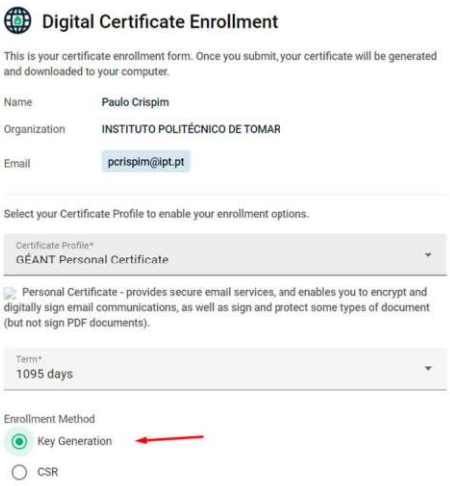


(*) Se o **nome** que aparece não for o pretendido, terá de interromper esta recolha de dados para o perfil do Certificado fechando o Navegador e terá de **alterar** o campo '**Nome abreviado**' no iManager (**Portal do I.P. Tomar**).

A partir do instante em que o **Nome** apresentado no **Perfil do Office 365** é o definido no "**Nome abreviado**", pode **reiniciar** o processo de **gerar** o **Certificado digital Pessoal**.

Deverá escolher o período de validade do certificado digital pessoal que será mais adequado ao seu tipo de contrato. Em caso de dúvida escolha 2 anos (730 dias)

No método, deve escolher 'key generation'.



No tipo, escolha a RSA com o mais valor absoluto.

No algoritmo tem de escolher 'Compatible TripleDES-SHA1' se for objetivo instalar o Certificado Digital Pessoal num MAC ou de o usar a partir de um ficheiro.

Por fim, deverá definir a password de instalação do certificado que pode conter até 8 caracteres do tipo alfanuméricos, bem como marcar a EULA (Acordo de licenciamento para o utilizador final) como lida após o ter feito e carregar no botão 'Submit'.

Ao submeter, o certificado será gerado e transferido para o seu computador.

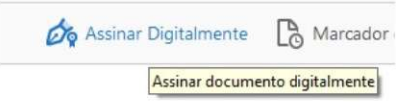
(siga para o ponto 7.2)

2. Usar o certificado no Acrobat Reader DC antes

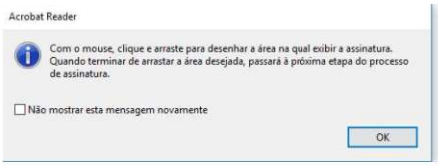
2.1. A Usar o Acrobat Reader DC antes de agosto de 23

Em **Ferramentas** clicar em abrir nos certificados.

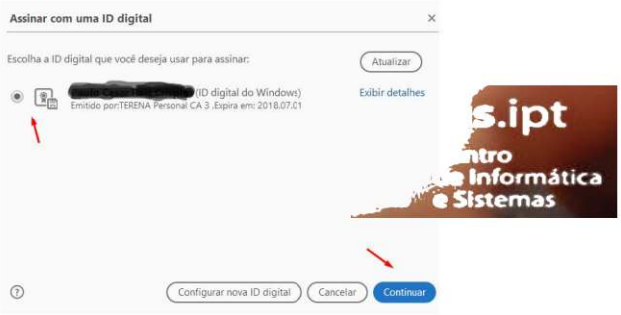
Escolher *"Assinar Digitalmente"*



É-lhe apresentado um evento a sinalizar como proceder no passo seguinte.



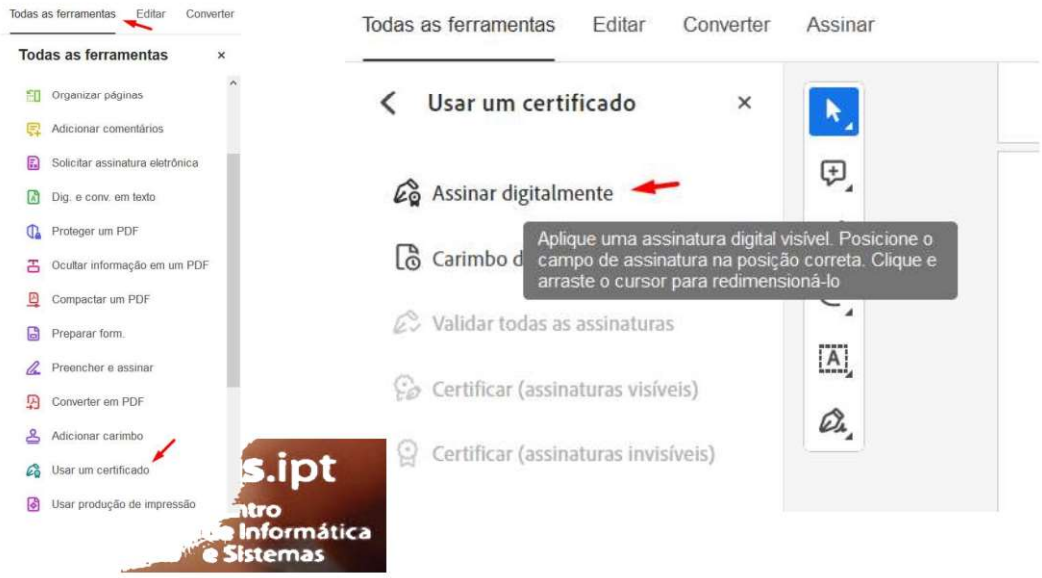
Assinalar a área pretendida e escolher o certificado pretendido.



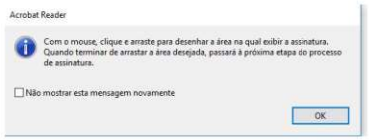
Ao apresentar o certificado, com que irá assinar o documento deverá clicar em *"Assinar"*, para que o documento seja assinado no espaço antes assinalado. Após a assinatura o documento terá de ser gravado e não poderá ser alterado. Um documento que seja bloqueado após assinado não poderá voltar a ser assinado.

2.2. A Usar o Acrobat Reader DC na versão 2023.003.10269 ou superior

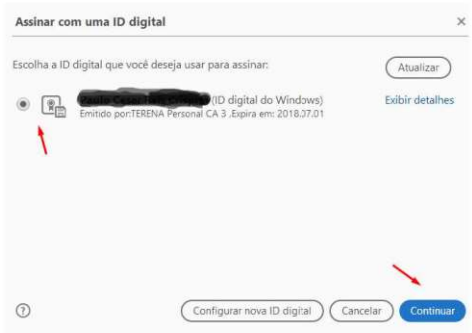
Em **Todas as Ferramentas**, no lado esquerdo escolher *'Usar um Certificado'* (pode ser necessário carregar em Ver mais) e escolher *'Assinar digitalmente'*.



É-lhe apresentado um evento a sinalizar como proceder no passo seguinte



Assinalar a área pretendida e escolher o certificado pretendido.

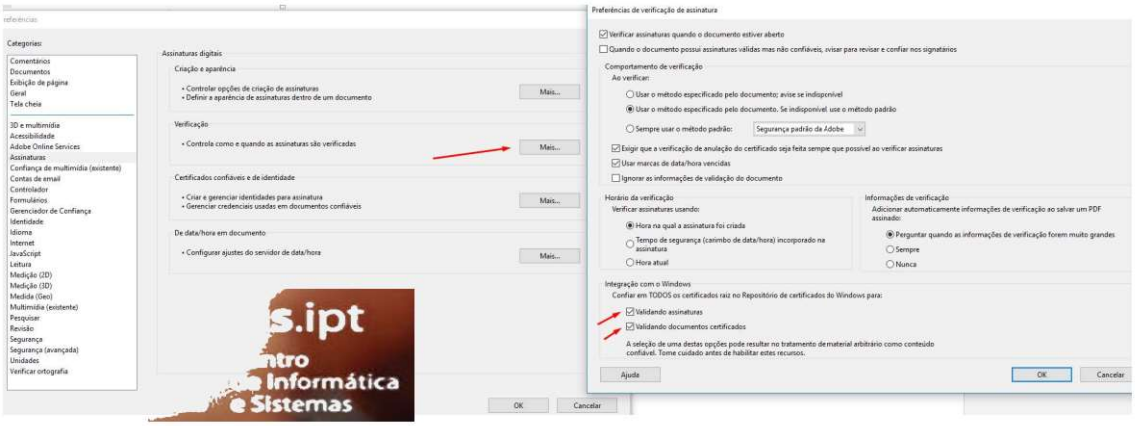


Ao apresentar o certificado, com que irá assinar o documento deverá clicar em *"Assinar"*, para que o documento seja assinado no espaço antes assinalado. Após a assinatura o documento terá de ser gravado e não poderá ser alterado. Um documento que seja bloqueado após assinado não poderá voltar a ser assinado.

3. Como validar as assinaturas baseadas em certificados quando o Adobe Reader as apresenta COMO INVÁLIDAS.

3.1. Verificação de assinaturas

Ir a **Editar**, **Preferências**, **Assinaturas** e escolher, na **Verificação** "Mais…"



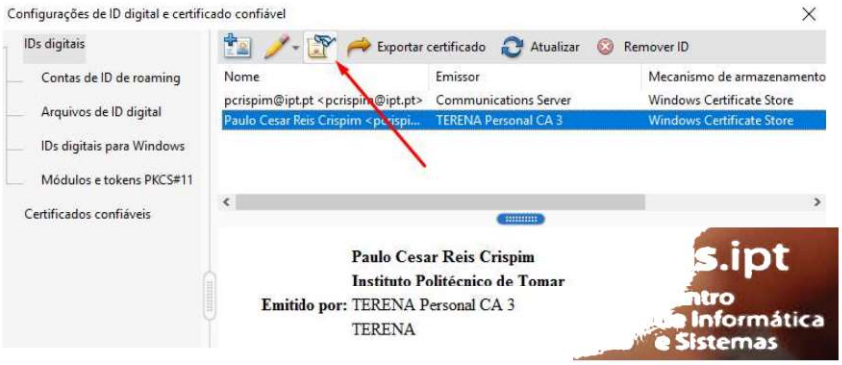
Na caixa *"Integração com o Windows"* marcar *"validando assinaturas" "validando documentos certificados"*.

O objetivo desta ação é forçar o Adobe Acrobat Reader a confiar nos certificados de raiz que estão presentes no repositório do Windows.

3.2. Inclusão do certificado digital nas assinaturas confiáveis do Acrobat Reader

Ir a **Editar**, **Preferências**, **Assinaturas** e escolher, na **Certificados confiáveis e de identidade** "Mais…"

Nesta Caixa, carregue no **Visualizador de certificados**.



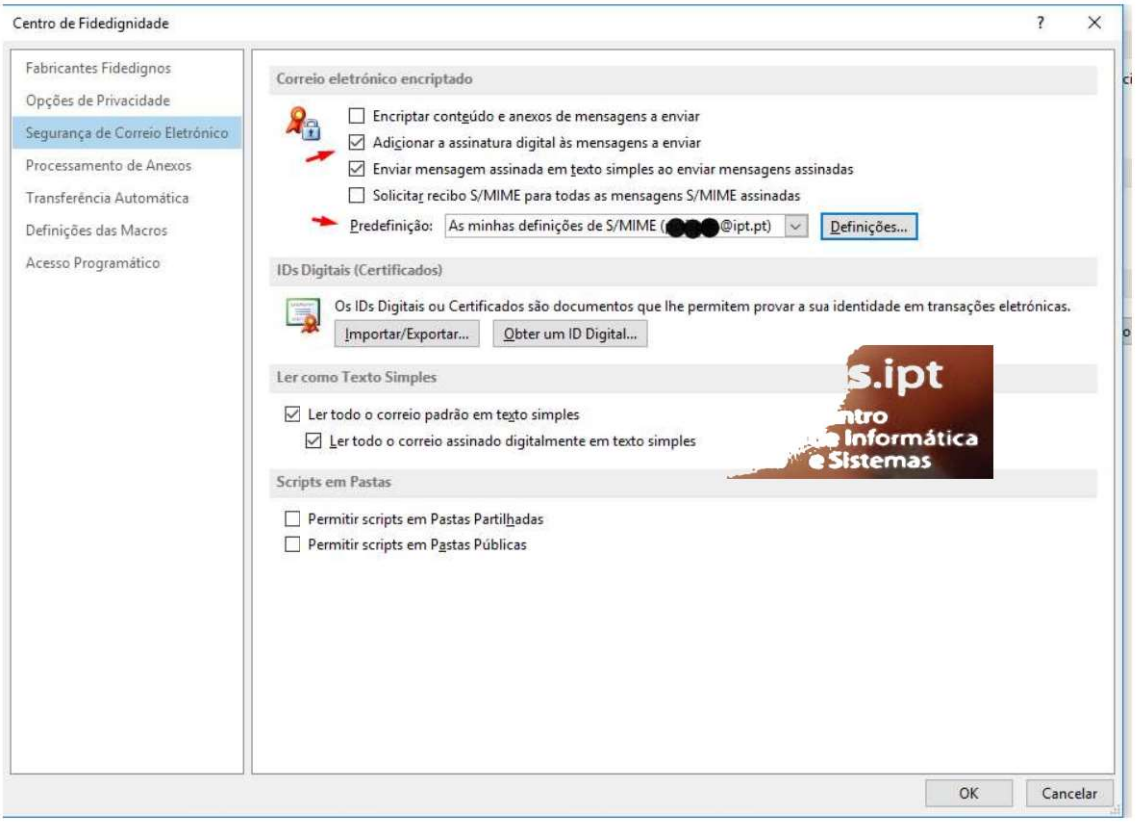
Na caixa *"Visualizador de certificados"* no separador Confiança, clicar no botão "Adicionar a certificados confiáveis…"

Em resultado, o documento certificado apresenta sinalizado a verde a validade da assinatura

4. Assinar Digitalmente todas as mensagens no Microsoft Outlook

-Carregue, nesta sequência, em **Ficheiro**, **Opções**, **Centro de Fidedignidade** e em **Definições do Centro de Fidedignidade**.

- Dentro das **Definições do Centro de Fidedignidade** escolher **Segurança do Correio Eletrónico**



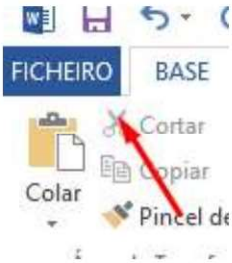
Em **Correio eletrónico encriptado** marcar *"Adicionar a assinatura digital às mensagens a enviar"*

Carregue em **Definições** e verifique se o certificado pretendido é o que está por defeito. No caso de não ser escolha o pretendido e carregue em **OK.**

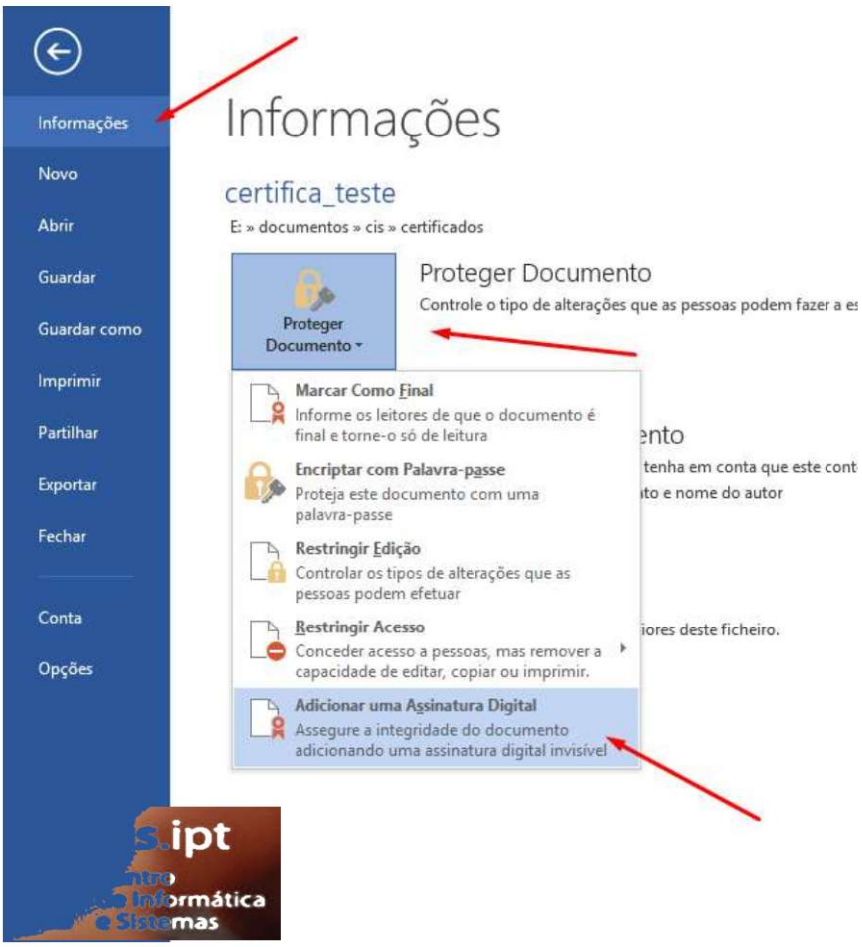
Feche as restantes janelas com **OK.**

5. Assinar digitalmente um documento do Microsoft Word

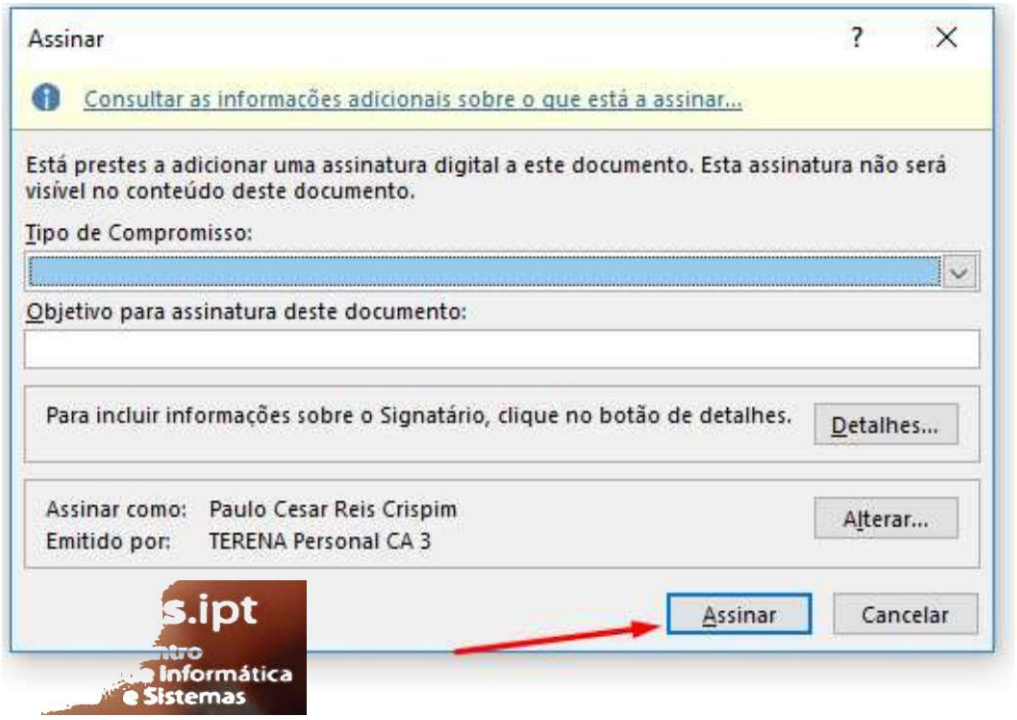
Após gravar o documento, para o assinar digitalmente terá de ir a ficheiro.



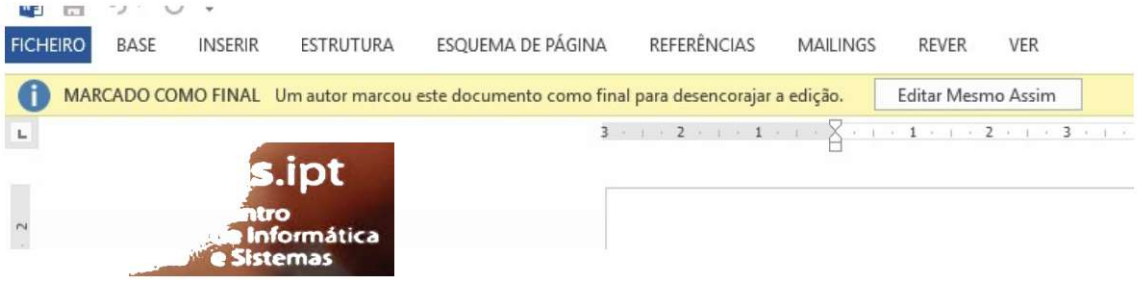
Escolher Informações, "proteger Documento" e escolher a opção "Adicionar uma assinatura Digital"



Após esta ação irá surgir uma caixa que lhe irá permitir escolher o certificado que irá ser usado para assinar o documento.



Após assinado, o documento irá mostrar uma informação onde alerta para o facto de o documento ter sido "MARCADO COMO FINAL".

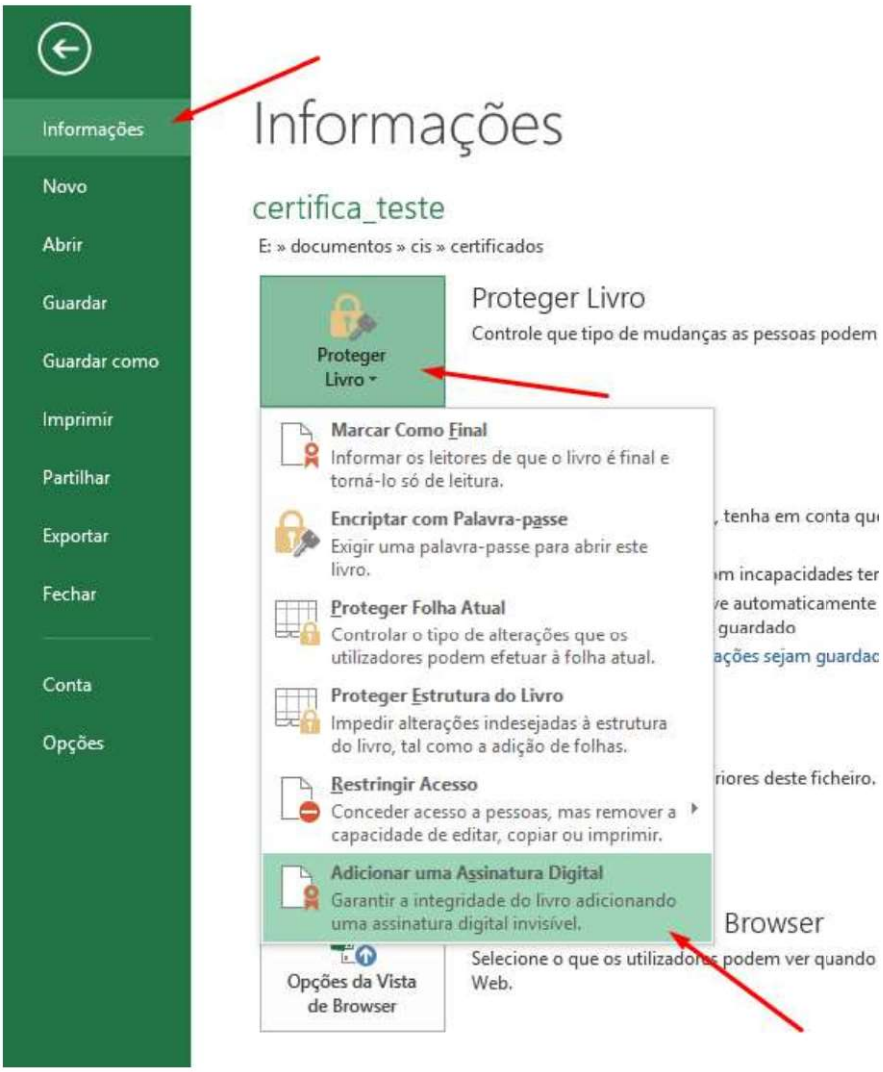


No caso de o documento ser alterado ou gravado após a assinatura, a assinatura será removida.

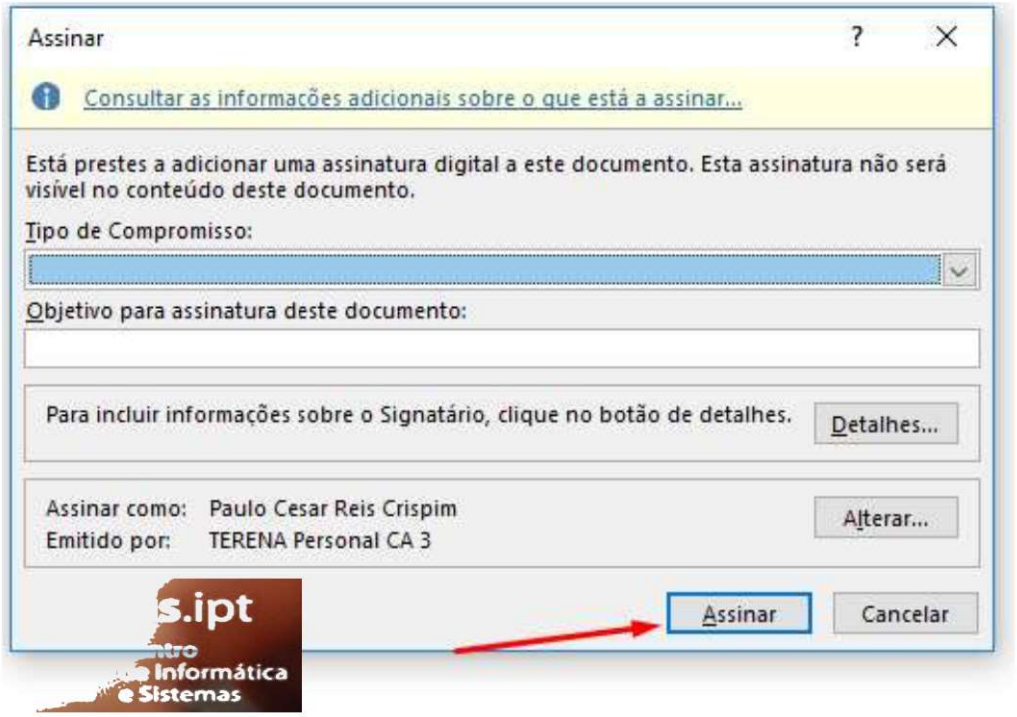
6. Assinar digitalmente um documento do Microsoft Excel

Após gravar o documento, para o assinar digitalmente terá de ir a ficheiro.

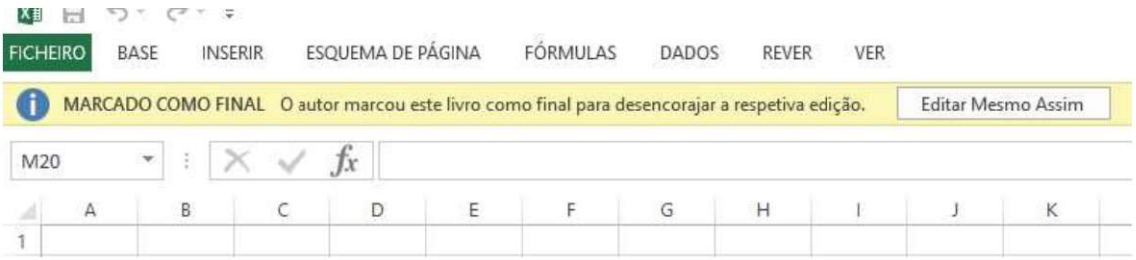
Escolher Informações, "proteger Documento" e escolher a opção "Adicionar uma assinatura Digital"



Após esta ação irá surgir uma caixa que lhe irá permitir escolher o certificado que irá ser usado para assinar o documento.



Após assinado, o documento irá mostrar uma informação onde alerta para o facto de o documento ter sido "MARCADO COMO FINAL".

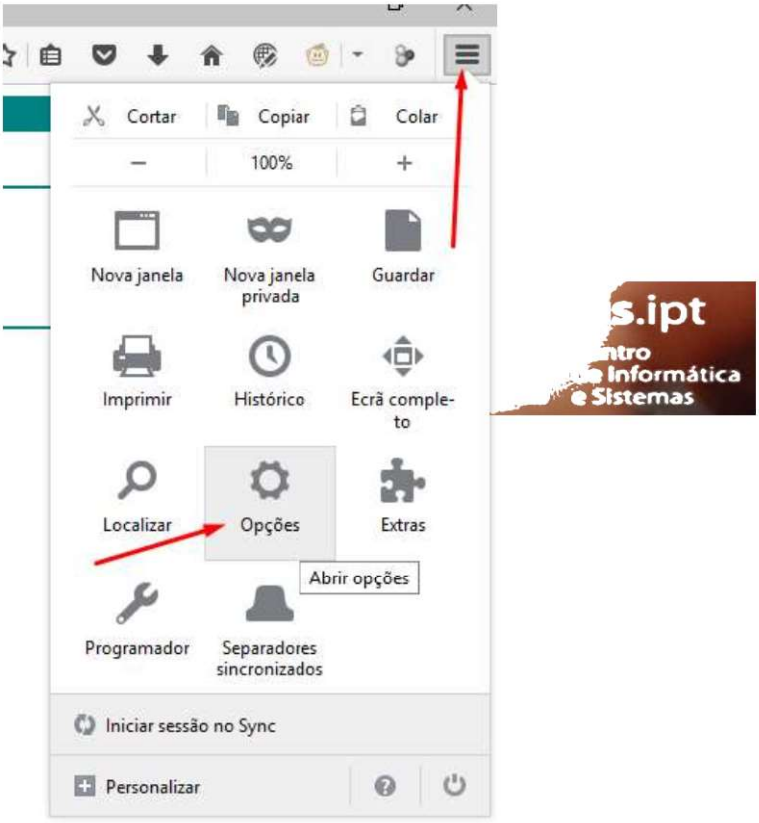


No caso de o documento ser alterado ou gravado após a assinatura, a assinatura será removida.

7. Transferir certificados do Mozila Firefox para o Microsoft Windows

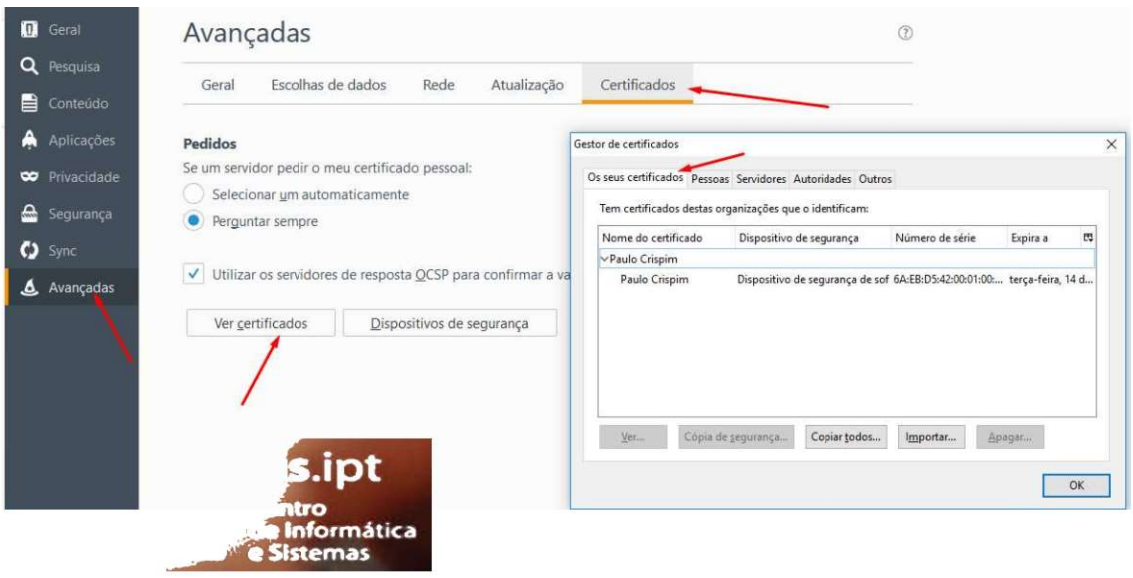
7.1. Exportar o certificado do Mozila Firefox até à versão 68

Carregar no icon do "menu" e escolher icon "opções"



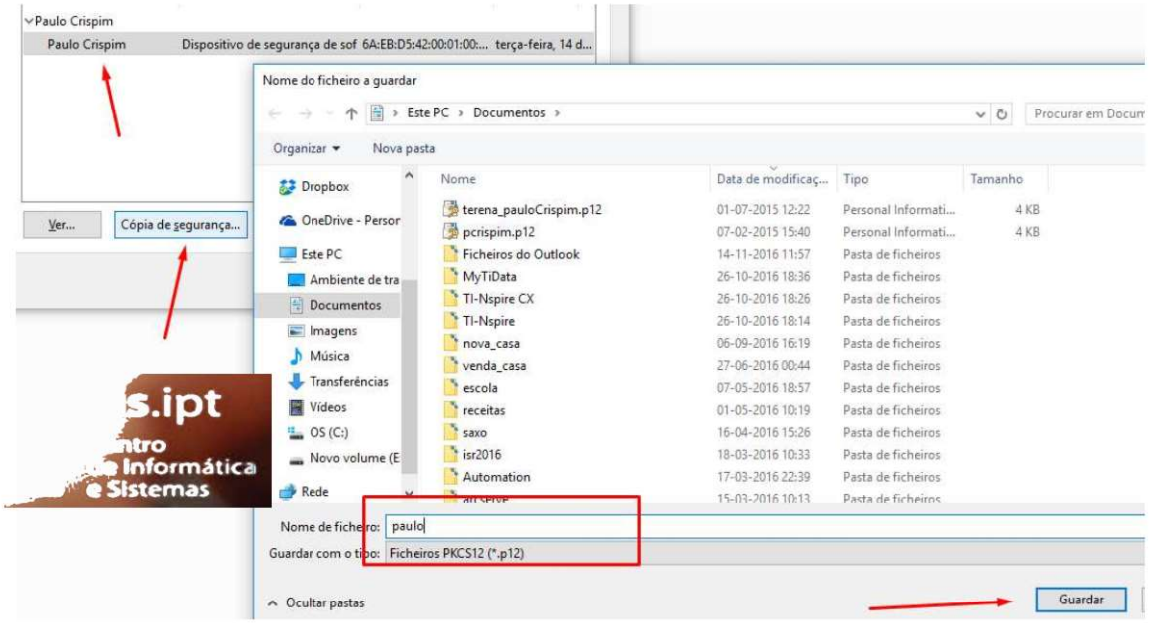
Nas opções escolher "Avançadas", "Certificados" e carregar no botão "Ver certificados".

Ao aparecer a janela do "Gestor de certificados", tem de escolher o separador "Os meus Certificados".

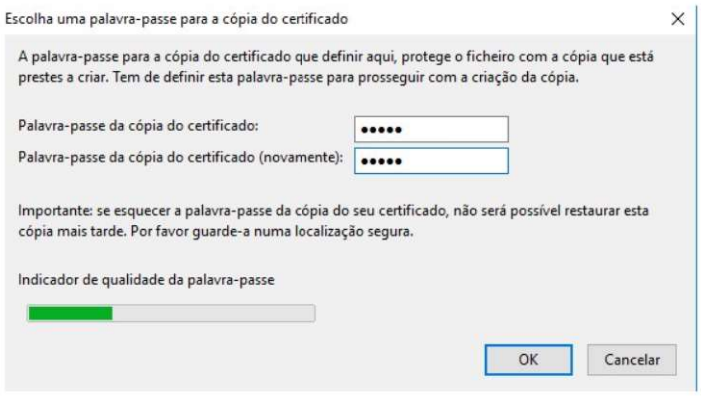


Ainda na janela do "Gestor de certificados" terá de marcar o certificado pretendido e escolher o botão "Cópia de segurança".

A cópia de segurança do certificado deverá ser guardado numa pasta, onde facilmente seja encontrado e identificado.



A palavra-passe a usar para proteger o certificado convém que seja simples. Ao carregar no botão "OK" a sua cópia do certificado ficará gravada na localização, acima, escolhida.

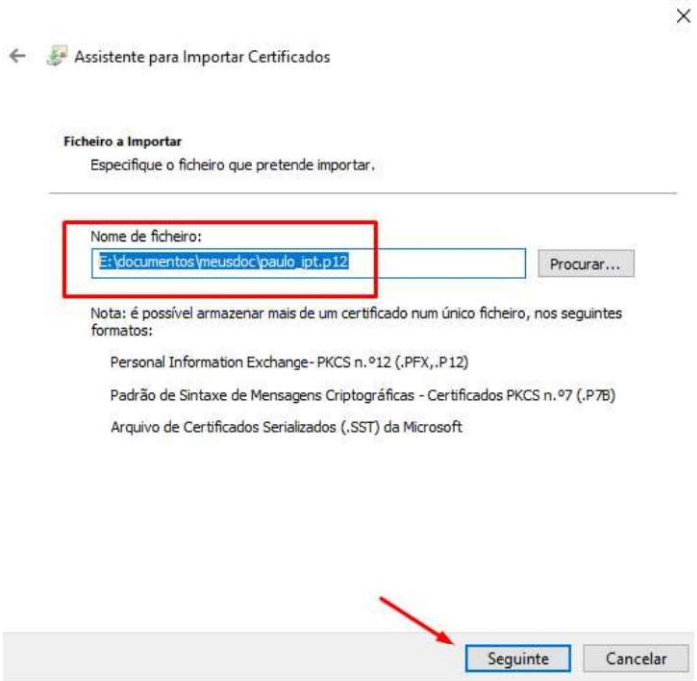


7.2. Importar o certificado para o Windows

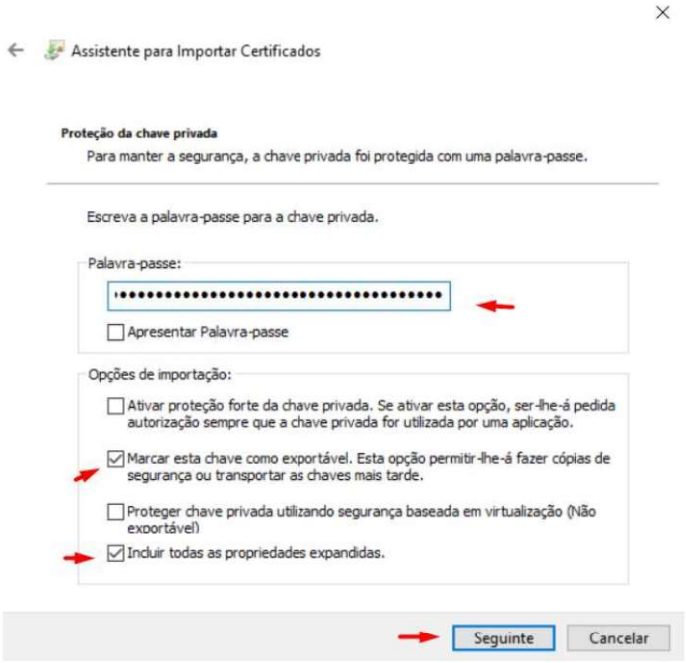
Localizar a cópia de segurança do certificado na pasta onde anteriormente ficou gravado.

Clicar nele duas vezes a fim de ser executado.

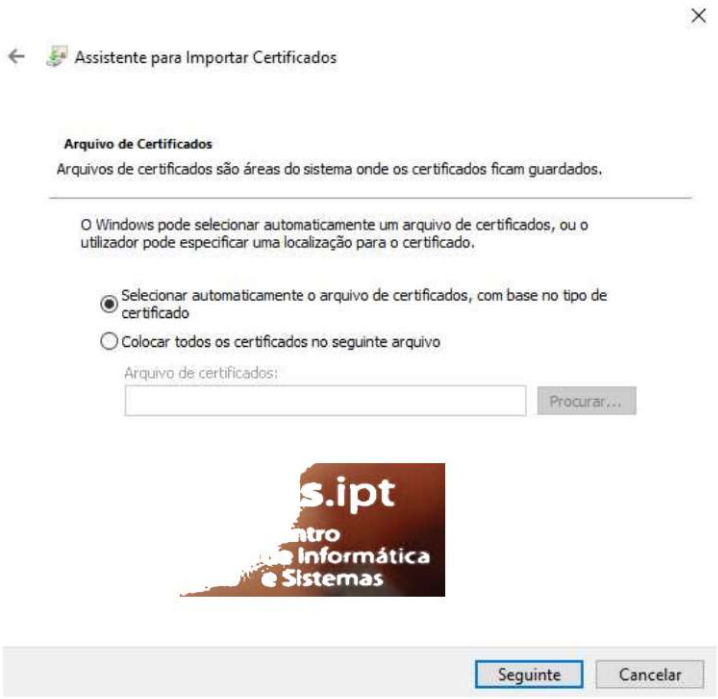
Confirmar a informação apresentada e carregar no botão “Seguinte”.



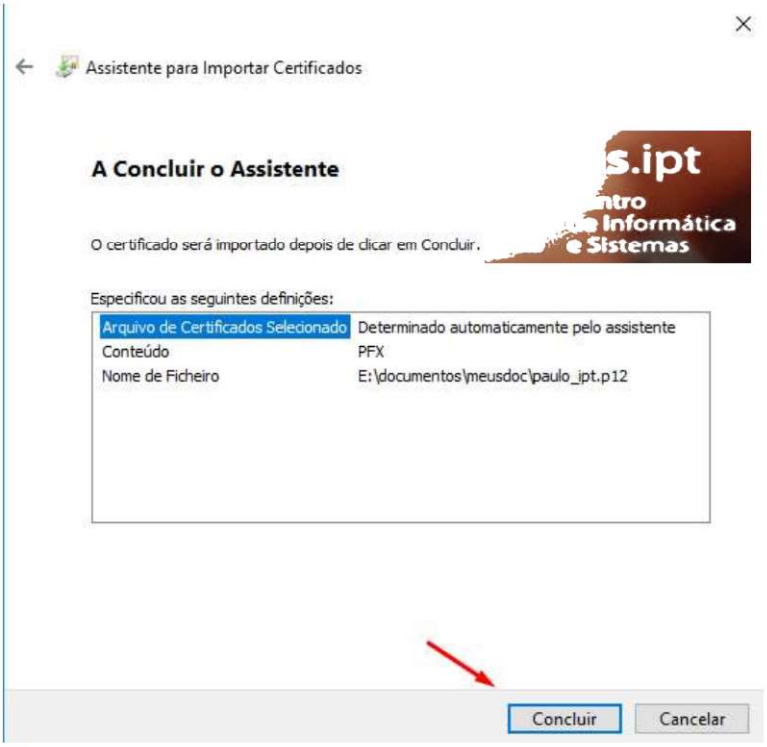
Colocar a palavra-passe anteriormente escolhida, marcar a chave privada como exportável, incluir todas as propriedades e voltar a carregar em “Seguinte”.



Manter as opções que aparecem por defeito e voltar a carregar em “Seguinte”.



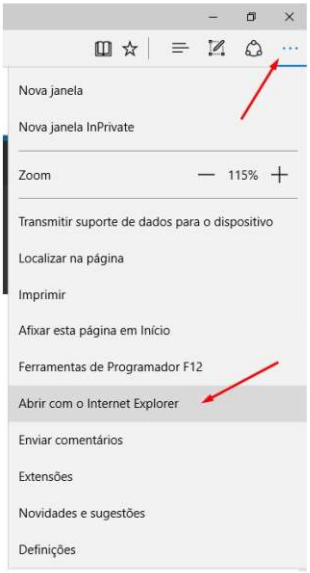
Após a apresentação do sumário da instalação do certificado deve carregar no botão “Concluir”.



8. Como transferir o conteúdo do Microsoft Edge para o Internet Explorer

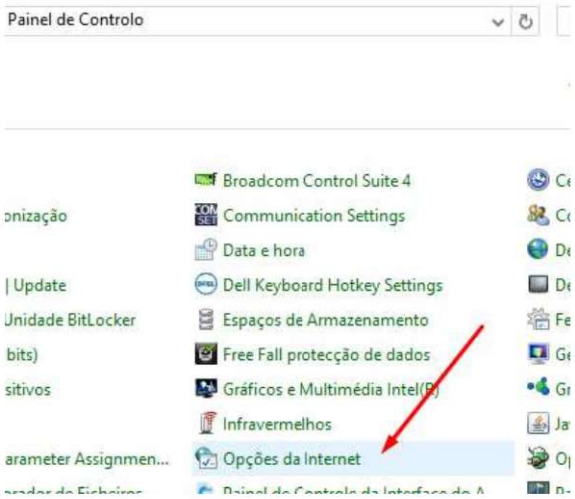
Ao abrir a ligação enviada pela Digicert no Microsoft Edge ( ), este não permite transferir o certificado para o seu computador. Para que a transferência se efetue terá de transferir a ligação para o Internet Explorer ( ).

Deve clicar em "Abrir mais" (Três pontos) e de seguida terá de escolher **Abrir com o internet Explorer**.

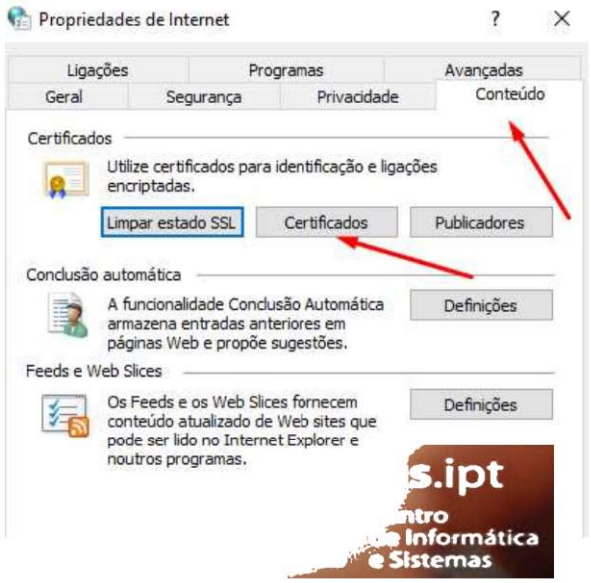


9. Verificar a existência do certificado do IPT na árvore do Windows

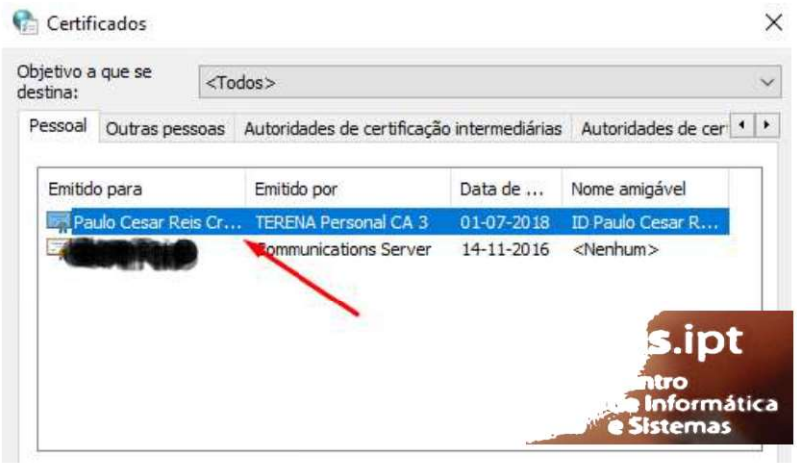
Abrir o **Painel de Controlo** e procurar a aplicação **Opções da Internet**.



Ao abrir as Opções da Internet, escolha o separador "Conteúdo" e carregue no botão "Certificados".



Na janela do Gestor de **Certificados** escolha o separador "Pessoal" e constate que o seu certificado se encontra corretamente instalado.


Certificados
Objetivo a que se destina:
<Todos>
Pessoal
Outras pessoas
Autoridades de certificação intermediárias
Autoridades de cer
Emitido para
Emitido por
Data de ...
Nome amigável
Paulo Cesar Reis Cr...
TERENA Personal CA 3
01-07-2018
ID Paulo Cesar R...
[redacted]
ommunications Server
14-11-2016
<Nenhum>
s.ipt
ntro
Informática
e Sistemas

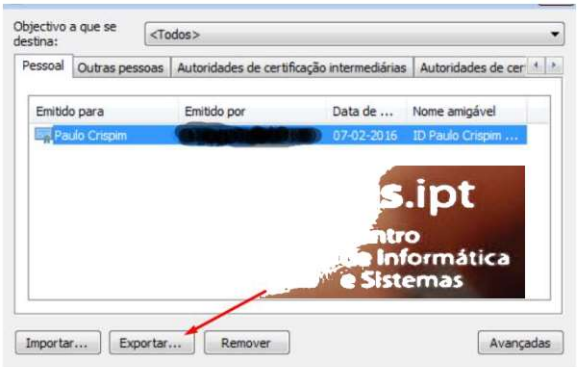
10. Exportar certificado com chave privada da árvore do Microsoft Windows

10.1 Exportar certificado com chave privada da árvore do Microsoft Windows anteriores ao windows 10

Abrir o **Painel de Controlo** e procurar a aplicação **Opções da Internet**.

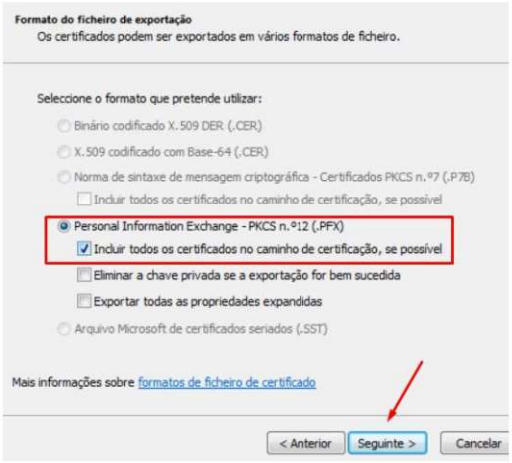
Ao abrir as Opções da Internet, escolha o separador "Conteúdo" e carregue no botão "Certificados"

Na janela do Gestor de **Certificados** escolha o separador "Pessoal", marque o certificado desejado e carregue no **botão** "Exportar".



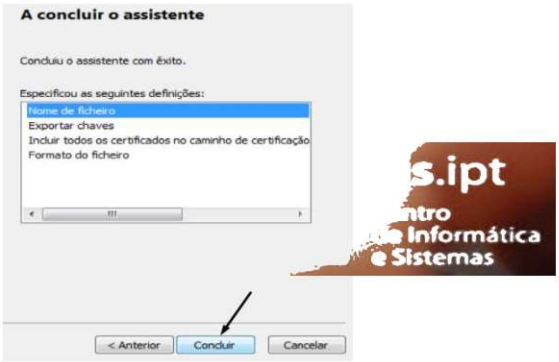
Antes de carregar no **botão** " Seguinte" marque a opção "*Sim, exportar a chave privada*".

No ecrã seguinte marque a opção PKCS12 (.pfx) e inclua a opção secundária que permite incluir todos os certificados no mesmo ficheiro PKCS12.



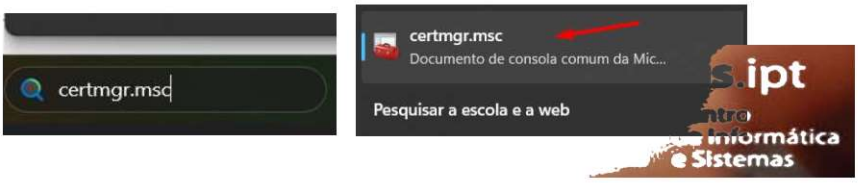
Grave o ficheiro com um nome que seja por si reconhecível e proteja-o com uma palavra-passe que seja facilmente recordável e mentalmente associável aquele ficheiro.

Após a apresentação do sumário da instalação do certificado deve carregar no botão “Concluir”.

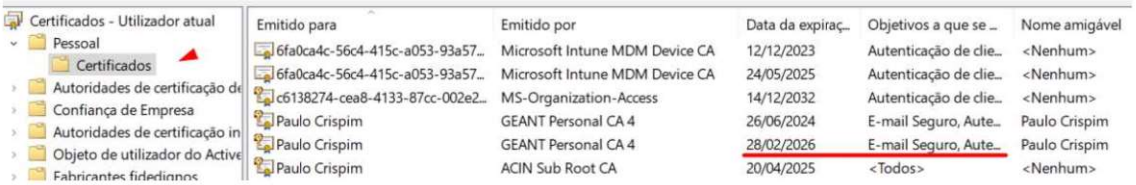


10.2 Exportar certificado com chave privada da árvore do Microsoft Windows 10 ou superior

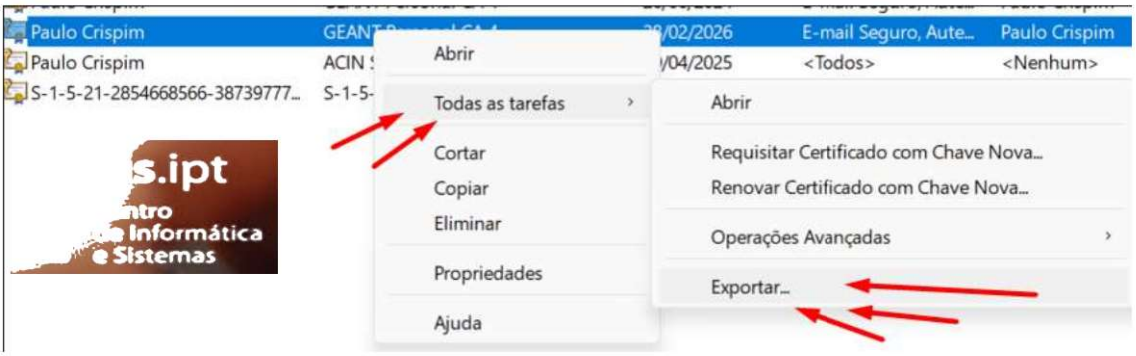
No **procurar** escreva *certmgr.msc* e **abra-o** quando lhe aparecer



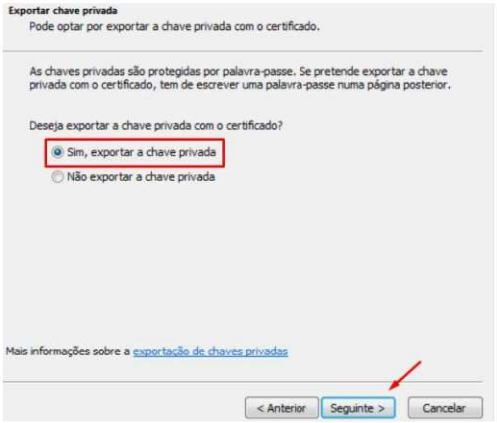
Escolha o certificado que se encontra a usar e se tiver mais do que 1 válido, escolha o que tiver a da de expiração mais avançada.



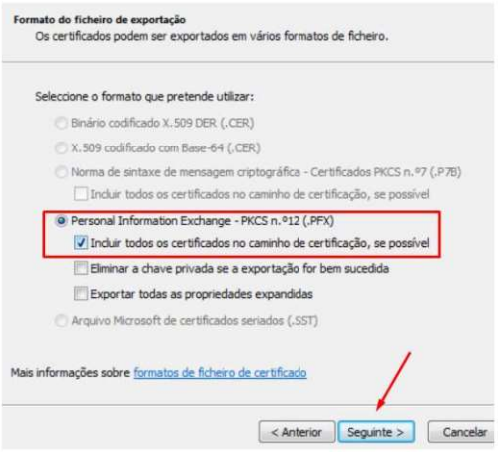
Carregue com o **botão** do rato do **lado direito** sobre o certificado escolhido e em todas as **tarefas** escolha **exportar**.



Antes de carregar no **botão** " Seguinte" marque a opção "*Sim, exportar a chave privada*".

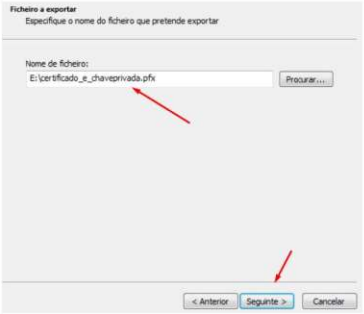


No ecrã seguinte marque a opção PKCS12 (.pfx) e inclua a opção secundária que permite incluir todos os certificados no mesmo ficheiro PKCS12.



Quando for para **definir a password** no certificado deve ter em atenção que esta password que pode conter até **8 caracteres do tipo alfanuméricos** e no **algoritmo** tem de escolher 'Compatible TripleDES-SHA1'. Carregue em *'Seguinte'* para **continuar**.

Grave o ficheiro com um nome que seja por si reconhecível e proteja-o com uma palavra-passe que seja facilmente recordável e mentalmente associável aquele ficheiro.



Após a apresentação do sumário da instalação do certificado deve carregar no botão “Concluir”.

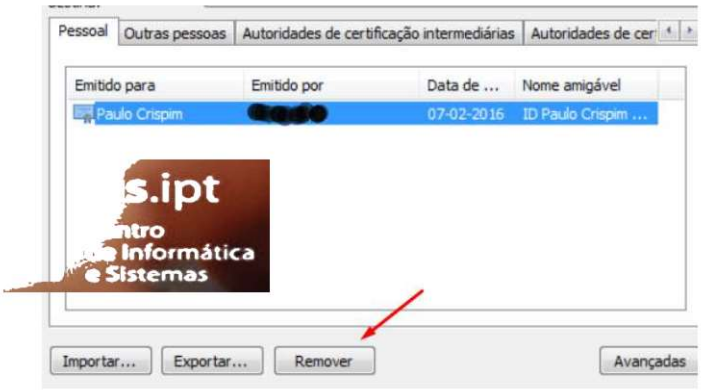
11. Remover certificado com chave privada

11.1 Remoção de certificado no Windows

Abrir o **Painel de Controlo** e procurar a aplicação **Opções da Internet**.

Ao abrir as Opções da Internet, escolha o separador "Conteúdo" e carregue no botão "Certificados"

Na janela do Gestor de **Certificados** escolha o separador "Pessoal", marque o certificado desejado e carregue no **botão** "Remover".



Na janela de confirmação, aceite a eliminação do certificado escolhendo o **Botão** "Sim".

Na janela do Gestor de **Certificados,** o certificado removido deixará de constar.

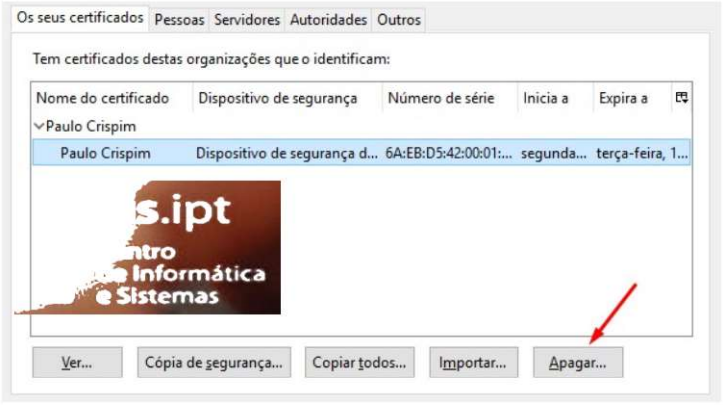
11.2 Remoção de certificado no Mozila Firefox

Carregar no ícone do "menu" e escolher ícone "opções"

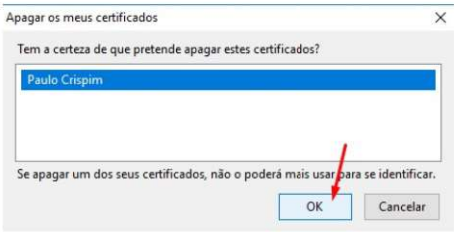
Nas opções escolher "Avançadas", "Certificados" e carregar no botão "Ver certificados".

Ao aparecer a janela do "Gestor de certificados", tem de escolher o separador "Os meus Certificados".

Ainda na janela do "Gestor de certificados" terá de marcar o certificado pretendido e escolher o botão "Apagar".



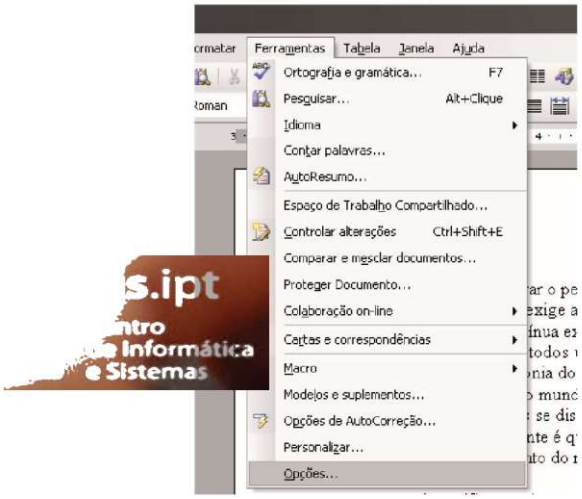
Na janela de confirmação, marque o nome do certificado anteriormente escolhido e confirme a eliminação clicando no **Botão** "OK".



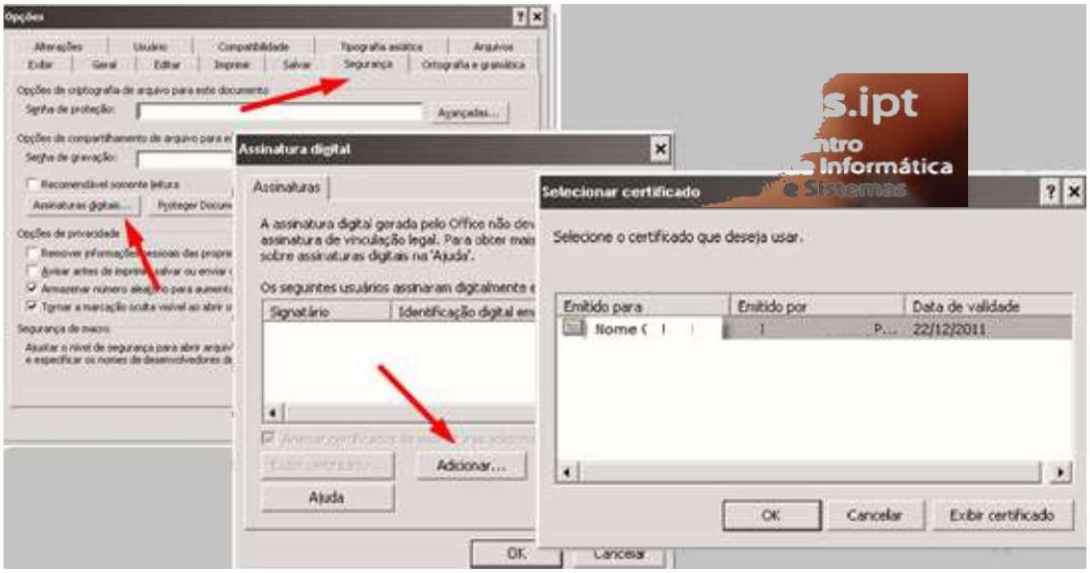
Na janela do Gestor de **Certificados,** verifique que o certificado já se encontra removido.

12. Assinar digitalmente um documento no Microsoft Word 2003

Após gravar o documento a ser assinado, clique em Ferramentas > Opções.



No menu Opções, clique no separador Segurança e depois em Assinaturas Digitais
Em Assinatura Digital clique em Adicionar e escolha o certificado que irá assinar o documento, e clique em OK. Feche as restantes janelas com OK

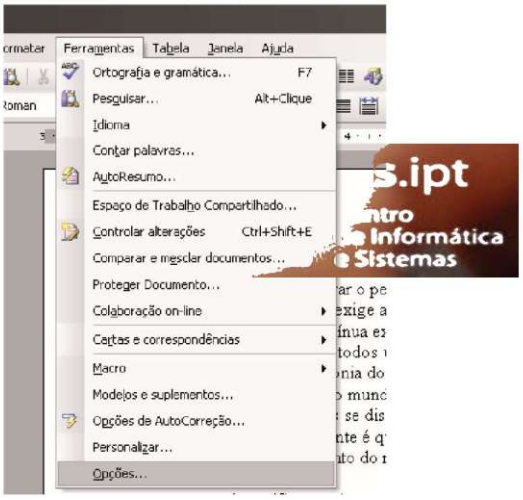


A pós assinado, aparecerá um ícone vermelho na barra de estado a informar que o documento foi assinado:

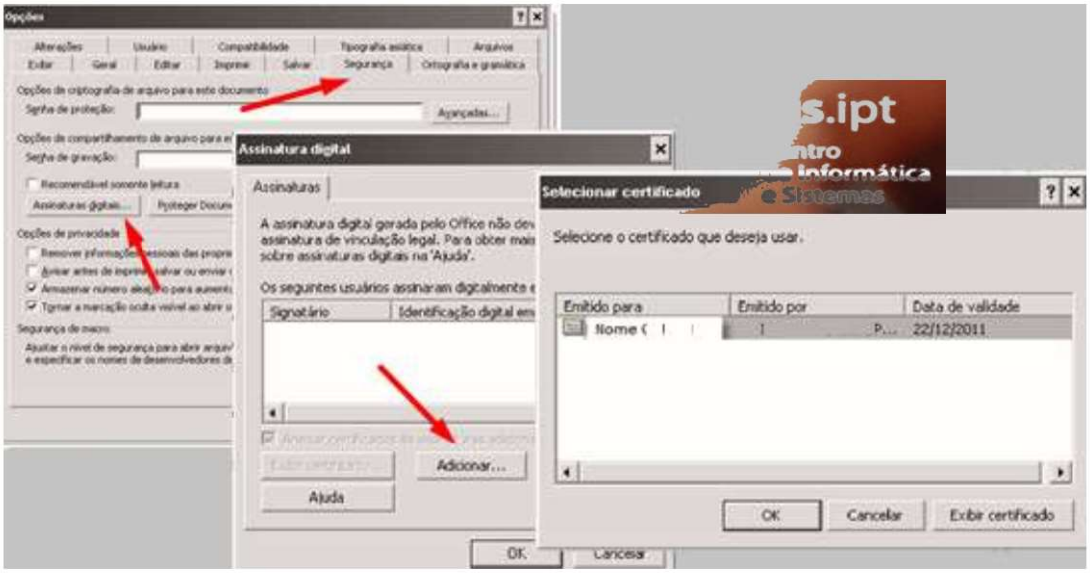
No caso de o documento ser alterado ou gravado após a assinatura, a assinatura será removida.

13. Assinar digitalmente um documento no Microsoft Excel 2003

Após gravar o documento a ser assinado, clique em Ferramentas > Opções.



No menu Opções, clique no separador Segurança e depois em Assinaturas Digitais
Em Assinatura Digital clique em Adicionar e escolha o certificado que irá assinar o documento, e clique em OK. Feche as restantes janelas com OK



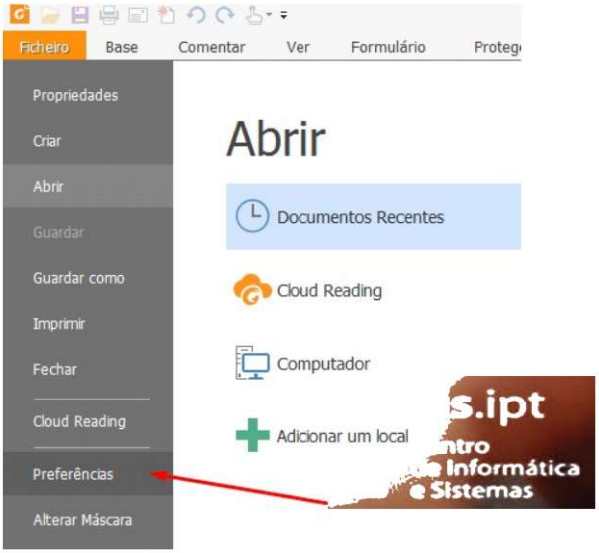
A pós assinado, aparecerá um ícone vermelho na barra de estado a informar que o documento foi assinado:

No caso de o documento ser alterado ou gravado após a assinatura, a assinatura será removida.

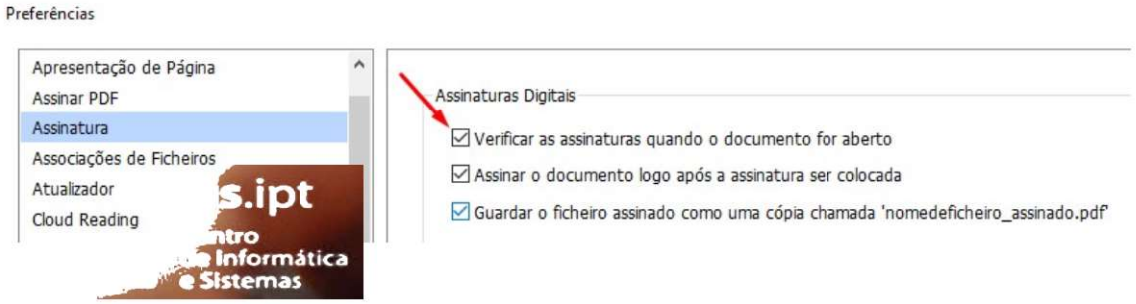
14. USAR O CERTIFICADO NO FOXIT

14.1. Configurar o foxit para verificar as assinaturas de forma automática

Em **Ficheiro** escolher **Preferências**.

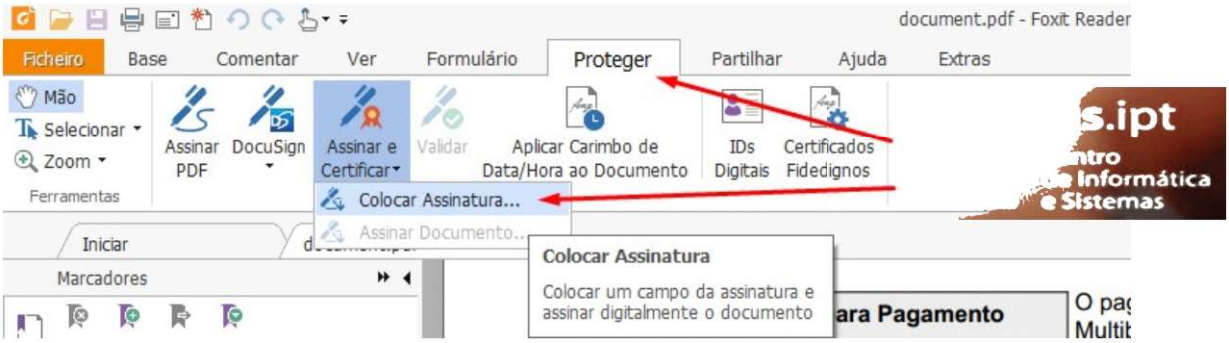


Escolher *"Assinatura"* e no painel direito marcar todas as opções que lhe são apresentadas. A marcação da opção *"Verificar as assinaturas quando o documento for aberto"* imprescindível.



14.2. Assinar documentos

Em **Proteger** clicar em Assinar e Certificar e escolha *"Colocar assinatura"*.



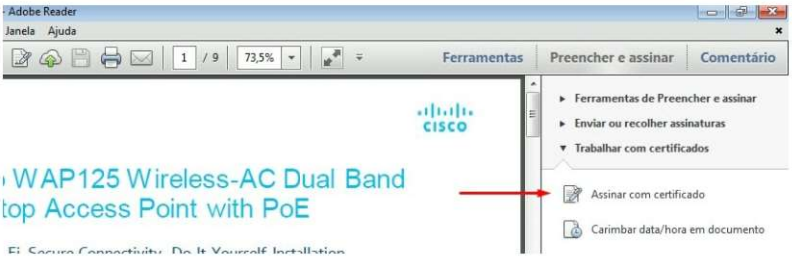
Assinalar a área pretendida e escolher o certificado pretendido.

Ao apresentar o certificado, com que irá assinar o documento deverá clicar em *"Assinar"*, para que o documento seja assinado no espaço antes assinalado. Após a assinatura o documento terá de ser gravado e não poderá ser alterado. Um documento que seja bloqueado após assinado não poderá voltar a ser assinado.

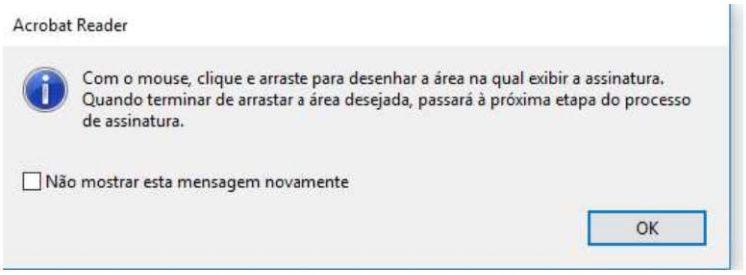
15. USAR O CERTIFICADO NO ACROBAT READER 11

15.1 Assinar Documentos

Escolher **Preencher e assinar** no canto superior direito do Acrobat Reader 11 e nos itens apresentados escolha *"Assinar com certificado"*.



É-lhe apresentado um evento a sinalizar como proceder no passo seguinte.



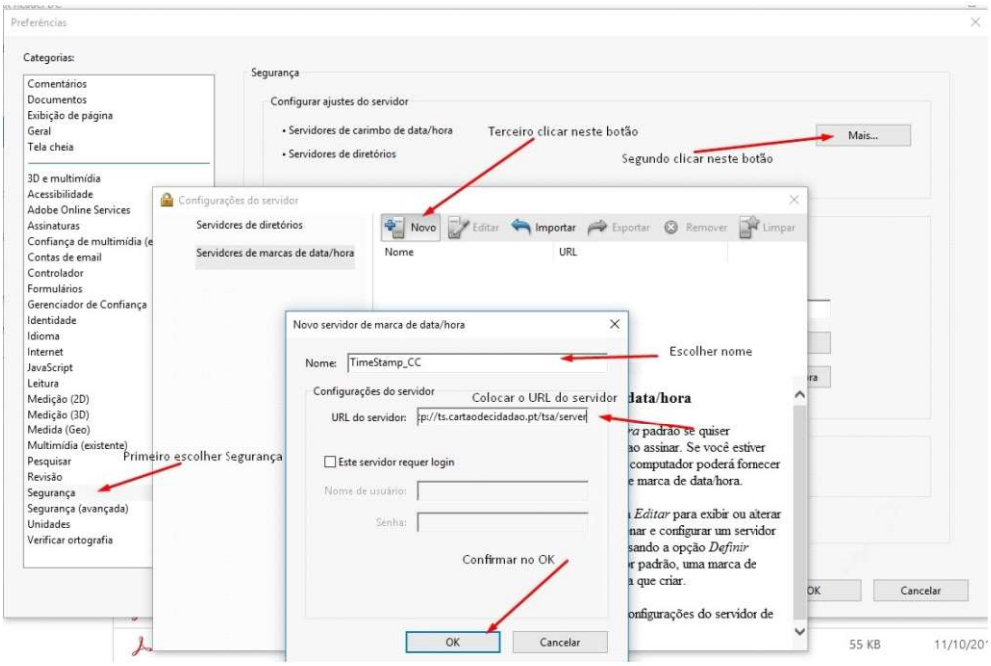
Deve assinalar a área pretendida e escolher o certificado pretendido.

Ao apresentar o certificado, com que irá assinar o documento deverá clicar em *"Assinar"*, para que o documento seja assinado no espaço antes assinalado. Após a assinatura o documento terá de ser gravado e não poderá ser alterado. Um documento que seja bloqueado após assinado não poderá voltar a ser assinado.

16. Usar servidor de Time Stamp (Marcar o documento com data e hora)

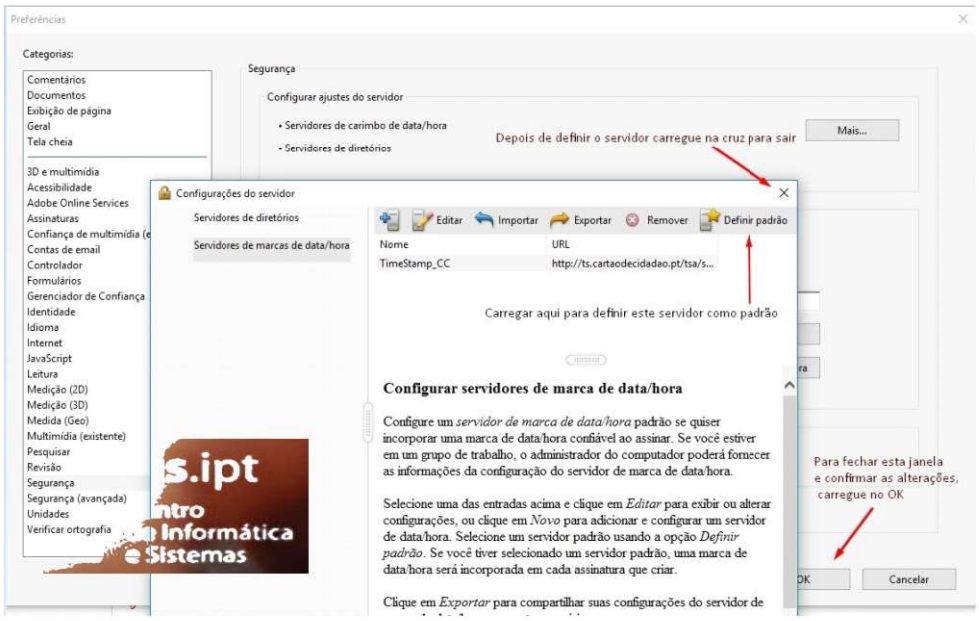
16.1. No Adobe Acrobat Reader

Ir a **Editar**, **Preferências**, **Segurança** e escolher, na **Segurança**, **Configurar ajustes do servidor** "Mais…"



Na caixa *"Configurações do Servidor"*, escolher *"Novo"* e na janela que abrir, colocar o nome que pretende com que fique identificado o **TimeStamp Server** e no URL do Servidor colocar **http://ts.cartaodecidadao.pt/tsa/server**

De retorno à janela *"Configurações do Servidor"* terá de definir o **TimeStamp Server** adicionado como padrão

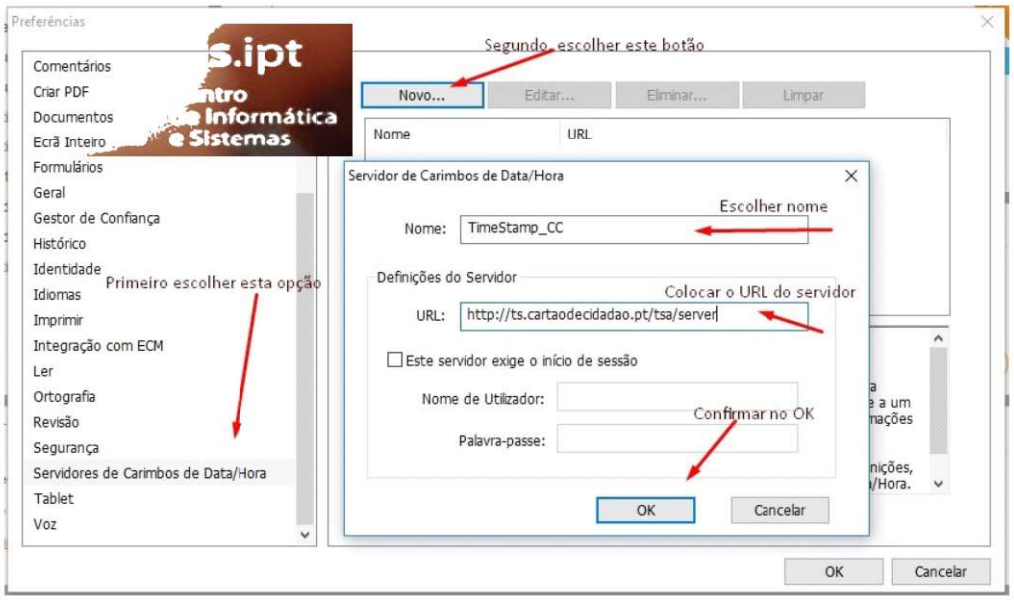


Depois de ter fechado a janela *"Configurações do Servidor"* na **Cruz**, deverá fechar a janela de *"preferências"* no botão *"OK"*.

O Objetivo desta operação é, de cada vez que a **assinatura digital** for usada o documento irá levar uma marcação com **data e hora** do servidor de **TimeStamp**. Quando não existe este tipo de configuração, a **data e hora** que ficam registadas na **assinatura digital** é a do **computador local**.

16.2. No FoxIT Reader

Ir a **Ficheiro**, **Preferências**, **Servidores de Carimbo de Data/Hora** e escolher o botão "Novo"



Na caixa *"Servidor de Carimbos de Data/Hora"*, escolher o nome que pretende com que fique identificado o **TimeStamp Server** e no URL do Servidor deverá colocar **http://ts.cartaodecidadao.pt/tsa/server**

De retorno à janela *"Configurações do Servidor"* terá de definir o **TimeStamp Server** adicionado como padrão

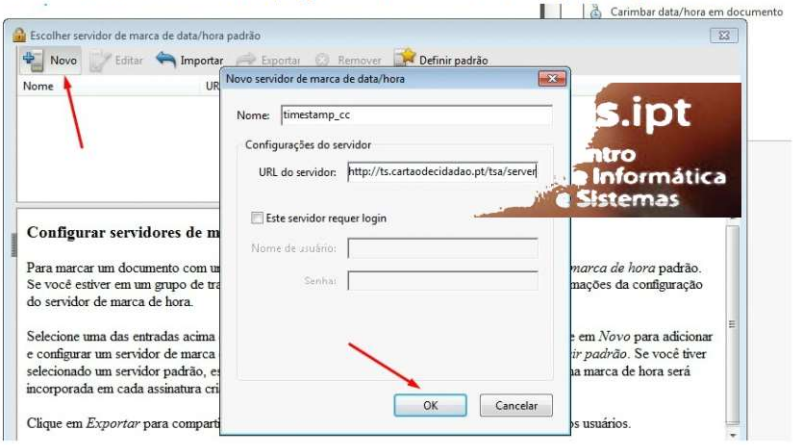
Depois de ter fechado a janela anterior, deverá clicar na linha a que corresponde o TimeStamp Server para o marcar. Após ter sido marcado irá predefini-lo, carregando no botão *"predefinir"*. Para fechar a janela de *"preferências"*, carregue no botão *"OK"*.

O Objetivo desta operação é, de cada vez que a **assinatura digital** for usada o documento irá levar uma marcação com **data e hora** do servidor de **TimeStamp**. Quando não existe este tipo de configuração, a **data e hora** que ficam registadas na **assinatura digital** é a do **computador local**.

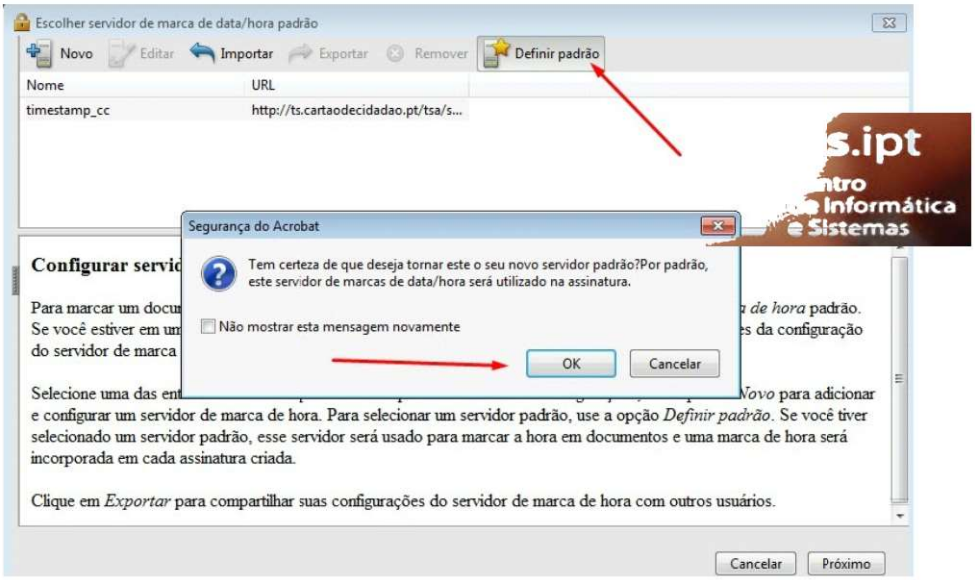
16.3. No Acrobat Reader 11

Escolher **Preencher e assinar** no canto superior direito do Acrobat Reader 11 e nos itens apresentados escolha *"Carimbar data/hora em Documento"*.

Na caixa *"Escolher servidor de marca de data/hora padrão"*, escolher *"Novo"* e na janela que abrir, colocar o nome que pretende com que fique identificado o **TimeStamp Server** e no URL do Servidor colocar **http://ts.cartaodecidadao.pt/tsa/server**



Na janela *"Escolher servidor de marca de data/hora padrão"* terá de definir o **TimeStamp Server** adicionado como padrão



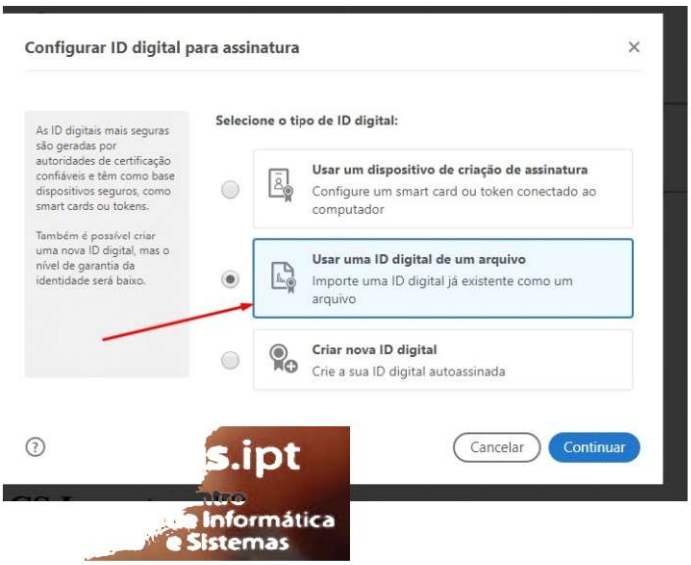
O Objetivo desta operação é, de cada vez que a **assinatura digital** for usada o documento irá levar uma marcação com **data e hora** do servidor de **TimeStamp**. Quando não existe este tipo de configuração, a **data e hora** que ficam registadas na **assinatura digital** é a do **computador local**.

17. Assinar Documentos PDF tendo o certificado numa PenDrive

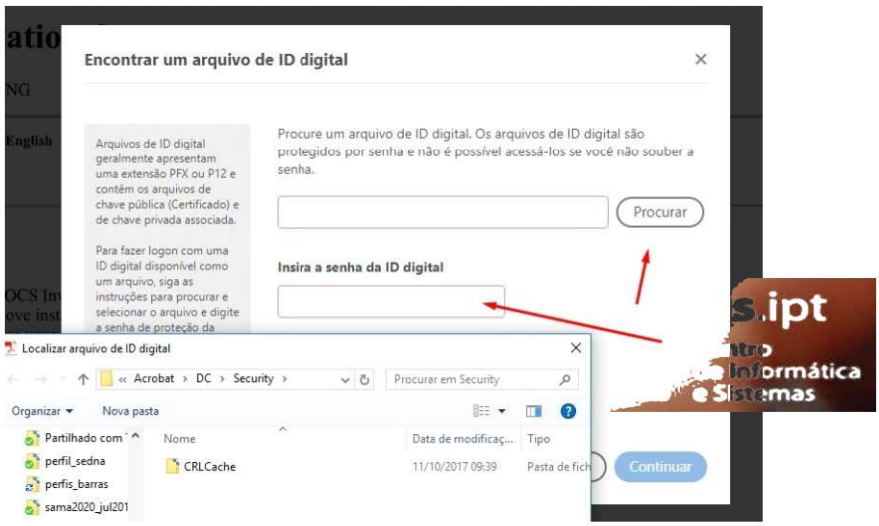
17.1 Acrobat reader DC

Após iniciar o procedimento do **Ponto 2** deste guia e imediatamente após assinalar a área pretendida para colocar a marca do seu certificado digital, na janela onde seleciona a assinatura a usar, terá de escolher **Configurar nova ID digital**.

Deve, também, escolher o meio onde a assinatura se encontra, e neste caso escolhe *"Usar uma ID digital de um arquivo"*.



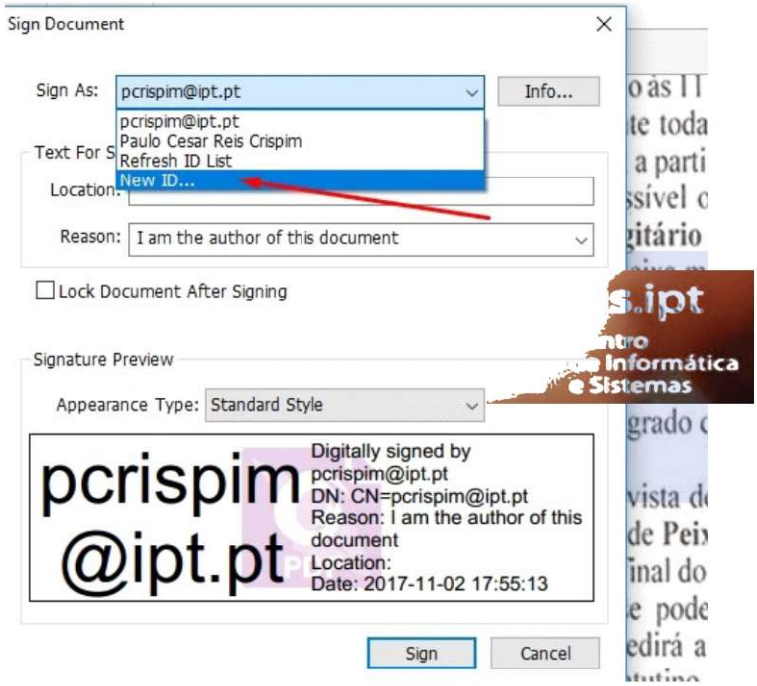
Ao escolher o ficheiro onde se encontra **o seu certificado (*.p12)**, coloca a palavra-passe que lhe colocou quando o exportou (**Ponto 7.1** ou **Ponto 10** deste guia) e carregue em **Continuar**.



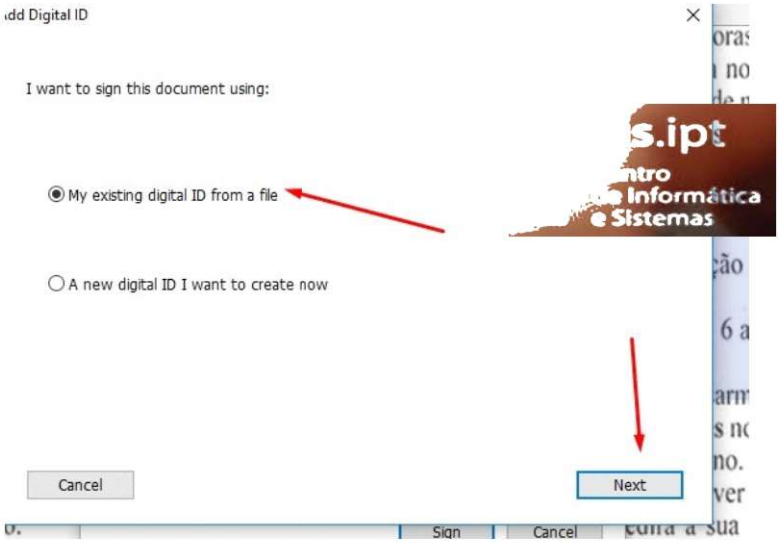
Após este passo terá de continuar o procedimento descrito no **Ponto 2** (página 6)

17.2 FoxIT reader

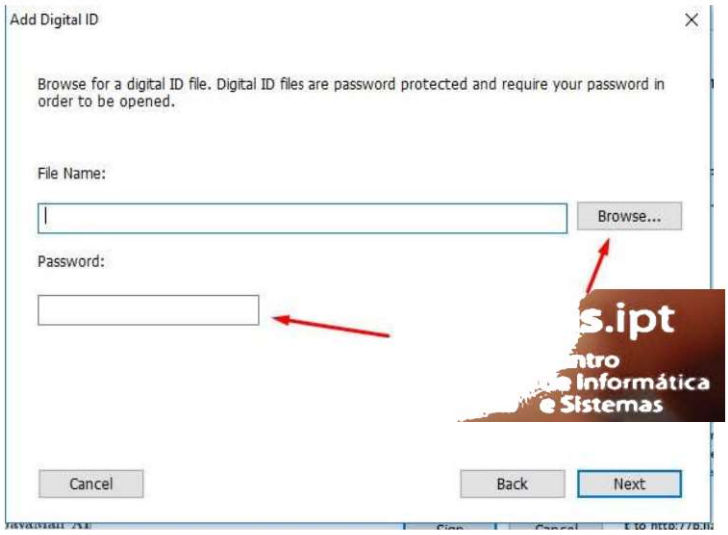
Após iniciar o procedimento do **Ponto 14.2** deste guia e imediatamente após assinalar a área pretendida para colocar a marca do seu certificado digital, na janela onde seleciona a assinatura a usar, em **Assinar como**, terá de escolher **New ID…** .



Deve, também, escolher o meio onde a assinatura se encontra, e neste caso escolhe *"My existing digital ID from file"*.



Ao escolher o ficheiro onde se encontra **o seu certificado (*.pfx)**[1], coloca a palavra-passe que lhe colocou quando o exportou (**Ponto 7.1** ou **Ponto 10** deste guia) e carregue em **Continuar**



Após este passo terá de continuar o procedimento descrito no **Ponto 14.2** (página 35)

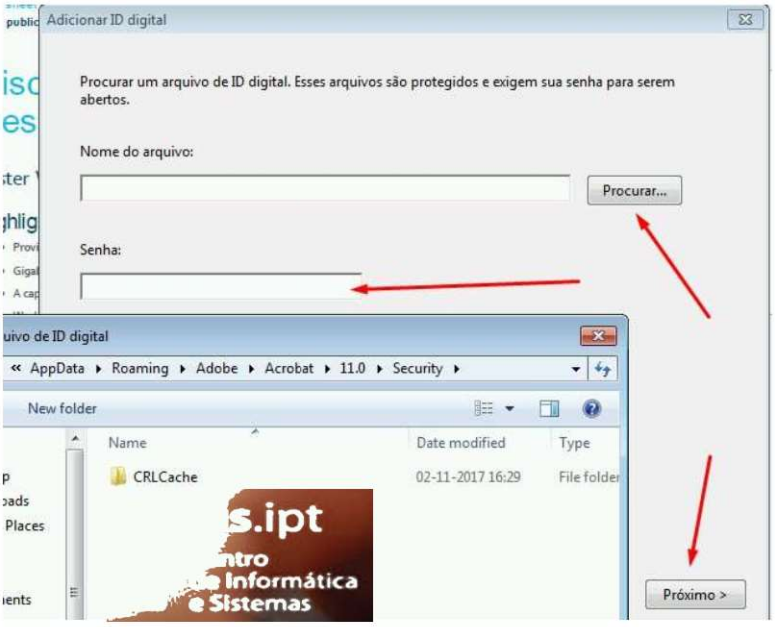
(1) Deve **renomear a extensão** do ficheiro do seu certificado de **.p12** para **.pfx**.

17.3 Acrobat Reader 11

Após iniciar o procedimento do **Ponto 15.1** deste guia e imediatamente após assinalar a área pretendida para colocar a marca do seu certificado digital, na janela onde seleciona a assinatura a usar, terá de escolher **Nova ID…** .

Na janela **Adicionar ID Digital** marque *"Minha ID digital existente de:"* e marque *"Um arquivo"*.

Ao escolher o ficheiro onde se encontra **o seu certificado (*.p12)**, coloca a palavra-passe que lhe colocou quando o exportou (**Ponto 1, ponto 7.1** ou **Ponto 10** deste guia) e carregue em **Próximo**.



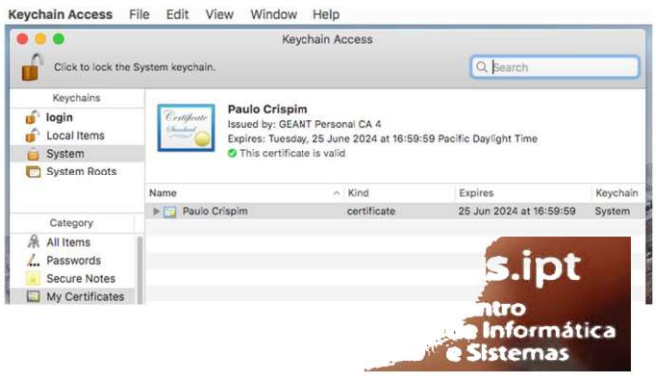
Após este passo terá de continuar o procedimento descrito no **Ponto 15.1** (página 36)

18. Gerar e transferir o certificado digital pessoal em MACOS

Para gerar e transferir o certificado digital pessoal em MACOS deve ser usado o procedimento descrito no **ponto 1** deste guia.

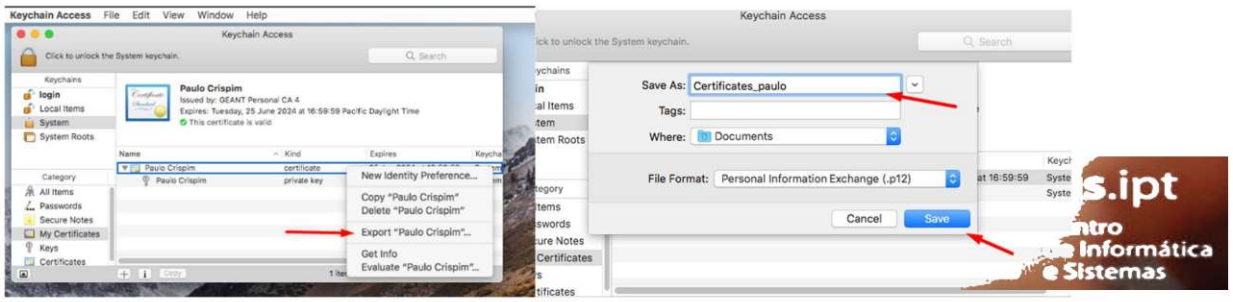
18.1. Instalar o certificado no Porta Chaves

Abrir **o seu certificado (*.p12)** usando o **keychain access**, que está por defeito associado a este tipo de ficheiros. A password usada para **associar o seu certificado** ao keychain access é a **password de instalação** escolhida quando gerou o seu certificado.



18.2. Exportar o Certificado do Porta Chaves com chave privada

Nas **propriedades do seu certificado** no keychain escolha **exportar**. Na janela seguinte, escolha um **nome que identifique** o que está a ser guardado. O seu certificado deve ser gravado numa **localização** da sua preferência e da qual se **recorde**.



Para garantir uma utilização exclusiva do **seu certificado** escolha uma **password** da qual não se esqueça.

Para poder **utilizar o certificado** que está a exportar **noutras aplicações** ou **noutros computadores**, terá que durante a exportação do seu certificado, **exportar a chave privada** do seu certificado. Por esse motivo é que lhe é solicitado e deverá **permitir**, o acesso da aplicação que exporta à chave privada do seu certificado que se encontra guardada no keychain.