



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

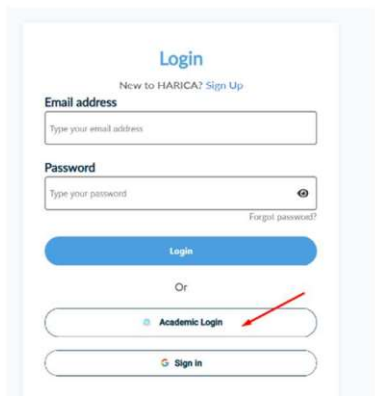
1.Como gerar um certificado digital pessoal na HARICA.	5
2. Usar o certificado no Acrobat Reader DC antes.....	10
2.1. A Usar o Acrobat Reader DC antes de agosto de 23	10
2.2. A Usar o Acrobat Reader DC na versão 2023.003.10269 ou superior	11
3. Como validar as assinaturas baseadas em certificados quando o Adobe Reader as apresenta como inválidas.....	12
3.1. Verificação de assinaturas.....	12
3.2. Inclusão do certificado digital nas assinaturas confiáveis do Acrobat Reader	12
4. Assinar Digitalmente todas as mensagens no Microsoft Outlook	14
5. Assinar digitalmente um documento do Microsoft Word	15
6. Assinar digitalmente um documento do Microsoft Excel	17
7. Transferir certificados do Mozilla Firefox para o Microsoft Windows.....	19
7.1. Exportar o certificado do Mozilla Firefox até à versão 68	19
7.2. Importar o certificado para o Windows	21
8. Como transferir o conteúdo do Microsoft Edge para o Internet Explorer.....	24
9. Verificar a existência do certificado do IPT na árvore do Windows.....	25
10. Exportar certificado com chave privada da árvore do Microsoft Windows	27
10.1 Exportar certificado com chave privada da árvore do Microsoft Windows anteriores ao windows 10	27
10.2 Exportar certificado com chave privada da árvore do Microsoft Windows 10 ou superior	29
11. Remover certificado com chave privada.....	32
11.1 Remoção de certificado no Windows	32
11.2 Remoção de certificado no Mozilla Firefox.....	33
12. Assinar digitalmente um documento no Microsoft Word 2003	34
13. Assinar digitalmente um documento no Microsoft Excel 2003	35
14. Usar o certificado no Foxit	36
14.1. Configurar o foxit para verificar as assinaturas de forma automática.....	36
14.2. Assinar documentos.....	37
15. Usar o certificado no Acrobat Reader 11	38
15.1 Assinar Documentos.....	38
16. Usar servidor de Time Stamp (Marcar o documento com data e hora)	39
16.1. No Adobe Acrobat Reader	39
16.2. No FoxIT Reader	41
16.3. No Acrobat Reader 11	42

17. Assinar Documentos PDF tendo o certificado numa PenDrive.....	44
17.1 Acrobat reader DC.....	44
17.2 FoxIT reader	45
17.3 Acrobat Reader 11.....	47
18. Gerar e transferir o certificado digital pessoal em MACOS	49
18.1. Instalar o certificado no Porta Chaves	49
18.2. Exportar o Certificado do Porta Chaves com chave privada.....	49

Página Intencionalmente deixada em branco

1.COMO GERAR UM CERTIFICADO DIGITAL PESSOAL NA HARICA.

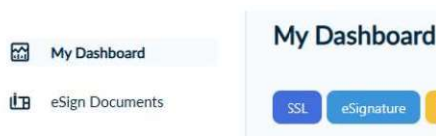
Aceda a <https://cm.harica.gr/>, escolha **Academic Login** e ‘**Instituto Politécnico de tomar**’ e use as suas credenciais para aceder.



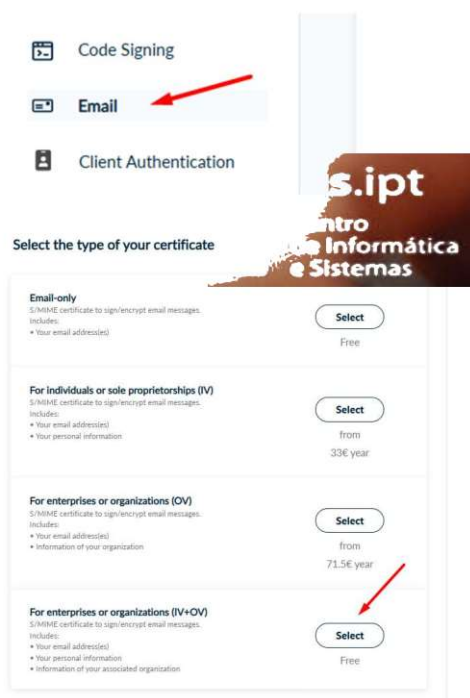
The login form is titled 'Login' and includes a link for 'New to HARICA? Sign Up'. It contains two input fields: 'Email address' and 'Password'. Below the password field is a 'Forgot password?' link. A blue 'Login' button is positioned below the password field. Below the button is the word 'Or'. At the bottom, there are two buttons: 'Academic Login' (highlighted with a red arrow) and 'Sign in'.



No seu **Dashboard**, em **Certificates Requests** encontre ‘**Email**’.



Para escolher o tipo de certificado terá de carregar em ‘**Email**’ e seleccionar o certificado de tipo **IV+OV (for enterprises or organizations)** e valide essa opção carregando em ‘**Next**’.



The screen shows the 'Select the type of your certificate' options. The 'Email' option is highlighted with a red arrow. Below, the 'For enterprises or organizations (IV+OV)' option is also highlighted with a red arrow. The table lists the following options:

Certificate Type	Description	Includes	Price
Email-only	S/MIME certificate to sign/encrypt email messages.	Your email address(es)	Free
For individuals or sole proprietorships (IV)	S/MIME certificate to sign/encrypt email messages.	Your email address(es) Your personal information	from 33€ year
For enterprises or organizations (OV)	S/MIME certificate to sign/encrypt email messages.	Your email address(es) Information of your organization	from 71.5€ year
For enterprises or organizations (IV+OV)	S/MIME certificate to sign/encrypt email messages.	Your email address(es) Your personal information Information of your associated organization	Free

Select the type of your certificate

For enterprises or organizations (IV+OV)
S/MIME certificate to sign/encrypt email messages.
Includes:
• Your email address(es)
• Your personal information
• Information of your associated organization.

Selected
Free

Enter your email address

Email Addresses
Include one or more email addresses in your certificate.
email: port@ipt.pt

Next

s.ipt
Centro de Informática e Sistemas

Repare que os seus dados, por enquanto, não se encontram pré-preenchidos. Por esse motivo terá de enviar uma prova de que a sua solicitação é fidedigna.

Além de colocar o seu **Nome, País, Cidade (tomar), Endereço (IPT)**, terá de enviar um **documento (pdf)** com informação que identifique quem origina o pedido.

1 Confirm that your personal information is accurate

My personal information (Given name and Surname) is accurate and fully matches (letter-by-letter) the information in the uploaded identity document.

Given name (in latin characters) Surname (in latin characters)

Paulo Crispim

Country Address

Portugal Rua...

Please fill at least one of the following (required)

City State or province

tomar state is required for USA, Canada, and Mexi

2 Upload identity documents

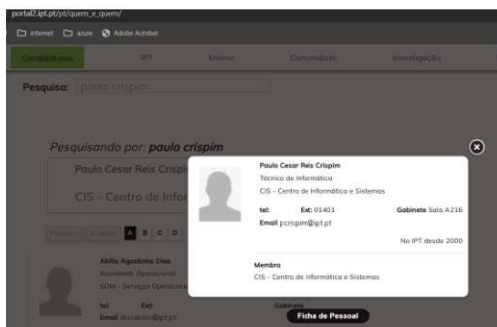
Upload a personal identification card, passport, driver's license, or other form of government generated photo I.D.

Cartão_de_Cidadão... Select file

Back Next

No 'quem é quem' (https://portal2.ipt.pt/pt/quem_e_quem/), na página web do IPT (www.ipt.pt), procure pelo seu nome e execute a impressão/cópia da sua ficha pessoal (**imprima o ecrã ou copie os dados da sua ficha pessoal**) para um documento, **grave-o como PDF ou JPG** e envie-o escolhendo 'Select file' em 'Upload identity Documents'.

Centro de informática e Sistemas do Instituto Politécnico de Tomar
Certificados Pessoais– Guia de utilizador Versão 14112017 Revisão 12042025



Após escolher 'Next', ser-lhe-á mostrada a **informação** que irá ser **enviada**.

Concorde a submissão dos dados e carregue em '**Submit**', após com ter lido os **termos de uso**, a **política de Certificação e declaração de práticas decorrentes do processo de certificação** bem como a sua **concordância** com o tratamento de dados tal como consta na **declaração de privacidade**.

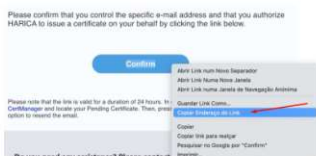
Após este passo terá de validar o seu email e esperar que um dos responsáveis do **Centro de Informática e Sistemas** pela validação dos certificados, confirme a informação que enviou.

Para **validar** o seu **email**, carregue no botão '**Confirm**' com a sua sessão na HARICA ativa e volte a carregar no botão '**Confirm**' na janela que se abriu no seu navegador.

Validate your email address



Se cliente de email que usa não permitir essa ação, copie o endereço e cole-o no navegador que tem a sessão na HARICA ativa.



Após o seu pedido de Certificado Digital Pessoal ter sido aprovado (recebe um email a indicar a aprovação ou a recusa), volte a aceder a <https://cm.harica.gr/> e execute '**enroll your Certificate**'.

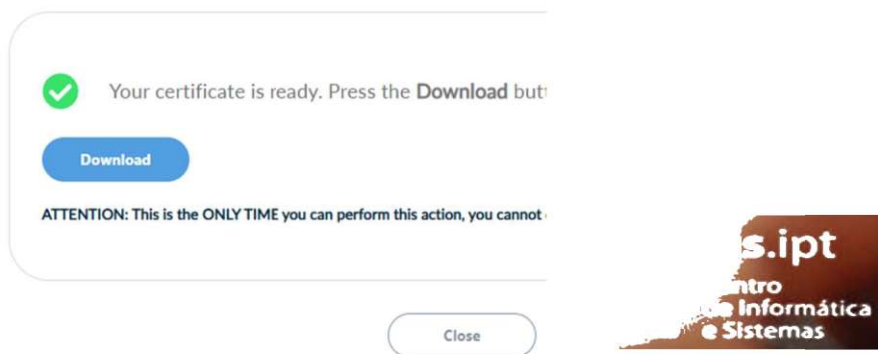


Para geral o seu Certificado Digital Pessoal, mantenha o algoritmo e prefira uma chave de **4096** bit. Defina um **Pin com 8** caracteres numéricos e escolha '**Enroll Certificate**'

Quando aparecer a indicação de que o **Certificado** se encontra **pronto**, carregue em '**Download**'

A screenshot of the certificate generation and enrollment form. At the top, there are two buttons: "Generate Certificate" and "Submit CSR manually". Below them, there is a note: "Generate your certificate in .p12 format." and "Use your (already created) CSR and submit it here". The main section is titled "Set a passphrase to protect your certificate. Please note that the passphrase is required to use the certificate and should therefore be secured and not forgotten." It contains a dropdown menu for "Algorithm" (RSA (default)) and a dropdown menu for "Key size" (2048 (default), 2048 (default), 3072, 4096). A red arrow points to the "4096" option. Below the key size dropdown, there is a text input field for "Type your passphrase" with a red label "Pin com 8 caracteres". Below this is a "Confirm passphrase" section with a text input field for "Retype your passphrase" and a red label "Pin com 8 caracteres". At the bottom, there is a checkbox with the text "I understand that this passphrase is under my sole knowledge and HARICA does not have access to it." and two buttons: "Cancel" and "Enroll Certificate". A red arrow points to the "Enroll Certificate" button.

Get your certificate



Para **Instalar** o seu Certificado Digital Pessoal deve seguir o **guia** que mais se adequar ao **sistema operativo** que estiver a usar.

.....

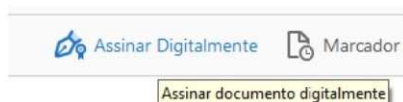
2. Usar o certificado no Acrobat Reader DC antes

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

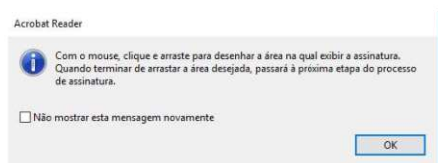
Em **Ferramentas** clicar em abrir nos certificados.



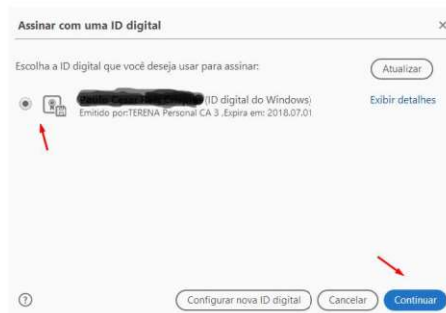
Escolher “Assinar Digitalmente”



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



Assinalar a área pretendida e escolher o certificado pretendido.

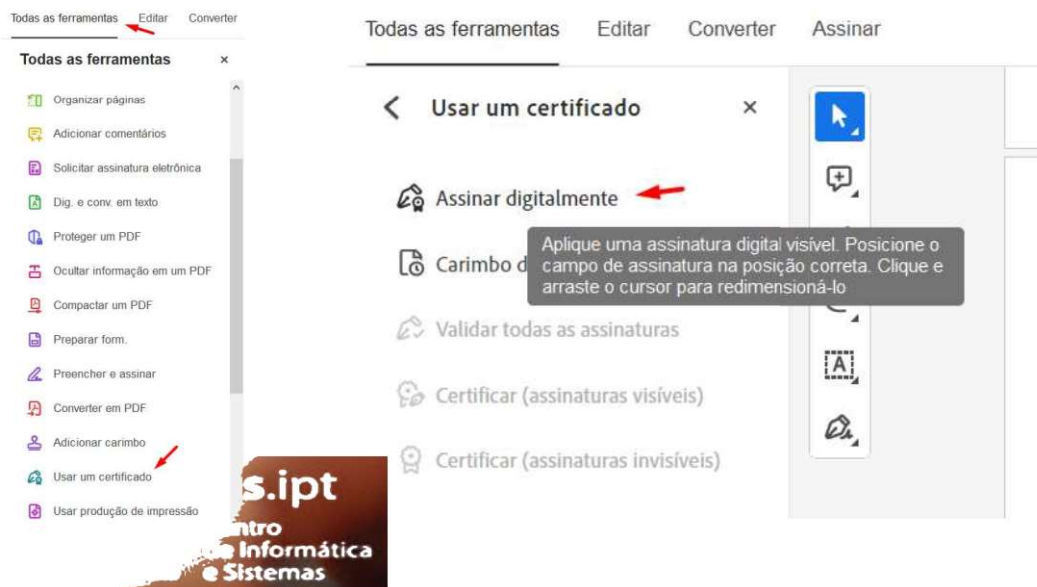


Ao apresentar o certificado, com que irá assinar o documento deverá clicar em “Assinar”, para que o documento seja assinado no espaço antes assinalado. Após a assinatura o documento terá de ser gravado e não poderá ser alterado. Um documento que seja bloqueado após assinado não poderá voltar a ser assinado.

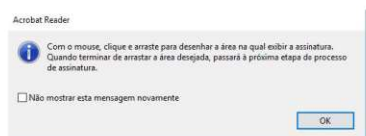


2.2. A Usar o Acrobat Reader DC na versão 2023.003.10269 ou superior

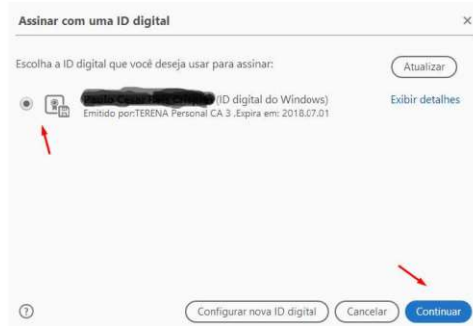
Em **Todas as Ferramentas**, no lado esquerdo escolher *‘Usar um Certificado’* (pode ser necessário carregar em Ver mais) e escolher *‘Assinar digitalmente’*.



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



Assinalar a área pretendida e escolher o certificado pretendido.



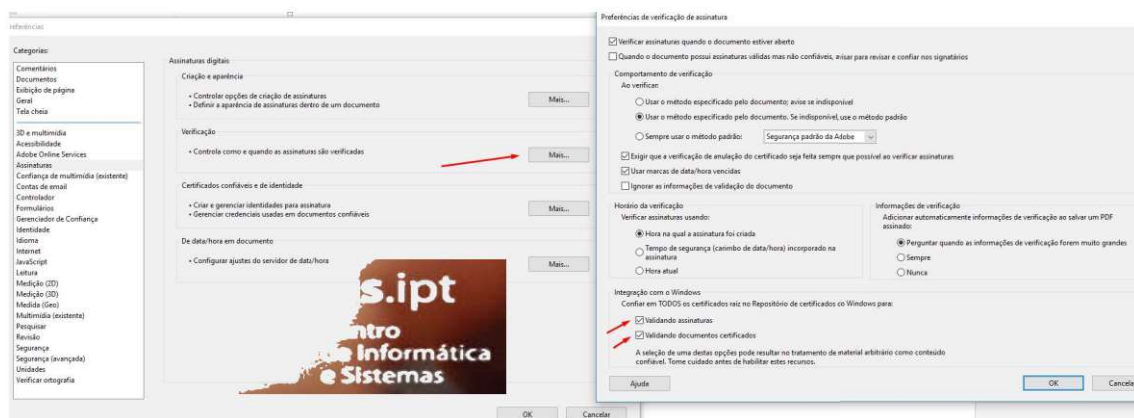
Ao apresentar o certificado, com que irá assinar o documento deverá clicar em *“Assinar”*, para que o documento seja assinado no espaço antes assinalado. Após a assinatura o documento terá de ser gravado e não poderá ser alterado. Um documento que seja bloqueado após assinado não poderá voltar a ser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



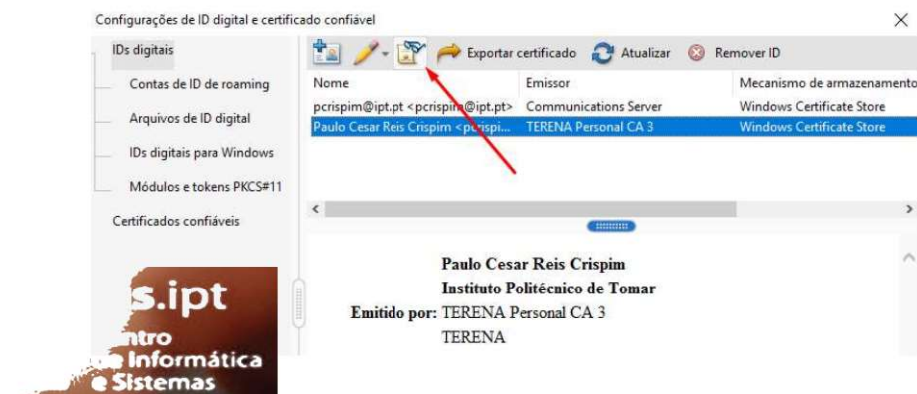
Na caixa “*Integração com o Windows*” marcar “*validando assinaturas*” “*validando documentos certificados*”.

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

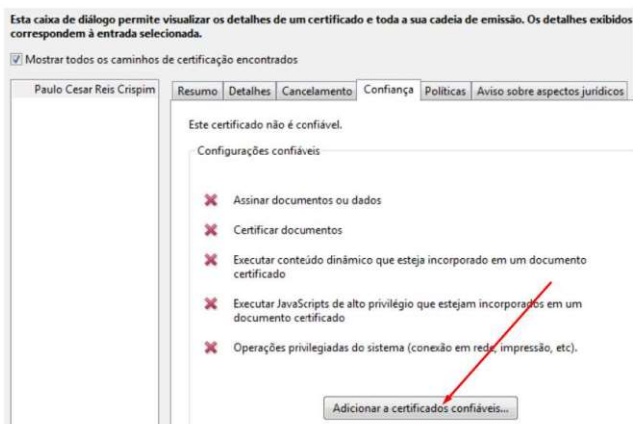
3.2. Inclusão do certificado digital nas assinaturas confiáveis do Acrobat Reader

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...”



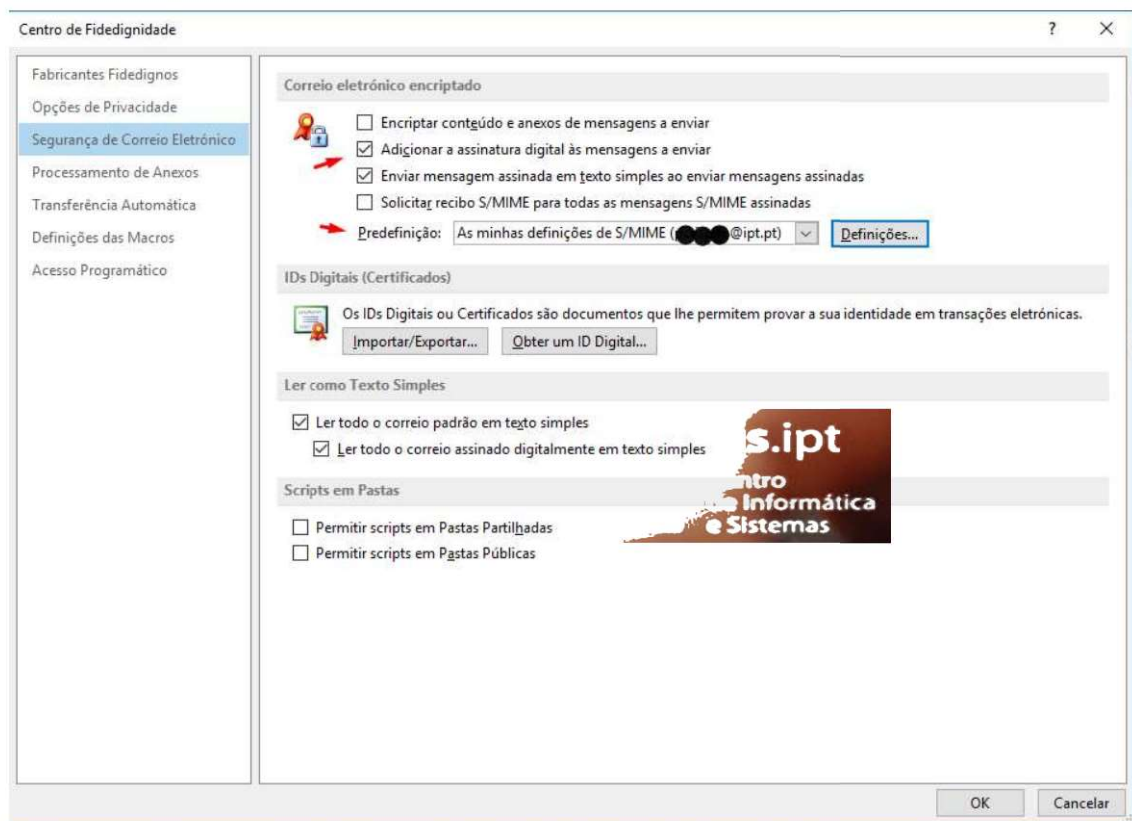
Em resultado, o documento certificado apresenta sinalizado a verde a validade da assinatura



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”*

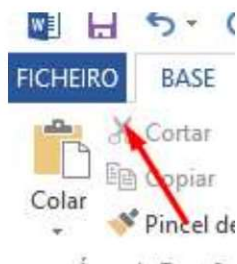
Carregue em **Definições** e verifique se o certificado pretendido é o que está por defeito. No caso de não ser escolha o pretendido e carregue em **OK**.

Feche as restantes janelas com **OK**.

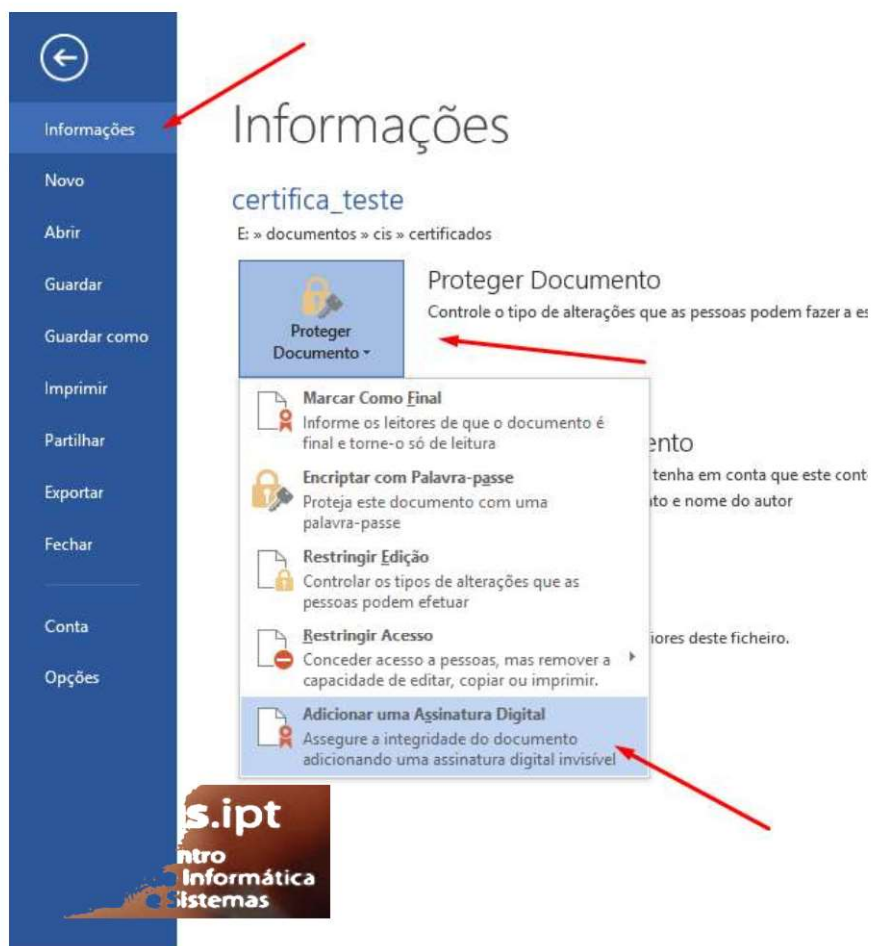
.....

5. Assinar digitalmente um documento do Microsoft Word

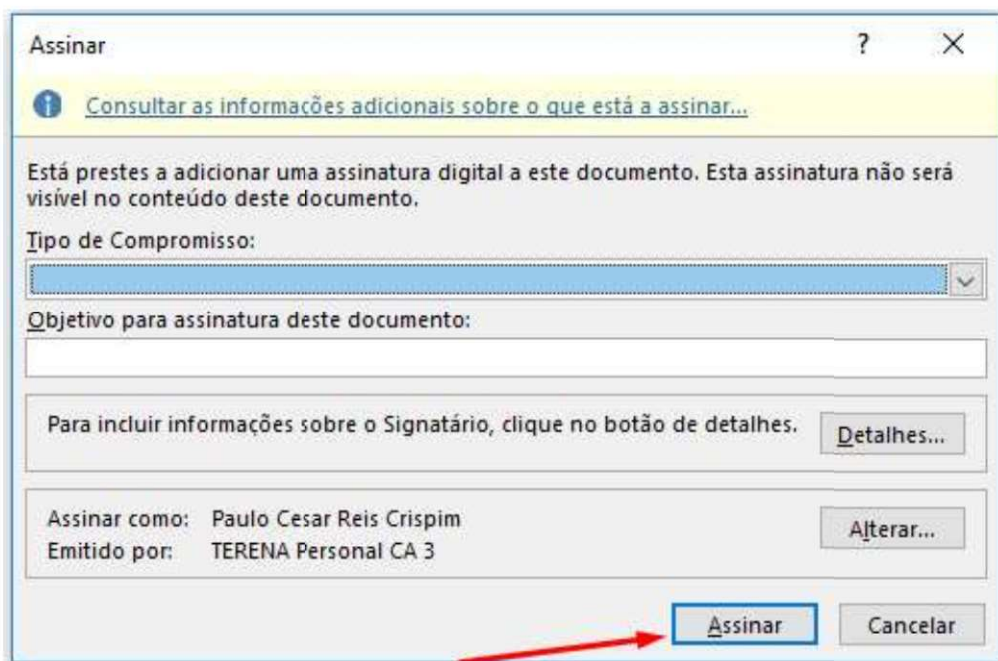
Após gravar o documento, para o assinar digitalmente terá de ir a ficheiro.



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”.

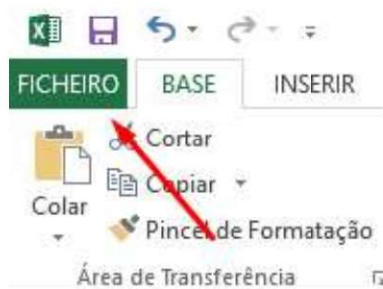


No caso de o documento ser alterado ou gravado após a assinatura, a assinatura será removida.

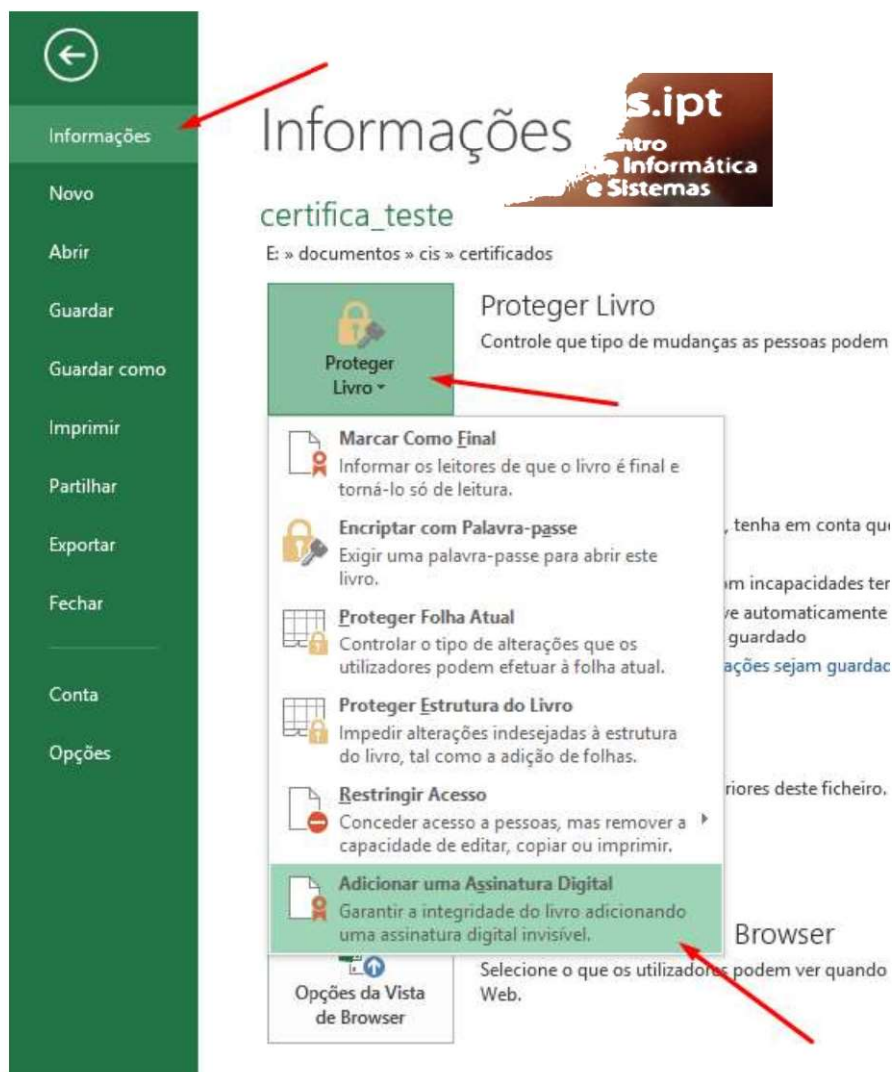
.....

6. Assinar digitalmente um documento do Microsoft Excel

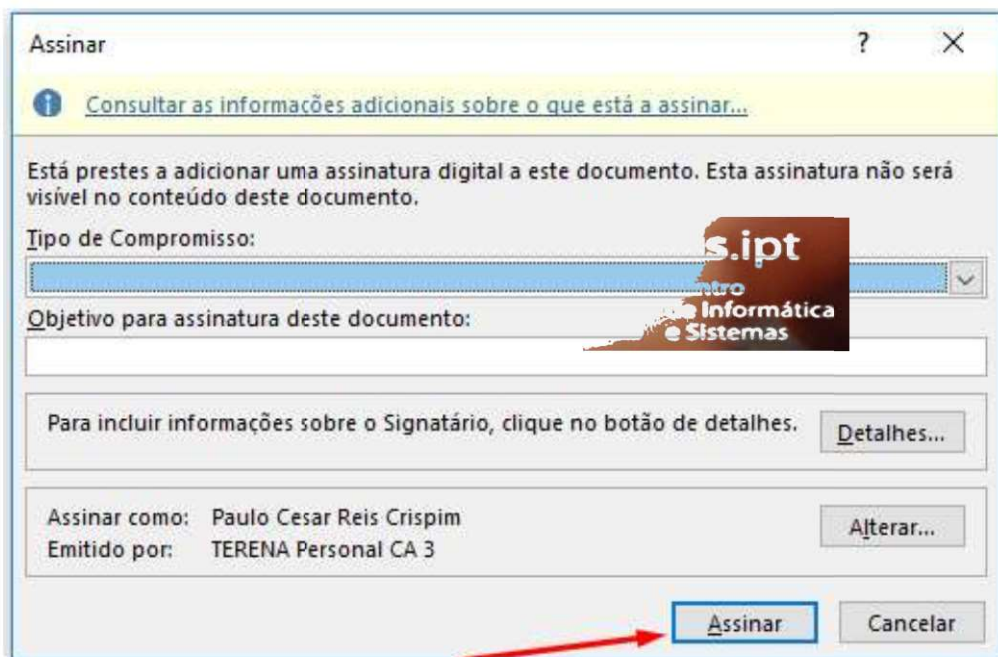
Após gravar o documento, para o assinar digitalmente terá de ir a ficheiro.



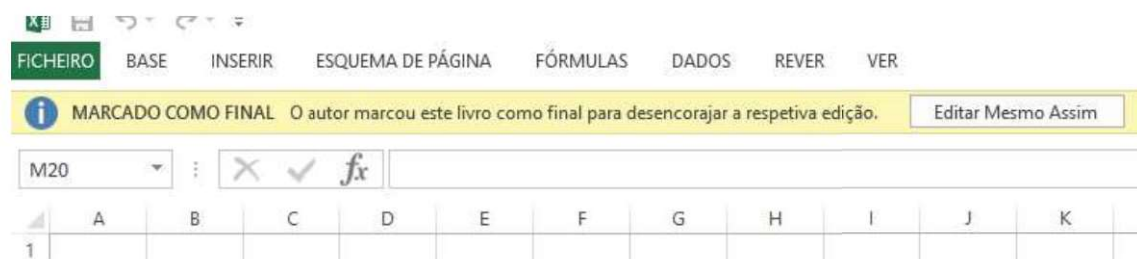
Escolher Informações, “proteger Documento” e escolher a opção “Adicionar uma assinatura Digital”



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 Mozilla Firefox para o Microsoft Windows

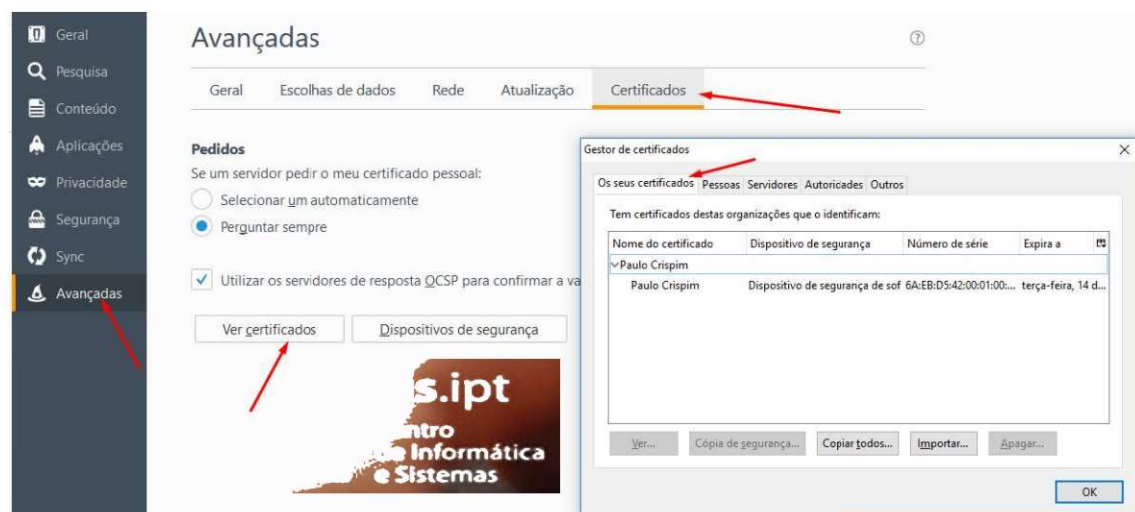
7.1. Exportar o certificado do Mozilla Firefox até à versão 68

Carregar no icon do “menu” e escolher icon “opções”



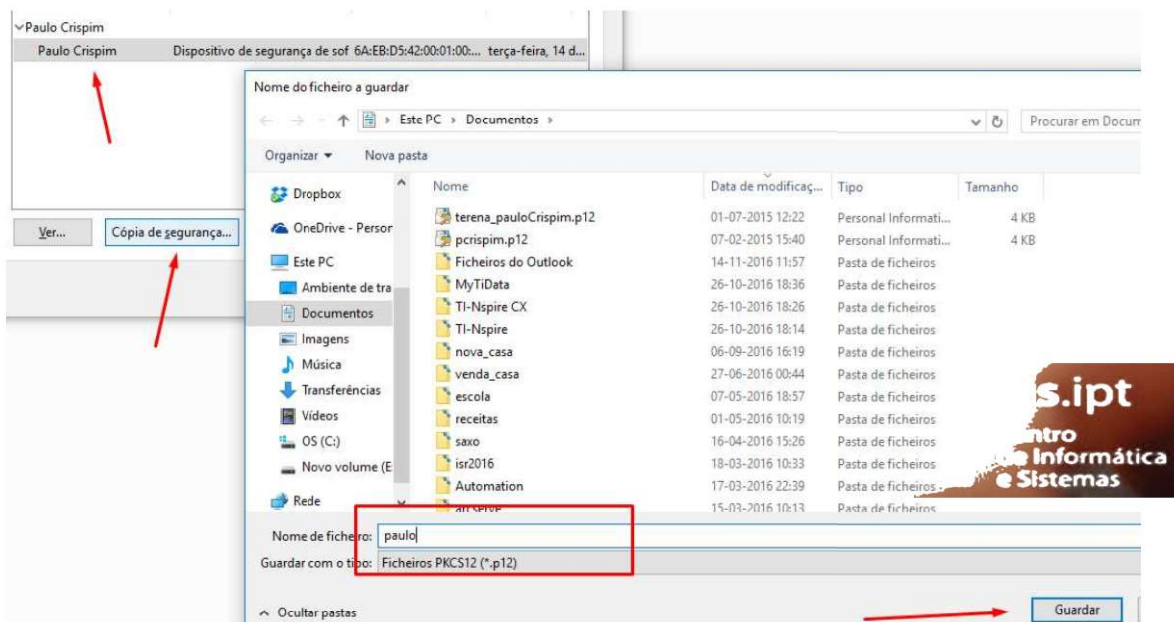
Nas opções escolher “Avançadas”, “Certificados” e carregar no botão “Ver certificados”.

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

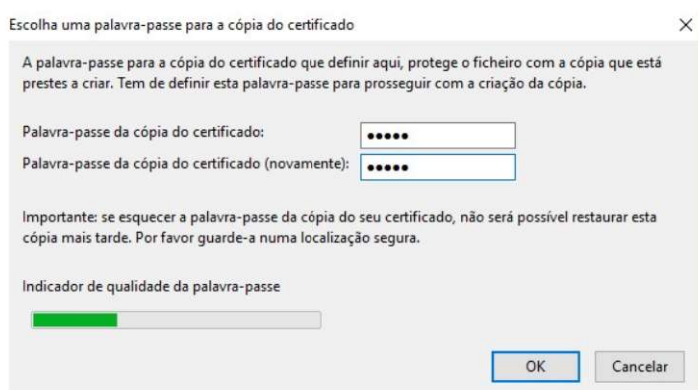


Ainda na janela do “Gestor de certificados” terá de marcar o certificado pretendido e escolher o botão “Cópia de segurança”.

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



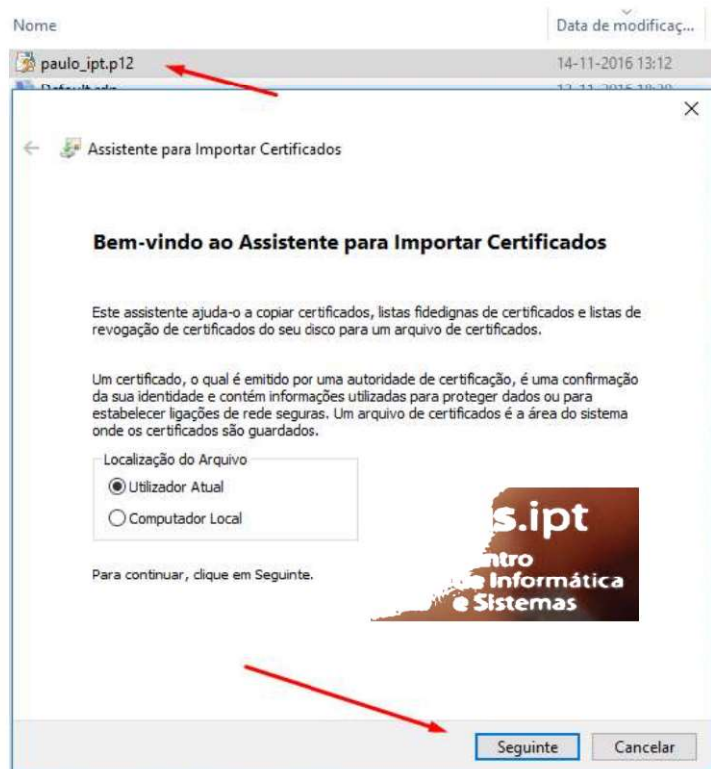
A palavra-passe a usar para proteger o certificado convém que seja simples. Ao carregar no botão “OK” a sua cópia do certificado ficará gravada na localização, acima, escolhida.



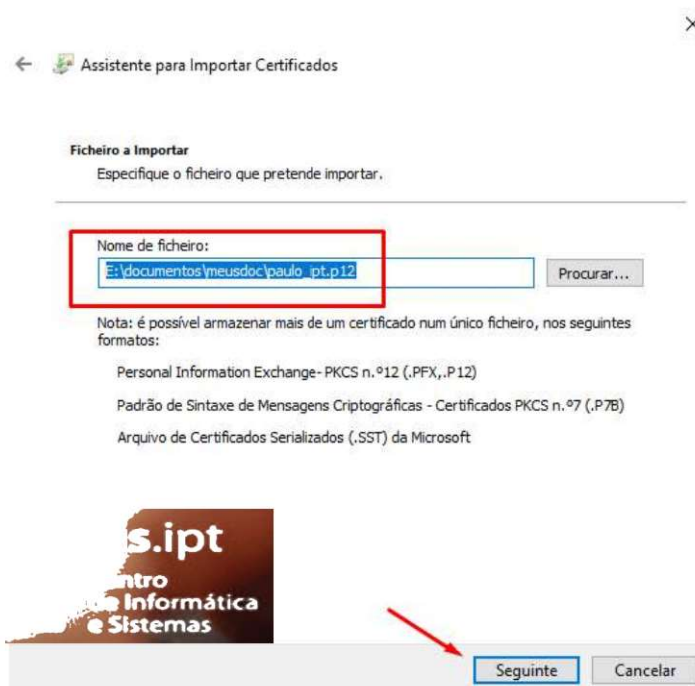
7.2. Importar o certificado para o Windows

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

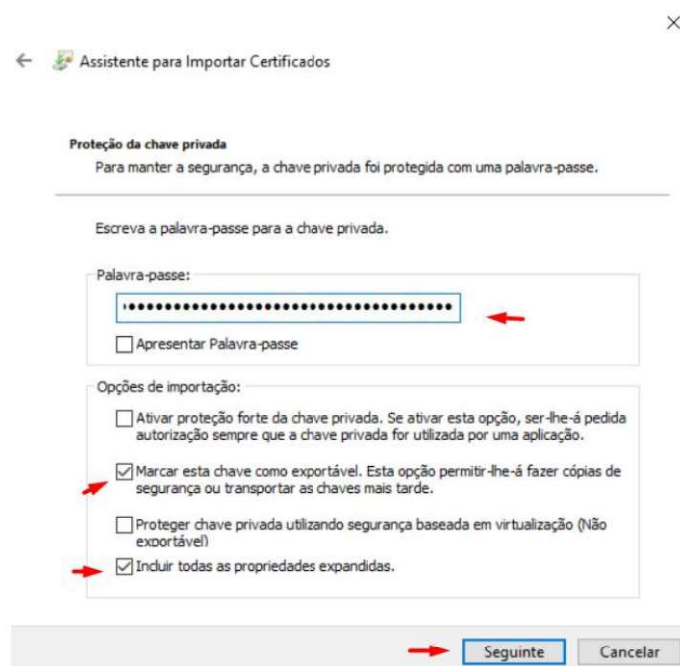
Clicar nele duas vezes a fim de ser executado.



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”.



Assistente para Importar Certificados

Proteção da chave privada
Para manter a segurança, a chave privada foi protegida com uma palavra-passe.

Escreva a palavra-passe para a chave privada.

Palavra-passe:
[Campo de texto com pontos] [Seta vermelha apontando para o campo]

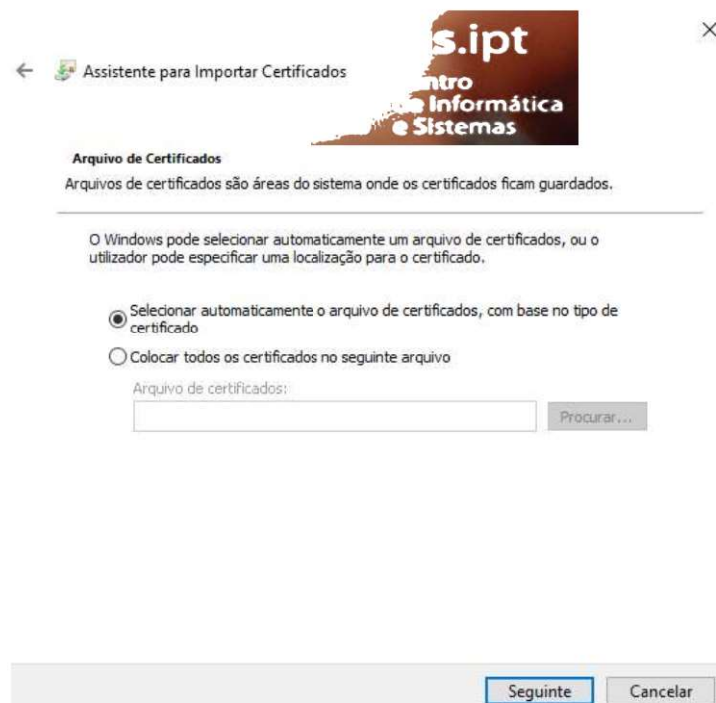
☐ Apresentar Palavra-passe

Opções de importação:

- ☐ Ativar proteção forte da chave privada. Se ativar esta opção, ser-lhe-á pedida autorização sempre que a chave privada for utilizada por uma aplicação.
- ☒ Marcar esta chave como exportável. Esta opção permitir-lhe-á fazer cópias de segurança ou transportar as chaves mais tarde. [Seta vermelha apontando para a opção]
- ☐ Proteger chave privada utilizando segurança baseada em virtualização (Não exportável)
- ☒ Incluir todas as propriedades expandidas. [Seta vermelha apontando para a opção]

[Seta vermelha apontando para o botão] **Seguinte** Cancelar

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



Assistente para Importar Certificados

Arquivo de Certificados
Arquivos de certificados são áreas do sistema onde os certificados ficam guardados.

O Windows pode selecionar automaticamente um arquivo de certificados, ou o utilizador pode especificar uma localização para o certificado.

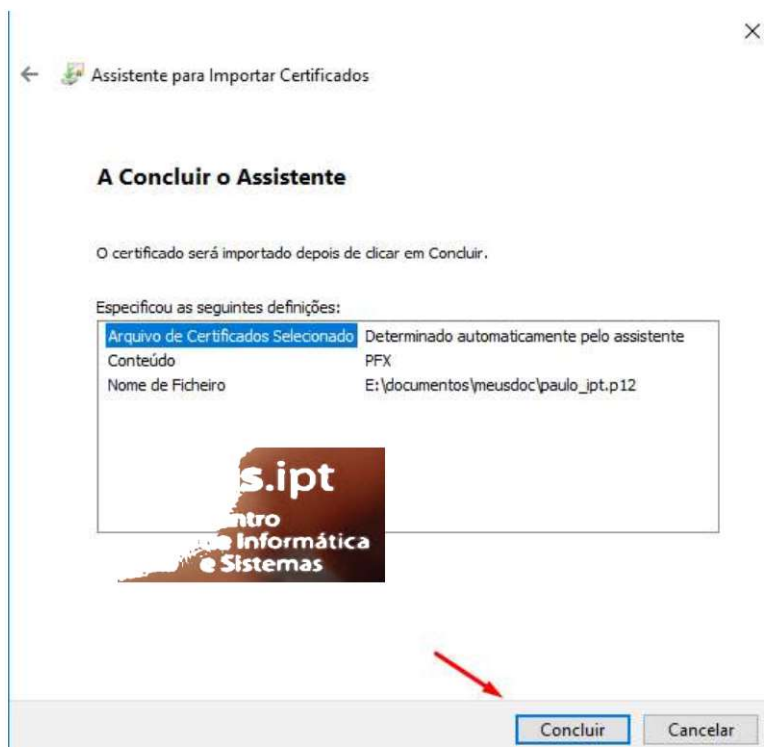
☒ Selecionar automaticamente o arquivo de certificados, com base no tipo de certificado

☐ Colocar todos os certificados no seguinte arquivo

Arquivo de certificados:
[Campo de texto] Procurar...

Seguinte Cancelar

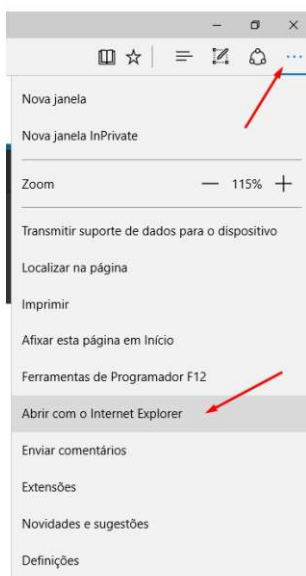
Após a apresentação do sumário da instalação do certificado deve carregar no botão “Concluir”.



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**.



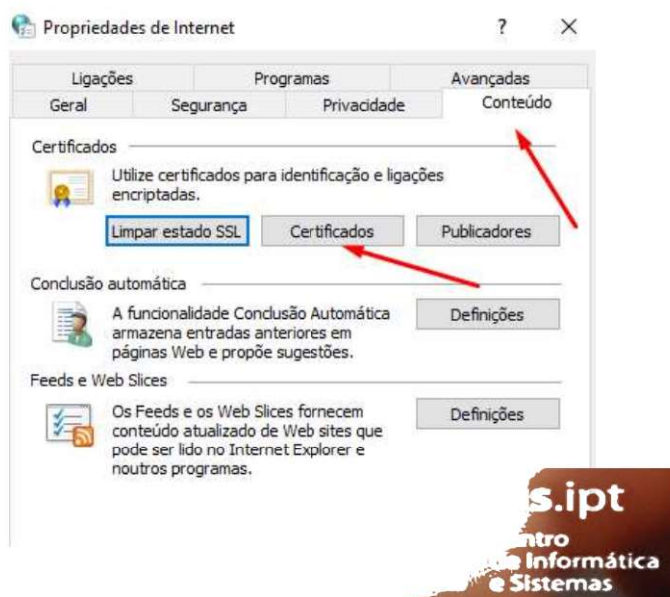
.....

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

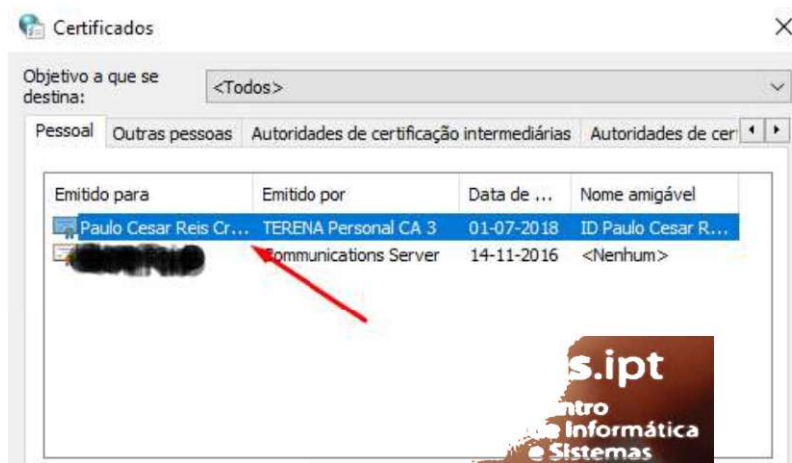
Abrir o **Painel de Controlo** e procurar a aplicação **Opções da Internet**.



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.



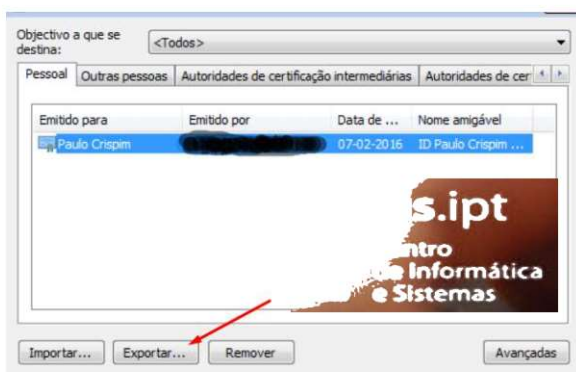
10. Exportar certificado com chave privada da árvore do Microsoft Windows

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

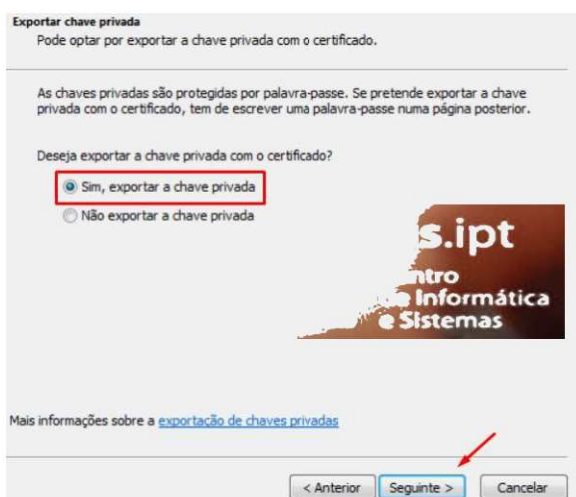
Abrir o **Painel de Controlo** e procurar a aplicação **Opções da Internet**.

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

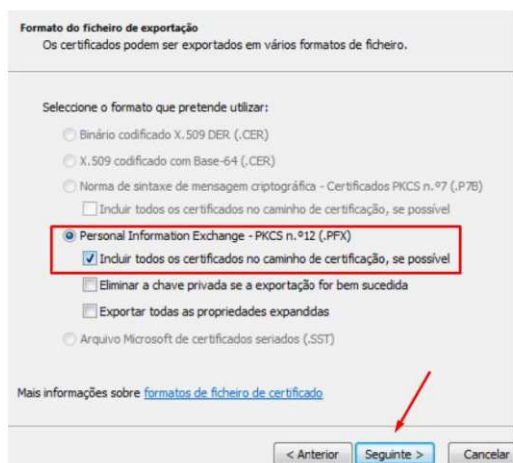
Na janela do Gestor de **Certificados** escolha o separador “Pessoal”, marque o certificado desejado e carregue no **botão “Exportar”**.



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



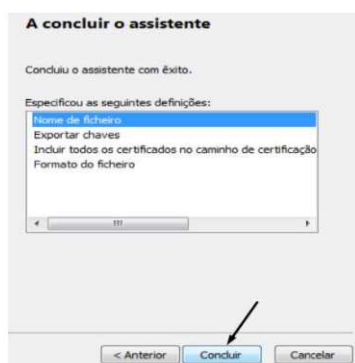
No ecrã seguinte marque a opção PKCS12 (.pfx) e inclua a opção secundária que permite incluir todos os certificados no mesmo ficheiro PKCS12.



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

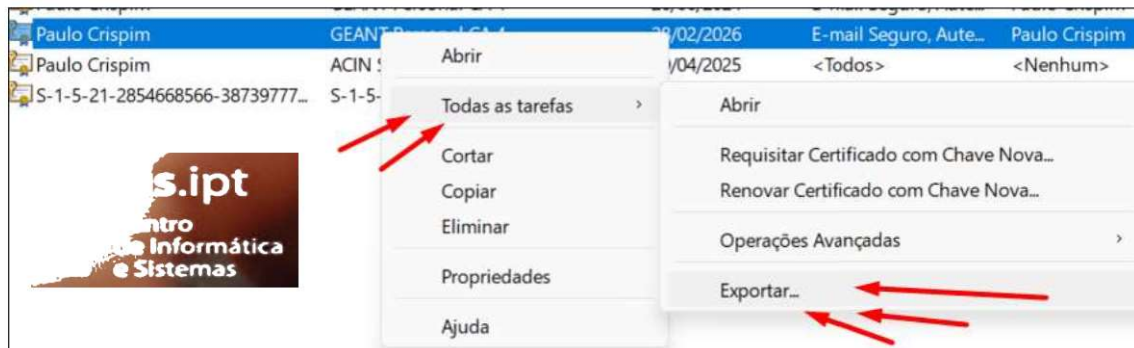
No **procurar** escreva *certmgr.msc* e **abra-o** quando lhe aparecer



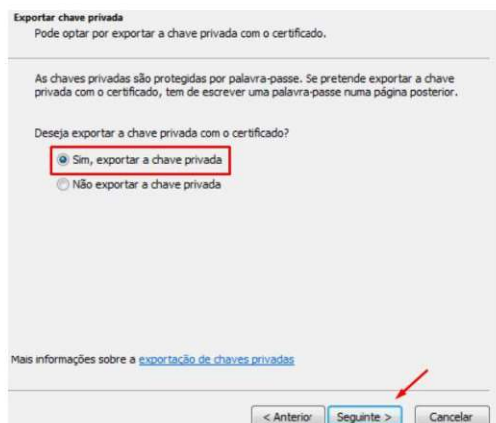
Escolha o certificado que se encontra a usar e se tiver mais do que 1 válido, escolha o que tiver a da de expiração mais avançada.

Certificados - Utilizador atual	Emitido para	Emitido por	Data da expiraç...	Objetivos a que se ...	Nome amigável
▼ Pessoal					
▼ Certificados					
▼ Autoridades de certificação de	6fa0ca4c-56c4-415c-a053-93a57...	Microsoft Intune MDM Device CA	12/12/2023	Autenticação de die...	<Nenhum>
▼ Confiança de Empresa	6fa0ca4c-56c4-415c-a053-93a57...	Microsoft Intune MDM Device CA	24/05/2025	Autenticação de die...	<Nenhum>
▼ Autoridades de certificação in	c6138274-cea8-4133-87cc-002e2...	MS-Organization-Access	14/12/2032	Autenticação de die...	<Nenhum>
▼ Objeto de utilizador do Active	Paulo Crispim	GEANT Personal CA 4	26/06/2024	E-mail Seguro, Aute...	Paulo Crispim
▼ Fabricantes fi	Paulo Crispim	GEANT Personal CA 4	28/02/2026	E-mail Seguro, Aute...	Paulo Crispim
	Paulo Crispim	ACIN Sub Root CA	20/04/2025	<Todos>	<Nenhum>

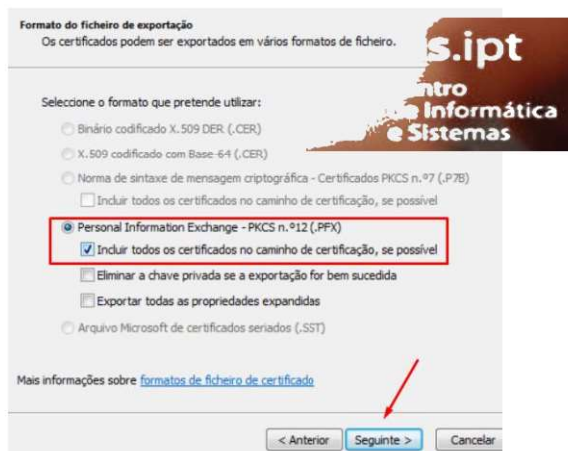
Carregue com o **botão** do rato do **lado direito** sobre o certificado escolhido e em todas as **tarefas** escolha **exportar**.



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.



Formato do ficheiro de exportação
Os certificados podem ser exportados em vários formatos de ficheiro.

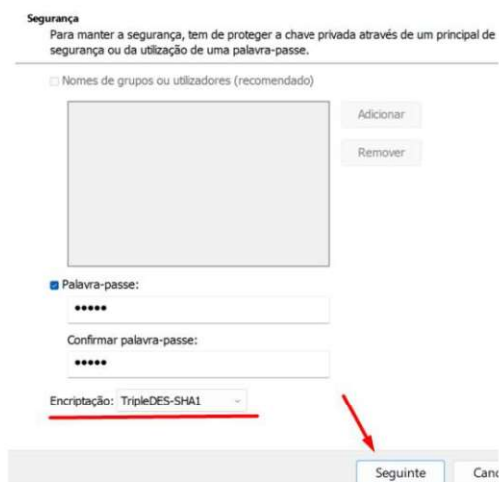
Selecione o formato que pretende utilizar:

- ☐ Binário codificado X.509 DER (.CER)
- ☐ X.509 codificado com Base-64 (.CER)
- ☐ Norma de sintaxe de mensagem criptográfica - Certificados PKCS n.º7 (.P7B)
 - ☐ Incluir todos os certificados no caminho de certificação, se possível
- ☒ Personal Information Exchange - PKCS n.º12 (.PFX)
 - ☒ Incluir todos os certificados no caminho de certificação, se possível
 - ☐ Eliminar a chave privada se a exportação for bem sucedida
 - ☐ Exportar todas as propriedades expandidas
- ☐ Arquivo Microsoft de certificados serializados (.SST)

Mais informações sobre [formatos de ficheiro de certificado](#)

< Anterior Seguinte > Cancelar

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**.



Segurança

Para manter a segurança, tem de proteger a chave privada através de um principal de segurança ou da utilização de uma palavra-passe.

☐ Nomes de grupos ou utilizadores (recomendado)

Adicionar
Remover

☒ Palavra-passe:

Confirmar palavra-passe:

Encriptação: TripleDES-SHA1

Seguinte Cancelar

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.



Ficheiro a exportar

Especifique o nome do ficheiro que pretende exportar

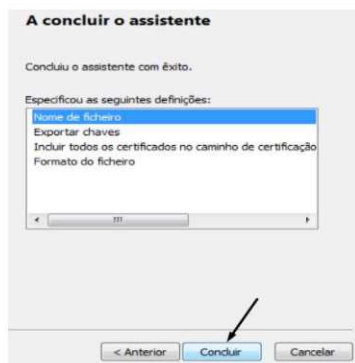
Nome de ficheiro:

E:\certificado_e_chaveprivada.pfx Procurar...

s.ipt
Centro de Informática e Sistemas

< Anterior Seguinte > Cancelar

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



.....

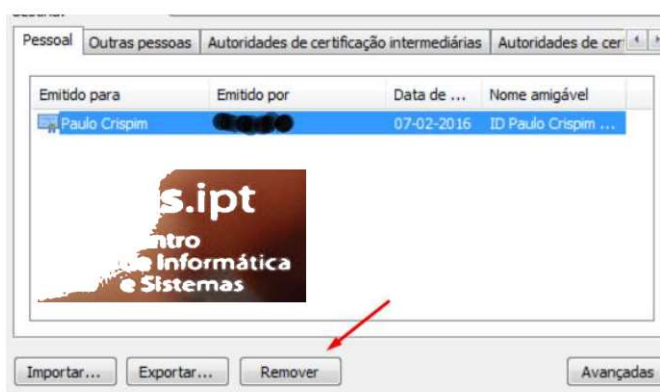
11. Remover certificado com chave privada

11.1 Remoção de certificado no Windows

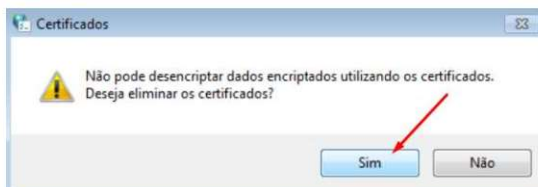
Abrir o **Painel de Controlo** e procurar a aplicação **Opções da Internet**.

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

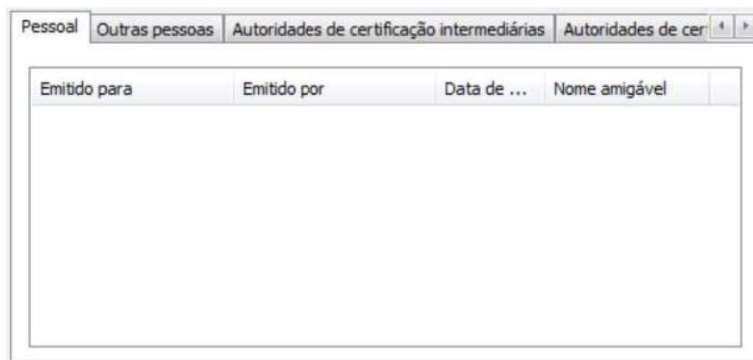
Na janela do Gestor de **Certificados** escolha o separador “Pessoal”, marque o certificado desejado e carregue no **botão** “Remover”.



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.



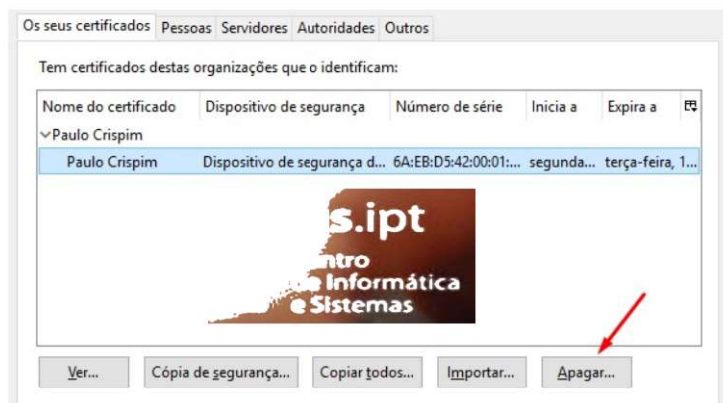
11.2 Remoção de certificado no Mozilla Firefox

Carregar no ícone do “menu” e escolher ícone “opções”

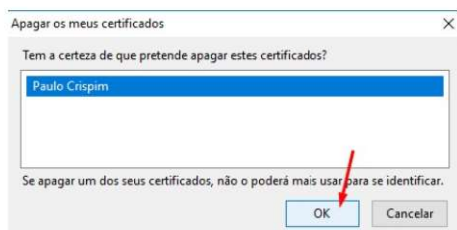
Nas opções escolher “Avançadas”, “Certificados” e carregar no botão “Ver certificados”.

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”**.



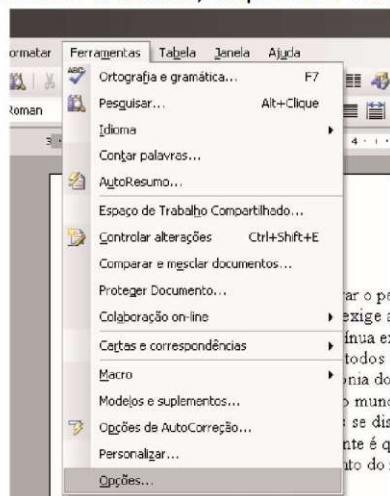
Na janela do Gestor de **Certificados**, verifique que o certificado já se encontra removido.



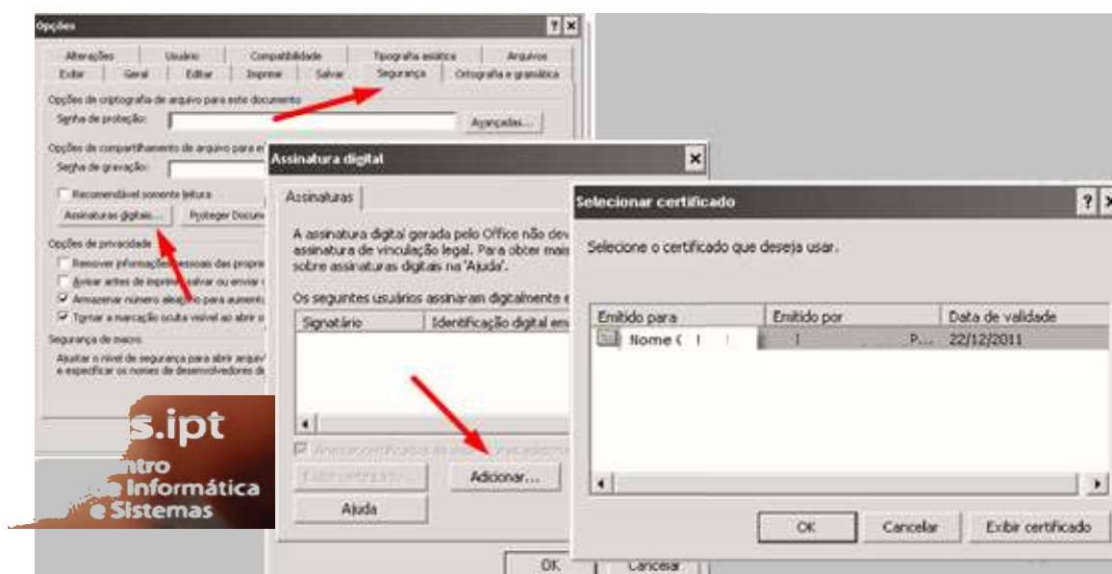
.....

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



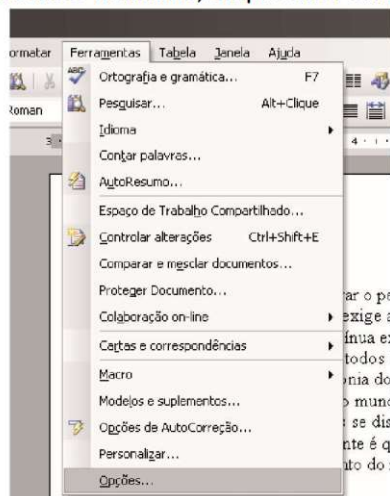
A pós assinado, aparecerá um ícone vermelho na barra de estado a informar que o documento foi assinado:



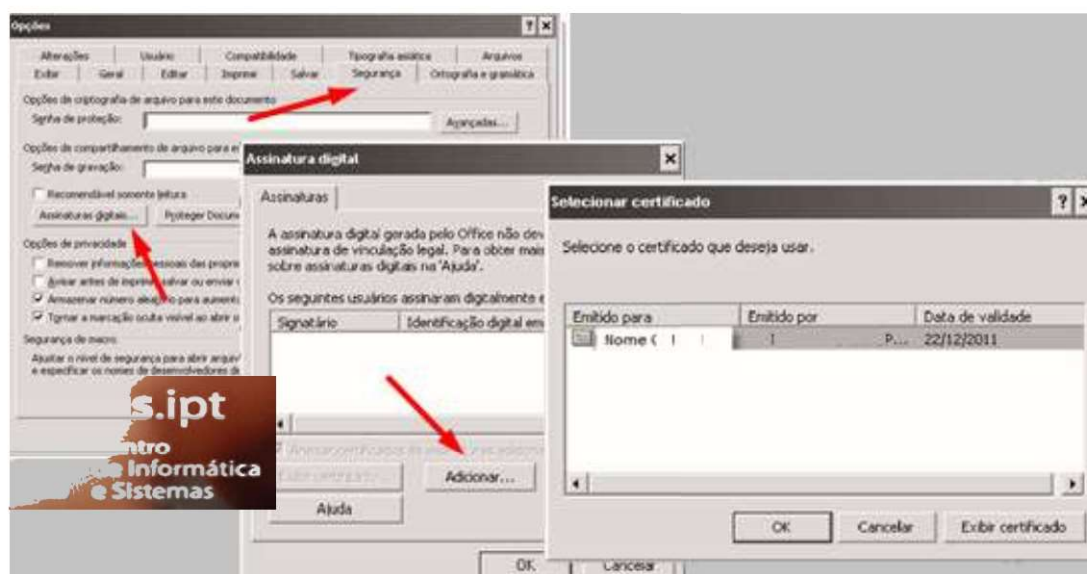
No caso de o documento ser alterado ou gravado após a assinatura, a assinatura será removida.

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:

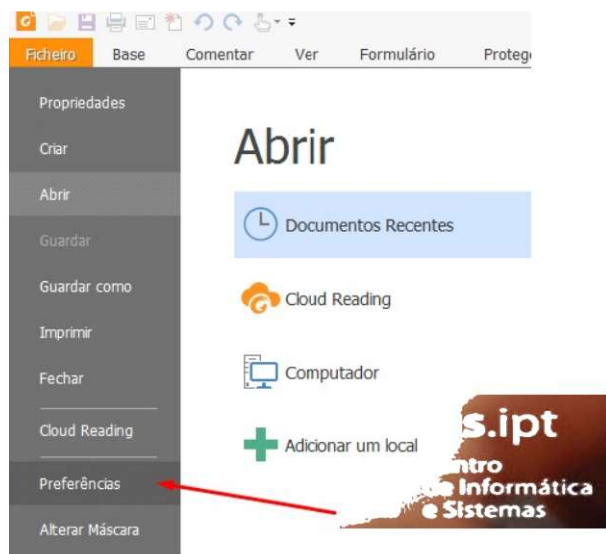


No caso de o documento ser alterado ou gravado após a assinatura, a assinatura será removida.

14. USAR O CERTIFICADO NO FOXIT

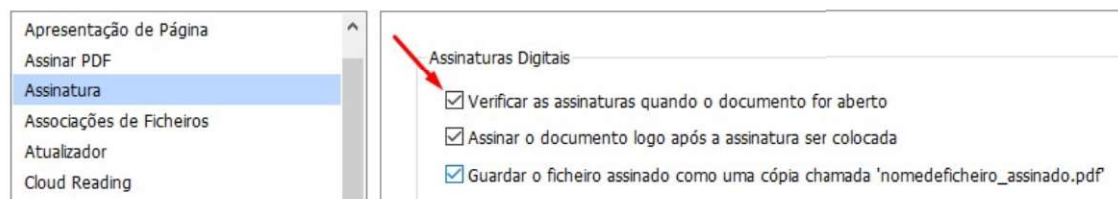
14.1. Configurar o foxit para verificar as assinaturas de forma automática

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



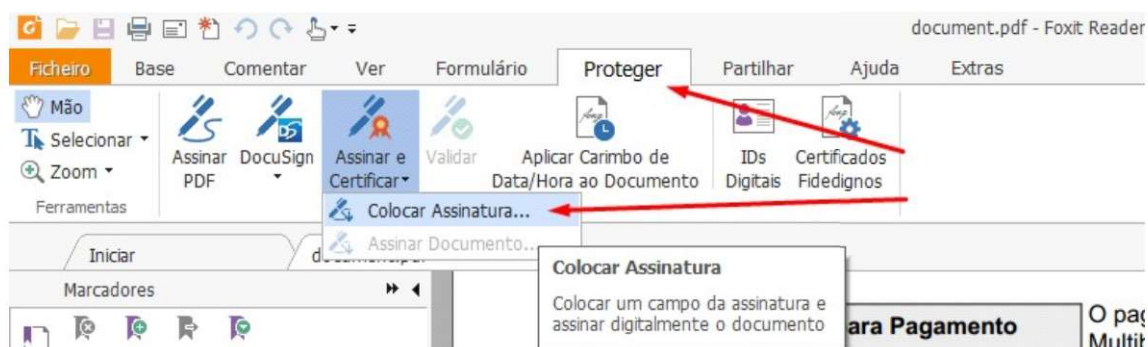
Escolher “Assinatura” e no painel direito marcar todas as opções que lhe são apresentadas. A marcação da opção “Verificar as assinaturas quando o documento for aberto” imprescindível.

Preferências

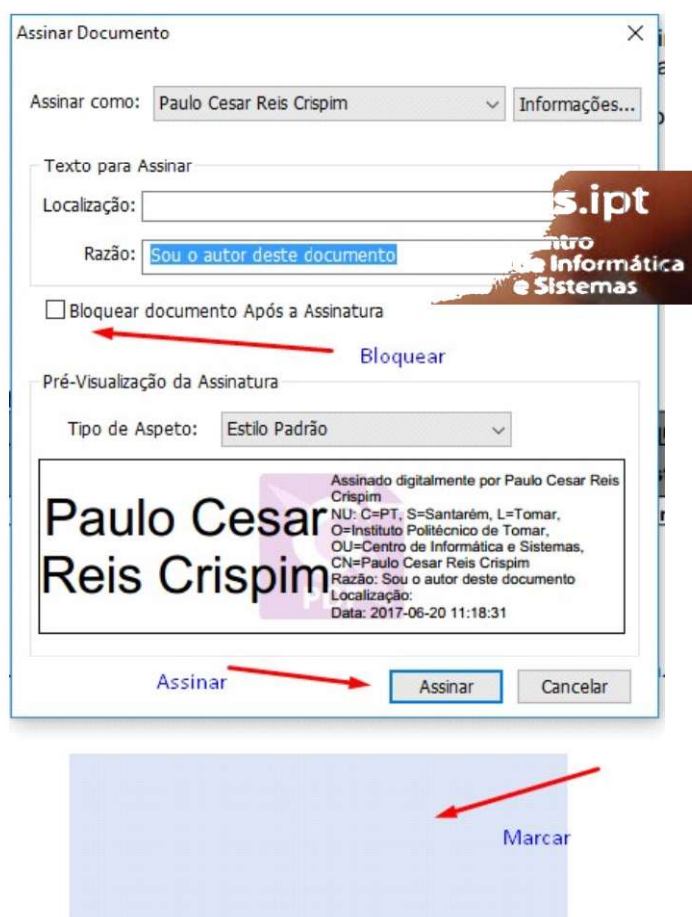


14.2. Assinar documentos

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 ADOBE 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.

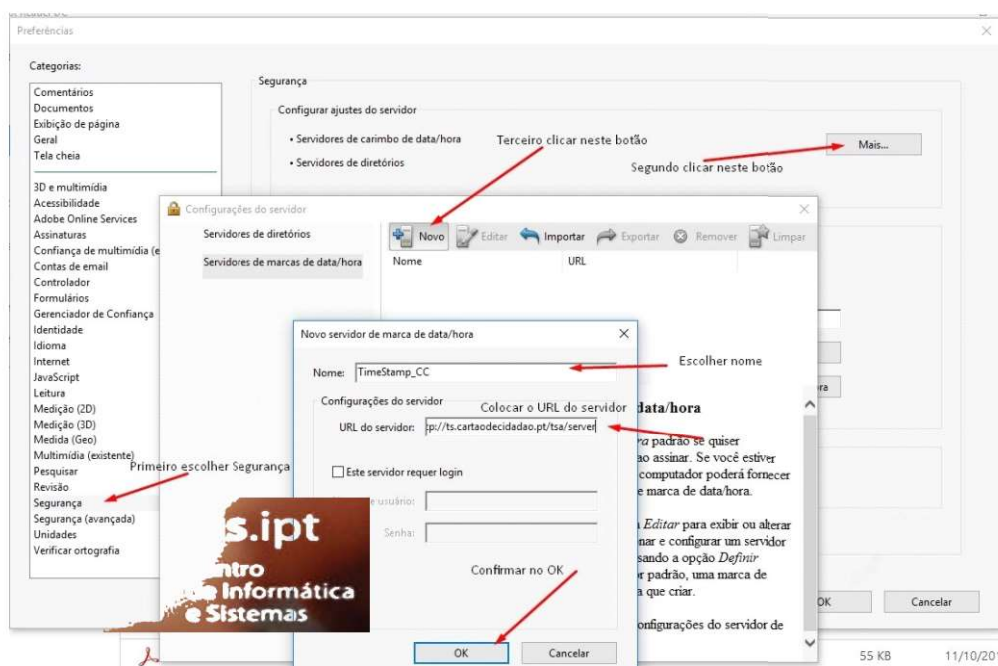
Ao apresentar o certificado, com que irá assinar o documento deverá clicar em *“Assinar”*, para que o documento seja assinado no espaço antes assinalado. Após a assinatura o documento terá de ser gravado e não poderá ser alterado. Um documento que seja bloqueado após assinado não poderá voltar a ser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

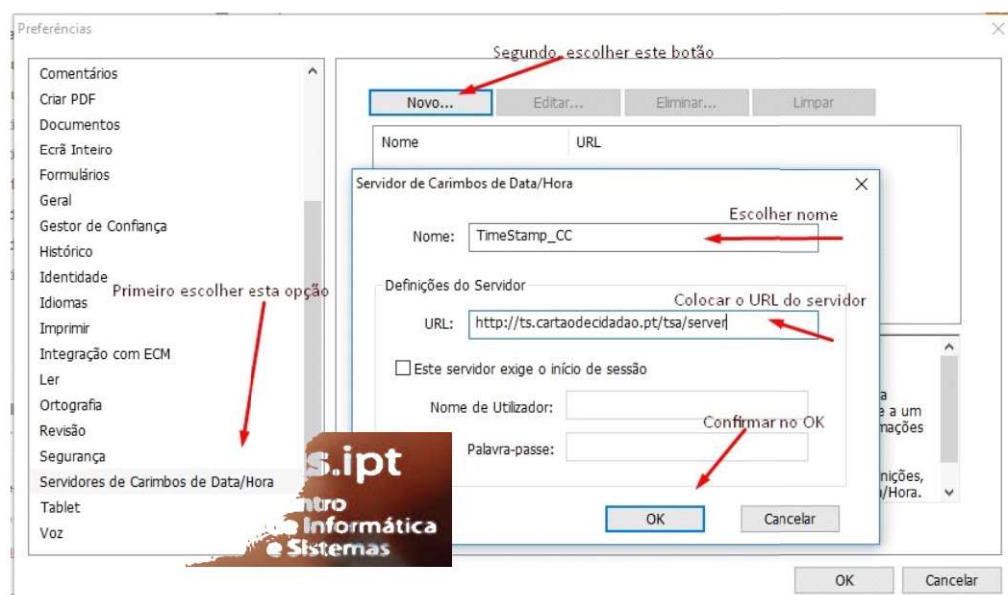


Depois de ter fechado a janela “*Configurações do Servidor*” na **Cruz**, deverá fechar a janela de “*preferências*” no botão “**OK**”.

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**.

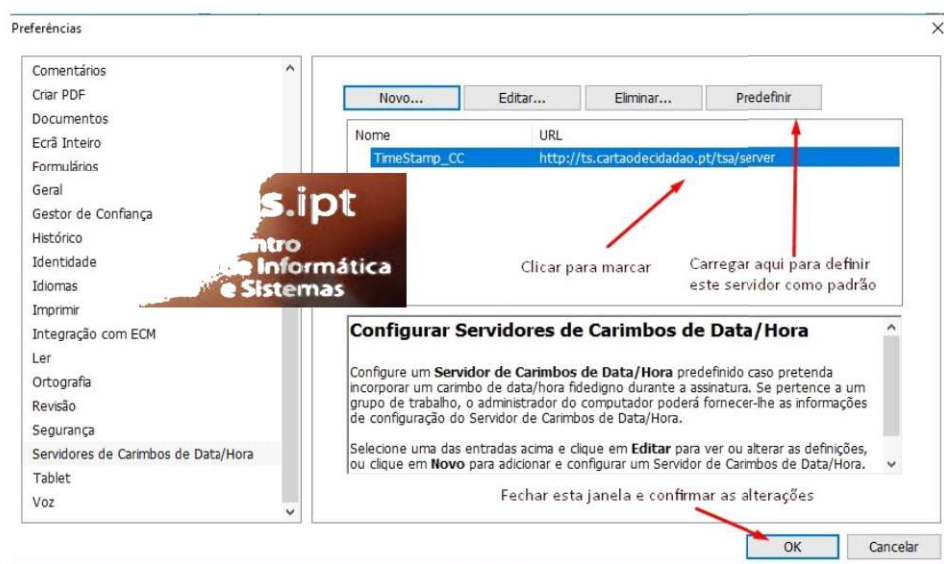
16.2. No FoxIT Reader

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



Na caixa “*Servidor de Carimbo de Data/Hora*”, escolher o nome que pretende com que fique identificado o **TimeStamp Server** e no URL do Servidor deverá colocar **<http://ts.cartao decidadao.pt/tsa/server>**

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

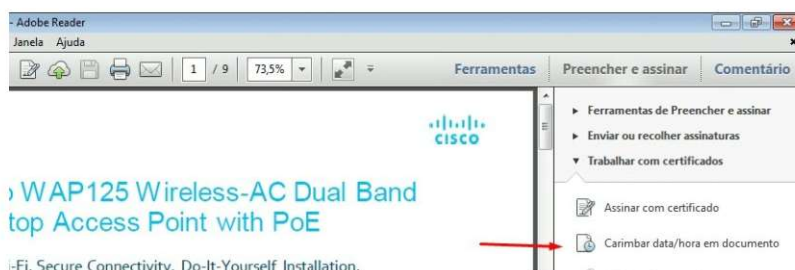


Depois de ter fechado a janela anterior, deverá clicar na linha a que corresponde o **TimeStamp Server** para o marcar. Após ter sido marcado irá predefini-lo, carregando no botão “*predefinir*”. Para fechar a janela de “*preferências*”, carregue no botão “*OK*”.

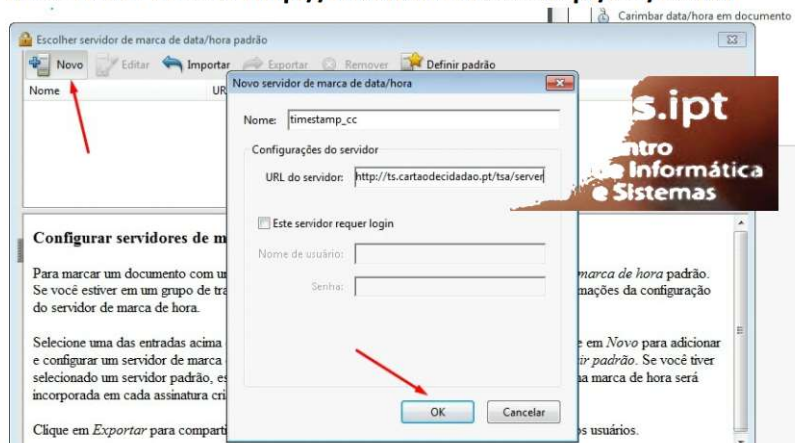
O Objetivo desta operação é, de cada vez que a **assinatura digital** for usada o documento irá levar uma marcação com **data e hora** do servidor de **TimeStamp**. Quando não existe este tipo de configuração, a **data e hora** que ficam registadas na **assinatura digital** é a do **computador local**.

16.3. No Acrobat Reader 11

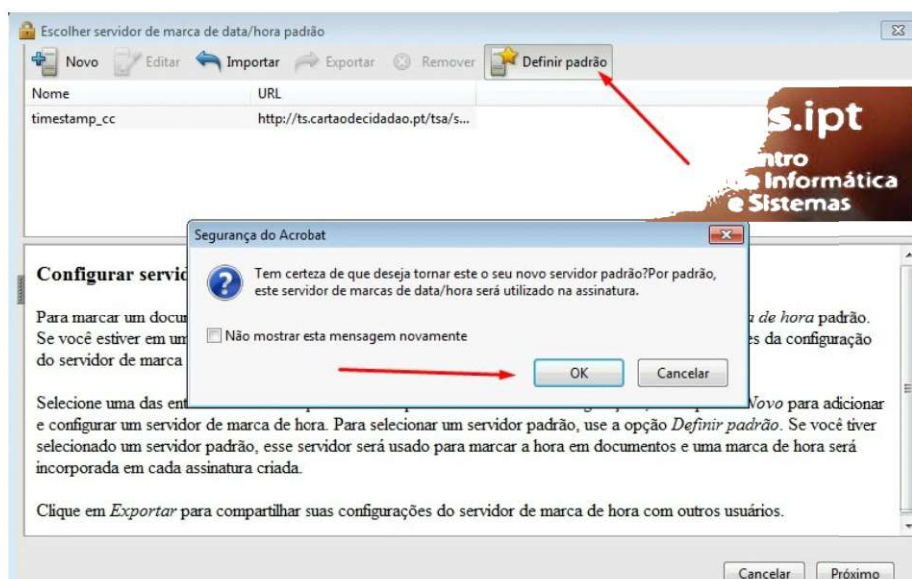
Escolher **Preencher e assinar** no canto superior direito do Acrobat Reader 11 e nos itens apresentados escolha “*Carimbar data/hora em Documento*”.



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**.

.....

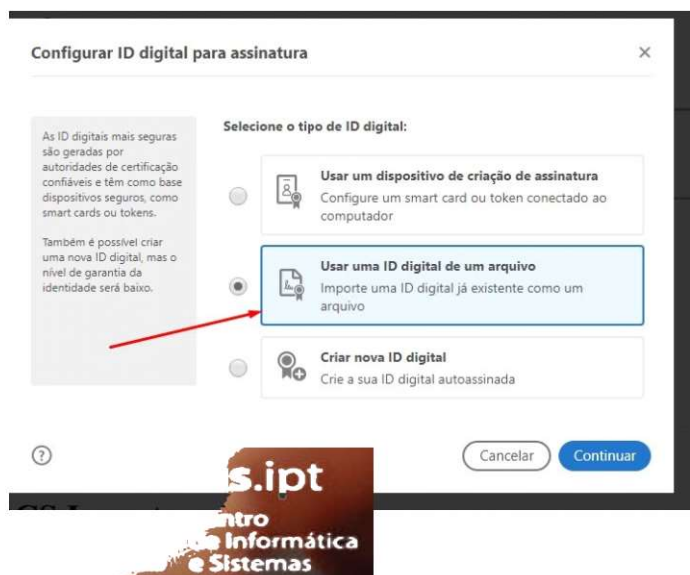
17. Assinar Documentos PDF tendo o certificado numa PenDrive

17.1 Acrobat reader DC

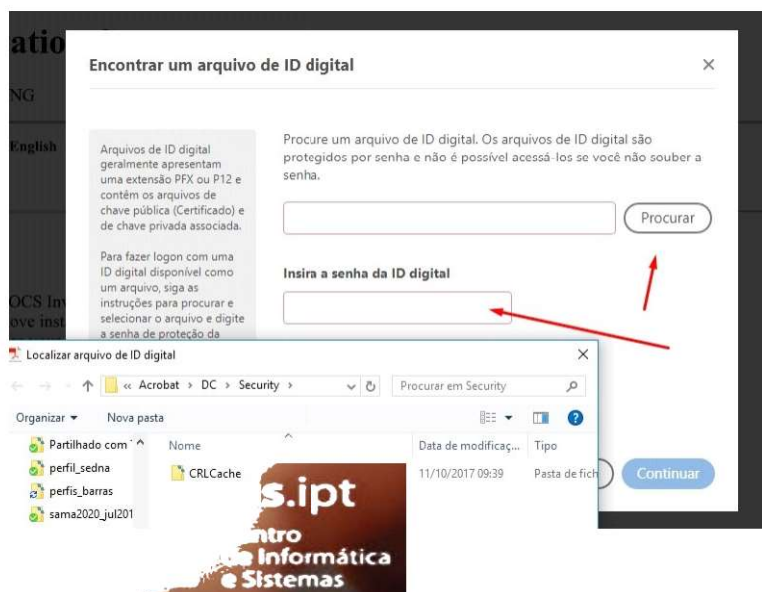
Após iniciar o procedimento do **Ponto 2** deste guia e imediatamente após assinalar a área pretendida para colocar a marca do seu certificado digital, na janela onde seleciona a assinatura a usar, terá de escolher **Configurar nova ID digital**.



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



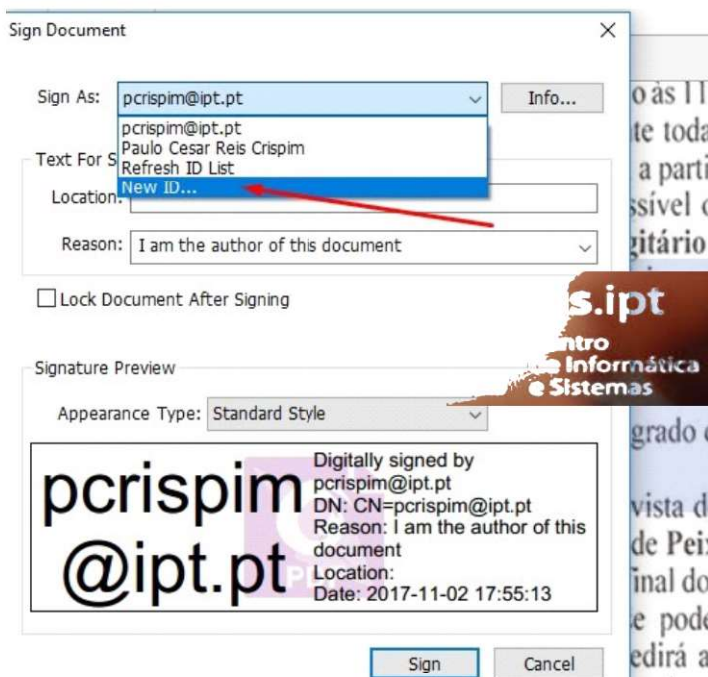
Ao escolher o ficheiro onde se encontra **o seu certificado (*.p12)**, coloca a palavra-passe que lhe colocou quando o exportou (**Ponto 7.1** ou **Ponto 10** deste guia) e carregue em **Continuar**.



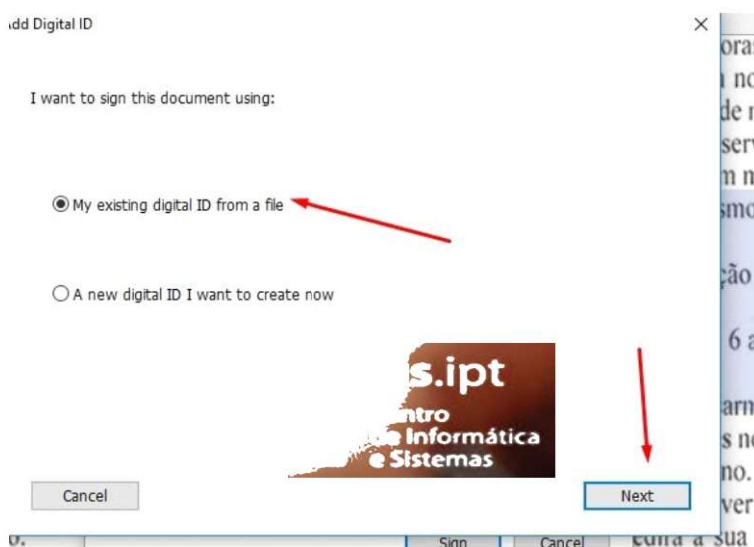
Após este passo terá de continuar o procedimento descrito no **Ponto 2** (página 6)

17.2 FoxIT reader

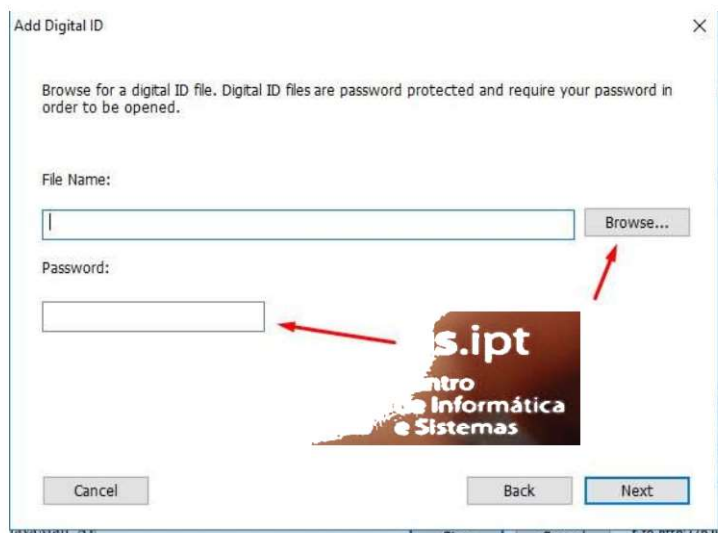
Após iniciar o procedimento do **Ponto 14.2** deste guia e imediatamente após assinalar a área pretendida para colocar a marca do seu certificado digital, na janela onde seleciona a assinatura a usar, em **Assinar como**, terá de escolher **New ID...** .



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**.

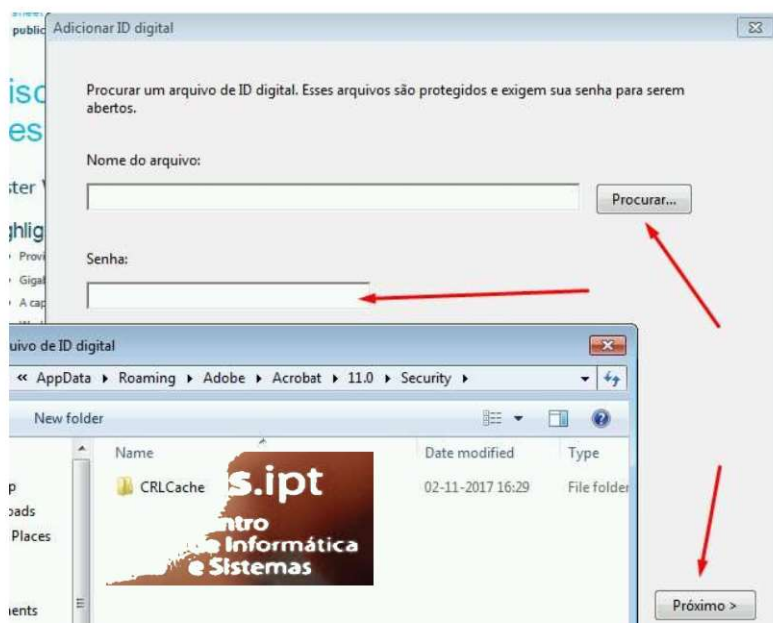
17.3 Acrobat Reader 11

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)

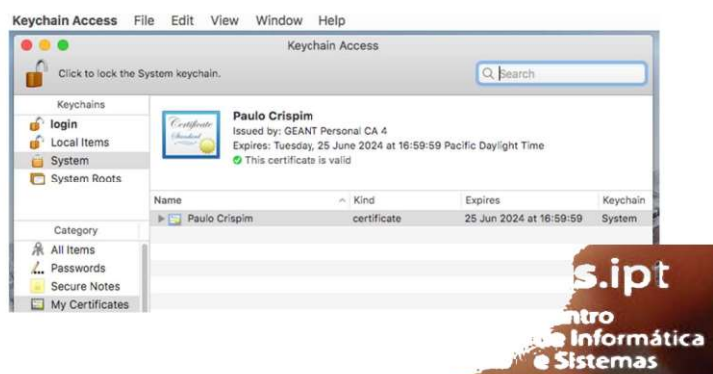
.....

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.

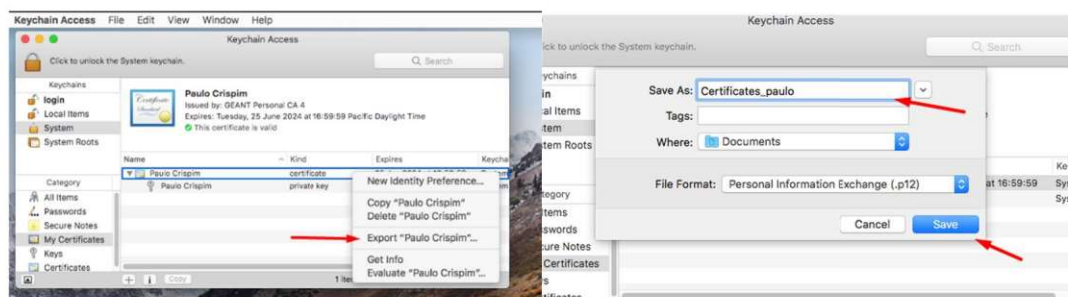
18.1. Instalar o certificado no Porta Chaves

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.



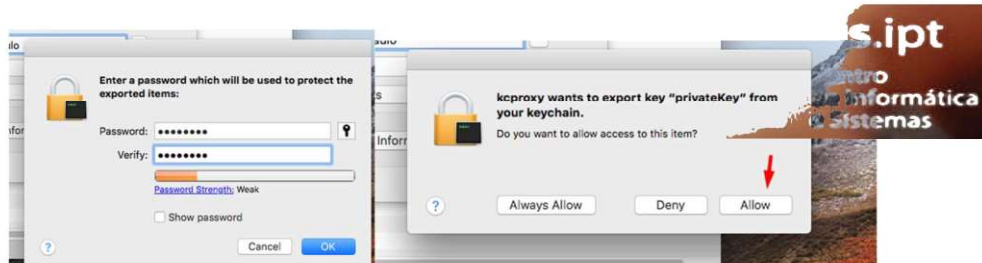
18.2. Exportar o Certificado do Porta Chaves com chave privada

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.



.....