

Manual da Aplicação Autenticação.gov para computador

Versão 3.12.0

25/03/2024

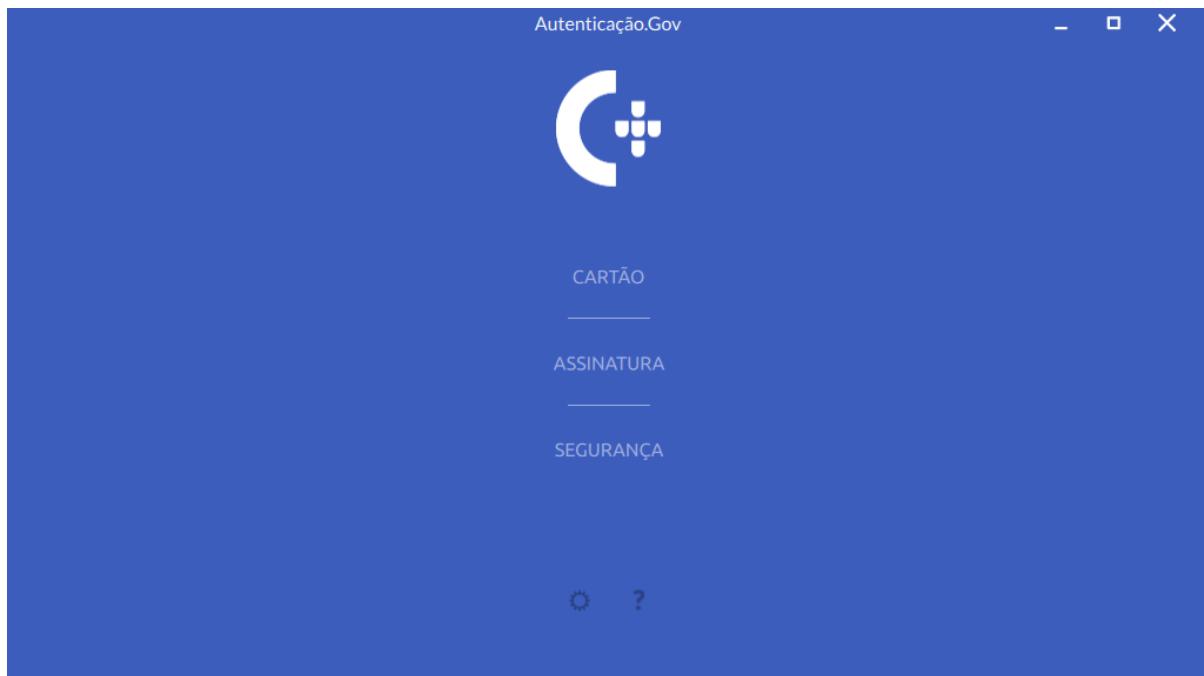


Tabela de Conteúdos

1	Introdução	5
2	Novidades	5
3	Download, instalação e remoção da aplicação	5
3.1	Sistemas Operativos oficialmente suportados	5
3.2	Download do pacote de instalação da aplicação	6
3.3	Instalação da aplicação	6
3.3.1	Instalação em Microsoft Windows	7
3.3.2	Instalação em Linux	8
3.3.3	Instalação em Mac OS	9
3.3.4	Instalação em ChromeOS	10
3.4	Remoção da aplicação	10
3.4.1	Remoção em <i>Microsoft Windows 7</i>	10
3.4.2	Remoção em <i>Microsoft Windows 10 ou 11</i>	11
3.4.3	Remoção em Linux e ChromeOS	13
3.4.4	Remoção em MacOS	13
3.5	Atualização da aplicação	14
3.5.1	Atualização em Linux	14
4	Aplicação Utilitária Autenticação.Gov	14
4.1	Apresentação da Aplicação	15
4.2	Funcionalidades da aplicação	15
4.2.1	Menu Cartão	15
4.2.2	Assinatura digital	19
4.2.3	Segurança	25
4.2.4	Configurações	28
4.2.5	Ajuda	34
4.2.6	Centro de Notificações	34
4.2.7	Acesso Contactless	35
5	Integração com aplicações	37
5.1	Integração com aplicações em Windows	37
5.2	Integração com aplicações via interface PKCS#11	39
5.3	Assinatura digital em aplicações comuns	39
5.3.1	Assinatura digital na suite <i>Microsoft Office</i>	39
5.3.2	Assinatura digital na suite <i>LibreOffice / OpenOffice</i>	40
5.3.3	Assinatura digital de email com <i>Microsoft Outlook</i>	41
5.3.4	Assinatura digital em <i>Adobe Acrobat Reader</i>	46

5.3.5	Assinatura digital em <i>Adobe Acrobat Reader</i> em MacOS (desde a versão 3.11.0)	46
5.3.6	Assinatura digital em <i>Adobe Acrobat Reader</i> em MacOS com PKCS#11	47
5.3.7	Assinatura digital com Chave Móvel Digital	51
5.3.8	Assinatura digital de email com Mozilla Thunderbird	52
5.3.9	Assinatura digital de ficheiros DWF	55
5.3.10	Assinatura digital de ficheiros DWG	58
5.4	Autenticação em portais WEB	65
5.4.1	Configurar autenticação para <i>Mozilla Firefox</i>	66
6	Resolução de Problemas	67
6.1	Exibida mensagem de erro quando se tenta adicionar o módulo PKCS#11 no <i>Firefox</i> / <i>Thunderbird</i>	67
6.2	Não é possível adicionar o módulo PKCS#11 ao <i>Adobe Acrobat Reader</i> em <i>MacOS</i>	67
6.3	Impossibilidade de assinatura em <i>Adobe Reader</i> , <i>Microsoft Office</i> e <i>LibreOffice</i> com Cartão de Cidadão	67
6.4	O leitor de cartões está instalado mas não é detetado pela aplicação do Cartão de Cidadão	69
6.4.1	Windows	69
6.4.2	Linux	71
6.5	Não são detetados quaisquer certificados durante a tentativa de assinatura na suite <i>LibreOffice</i> / <i>Apache OpenOffice</i>	71
6.6	Problemas gráficos na aplicação	71
6.7	Problemas com placas gráficas integradas	72
6.8	Não é possível mover/arrastar a aplicação (Linux em Wayland)	72
6.9	Aplicação não arranca	72
6.10	Problemas com a nova cadeia de confiança	73
6.11	Problemas na validação das assinaturas	73
6.12	Problemas com ficheiros PDF não suportados	73
6.13	Erro na Comunicação em assinatura com Chave Móvel Digital	73
6.14	Serviços online usados pela aplicação	73
6.15	Obtenção do relatório para análise através do menu Configurações	75
6.16	Remoção de metadados de ficheiros PDF	75
7	Interface de linha de comandos	76
7.1	Consultar ajuda e versão	76
7.2	Atalho para configurar modo de renderização gráfica	76
7.3	Atalho para submenu de assinatura	76

8 Instruções de configuração em ambientes empresariais	77
8.1 Configurações através de chaves de registo Windows	77
8.2 Configurações através de ficheiro de configuração em Linux e MacOS	81
8.3 Instalação automatizada em ambientes Windows	81
8.4 Informação sobre servidores de Proxy	81
8.4.1 Configuração em <i>Windows</i>	81
8.4.2 Configuração em <i>MacOS</i>	82
9 Notas do Utilizador	83

1 Introdução

NOTA: A partir da versão 3.2.0, houve uma alteração de nomenclatura no manual. As referências a "Middleware do Cartão de Cidadão" foram substituídas por "aplicação Autenticação.gov para computador", excepto quando o termo "*middleware*" é mais apropriado.

Este manual pretende descrever todas as funcionalidades providenciadas pela aplicação Autenticação.gov para computador.

A instalação da aplicação Autenticação.gov para computador inclui o *middleware* do Cartão de Cidadão. Este *middleware* pode definir-se como a camada de software entre o computador e o seu Cartão de Cidadão e é através deste que são disponibilizadas ao sistema operativo e outras aplicações funcionalidades de autenticação e assinatura eletrónica.

A aplicação Autenticação.gov para computador permite a gestão do seu Cartão de Cidadão. Nesta poderá visualizar as suas informações, editar as suas notas, modificar os seus PINs pessoais e assinar digitalmente ficheiros.

Este manual pode-se dividir nas seguintes fundamentais áreas de utilização:

- Na primeira área (no capítulo dois), aborda o descarregamento, instalação e remoção da aplicação;
- Na segunda área (no capítulo três), descreve as funcionalidades da aplicação de gestão do Cartão de Cidadão e de assinatura digital de ficheiros;
- Na terceira área (nos capítulos quatro e cinco), documenta as integrações do *middleware* com o sistema operativo e aplicações;
- Na quarta área (no capítulo seis), documenta a instalação automatizada em ambientes Windows e configuração em ambientes empresariais;

2 Novidades

Suporte ao novo Cartão de Cidadão

Desde a versão 3.12.0 da aplicação é suportado o novo Cartão de Cidadão que tem a possibilidade de leitura por aproximação (*contactless*) se utilizado um leitor de cartões apropriado.

Continua a existir a possibilidade de leitura na interface de contacto mas deve garantir que o cartão está inserido no leitor de forma correta, porque no novo Cartão de Cidadão os contactos do chip encontram-se no verso do documento.

É recomendada a consulta da nova secção Acesso Contactless

3 Download, instalação e remoção da aplicação

Neste ponto são apresentadas as instruções para a instalação e remoção da aplicação Autenticação.gov para computador.

3.1 Sistemas Operativos oficialmente suportados

- Sistemas Windows:
 - Microsoft Windows 7
 - Microsoft Windows 8
 - Microsoft Windows 8.1
 - Microsoft Windows 10
 - Microsoft Windows 11
- Sistemas Linux:
 - Fedora 38 e superiores

- OpenSUSE Leap 15.2 e superiores
- Ubuntu 20.04 e superiores
- Outras distribuições Linux com suporte para pacotes Flatpak e arquitetura Intel x86_64
- Sistemas Apple MacOS:
 - Mac OS High Sierra (10.13) e superiores

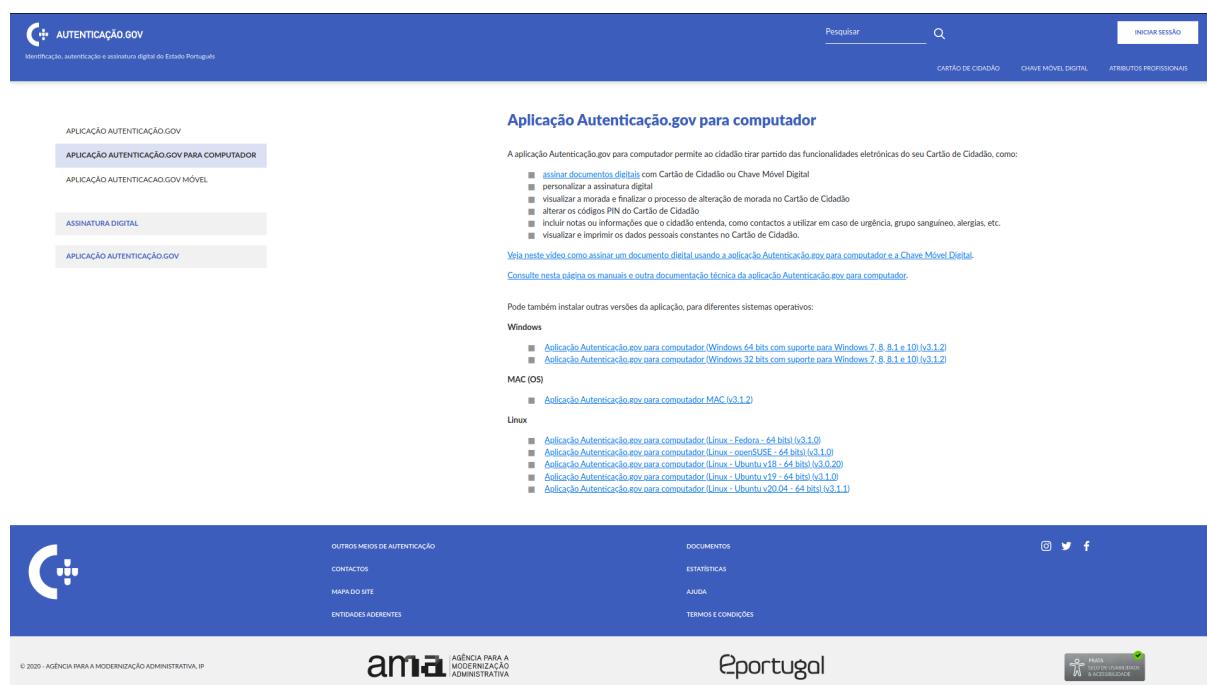
3.2 Download do pacote de instalação da aplicação

Para obter o pacote de instalação da aplicação, deverá aceder ao site oficial do Cartão de Cidadão em Aplicação Autenticação.gov para computador e fazer download da versão correta para o seu sistema operativo.

Ao clicar no link será efetuada uma tentativa de identificar o sistema operativo através dos dados fornecidos pelo navegador e na área de conteúdos do lado direito será apresentada uma hiperligação que permite efetuar o descarregamento do pacote de instalação adequado ao seu sistema.

Nos casos dos sistemas operativos *Linux*, não é possível identificar a distribuição, deste modo será apresentada a lista das distribuições suportadas para a arquitetura detetada.

Esta página contém a lista de todos os pacotes de instalação dos sistemas operativos oficialmente suportados e manuais de utilização.



The screenshot shows the main page of the Autenticação.gov website. At the top, there's a navigation bar with the logo, search bar, and session management links. Below the header, there's a sidebar with links for 'APLICAÇÃO AUTENTICAÇÃO.GOV', 'APLICAÇÃO AUTENTICAÇÃO.GOV PARA COMPUTADOR' (which is highlighted), 'APLICAÇÃO AUTENTICAÇÃO.GOV MÓVEL', 'ASSINATURA DIGITAL', and 'APLICAÇÃO AUTENTICAÇÃO.GOV'. The main content area is titled 'Aplicação Autenticação.gov para computador'. It contains a brief description of what the application does, followed by a list of supported operating systems and their specific download links. The supported OSes listed are Windows 7, 8, 8.1, 10, and Linux (openSUSE, Ubuntu). At the bottom of the page, there's a footer with links to 'OUTROS MEIOS DE AUTENTICAÇÃO', 'CONTACTOS', 'MAPA DO SITE', 'ENTIDADES ADERENTES', 'DOCUMENTOS', 'ESTATÍSTICAS', 'AJUDA', 'TERMOS E CONDIÇÕES', social media icons, and logos for amai and Eportugal.

Após efetuado o download da respetiva versão, avance para o ponto seguinte Instalação da aplicação.

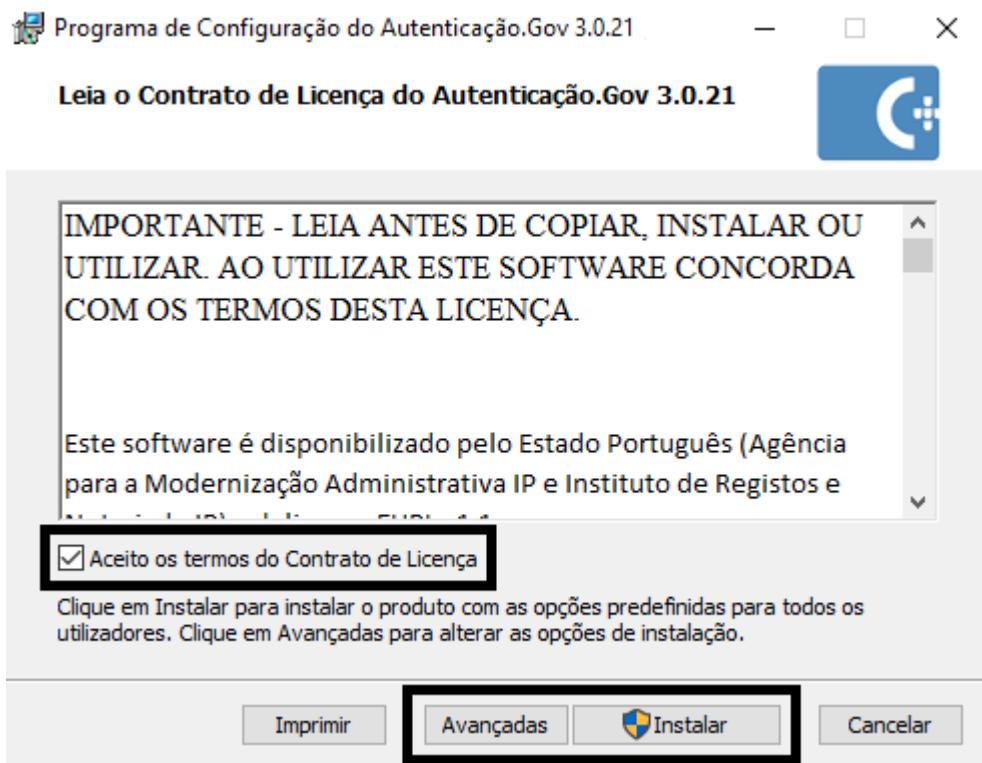
3.3 Instalação da aplicação

As instruções apresentadas de seguida pressupõem que o ficheiro de instalação da aplicação foi descarregado previamente da Internet. Caso não tenha sido, efetue os passos descritos no ponto anterior Download do pacote de instalação da aplicação.

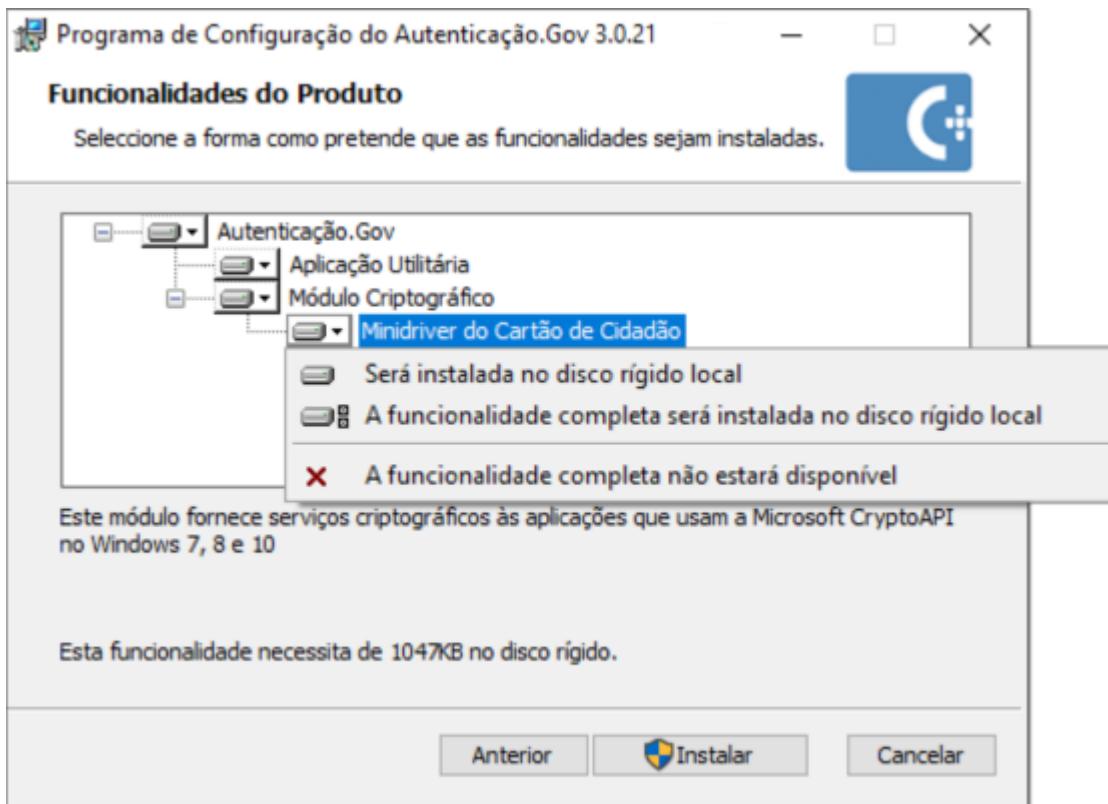
Para a instalação da aplicação Autenticação.gov para computador, deverão ser executados os passos descritos nos pontos seguintes, relativos ao sistema operativo utilizado.

3.3.1 Instalação em Microsoft Windows

1. Executar o pacote de instalação: Após ter descarregado o ficheiro de instalação, deverá fazer duplo clique sobre este.
2. No primeiro ecrã interativo, deverá marcar a caixa para aceitar os termos e condições da aplicação. Para uma instalação simples, pressione **Instalar** (prossiga para o passo 5). Para uma instalação avançada, pressione **Avançadas**. A instalação avançada permite configurar o caminho para a pasta de instalação e as funcionalidades a serem instaladas.



3. Após selecionar **Avançadas**, poderá escolher a pasta onde deseja instalar a aplicação. Se desejar alterar a pasta predefinida, carregue em **Alterar** e na janela que surgir, navegue até à pasta de destino e carregue **OK**. Para continuar a instalação na pasta de destino, deverá premir o botão **Seguinte**.
4. Deverá aparecer um ecrã para escolher as funcionalidades a serem instaladas. As funcionalidades são representadas numa árvore em que cada funcionalidade possui um botão para a incluir ou excluir da instalação. Ao selecionar uma funcionalidade, será apresentada a sua descrição e o espaço necessário para a sua instalação. Para instalar as funcionalidades selecionadas, clique em **Instalar**.



5. Após a conclusão deste assistente, este solicitará a reinicialização do computador.
6. No próximo arranque do *Windows* a instalação da aplicação estará finalizada.

3.3.2 Instalação em Linux

3.3.2.1 Instalação através da linha de comandos Instalação de pacote Flatpak

A partir da versão 3.9.0 da aplicação foi introduzido um novo formato de pacote para Linux. O formato Flatpak tem o objetivo de suportar um maior número de distribuições Linux de uma forma uniforme.

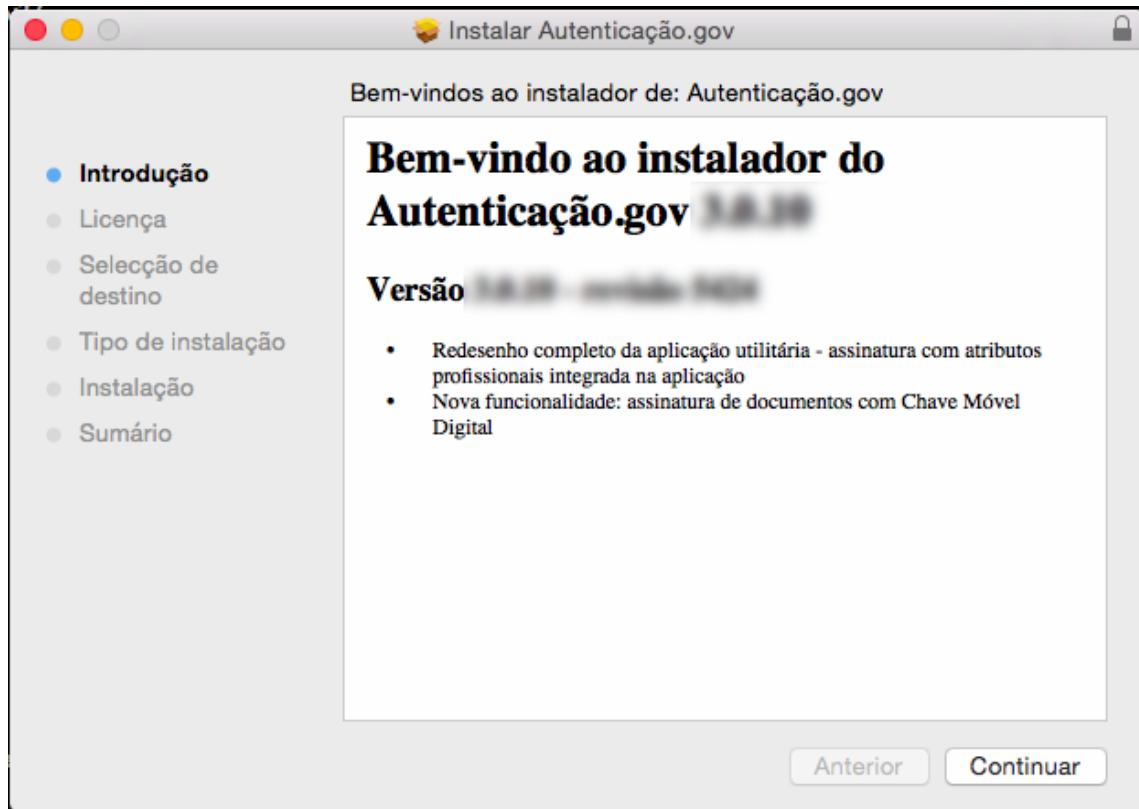
Para instalar esta versão da aplicação deve seguir este procedimento:

1. Desinstalar alguma versão nativa do pacote pteid-mw que esteja instalada no sistema. Por exemplo em Ubuntu deverá utilizar o comando: `sudo apt remove pteid-mw`
2. Instalar o software Flatpak seguindo as instruções específicas da distribuição: <https://flatpak.org/setup/>
3. Instalar o pacote `pcsc-lite/pcscd` no sistema usando os pacotes nativos da distribuição. A aplicação funciona sem este componente, apenas as funcionalidades que exigem acesso ao Cartão de Cidadão dependem do pcscd.
4. Executar o comando `flatpak install pteid-mw-linux.x86_64.flatpak` na diretoria onde estiver o pacote flatpak descarregado.

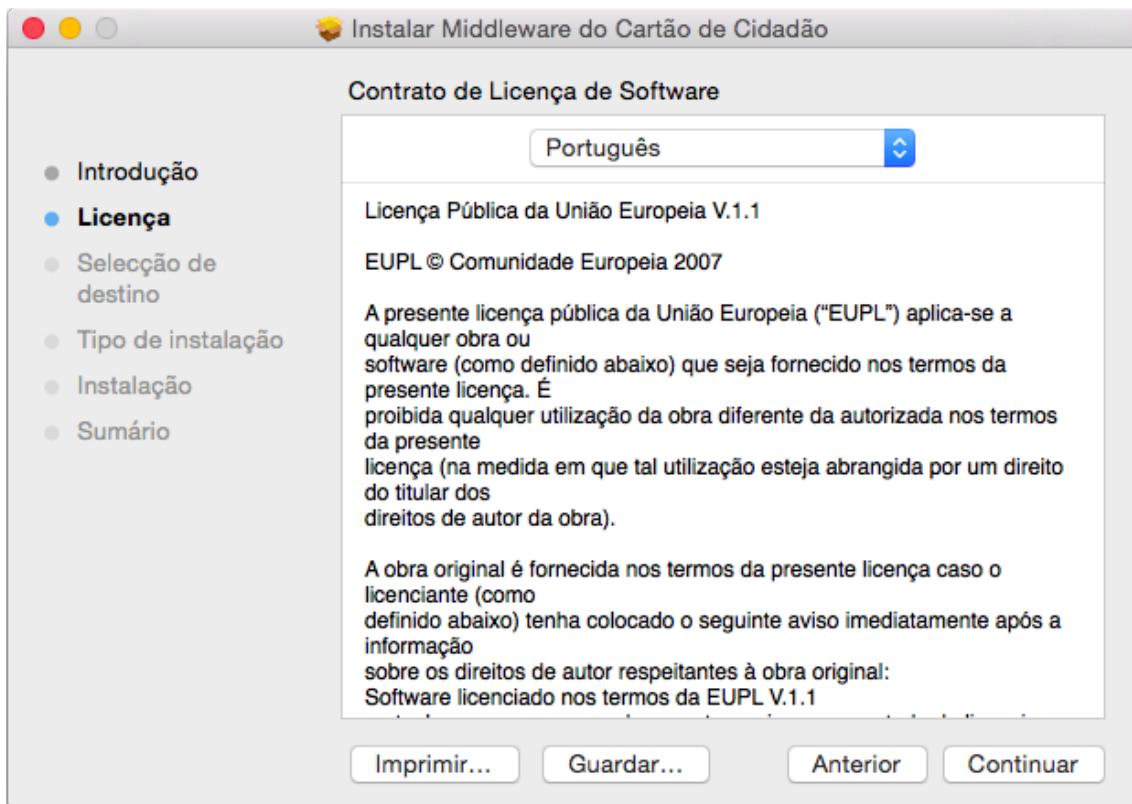
1. O software Flatpak deverá ter versão igual ou superior à 1.3.2 para permitir que a aplicação acesse ao Cartão de Cidadão. Este requisito é cumprido por distribuições como o Ubuntu 20.04 e 22.04, OpenSUSE Leap 15.3 e 15.4, entre outras.
2. Em Ubuntu 22.04 é importante executar um comando extra para garantir que o acesso ao Cartão de Cidadão funcione sempre: `sudo systemctl enable pcscd.socket`

3.3.3 Instalação em Mac OS

1. Executar o instalador: após ter descarregado o ficheiro de instalação, deverá fazer duplo clique sobre este, surgindo um ecrã semelhante ao apresentado de seguida:



2. Escolher a opção **Continuar**. Em seguida é necessário ler e aceitar os termos da licença do software.



3. A partir deste ponto no assistente deverá premir o botão **Continuar** até concluir a instalação.
4. Após a conclusão deste assistente, a aplicação estará instalada no computador. Neste momento a aplicação utilitária Autenticacão.Gov já estará disponível na pasta Aplicações / *Applications*.

3.3.4 Instalação em ChromeOS

1. Instalar o software Flatpak seguindo as instruções específicas do ChromeOS: <https://flatpak.org/setup/Chrome%20OS>
2. Obter o instalador Linux em formato Flatpak a partir da página oficial.
3. Executar o comando `flatpak install pteid-mw-linux.x86_64.flatpak` na diretoria onde estiver o pacote flatpak descarregado.
4. Após a instalação, a aplicação pode ser executada com o comando `flatpak run pt.gov.autenticacao`

Nota: A funcionalidade da aplicação é atualmente limitada em ChromeOS, sendo possível utilizar apenas a Chave Móvel Digital.

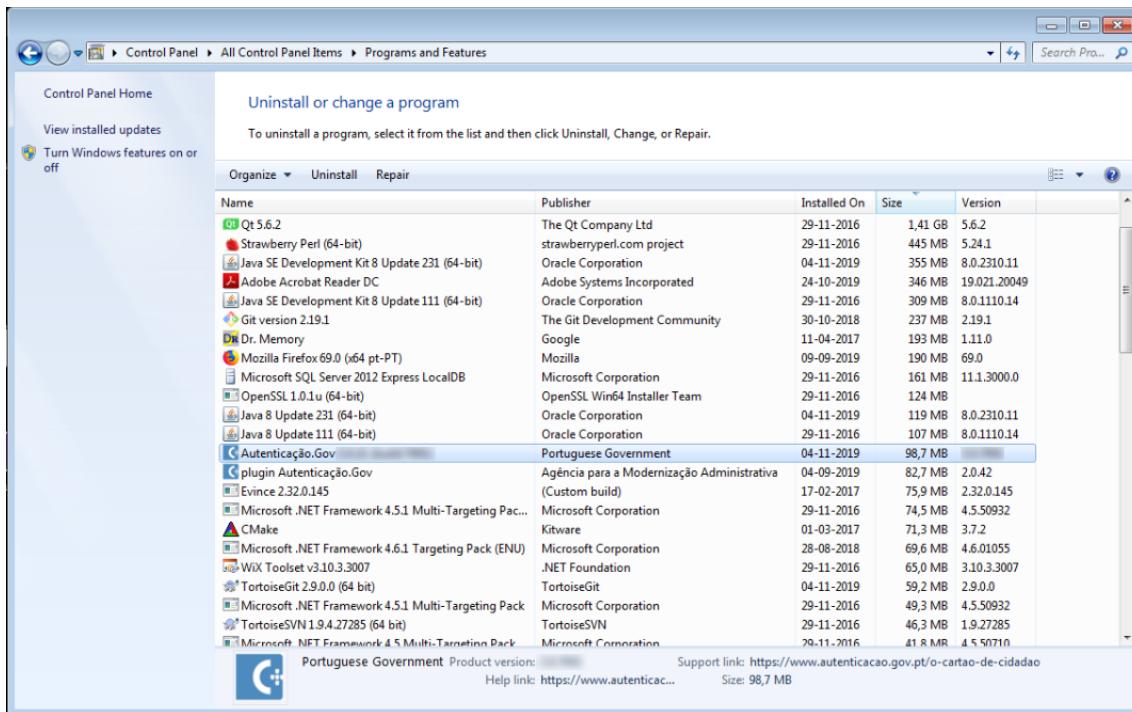
3.4 Remoção da aplicação

Para proceder à remoção da aplicação do Cartão de Cidadão, deverão ser executados os passos descritos nos pontos seguintes, relativos ao sistema operativo utilizado.

3.4.1 Remoção em Microsoft Windows 7

1. Aceda ao **Painel de Controlo**.
2. Selecione a **Opção Adicionar ou Remover Programas**.

3. Selecione o programa **Autenticação.Gov**, conforme apresentado na janela seguinte:

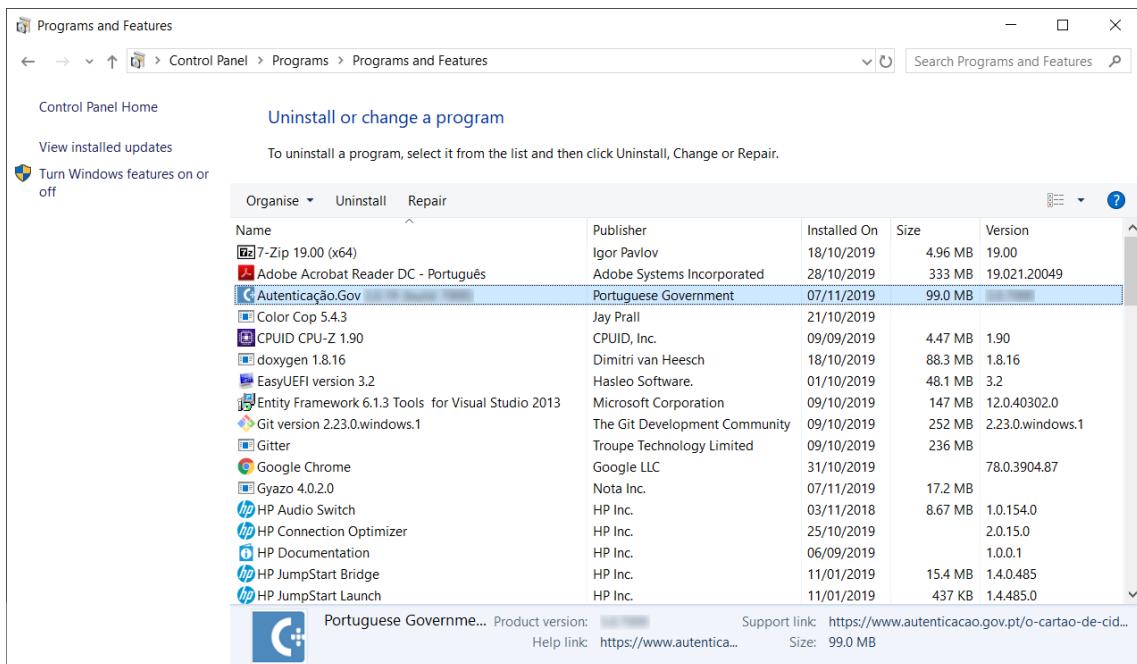


4. Clique em **Desinstalar**. Confirme todas as janelas de diálogo que irão surgir.
5. Após estes passos, a aplicação estará removida do computador. Recomenda-se que o computador seja reiniciado no final destes passos.

3.4.2 Remoção em *Microsoft Windows 10 ou 11*

3.4.2.1 Através do Painel de Controlo

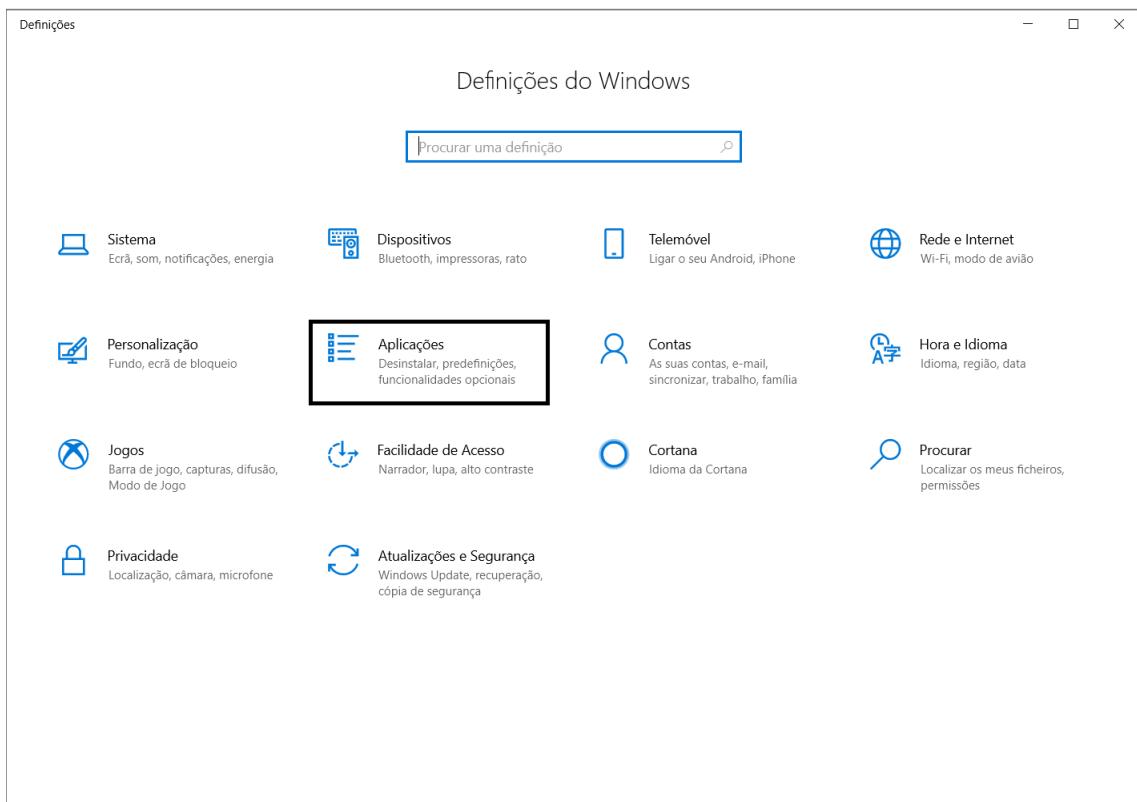
1. Aceda ao **Painel de Controlo**.
2. Selecione a **Opção Adicionar ou Remover Programas**.
3. Selecione o programa **Autenticação.Gov**, conforme apresentado na janela seguinte:



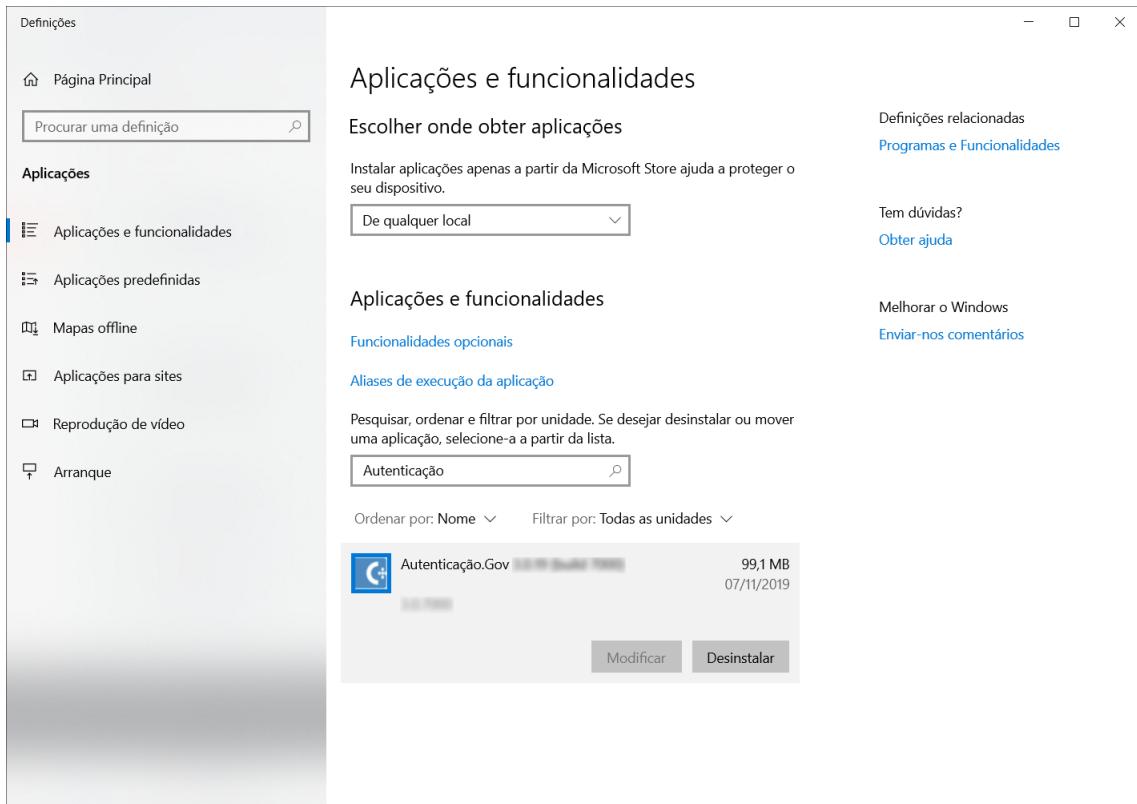
- Clique em **Desinstalar**. Confirme todas as janelas de diálogo que irão surgir.
- Após estes passos, a aplicação estará removida do computador. Recomenda-se que o computador seja reiniciado no final destes passos.

3.4.2.2 Através das Definições do Windows

- Aceda a **Menu Iniciar -> Definições do Windows**.
- Prima o botão **Aplicações** (Desinstalar, predefinições, funcionalidades opcionais):



3. Procure a aplicação **Autenticação.Gov**; selecione a aplicação e pressione **Desinstalar**, conforme apresentado na figura seguinte:



4. Clique em **Desinstalar**. Confirme todas as janelas de diálogo que irão surgir.
5. Após estes passos, a aplicação estará removida do computador. Recomenda-se que o computador seja reiniciado no final destes passos.

Nota: a diretoria e ficheiros de *log*, que se encontram na pasta de instalação (por defeito em `C:\Program Files\Portugal Identity Card\log\`), não serão removidos ao desinstalar a aplicação Autenticação.Gov.

3.4.3 Remoção em Linux e ChromeOS

3.4.3.1 Remoção através da linha de comandos Remoção de pacote Flatpak

1. Verifique se a aplicação está de facto instalada via flatpak: isto acontece se existir uma entrada com o ID `pt.gov.autenticacao` na listagem devolvida pelo comando `flatpak --columns=app list`.
2. Em caso afirmativo pode remover o pacote com o seguinte comando: `flatpak remove pt.gov.autenticacao`

3.4.4 Remoção em MacOS

1. Abra a aplicação "Terminal" no MacOS.
2. Execute o seguinte comando para desinstalar todos os ficheiros da aplicação.
`sudo /usr/local/bin/pteid_uninstall.sh`

3.5 Atualização da aplicação

3.5.1 Atualização em Linux

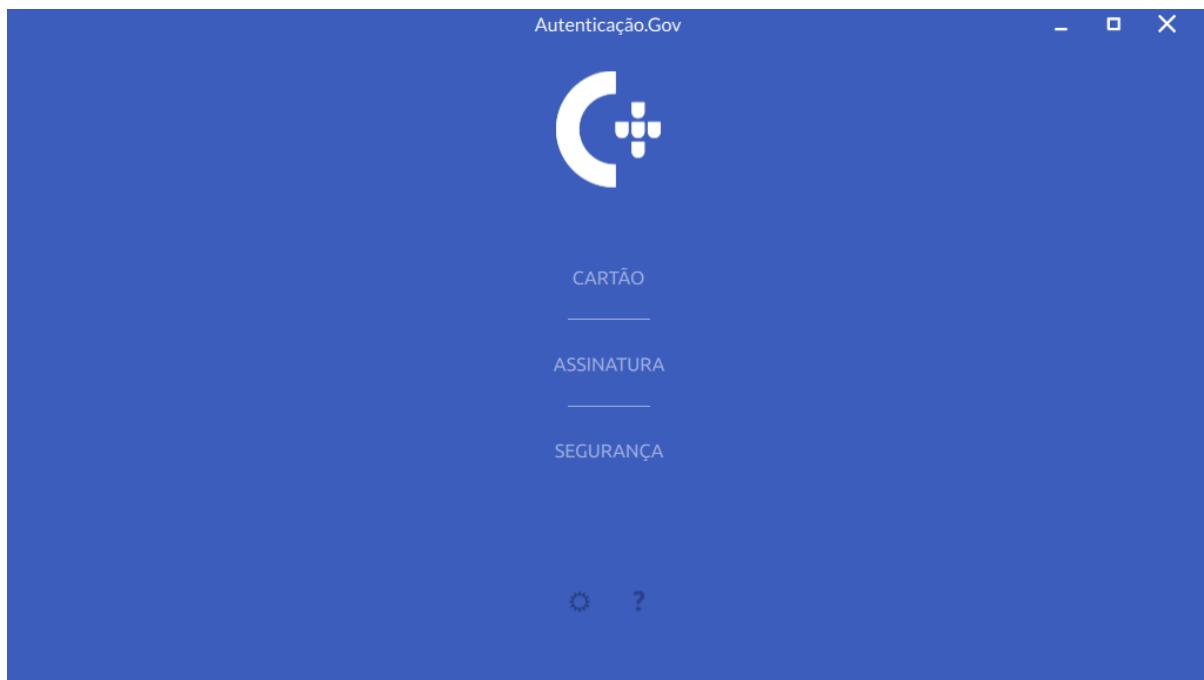
Ao transferir o ficheiro de instalação através do menu **Configurações** -> **Atualizações** da aplicação, este ficará disponível na diretoria de **Transferências**, por defeito em `~/Downloads`.

Pode também transferir a última versão da aplicação através da página oficial.

Depois de ter transferido o ficheiro de instalação, para concluir a atualização siga os passos indicados na secção Instalação através da linha de comandos.

4 Aplicação Utilitária Autenticação.Gov

A aplicação utilitária Autenticação.Gov pode ser utilizada para visualizar e gerir os dados no Cartão de Cidadão e assinar documentos digitais.



Nesta aplicação poderá efetuar as seguintes operações:

- Visualização da informação e foto do cidadão;
- Visualização da morada do cidadão;
- Edição das notas;
- Imprimir os dados do Cartão de Cidadão;
- Assinatura digital de documentos PDF e outros ficheiros;
- Visualização dos certificados do Estado e do cidadão;
- Registo dos certificados do Estado e do cidadão (específico de Microsoft Windows);
- Gestão de PINs (Testar PIN, Alterar PIN).

O aspecto e comportamentos da aplicação é semelhante nos três tipos de sistemas operativos, à exceção de algumas funcionalidades que estão apenas disponíveis em Windows, visto serem funcionalidades nativas ou configurações específicas do ambiente Windows.

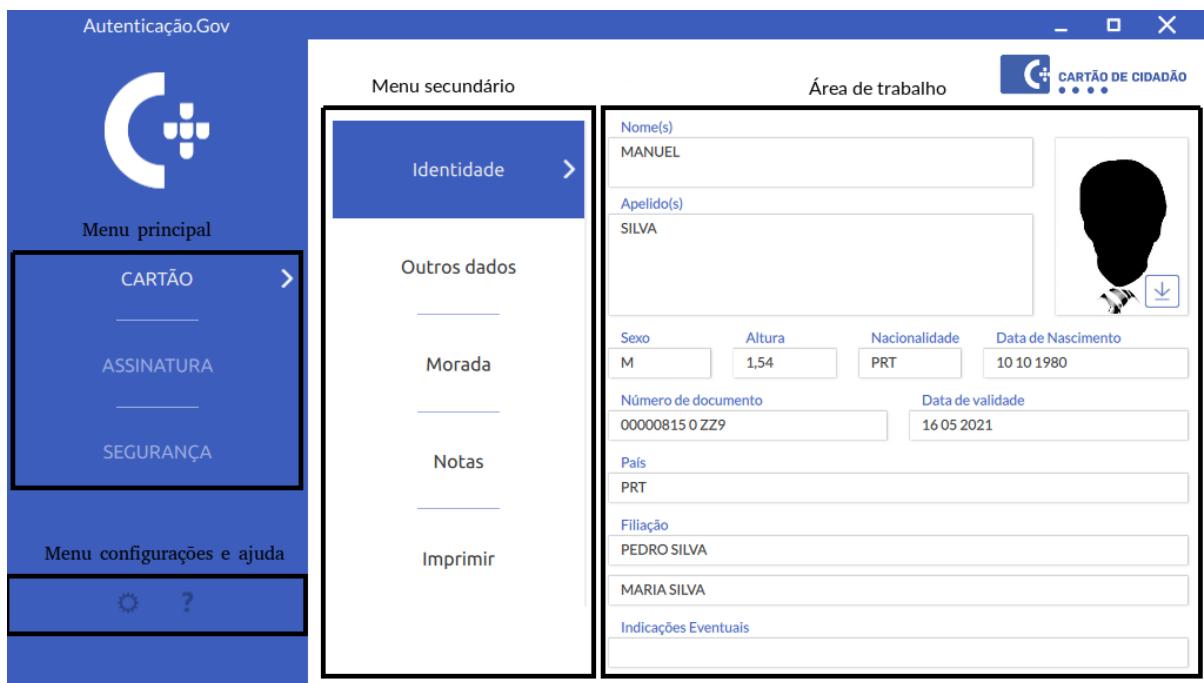
O atalho para a aplicação fica disponível em localizações diferentes consoante o tipo de sistema operativo:

- Em Windows surgirá em: **Iniciar Programas Autenticação.Gov**
- Em Linux surgirá em: **Aplicações Acessórios Autenticação.Gov**
- Em MacOS, surgirá na localização escolhida pelo utilizador durante o processo de instalação.

4.1 Apresentação da Aplicação

A aplicação é composta por 4 áreas principais de interação:

- **Menu principal:** São disponibilizadas as três funcionalidades básicas da aplicação;
- **Menu secundário:** São disponibilizadas as funcionalidades específicas de cada opção do menu principal;
- **Menu configurações e ajuda:** São disponibilizados os menus de configuração e ajuda;
- **Área de trabalho:** Área de visualização de dados do Cartão de Cidadão e área de trabalho para os menus de assinatura e segurança.



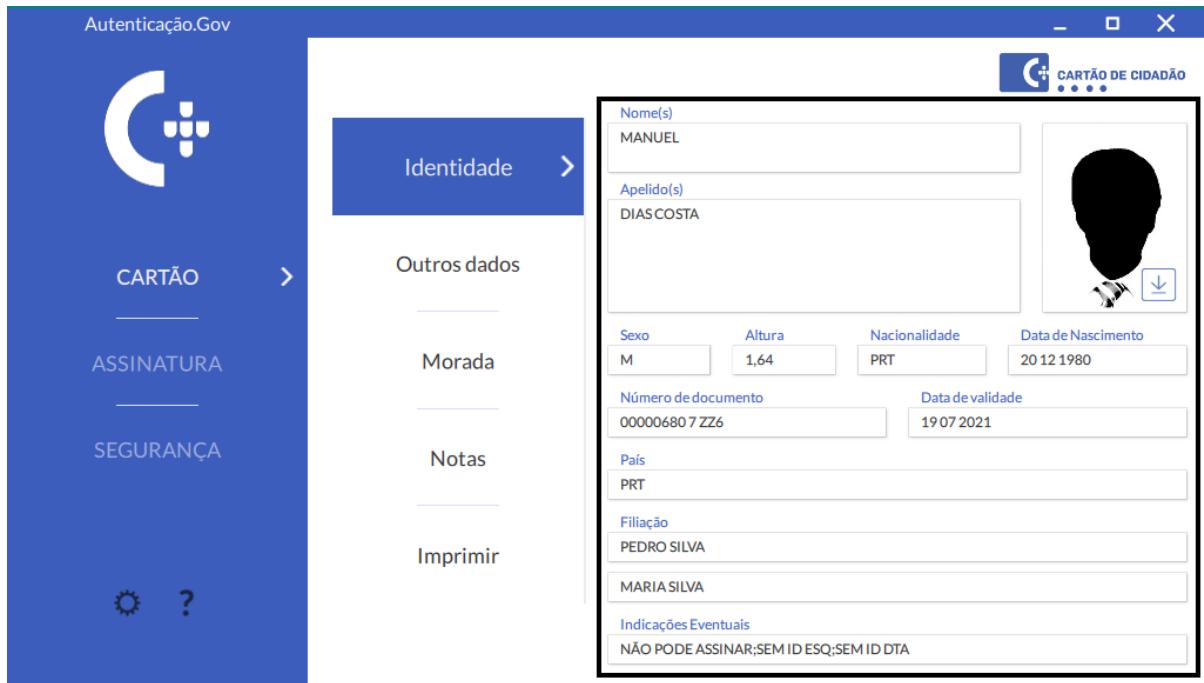
4.2 Funcionalidades da aplicação

As funcionalidades da aplicação estão divididas, em três menus principais: Menu Cartão, Menu Assinatura e Menu Segurança.

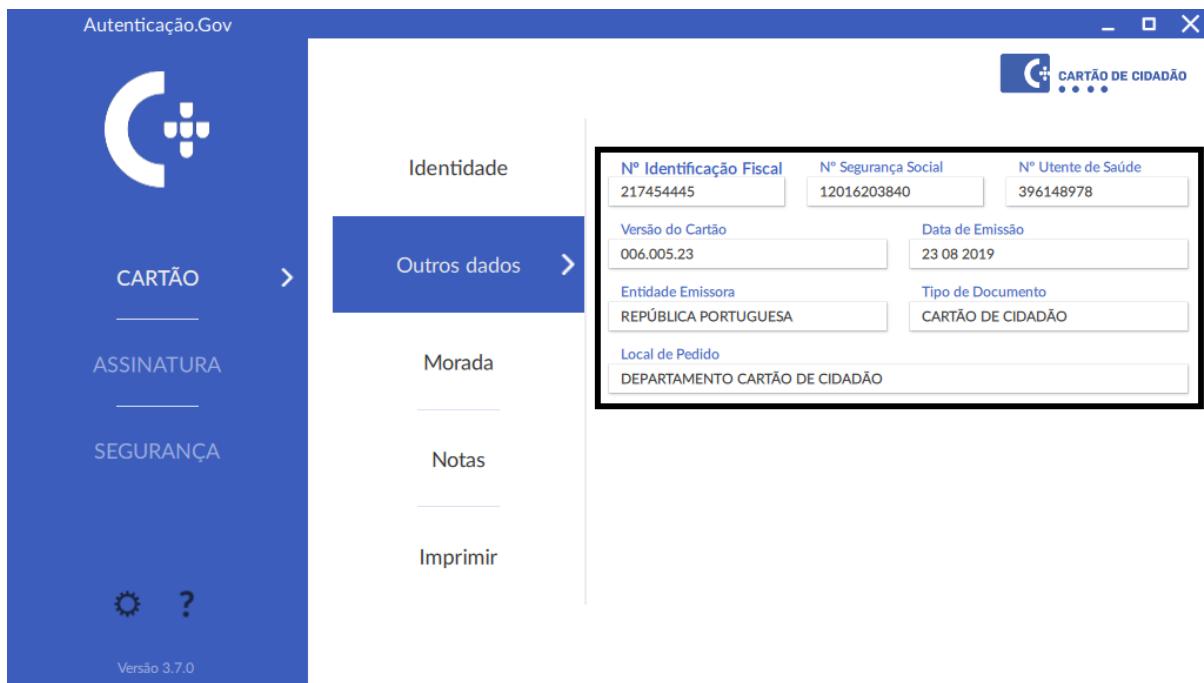
4.2.1 Menu Cartão

Permite visualizar a informação de identidade e foto do cidadão, visualizar a morada do cidadão, edição das notas, bem como imprimir os dados do Cartão de Cidadão. A foto do cidadão pode ser exportada para um ficheiro.

4.2.1.1 Identidade Permite visualizar os dados de identificação e foto do cidadão presentes no Cartão de Cidadão. Através desta página é ainda possível exportar foto do cidadão.



4.2.1.2 Outros dados Permite visualizar outros dados do cartão do cidadão e verificar o estado do Cartão de Cidadão.



4.2.1.3 Morada e Alteração de morada

IMPORTANTE: Consulta de Morada do Cartão de Cidadão.

Desde a versão 3.9.0 da aplicação local Autenticação.gov a morada do Cartão de Cidadão é lida a partir dos serviços centrais. Isto implica uma ligação à Internet funcional para a leitura da morada. É por isso necessário garantir que não existe *firewall* ou outro *software* na rede local que impeça a ligação ao endereço `morada.cartaoecidadao.pt` no porto 443. Para

processos de alteração de morada iniciados desde o fim de dezembro de 2022, a confirmação de morada fica apenas disponível no portal eportugal.gov.pt.

Dentro do separador Morada é possível visualizar a morada atual e aceder ao portal eportugal.gov.pt para completar o processo de alteração da morada.

Ambas as funcionalidades requerem uma ligação à Internet. Por favor certifique-se que está ligado antes de iniciar o processo.

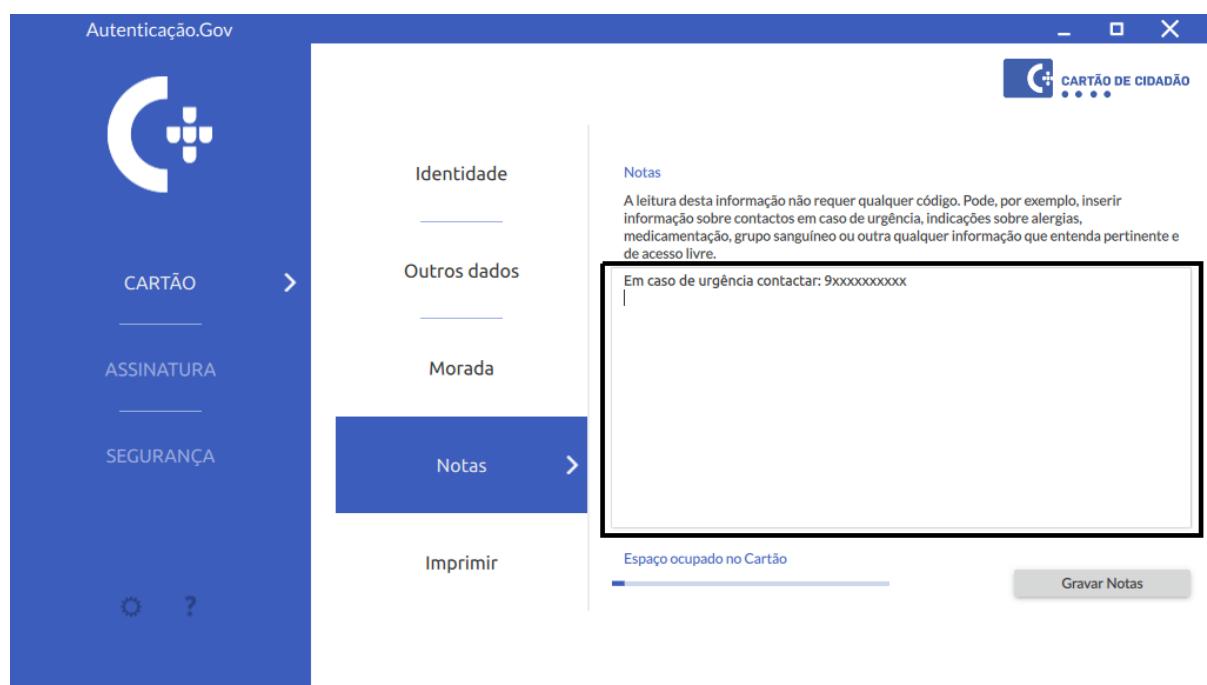
Para terminar o processo de alteração de morada, consulte a seguinte página Web:

Confirmar a alteração de morada.

4.2.1.4 Notas

A aplicação permite editar as notas gravadas no cartão do cidadão.

A leitura desta informação não requer qualquer código. Pode, por exemplo, inserir informação sobre contactos em caso de urgência, indicações sobre alergias, medicação, grupo sanguíneo ou outra qualquer informação que entenda pertinente e de acesso livre.

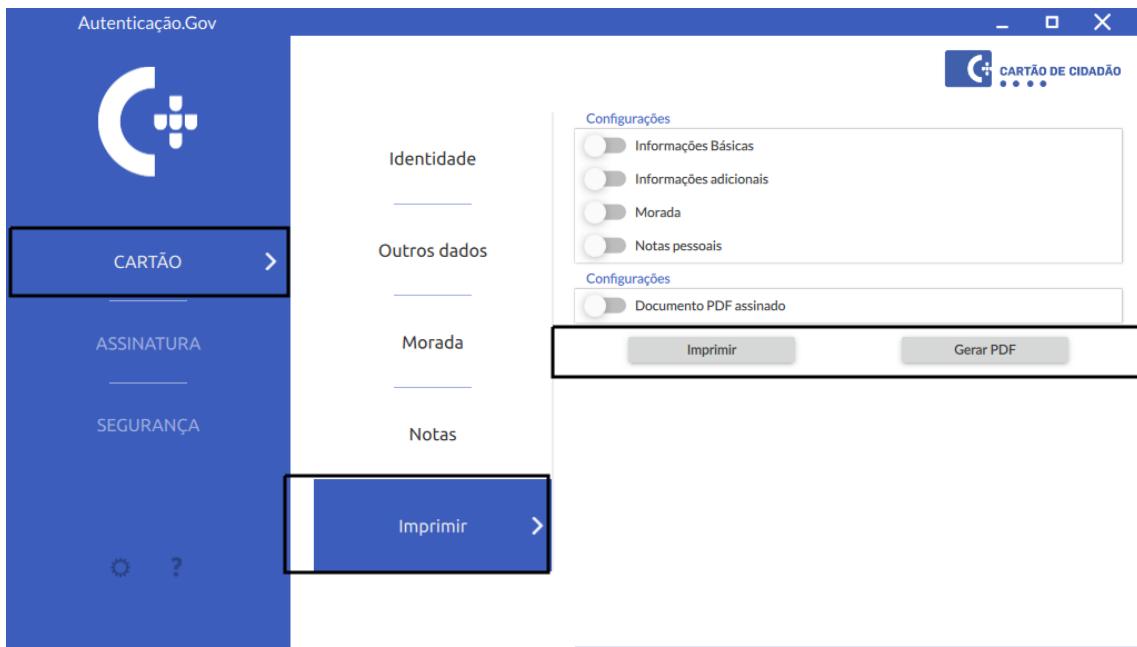


4.2.1.5 Imprimir

A aplicação permite a exportação dos dados do Cartão de Cidadão para um documento no formato PDF ou a impressão direta do documento.

Para executar estas operações deverá executar os seguintes passos:

1. No menu principal, selecionar **Cartão** e no menu secundário a opção **Imprimir**.
2. Na área de trabalho deverá selecionar os grupos de campos a incluir no documento e selecionar a opção **Imprimir** ou **Gerar PDF**.



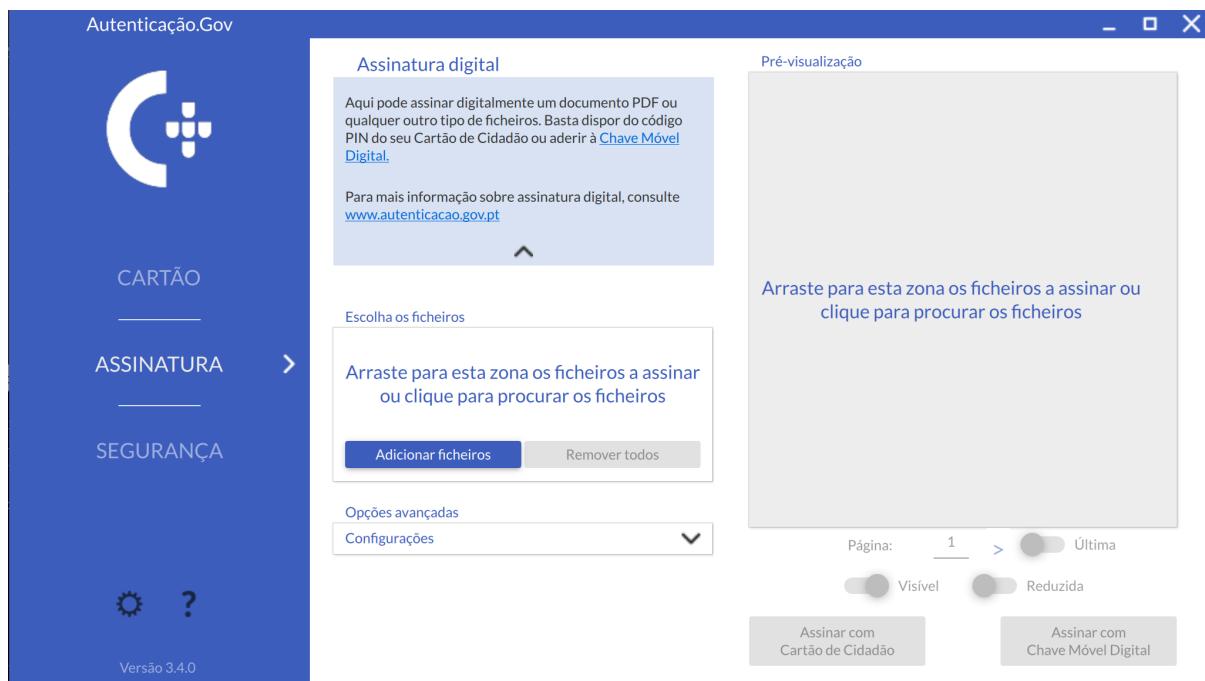
O documento a ser exportado e/ou impresso terá um aspeto gráfico conforme a imagem seguinte.

 CARTÃO DE CIDADÃO																																			
DADOS PESSOAIS																																			
<table border="0"> <tr> <td colspan="2">IDENTIDADE</td> </tr> <tr> <td><u>Nome(s)</u></td> <td>MANUEL</td> </tr> <tr> <td><u>Apelido(s)</u></td> <td>DIAS COSTA</td> </tr> <tr> <td><u>Sexo</u></td> <td><u>Altura</u></td> </tr> <tr> <td>M</td> <td>1,64</td> </tr> <tr> <td><u>Número de Documento</u></td> <td>00000680 7 ZZ6</td> </tr> <tr> <td><u>Pai</u></td> <td>PEDRO SILVA</td> </tr> <tr> <td colspan="2"><u>Indicações Eventuais</u></td> </tr> <tr> <td colspan="2">Não pode assinar;Sem ID Esq;Sem ID Dta</td> </tr> </table>			IDENTIDADE		<u>Nome(s)</u>	MANUEL	<u>Apelido(s)</u>	DIAS COSTA	<u>Sexo</u>	<u>Altura</u>	M	1,64	<u>Número de Documento</u>	00000680 7 ZZ6	<u>Pai</u>	PEDRO SILVA	<u>Indicações Eventuais</u>		Não pode assinar;Sem ID Esq;Sem ID Dta																
IDENTIDADE																																			
<u>Nome(s)</u>	MANUEL																																		
<u>Apelido(s)</u>	DIAS COSTA																																		
<u>Sexo</u>	<u>Altura</u>																																		
M	1,64																																		
<u>Número de Documento</u>	00000680 7 ZZ6																																		
<u>Pai</u>	PEDRO SILVA																																		
<u>Indicações Eventuais</u>																																			
Não pode assinar;Sem ID Esq;Sem ID Dta																																			
<table border="0"> <tr> <td><u>Nacionalidade</u></td> <td><u>Data de Nascimento</u></td> </tr> <tr> <td>PRT</td> <td>20 12 1980</td> </tr> <tr> <td><u>Data de Validade</u></td> <td>19 07 2021</td> </tr> <tr> <td><u>Mãe</u></td> <td>MARIA SILVA</td> </tr> </table>			<u>Nacionalidade</u>	<u>Data de Nascimento</u>	PRT	20 12 1980	<u>Data de Validade</u>	19 07 2021	<u>Mãe</u>	MARIA SILVA																									
<u>Nacionalidade</u>	<u>Data de Nascimento</u>																																		
PRT	20 12 1980																																		
<u>Data de Validade</u>	19 07 2021																																		
<u>Mãe</u>	MARIA SILVA																																		
<table border="0"> <tr> <td colspan="3">OUTROS DADOS</td> </tr> <tr> <td><u>Nº Identificação Fiscal</u></td> <td><u>Nº Segurança Social</u></td> <td><u>Nº Utente de Saúde</u></td> </tr> <tr> <td>217454445</td> <td>12016203840</td> <td>396148978</td> </tr> <tr> <td><u>Entidade Emissora</u></td> <td colspan="2"><u>Data de Emissão</u></td> </tr> <tr> <td>República Portuguesa</td> <td colspan="2">20 07 2016</td> </tr> <tr> <td><u>Tipo de Documento</u></td> <td><u>Local de Pedido</u></td> <td><u>Estado do Cartão</u></td> </tr> <tr> <td>Cartão de Cidadão</td> <td>Departamento Cartão de Cidadão</td> <td>O Cartão de Cidadão não foi ativado.</td> </tr> <tr> <td><u>Versão do Cartão</u></td> <td colspan="2"></td> </tr> <tr> <td>006.004.22</td> <td colspan="2"></td> </tr> </table>			OUTROS DADOS			<u>Nº Identificação Fiscal</u>	<u>Nº Segurança Social</u>	<u>Nº Utente de Saúde</u>	217454445	12016203840	396148978	<u>Entidade Emissora</u>	<u>Data de Emissão</u>		República Portuguesa	20 07 2016		<u>Tipo de Documento</u>	<u>Local de Pedido</u>	<u>Estado do Cartão</u>	Cartão de Cidadão	Departamento Cartão de Cidadão	O Cartão de Cidadão não foi ativado.	<u>Versão do Cartão</u>			006.004.22								
OUTROS DADOS																																			
<u>Nº Identificação Fiscal</u>	<u>Nº Segurança Social</u>	<u>Nº Utente de Saúde</u>																																	
217454445	12016203840	396148978																																	
<u>Entidade Emissora</u>	<u>Data de Emissão</u>																																		
República Portuguesa	20 07 2016																																		
<u>Tipo de Documento</u>	<u>Local de Pedido</u>	<u>Estado do Cartão</u>																																	
Cartão de Cidadão	Departamento Cartão de Cidadão	O Cartão de Cidadão não foi ativado.																																	
<u>Versão do Cartão</u>																																			
006.004.22																																			
<table border="0"> <tr> <td colspan="3">MORADA</td> </tr> <tr> <td><u>Distrito Nacional</u></td> <td><u>Concelho</u></td> <td><u>Lado</u></td> </tr> <tr> <td>PORTO</td> <td>PORTO</td> <td>A</td> </tr> <tr> <td><u>Freguesia</u></td> <td colspan="2"><u>Localidade</u></td> </tr> <tr> <td>CEDOFEITA,ILDEFONSO,SÉ,MIRAGAIA,NICOLAU,VITÓRIA</td> <td colspan="2">PORTO</td> </tr> <tr> <td><u>Tipo de Via</u></td> <td><u>Nome da Via</u></td> <td><u>Localidade Postal</u></td> </tr> <tr> <td>PONTE</td> <td>DE DOM LUIΣ I</td> <td>PORTO</td> </tr> <tr> <td><u>Nº da Porta</u></td> <td><u>Andar</u></td> <td><u>Código Postal</u></td> </tr> <tr> <td>12</td> <td>1</td> <td>4000-018</td> </tr> <tr> <td><u>Lugar</u></td> <td colspan="2"><u>Localidade Postal</u></td> </tr> <tr> <td>TABULEIRO SUPERIOR</td> <td colspan="2">PORTO</td> </tr> </table>			MORADA			<u>Distrito Nacional</u>	<u>Concelho</u>	<u>Lado</u>	PORTO	PORTO	A	<u>Freguesia</u>	<u>Localidade</u>		CEDOFEITA,ILDEFONSO,SÉ,MIRAGAIA,NICOLAU,VITÓRIA	PORTO		<u>Tipo de Via</u>	<u>Nome da Via</u>	<u>Localidade Postal</u>	PONTE	DE DOM LUIΣ I	PORTO	<u>Nº da Porta</u>	<u>Andar</u>	<u>Código Postal</u>	12	1	4000-018	<u>Lugar</u>	<u>Localidade Postal</u>		TABULEIRO SUPERIOR	PORTO	
MORADA																																			
<u>Distrito Nacional</u>	<u>Concelho</u>	<u>Lado</u>																																	
PORTO	PORTO	A																																	
<u>Freguesia</u>	<u>Localidade</u>																																		
CEDOFEITA,ILDEFONSO,SÉ,MIRAGAIA,NICOLAU,VITÓRIA	PORTO																																		
<u>Tipo de Via</u>	<u>Nome da Via</u>	<u>Localidade Postal</u>																																	
PONTE	DE DOM LUIΣ I	PORTO																																	
<u>Nº da Porta</u>	<u>Andar</u>	<u>Código Postal</u>																																	
12	1	4000-018																																	
<u>Lugar</u>	<u>Localidade Postal</u>																																		
TABULEIRO SUPERIOR	PORTO																																		

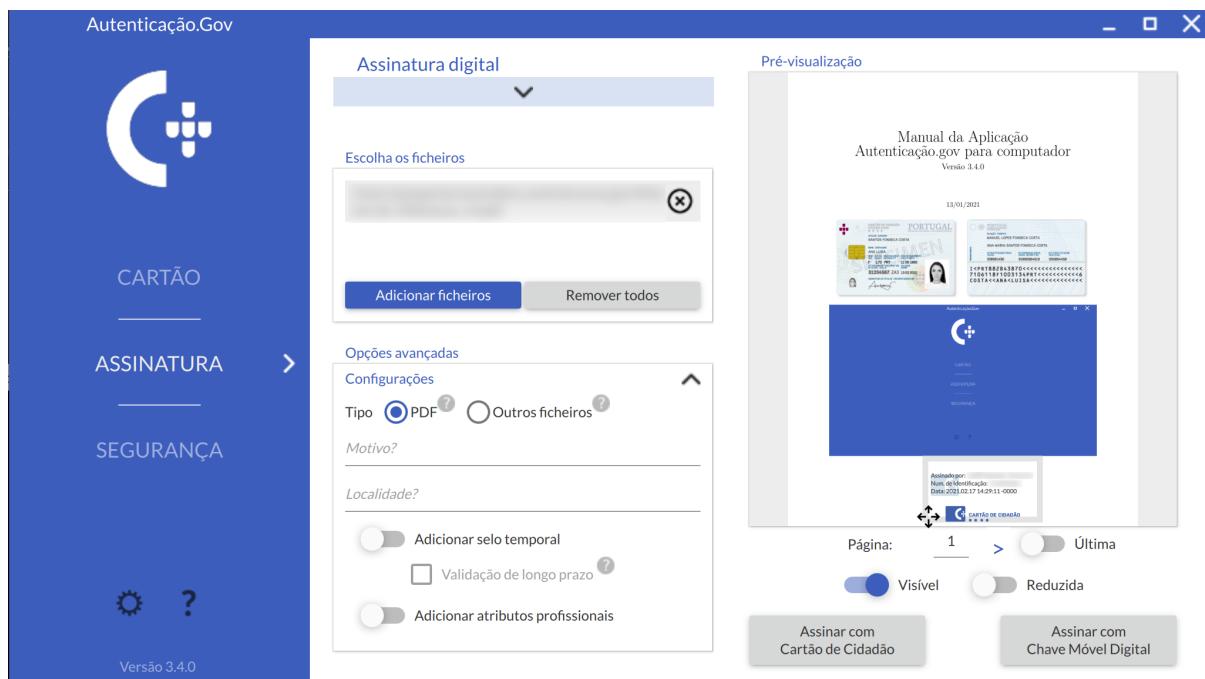
4.2.2 Assinatura digital

A assinatura digital permite ao titular de um **Cartão de Cidadão** ou da **Chave Móvel Digital**, por vontade própria, assinar com a chave pessoal existente no seu Cartão de Cidadão ou com a Chave Móvel Digital.

No menu **Assinatura** pode assinar um documento PDF ou outro qualquer documento com possibilidade de assinar vários documentos ao mesmo tempo, adicionar atributos profissionais, bem como configurar outras opções. A assinatura digital em documentos PDF foi desenvolvida de acordo com a especificação da Adobe, podendo assim ser validada posteriormente no software *Adobe Reader*.



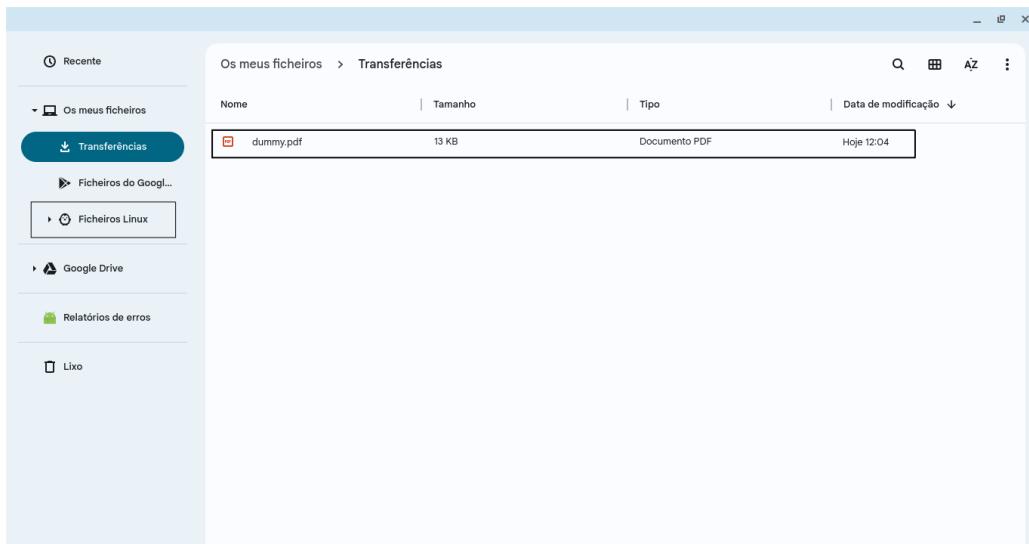
Os ficheiros a assinar podem ser selecionados arrastando-os para a área de pré-visualização ou utilizando a combinação de teclas **CTRL+V** (colar). Pode também clicar na área de pré-visualização ou no botão **Adicionar ficheiros** e selecionar manualmente os ficheiros. Será exibida uma janela para selecionar os ficheiros que pretende assinar. Os ficheiros selecionados serão apresentados na secção Escolha os ficheiros, como podemos visualizar na imagem seguinte.



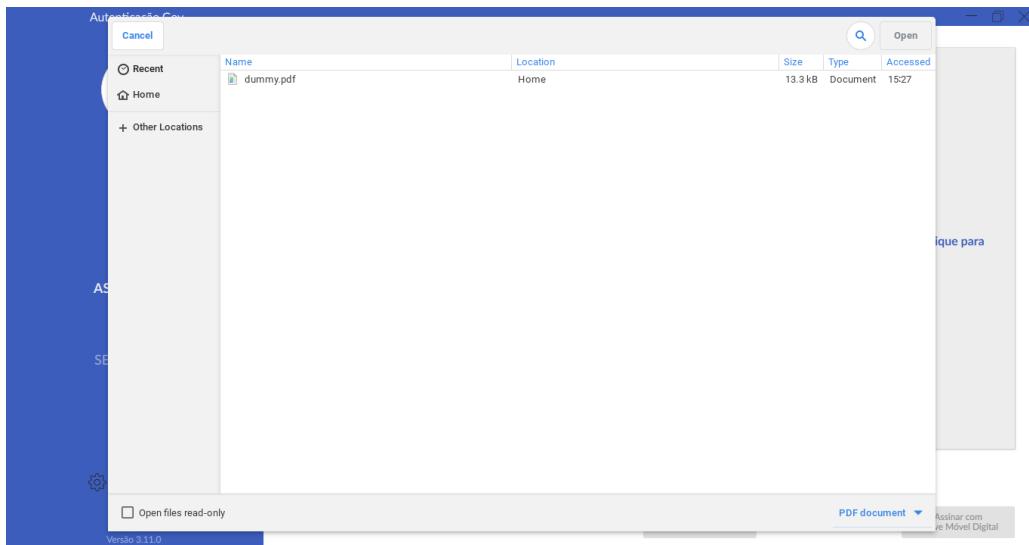
- **Escolha os ficheiros:**

- O botão **Adicionar ficheiros** Abre uma nova janela que permitirá selecionar os documentos a serem assinados.
- É possível remover ficheiros individualmente, utilizando o botão que se encontra junto ao nome de cada ficheiro, ou todos, pressionando o botão **Remover todos**.
- **Em ChromeOS**, para que os ficheiros aparecerem para serem selecionados, é necessário o seguinte procedimento:

- * Arrastar o ficheiro que quer assinar para a pasta **Ficheiros Linux**.



- * Após arrastar o ficheiro, este aparecerá quando clickar no botão **Adicionar ficheiros**.



- **Pré-visualização da assinatura:** Permite visualizar o documento a ser assinado e ajustar a posição e o tamanho do selo de assinatura, movendo-o para o local pretendido com as dimensões desejadas. A pré-visualização existe apenas para assinatura do tipo **PDF**, sendo possível pré-visualizar qualquer um dos ficheiros de uma multi-assinatura através de um clique no nome do ficheiro na aplicação.

• Opções avançadas - Configurações:

Após a seleção dos ficheiros, deverá selecionar as opções da assinatura. As configurações da assinatura são as seguintes:

- **Tipo:** Tipo de assinatura campo obrigatório permite selecionar assinatura de ficheiros:
 - * **PDF:** PAdES (*PDF Advanced Electronic Signatures*).
 - * **Outros ficheiros:** Pacote ASiC com *XML Advanced Electronic Signatures* (XAdES). Este pacote é um arquivo ZIP criado de acordo com a especificação ASiC (Associated

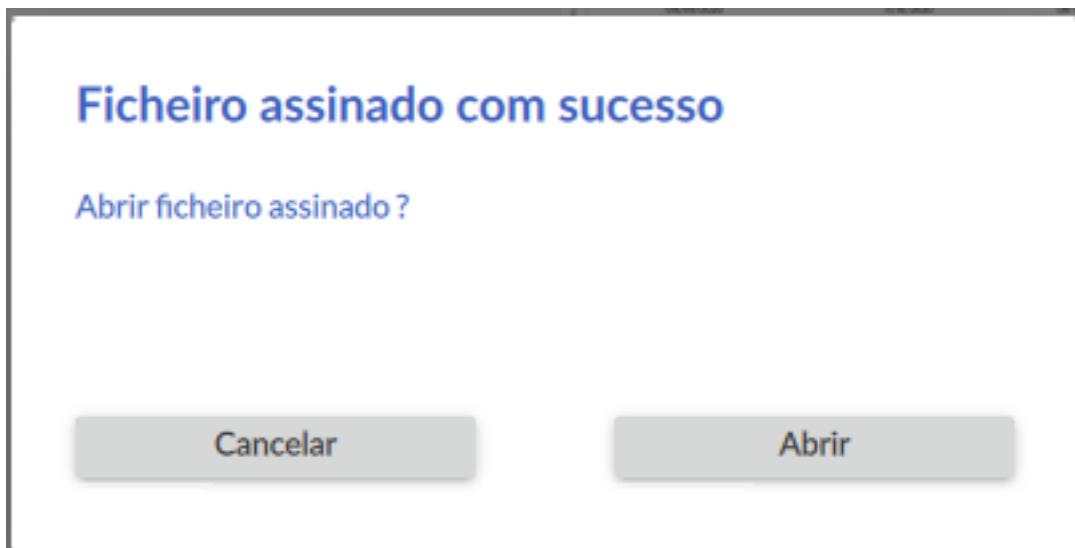
Signature Container) desenvolvido pela ETSI (European Telecommunications Standards Institute) e segue os padrões da UE. Este arquivo contém a informação assinada (ficheiros originais) e a respetiva assinatura no formato XAdES.

- **Motivo:** Motivo da assinatura campo opcional permite ao signatário indicar o motivo da sua assinatura. Disponível para assinaturas do tipo **PDF**.
- **Localização:** Local onde a assinatura foi efetuada campo opcional - permite ao signatário indicar o local onde esta assinatura foi efetuada. Disponível para assinaturas do tipo **PDF**.
- **Adicionar selo temporal:** Adiciona um selo temporal, provando a data à qual a assinatura foi efetuada. Esta é a única forma de provar que o documento existia a determinada hora, pois é aplicada ao documento a data e hora que este está a ser assinado, de forma segura. Note-se que a hora apresentada no selo visível é a hora local do computador onde foi efetuada a assinatura e pode não coincidir com a hora do selo temporal (obtida a partir de um servidor remoto). Disponível para assinaturas do tipo **PDF** e **Outros Ficheiros**. Ver tópico Serviço de Selos Temporais na página Configuração de assinaturas
 - * **Validação de longo prazo:** Com a opção ativa, os dados necessários para validar a assinatura digital serão incluídos no ficheiro final assinado. Deste modo, é possível provar no futuro que no momento da assinatura o certificado do cartão (ou Chave Móvel Digital) e respetiva cadeia não estavam revogados ou expirados. Este nível é recomendado para documentos que estão destinados a serem arquivados por um longo período de tempo. A assinatura com validação de longo prazo obedece à especificação do perfil PAdES-LTA.
- **Adicionar atributos profissionais:** A funcionalidade de assinatura de profissionais permite ao cidadão autenticar-se na qualidade das funções que desempenha na sociedade enquanto profissional qualificado. Na secção Atributos Profissionais é indicado o procedimento para carregar os atributos profissionais. Disponível para assinaturas do tipo **PDF**.
Para mais informações sobre atributos profissionais, consulte o seguinte website:
<https://www.autenticacao.gov.pt/a-autenticacao-de-profissionais>
- **Visível:** Permite que a assinatura fique visível no documento PDF. Disponível para assinaturas do tipo **PDF**.
- **Página:** Poderá escolher a página onde será apresentada a assinatura. Disponível para assinaturas do tipo **PDF**.
- **Última:** Poderá escolher a última página para apresentar a assinatura. Disponível para assinaturas do tipo **PDF**.
- **Reduzida:** Permite utilizar um selo de assinatura de tamanho reduzido. O selo reduzido apresenta, sempre pela mesma ordem, os campos: "Nome Completo", "NIC" e "Data de assinatura", excepto se o espaço não for suficiente (nomes completos longos). Nesse caso são colocados apenas campos até preencher o espaço, pela mesma ordem. Disponível para assinaturas do tipo **PDF**.

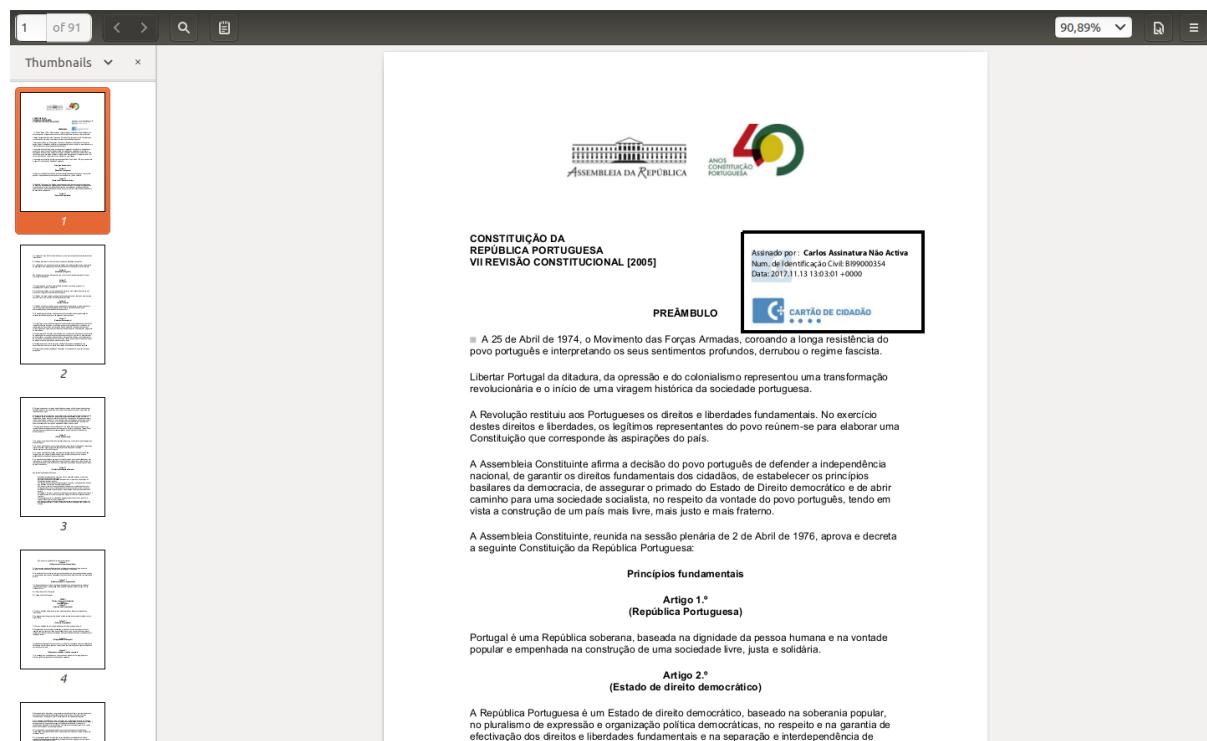
Após selecionar as opções pretendidas, na área indicada na figura anterior, arraste a pré-visualização do selo de assinatura para a localização pretendida e de seguida prima o botão **Assinar com Cartão de Cidadão** ou **Assinar com Chave Móvel Digital**.

O botão **Assinar com Cartão de Cidadão** só está disponível quando o Cartão de Cidadão estiver inserido no leitor de cartões e for corretamente lido pela aplicação.

Após clicar em **Assinar** deverá escolher a localização da pasta e do ficheiro onde guardar o ficheiro assinado (Não é possível substituir o ficheiro original) e seguir o procedimento de assinatura (ver secção Introdução de chave). Em seguida é apresentado uma mensagem a indicar que a assinatura digital foi efetuada com sucesso.



A imagem seguinte é um exemplo de um ficheiro assinado com a aplicação **Autenticação.Gov**.



Em caso de problemas na validação das assinaturas, verifique se está relacionado com o tópico Problemas com a nova cadeia de confiança.

4.2.2.1 Introdução de chave A assinatura digital permite ao titular de um **Cartão de Cidadão** ou da **Chave Móvel Digital**, por vontade própria, assinar com a chave pessoal existente no seu Cartão de Cidadão ou com a Chave Móvel Digital.

No caso de pretender assinar com a chave pessoal existente no seu Cartão de Cidadão, ao selecionar a opção **Assinar com Cartão de Cidadão**, deverá introduzir o PIN de assinatura, conforme a figura seguinte.

Assinar com Cartão de Cidadão



ATENÇÃO: Vai realizar uma assinatura eletrónica válida com o seu Cartão de Cidadão.

PIN de assinatura

CANCELAR **CONFIRMAR**

No caso, de pretender assinar com a Chave Móvel Digital, ao selecionar a opção **Assinar com Chave Móvel Digital**, deverá introduzir as respetivas credenciais, conforme a figura seguinte.

Assinar com Chave Móvel Digital



Clique para ativar ou gerir a assinatura da sua Chave Móvel Digital

Inserir número de telemóvel associado

+351 - Portugal ▾

Inserir PIN da assinatura da Chave Móvel Digital

CANCELAR **CONFIRMAR**

4.2.2.2 Verificação de documento PDF assinado em Windows ou MacOS Após aplicar uma assinatura digital num documento, esta deverá ser identificada automaticamente ao abrir o documento em *Adobe Reader*. A imagem seguinte ilustra o *Adobe Reader* com um documento PDF que inclui a assinatura efetuada no passo anterior:

Assinado por: **Carlos Assinatura Não Activa**
Num. de Identificação Civil: BI99000354
Data: 2016.11.23 12:51:14 +0000



Mesmo quando a assinatura não esteja visível (se a opção "Visível" não for selecionada no momento da assinatura), a assinatura deverá ser sempre validada no painel de assinaturas, dado que permite a visualização do estado da assinatura tendo em conta a cadeia de confiança e as propriedades criptográficas da mesma.

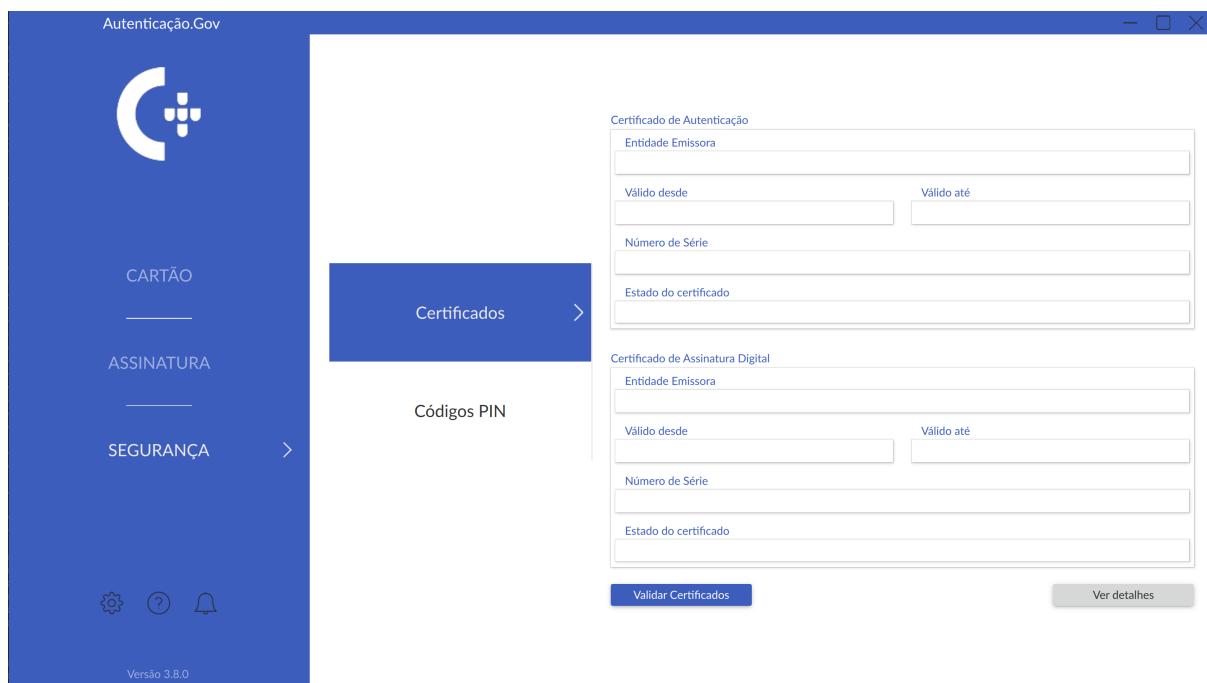
A captura de tela mostra o painel de assinaturas do Adobe Reader. No topo, uma barra azul indica: "Assinado e todas as assinaturas são válidas.". Abaixo, uma lista de assinaturas é exibida. A única assinatura visível é a "Rev. 1: Assinado por Carlos Assinatura Não Activa", que está marcada com um ícone de checkmark verde. O detalhe da assinatura mostra que ela é válida porque o documento não foi modificado desde a aplicação da assinatura, foi assinado pelo usuário atual, o horário de assinatura é o constante no computador do signatário, e a assinatura é habilitada para LTV. Um link para "Detalhes da assinatura" está disponível.

Nota: Ao utilizar a função do Adobe Reader "bloquear o conteúdo depois de assinar", evite assinar digitalmente o documento de novo. Apesar de ser permitido adicionar mais assinaturas segundo o standard PAdES, o Adobe Reader invalida a primeira assinatura neste processo.

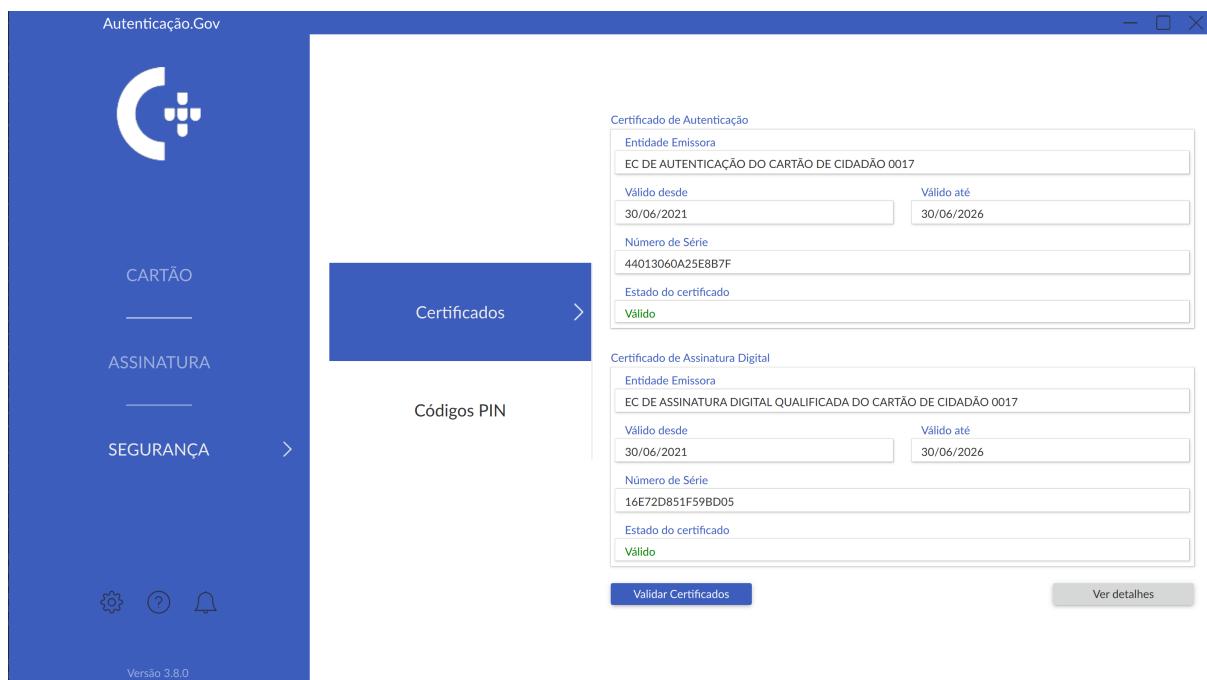
4.2.3 Segurança

A aplicação permite efetuar operações relativas à segurança do Cartão de Cidadão.

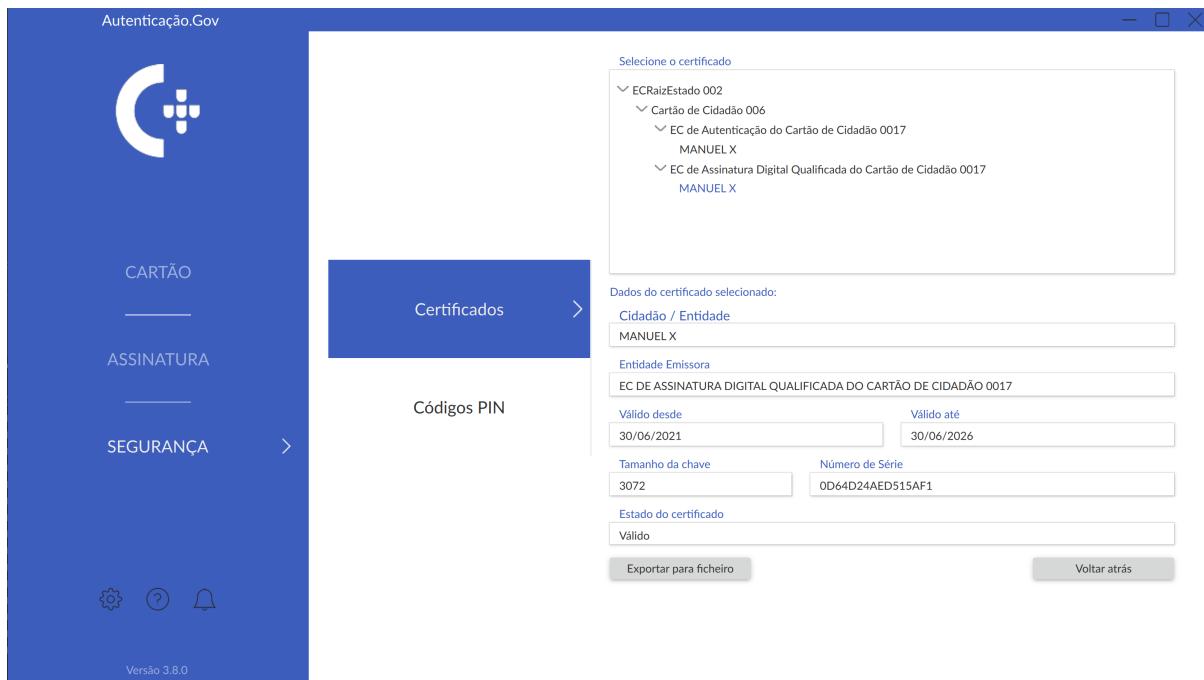
4.2.3.1 Certificados Neste menu é possível verificar os certificados do Cidadão e a cadeia de confiança formada pelas várias Entidades de Certificação do Cartão de Cidadão e do Estado Português.



O preenchimento dos campos "Estado do certificado" correspondem a uma validação junto da Infraestrutura do Cartão de Cidadão e como tal exige ligação à Internet. Esta validação é acionada ao pressionar o botão *Validar Certificados*.



É possível consultar a cadeia de certificados e os detalhes de cada certificado pressionando o botão *Ver detalhes*, visível na imagem anterior.



4.2.3.2 Código PIN Neste menu é possível verificar e alterar os códigos PIN do Cartão de Cidadão.

- **PIN de Autenticação:** Este PIN é usado para se autenticar em sites e aplicações que suportem o Cartão de Cidadão.
- **PIN de Assinatura:** Este PIN é usado para assinar documentos ou transações em aplicações que suportem o Cartão de Cidadão.
- **PIN de Morada:** Este PIN é usado para leitura de morada.



Alterar PIN de autenticação



Introduza o seu PIN de autenticação do Cartão de Cidadão.

PIN Actual

Novo PIN

Confirmar novo PIN

CANCELAR **CONFIRMAR**

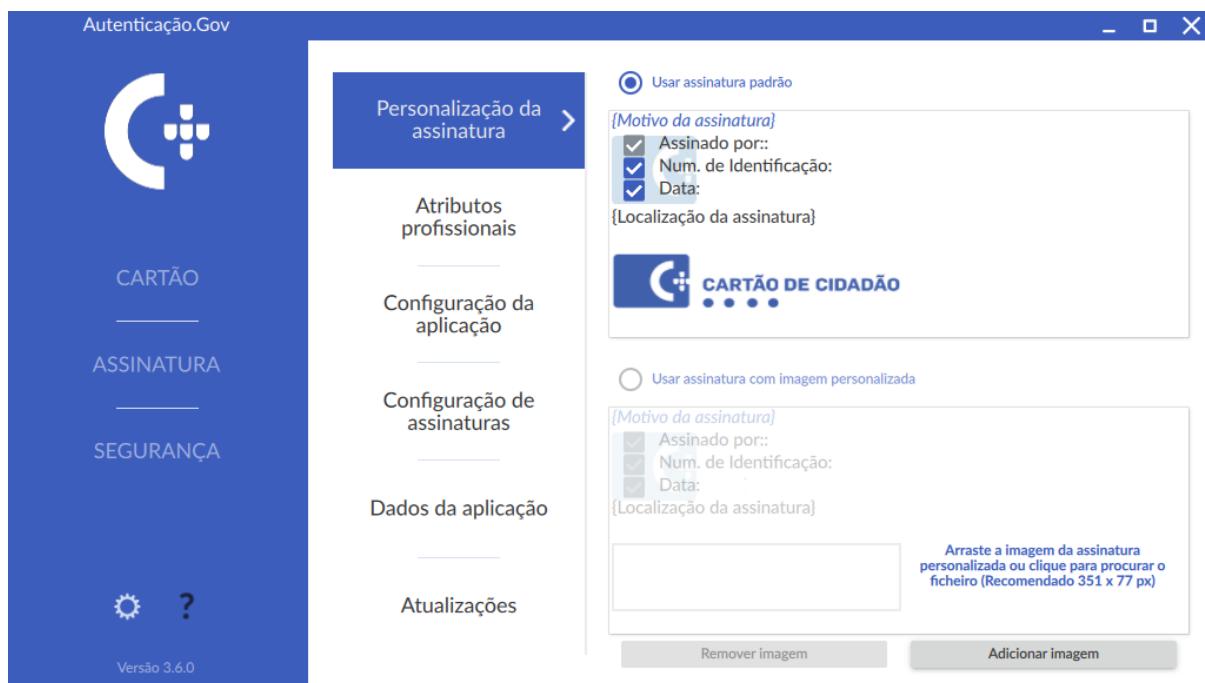
4.2.4 Configurações

4.2.4.1 Personalização da Assinatura Neste menu é possível personalizar a assinatura digital, substituindo a imagem do cartão do cidadão por uma imagem à escolha do utilizador.

O botão **Adicionar assinatura** permite selecionar uma imagem que será utilizada na assinatura personalizada. Após adicionar uma imagem, esta página da aplicação permitirá selecionar a opção **Usar assinatura padrão** ou **Usar assinatura personalizada**, conforme a escolha do utilizador.

O tamanho mínimo recomendado para a imagem é de 351 x 77px.

É, também, possível escolher incluir, ou não, a data de assinatura e o número de identificação civil na assinatura. Para tal, basta selecionar as checkboxes pretendidas neste menu.

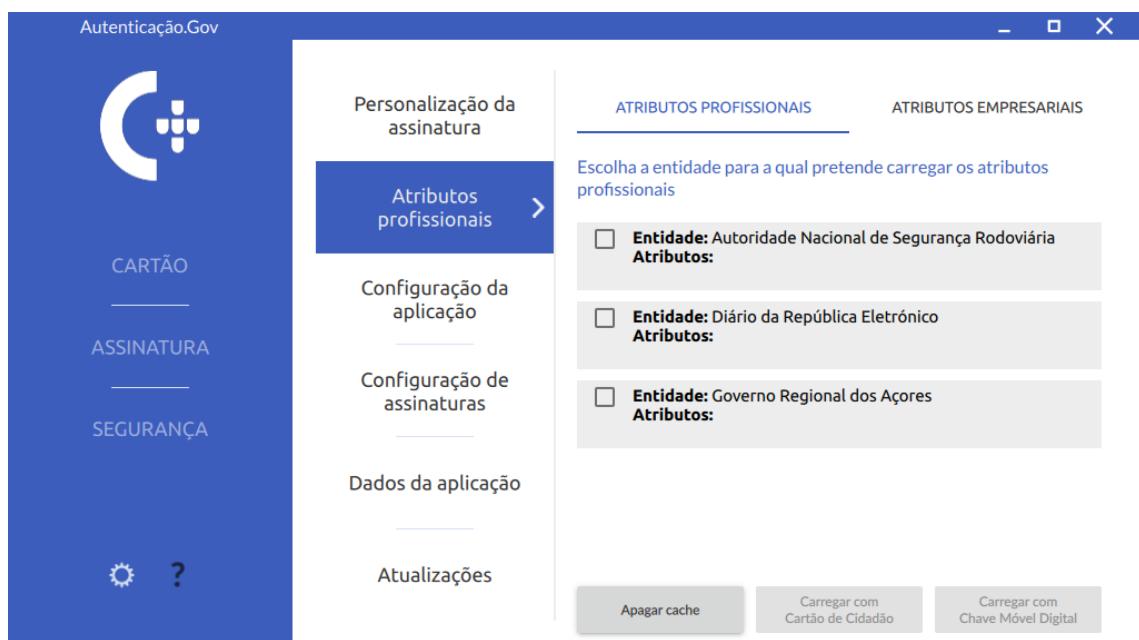


4.2.4.2 Atributos Profissionais O Sistema de Certificação de Atributos Profissionais (SCAP) permite ao cidadão, através do Cartão de Cidadão ou da Chave Móvel Digital, assinar um documento na qualidade das funções que desempenha enquanto profissional. Para mais informações, consulte o seguinte website:

<https://www.autenticacao.gov.pt/a-autenticacao-de-profissionais>

Em primeiro lugar, selecione o tipo de atributos:

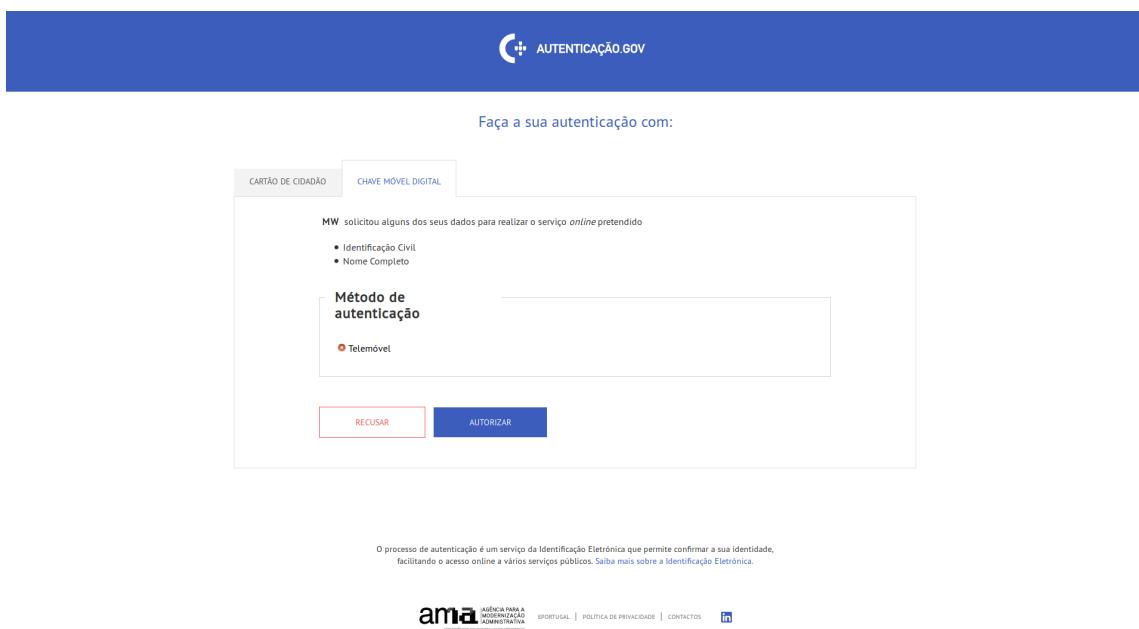
- **No caso dos Atributos Profissionais** selecione a(s) entidade(s) fornecedora(s) dos seus atributos profissionais que pretende carregar atributos e clique em **Carregar atributos**.
- **No caso dos Atributos Empresariais** os atributos do utilizador são carregados automaticamente, quando clicar no botão de carregamento de atributos.



Seguidamente, deverá clicar num dos botões de carregamento de atributos, consoante pretenda, respetivamente, carregar os atributos com o Cartão de Cidadão ou Chave Móvel Digital (CMD):

- **Carregar com Cartão de Cidadão:** após selecionar este botão, deverá introduzir o PIN de autenticação e aguardar pelo carregamento de atributos.
- **Carregar com Chave Móvel Digital:** ao selecionar este botão será iniciado um processo de autenticação no seu navegador web predefinido (por exemplo, Google Chrome, Mozilla Firefox, Safari ou outro). Deverá carregar em **Autorizar** e preencher o formulário com número de telemóvel associado à sua Chave Móvel Digital e respetivo PIN. De seguida, carregue **Autenticar** e introduza o código de segurança que recebeu no telemóvel por SMS ou notificação da aplicação Autenticação.gov. Pressione **Confirmar** para completar a autenticação.

Se concluiu a autenticação com sucesso, pode regressar à aplicação e aguardar pelo carregamento de atributos.



4.2.4.3 Configuração da aplicação Nesta janela é possível configurar alguns aspetos do funcionamento da aplicação, nomeadamente:

- **Leitor de Cartões:** Permite selecionar o leitor de cartões a utilizar. Existe também uma opção que permite ativar ou desativar a funcionalidade PINPAD (Os leitores com PINPAD são os leitores de cartões que possuem teclado para introdução segura do código PIN) nos leitores. Se esta opção estiver desativada, os leitores com PINPAD terão comportamento idêntico aos leitores sem PINPAD.
- **Início:** Opções relativas ao arranque da aplicação.
- **Atualizações automáticas:** Permite ativar ou desativar a verificação de novas atualizações quando se inicia a aplicação. Esta opção apenas ativa ou desativa a verificação de novas versões da aplicação e não tem qualquer influência na atualização dos certificados, esta é feita automaticamente, sempre que necessário, aquando do início da aplicação.
- **Idioma:** Selecionar o idioma da aplicação.
- **Aparência:** Opções relativas à aparência da aplicação. Nesta secção há uma opção que permite ativar e desativar as animações de transição entre menus.
- **Escala da aplicação:** Opções relativas ao tamanho do texto e outros componentes da aplicação.

- **Modo diagnóstico:** Permite ativar ou desativar o modo de diagnóstico da aplicação. Este modo eleva o nível de detalhe do *log* para *debug*, o que, em caso de problemas com a aplicação, pode ajudar a equipa de suporte na resolução do problema.

A partir da versão 3.5.0 da aplicação, para todos os sistemas operativos, para ajudar a obter os ficheiros de log, existe uma nova funcionalidade que permite criar um "Relatório de Suporte". Para isso só é necessário pressionar o botão "Criar relatório". Ao pressionar o botão Criar relatório é criada uma pasta comprimida (ficheiro zip) no Ambiente de Trabalho que contém todos os ficheiros de log. Deve enviar esta pasta (zip), anexada à descrição do problema, para o contacto de suporte. Para mais informações consulte o capítulo Obtenção do relatório para análise através do menu Configurações.

Os ficheiros de *log* por omissão são criados nas seguintes localizações e têm como nome o prefixo .PTEID:

- **Windows:** Na pasta `log`, que se encontra na pasta de instalação (que por defeito é `C:\Program Files\Portugal Identity Card`), i.e.:
`C:\Program Files\Portugal Identity Card\log\`
- **MacOS:** Directória Home do utilizador, i.e.:
`/Users/Utilizador/`
- **Linux:** Directória Home do utilizador, i.e.:
`/home/Utilizador/`

No caso da aplicação não arrancar, é possível ativar o modo de diagnóstico usando as configurações do software Autenticação.gov via chaves de Registo em Windows ou ficheiro de configuração em Linux e MacOS.

- Em **Windows**, a chave de registo:
`HKEY_CURRENT_USER\Software\PTEID\logging\log_level;`
- Em **Linux**, a chave com nome "log_level" na secção logging do ficheiro:
`$HOME/.config/pteid.conf;`
- Em **MacOS**, a chave com nome "log_level" na secção logging do ficheiro:
`$HOME/Library/Preferences/pteid.conf.`

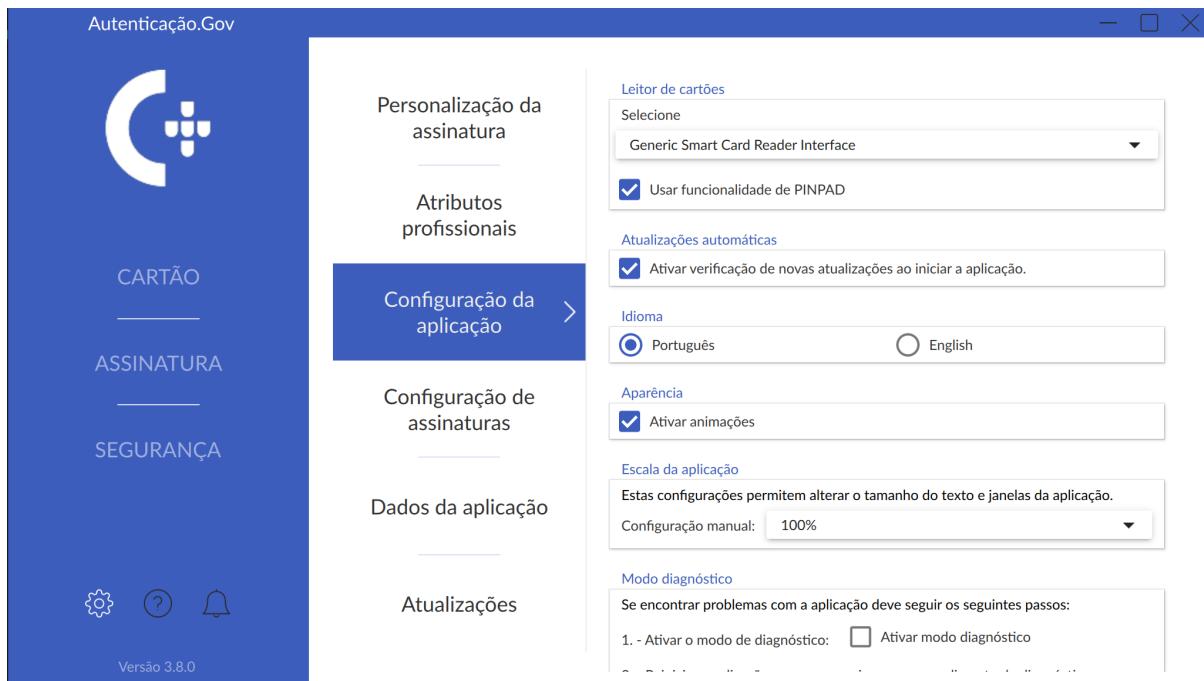
Os valores que a chave pode tomar são:

- debug (em caso de problemas com a aplicação, pode ajudar a equipa de suporte na resolução do problema)
- info
- warning
- error (valor por omissão)

Em ambiente empresariais deve alterar a seguinte configuração conforme descrito no capítulo Instruções de configuração em ambientes empresariais.

- **Aceleração gráfica:** Permite ativar escolher o modo de renderização gráfica da aplicação. A opção "Hardware (Placa gráfica)" deverá oferecer um melhor desempenho, mas em caso de problemas poderá ser necessário configurar uma opção alternativa (ver secção Problemas gráficos na aplicação.)
- **Configurações de rede:** Opções relativas à configuração de servidor de proxy. Em redes onde o acesso à Internet só é possível através de servidor de proxy HTTP/S será necessário configurar as seguintes informações de acesso:
 - **Proxy de sistema (Windows e MacOS).** Ao selecionar esta opção e se estiver definida uma configuração de *proxy* de sistema ou um *script* de auto configuração (*Proxy Autoconfig*), esta configuração será automaticamente utilizada pela aplicação e por outras aplicações que usem o *middleware* do cartão de cidadão.
 - **Servidor proxy:** Endereço IP / Hostname / Porto.
 - **Autenticação proxy:** Credenciais de acesso (se necessário).

A imagem seguinte permite visualizar o menu de configurações da aplicação.



4.2.4.4 Configuração de assinaturas Nesta janela é possível configurar alguns aspetos relativos à assinatura com o Cartão de Cidadão:

- **Certificados:** Opções relativas ao registo e remoção de certificados durante a inserção e remoção do cartão.

As opções de registo e remoção de certificados requerem que esta aplicação esteja em funcionamento (minimizada ou maximizada).

- **Serviço de Selos Temporais:** Configurar um serviço de selos temporais personalizado.

A aplicação permite seleccionar uma servidor diferente para a obtenção de selos temporais, uma vez que o servidor por defeito do Cartão do Cidadão (<http://ts.cartaodecidadao.pt/tsa/server>) tem um limite máximo de 20 pedidos em cada período de 20 minutos que se podem efectuar. Se este valor for excedido o serviço será bloqueado durante 24 horas, sem prejuízo de outras consequências em caso de repetição de situações de bloqueio. (para mais informações sobre o serviço de selo temporal/timestamps do Cartão do Cidadão, consulte a página <https://pki.cartaodecidadao.pt>).

Para usar um servidor diferente basta introduzir o url do servidor na caixa de texto.

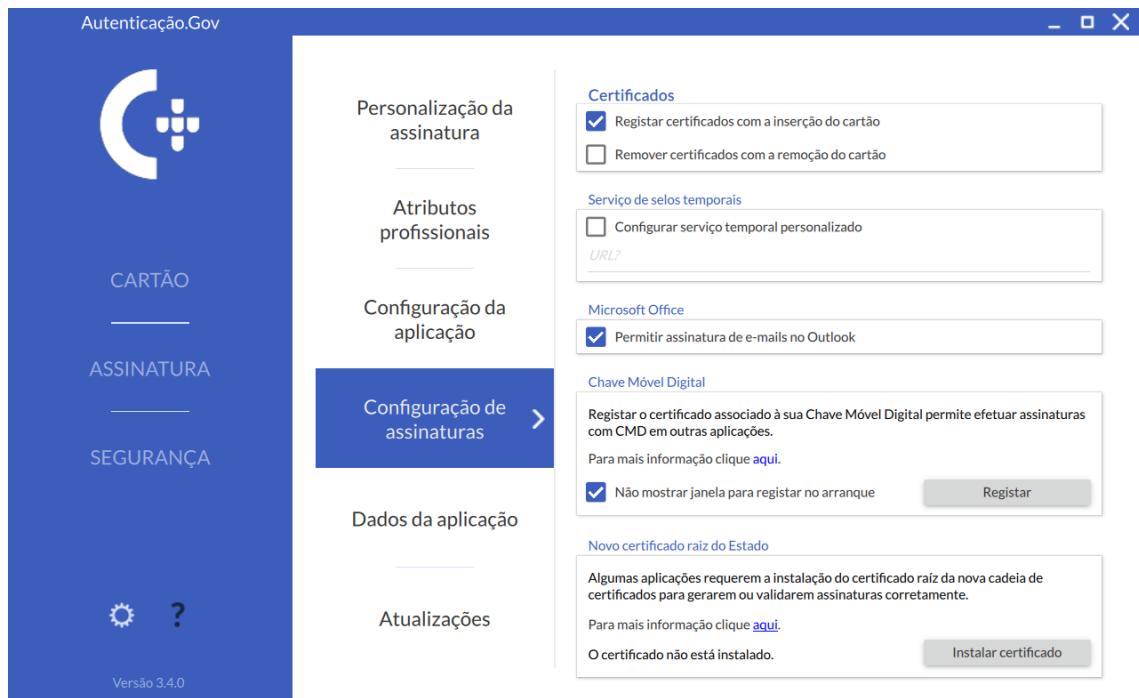
Após esta configuração tanto as assinaturas de documentos PDF (PAdES) bem como a assinaturas em formato XAdES vão usar este novo servidor configurado para obter os selos temporais ao assinar.

- **Microsoft Office (Windows):** Configurações relativas a assinaturas em aplicações do Microsoft Office.

- **Chave Móvel Digital (Windows):** Permite registar o certificado associado à sua conta da Chave Móvel Digital. Para saber mais consulte a secção Assinatura digital com Chave Móvel Digital.

- **Novo certificado raiz do Estado (Windows):** Permite instalar o certificado raiz da nova cadeia de certificados do cartão de cidadão na *Store* de certificados raiz confiáveis do Windows. Para saber mais consulte a secção Problemas com a nova cadeia de confiança.

A imagem seguinte permite visualizar o menu de configurações de assinaturas.

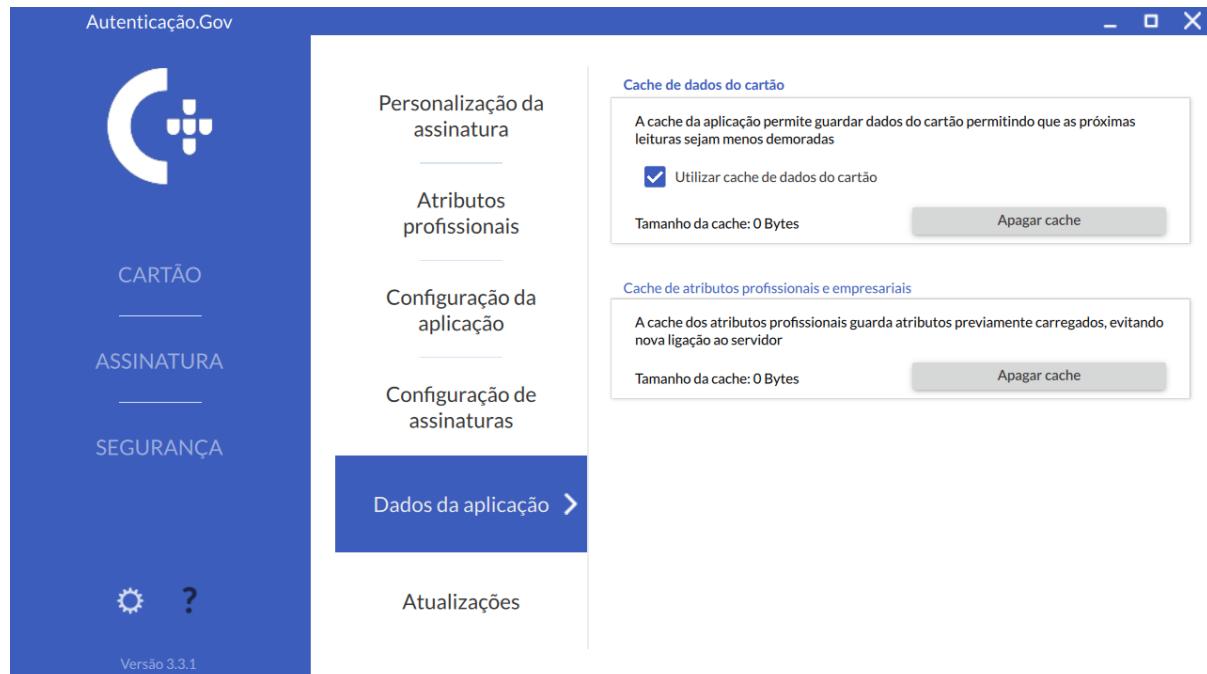


4.2.4.5 Dados da aplicação Neste separador é possível apagar os dados de cache armazenados das leituras dos cartões e do carregamento de atributos profissionais e empresariais.

Os dados armazenados relativos ao Cartão de Cidadão são os dados de identidade, a foto e a cadeia de certificação de autenticação e assinatura.

Relativamente aos atributos profissionais e empresariais são armazenados a lista de atributos pré-carregados.

Existe também a possibilidade de desabilitar a cache dos dados dos cartões, desativando a opção "Utilizar cache de dados do cartão".



4.2.4.6 Atualizações Nesta janela é possível verificar manualmente se existem atualizações para a aplicação. Caso existam atualizações, e se o utilizador o pretender, o download do instalador da aplicação

é feito automaticamente e em seguida iniciado o processo de instalação.

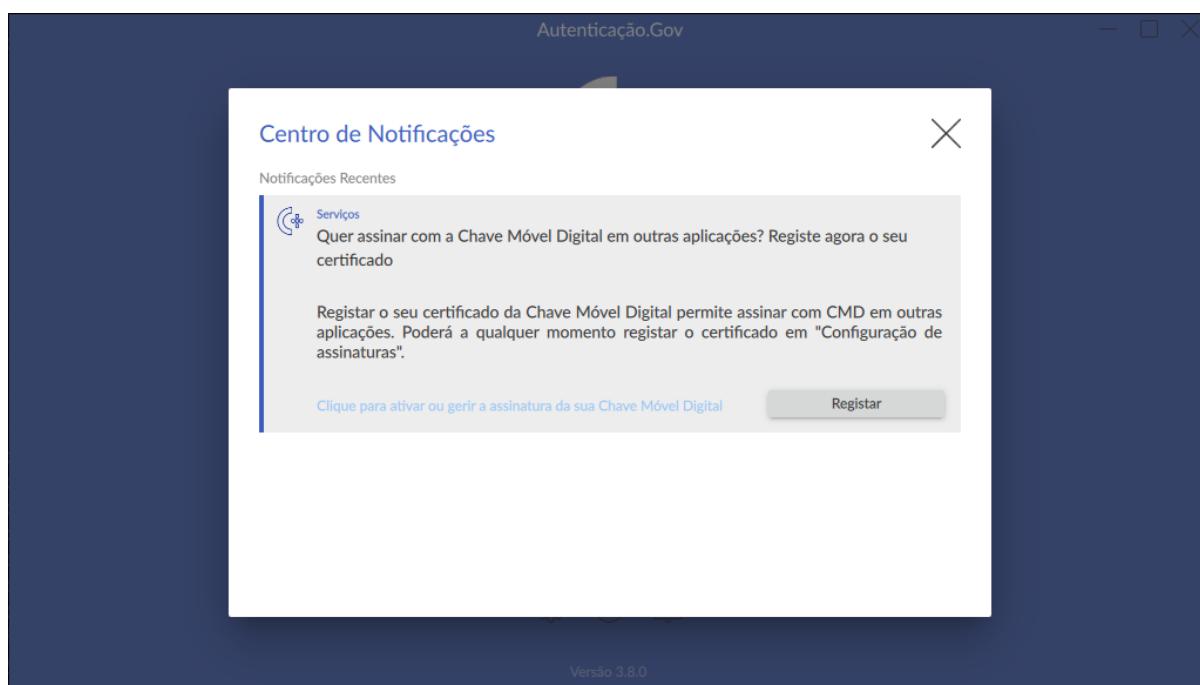
4.2.5 Ajuda

A janela ajuda fornece um resumo das funcionalidades da aplicação, indica o caminho para chegar a este mesmo manual e a página de suporte da aplicação.

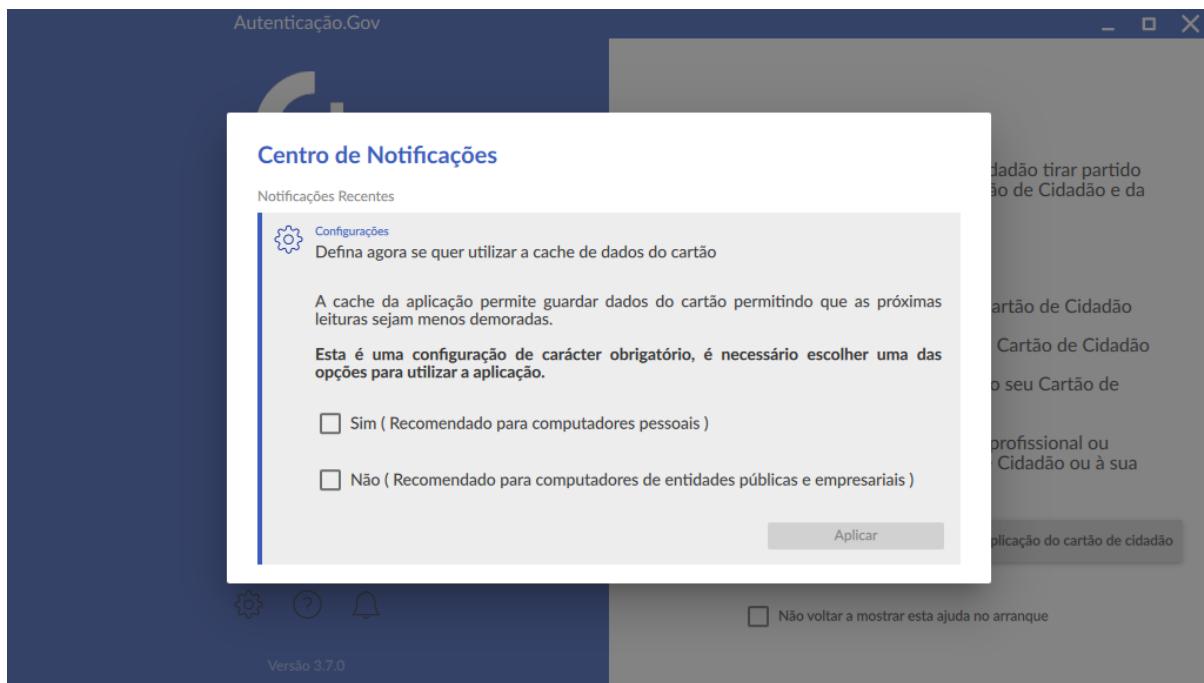


4.2.6 Centro de Notificações

Este menu disponibiliza aos utilizadores informações relativas a notícias, configurações e atualizações, no formato de notificações, e é aberto automaticamente no arranque da aplicação, caso existam notificações novas para mostrar ao utilizador.



No que diz respeito às configurações, podem existir notificações de caráter obrigatório cuja interação é necessária para utilizar a aplicação, como é o caso do uso da cache:



4.2.7 Acesso Contactless

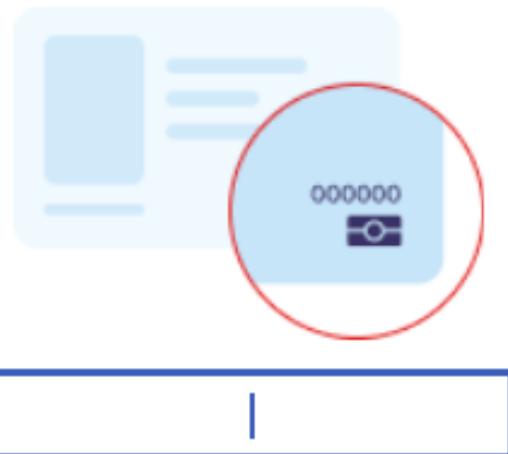
Importante: Funcionalidade disponível desde a versão 3.12.0 da aplicação

Para usar a interface contactless do novo Cartão de Cidadão será apresentada uma nova janela de diálogo na página que estiver em uso, por exemplo, página de Identidade, Morada, Certificados ou Assinatura. Esta janela exige que o utilizador insira o código de acesso ao cartão, que tem o objetivo de prevenir acessos não autorizados na leitura *contactless*.

Leitura de Cartão Contactless

Por favor insira o código de acesso ao seu cartão.

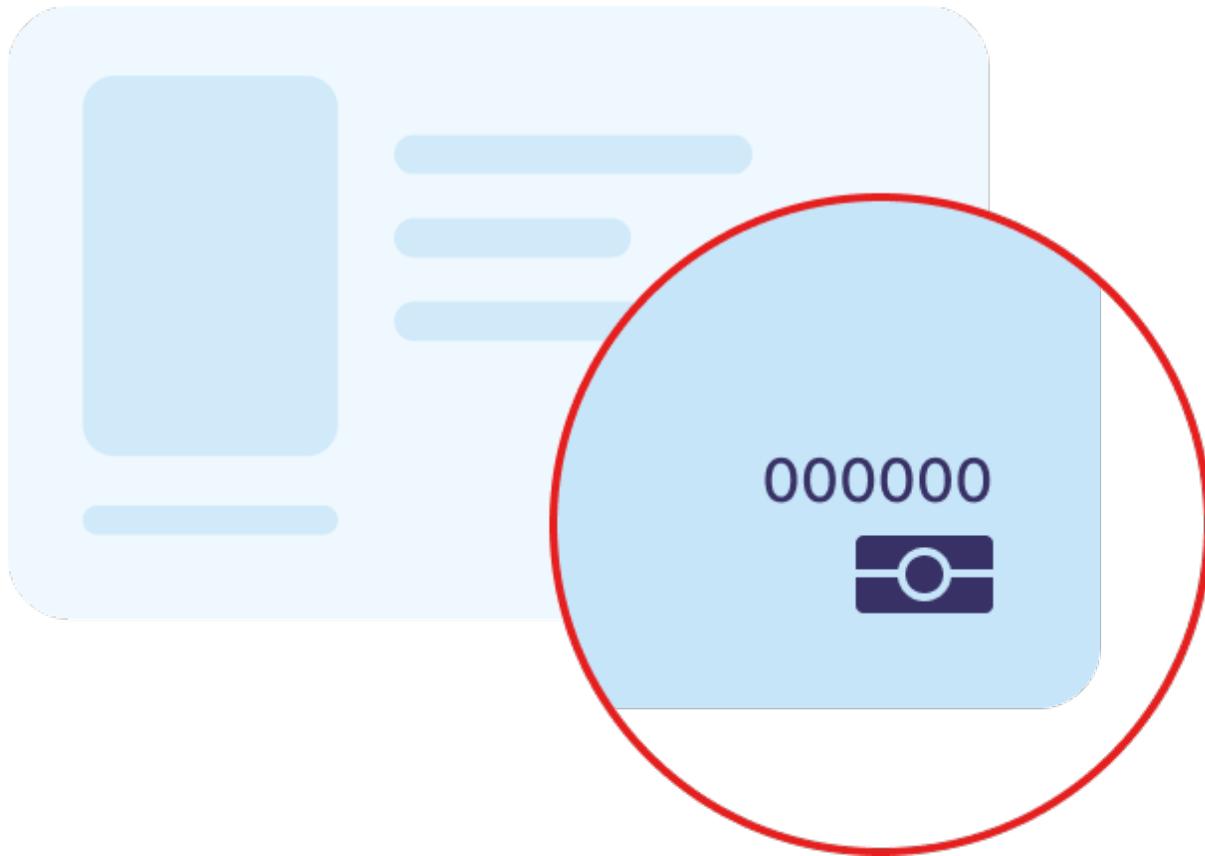
Este número de 6 dígitos está impresso no seu cartão no canto inferior direito.



Cancelar

OK

O código de acesso ao cartão é o código de 6 dígitos que se encontra no canto inferior direito dos novos Cartões de Cidadão.



Este código não será requerido em posteriores utilizações da aplicação com o mesmo cartão.

No entanto se não pretende que seja guardado o código de acesso, pode desligar esta opção no separador "Dados da aplicação" dentro do menu Configurações da aplicação.

NOTA: A utilização do cartão pelo interface contactless para assinatura ou autenticação em aplicações externas tais como o Adobe Acrobat Reader exige que este tenha sido lido uma vez na aplicação Autenticação.gov e que esteja ativa a opção "Guardar códigos de acesso" nas Configurações.

5 Integração com aplicações

O *middleware* do Cartão de Cidadão, instalado com a aplicação Autenticação.Gov, permite a integração com outras aplicações do sistema operativo, disponibilizando duas funcionalidades: Autenticação e Assinatura Digital.

O *middleware* disponibiliza suporte criptográfico às aplicações via suporte criptográfico nativo do sistema operativo Windows ou via interface PKCS#11.

5.1 Integração com aplicações em Windows

Integração com aplicações com o Cartão de Cidadão:

A instalação do *middleware* em Windows permite que, ao introduzir um Cartão de Cidadão no leitor, os certificados deste fiquem automaticamente registados no sistema operativo, ficando assim as funcionalidades de autenticação e assinatura disponíveis às aplicações que utilizam a camada criptográfica do sistema operativo, para operações de autenticação e assinatura.

Alguns exemplos dessas aplicações são: *Microsoft Word*, *Microsoft Excel*, *Microsoft Outlook* e *Adobe Acrobat Reader*.

Para que os certificados fiquem automaticamente registados é necessário:

- A opção "Registrar certificados com a inserção do cartão" disponível no separador Configuração de assinaturas estar ativa.
- Abrir a aplicação local Autenticação.Gov antes de inserir o cartão. É aconselhado fazer pelo menos uma leitura do cartão na aplicação.

Integração com aplicações com a Chave Móvel Digital:

A integração com aplicações é também possível com a Chave Móvel Digital, ao nível da componente de assinatura digital. Para tal, siga o procedimento descrito em Assinatura digital com Chave Móvel Digital.

Na assinatura com Chave Móvel Digital, a mensagem de verificação enviada ao utilizador segue um dos 2 seguintes formatos:

- No caso de aplicações como o *Adobe Acrobat Reader* ou *Microsoft Office*:
Código de segurança: <código>.
Assinatura de documento "<título do documento/email>".
Exemplo:

Código de segurança: 121597.
Assinatura de documento
"Email: Teste".

- No caso de outras aplicações que suportem assinatura digital ou quando não é possível verificar o nome do documento:
Código de segurança: <código>.
Assinatura de documento "Aplicação: <Nome da aplicação> - Id: <últimos 8 dígitos da hash do conteúdo a ser assinado>".
Exemplo:

Código de segurança: 230029.
Assinatura de documento
"Aplicação: Microsoft Outlook -
Id: uJ3Ak9E=".

5.2 Integração com aplicações via interface PKCS#11

No caso das aplicações com suporte PKCS#11, geralmente é necessário configurar a localização do ficheiro da aplicação, que permite o suporte. A localização deste ficheiro, depende do sistema operativo a ser utilizado.

Windows: C:\Windows\System32\pteidpkcs11.dll

Linux: /usr/local/lib/libpteidpkcs11.so

MacOS: /usr/local/lib/libpteidpkcs11.dylib

5.3 Assinatura digital em aplicações comuns

Nos pontos seguintes será explicada a utilização das funcionalidades de assinatura digital nas seguintes aplicações:

Assinatura digital:

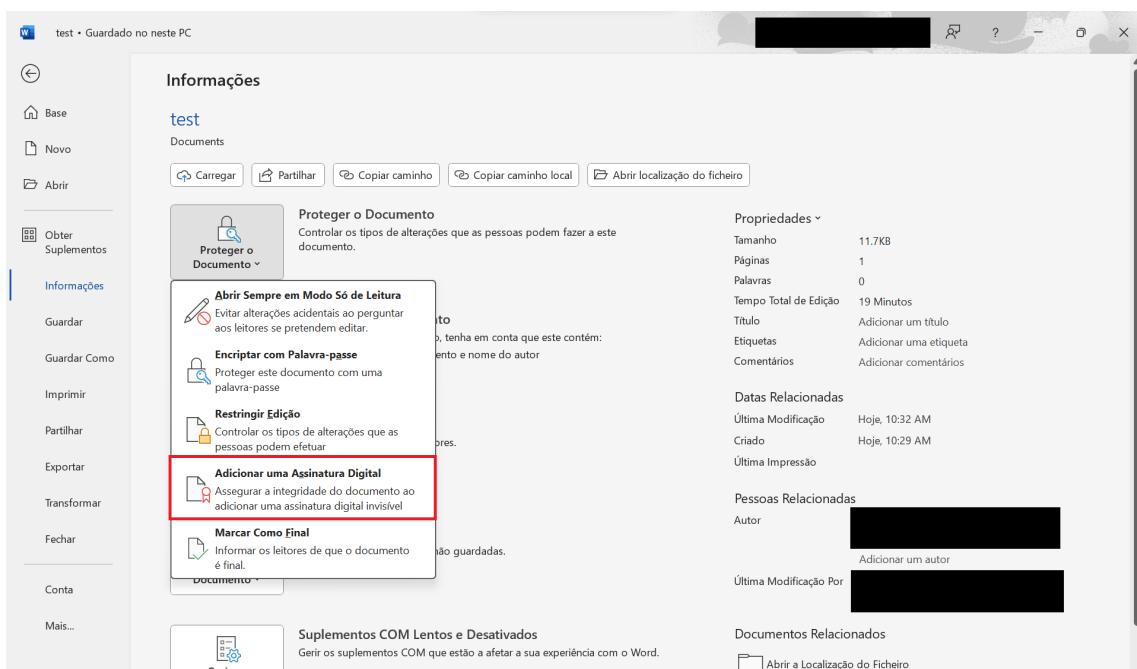
- Suite Microsoft Office
- Suite LibreOffice / OpenOffice
- Microsoft Outlook
- Adobe Acrobat Reader
- Adobe Acrobat Reader em MacOS (desde a versão 3.11.0)
- Adobe Acrobat Reader em MacOS com PKCS#11
- Mozilla Thunderbird com PKCS#11

5.3.1 Assinatura digital na suite *Microsoft Office*

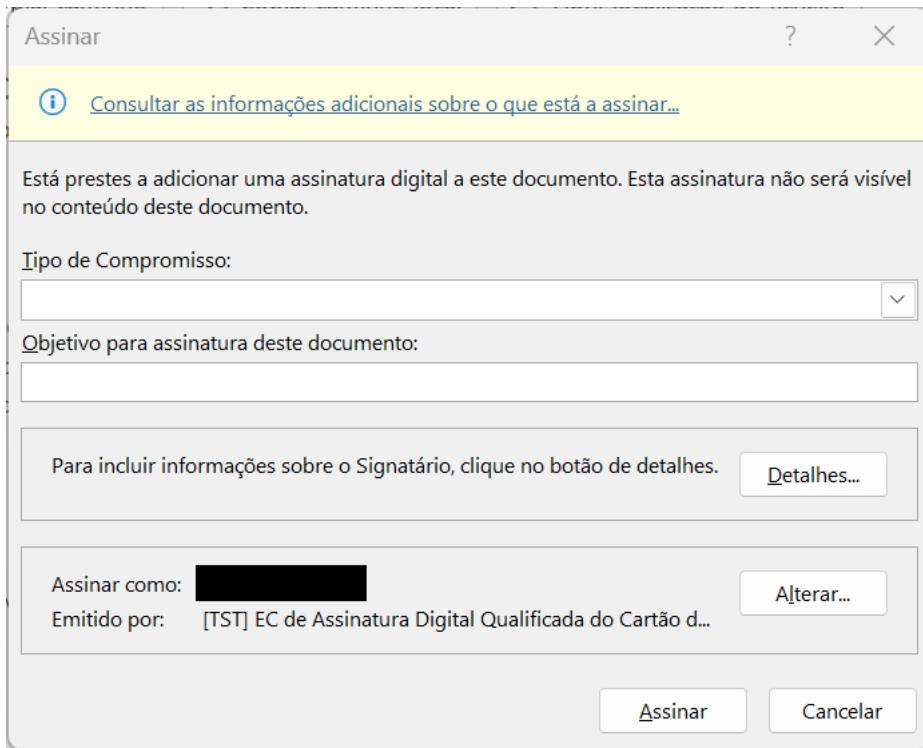
Nesta secção é apresentada a assinatura digital de documentos em ficheiros *Office*, nomeadamente, nas aplicações: *Word*, *Excel* e *PowerPoint*.

Para assinar digitalmente um documento, deverá efetuar os seguintes passos:

1. Aceder ao menu **Ficheiro**.
2. Na secção **Informações** clicar no botão **Proteger Documento** e selecionar a opção **Adicionar uma assinatura Digital**, conforme a imagem abaixo:



3. Aparecerá uma mensagem específica da aplicação que está a utilizar (*Word, Excel ou Powerpoint*), clique em **OK**.
4. Na Caixa de diálogo **Assinar**, introduza o **Objetivo** da assinatura, conforme a imagem abaixo:



5. Clique em assinar e introduza o seu PIN de assinatura na respetiva janela.
6. O documento ficará assinado digitalmente, e ficará só de leitura de forma a impossibilitar alterações ao mesmo.

Poderá encontrar informação mais detalhada no seguinte link: Adicionar/Remover uma Assinatura Digital nos ficheiros do Office.

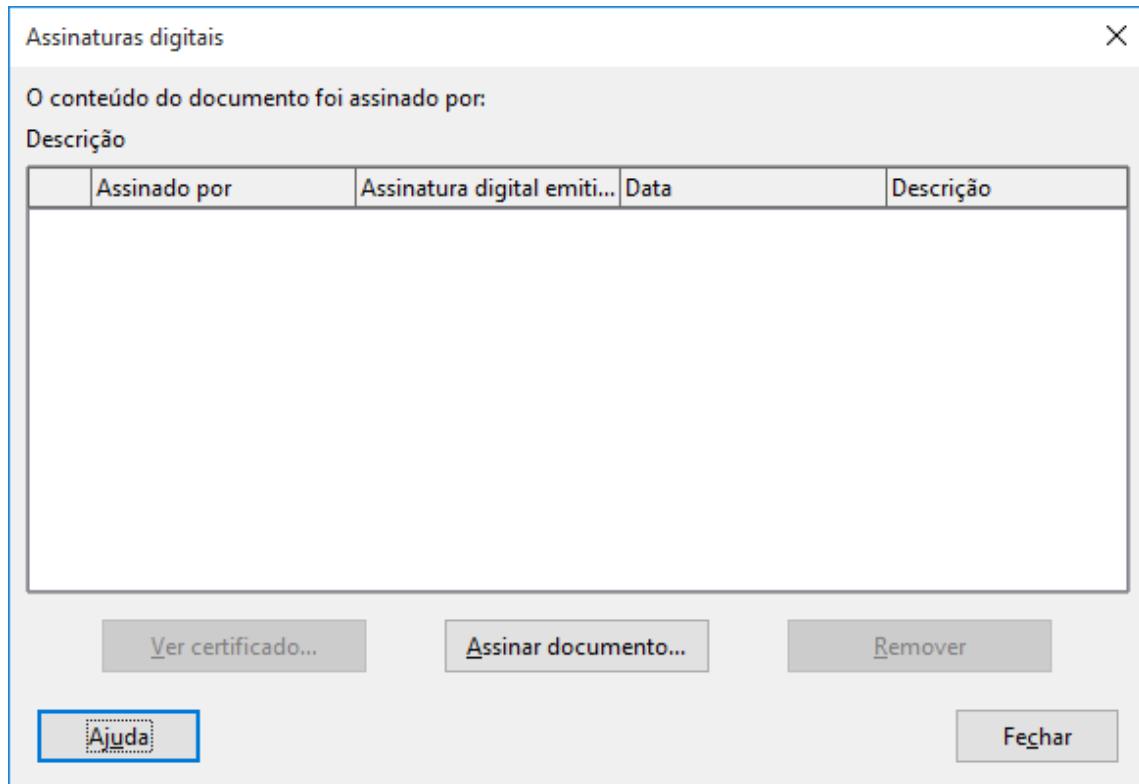
5.3.2 Assinatura digital na suite *LibreOffice / OpenOffice*

Nesta secção é apresentada a assinatura digital de documentos em ficheiros *LibreOffice*, nomeadamente, nas aplicações, *Calc*, *Write* e *Impress*. A versão utilizada neste manual foi a versão *LibreOffice 5.3*. A interface desta funcionalidade é bastante semelhante em todas as versões a partir de 4.0.0.

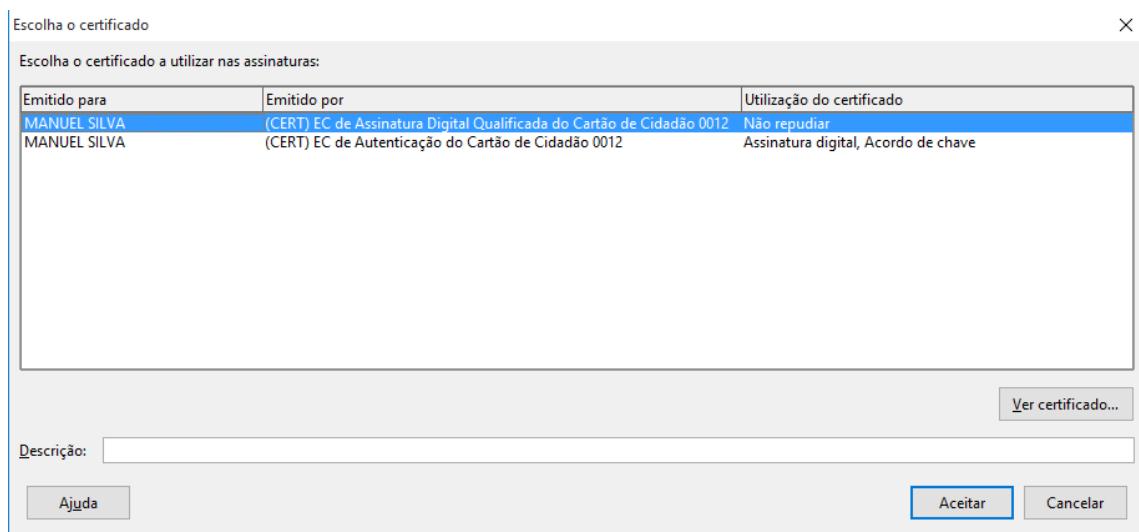
Em sistemas operativos Linux, a deteção dos certificados digitais nesta Suite depende das configurações de segurança do *Mozilla Thunderbird* ou *Mozilla Firefox*. Assim, para que esta funcionalidade esteja disponível deverá configurar previamente a integração com o Cartão de Cidadão no *Mozilla Thunderbird* ou *Firefox*. Ver as instruções em: Assinatura digital de email com Mozilla Thunderbird.

Para assinar digitalmente um documento, deverá efetuar os seguintes passos:

1. Aceder ao menu **Ficheiro Assinaturas Digitais**.
2. Aparecerá a janela com as assinaturas digitais do documento. Caso não exista ainda nenhuma assinatura, a lista aparecerá vazia conforme a imagem abaixo. Clique no botão **Assinar documento...**



3. Será apresentada uma janela para seleção do certificado. Deverá selecionar o certificado que tem o seu nome e emitido por **EC de Assinatura Digital Qualificada do Cartão...** conforme ilustrado na imagem abaixo:



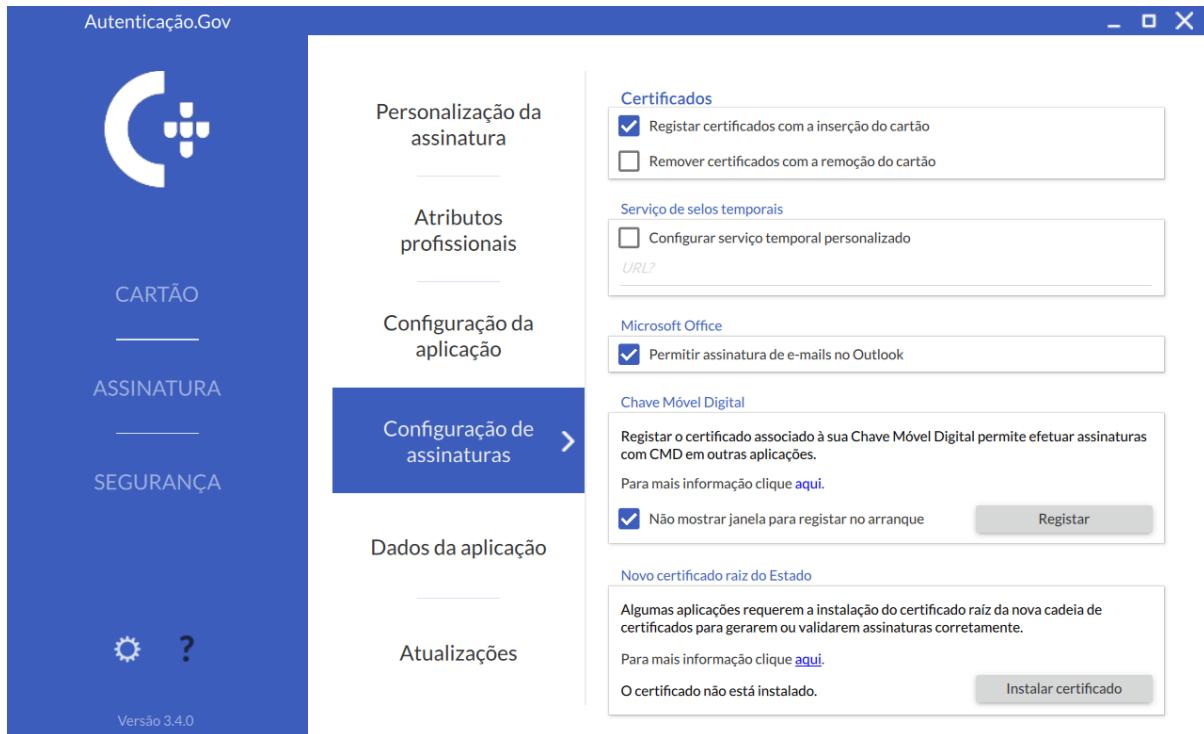
4. Clique em **Aceitar** e introduza o seu PIN de assinatura na respetiva janela.
5. O documento ficará assinado digitalmente.

5.3.3 Assinatura digital de email com *Microsoft Outlook*

A assinatura digital no *Outlook*, por omissão, obriga a que o certificado digital inclua o endereço de email, e este corresponda com o email que se pretende assinar.

Nos certificados existentes no Cartão de Cidadão e na Chave Móvel Digital não existe qualquer endereço de email. Desta forma, para que seja possível efetuar assinaturas digitais no *Outlook* com o Cartão de Cidadão e Chave Móvel Digital, é assim necessário desativar esta validação.

Na aplicação poderá desactivar essa validação selecionando a opção **Permitir assinatura de e-mails no Outlook** no submenu **Configuração de assinaturas** da aplicação Autenticação.gov para computador.



Alternativamente, para **desativar a correspondência com endereço de email do certificado digital**, poderá seguir as instruções disponibilizadas no *website* da *Microsoft*:

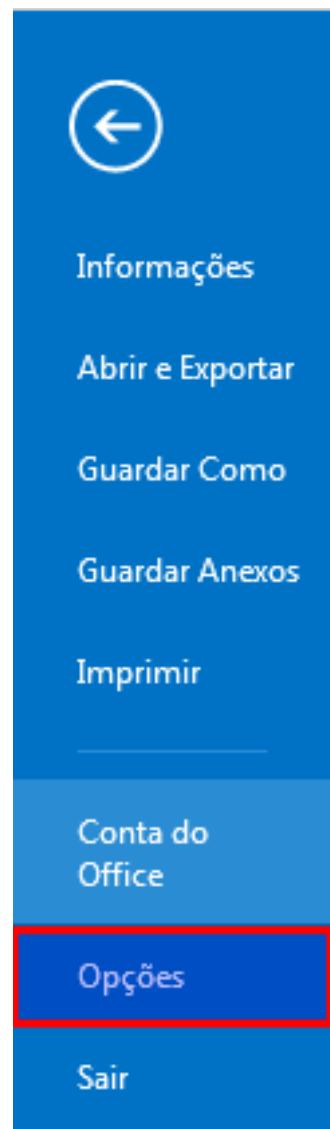
- Versão PT: <http://support.microsoft.com/kb/276597/pt>
- Versão EN (original): <http://support.microsoft.com/kb/276597/>

Para poder assinar digitalmente um email no *Outlook*, é necessário inicialmente efetuar a respetiva configuração. Os passos descritos de seguida, estão divididos em **configuração**, consistindo na configuração inicial necessária, e **assinatura**, consistindo na assinatura propriamente.

Nota: As imagens apresentadas são referentes ao *Microsoft Outlook 2016*.

Configuração Esta operação é realizada apenas uma vez.

1. Assegurar que a correspondência com endereço de email do certificado digital está desativada, conforme instruções acima.
2. No Outlook, aceder ao menu **Ficheiro Opções**



3. Clicar em **Centro de Confiança**.

- Geral
- Correio
- Calendário
- Pessoas
- Tarefas
- Pesquisa
- Idioma
- Avançadas

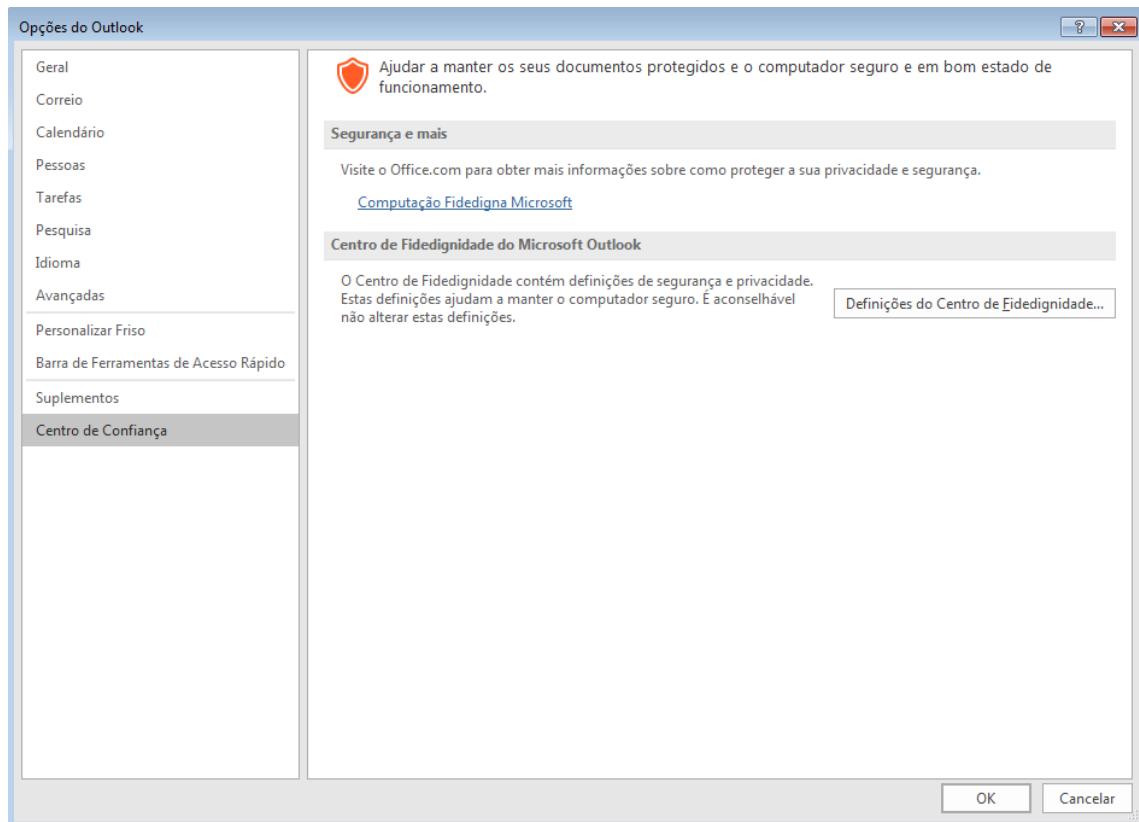
Personalizar Friso

Barra de Ferramentas de Acesso Rápido

Suplementos

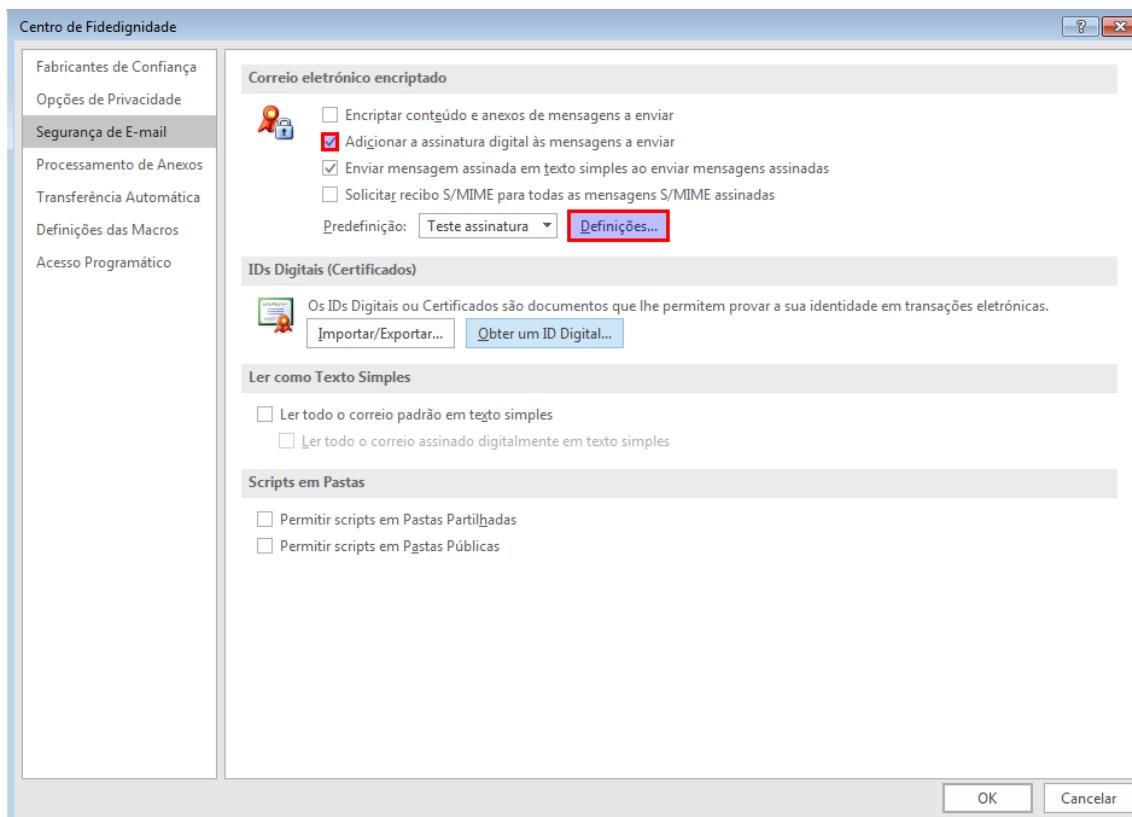
Centro de Confiança

4. Selecionar a secção **Definições do Centro de Fidedignidade**.

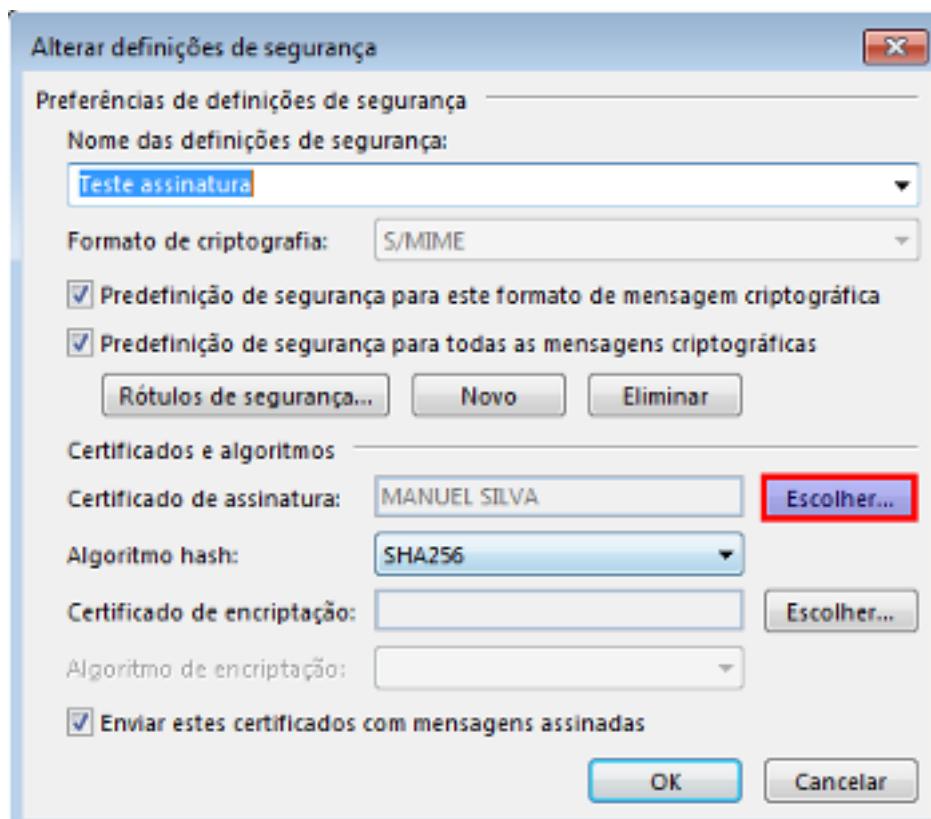


5. Nesta secção, selecionar a opção **Adicionar a assinatura digital às mensagens a enviar** e

clicar no botão **Definições**



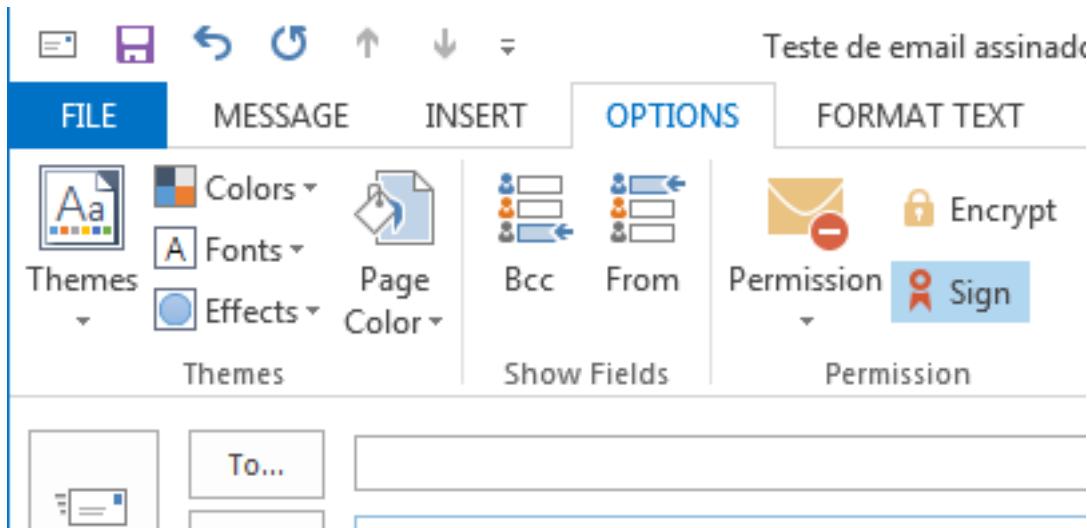
6. Adicione uma descrição a esta configuração, p. ex.: Assinatura com Cartão de Cidadão e clique no botão **Escolher** para selecionar o certificado. Selecione o seu certificado de assinatura do Cartão de Cidadão ou Chave Móvel Digital.



7. Na configuração **Algoritmo hash** escolha **SHA256** e clique em **OK**.
8. Clique em **OK** em todas as janelas de configuração abertas. A configuração está terminada.

Assinatura - a efetuar cada vez que pretenda enviar um email assinado.

1. Ao clicar em **Enviar**, será solicitado o PIN de assinatura e o seu email será assinado e enviado.



5.3.4 Assinatura digital em *Adobe Acrobat Reader*

Nota: para assinar um documento no *Adobe Acrobat Reader DC* em MacOS, siga as instruções da secção Assinatura digital em *Adobe Acrobat Reader* em MacOS (desde a versão 3.11.0).

Nota: a assinatura com atributos profissionais só é possível na aplicação Autenticação.Gov.

Para assinar um documento aberto no *Adobe Acrobat Reader* deve:

1. Certos documentos PDF foram criados pelo seu autor com campos de assinatura. Se for esse o caso do seu documento deve localizar o campo de assinatura que pretende utilizar e clicar no mesmo. Em seguida pode saltar para o ponto 4 deste procedimento. Caso contrário será necessário criar um novo campo de assinatura num local á sua escolha. Para isso deve aceder ao separador **Ferramentas** e selecionar **Certificados**.
2. Clique em **Assinar Digitalmente** na barra horizontal por cima do documento.
3. Clique e arraste o rato para determinar a posição do selo de assinatura no documento.
4. Certifique-se de que o cartão de cidadão está inserido no leitor e escolha o seu certificado de assinatura, emitido por **EC de Assinatura Digital Qualificada do Cartão de Cidadão X** (onde "X" é um número com 4 dígitos, por exemplo 0010), e carregue **Continuar**.
5. Clique em **Assinar** e escolha o nome e pasta onde deseja guardar o documento assinado.
6. Para concluir, introduza o seu PIN de assinatura. A janela de introdução de PIN deverá ter o título de "Segurança do Windows" e a mensagem "Introduza o PIN de não rejeição".

5.3.5 Assinatura digital em *Adobe Acrobat Reader* em MacOS (desde a versão 3.11.0)

Desde a versão 3.11.0 da aplicação é possível utilizar o Cartão de Cidadão em aplicações nativas MacOS utilizando o módulo *PteidToken* que implementa a framework CryptoTokenKit.

A configuração inicial deste módulo no Acrobat Reader fica bastante facilitada face às versões anteriores. Para poder assinar um documento no *Adobe Acrobat Reader*, em MacOS, deve primeiro ativar a utilização do módulo CryptoTokenKit da seguinte forma:

1. No *Adobe Acrobat Reader*, aceda ao menu **Preferências....**
2. Selecione a categoria **Assinaturas** e na secção "Criação e aparência" pressione **Mais....**
3. Clique na caixa de seleção "Habilitar suporte à estrutura CryptoTokenKit"

Se já tinha assinado com CC usando versões anteriores da Autenticação.gov deve também garantir que o Acrobat Reader está a funcionar em modo nativo caso o seu computador tenha um processador Apple M1 ou sucessor. Neste sentido pode consultar a seguinte página de ajuda:

- <https://helpx.adobe.com/pt/acrobat/kb/apple-silicon-m1-processor-support.html>

Depois desta configuração que é necessária antes da primeira utilização, deve inserir o Cartão de Cidadão no leitor e já deverá ter disponível o seu certificado de assinatura na funcionalidade do menu **Certificados -> Assinar Digitalmente**.

5.3.6 Assinatura digital em *Adobe Acrobat Reader* em MacOS com PKCS#11

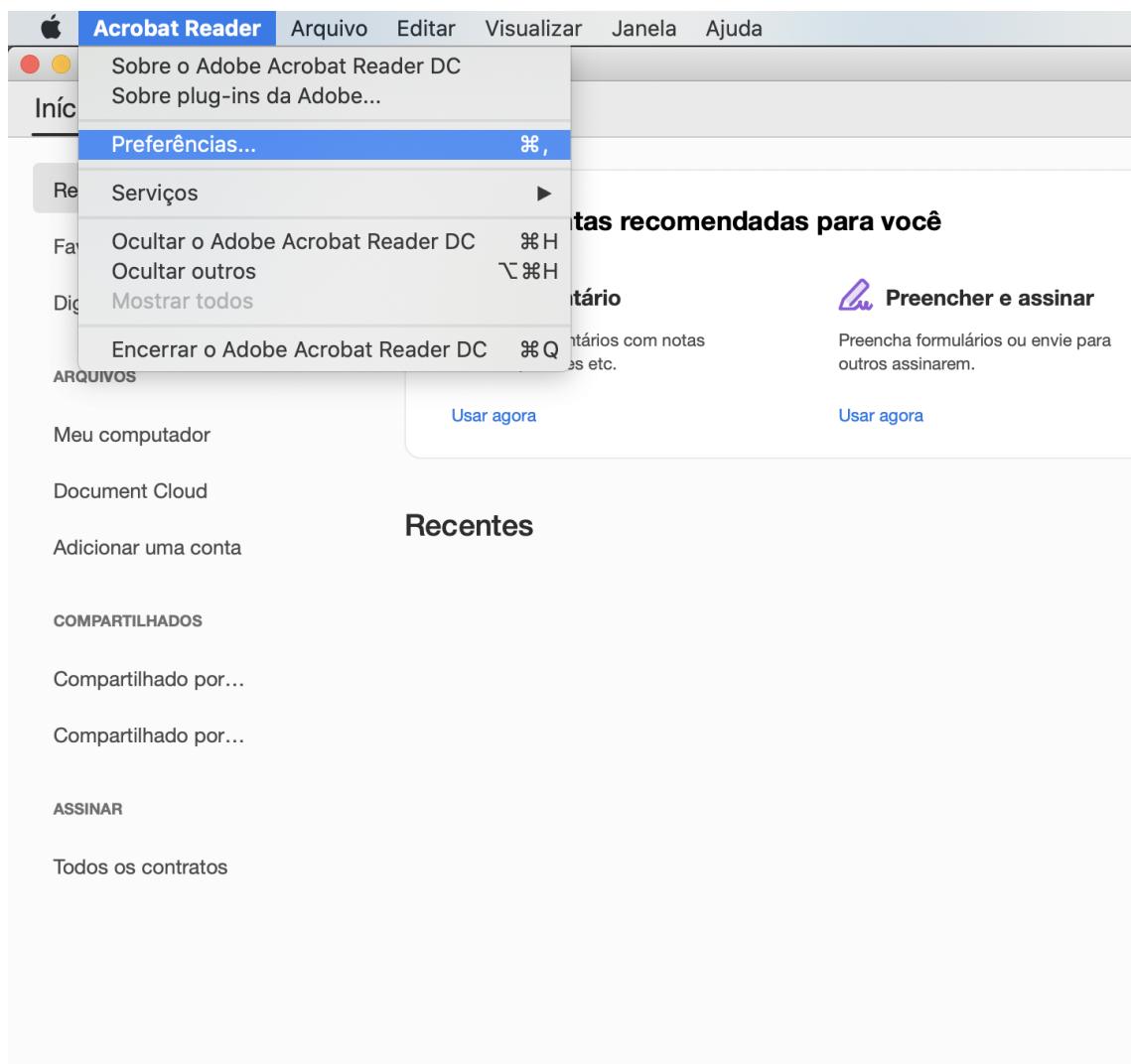
Nota: Em computadores MacOS com processador ARM, Apple M1 ou sucessores, só é possível utilizar o módulo de assinatura no Adobe Reader se esta aplicação for executada em modo Intel emulado.

Pode consultar as instruções do fabricante para desligar o modo nativo na página de ajuda:

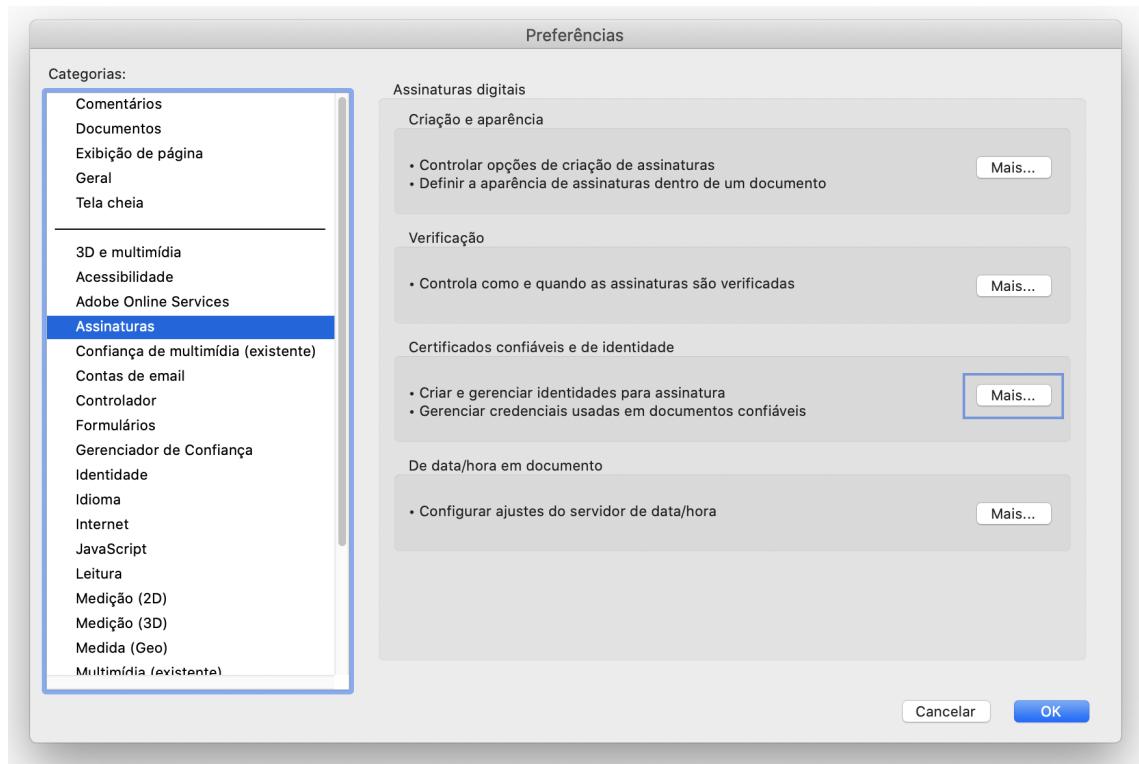
- <https://helpx.adobe.com/pt/acrobat/kb/apple-silicon-m1-processor-support.html>

Para assinar um documento aberto no *Adobe Acrobat Reader*, em MacOS, deve primeiro carregar o módulo PKCS#11. Para tal, siga as seguintes instruções:

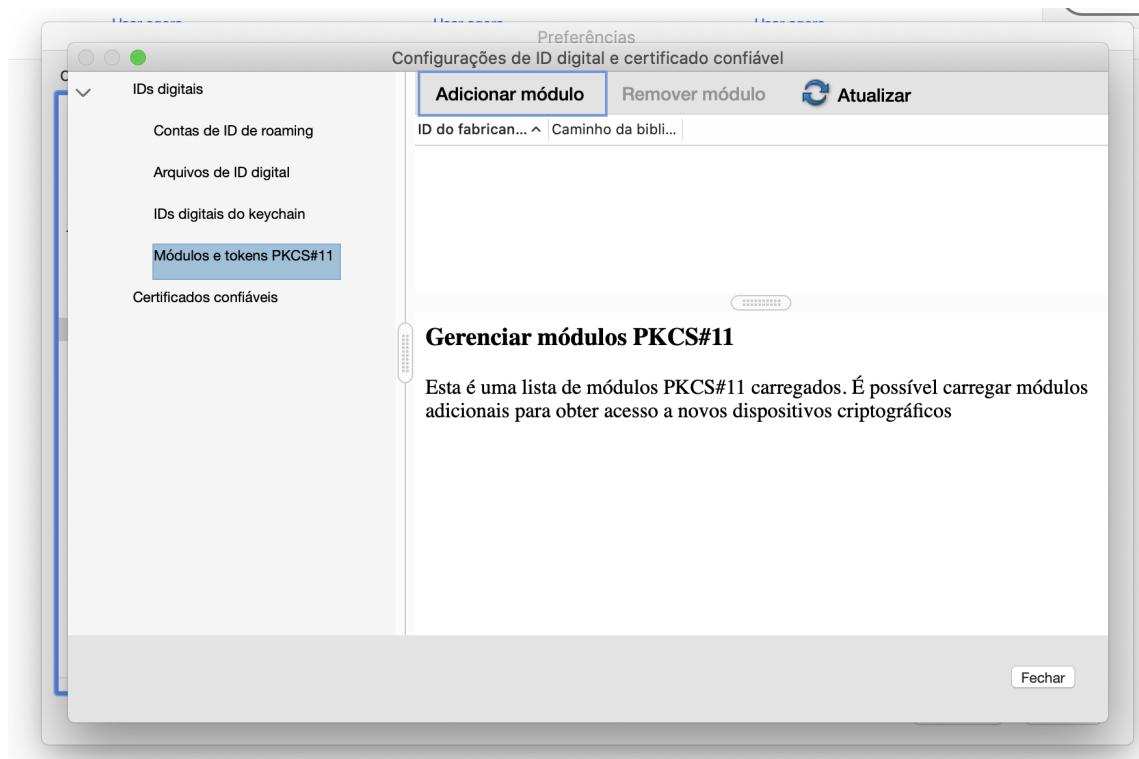
1. No *Adobe Acrobat Reader*, aceda a **Preferências**.



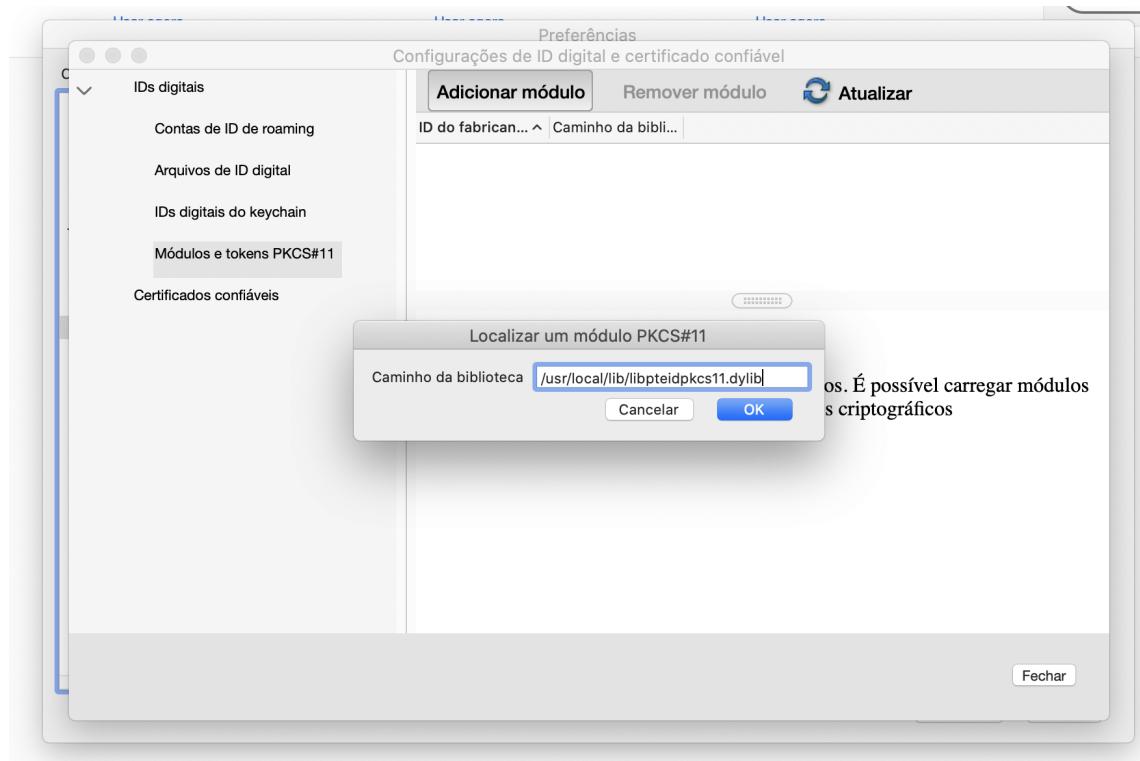
2. Selecione a Categoria **Assinaturas** e na secção "Certificados confiáveis e de identidade" pressione **Mais....**



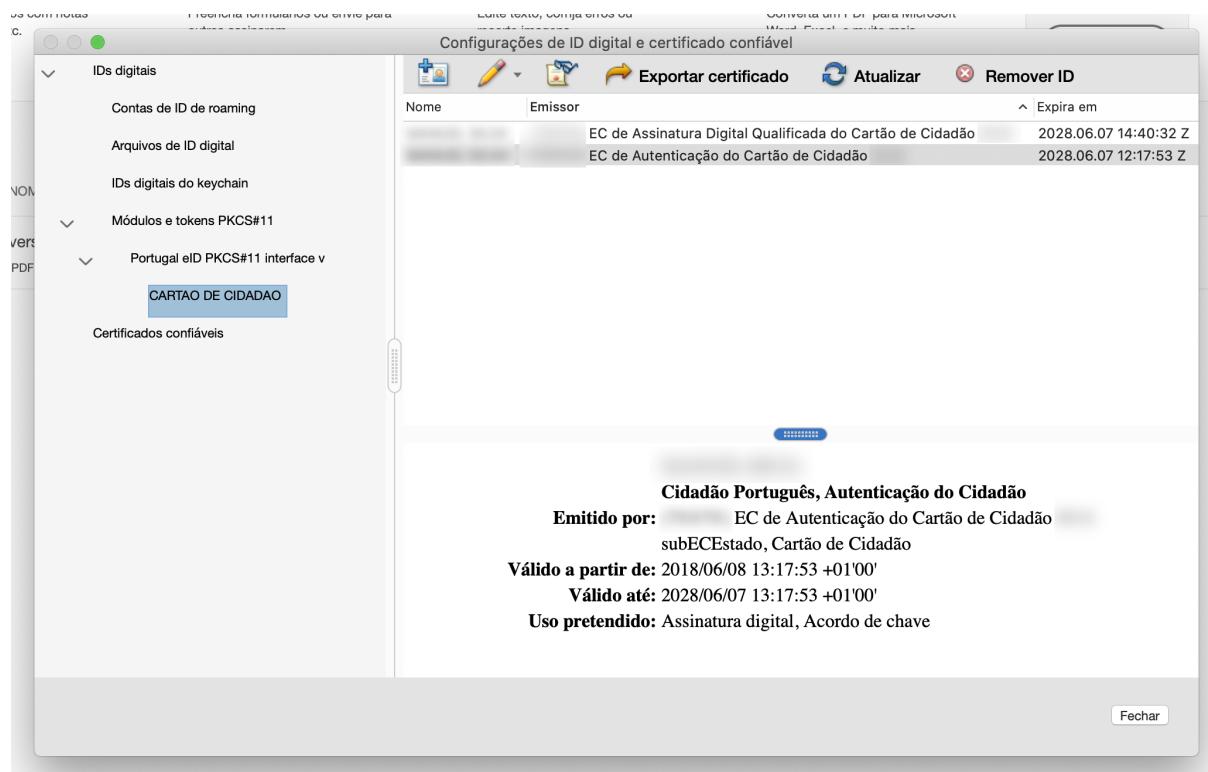
3. No separador "IDs digitais" selecione **Módulos e tokens PKCS#11** e clique **Adicionar módulo**.



4. No campo de texto insira o caminho da biblioteca: `/usr/local/lib/libpteidpkcs11.dylib` e pressione **OK**.



Se o seu cartão de cidadão estiver inserido no leitor e o módulo tiver sido adicionado com sucesso, ao pressionar **Atualizar** os certificados ficarão disponíveis e visíveis conforme na imagem seguinte. No caso dos certificados não ficarem disponíveis como na imagem, verifique que o cartão está inserido no leitor, reinicie o *Adobe Acrobat Reader* e volte a verificar.



Depois de ter adicionado o módulo PKCS#11, para assinar um documento aberto no *Adobe Acrobat Reader DC* deve, com o cartão de cidadão inserido no leitor:

1. Aceder ao separador **Ferramentas** e selecionar **Certificados**.
2. Clique em **Assinar Digitalmente** na barra horizontal por cima do documento.
3. Clique e arraste o rato para determinar a posição do selo de assinatura no documento.
4. Escolha o seu certificado de assinatura, emitido por **EC de Assinatura Digital Qualificada do Cartão de Cidadão X** (onde "X" é um número com 4 dígitos, por exemplo 0010), e carregue **Continuar**.
5. Clique em **Assinar** e escolha o nome e local onde deseja guardar o documento assinado.
6. Para concluir, introduza o seu PIN de assinatura.

5.3.7 Assinatura digital com Chave Móvel Digital

Pode assinar documentos ou emails com a Chave Móvel Digital no Windows em aplicações como *Microsoft Word*, *Microsoft Excel*, *Microsoft Outlook* e *Adobe Acrobat Reader*. O procedimento é muito semelhante aos descritos nas secções anteriores mas difere em dois aspetos:

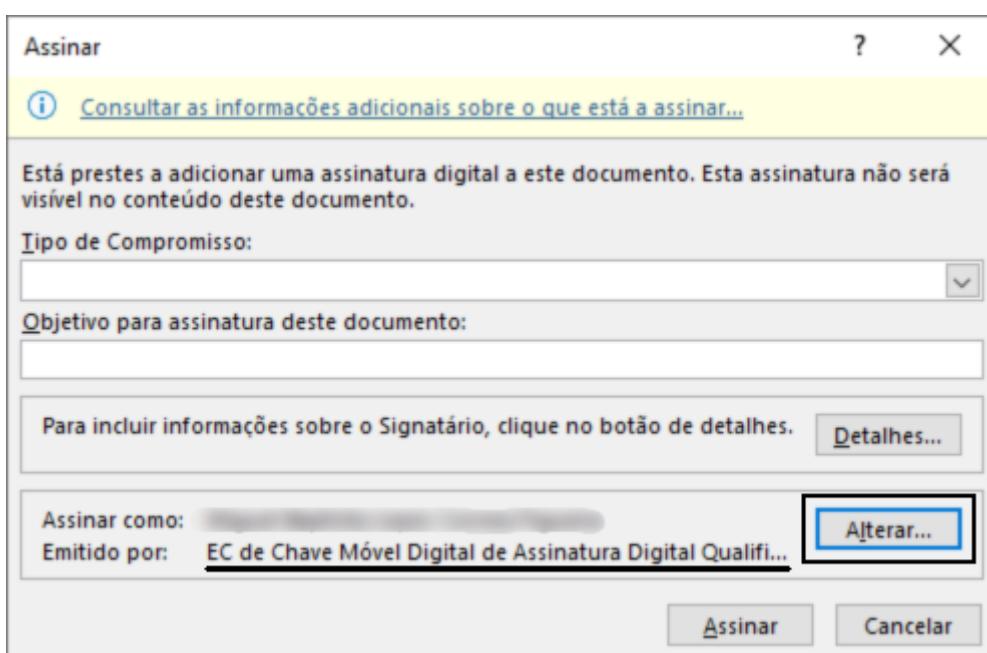
Registo do certificado deverá registar no Windows o certificado associado à sua Chave Móvel Digital.

1. No separador Configuração de assinaturas da aplicação Autenticacão.Gov há um segmento destinado a configurações da Chave Móvel Digital com um botão **Registar**. Pressione o botão para abrir uma janela de registo do certificado.
2. Insira o número de telemóvel associado à sua conta da Chave Móvel Digital e o PIN de Assinatura da Chave Móvel Digital e pressione **OK**.
3. Se as credenciais inseridas no passo anterior estavam corretas, deverá receber no telemóvel um código que deverá introduzir para concluir o processo de registo do certificado. Esse código será enviado por SMS ou através de notificação da aplicação móvel Autenticação.gov.

No caso de ainda não ter registado o seu certificado após uma re-ativação da Assinatura da Chave Móvel Digital ou o certificado atualmente registado estar expirado terá de repetir o procedimento de registo.

Assinatura similar à assinatura com o Cartão de Cidadão com as seguintes diferenças:

- Durante a configuração ou no momento da assinatura, deverá escolher o certificado emitido por **EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão X** (onde "X" é um número com 5 dígitos, por exemplo 00001 ou 00002).



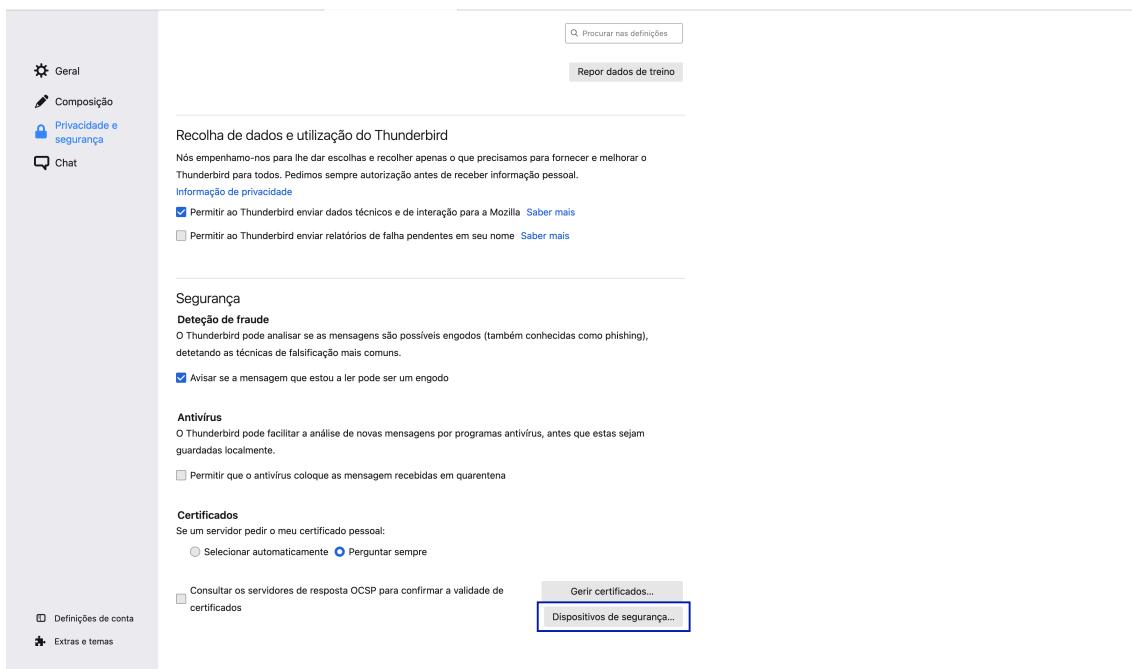
- Após confirmar na aplicação em uso que pretende assinar será mostrada uma janela onde, tal como no registo do certificado, deverá introduzir o seu PIN de assinatura da Chave Móvel Digital. Se o PIN estiver correto, deverá receber um SMS com o código de confirmação que deverá introduzir na janela para concluir a assinatura.

5.3.8 Assinatura digital de email com Mozilla Thunderbird

Para poder assinar digitalmente um email no *Thunderbird*, é necessário inicialmente efetuar a respetiva configuração. Os passos descritos de seguida, estão divididos em **configuração**, consistindo na configuração inicial necessária, e **assinatura**, consistindo na assinatura propriamente dita. Os printscreens coincidem com a versão 91 do Mozilla Thunderbird.

Configuração Esta configuração é necessária efetuar uma única vez e os passos descritos aplicam-se também à configuração dos certificados em *Firefox*.

1. Abra as **Preferências** e selecione o separador **Privacidade e segurança**. Navegue até à secção **Segurança -> Certificados**.
2. Pressione o botão **Dispositivos de segurança**.



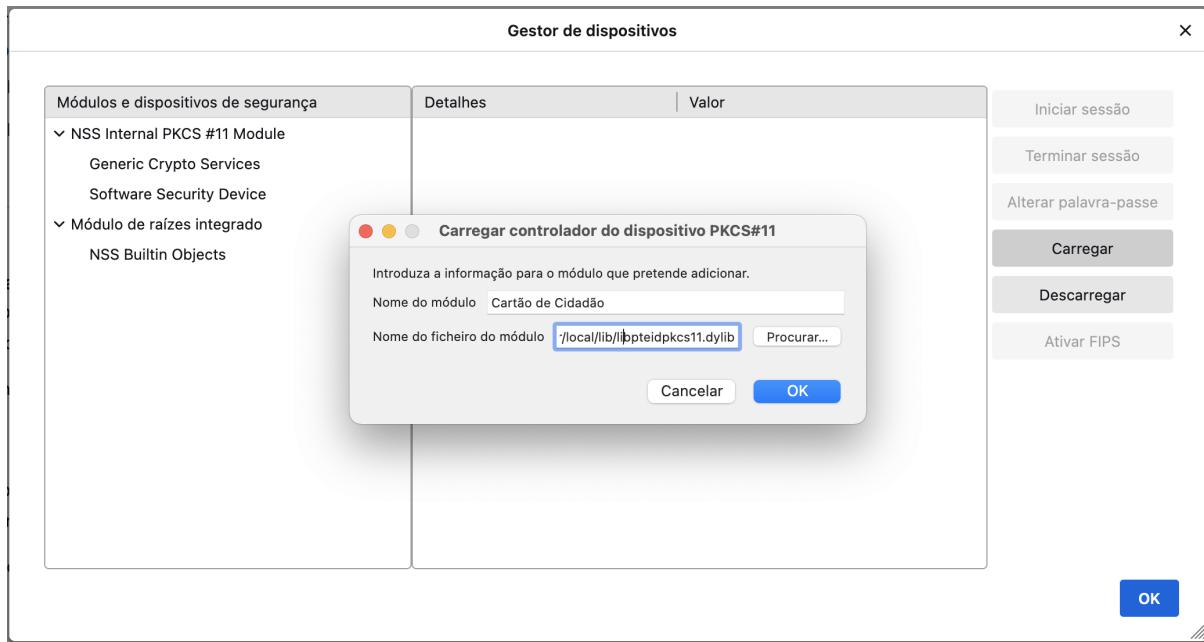
3. Clique no botão **Carregar**.
4. Na nova janela, preencha o nome do módulo (p.e. "Cartão de Cidadão") e o caminho para o módulo **PKCS#11**, que se encontra numa das seguintes localizações (recomendação: copie o caminho para o módulo, de acordo com o seu sistema operativo, da lista seguinte):

Em Windows:

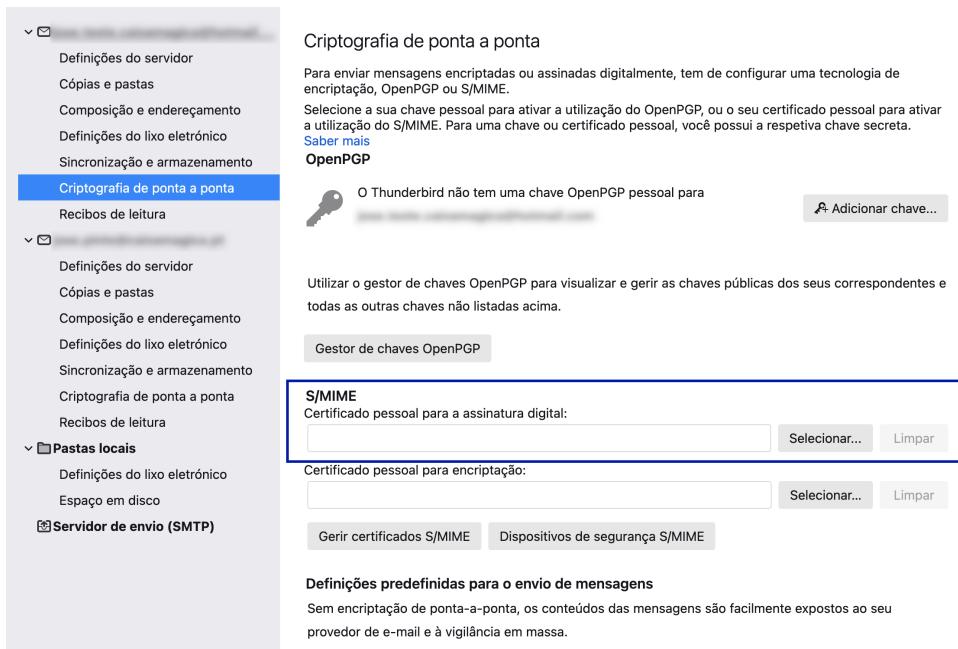
- C:\Windows\SysWOW64\pteidpkcs11.dll (Windows 32-bits)
- C:\Windows\System32\pteidpkcs11.dll (Windows 64-bits)

Em Linux: /usr/local/lib/libpteidpkcs11.so

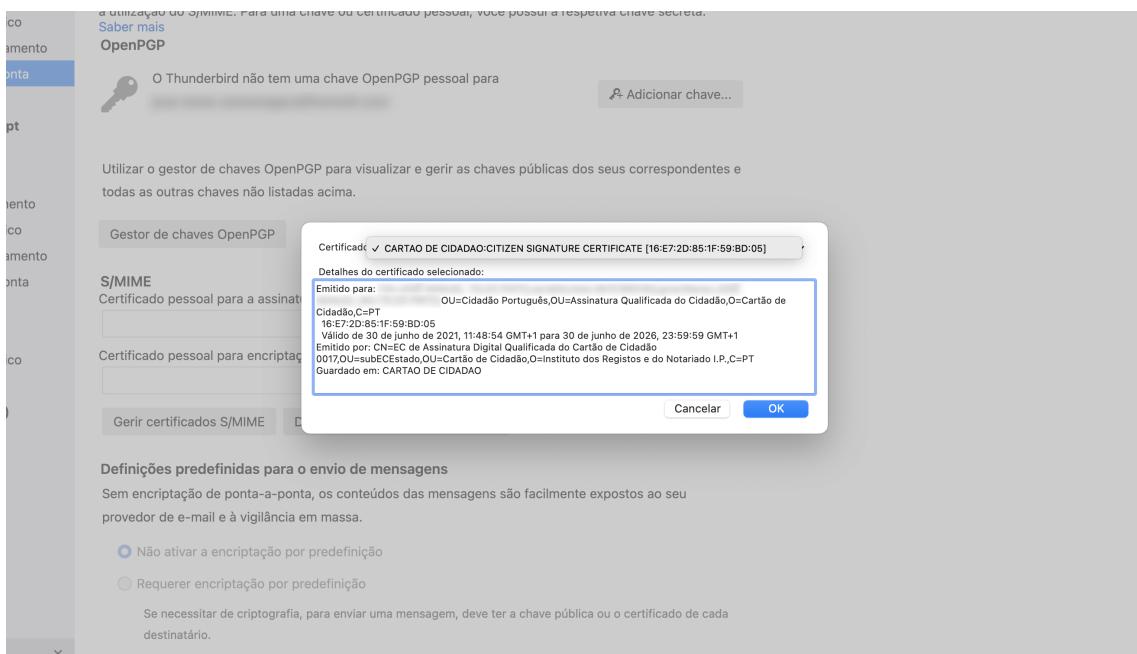
Em MacOS: /usr/local/lib/libpteidpkcs11.dylib



5. Pressione **OK** em todas as janelas.
6. Abra as **Definições de conta** e selecione a sua conta de email.
7. Selecione o separador **Criptografia de ponta a ponta**.
8. Na secção **S/MIME**, pressione o botão **Selecionar** no campo com a indicação "*Certificado pessoal para a assinatura digital*".



9. Selecione o certificado com a descrição "**CARTAO DE CIDADAO:CITIZEN SIGNATURE CERTIFICATE**" e clique **OK**.

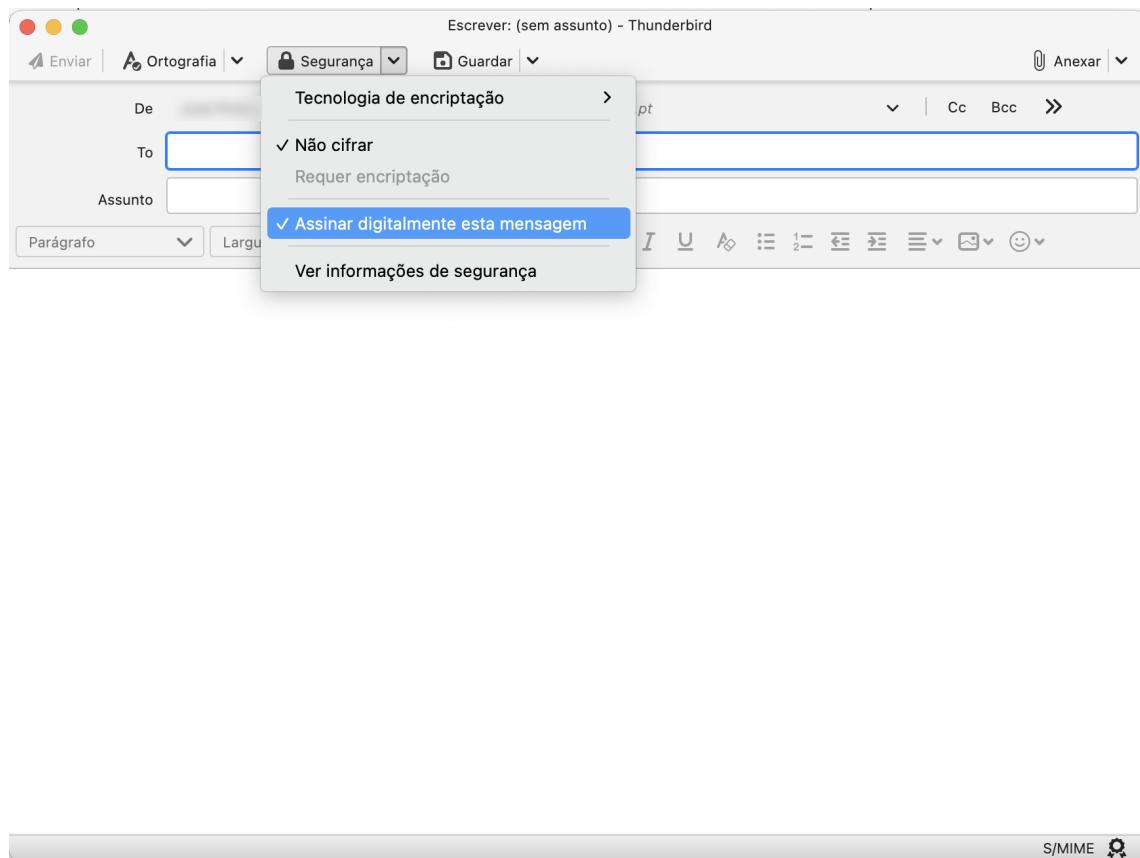


10. Se utilizar o Thunderbird 102 ou superior, no separador **Criptografia de ponta a ponta** selecione a caixa "Adicionar a minha assinatura por predefinição".
11. Para o Thunderbird poder utilizar o certificado do Cartão de Cidadão para assinatura é necessário registar e confiar no certificado raiz da cadeia de certificação do Estado Português.
 - Para cartões emitidos a partir de abril de 2020 o certificado a registar deve ser o certificado com nome "ECRaizEstado 002" disponível em: <http://trust.ecee.gov.pt/ecraiz002.crt>
 - Para cartões emitidos antes de abril de 2020 o certificado a registar deve ser o certificado com nome "ECRaizEstado" disponível em: <http://trust.ecee.gov.pt/ecraiz.crt>

Para importar o certificado raiz clique em "Gerir certificados..." na janela utilizada no ponto 1 e selecione o separador "Autoridades". Deve importar o certificado raiz correto para o seu cartão e na questão "Pretende confiar em "ECRaizEstado/EcRaizEstado 002" para os seguintes propósitos?" selecionar a opção: "Confiar nesta CA para identificar utilizadores de email".

Assinatura - a efetuar cada vez que pretenda enviar um email assinado. Apenas necessário para versões do Thunderbird anteriores à versão 102.

1. Abra a janela de composição de email.
2. Clique na caixa de opções **Segurança** e clique em **Assinar digitalmente esta mensagem**. Esta opção ficará ativa.

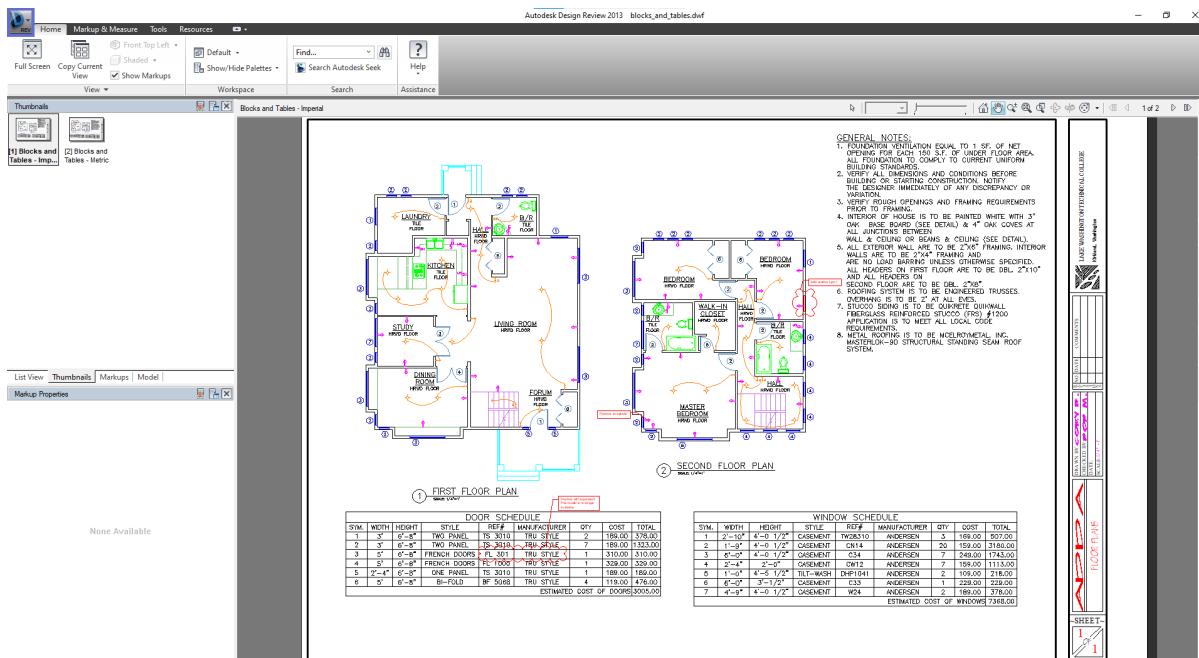


3. Ao clicar em **Enviar**, será solicitado o PIN de assinatura e o seu email será assinado e enviado.

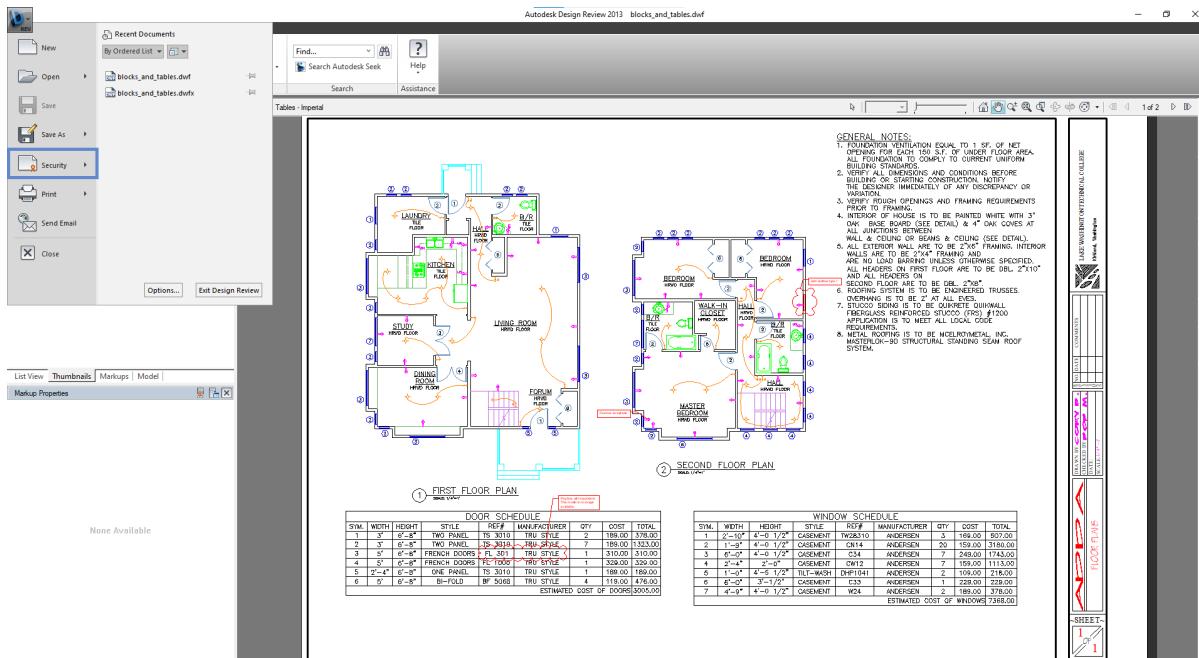
5.3.9 Assinatura digital de ficheiros DWF

NOTA: A assinatura de ficheiros DWF apenas suporta assinatura com Cartão de Cidadão

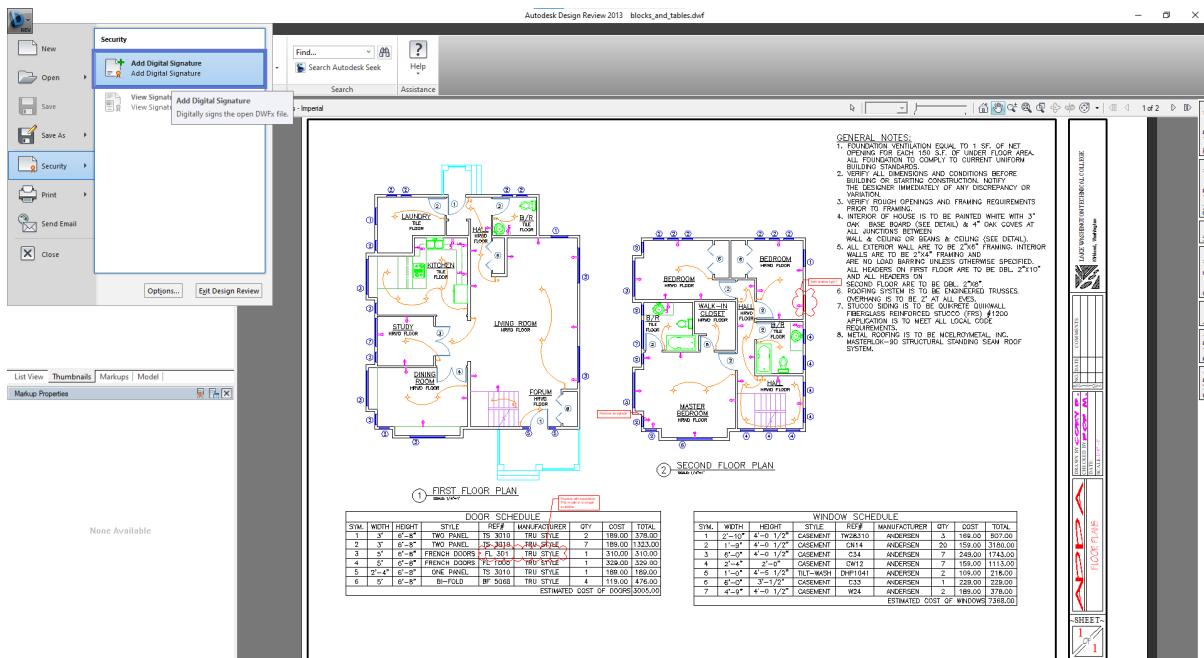
1. Em primeiro lugar, deverá ter instalado no seu computador o **Autodesk Design Review 2013** (as versões mais recentes não disponibilizam a funcionalidade de assinatura digital).
2. Abra o ficheiro DWF na aplicação.
3. Aceda ao menu no campo superior esquerdo:



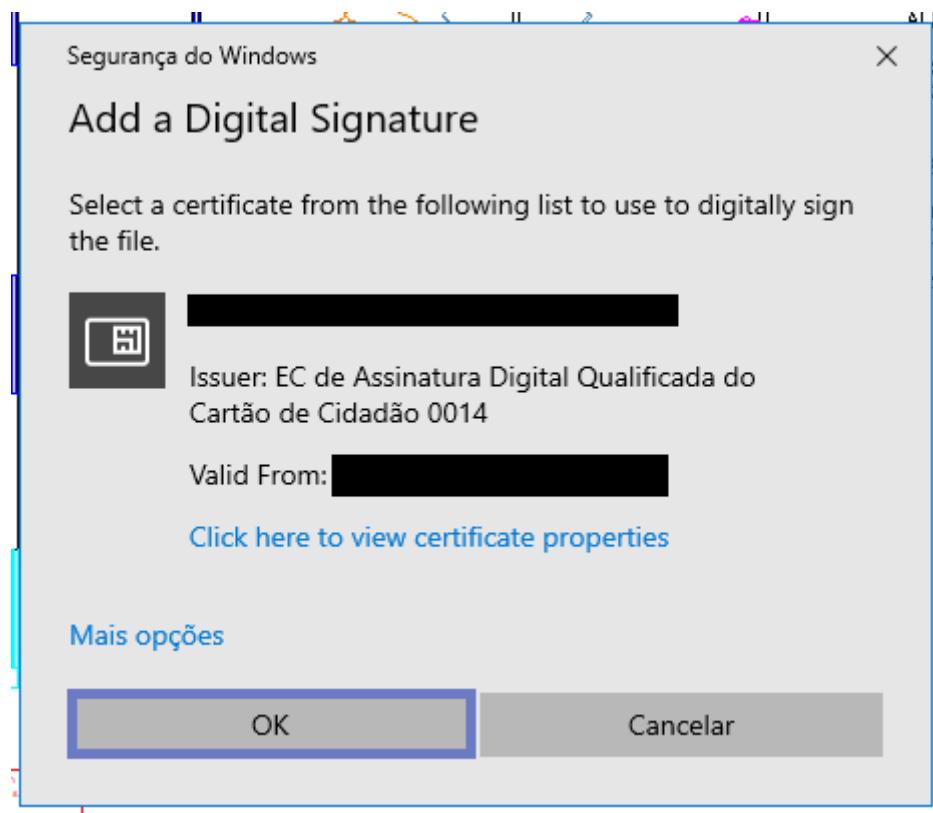
4. Aceda à opção Security:



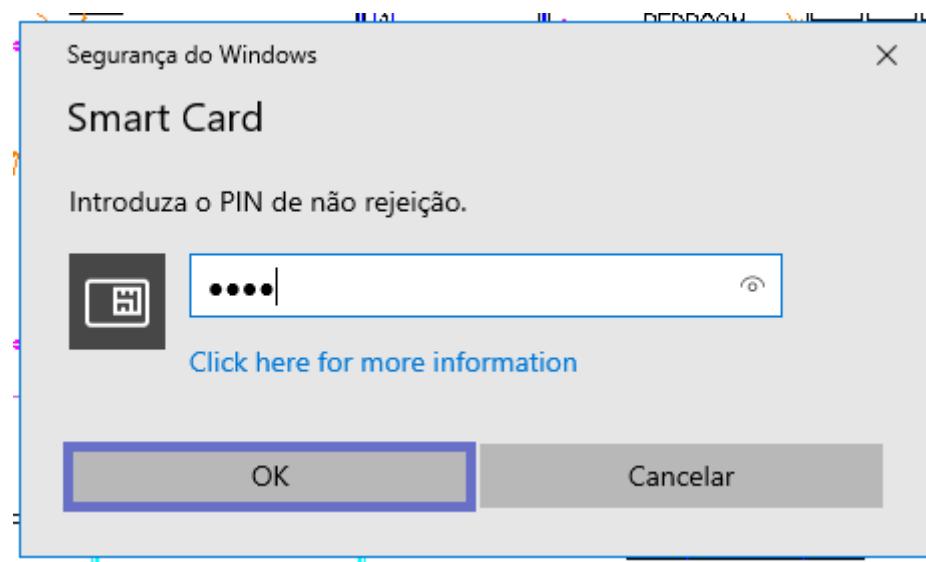
5. Selecione a opção Add Digital Signature:



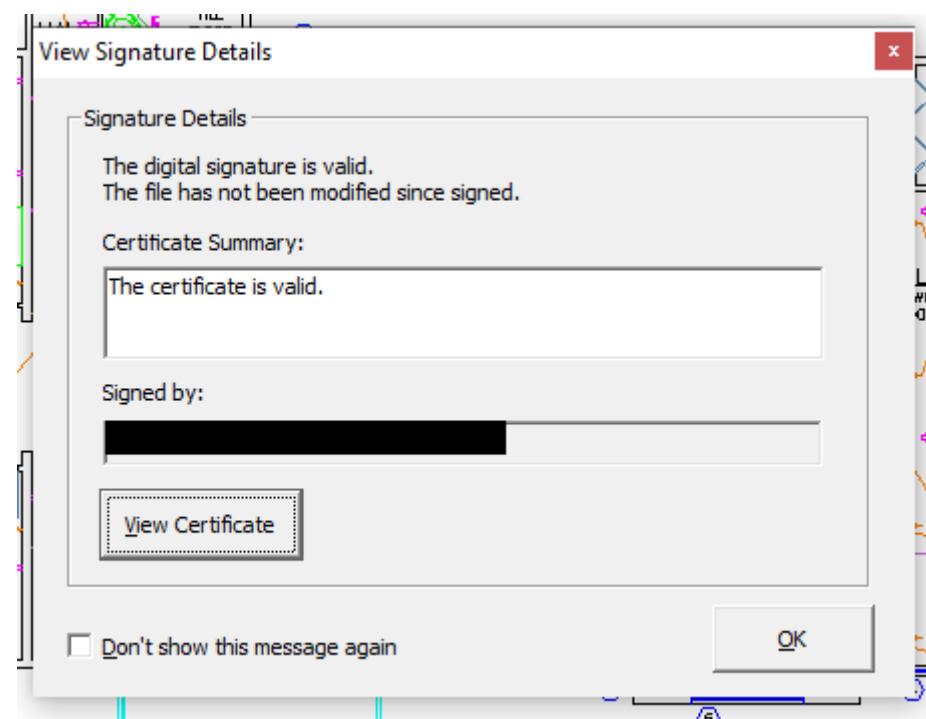
6. Nesta janela vai aparecer os certificados presentes do computador, pode carregar em **Mais Opções** para selecionar outro certificado. Certifique-se que o certificado selecionado corresponde ao de assinatura digital. Por fim, basta carregar **OK**:



7. Introduza o PIN de assinatura pedido na janela:

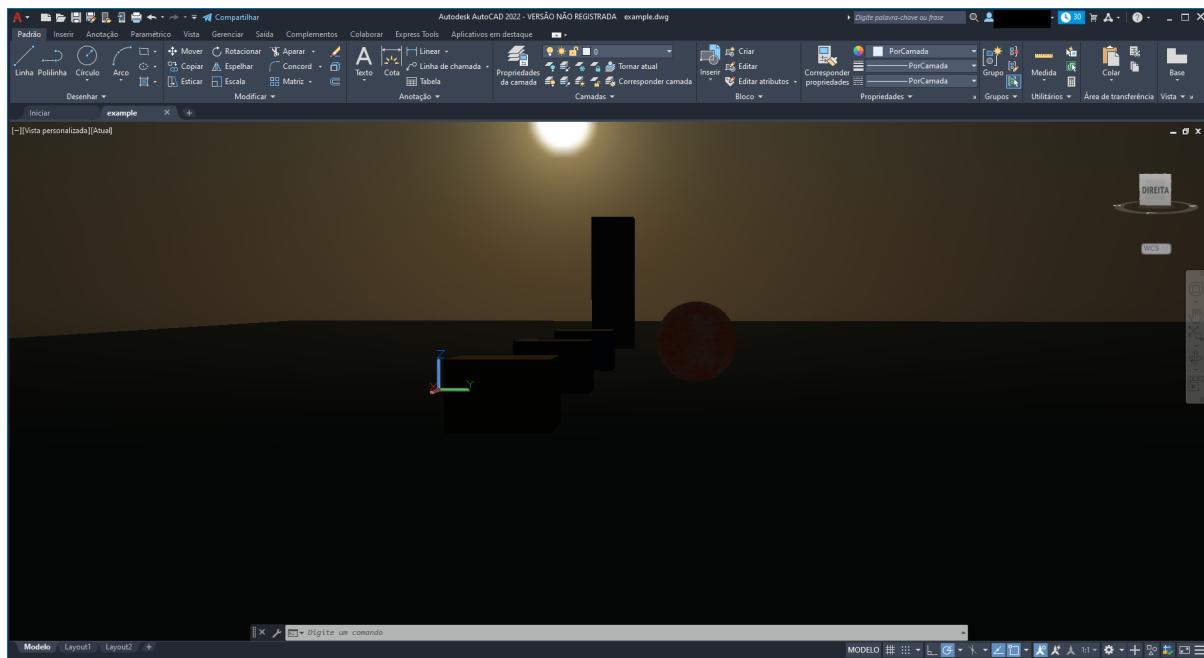


8. Após este procedimento, o processo de assinatura digital está concluído e vai aparecer uma janela a confirmar que assinatura está valida:

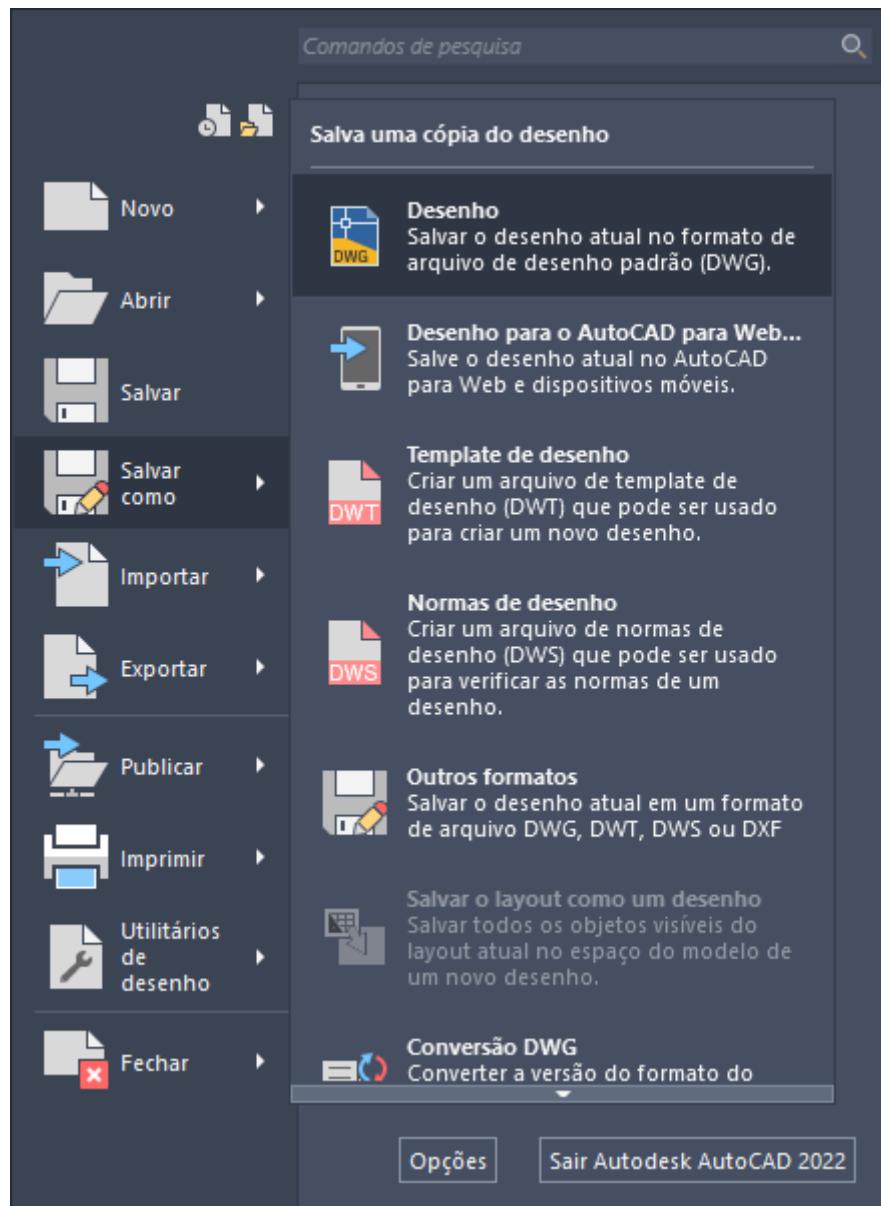


5.3.10 Assinatura digital de ficheiros DWG

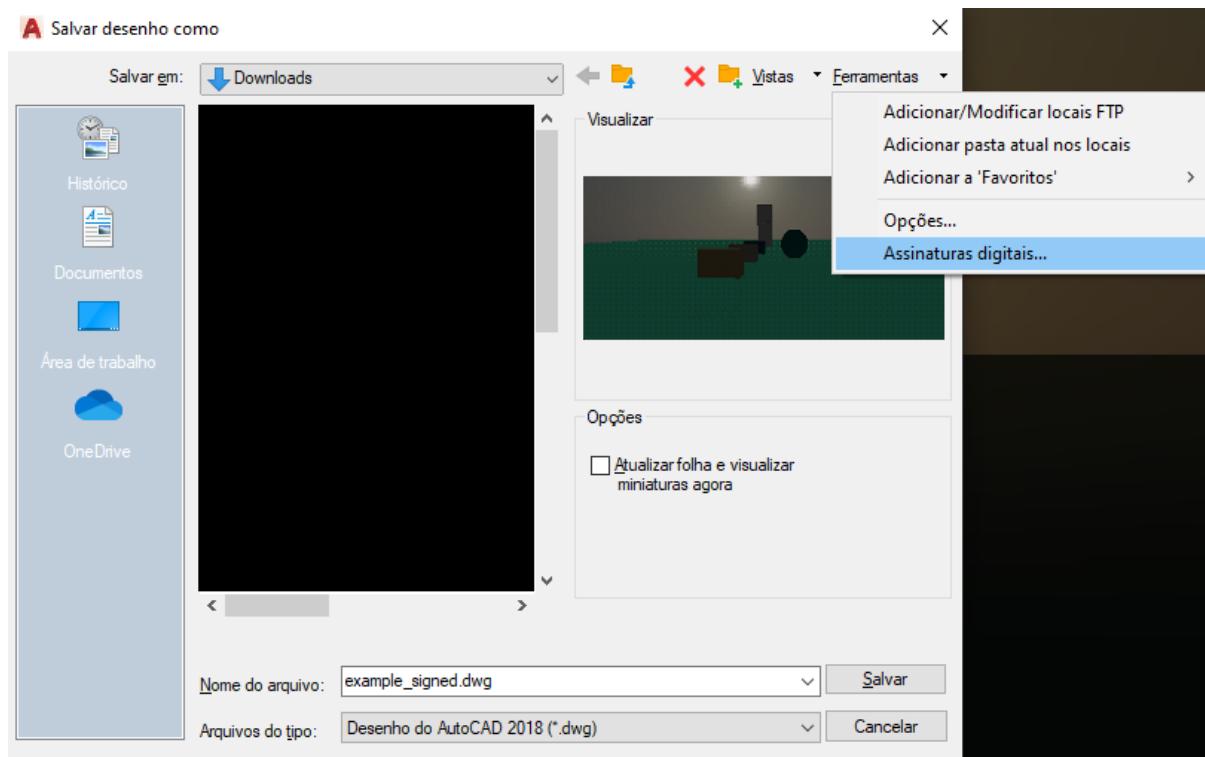
1. Em primeiro lugar, deverá ter instalado no seu computador uma versão atualizada da aplicação **AutoCAD** (a versão testada e cujo funcionamento foi confirmado foi a versão **AutoCAD 2022**).
2. Abra o ficheiro DWG na aplicação.
3. Aceda ao menu no campo superior esquerdo:



4. Aceda à opção **Salvar como** e selecione **Desenho**:



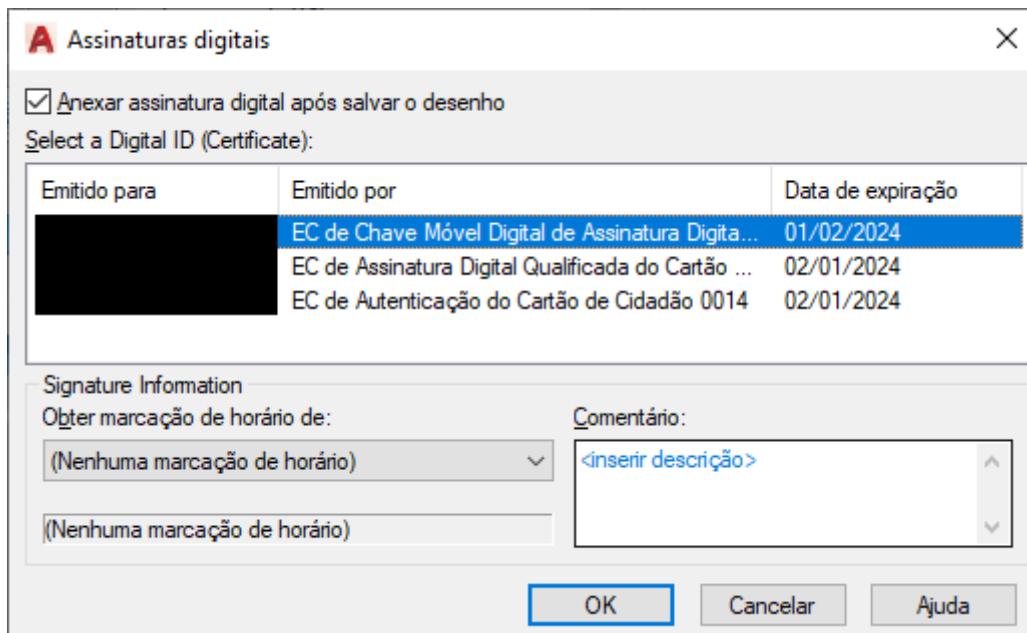
5. Aceda à opção **Ferramentas** e selecione **Assinaturas digitais...**:



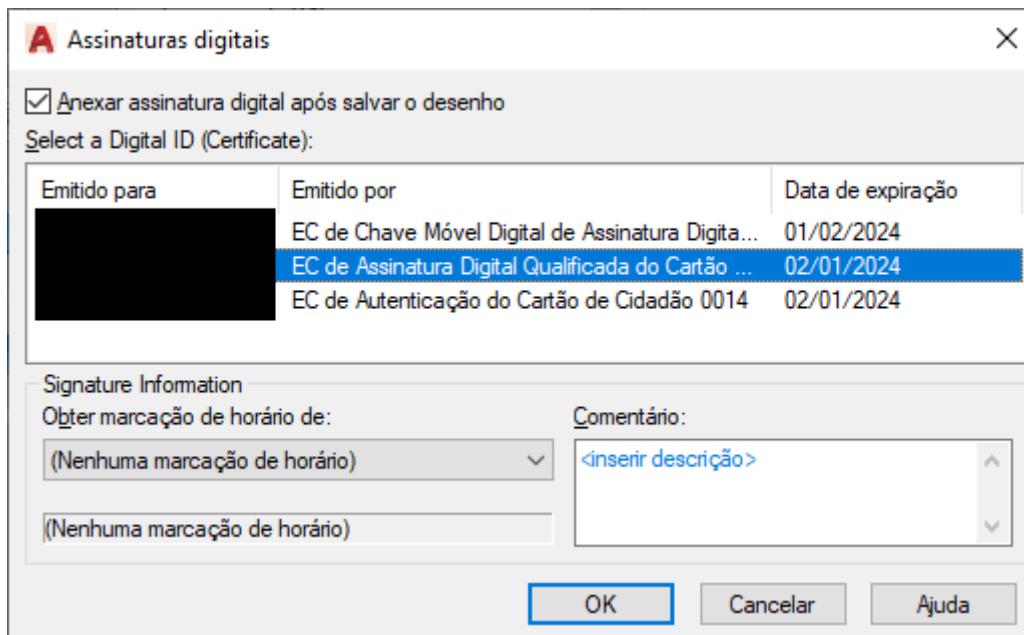
6. Ative a checkbox **Anexar assinatura digital após salvar o desenho**. Nesta janela vai aparecer os certificados presentes do computador, selecione **EC de Chave Móvel Digital...**, se pretender assinar com a Chave Móvel, ou **EC de Assinatura Digital Qualificada do Cartão...**, se pretender assinar com o Cartão de Cidadão. Por fim, basta carregar **OK**:

NOTA: Para efetuar a assinatura com Chave Móvel Digital deve efetuar o procedimento descrito nesta secção Assinatura digital com Chave Móvel Digital .

- Chave Móvel Digital:



- Cartão de Cidadão:



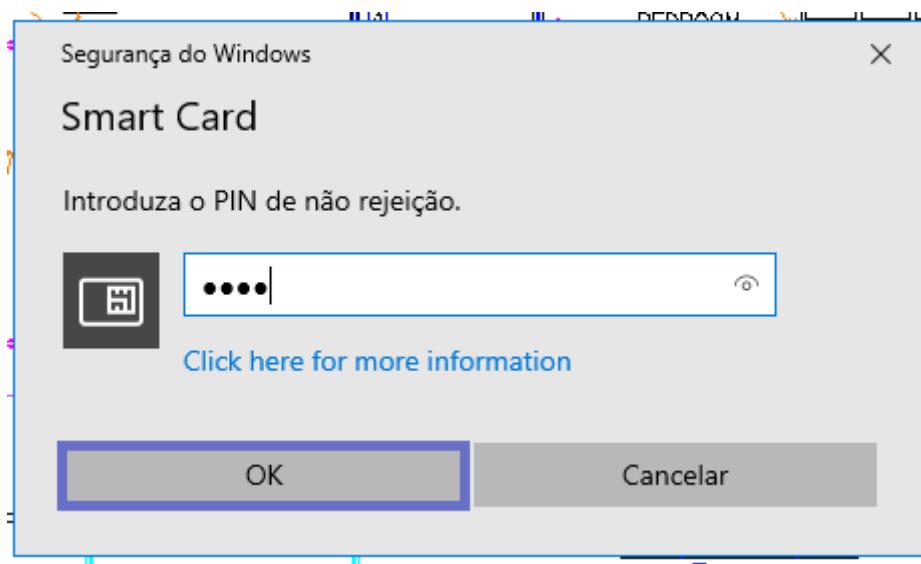
7. No caso da assinatura com o Cartão de Cidadão basta introduzir o PIN de assinatura (denominado na janela como PIN de não rejeição) e carregar **OK**. No caso da assinatura com Chave Móvel Digital vai-lhe ser pedido o seu pin de assinatura da Chave Móvel Digital e, após o ter introduzido corretamente, ser-lhe-á pedido o código de confirmação, enviado para o número de telemóvel registado.

- Chave Móvel Digital:



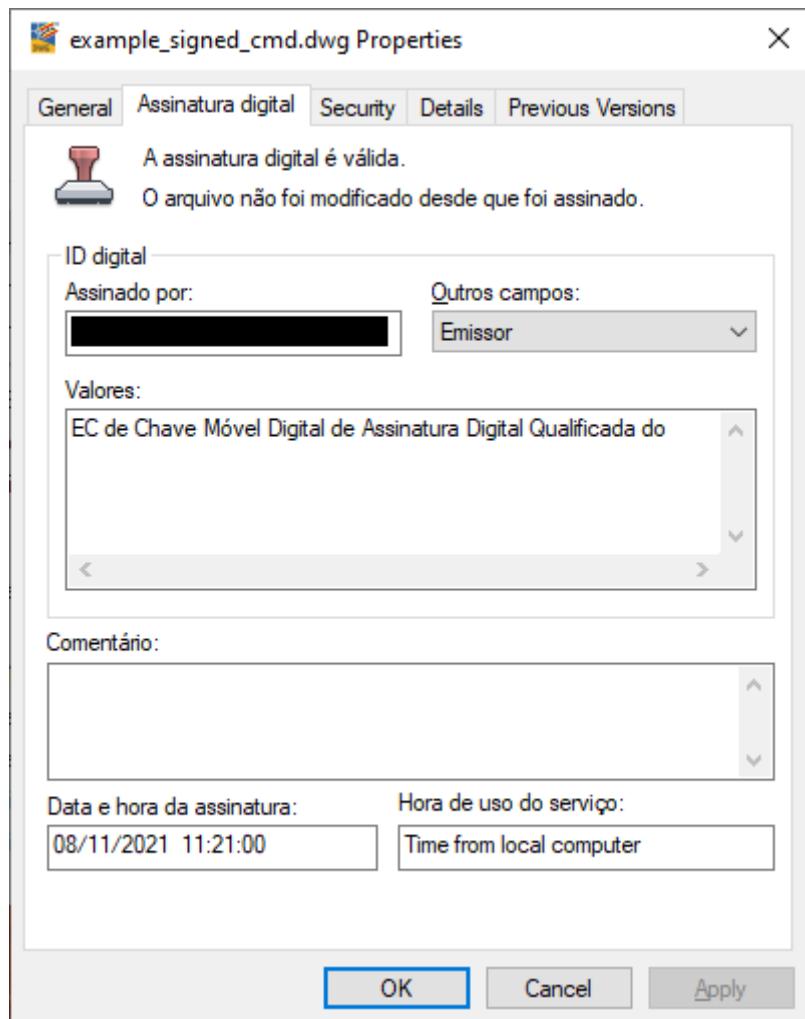


- Cartão de Cidadão:

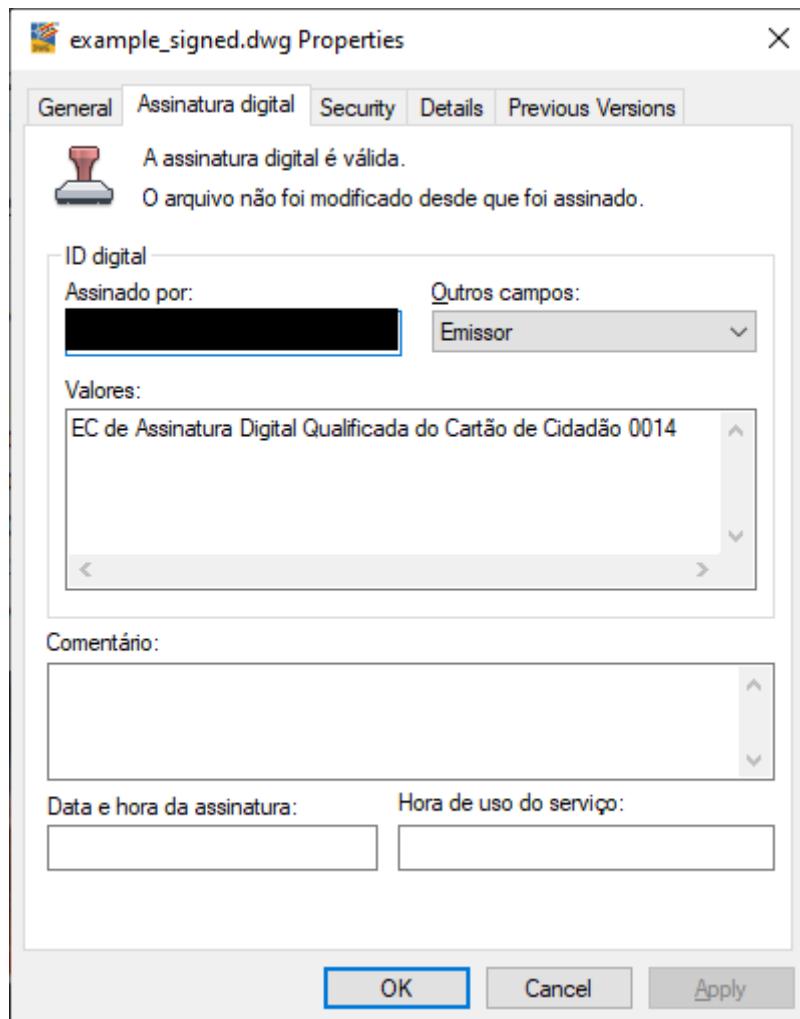


8. Após este procedimento, o processo de assinatura digital está concluído. Pode confirmar a assinatura, carregando com o botão direito do rato no documento, selecionando **Propriedades** e accedendo ao menu **Assinatura Digital**:

- Chave Móvel Digital:



- Cartão de Cidadão:



5.4 Autenticação em portais WEB

Existem duas formas de se autenticar perante um portal web utilizando o Cartão de Cidadão:

- Autenticação por certificado cliente através do navegador.
- Autenticação por certificado através do portal **Autenticação.gov.pt**.

A forma de autenticação depende totalmente da configuração do website, não sendo possível ao utilizador escolher uma ou outra forma.

A **Autenticação por certificado cliente através do navegador**, tende a ser descontinuada, visto a apresentar desvantagens na recolha de dados, no entanto alguns sítios ainda utilizam esta forma.

Para poder utilizar este método de autenticação, tem de ter obrigatoriamente a aplicação instalada no seu computador.

Neste caso utilizando Sistema Operativo *Windows* os browsers *Internet Explorer*, *Microsoft Edge* e *Google Chrome* não exigem nenhuma configuração uma vez registado o certificado de autenticação do Cidadão.

Para o *Mozilla Firefox* em qualquer Sistema Operativo é necessário efetuar algumas configurações descritas em Configurar autenticação para *Mozilla Firefox*.

A autenticação por certificado através do portal autenticação.gov.pt não exige a instalação da aplicação mas sim do plugin **Autenticação.Gov**.

Para mais informação, consulte esta página de ajuda:

- <https://autenticacao.gov.pt/fa/ajuda/autenticacaogovpt.aspx>

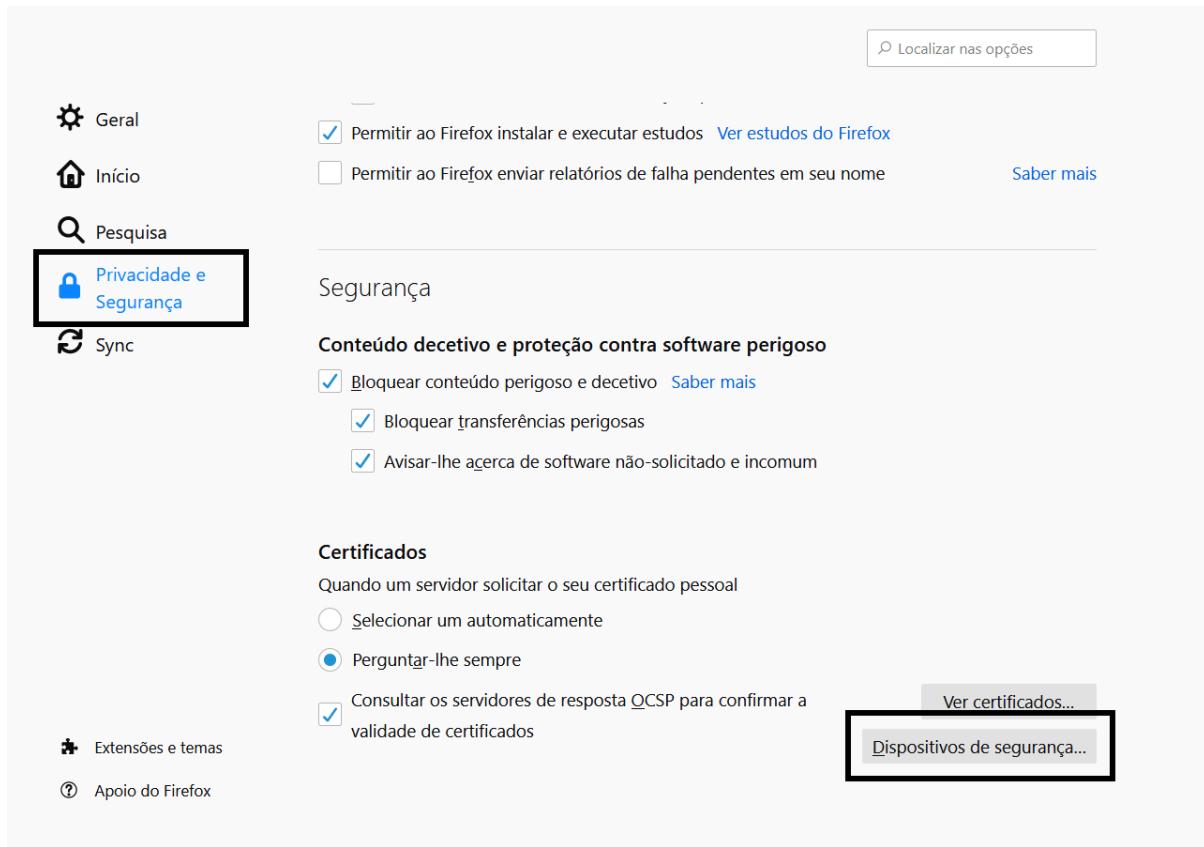
De forma a que a configuração do seu computador suporte qualquer uma das alternativas, recomenda-se que instale a aplicação no seu computador e também o plugin **Autenticação.Gov**.

5.4.1 Configurar autenticação para *Mozilla Firefox*

Para configurar o *Mozilla Firefox* tem que carregar o módulo PKCS#11 do Cartão do Cidadão.

Na versão 73.0.1 (para outras versões deverá ser semelhante):

1. Nas opções do *Mozilla Firefox* aceda a **Privacidade e Segurança**. Pode aceder diretamente inserindo `about:preferences#privacy` na barra de endereço.
2. Navegue até ao final da página e, na secção **Certificados**, carregue em **Dispositivos de segurança...** para abrir a janela "Gestor de dispositivos".



3. Pressione **Carregar**. Preencha o nome do módulo, por exemplo "PKCS#11 do Cartao de Cidadao" (evite o "ç" e "ã"). Seguidamente, carregue em **Procurar...** e navegue até ao módulo PKCS#11 do Cartão de Cidadão, cuja localização se encontra descrita na secção Integração com aplicações.

Nota: em MacOS o que se recomenda neste passo é copiar e colar no campo "Nome do ficheiro do módulo" o seguinte nome: `/usr/local/lib/libpteidpkcs11.dylib`

4. Pressione **Ok** nas janelas abertas para terminar.

6 Resolução de Problemas

6.1 Exibida mensagem de erro quando se tenta adicionar o módulo PKCS#11 no *Firefox* / *Thunderbird*

Para que consiga adicionar o módulo PKCS#11 no Firefox tem de ter um leitor de cartões instalado no seu computador.

Certifique-se que o leitor está ligado e instalado e um cartão inserido antes de adicionar o módulo PKCS#11.

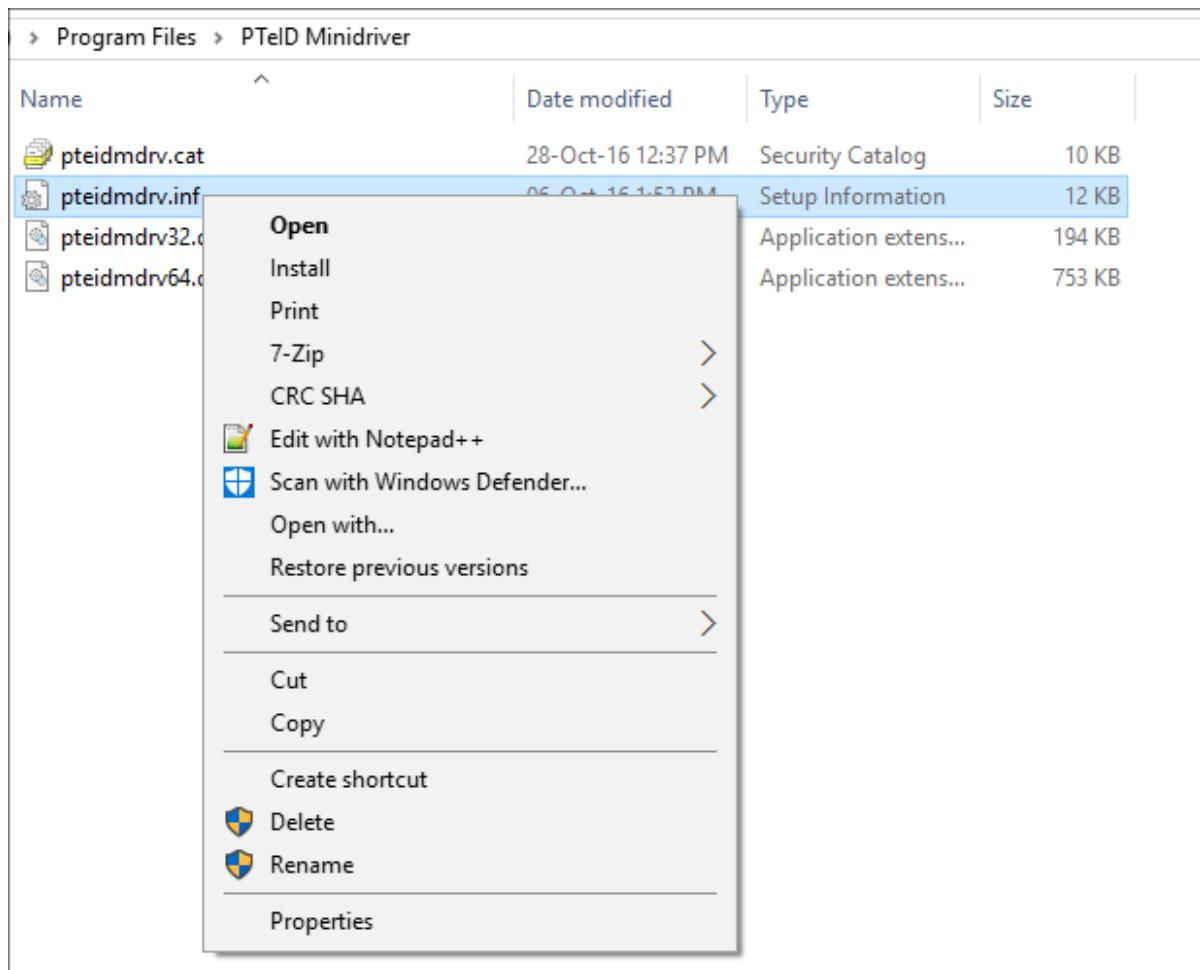
Caso esteja a utilizar uma versão de MacOS ou Linux 64-bit terá de utilizar uma versão 64-bit do *Firefox* / *Thunderbird*.

6.2 Não é possível adicionar o módulo PKCS#11 ao *Adobe Acrobat Reader* em *MacOS*

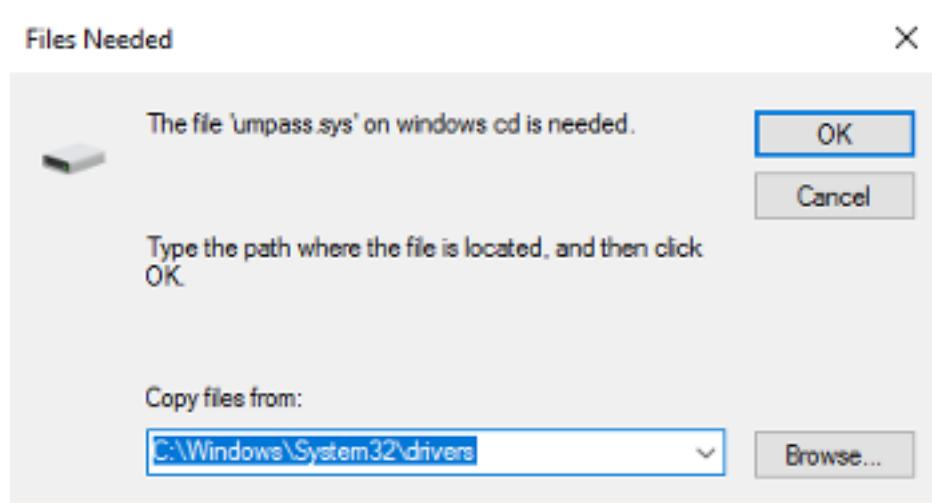
Em versões anteriores do *Adobe Acrobat Reader* para *MacOS* não é possível adicionar o módulo PKCS#11. Recomendamos a atualização do *Adobe Acrobat Reader* para a versão DC.

6.3 Impossibilidade de assinatura em *Adobe Reader*, *Microsoft Office* e *LibreOffice* com Cartão de Cidadão

Deverá aceder ao ficheiro `pteidmdrv.inf`, presente por defeito na diretoria `C:\Program Files\Portugal Identity` (ou na directoria selecionada durante a instalação). Após ter aberto a directoria, abra o menu de opções do ficheiro e selecionar a opção **Instalar**.



Após a escolha desta opção, poderá aparecer uma janela de diálogo (Ver imagem seguinte) com o título "Ficheiros Necessários", na qual terá de selecionar a pasta "drivers" que esta na diretoria C:\Windows\System32 .

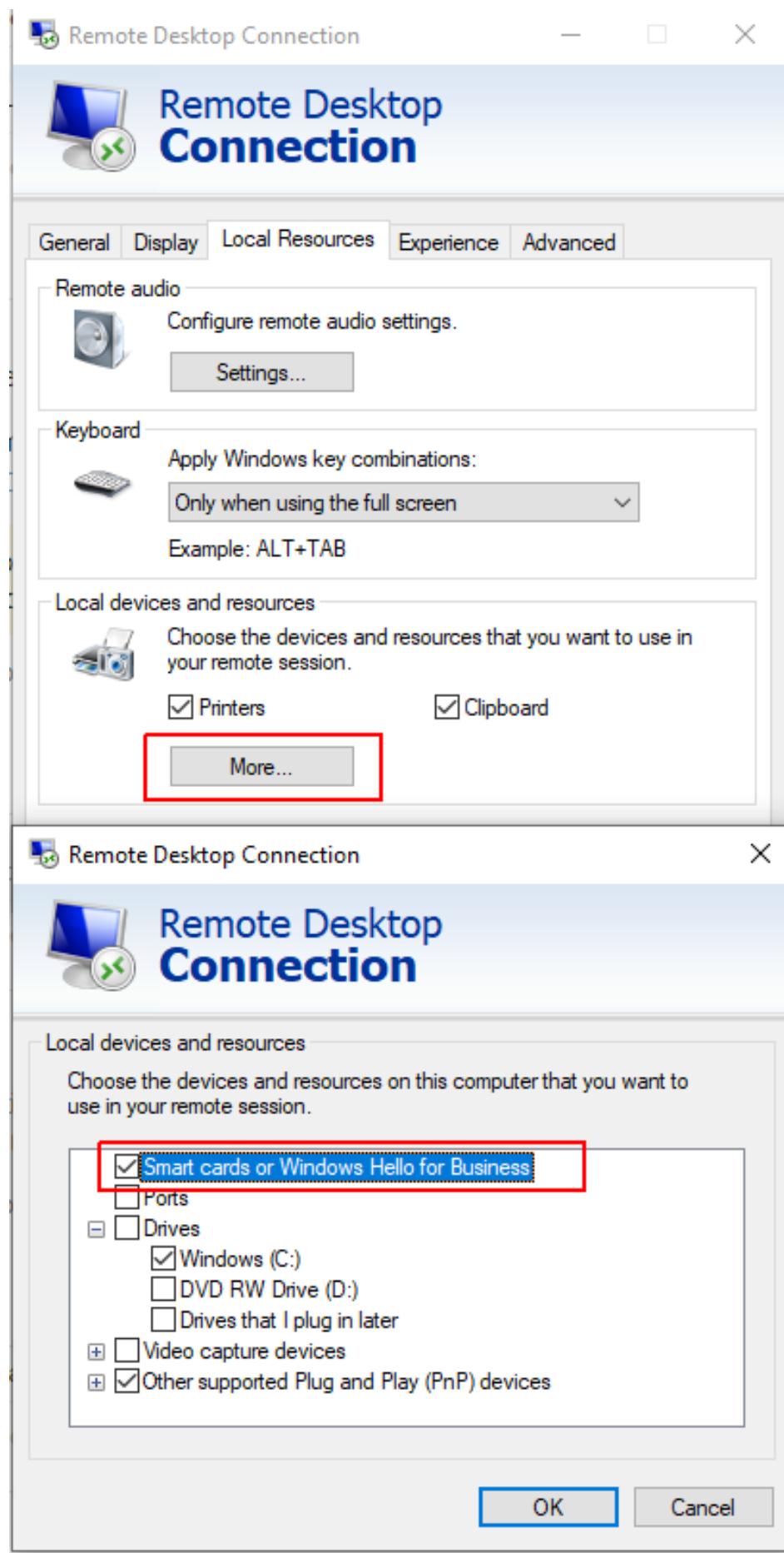


Em caso de problemas verifique se está relacionado com o tópico Problemas com a nova cadeia de confiança.

6.4 O leitor de cartões está instalado mas não é detetado pela aplicação do Cartão de Cidadão

6.4.1 Windows

1. Verifique se o leitor de cartões é compatível com o standard PC/SC (consulte a documentação do leitor de cartões ou contacte o fabricante).
2. Verifique se os controladores do leitor estão corretamente instalados (consulte a documentação do leitor de cartões).
3. Verifique se o serviço Cartão Inteligente (Smart Card) está iniciado:
 - a) Aceda ao **Painel de Controlo** e em seguida aceda a **Ferramentas de Administração**
 - b) Clique em **Serviços**
 - c) Verifique se o serviço **Cartão Inteligente** (Smart Card) está iniciado (Started). Caso não esteja, clique com o botão direito no serviço e clique em **Start**.
 - d) Desligue o leitor do computador.
 - e) Encerre a aplicação do Cartão de Cidadão.
 - f) Volte a inserir o leitor e abra novamente a aplicação.
4. Se estiver a usar uma ligação a uma máquina remota e pretende partilhar o leitor de cartões, verifique se:
 - a) Está a ligar o leitor de cartões no computador local
 - b) Escolheu o **Smart Card** na lista de dispositivos e recursos locais que pretende utilizar na ligação remota (Ver imagem seguinte).



6.4.2 Linux

Para sistemas Ubuntu 22.04 deve consultar a nota 2 desta secção

1. Verifique se o leitor de cartões é compatível com o standard PC/SC (consulte a documentação do leitor ou contacte o fabricante).
 2. Verifique se o driver/controlador do leitor estão corretamente instalados (consulte a documentação do leitor). A maioria dos leitores de smartcards são suportados hoje em dia pelo driver de código aberto CCID: <https://ccid.apdu.fr/>
 3. Verifique se o **pcsc daemon** está instalado e em execução:
 - a) Numa janela de terminal execute o seguinte comando:
`ps -e | grep pcscd`
 - b) Procure uma referência ao processo `pcscd`.
 - c) Caso não esteja listado por favor inicie o serviço através do comando: `sudo systemctl start pcscd`
- d) Caso obtenha uma mensagem de erro é possível que o daemon não esteja instalado. Utilize o gestor de pacotes da sua distribuição para instalar o pcscd (por vezes está incluído num pacote de nome pcsc-lite).

6.5 Não são detetados quaisquer certificados durante a tentativa de assinatura na suite *LibreOffice / Apache OpenOffice*

A suite *LibreOffice / OpenOffice* em Linux, utiliza as configurações da aplicação *Mozilla Firefox* (ou como alternativa, *Thunderbird*) para a deteção dos certificados.

Para que os certificados passem a ser detetados na *Suite LibreOffice / Apache OpenOffice*, terá que efetuar a respetiva configuração no *Mozilla Firefox*, caso tenha esta aplicação instalada. Caso não tenha, poderá configurar o *Mozilla Thunderbird* para poder assinar documentos no *LibreOffice*.

Para mais informações consultar a página de ajuda:

- https://help.libreoffice.org/Common/Applying_Digital_Signatures/pt

6.6 Problemas gráficos na aplicação

O modo de renderização que está configurado na aplicação no momento da instalação é o que permite o melhor desempenho na maioria dos casos: a renderização por Hardware. No entanto este modo exige um driver OpenGL funcional no sistema para a placa gráfica do computador.

No caso de existirem problemas gráficos, recomenda-se alterar o modo de renderização gráfica. Pode fazê-lo na secção Aceleração gráfica do submenu Configuração da aplicação.

No caso da aplicação não arrancar ou tiver problemas no arranque, é possível alterar essa opção de três formas distintas:

1. [Exclusivo para Windows a partir da versão 3.4.0 da aplicação] Na pasta de instalação da aplicação (que por omissão é `C:\Program Files\Portugal Identity Card`) existem três atalhos que permitem abrir a aplicação alterando o modo de renderização gráfica. Os atalhos são ícones clicáveis com o símbolo da aplicação e têm os seguintes nomes:
 - **Autenticação.Gov Software** para renderização por Software (OpenGL);
 - **Autenticação.Gov Hardware** para renderização por Hardware (Placa gráfica);
 - **Autenticação.Gov Direct3d** para renderização por Software (ANGLE, que emula o OpenGL usando Direct3D);

No caso de existirem problemas gráficos, ou a aplicação não arrancar, deverá experimentar as três opções e ver qual tem melhor resultado. A última opção escolhida, ficará guardada e poderá voltar a arrancar a aplicação clicando no ícone no ambiente de trabalho ou no menu iniciar.

2. Usando as configurações do software Autenticação.gov (via Chaves de Registo em Windows ou ficheiro de configuração em Linux e MacOS).

- Em **Windows**, a chave de registo:
HKEY_CURRENT_USER\Software\PTEID\configuretool\graphics_accelaration;
- Em **Linux**, a chave com nome "graphics_accelaration" na secção configuretool do ficheiro:
\$HOME/.config/pteid.conf;
- Em **MacOS**, a chave com nome "graphics_accelaration" na secção configuretool do ficheiro:
\$HOME/Library/Preferences/pteid.conf.

Os valores que a chave pode tomar são:

- 0 para renderização por Software (OpenGL);
- 1 para renderização por Hardware (Placa gráfica);
- 2 (Exclusivo para Windows) para renderização por Software (ANGLE, que emula o OpenGL usando Direct3D).

3. Usando o Interface de linha de comandos.

Em ambiente empresariais deve alterar esta configuração conforme descrito no capítulo Instruções de configuração em ambientes empresariais.

6.7 Problemas com placas gráficas integradas

No caso de existirem problemas com placas gráficas, consulte o tópico Problemas gráficos na aplicação.

6.8 Não é possível mover/arrastar a aplicação (Linux em Wayland)

Em sistemas Linux que utilizem um sistema de interface gráfico baseado em Wayland foram detetados vários problemas de interação, entre os quais a impossibilidade de mover a janela arrastando-a a partir da barra de título.

Recomendamos a seguinte solução temporária, assumindo que existe o componente XWayland:
Usar o parâmetro **-platform xcb** , ou a variável de ambiente **QT_QPA_PLATFORM=xcb** , para forçar a aplicação a correr em modo X11, usando o XWayland.

```
$ eidguiV2 -platform xcb
```

ou

```
$ QT_QPA_PLATFORM=xcb eidguiV2
```

6.9 Aplicação não arranca

No caso da aplicação não arrancar e consequentemente não ser possível alterar as configurações da aplicação na aplicação, é possível alterar as opções da aplicação usando as configurações do software Autenticação.gov (via Chaves de Registo em Windows ou ficheiro de configuração em Linux e MacOS).

Uma causa que pode causar problemas está relacionado com a placa gráfica do computador, consulte o tópico Problemas gráficos na aplicação.

6.10 Problemas com a nova cadeia de confiança

O Sistema de Certificação Eletrónica do Estado colocou em produção um novo certificado raiz do Estado. Em consequência, os certificados do Cartão de Cidadão passaram a ser emitidos, desde 4 de abril de 2020, sob a nova cadeia de confiança do Estado Português. O certificado raiz da nova cadeia, no caso de não ser disponibilizado pelo sistema operativo, deverá ser instalado para que os certificados dos cartões emitidos após essa data sejam automaticamente confiáveis pelo sistema operativo Windows, assim como por algumas aplicações que não utilizam a lista de serviços confiáveis publicada pela União Europeia.

Pode instalar o certificado na *Store* do Windows através da aplicação do Cartão de Cidadão no submenu Configuração de assinaturas. Para tal, clique no botão **Instalar certificado** na secção **Novo certificado raiz do Estado**. O certificado será adicionado à *Store* Trusted Root Certification Authorities associada ao Current User. **Nota:** A funcionalidade de instalar certificado automaticamente só está disponível a partir da versão 3.4.0 da aplicação, versões anteriores deve usar o método manual apresentado em seguida.

Alternativamente, pode instalar o certificado manualmente seguindo as instruções no manual de instalação da cadeia do SCEC disponível em <https://www.ecce.gov.pt/certificados/>. Deverá seguir as instruções específicas para o Certificado da Entidade de Certificação Eletrónica do Estado - ECRaizEstado 002 (passos 4.1 a 4.10 do manual).

6.11 Problemas na validação das assinaturas

Em caso de problemas na validação das assinaturas, verifique se está relacionado com o tópico Problemas com a nova cadeia de confiança.

6.12 Problemas com ficheiros PDF não suportados

A aplicação Autenticação.Gov atualmente não suporta os seguintes ficheiros PDF:

- Ficheiros PDF Encriptados;
- Ficheiros PDF com formulários XFA (criados, por exemplo, na aplicação *Adobe LiveCycle*).

No entanto, é possível assinar estes ficheiros com o cartão de cidadão ou Chave Móvel Digital recorrendo a uma aplicação externa, por exemplo o *Adobe Acrobat Reader*. Para o fazer siga os passos descritos na secção Assinatura digital em *Adobe Acrobat Reader*.

6.13 Erro na Comunicação em assinatura com Chave Móvel Digital

Neste tipo de ocorrências é comum o cidadão estar ligado numa rede empresarial. Caso se verifique, é provável que exista na rede uma *gateway* de segurança ou *proxy* HTTPS que filtra o tráfego HTTPS e interfere com a ligação ao serviço de assinatura com Chave Móvel Digital.

Deve pedir ao Administrador de redes ou suporte informático da sua empresa ou organização para configurar uma exceção à filtragem do tráfego HTTPS para o serviço de **Assinatura com Chave Móvel Digital**. As informações necessárias estão na secção abaixo Serviços online usados pela aplicação. Recomendamos que adicione à lista de exceções os endereços dos vários serviços online usados pela aplicação.

6.14 Serviços online usados pela aplicação

Algumas funcionalidades da aplicação requerem a ligação a serviços online para funcionarem corretamente. É por isso necessário garantir que não existe *firewall* ou outro *software* na rede local que impeça a ligação a estes serviços.

Os *hostnames* e respetivos portos utilizados são listados em seguida por funcionalidade.

Assinatura com Chave Móvel Digital:

- cmd.autenticacao.gov.pt (porto 443)

Validação de certificados:

Servidores OCSP:

- ocsp.ecee.gov.pt (porto 80 e 443)
- ocsp.multicert.com (porto 80)
- ocsp.root.cartaoecidadao.pt (porto 80)
- ocsp.auc.cartaoecidadao.pt (porto 80)
- ocsp.asc.cartaoecidadao.pt (porto 80)

Servidores CRL:

- crls.ecee.gov.pt (porto 80)
- pkiroot.multicert.com (porto 80)
- pki.cartaoecidadao.pt (porto 80)

Assinatura com atributos Profissionais:

- scap.autenticacao.gov.pt (porto 443)
- autenticacao.gov.pt (porto 443) (apenas para carregamento com CMD)

Leitura da morada:

- morada.cartaoecidadao.pt (porto 443) (utilizado desde a versão 3.9.0 da aplicação)

Atualização da aplicação:

- autenticacao.gov.pt (porto 443)
- aplicacoes.autenticacao.gov.pt (porto 443)

Atualização de certificados e notícias:

- raw.githubusercontent.com
 - Na obtenção do ficheiro em https://raw.githubusercontent.com/amagovpt/autenticacao.gov/master/pteid-mw-pt/_src/eidmw/news.json
- github.com
 - URLs da forma: https://github.com/amagovpt/autenticacao.gov/blob/master/pteid-mw-pt/_src/eidmw/misc/certs/NOME_DO_FICHEIRO

Documentação:

- URLs da forma: https://amagovpt.github.io/docs.autenticacao.gov/NOME_DO_FICHEIRO

Selo temporal (por defeito):

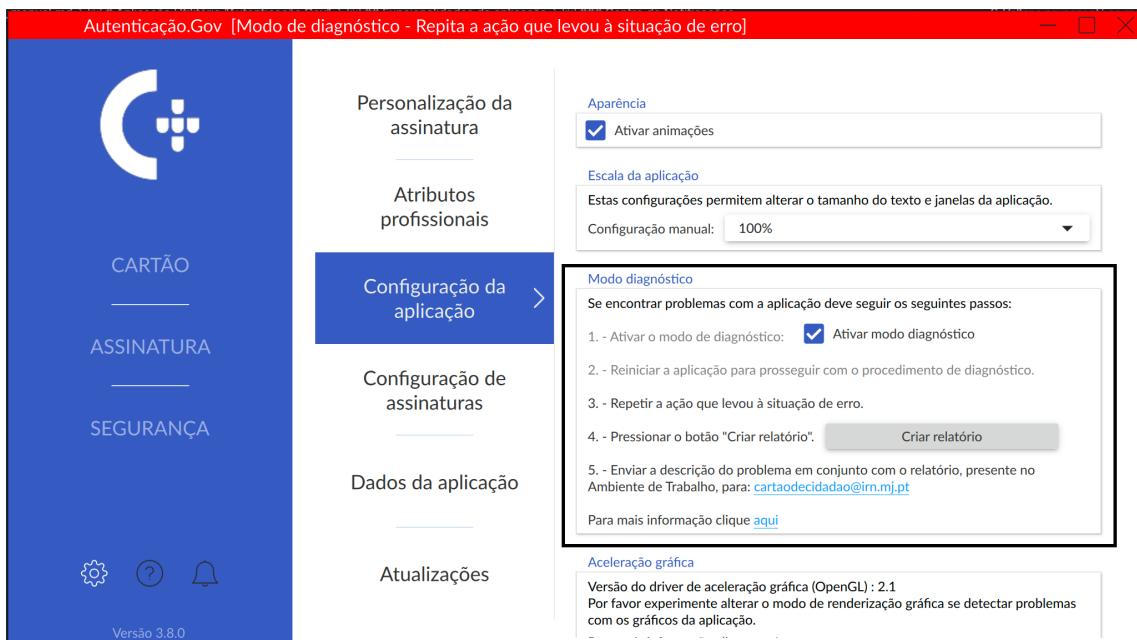
- ts.cartaoecidadao.pt (porto 80)

6.15 Obtenção do relatório para análise através do menu Configurações

A partir da versão 3.5.0 da aplicação, para todos os sistemas operativos, para ajudar a diagnosticar um problema com a aplicação local **Autenticação.gov**, é possível criar um **Relatório de Suporte**. Este **Relatório de Suporte** contém os ficheiros de log com informações sobre o funcionamento da aplicação, essenciais para o diagnóstico de eventuais problemas.

Para obter o **Relatório de Suporte** deve:

1. Abrir a aplicação e navegar até ao menu **Configurações -> Configurações da Aplicação**.
2. Na secção "Modo diagnóstico" selecionar a opção **Ativar modo diagnóstico**.
3. Reiniciar a aplicação.
4. Após reiniciar, a aplicação deverá indicar o modo de diagnóstico ativo na barra de topo da aplicação, bem como a cor da mesma barra mudar para vermelho. Ver imagem seguinte.
5. Repetir a ação que resultou na situação de erro/problema. Desta forma, com o modo diagnóstico ativo, as informações sobre o erro/problema constantes nos ficheiros de log serão mais detalhadas.
6. Voltar a navegar até ao menu **Configurações -> Configurações da Aplicação**.
7. Pressionar o botão **Criar relatório**. Ao pressionar o botão **Criar relatório** é criado um ficheiro zip no Ambiente de Trabalho que contém os ficheiros de log da aplicação, com um nome deste tipo: **Autenticacao.gov_logs_DATA.zip**.
8. Por fim, deve enviar este ficheiro zip, juntamente com uma descrição o mais detalhada possível do problema, para o contacto de suporte através do email **cartaodecidadao@irn.mj.pt**.



6.16 Remoção de metadados de ficheiros PDF

A remoção de metadados de ficheiros PDF, através, por exemplo, da opção "Imprimir para PDF" de alguns browsers, pode remover as assinaturas digitais existentes no ficheiro, mesmo que o selo visual se mantenha.

Por este motivo, caso seja necessária a remoção de metadados, através desse ou de outro processo semelhante, esta deve ser feita antes de realizar qualquer assinatura.

7 Interface de linha de comandos

Nota: Esta funcionalidade só está disponível a partir da versão 3.3.0 da aplicação.

Quando executada a partir da linha de comandos, a aplicação Autenticação.gov para computador aceita alguns modos e opções descritos nas seguintes subsecções.

7.1 Consultar ajuda e versão

A opção `--help` (ou `-h`) permite, para cada modo, consultar as opções disponíveis na linha de comandos.

A versão instalada pode ser consultada com `--version` (ou `-v`).

Exemplo (Linux):

```
$ eidguiV2 -h
```

7.2 Atalho para configurar modo de renderização gráfica

É possível configurar o modo de renderização gráfica com umas das seguintes opções:

- `-w`: (Exclusivo para Windows) para renderização por Software (ANGLE, que emula o OpenGL usando Direct3D).
- `-s`: para renderização por Software (OpenGL);
- `-c`: para renderização por Hardware (Placa gráfica)(Valor por omissão);

No caso de existirem problemas gráficos, ou a aplicação não arrancar, deverá experimentar as três opções e ver qual tem melhor resultado. A última opção escolhida, ficará guardada e poderá voltar a arrancar a aplicação clicando no ícone no ambiente de trabalho, no menu iniciar ou mesmo pela linha de comandos sem passar este parâmetro.

No caso de existirem problemas com placas gráficas, consulte o tópico Problemas gráficos na aplicação.

Exemplo (Linux):

```
$ eidguiV2 -c
```

Exemplo (Windows):

```
$ "C:\Program Files\Portugal Identity Card\pteidguiV2.exe" -c
```

7.3 Atalho para submenu de assinatura

Através da interface de linha de comandos, é possível iniciar a aplicação diretamente no submenu de assinatura digital.

O atalho para o submenu de assinatura (*sign*) requer os caminhos dos ficheiros a serem carregados para assinatura.

As opções suportadas são as seguintes:

- `--destino DESTINO` (`-d DESTINO`): configura a pasta de destino do ficheiro assinado. A pasta de destino não será pedida ao utilizador no momento da assinatura.
- `--tsa`: ativa a assinatura com timestamp;
- `--motivo MOTIVO` (`-m MOTIVO`): configura o campo 'motivo' da assinatura;
- `--localidade LOCALIDADE` (`-l LOCALIDADE`): configura o campo 'localidade' da assinatura.

Exemplos (Linux):

```
$ eidguiV2 sign -d /home/user/Documents/ ficheiro.pdf  
$ eidguiV2 sign --tsa -m "motivo" -l "localidade" -d /home/user/Documents/ \  
ficheiro1.pdf ... ficheiroN.pdf
```

Exemplo (Windows):

```
> "C:\Program Files\Portugal Identity Card\pteidguiV2.exe" sign^  
-d C:\Users\USER\Documents ficheiro.pdf
```

Nota: As opções passadas por parâmetros, que contêm um caracter espaço, devem ser colocadas entre aspas. Por exemplo (Linux):

```
$ eidguiV2 sign -d /home/user/Documents/ "ficheiro para assinar.pdf"
```

8 Instruções de configuração em ambientes empresariais

8.1 Configurações através de chaves de registo Windows

As configurações do software Autenticação.gov são guardadas em *Windows* em chaves de registo sendo que as alterações feitas pelo utilizador no interface gráfico se sobreponem aos valores predefinidos e ficam guardadas em sub-chaves de:

`HKCU\Software\PTEID`

Pode-se, no entanto, configurar de forma padronizada uma instalação adicionando alguns valores no registo do *Windows* para todos os utilizadores da máquina após a instalação do software, usando as chaves listadas abaixo, sub-chaves da chave raiz: `HKLM\Software\PTEID`

Nota: Não se devem nunca remover ou alterar os seguintes registos:

`HKLM\Software\PTEID\general\install_dirname`

`HKLM\Software\PTEID\general\certs_dir`

Os seguintes registos podem ser adicionados:

`HKLM\Software\PTEID\logging\log_level`

- **Tipo:** String (debug, info, warning, error)
- **Descrição:** Nível de detalhe do log do Middleware e da aplicação.
- **Valor por omissão:** error

`HKLM\Software\PTEID\logging\log_dirname`

- **Tipo:** String
- **Descrição:** Directória onde são gerados os ficheiros de log do Middleware e da aplicação.
- **Valor por omissão:** `C:\Program Files\Portugal Identity Card\log`

HKLM\Software\PTEID\logging\log_prefix

- **Tipo:** String
 - **Descrição:** Prefixo do nome dos ficheiros de log.
 - **Valor por omissão:** .PTEID_
-

HKLM\Software\PTEID\general\admin_config

- **Tipo:** Número (0 / 1)
 - **Descrição:** Ativar (1) ou desativar (0) a configuração de administrador, forçando o uso da proxy configurada pelo administrador na secção de registo de proxy em HKLM. Desta forma valores inseridos pelo utilizador são ignorados e a configuração de proxy torna-se desabilitada nas definições da aplicação.
 - **Valor por omissão:** 0 (desativo)
-

HKLM\Software\PTEID\general\cache dirname

- **Tipo:** String
 - **Descrição:** Directória onde é guardada a cache do Middleware e da aplicação.
 - **Valor por omissão:** C:\Users\[User]\AppData\Roaming\.pteid-ng
-

HKLM\Software\PTEID\general\cache_enabled

- **Tipo:** Número (0 / 1)
 - **Descrição:** Ativar (1) ou desativar (0) a cache relativa aos dados do Cartão do Cidadão.
 - **Valor por omissão:** 1 (ativa)
-

HKLM\Software\PTEID\general\scap_host

- **Tipo:** String
 - **Descrição:** Hostname do serviço de Atributos Profissionais (SCAP).
 - **Valor por omissão:** scap.autenticacao.gov.pt
-

HKLM\Software\PTEID\general\scap_port

- **Tipo:** Número (1 a 65535)
 - **Descrição:** Porto do serviço de Atributos Profissionais (SCAP).
-

HKLM\Software\PTEID\general\use_pinpad

- **Tipo:** Número (0 / 1)
 - **Descrição:** Usar funcionalidade de PINPAD.
 - **Valor por omissão:** 1 (Sim)
-

HKLM\Software\PTEID\general\auth_pin_cache_normal

- **Tipo:** Número (0 / 1)
 - **Descrição:** Permitir cache do PIN de autenticação via minidriver.
 - **Valor por omissão:** 0 (Não). Para versões anteriores à 3.1.0 o valor por omissão é 1.
 - **Configurável a partir da versão:** 3.1.0
-

HKLM\Software\PTEID\configuretool\start_autoupdate

- **Tipo:** Número (0 / 1)
 - **Descrição:** Verificar se existem atualizações de software ou certificados no arranque da aplicação e notificar o utilizador
 - **Valor por omissão:** 1 (Sim)
-

HKLM\Software\PTEID\configuretool\graphics_accelaration

- **Tipo:** Número (0 / 1 / 2 (somente em Windows))
 - **Descrição:** Modo de renderização gráfica. 0 para renderização por Software (OpenGL), 1 para renderização por Hardware (Placa gráfica) ou 2 para rederização por Software (ANGLE que emula o OpenGL usando Direct3D).
 - **Valor por omissão:** 1 (Placa gráfica)
-

HKLM\Software\PTEID\configuretool\start_with_windows

- **Tipo:** Número (0 / 1)
 - **Descrição:** Arrancar a aplicação com o Windows.
 - **Valor por omissão:** 1 (Sim)
-

HKLM\Software\PTEID\configuretool\registrate_certificate

- **Tipo:** Número (0 / 1)
 - **Descrição:** Registar certificados no Windows com a inserção do cartão. As opções de registo e remoção de certificados requerem que esta aplicação esteja em funcionamento (minimizada ou maximizada).
 - **Valor por omissão:** 1 (Sim)
-

HKLM\Software\PTEID\configuretool\remove_certificate

- **Tipo:** Número (0 / 1)
 - **Descrição:** Remover certificados do Windows com a remoção do cartão.
 - **Valor por omissão:** 0 (Não)
-

HKLM\Software\PTEID\proxy\use_system_proxy

- **Tipo:** Número (0 / 1)
 - **Descrição:** Utilizar servidor de proxy definido no Windows/ MacOS.
 - **Valor por omissão:** 1 (Sim)
-

HKLM\Software\PTEID\proxy\proxy_host

- **Tipo:** String (hostname ou endereço IP)
 - **Descrição:** Endereço do servidor de proxy.
-

HKLM\Software\PTEID\proxy\proxy_port

- **Tipo:** Número (1 a 65535)
 - **Descrição:** Porto TCP do servidor de proxy.
-

HKLM\Software\PTEID\certificatecache\cert_cache_validity

- **Tipo:** Número (0 a 2147483647)
 - **Descrição:** Tempo de cache local (em segundos) do estado de validade dos certificados.
 - **Valor por omissão:** 60
-

HKLM\Software\PTEID\xsign\tsa_url

- **Tipo:** String
 - **Descrição:** Servidor de timestamps usado na assinatura de documentos no formato http(s)://HOST:PORTO
 - **Valor por omissão:** http://ts.cartadecidadao.pt/tsa/server
-

8.2 Configurações através de ficheiro de configuração em Linux e MacOS

As configurações do software Autenticação.gov são guardadas em Linux e MacOS num ficheiro de configuração. Este ficheiro de configuração está localizado no seguinte caminho:

Linux: `$HOME/.config/pteid.conf`

MacOS: `$HOME/Library/Preferences/pteid.conf`

onde **\$HOME** indica a directória Home do utilizador de sistema.

O formato do ficheiro segue o formato INI com a respectiva secção de configuração a ser indicada por uma tag. Os valores que se podem especificar em cada secção/tag são os que foram indicados na tabela anterior referente às Configurações através de chaves de registo Windows.

Por exemplo para ativar manualmente o modo de diagnóstico devem ser adicionadas ao ficheiro as 2 seguintes linhas:

```
[logging]
log_level=debug
```

8.3 Instalação automatizada em ambientes Windows

Para instalar o software de forma automatizada é necessário seguir o seguinte procedimento (com permissões de administrador):

1. Adicionar o certificado de *codesigning* da AMA Agência para a Modernização Administrativa à Store Trusted Publishers associada ao Local Computer através da ferramenta MMC ou através do seguinte comando:

```
certmgr -add AMA\_codesigning.cer -c -s -r localMachine TrustedPublisher
```

O certificado pode ser obtido a partir do instalador MSI visualizando a assinatura do ficheiro no menu de contexto em:

Properties Digital Signatures Details

2. Se o sistema operativo for *Windows 7* deverá ser instalado um *Hotfix* fornecido pela *Microsoft* para resolver uma incompatibilidade com o certificado de *codesigning* do software. Para tal seguir as instruções deste artigo:

<https://support.microsoft.com/en-us/help/2921916/the-untrusted-publisher-dialog-box-appears-when-you-install-a-driver-i>

3. Tendo já obtido o instalador em formato MSI podemos instalar o software sem interacção com o utilizador usando o seguinte comando:

```
msiexec /i Autenticacao.gov-xxx.msi /qn
```

Se se pretende evitar o reinício do sistema após a instalação deve ser adicionado ao comando o parâmetro */norestart*.

8.4 Informação sobre servidores de Proxy

8.4.1 Configuração em *Windows*

Se a máquina em questão tiver um proxy correctamente configurado no Windows, seja por IP/Hostname + Porto ou por script de autoconfiguração (PAC file) não é necessária qualquer configuração no MW.

O software tem neste momento uma limitação com alguns tipos de servidores de proxy designadamente com autenticação NTLM ou Kerberos. Para utilizar as funcionalidades que exigem acesso à Internet (leitura de morada, desde a versão 3.9.0 da aplicação, validação de certificados, assinatura com atributos profissionais ou assinatura com Chave Móvel) será necessário nestes ambientes uma reconfiguração de rede ou o uso de uma proxy aberta ou com autenticação Basic.

8.4.2 Configuração em *MacOS*

Em MacOS é suportada a proxy do sistema mas apenas se for configurada por IP/Hostname + Porto

9 Notas do Utilizador