Manual de Utilização do Middleware da Identificação Eletrónica em Cabo Verde

Versão 1.9.7

04/11/2021

Tabela de Conteúdos

1 Introdução **3**

2 Download, instalação e remoção do middleware **4**
2.1 Sistemas Operativos oficialmente suportados . . . 4
2.2 Download do pacote de instalação do middleware . . . 4
2.3 Instalação do *middleware* . . . 4
2.3.1 Instalação em Microsoft Windows . . . 4
2.3.2 Instalação em Linux . . . 6
2.3.3 Instalação em Mac OS . . . 7
2.4 Remoção do *middleware* . . . 7
2.4.1 Remoção em Microsoft Windows . . . 7
2.4.2 Remoção em Linux . . . 9
2.4.3 Remoção em MacOS . . . 10

3 Aplicação Utilitária "Cabo Verde eID" **11**
3.1 Apresentação da Aplicação . . . 11
3.2 Funcionalidades da aplicação . . . 12
3.2.1 Menu Cartão . . . 12
3.2.2 Serviços Online . . . 15
3.2.3 Assinatura digital . . . 17
3.2.4 Segurança . . . 24
3.2.5 Configurações . . . 31
3.2.6 Ajuda . . . 34

4 Integração com aplicações **35**
4.1 Assinatura digital na suite *Microsoft Office* . . . 35
4.2 Assinatura digital na suite *LibreOffice / OpenOffice* . . . 36
4.3 Assinatura digital de email com *Microsoft Outlook* . . . 37
4.4 Autenticação em *Mozilla Firefox* . . . 42

5 Resolução de Problemas **43**
5.1 Mensagens de erro na ativação de certificados e leitura dos dados online . . . 43
5.2 Impossibilidade de assinatura com *Adobe Reader*, *Microsoft Office* e *LibreOffice* . . . 43
5.3 O leitor de cartões está instalado mas não é detetado pela aplicação Cabo Verde eID . . . 44
5.4 Problemas com placas gráficas integradas em *Windows* . . . 44

6 Instruções de configuração em ambientes empresariais **45**
6.1 Configurações através de chaves de registo Windows . . . 45
6.2 Configurações através de ficheiro de configuração em MacOS . . . 46
6.3 Informação sobre servidores de Proxy . . . 46
6.3.1 Configuração em *Windows* . . . 46
6.3.2 Configuração em *MacOS* . . . 46

7 Notas do Utilizador **47**

1 Introdução

Este manual pretende descrever todas as funcionalidades providenciadas pelo *middleware* da Identificação Eletrónica em Cabo Verde.

O *middleware* da Identificação Eletrónica em Cabo Verde, pode definir-se como a "camada" de software entre o computador e o seu documento de identificação. Através do *middleware* são disponibilizadas ao sistema operativo e aplicações funcionalidades de autenticação.

Além do *middleware*, existe também uma aplicação para a gestão do seu documento de identificação, onde poderá visualizar as suas informações, editar as suas notas, modificar os seus *PIN*s pessoais e assinar digitalmente ficheiros.

Este *middleware* suporta o Cartão Nacional de Identificação (CNI) e o Título de Residência para Estrangeiros (TRE).

Este manual abrange três áreas fundamentais da utilização do *middleware*:

- Na primeira área, aborda o descarregamento, instalação e remoção do *middleware*;
- Na segunda área, descreve as funcionalidades da aplicação de gestão do documento de identificação;
- Na terceira área, documenta a resolução de problemas e configuração em ambientes empresariais;

2 Download, instalação e remoção do middleware

Neste ponto são apresentadas as instruções para a instalação e remoção do *middleware* da Identificação Eletrónica em Cabo Verde.

2.1 Sistemas Operativos oficialmente suportados

A lista de sistemas operativos suportados, nas suas arquiteturas de 32 e 64 bits, são:

- Sistemas operativos Windows:
  - Windows 7;
  - Windows 8/8.1;
  - Windows 10
- Distribuições de Linux:
  - Ubuntu: 20.04 e superiores
- Sistemas operativos Apple MacOS:
  - Versões MacOS Mojave (10.14) e superiores.

2.2 Download do pacote de instalação do middleware

Para obter o pacote de instalação do *middleware*, deverá aceder ao sítio oficial da Identificação Eletrónica em Cabo Verde em https://sniac.cv/.

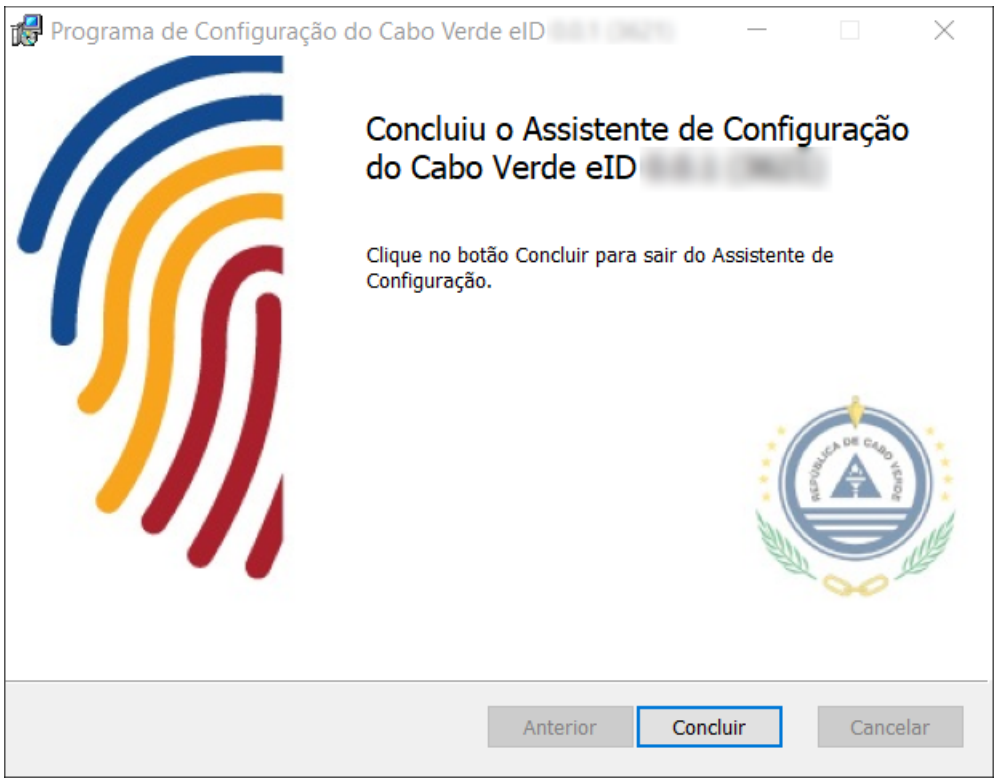
2.3 Instalação do *middleware*

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

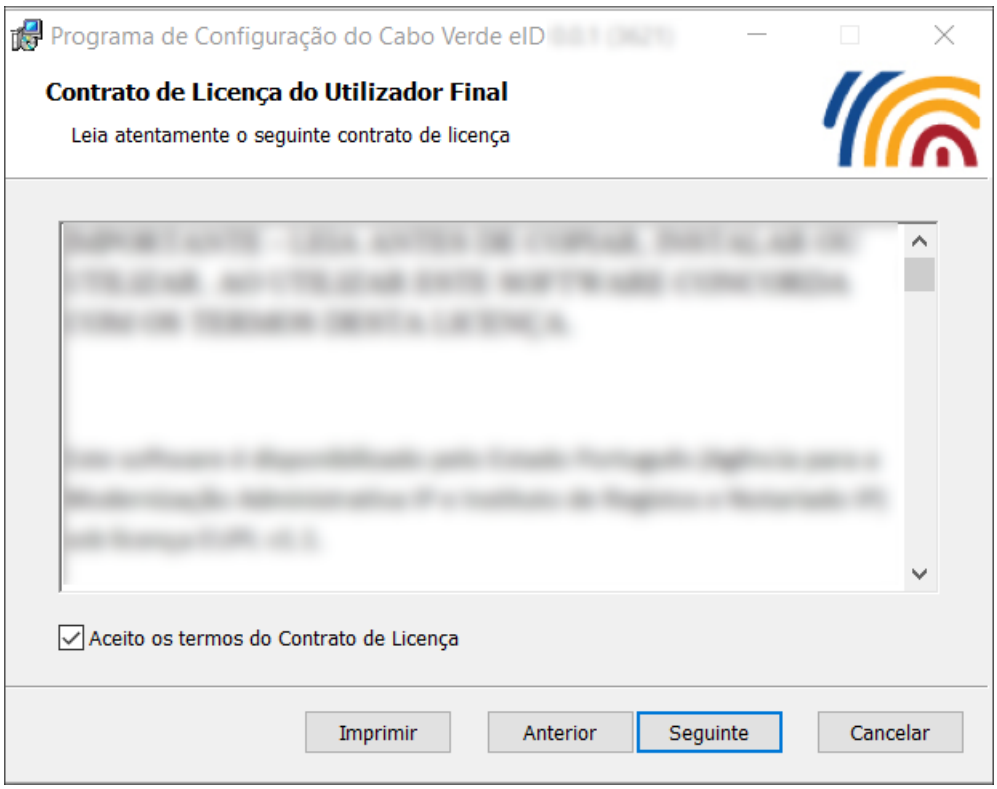
Para a instalação do *middleware* da Identificação Eletrónica em Cabo Verde, deverão ser executados os passos descritos nos pontos seguintes, relativos ao sistema operativo utilizado.

2.3.1 Instalação em Microsoft Windows

1. Executar o pacote de instalação: Após ter descarregado o ficheiro de instalação, deverá fazer duplo clique sobre este, surgindo um ecrã semelhante aos apresentados de seguida:



2. Neste ecrã, deverá premir o botão **Seguinte** e marcar a caixa (com um certo, clicando no botão esquerdo do rato), para aceitar os termos e condições da aplicação.



3. Neste passo, poderá escolher a pasta onde deseja instalar o *middleware*. Se desejar alterar a pasta predefinida, carrege 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 também um ecrã com a opção de **Instalar**, deverá premir esse botão.
5. Após a conclusão deste assistente, este solicitará a reinicialização do computador.

6. No próximo arranque do *Windows* a instalação do *middleware* estará finalizada.

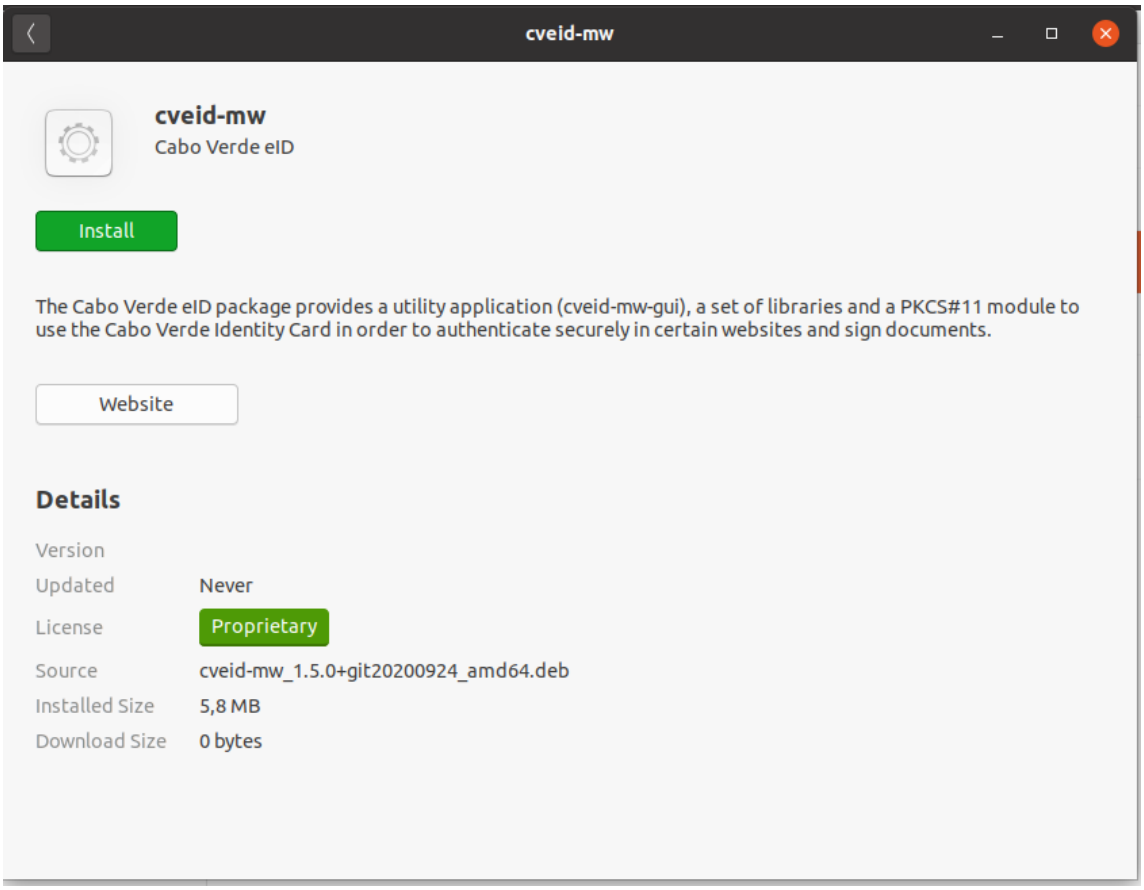
2.3.2 Instalação em Linux

Algumas distribuições de Linux, disponibilizam um gestor de aplicações - "*Ubuntu Software*" - onde é possível instalar o software através de um assistente gráfico. Este ecrã poderá variar consoante a distribuição, neste manual apresenta-se as imagens da utilização do *Ubuntu Software* em Linux Ubuntu 20.04 LTS.

Em alternativa, a aplicação poderá também ser instalada recorrendo à linha de comandos.

2.3.2.1 Instalação através do *Ubuntu Software*

1. Executar o pacote de instalação: Após ter descarregado o ficheiro de instalação, deverá fazer duplo clique sobre este. O sistema deverá apresentar o ecrã de gestão de aplicações - "Ubuntu Software" - para a instalação do software. Este ecrã varia consoante a distribuição que está a utilizar, no entanto, as opções são semelhantes em todos. Nos ecrãs seguintes são apresentados os ecrãs utilizando Linux Ubuntu 20.04 LTS.



2. Deverá premir o botão **Instalar** para prosseguir.
3. Será pedida a introdução da sua senha de utilizador. (É necessário que tenha privilégios de administração da máquina)
4. Após a conclusão do passo acima, a instalação da aplicação está terminada.
5. Recomenda-se a reinicialização do sistema para assegurar o bom funcionamento da aplicação.

2.3.2.2 Instalação através da linha de comandos

1. Execute o comando de instalação de software no sistema, consoante o gestor de pacotes utilizado pelo seu sistema.

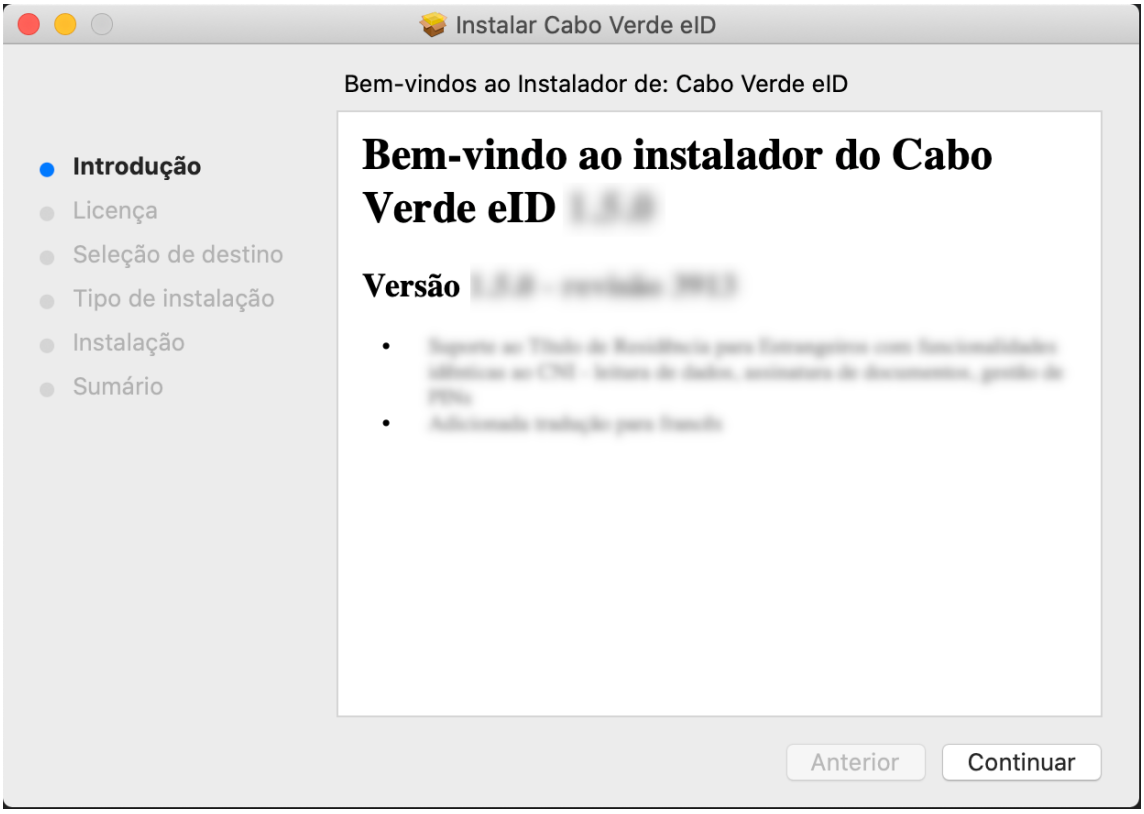
Sistema baseado em pacotes .deb, execute o comando:

```
sudo apt install PACKAGE_NAME
```

2. Após este passo, a aplicação terá sido instalada no computador.
3. Recomenda-se a reinicialização do sistema para assegurar o bom funcionamento da aplicação.

2.3.3 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 "Cabo Verde eID" já estará disponível na pasta Aplicações / *Applications*.

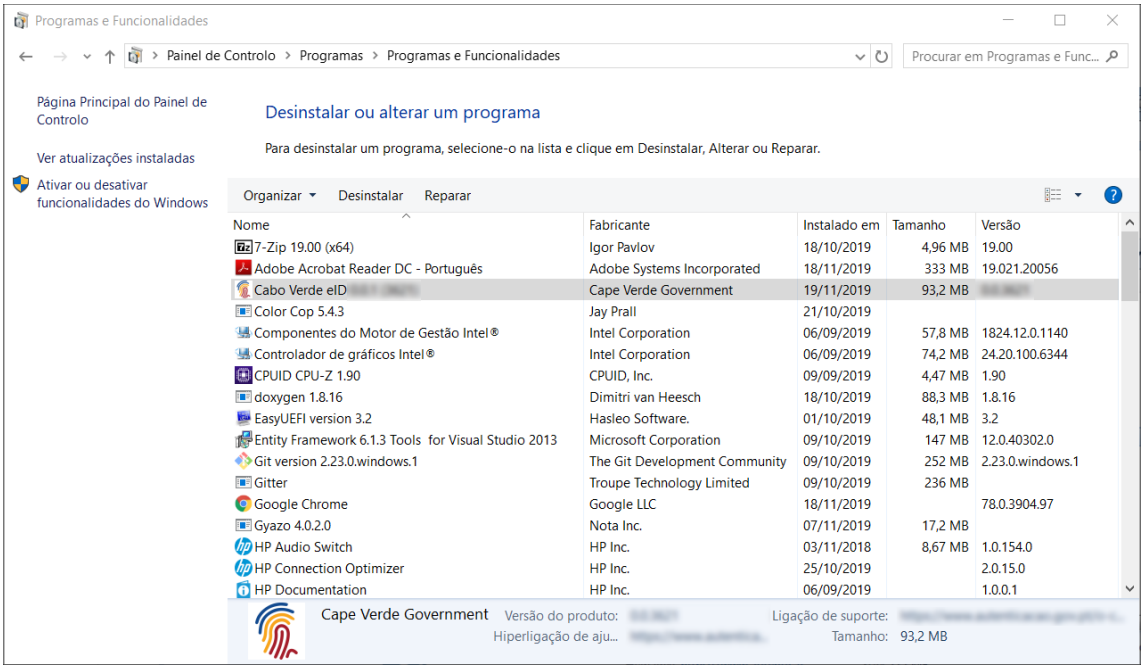
2.4 Remoção do *middleware*

Para proceder à remoção do *middleware* da Identificação Eletrónica em Cabo Verde, deverão ser executados os passos descritos nos pontos seguintes, relativos ao sistema operativo utilizado.

2.4.1 Remoção em Microsoft Windows

2.4.1.1 Através do Painel de Controlo

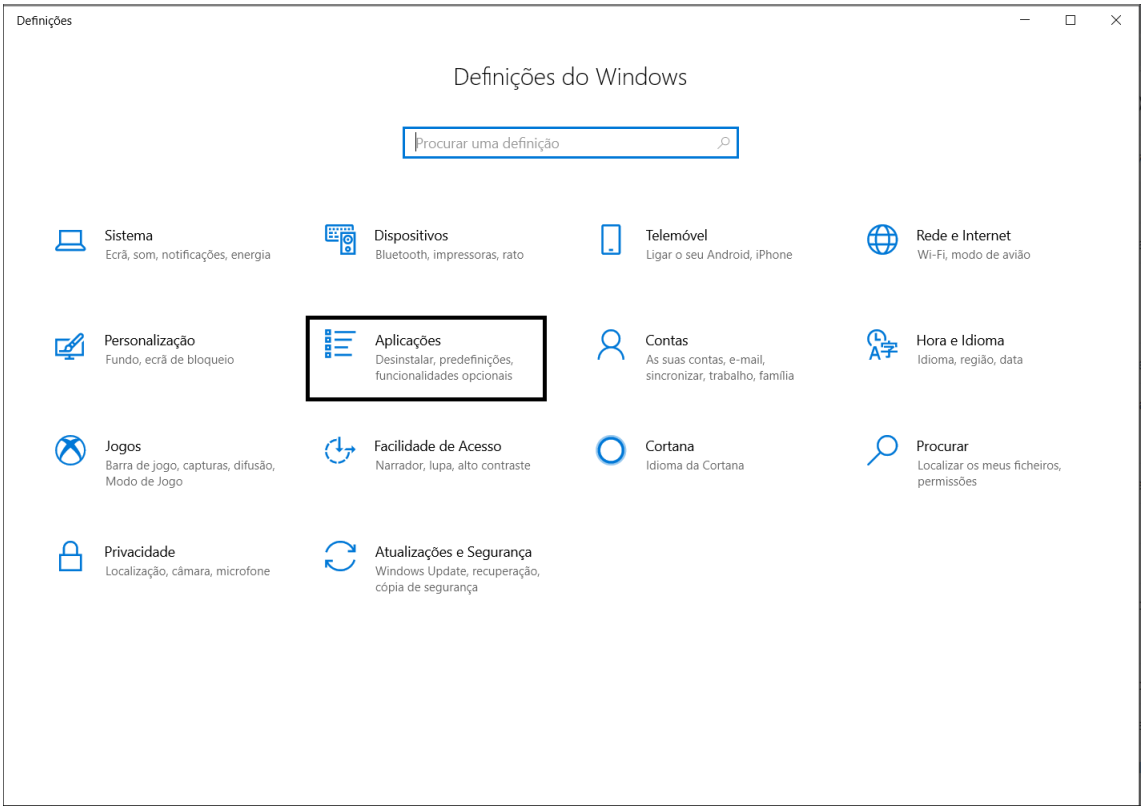
1. Aceda ao **Painel de Controlo**.
2. Selecione a **Opção Adicionar ou Remover Programas**.
3. Selecione o programa **Cabo Verde eID**, conforme apresentado na janela seguinte:



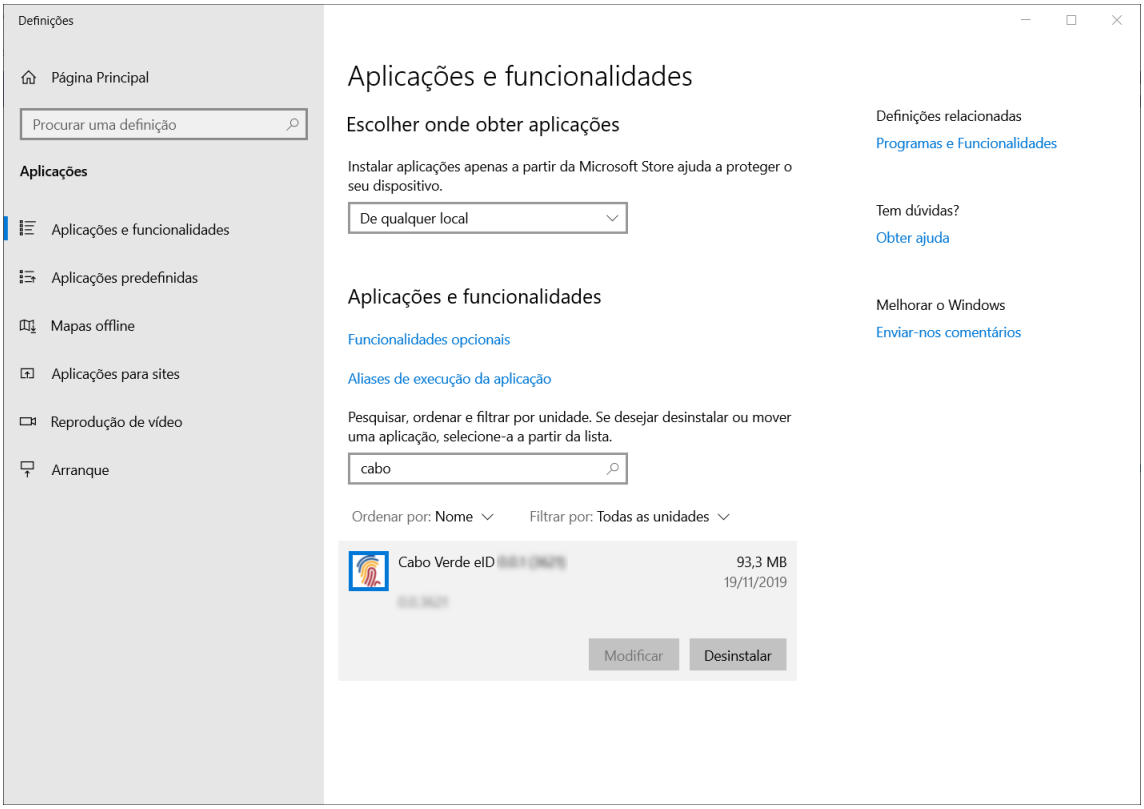
4. Clique em **Desinstalar**. Confirme todas as janelas de diálogo que irão surgir.
5. Após estes passos, o *middleware* estará removido do computador. Recomenda-se que o computador seja reiniciado no final destes passos.

2.4.1.2 Através das Definições do Windows (Windows 10)

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



3. Procure a aplicação **Cabe Verde eID**; 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, o *middleware* estará removido do computador. Recomenda-se que o computador seja reiniciado no final destes passos.

2.4.2 Remoção em Linux

Algumas distribuições de Linux, disponibilizam um gestor de aplicações - "**Ubuntu Software**" - onde é possível remover o software através de um assistente gráfico. Este ecrã poderá variar consoante a distribuição, neste manual apresenta-se as instruções da utilização do *Ubuntu Software* em Linux Ubuntu 20.04 LTS.

Em alternativa, a aplicação poderá também ser removida recorrendo à linha de comandos.

2.4.2.1 Remoção através do *Ubuntu Software* Este ecrã varia consoante a distribuição que está a utilizar, no entanto, as opções são semelhantes em qualquer distribuição.

1. Abra o **Ubuntu Software** (Menu Aplicações → Ubuntu Software).
2. Prima o botão **Instalado** na barra superior.
3. Localize o pacote **cveid-mw** e prima o botão **Remover**.
4. Confirme a operação, voltando a primir o botão **Remover**.
5. Será pedida a introdução da sua senha de utilizador. É necessário que tenha privilégios de administração da máquina.
6. Após a conclusão do passo acima a o processo de desinstalação da aplicação está terminado.

2.4.2.2 Remoção através da linha de comandos

1. Execute o comando de remoção de software no sistema.

   Gestor de pacotes baseado em ficheiros .deb, execute o comando:

   ```
   sudo dpkg -r cveid-mw
   ```

2. Após este passo, a aplicação terá sido removida do computador.

2.4.3 Remoção em MacOS

1. Abra a aplicação "**Terminal**" no MacOS.
2. Execute o seguinte comando para desinstalar todos os ficheiros do *middleware*. Nota: O utilizador que executar este comando terá de ser administrador do Sistema.

```
sudo /usr/local/bin/cvmw_uninstall.sh
```

3 Aplicação Utilitária "Cabo Verde eID"

A aplicação utilitária "Cabo Verde eID" pode ser utilizada para visualizar e gerir os dados no documento de identificação.

Nesta aplicação poderá efetuar as seguintes operações:

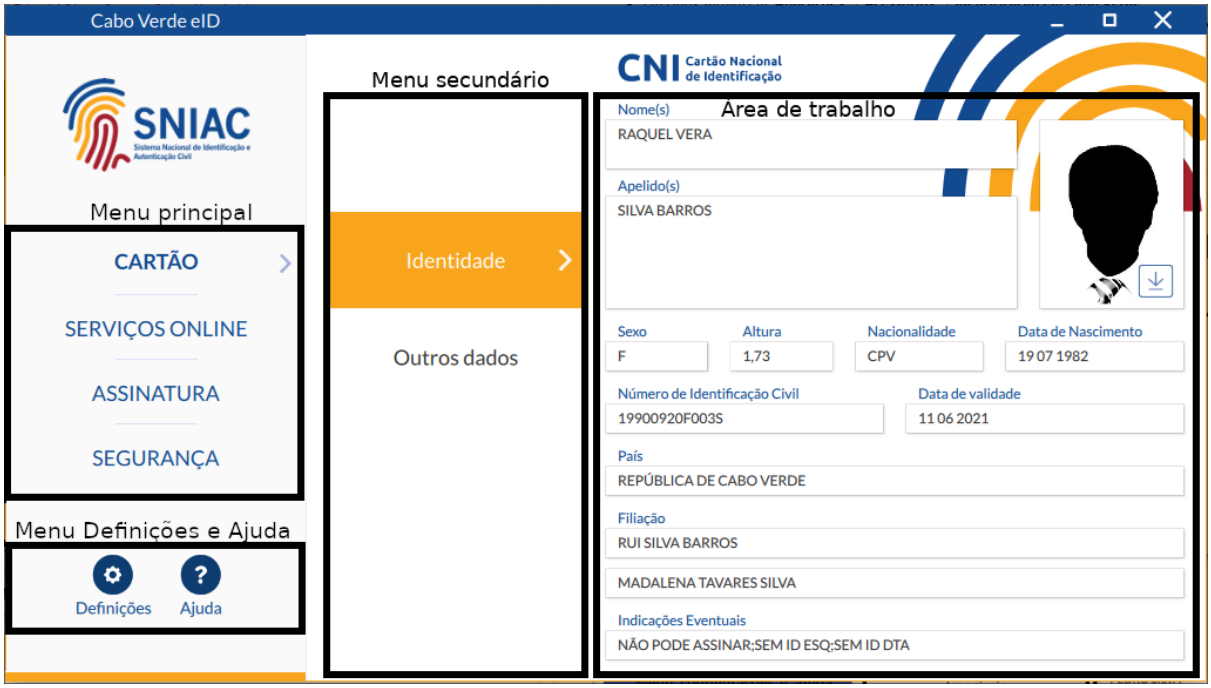
- Visualização da informação, foto do cidadão e residência (exclusivo do Título de Resiência para Estrangeiros(TRE));
- Edição das notas públicas e privadas;
- Registo dos certificados do Estado e do cidadão (específico de Microsoft Windows);
- Desbloqueio e alteração dos códigos PIN associados ao documento de identificação;
- Ativação dos certificados de autenticação e assinatura;
- Assinatura digital de documentos PDF e outros ficheiros;
- Consulta de outros dados do titular do documento de identificação;
- Acesso ao serviço de alteração de morada online.

O atalho para a aplicação fica disponível em: **Iniciar** → **Programas** → **Cabo Verde eID**

3.1 Apresentação da Aplicação

A aplicação é composta por 4 áreas principais de interação:

- **Menu principal:** São disponibilizadas as 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 documento de identificação.

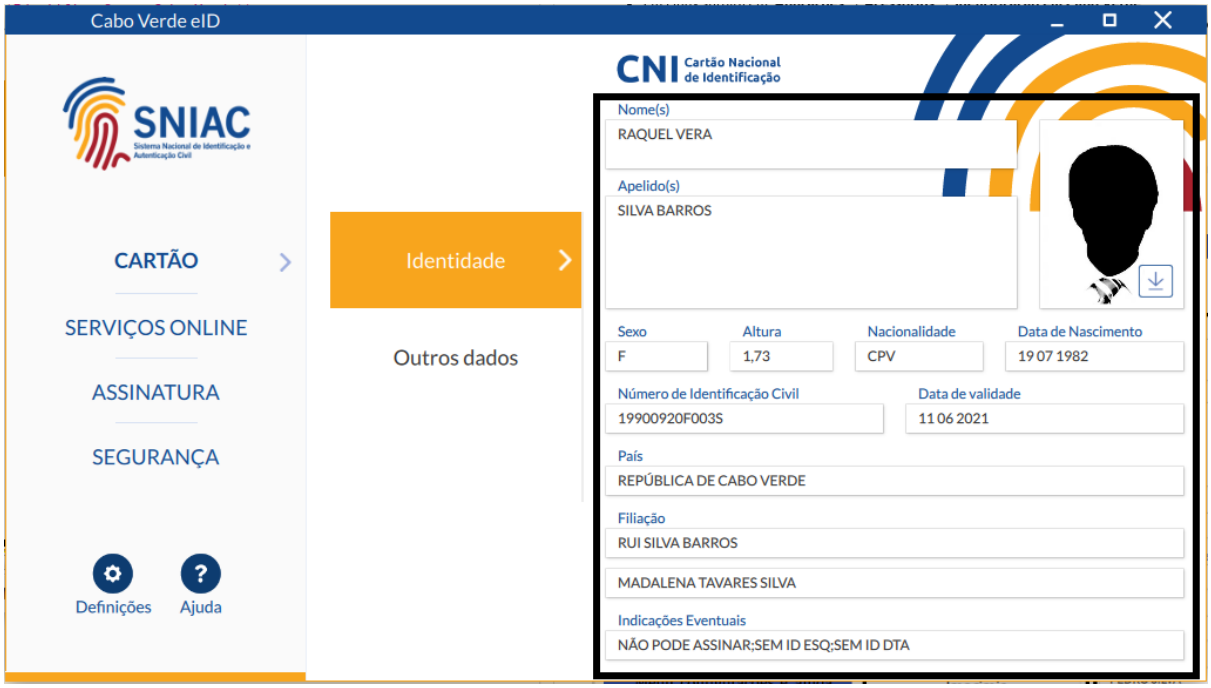


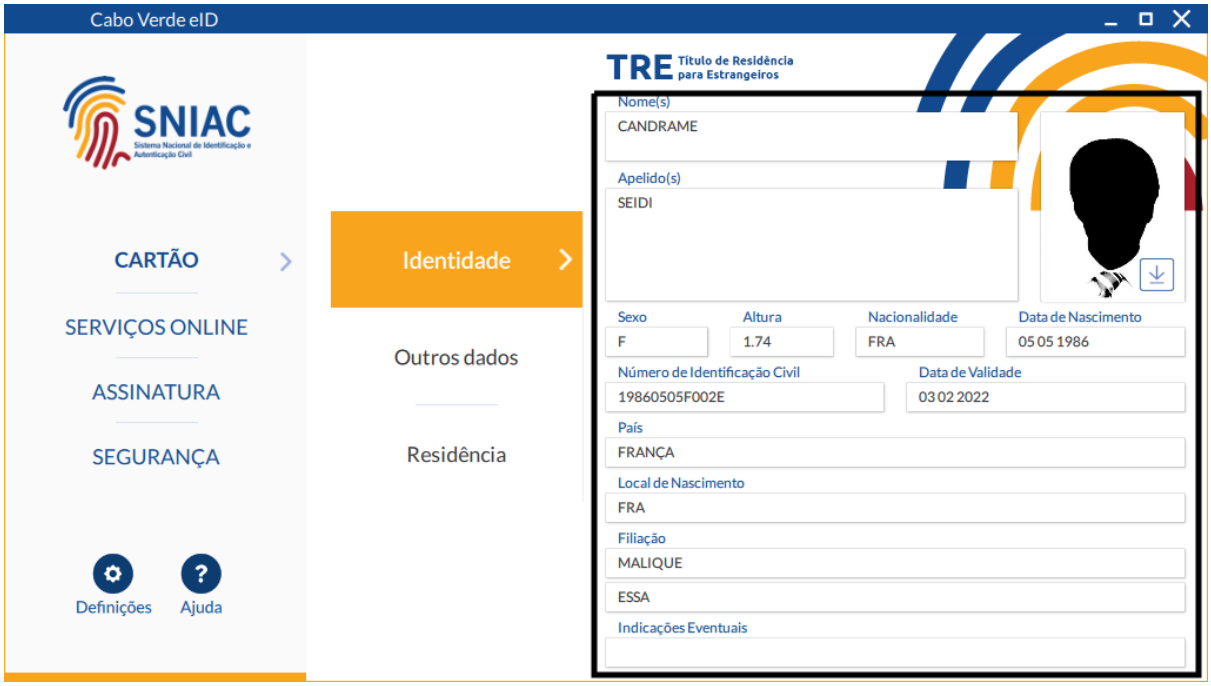
3.2 Funcionalidades da aplicação

3.2.1 Menu Cartão

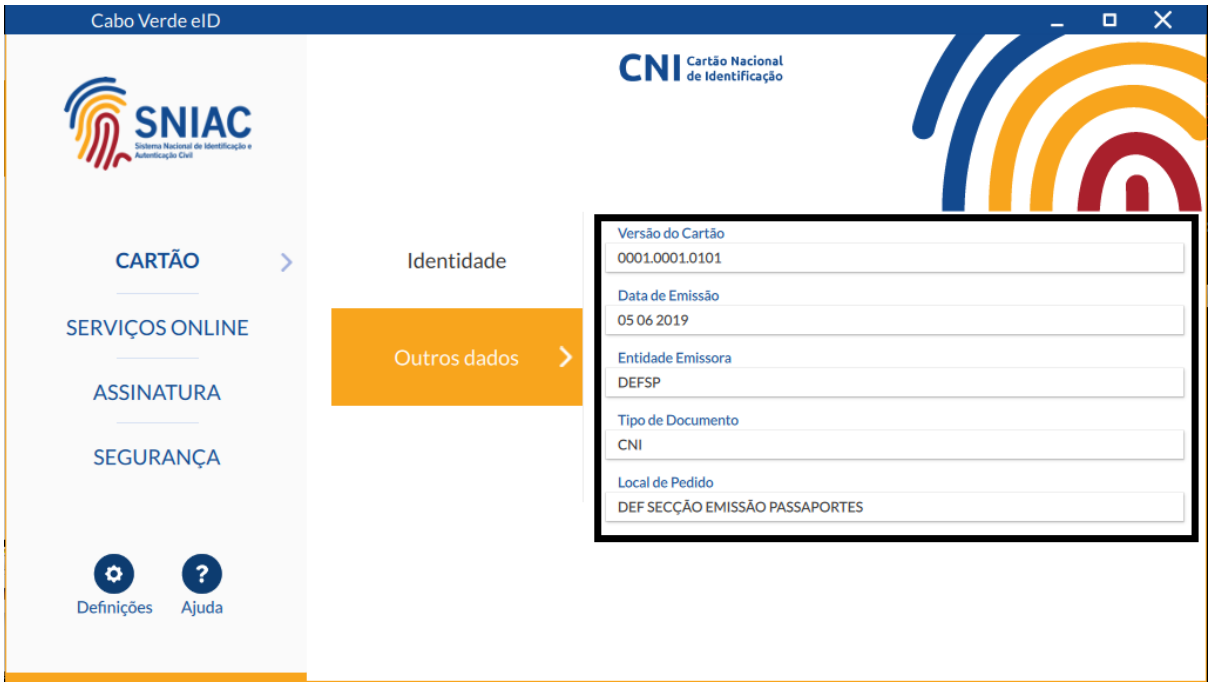
Permite visualizar a informação de identidade, foto do cidadão, residência (exclusivo do Título de Resiência para Estrangeiros(TRE)) e edição das notas. A foto do cidadão pode ser exportada para ficheiro.

3.2.1.1 Identidade Permite visualizar os dados de identificação e foto do cidadão presentes no documento de identificação.

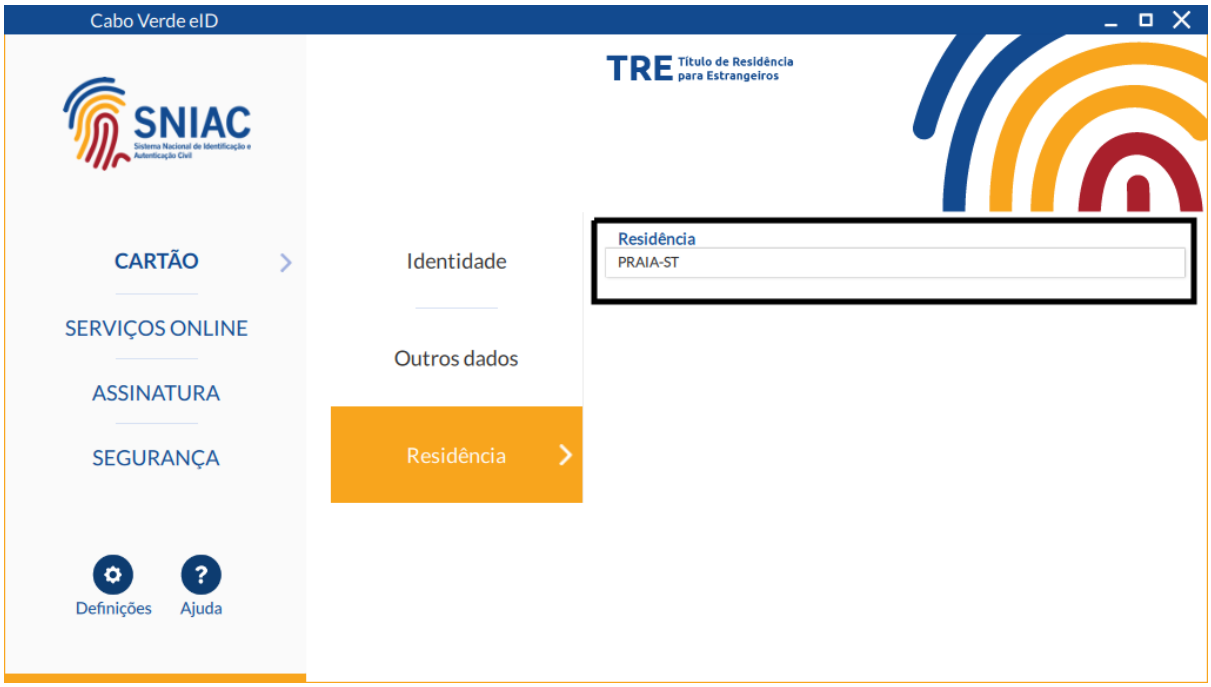




3.2.1.2 Outros dados Permite visualizar outros dados presentes no documento de identificação.



3.2.1.3 Residência Permite visualizar os dados da Residência. Página exclusiva do Título de Resiência para Estrangeiros(TRE)

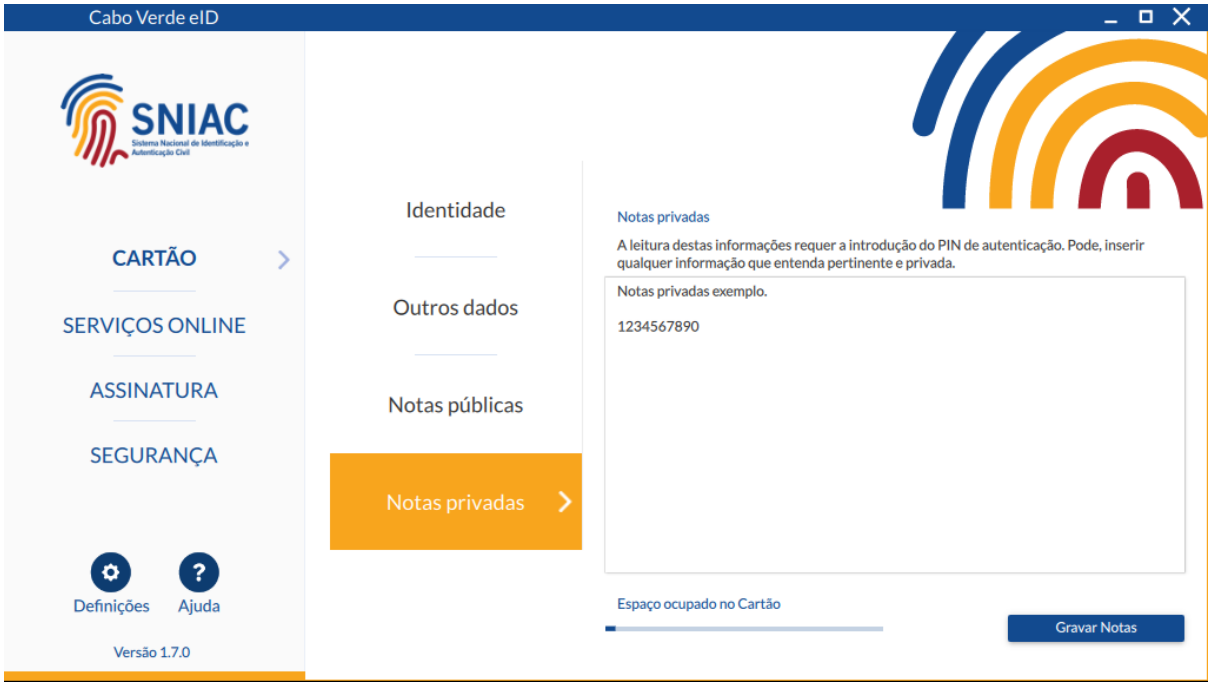


3.2.1.4 Notas públicas A aplicação permite editar as notas públicas gravadas no documento de identificação.

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

3.2.1.5 Notas privadas A aplicação permite editar as notas privadas gravadas no documento de identificação.

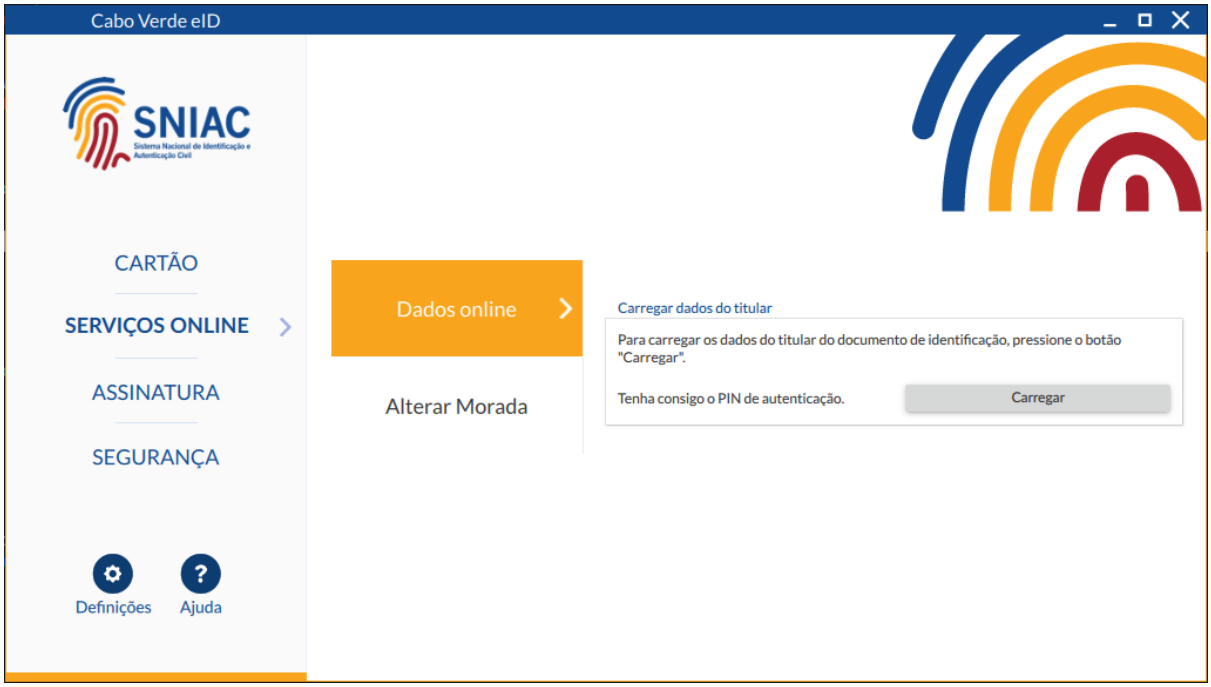
A leitura destas informações requer a introdução do PIN de autenticação. Pode, inserir qualquer informação que entenda pertinente e privada.



3.2.2 Serviços Online

3.2.2.1 Dados Online Permite visualizar outros dados do titular do documento de identificação, que não se encontram no próprio documento.

Para carregar e visualizar os seus dados, deve pressionar o botão "Carregar" e introduzir o código PIN de autenticação quando solicitado.

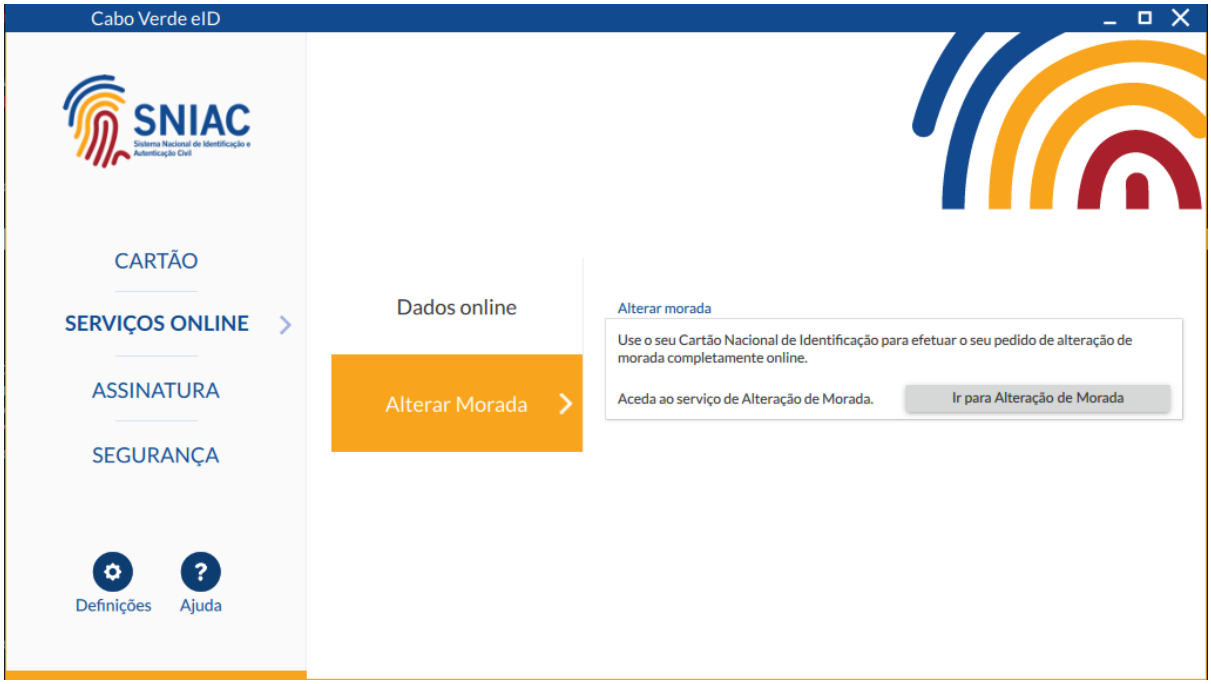


A imagem seguinte é um exemplo ilustrativo da situação de sucesso na operação de carregamento dos dados do titular do documento de identificação. Os campos apresentados podem diferir, consoante os dados disponíveis para cada titular.

No caso de a operação não ter sucesso, verifique o tópico Mensagens de erro na ativação de certificados e leitura dos dados online.

3.2.2.2 Alterar Morada Pode utilizar o seu Cartão Nacional de Identificação para efectuar o seu pedido de alteração de morada, completamente online. Para o fazer, carregue no botão "Ir para Alteração de Morada".

Será direcionado para a página com o serviço de alteração de morada online, no seu navegador web predefinido (por exemplo, Google Chrome, Mozilla Firefox, Safari ou outro).



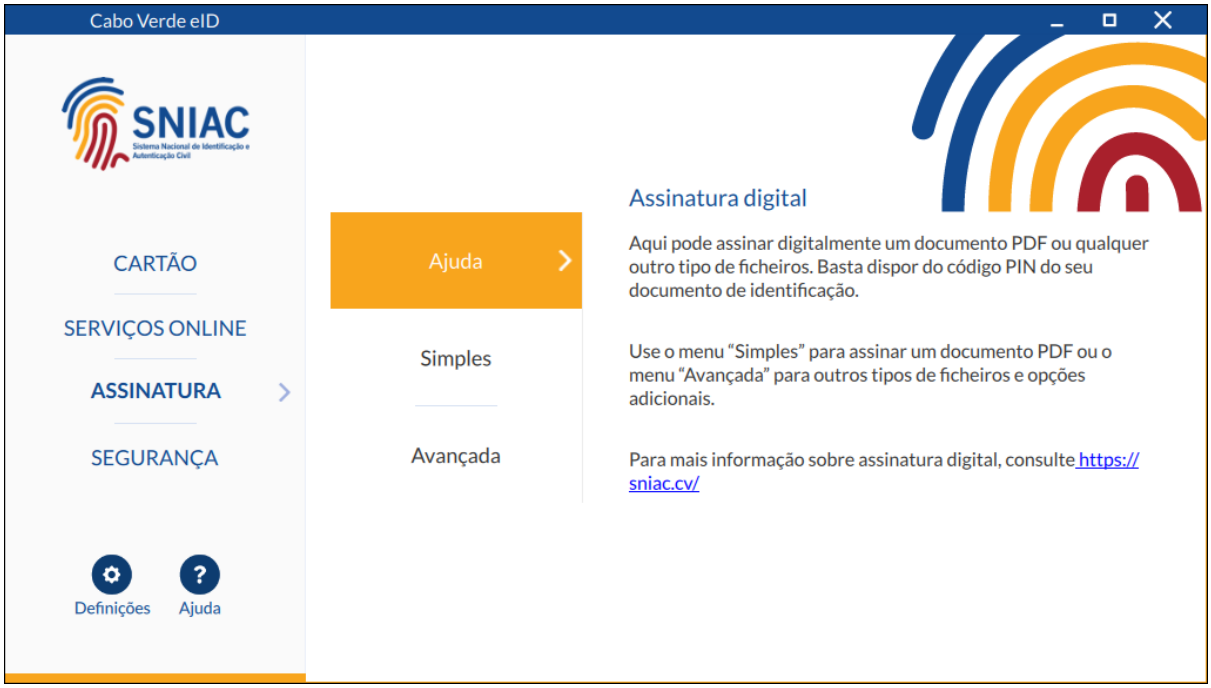
3.2.3 Assinatura digital

A aplicação permite assinar digitalmente, de forma nativa, ficheiros PDF. A assinatura digital em documentos PDF foi desenvolvida de acordo com a especificação da Adobe, podendo assim ser validada posteriormente no software *Adobe Reader*.

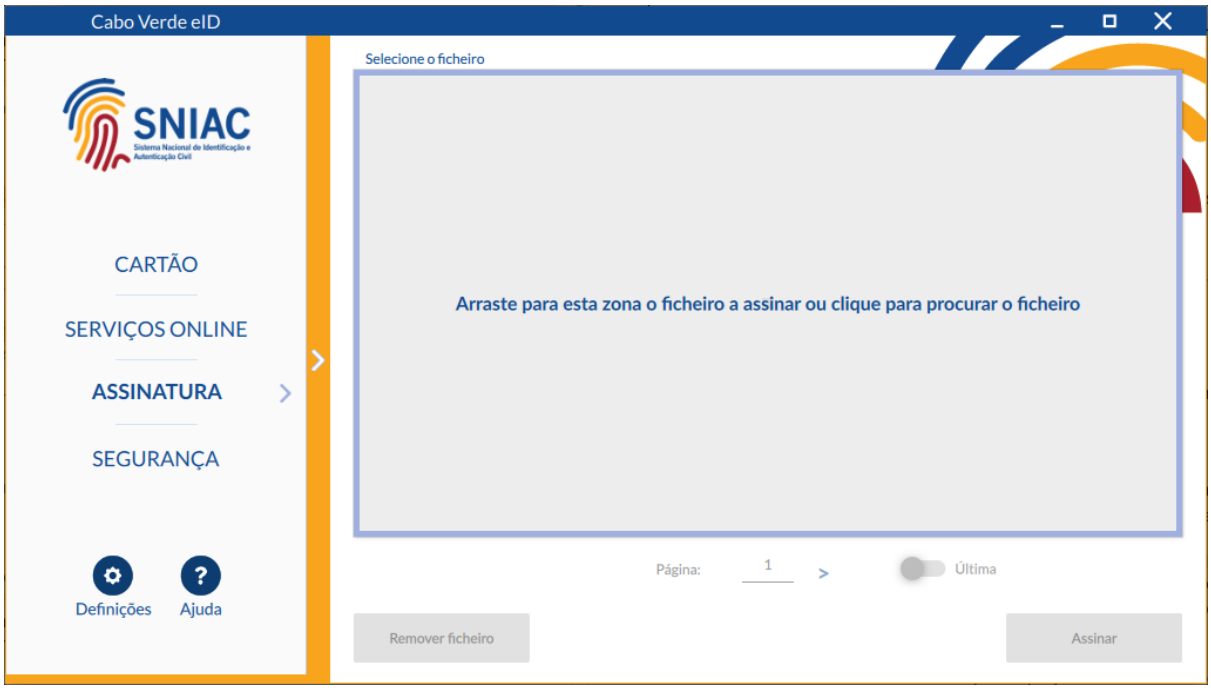
A assinatura digital permite ao titular de um documento de identificação, por vontade própria, assinar com a chave pessoal existente no seu documento de identificação. É possível assinar usando dois modos diferentes:

Assinatura Simples: Assinatura digital de um documento PDF.

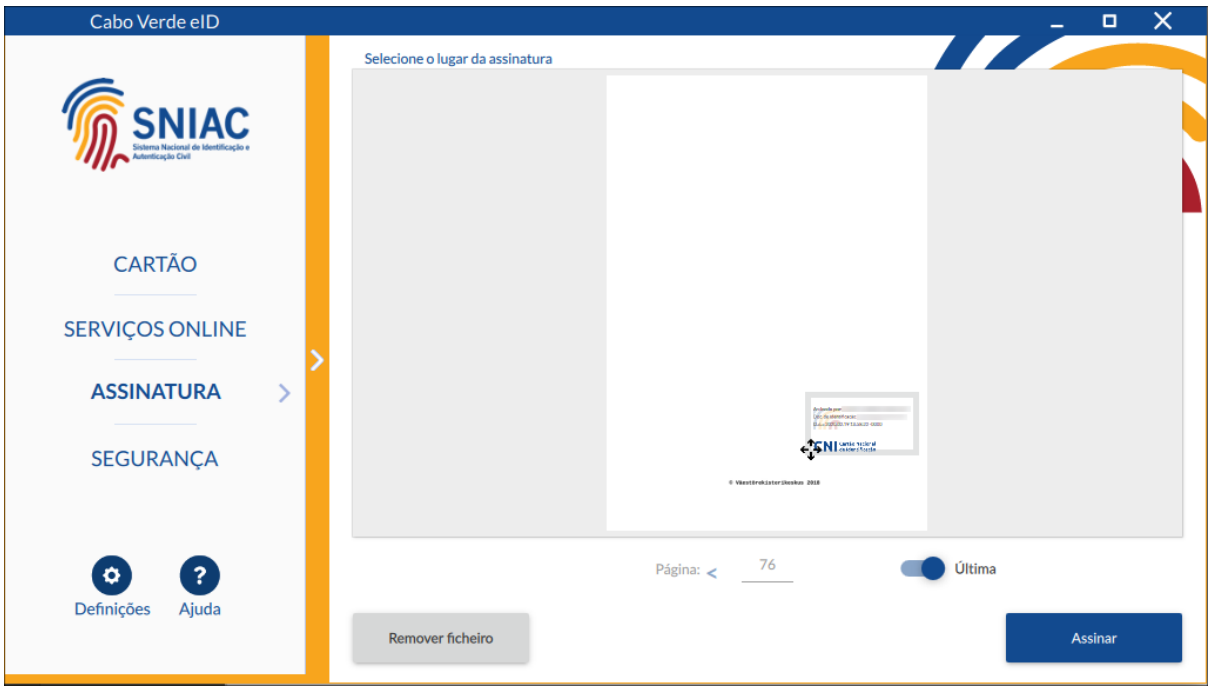
Assinatura Avançada: Assinatura digital de um documento PDF ou outro qualquer documento com possibilidade de assinar vários documentos ao mesmo tempo, bem como configurar outras opções.



3.2.3.1 Simples Assinatura digital simples de um único documento PDF. O ficheiro a assinar pode ser selecionado arrastando-o para a área de pré-visualização ou utilizando a combinação de teclas **CTRL+V**. Pode também clicar na área de pré-visualização ou no botão **Adicionar ficheiro** e selecionar manualmente o ficheiro. Será exibida uma janela para selecionar o ficheiro que pretende assinar.



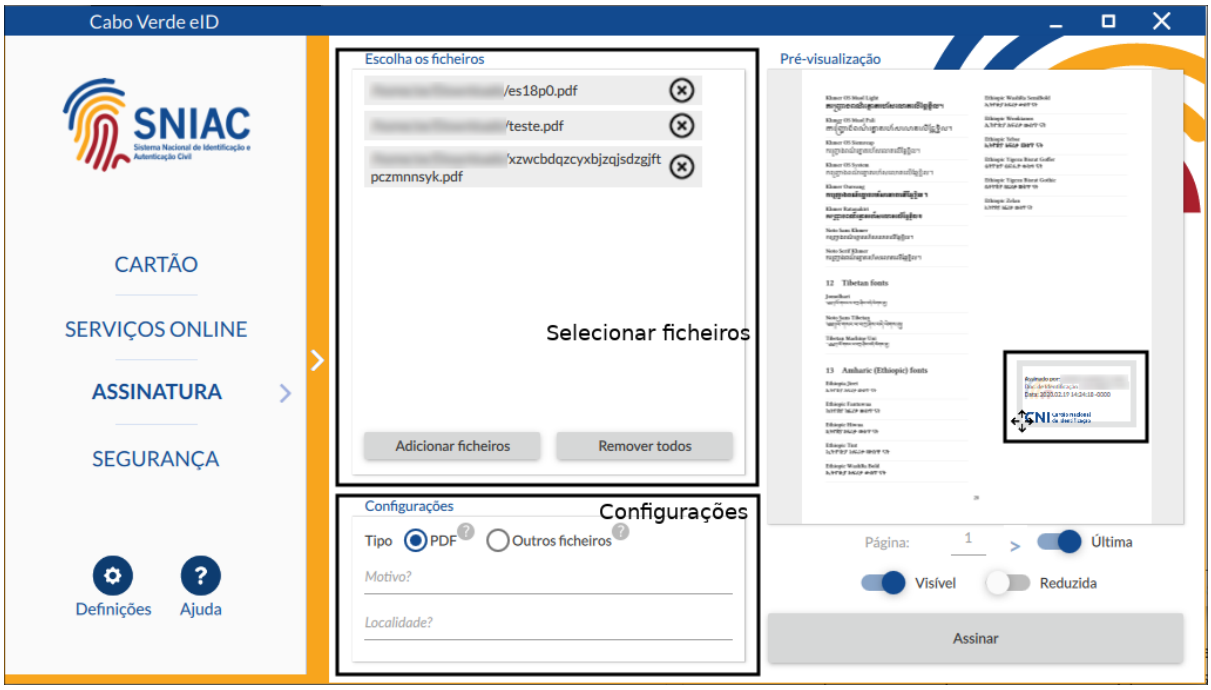
Neste modo, assinatura simples, apenas é possível selecionar a página e mover a assinatura digital para o local pretendido, conforme a figura seguinte.



Por fim, carregar no botão **Assinar**.

3.2.3.2 Avançada Assinatura digital de um documento PDF ou outro qualquer documento com possibilidade de assinar vários documentos ao mesmo tempo, bem como configurar outras opções.

Os ficheiros a assinar podem ser selecionados arrastando-os para a área de pré-visualização ou utilizando a combinação de teclas **CTRL+V**. 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 janela "Escolha os ficheiros", como podemos visualizar na imagem seguinte.



- **Adicionar ficheiros:** Abre uma nova janela que permitirá selecionar os documentos a serem assinados. É possível adicionar e remover ficheiros individualmente ou todos.
- **Pré-visualização da assinatura:** Permite visualizar o documento a ser assinado, bem como a pré-visualização da própria assinatura. A pré-visualização existe apenas para assinatura do tipo **PDF**.
- **Configurações:** Neste modo, é possível selecionar um conjunto de opções e mover a assinatura digital para o local pretendido. Após a seleção dos ficheiros, deverá selecionar as opções da assinatura.

As configurações da assinatura são as seguintes e podem ser visualizadas na imagem anterior:

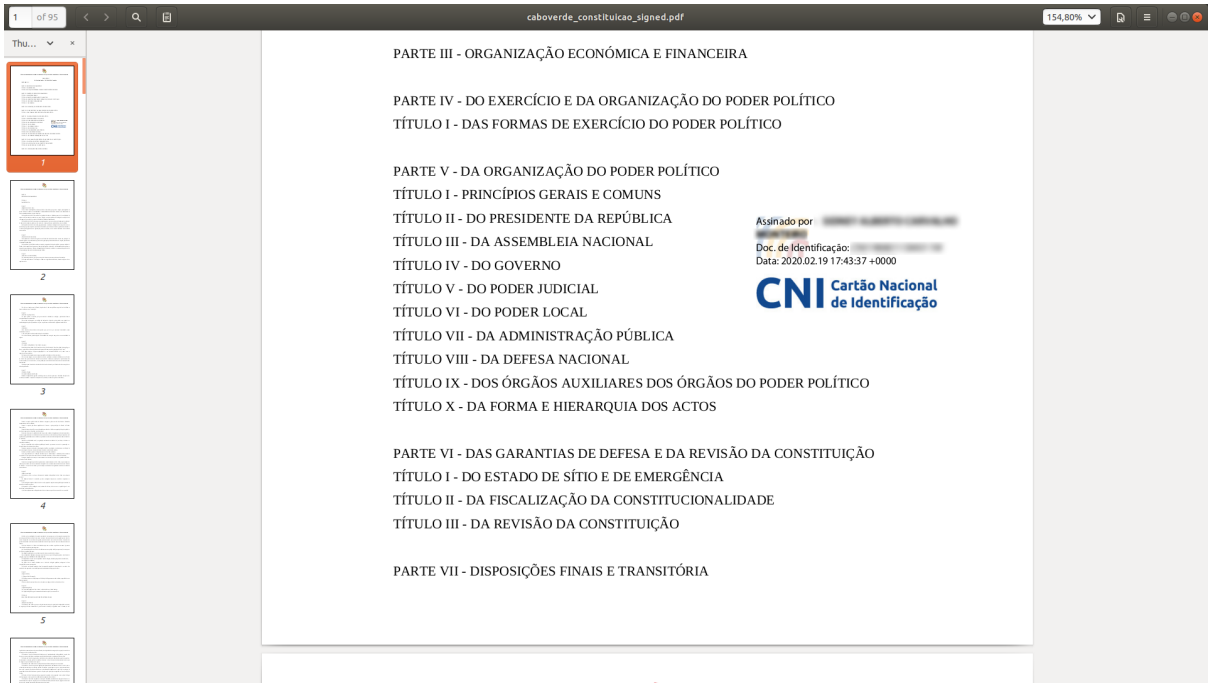
- **Tipo:** Tipo de assinatura – campo obrigatório – permite selecionar assinatura de ficheiros:
  - **PDF:** PAdES (*PDF Advanced Electronic Signatures*).
  - **Outros ficheiros:** Pacote ASiC com *XML Advanced Electronic Signatures* (XadES).
- **Motivo:** Motivo da assinatura – campo opcional – permite 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**.

Após selecionar as opções pretendidas, na área indicada na figura anterior, arraste a pré-visualização da assinatura para a localização pretendida e de seguida prima o botão **Assinar**.

O botão **Assinar** só está disponível quando o documento de identificação estiver inserido no leitor de cartões e for correctamente lido pela aplicação.

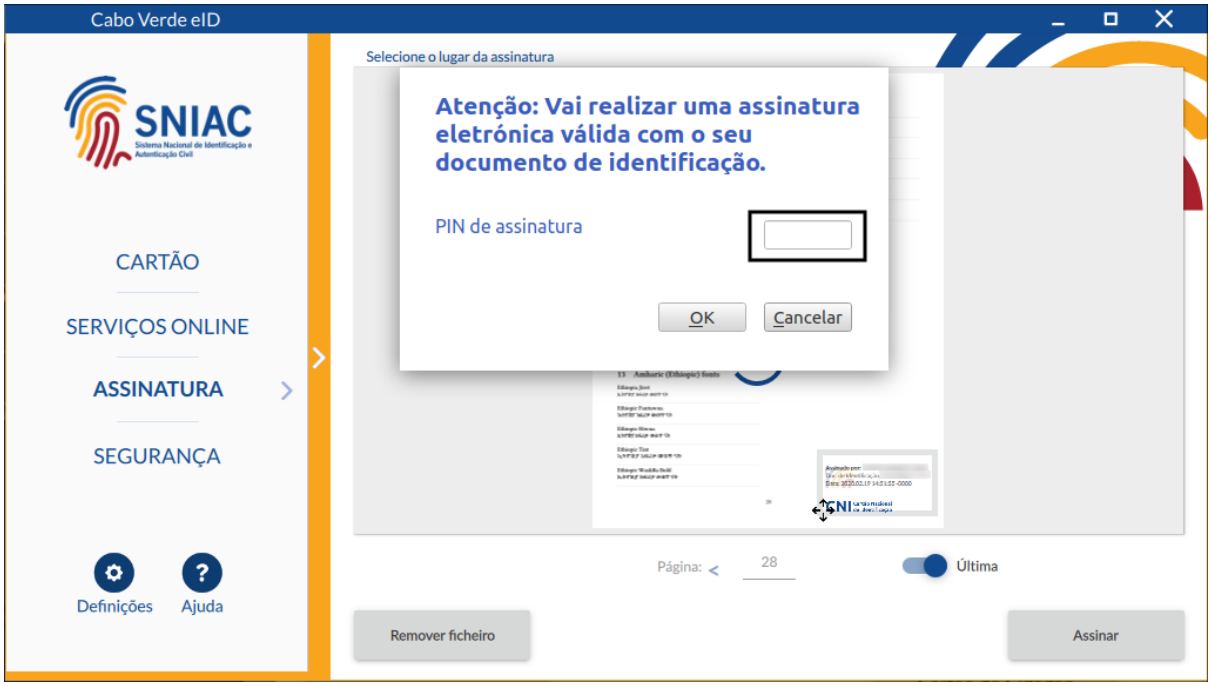
Após clicar em **Assinar** deverá escolher a localização da pasta e do ficheiro onde guardar o ficheiro assinado e seguir o procedimento de assinatura (ver secção Introdução de chave). Em seguida é apresentado uma mensagem a indicar se a assinatura digital foi efetuada com sucesso.

A imagem seguinte é um exemplo de um ficheiro assinado com a aplicação **Cabo Verde eID**.



3.2.3.3 Introdução de chave A assinatura digital permite ao titular de um documento de identificação, por vontade própria, assinar com a chave pessoal existente no seu documento de identificação.

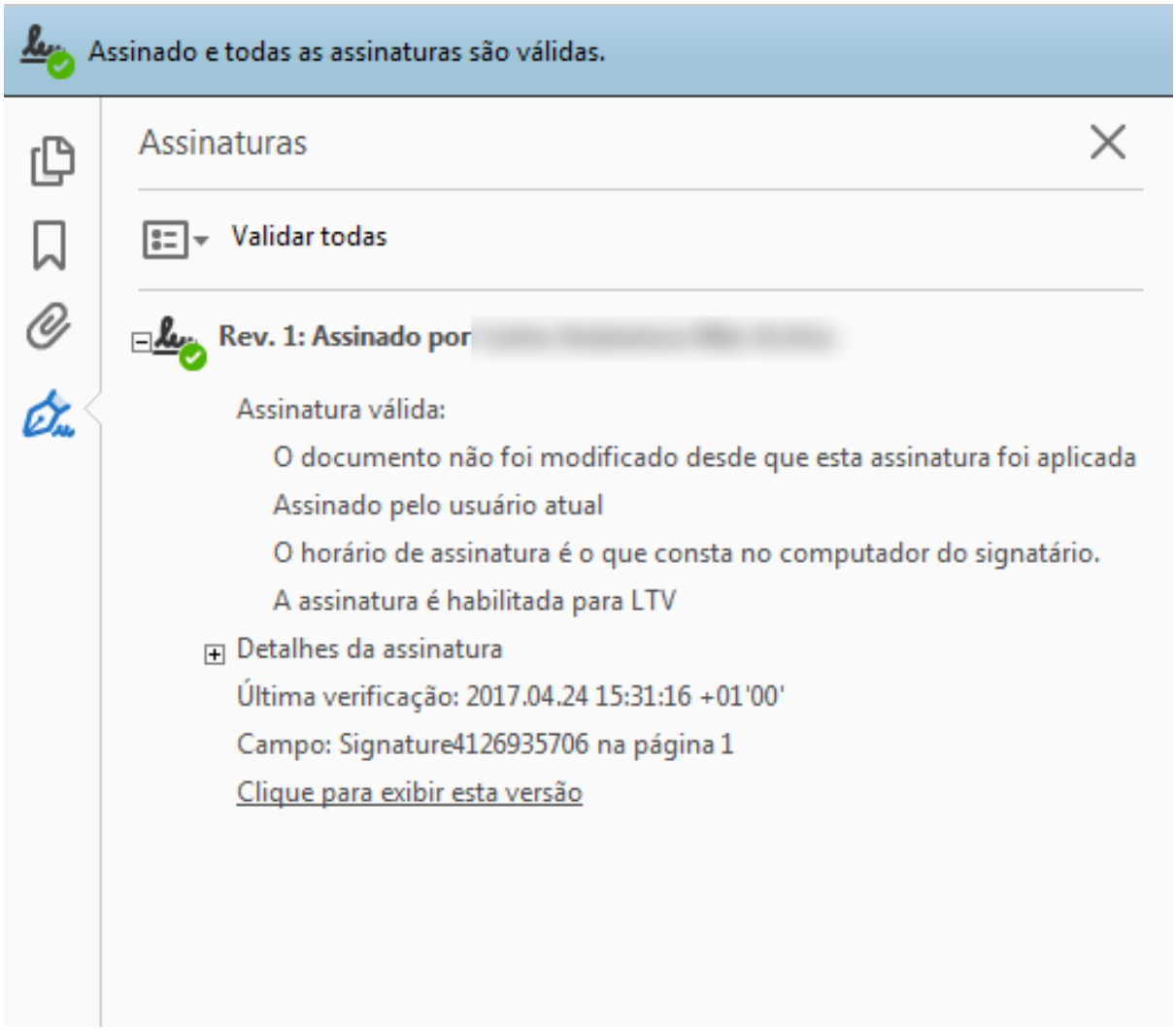
No caso de pretender assinar com a chave pessoal existente no seu documento de identificação, ao selecionar a opção **Assinar**, deverá introduzir o PIN de assinatura, conforme a figura seguinte.



3.2.3.4 Verificação de assinatura digital em documento PDF em Windows no *Adobe Reader*

Após aplicar uma assinatura digital num documento, esta deverá ser identificada automaticamente ao abrir o documento em *Adobe Reader*.

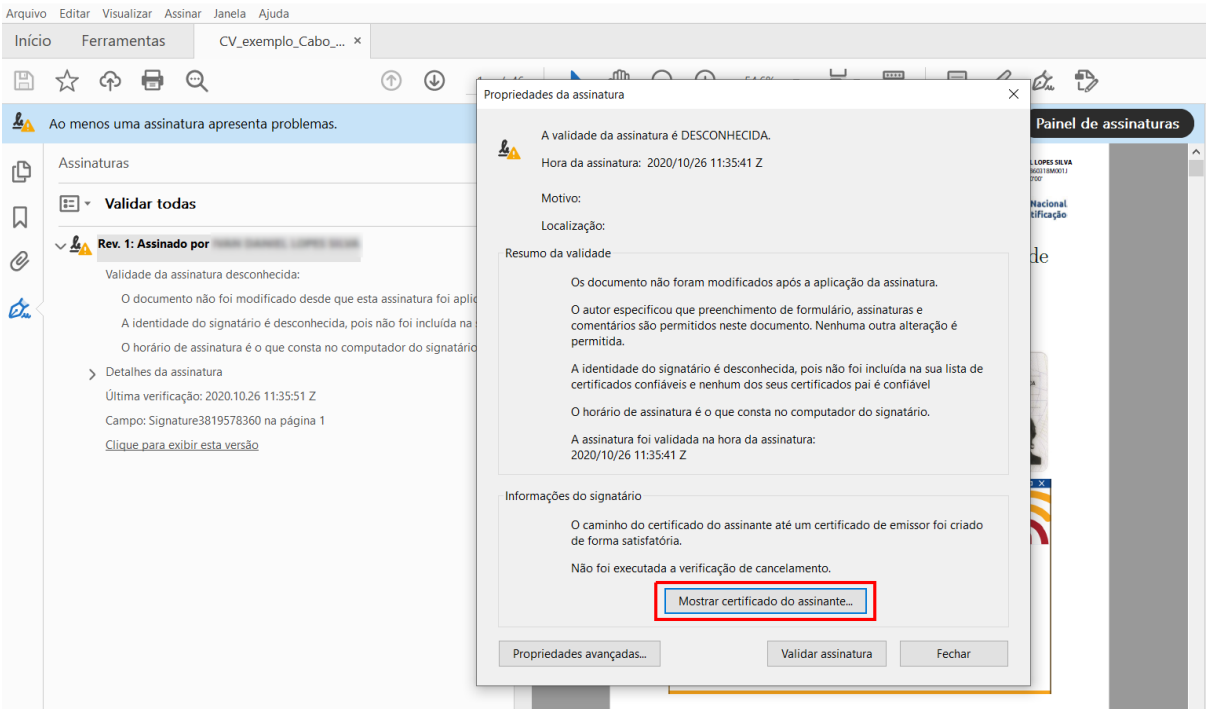
Mesmo quando a assinatura não esteja visível (se a opção **Visível** não for selecionada no momento da assinatura), a assinatura deverá ser sempre validada no painel de assinaturas, dado que permite a visualização do estado da assinatura tendo em conta a cadeia de confiança e as propriedades criptográficas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



Se a assinatura não for considerada válida pelo *Adobe Reader*, poderá ser porque o certificado Raiz de Cabo Verde ainda não é considerado confiável pelo *Adobe Reader*. Adicionar o certificado raiz de Cabo Verde à store do *Adobe Reader*.

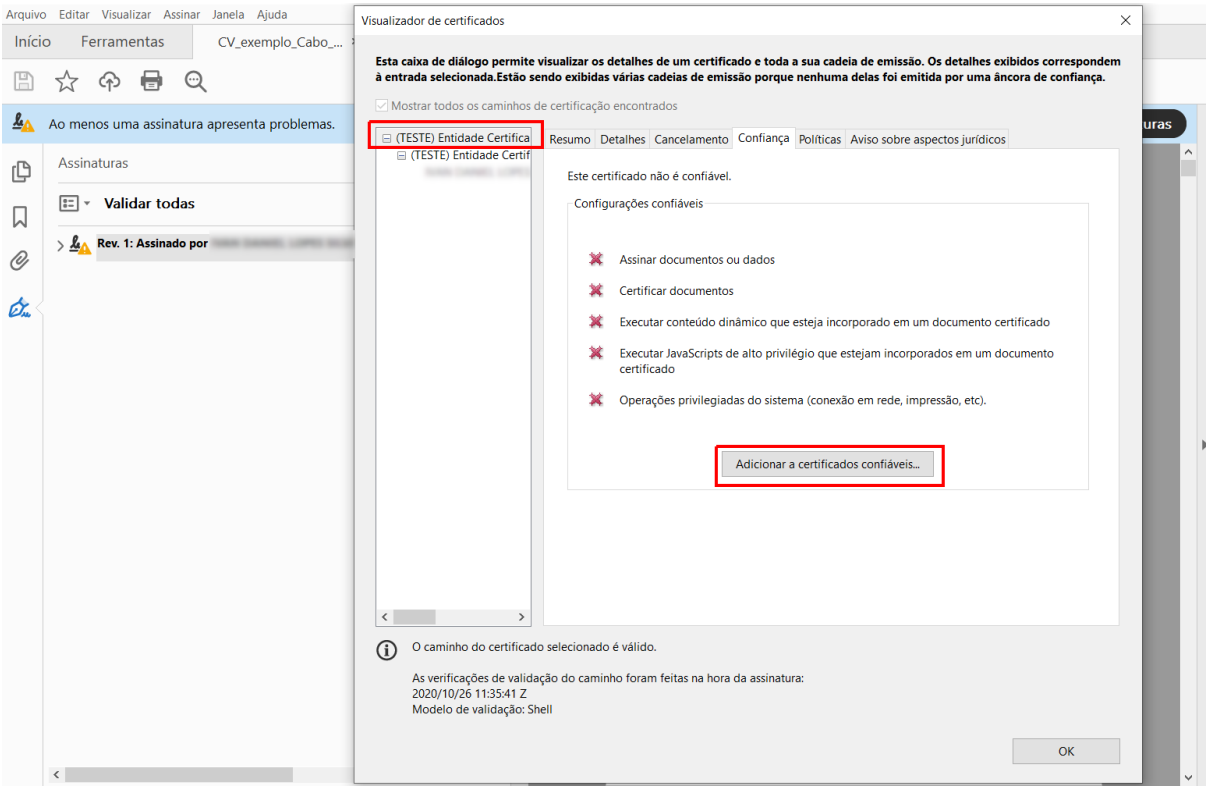
3.2.3.5 Adicionar o certificado raiz de Cabo Verde à store do *Adobe Reader* Para as assinaturas serem consideradas válidas no *Adobe Reader* o certificado da Entidade de Certificação Raiz de Cabo Verde pode ser adicionado à store do *Adobe Reader*. Isto pode ser efectuado seguindo os seguintes passos:

1. Fazer o clique na etiqueta de alerta da assinatura com o botão direito do rato e ir em "Mostrar propriedade da assinatura" e em seguida “Mostrar certificado do assinante”.



2. Na janela "Visualizador de certificados", seleccionar a entrada "Entidade de Certificação Raiz de Cabo Verde 001", na lista do lado esquerdo. Nessa mesma janela no separador "Detalhes" poderá ler os detalhes do certificado e verificar que está a selecionar o certificado correcto. Se pretender garantir que está a adicionar o certificado correcto, verifique se é o mesmo certificado raiz disponível em https://ecrcv.cv/.

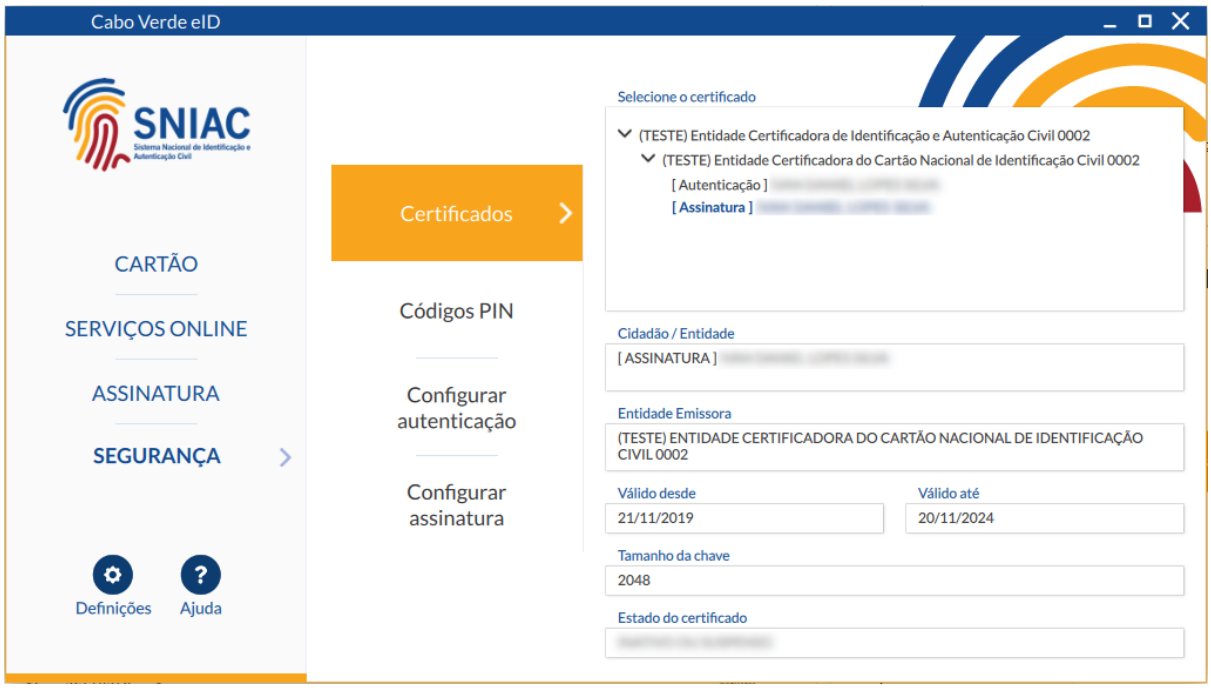
3. Ainda na janela "Visualizador de certificados", no separador "Confiança" ao clicar em "Adicionar a certificados confiáveis" vai adicionar o certificado selecionado à store do *Adobe Reader*. Seguindo o processo até o fim, a verificação da assinatura deverá passar a válida.



3.2.4 Segurança

A aplicação permite efetuar operações relativas à segurança do documento de identificação.

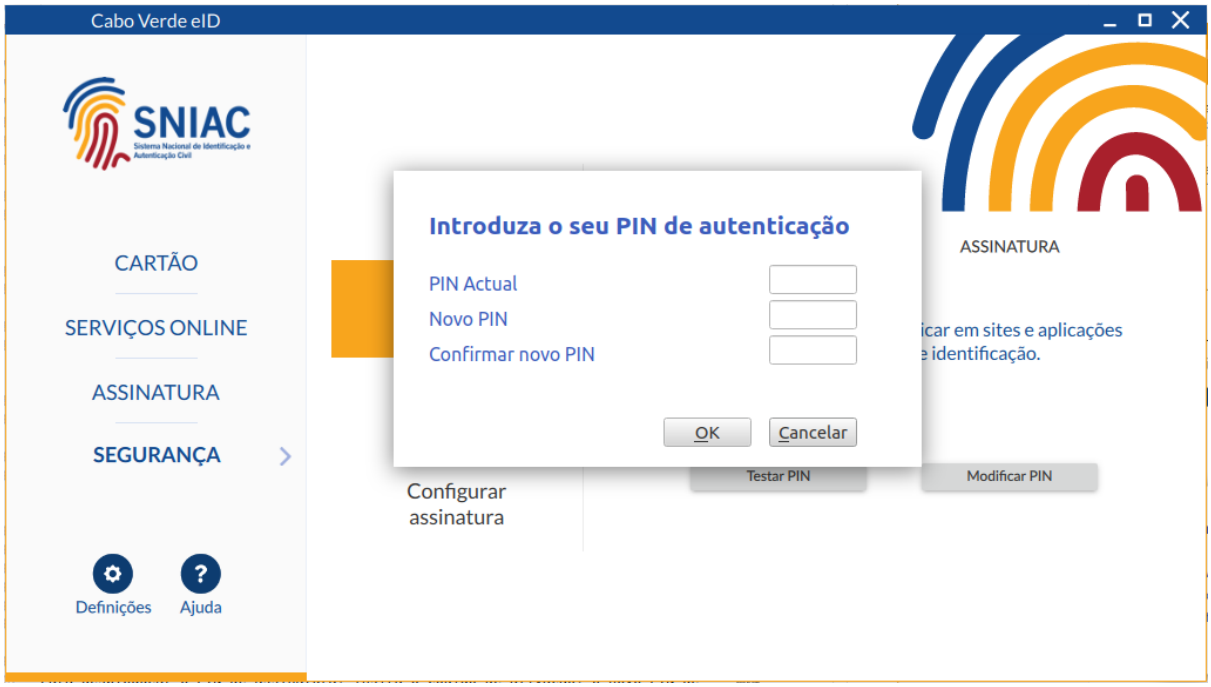
3.2.4.1 Certificados Neste menu é possível verificar os certificados do cidadão e a cadeia de confiança formada pelas várias Entidades de Certificação do documento de identificação. O preenchimento do campo "Estado do certificado" exige ligação à Internet.



3.2.4.2 Código PIN Neste menu é possível verificar e alterar os códigos PIN do documento de identificação.

- **PIN de Autenticação:** Este PIN é usado para se autenticar em sites e aplicações que suportem os documentos de identificação.
- **PIN de Assinatura:** Este PIN é usado para assinar documentos ou transações em aplicações que suportem os documentos de identificação.

Para alterar o PIN de Autenticação ou de Assinatura, verifique que se encontra no separador pretendido, *Autenticação* ou *Assinatura*, e clique no botão **Modificar PIN**. Uma janela será aberta para fornecer o PIN atual e o novo PIN.



3.2.4.3 Configurar autenticação Nesta janela é possível desbloquear o PIN de autenticação, fazendo uso do Código de desbloqueio do PIN de autenticação, e ativar o certificado de autenticação.

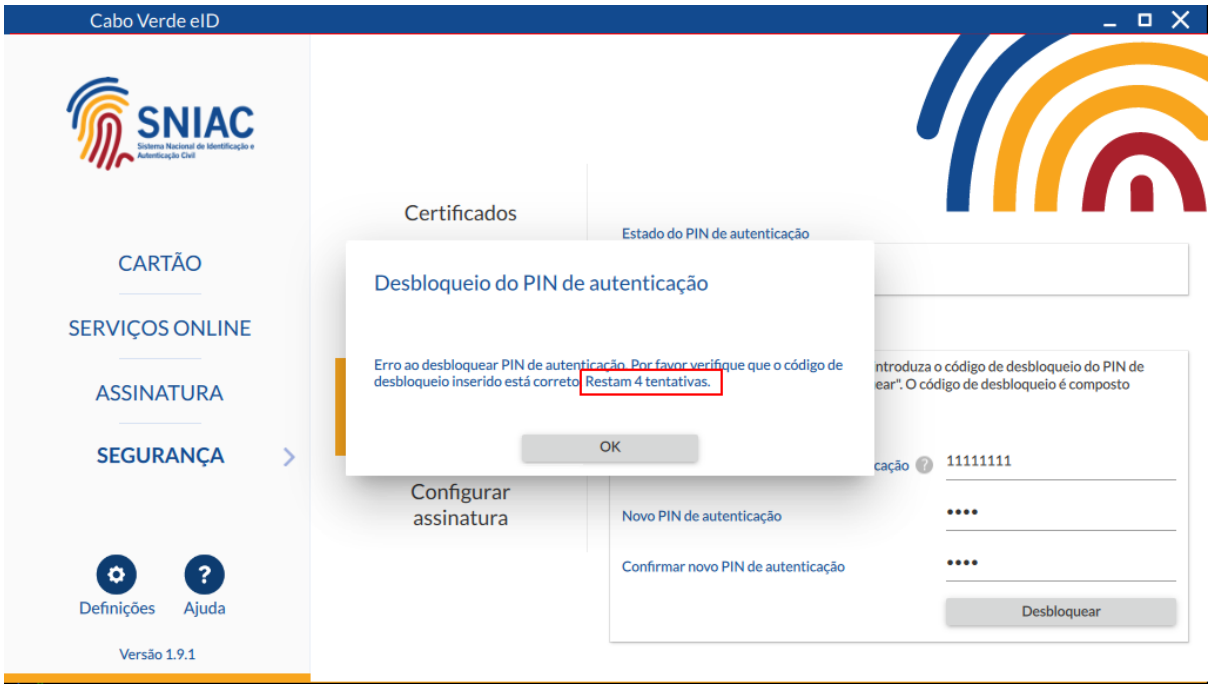
Para desbloquear o PIN de autenticação, insira o código de desbloqueio, o novo PIN de autenticação e a confirmação do novo PIN de autenticação (repetir a introdução do novo PIN), nos campos visíveis, conforme a figura seguinte.

O **Código de desbloqueio do PIN de autenticação** é constituído por 8 dígitos em duas partes de 4 dígitos: A primeira parte vem escrita na sua carta-Pin e a segunda é disponibilizada pelo serviço no momento da entrega da sua carta-Pin. Junte as 2 partes na caixa de texto seleccionada na figura a seguir.

Deve guardar em segurança os seus códigos todos e não partilhar com ninguém.

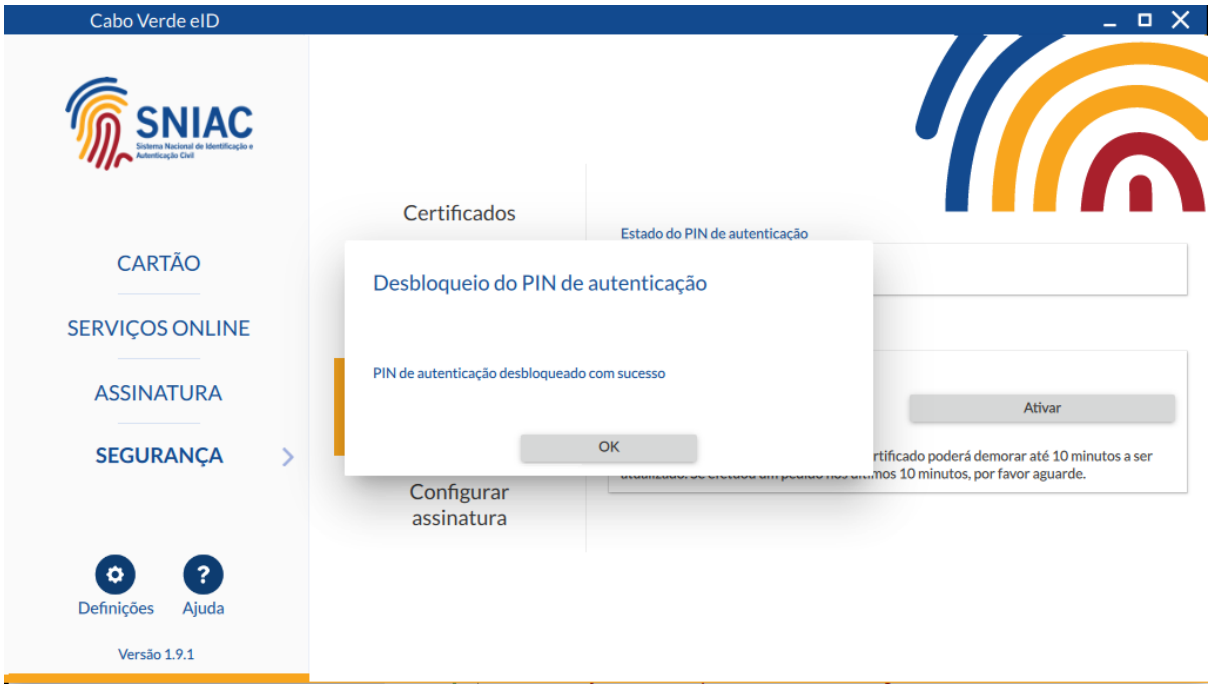
Nesta mesma janela e como podemos ver na figura a seguir, é também apresentado o número de tentativas restantes do **Código de desbloqueio do PIN de autenticação**. Se usar todas as tentativas sem sucesso o código fica bloqueado, não sendo possível desbloquear.

A imagem seguinte corresponde a uma tentativa de desbloqueio do PIN de autenticação sem sucesso. Neste caso deve verificar se introduziu os códigos correctamente e ter cuidado para não ultrapassar o número de tentativas, caso contrário, vai bloquear o **Código de desbloqueio do PIN de autenticação**, não sendo possível desbloquear.



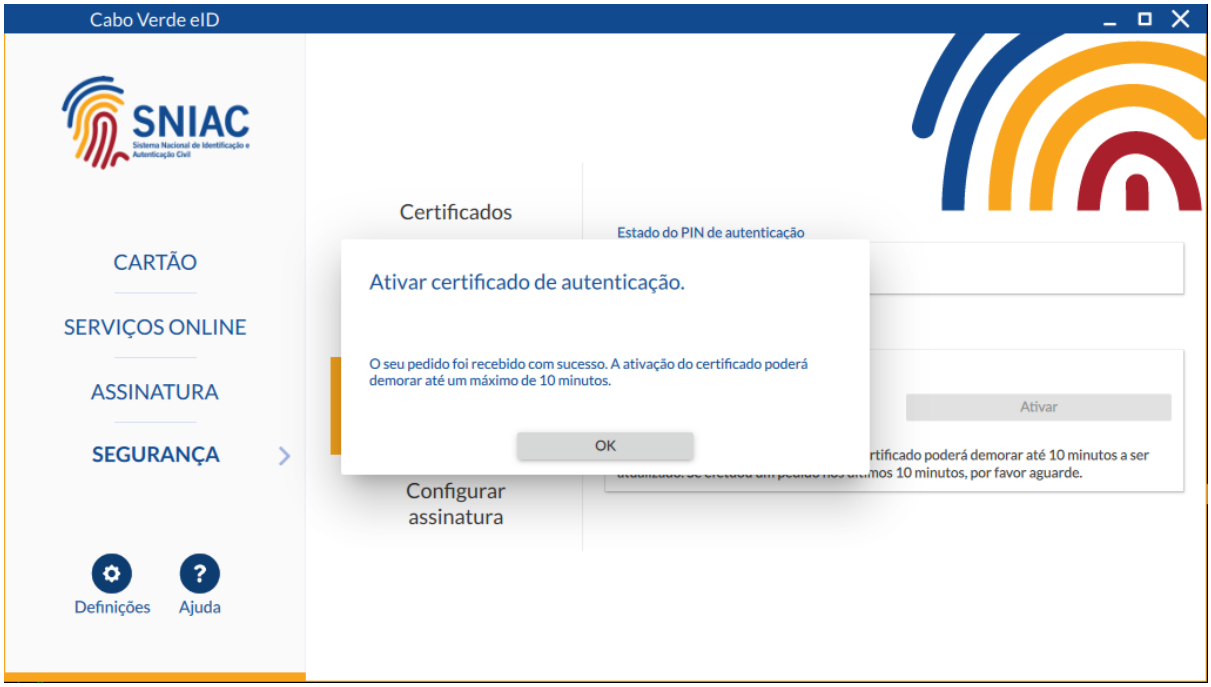
A imagem seguinte corresponde a uma tentativa de desbloqueio do PIN de autenticação sem sucesso e depois de ultrapassar o número de tentativas. Neste caso o **Código de desbloqueio do PIN de autenticação** fica bloqueado, não sendo possível desbloquear.

A imagem seguinte é a janela que indica que o PIN de autenticação foi desbloqueado com sucesso.



Quando o PIN de autenticação está desbloqueado, é possivel verificar o estado do certificado de autenticação. No caso deste se encontrar no estado "INATIVO OU SUSPENSO", pode ativá-lo pressionando o botão "Ativar", conforme a figura seguinte.

O estado do certificado poderá demorar até 10 minutos a ser atualizado. Caso tenha efectuado um pedido de ativação nos últimos 10 minutos, por favor aguarde.
A imagem seguinte ilustra a situação de sucesso na operação de ativação do certificado de autenticação.



No caso de a operação não ter sucesso, verifique o tópico Mensagens de erro na ativação de certificados e leitura dos dados online.

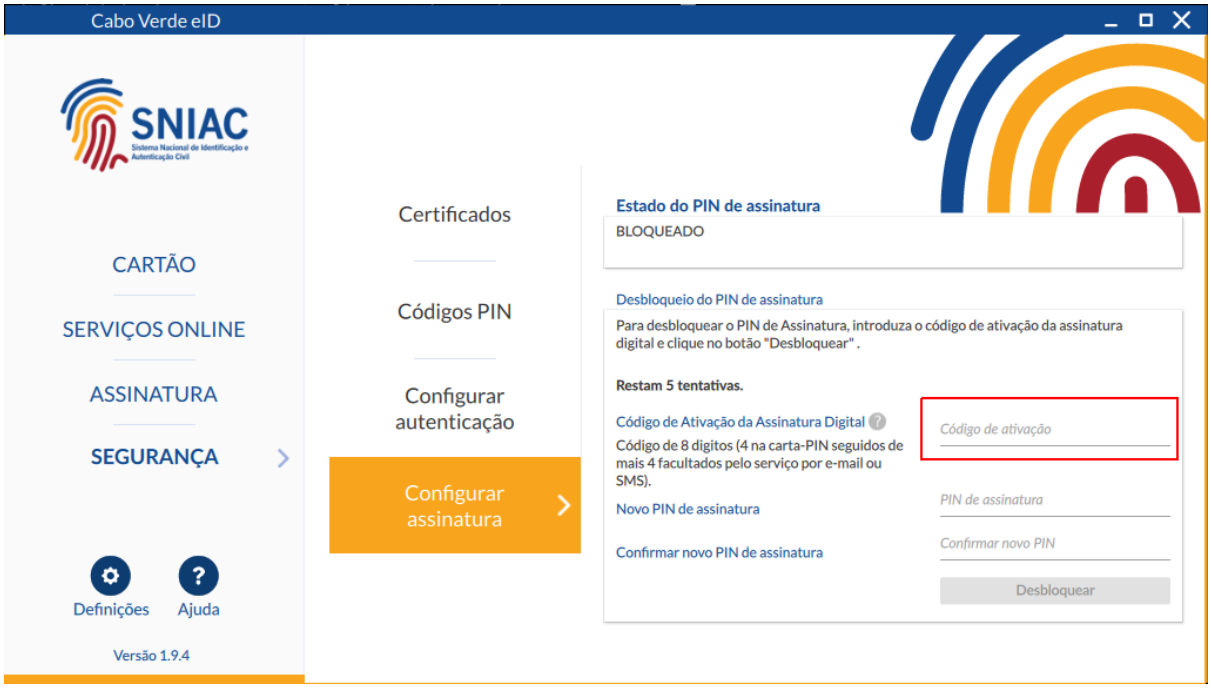
3.2.4.4 Configurar assinatura Nesta janela é possível desbloquear o PIN de assinatura, fazendo uso do Código de Ativação da Assinatura Digital, e ativar o certificado de assinatura.

Para desbloquear o PIN de assinatura, insira o Código de Ativação da Assinatura Digital, o novo PIN de assinatura e a confirmação do novo PIN de assinatura (repetir a introdução do novo PIN), nos campos visíveis, conforme a figura seguinte.

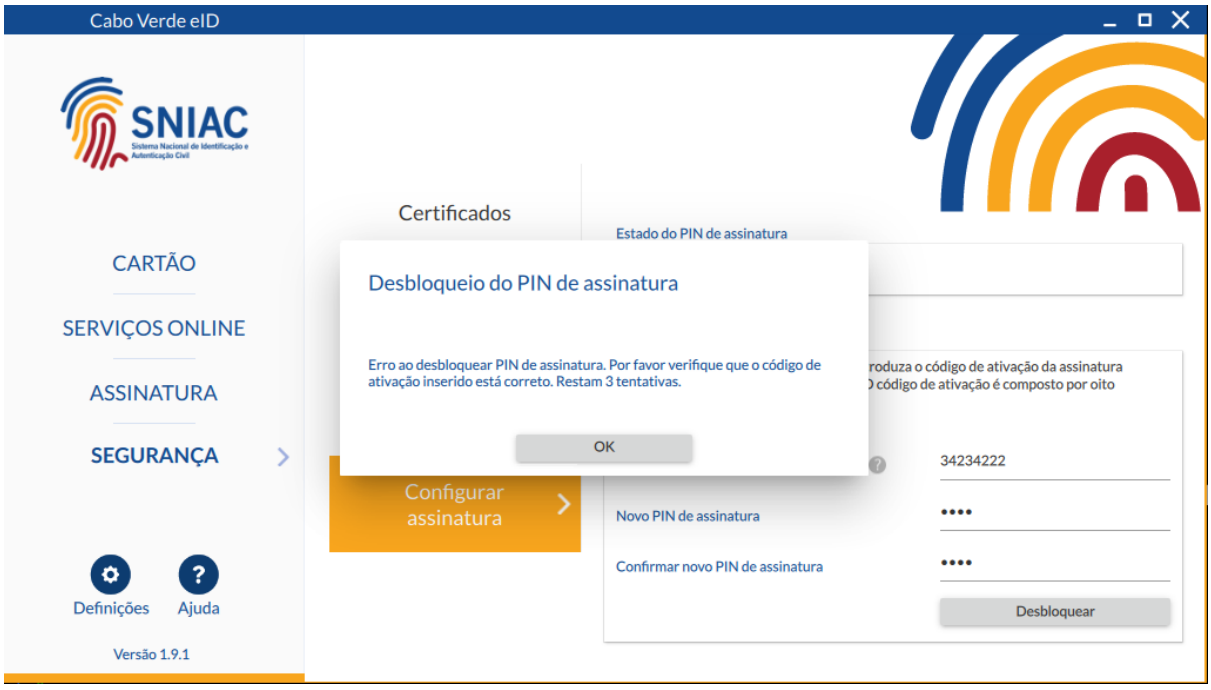
O **Código de Ativação da Assinatura Digital** é constituído por 8 dígitos em duas partes de 4 dígitos: A primeira parte vem escrita na sua carta-Pin e a segunda é disponibilizada pelo serviço no momento

da entrega da sua carta-Pin. Junte as 2 partes na caixa de texto seleccionada na figura a seguir. Deve guardar em segurança os seus códigos todos e não partilhar com ninguém.

Nesta mesma janela e como podemos ver na figura a seguir, é também apresentado o número de tentativas restantes do **Código de desbloqueio do PIN de Assinatura Digital**. Se usar todas as tentativas sem sucesso o código fica bloqueado, não sendo possível desbloquear.

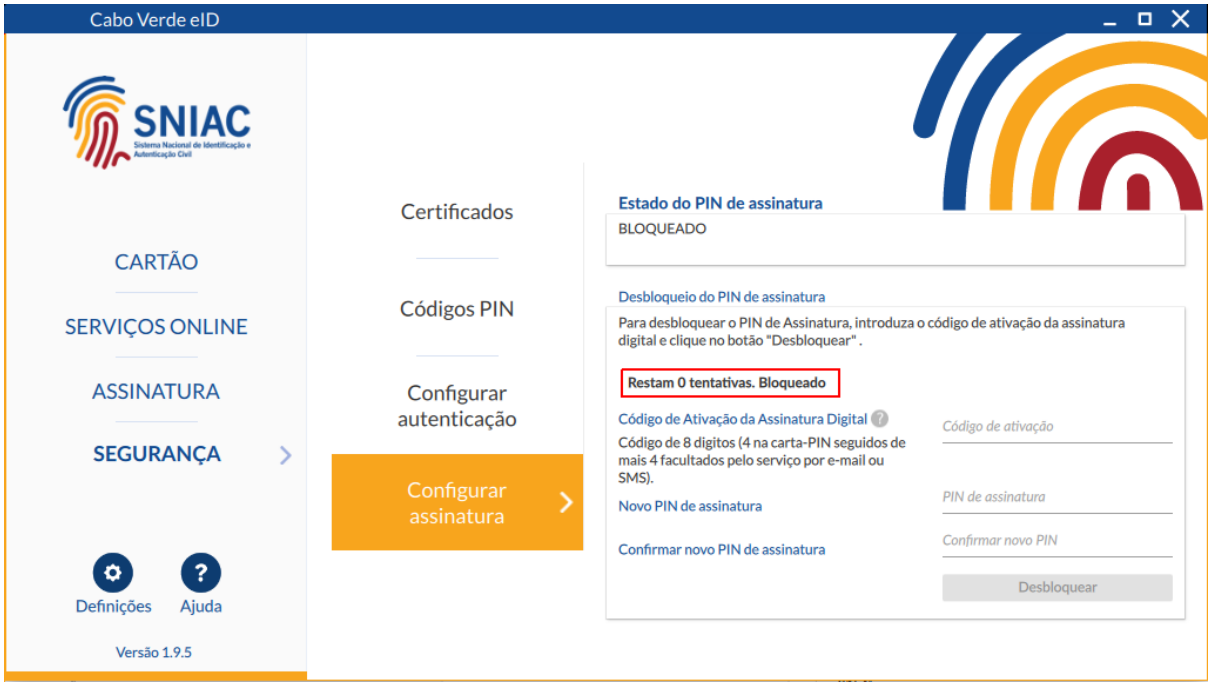


A imagem seguinte corresponde a uma tentativa de desbloqueio do PIN de assinatura sem sucesso. Neste caso deve verificar se introduziu os códigos correctamente e ter cuidado para não ultrapassar o número de tentativas, caso contrário, vai bloquear o **Código de desbloqueio do PIN de Assinatura Digital**, não sendo possível desbloquear.

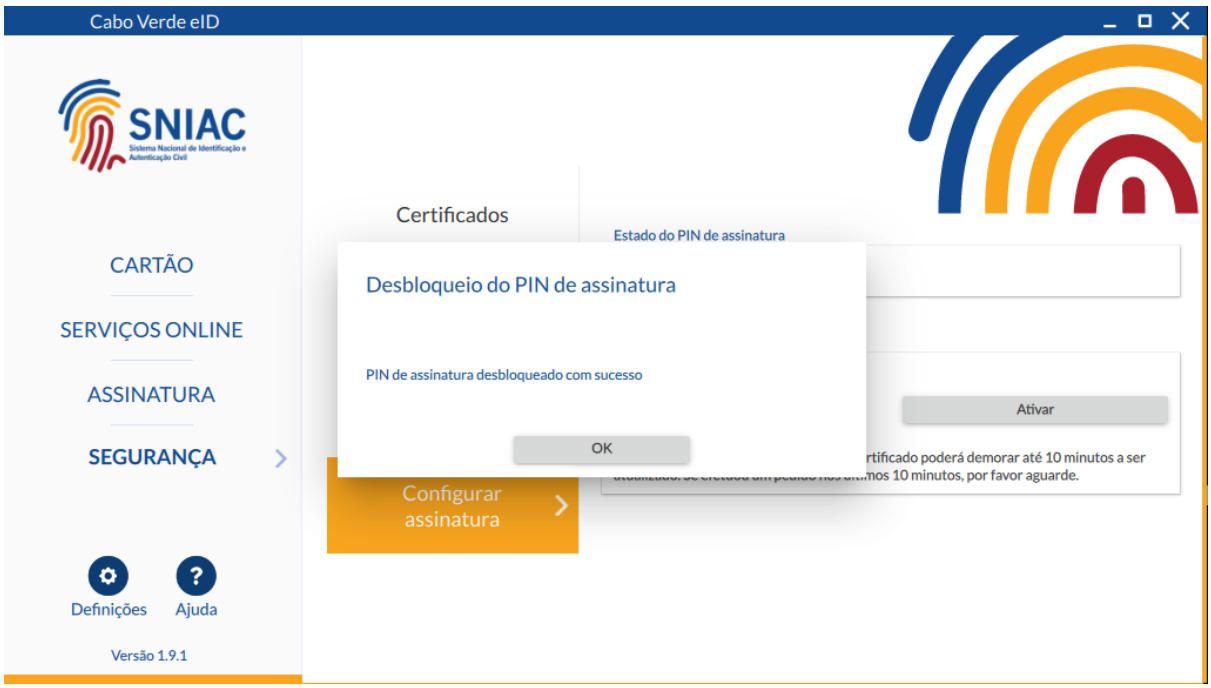


A imagem seguinte corresponde a uma tentativa de desbloqueio do PIN de assinatura Digital sem sucesso e depois de ultrapassar o número de tentativas. Neste caso o **Código de desbloqueio do PIN de**

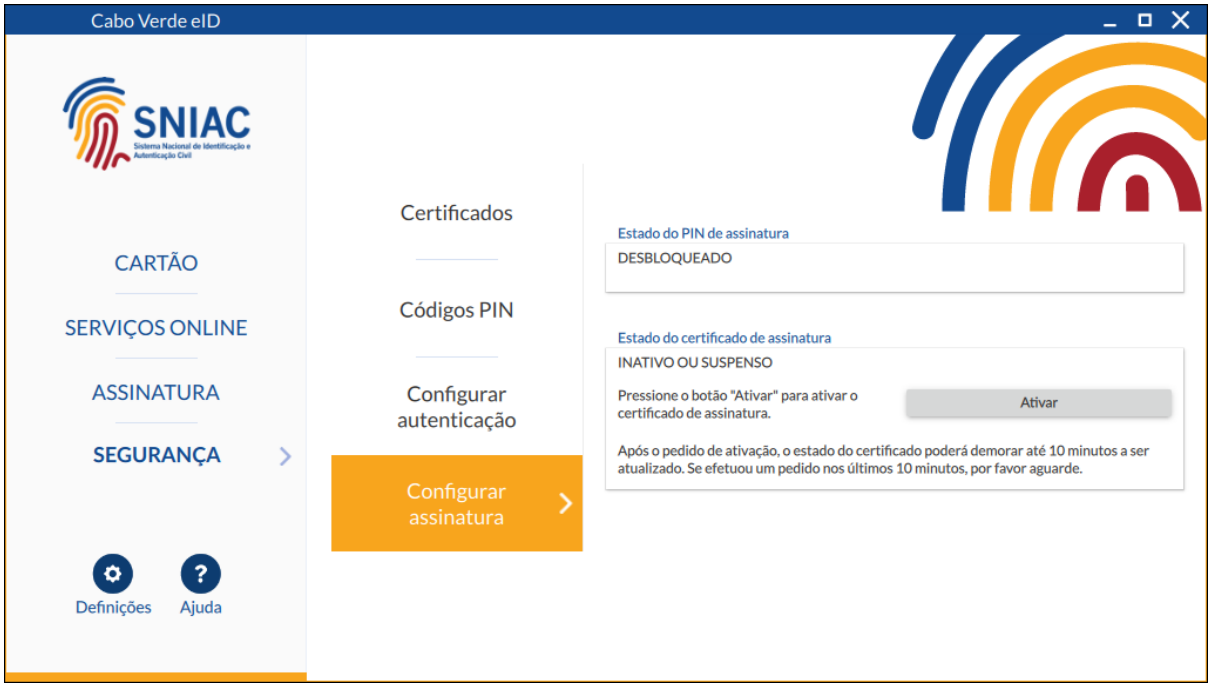
assinatura Digital fica bloqueado, não sendo possível desbloquear.



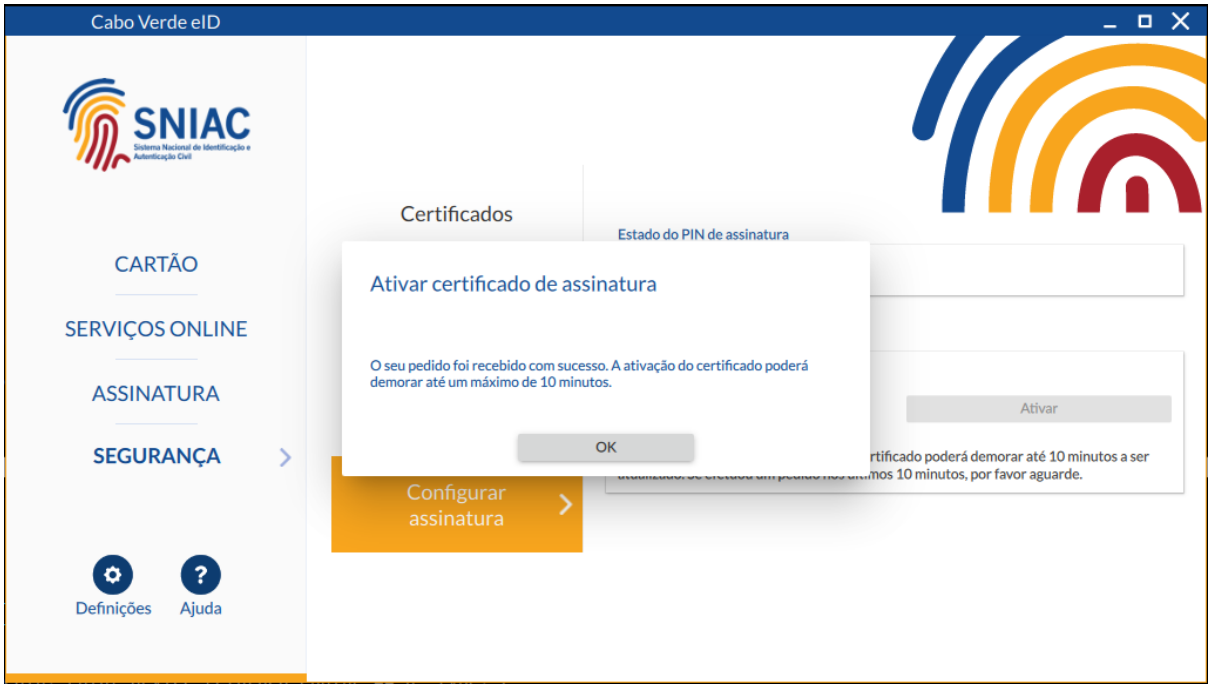
A imagem seguinte é a janela que indica que o PIN de assinatura foi desbloqueado com sucesso.



Quando o PIN de assinatura está desbloqueado, é possivel verificar o estado do certificado de assinatura. No caso deste se encontrar no estado "INATIVO OU SUSPENSO", pode ativá-lo pressionando o botão "Ativar", conforme a figura seguinte. É necessário ter o PIN de autenticação desbloqueado.



O estado do certificado poderá demorar até 10 minutos a ser atualizado. Caso tenha efectuado um pedido de ativação nos últimos 10 minutos, por favor aguarde.
A imagem seguinte ilustra a situação de sucesso na operação de ativação do certificado de assinatura.



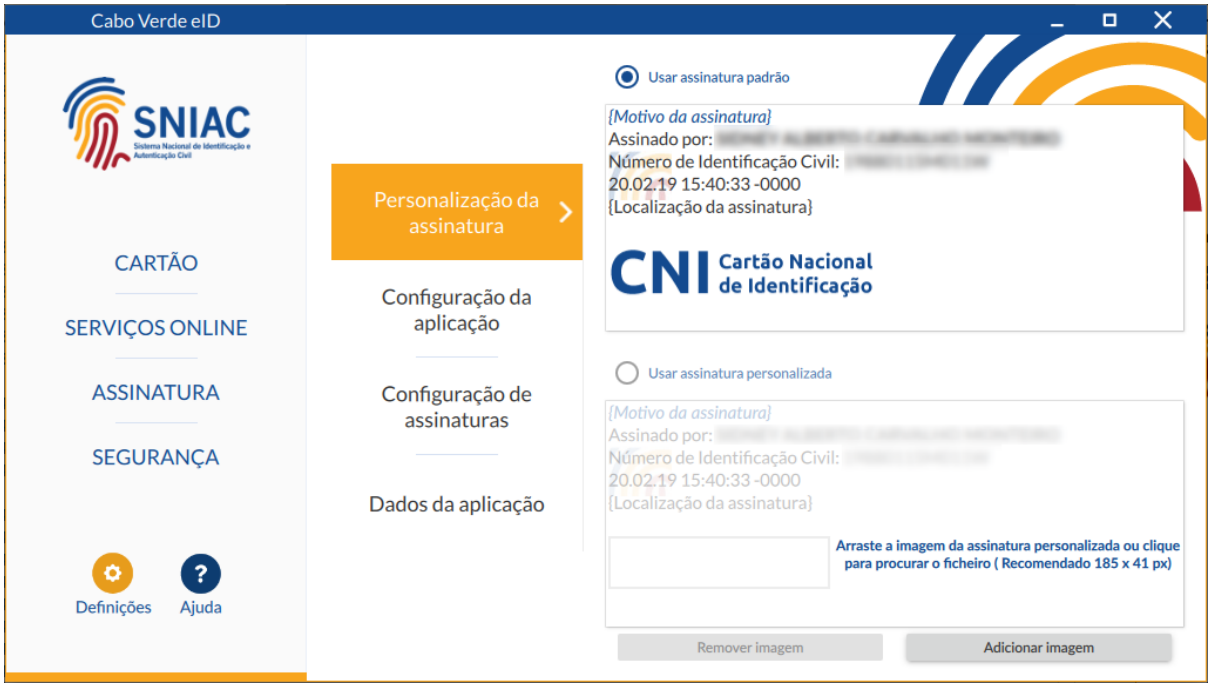
No caso de a operação não ter sucesso, verifique as mensagens de erro na ativação de certificados e leitura dos dados online.

3.2.5 Configurações

3.2.5.1 Personalização da Assinatura Neste menu é possível personalizar a assinatura digital, substituindo a imagem do documento de identificação por uma imagem à escolha do utilizador.

O botão **Adicionar imagem** 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 recomendado para a imagem é de 185 x 41px.



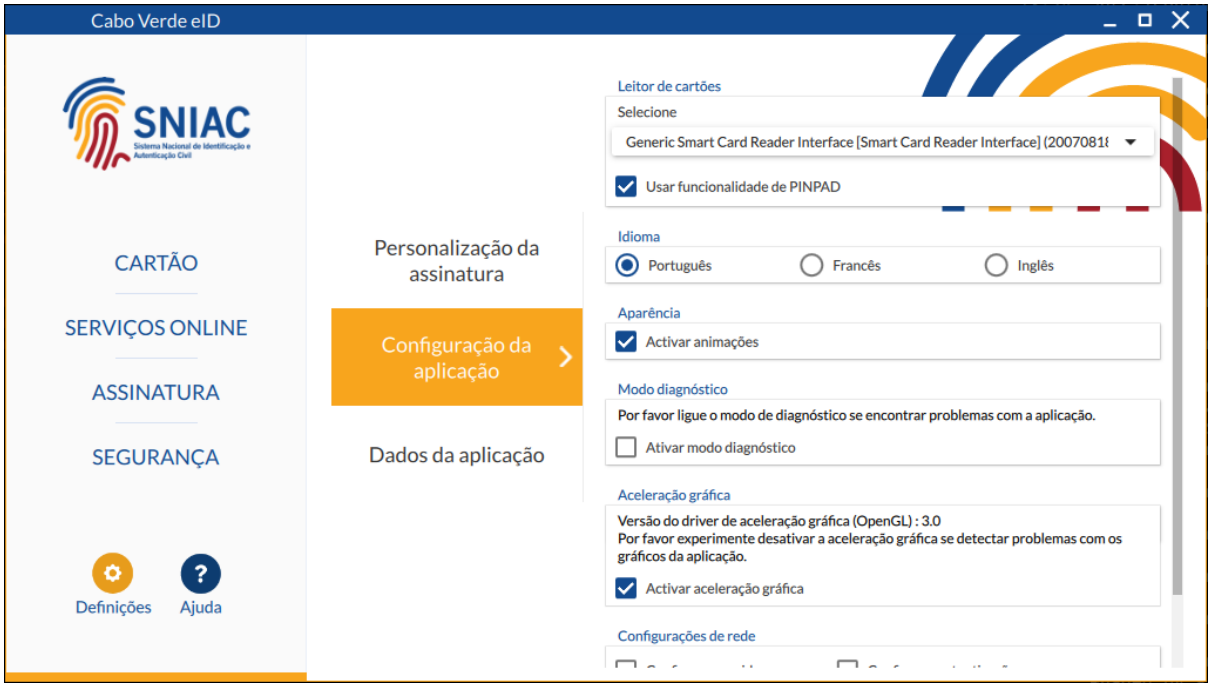
3.2.5.2 Configuração da aplicação Nesta janela é possível configurar alguns aspetos do funcionamento da aplicação, nomeadamente:

- **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.
- **Idioma:** Selecionar o idioma da aplicação, escolhendo entre Português, Francês ou Inglês.
- **Aparência:** Opções relativas à aparência 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.

  Os ficheiros de log por omissão são criados nas seguintes localizações e tem como nome o prefixo .CVMW:

  ```
  Windows: C:\Program Files\Cabo Verde eID\log\
  ```
- **Aceleração gráfica**: Permite ativar ou desativar a aceleração gráfica 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)**. 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 pelo *middleware*.
  - **Servidor proxy:** Endereço IP / Hostname / Porto.
  - **Autenticação proxy:** Credenciais de acesso (se necessário).

A imagem seguinte permite visualizar o menu de configurações da aplicação

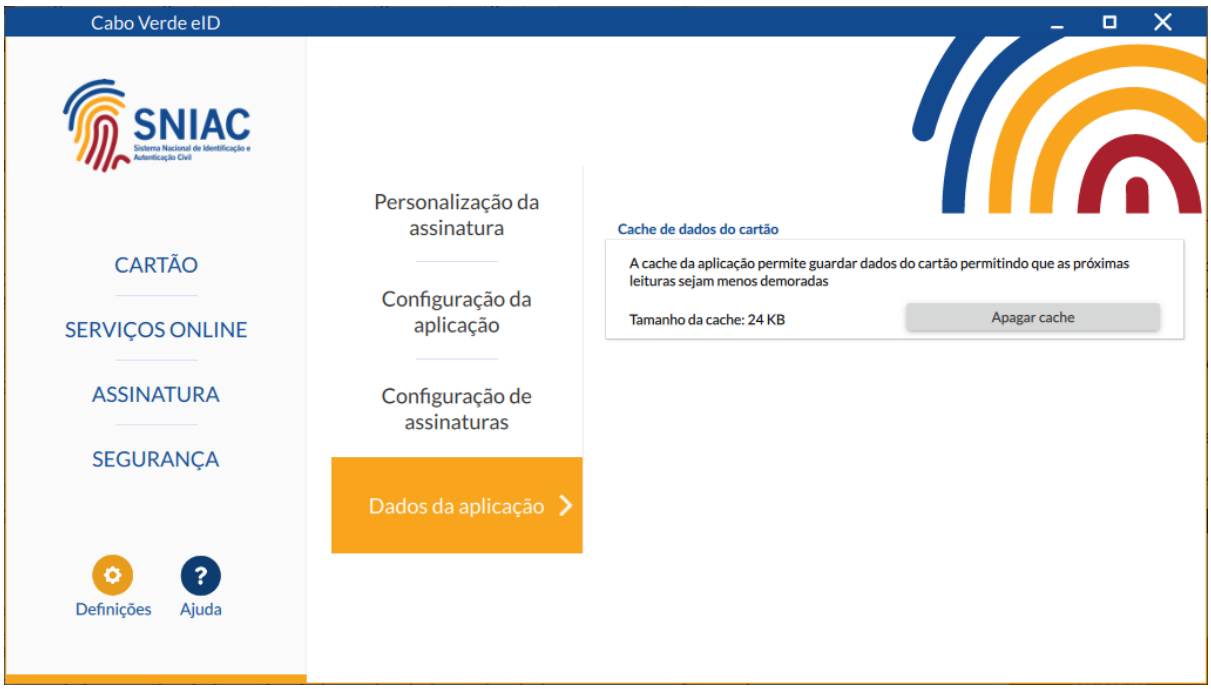


3.2.5.3 Configuração de assinaturas Nesta janela é possível configurar alguns aspetos relativos à assinatura com o documento de identificação:

- **Certificados**: Opções relativas ao registo e remoção de certificados durante a inserção e remoção do cartão.
- **Microsoft Office (Windows):** Configurações relativas a assinaturas em aplicações do Microsoft Office.

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

3.2.5.4 Dados da aplicação Neste separador é possível apagar os dados de cache armazenados das leituras dos cartões.



3.2.6 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 Integração com aplicações

O *middleware* permite a interação com outras aplicações do sistema operativo, disponibilizando duas funcionalidades: Autenticação e Assinatura Digital.

A instalação do *middleware* em Windows permite que, ao introduzir um documento de identificação 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. Alguns exemplos dessas aplicações são: *Microsoft Word*, *Microsoft Excel* e *Microsoft Outlook*.

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

Autenticação

- Mozilla Firefox

Além das aplicações acima referidas, o middleware disponibiliza suporte criptográfico às aplicações com interface PKCS#11 ou suporte criptográfico nativo do sistema operativo.

No caso das aplicações com suporte PKCS#11, geralmente é necessário configurar a localização do ficheiro da aplicação, que permite o suporte.

4.1 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.
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.

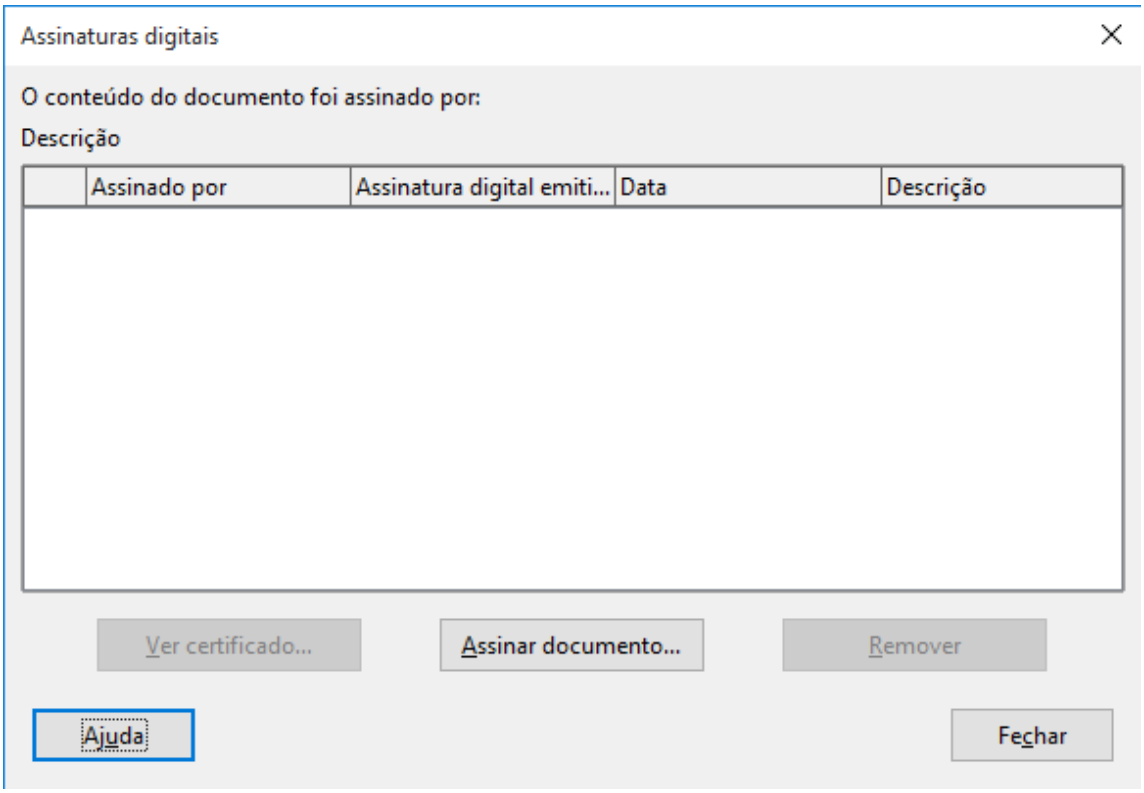
Poderá encontrar informação mais detalhada no seguinte link: Adicionar/Remover uma Assinatura Digital nos ficheiros do Office.

4.2 Assinatura digital na suite *LibreOffice / OpenOffice*

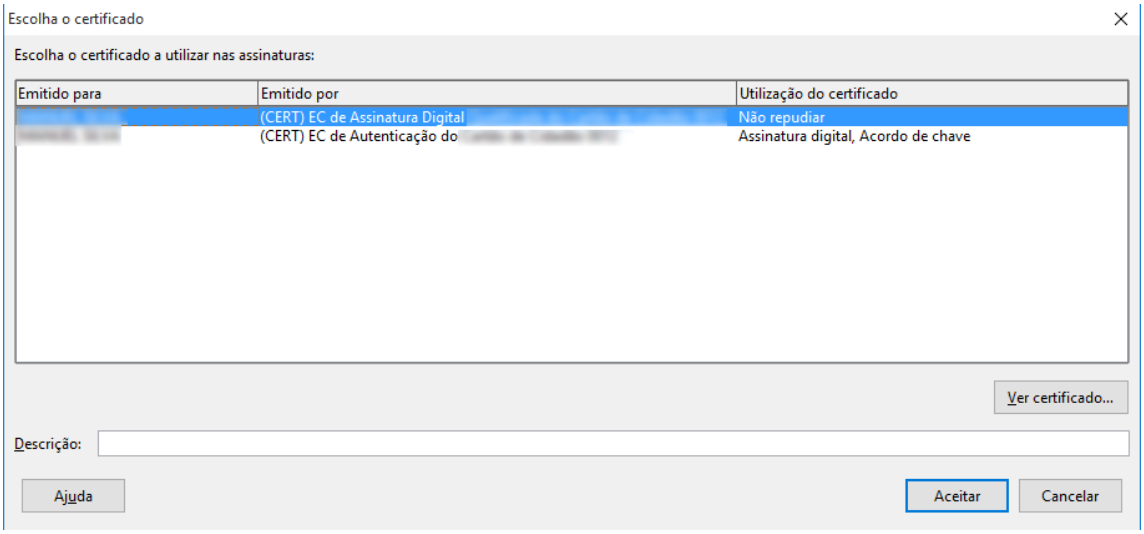
Nesta secção é apresentada a assinatura digital de documentos em ficheiros *LibreOffice*, nomeadamente, nas aplicações, *Calc*, *Write* e *Impress*. A versão utilizada neste manual foi a versão *LibreOffice 5.3*. A interface desta funcionalidade é bastante semelhante em todas as versões a partir de 4.0.0.

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.

4.3 Assinatura digital de email com *Microsoft Outlook*

A assinatura eletrónica 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 documento de identificação não existe qualquer endereço de email. Desta forma, para que seja possível efetuar assinaturas digitais no *Outlook*, é assim necessário desativar esta validação através da alteração das configurações no sistema operativo.

Para **desativar a correspondência com endereço de email do certificado digital**, deve 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/

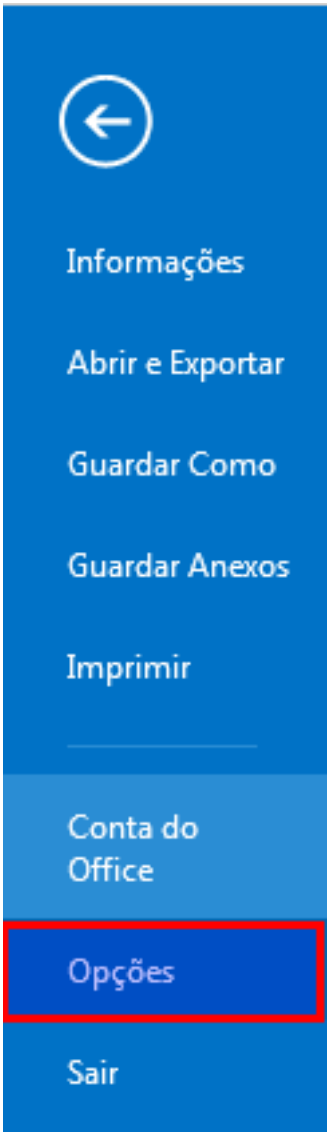
Alternativamente, poderá selecionar a opção **Permitir assinatura de e-mails no Outlook** no submenu **Configuração de assinaturas** da aplicação Cabo Verde eID.

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.

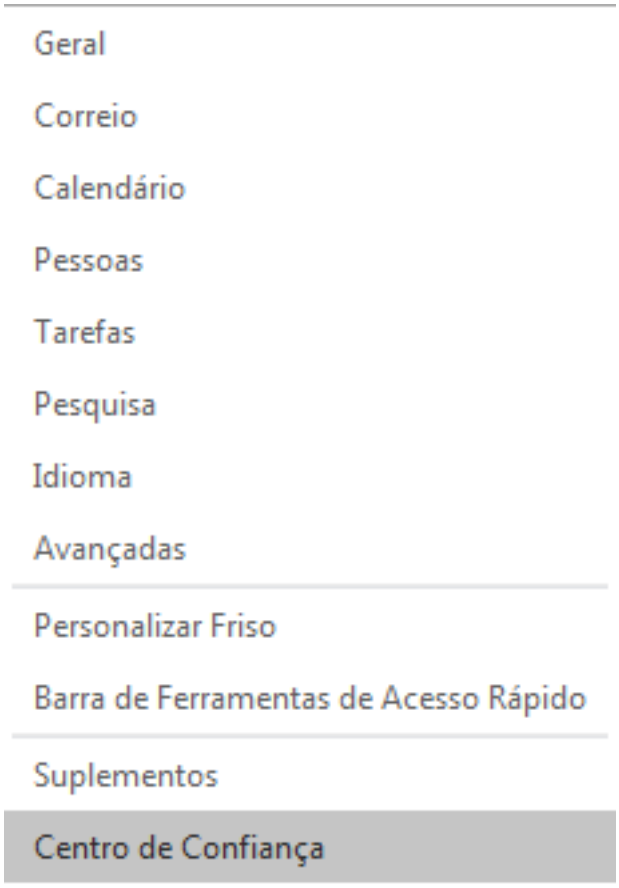
Nota: As imagens apresentadas são referentes ao *Microsoft Outlook 2016*.

Configuração – Esta operação é realizada apenas uma vez.

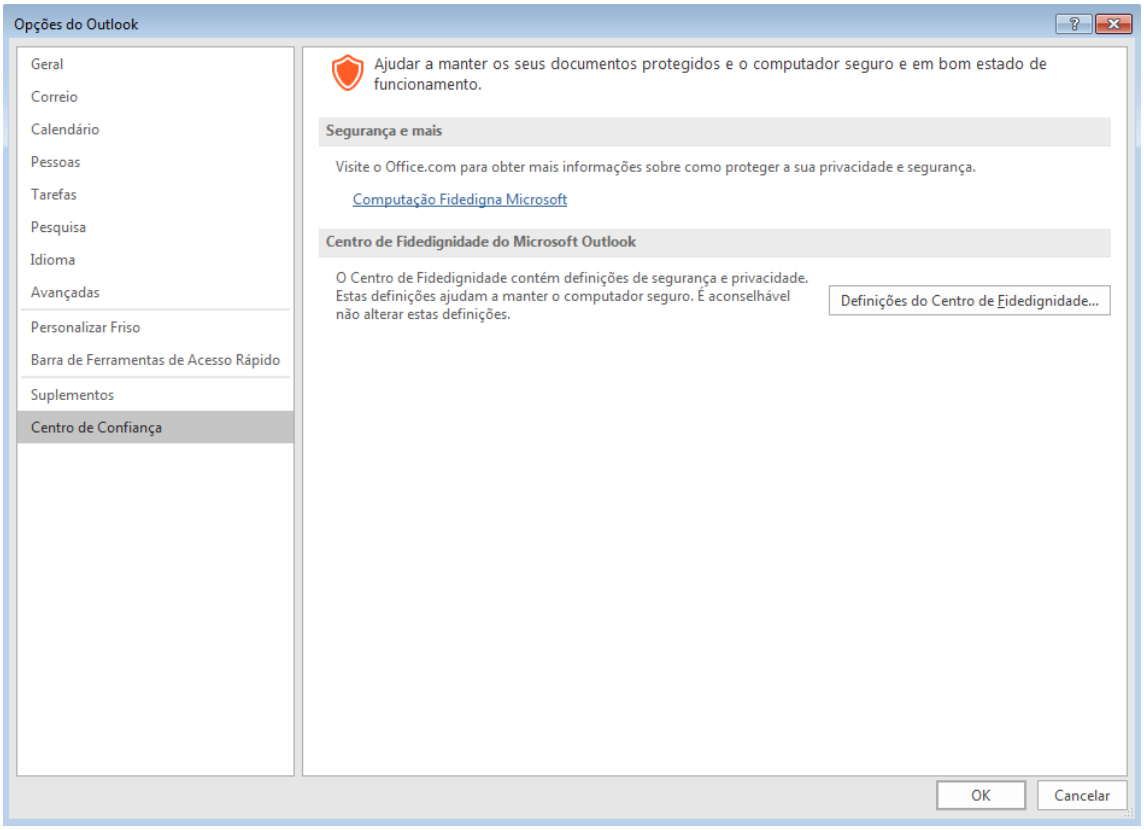
1. Assegurar que a correspondência com endereço de email do certificado digital está desativada, conforme instruções acima.
2. No Outlook, aceder ao menu **Ficheiro** → **Opções**



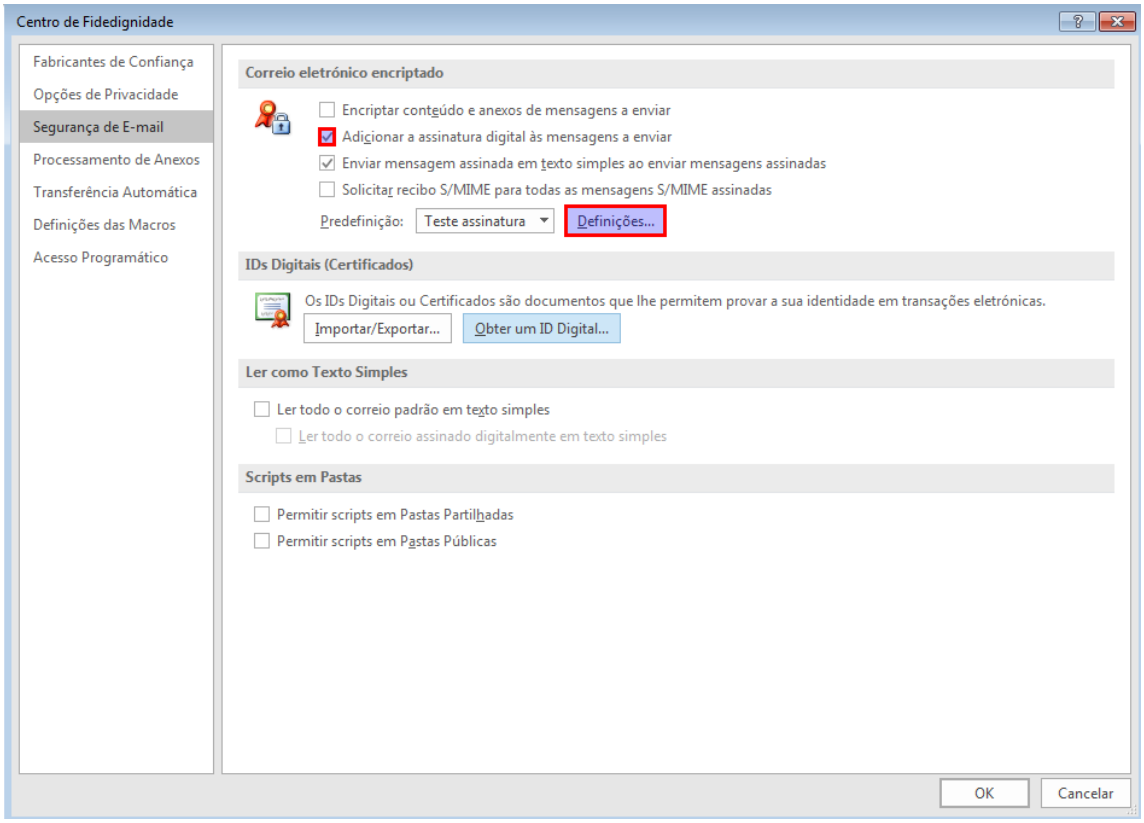
3. Clicar em **Centro de Confiança**.



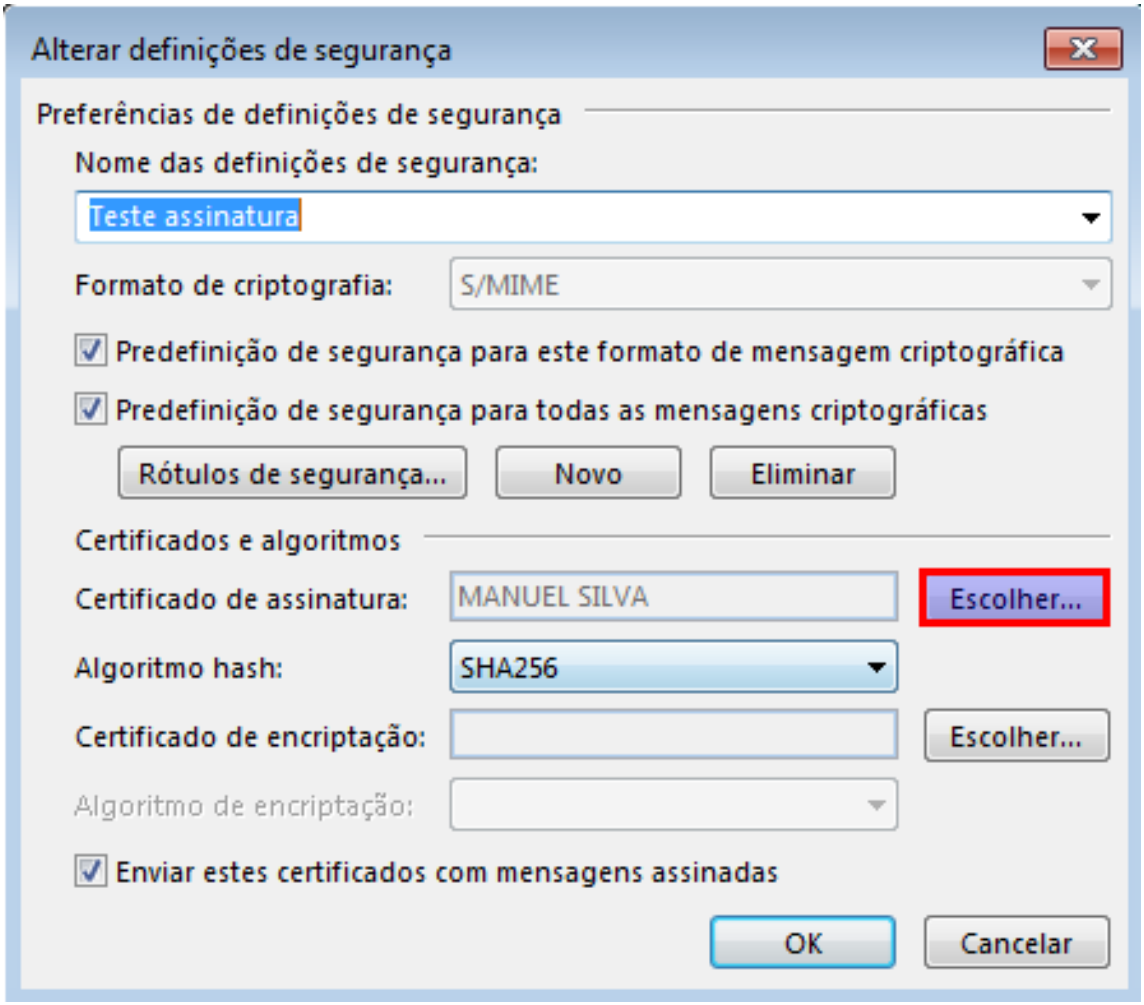
4. Selecionar a secção **Definições do Centro de Fidedignidade**.



5. Nesta secção, selecionar a opção **Adicionar a assinatura digital às mensagens a enviar** e clicar no botão **Definições**



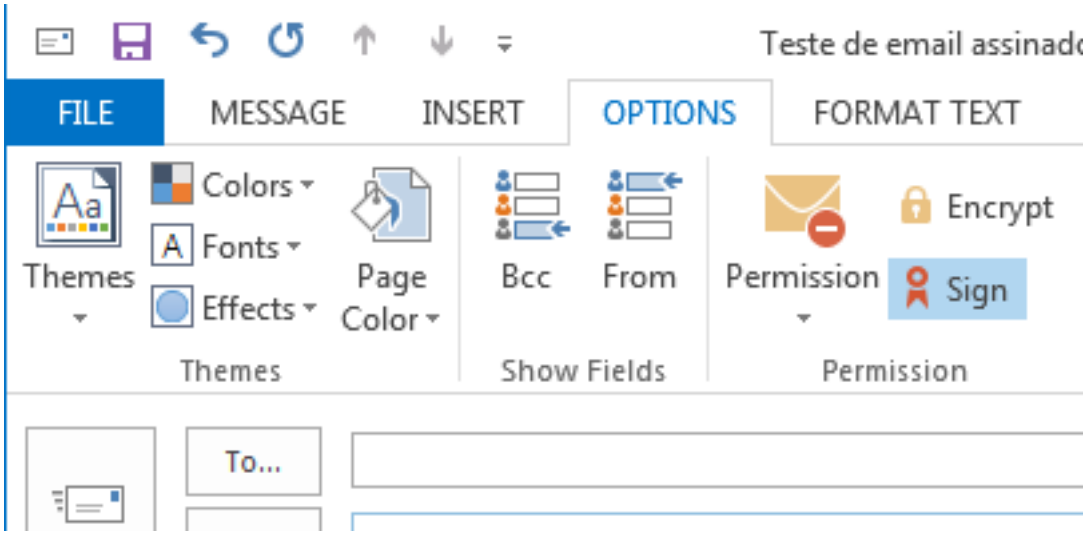
6. Adicione uma descrição a esta configuração, p. ex.: “Assinatura com documento de identificação” e clique no botão **Escolher** para selecionar o certificado.



7. Selecione o seu certificado de assinatura 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.

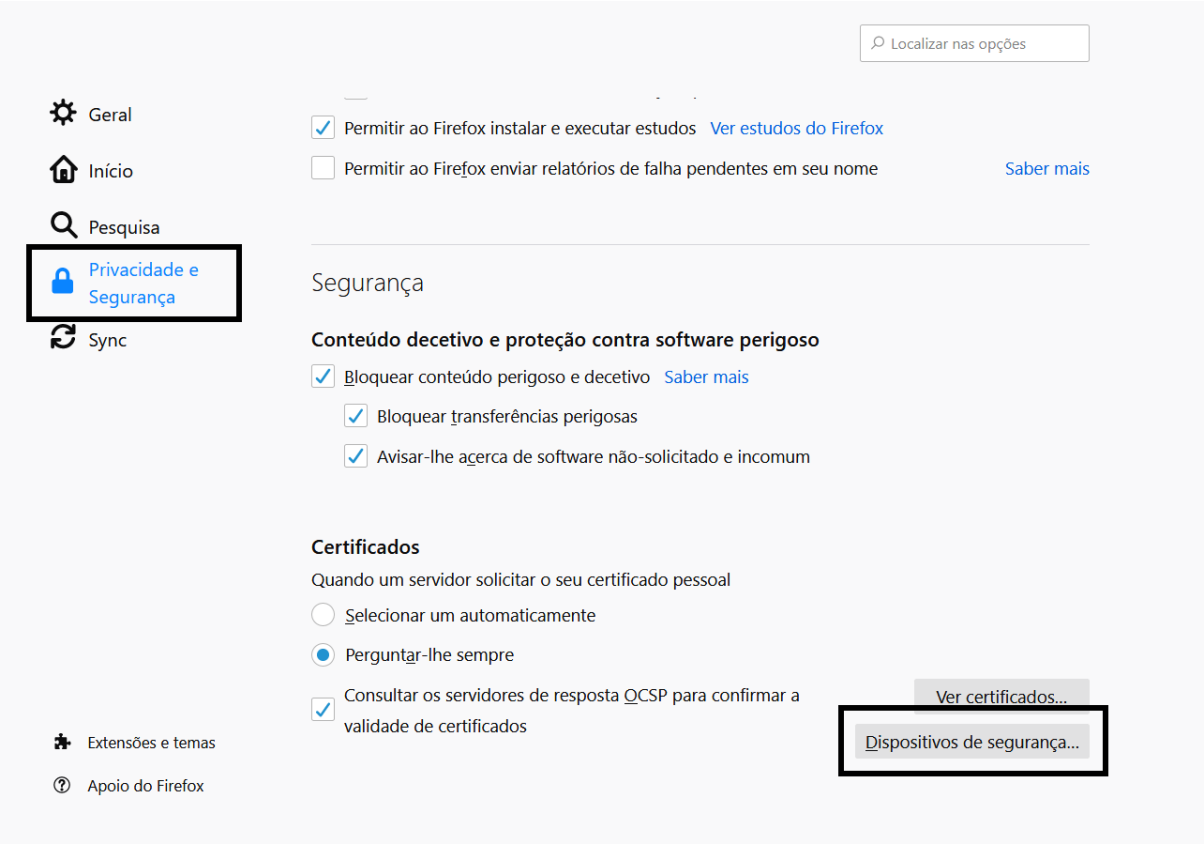


4.4 Autenticação em *Mozilla Firefox*

Para configurar o *Mozilla Firefox* tem que carregar o módulo PKCS#11 do Middleware de Identificação Eletrónica em Cabo Verde.

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".



1. Pressione **Carregar**. Preencha o nome do módulo, por exemplo "Cabo Verde eID". Seguidamente, carregue em **Procurar...** e navegue até ao módulo PKCS#11 do Middleware de Identificação Eletrónica em Cabo Verde, cuja localização deste ficheiro, depende do sistema operativo a ser utilizado.

   Windows: C:\Windows\System32\cvmw-pkcs11.dll

   Linux: /usr/lib/cveid-mw/libcvmwpkcs11.so

   MacOS: /usr/local/lib/cveid-mw/libcvmwpkcs11.dylib

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

5 Resolução de Problemas

5.1 Mensagens de erro na ativação de certificados e leitura dos dados online

Nas funcionalidades de ativação de certificados e leitura dos dados online a aplicação no caso de a operação não ter sucesso apresenta uma janela de erro com os seguintes códigos de erro e descrição.

Código de Erro	Mensagem
0	O certificado selecionado está errado.
1	Erro no carregamento do Plugin.
2	Erro na ligação ao servidor. Por favor verifique a sua ligação a internet.
3	Servidor temporariamente indisponível.
4	Servidor temporariamente indisponível.
5	Servidor temporariamente indisponível.
6	A operação foi cancelada pelo Cidadão.
7	Ocorreu um erro ao tentar ler o cartão.
8	Servidor temporariamente indisponível.

Em todas estas mensagens é ainda apresentada a seguinte mensagem com indicações para contactar o suporte:

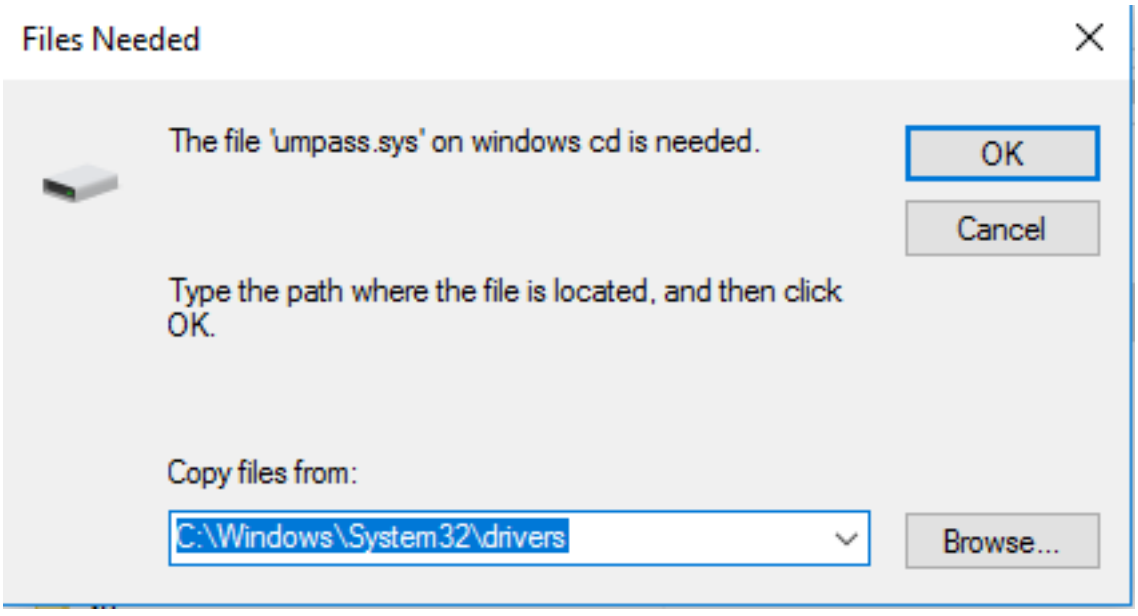
Por favor tente novamente e, caso o erro persista, contacte os serviços de apoio:

- Casa do Cidadão através do número 8002008 (linha grátis nacional) ou (+238) 260 55 00 do estrangeiro ou do e-mail **casadocidadao@casadocidadao.gov.cv**;
- Direção Geral dos Registos, Notariado e Identificação (DGRNI) para linha grátis 8001016 ou pelos contactos disponível no site oficial do SNIAC em **www.sniac.cv**

5.2 Impossibilidade de assinatura com *Adobe Reader*, *Microsoft Office* e *LibreOffice*

Deverá aceder ao ficheiro "cvmw-mdrv.inf", presente por defeito na diretoria " C:\ProgramFiles\CVMW Minidriver" (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".



5.3 O leitor de cartões está instalado mas não é detetado pela aplicação Cabo Verde eID

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** | **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 Cabo Verde eID.
   f) Volte a inserir o leitor e abra novamente a aplicação.

5.4 Problemas com placas gráficas integradas em *Windows*

No caso de existirem problemas gráficos, recomenda-se testar desabilitar a aceleração gráfica por hardware. No menu Definições / Configuração da aplicação / Aceleração Gráfica é possivel ativar ou desativar a aceleração gráfica na aplicação.

No caso da aplicação não arrancar, o procedimento para desabilitar a aceleração gráfica por hardware consiste em adicionar às variáveis de ambiente do sistema a variável **QT_OPENGL** com o valor **software**. Em alternativa é possivel configurar essa opção usando as configurações do software Identificação em Cabo Verde.

Em **Windows** na chave de registo:

HKEY_CURRENT_USER\Software\CVMW\configuretool\graphics_accelaration

```
graphics_accelaration = 1 // Aceleração gráfica ativada
```

```
graphics_accelaration = 0 // Aceleração gráfica desativada
```

6 Instruções de configuração em ambientes empresariais

6.1 Configurações através de chaves de registo Windows

As configurações do software Identificação em Cabo Verde são guardadas em *Windows* em chaves de registo sendo que as alterações feitas pelo utilizador no interface gráfico se sobrepõem aos valores predefinidos e ficam guardadas em sub-chaves de:

`HKCU\Software\CVMW`

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

`HKLM\Software\CVMW\general\install_dirname`

`HKLM\Software\CVMW\general\certs_dir`

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\CVMW`**

`HKLM\Software\CVMW\logging\log_level`

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

`HKLM\Software\CVMW\logging\log_dirname`

- **Tipo**: String
- **Descrição**: Directoria onde são gerados os ficheiros de log do Middleware.
- **Valor por omissão**: `C:\Program Files\Cabo Verde eID\log`

`HKLM\Software\CVMW\logging\log_prefix`

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

`HKLM\Software\CVMW\general\install_dirname`

- **Tipo**: String
- **Descrição**: Directoria onde é instalado o Middleware.
- **Valor por omissão**: `C:\Program Files\Cabo Verde eID`

`HKLM\Software\CVMW\general\cache_dirname`

- **Tipo**: String
- **Descrição**: Directoria onde é guardada a cache do Middleware.
- **Valor por omissão**: `C:\Users\[User]\AppData\Roaming\.cvmw-ng`

`HKLM\Software\CVMW\general\use_pinpad`

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

`HKLM\Software\CVMW\configuretool\start_with_windows`

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

`HKLM\Software\CVMW\proxy\use_system_proxy`

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

`HKLM\Software\CVMW\proxy\proxy_host`

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

`HKLM\Software\CVMW\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 65535)
- **Descrição**: Tempo de cache local (em segundos) do estado de validade dos certificados.
- **Valor por omissão**: 30

6.2 Configurações através de ficheiro de configuração em MacOS

As configurações do software Cabo Verde eID são guardadas em MacOS num ficheiro de configuração. Este ficheiro de configuração está localizado no seguinte caminho:

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

onde **$HOME** indica a directoria 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.

6.3 Informação sobre servidores de Proxy

6.3.1 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.

6.3.2 Configuração em *MacOS*

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

7 Notas do Utilizador