#### Segurança em Redes de Computadores

##### **TP3 - Cifra, assinaturas, certificados e o ADSS**

##### MESTRADO INTEGRADO EM ENGenharia de Telecomunicações e informática

**Grupo 4:**

70020 – José Pedro Afonso Rocha

73232 – Luís Pedro Lobo de Araújo

Índice

[Introdução 3](#_Toc4781195)

[Conceitos Teóricos 4](#_Toc4781196)

[Chave Pública 4](#_Toc4781197)

[Chave Privada 4](#_Toc4781198)

[Certificados Digitais 4](#_Toc4781199)

[Parte Prática 5](#_Toc4781200)

[Gerar par de Chaves 5](#_Toc4781201)

[Criar Certificado do grupo 6](#_Toc4781202)

[Criar CA no ADSS 8](#_Toc4781203)

[Criação de Certificados por elemento 12](#_Toc4781204)

[Importação de Certificados para o Sistema Operativo 13](#_Toc4781205)

[Envio de e-mails Assinados e Encriptados 16](#_Toc4781206)

[Mensagem entre grupos 19](#_Toc4781207)

[Revogação de um certificado 19](#_Toc4781208)

[Conclusão 21](#_Toc4781209)

# Introdução

No âmbito da Unidade Curricular de Segurança em Redes de Computadores foi-nos proposto criar um par de chaves por aluno, e ainda certificados utilizando a ferramenta ADSS (Advanced Digital Signature Service) com o intuito de enviar mensagens de e-mail assinadas e encriptadas entre o grupo.

A ferramenta que será usada, o ADSS, é um produto da Ascertia que serve para gerar e verificar assinaturas digitais, validar certificados e outros serviços relacionados com a gestão de uma PKI. Será também utilizado o OpenSSL que nos irá permitir fazer a criação das chaves públicas e privadas.

É muito importante, ao longo deste trabalho, consolidar as noções de chaves privadas e públicas, de certificações digitais, perceber como um certificado pode ser considerado válido ou torná-lo válido e aprender um conjunto de comandos e técnicas que nos permite importar para o sistema operativo de uma máquina certificados pessoais e chaves pessoais de modo a conseguir realizar o proposto para este trabalho.

# Conceitos Teóricos

## Chave Pública

A chave pública é uma chave criada através de algoritmos de encriptação de chave assimétrica e são usadas para converter uma mensagem em um formato ilegível.

Para desencriptar esta chave será preciso uma chave privada diferente, mas correspondente à chave pública, ou seja, elas serão emparelhadas para permitir uma comunicação segura.

Esta chave pode ser colocada num diretório de livre acesso para desencriptação da assinatura digital de um remetente, podendo ser enviada por e-mail para contactos e utilizadores confiáveis.

Pretty Good Privacy (PGP) é uma forma popular de criptografia de chave pública onde as chaves são hospedadas num diretório de um servidor de chaves públicas para permitir a partilha de chaves públicas.

## Chave Privada

A chave privada é um bocado de código que está emparelhado com uma chave pública para definir algoritmos para criptografia e desencriptação de texto.

Esta chave apenas é partilhada com o iniciador da chave, garantido a segurança da mesma. Por exemplo, A e B representam um remetente da mensagem e um destinatário da mensagem, respetivamente e cada um tem o seu próprio par de chaves públicas e privadas. A, o iniciador ou remetente da mensagem, envia uma mensagem para B, sendo a mensagem de A encriptada com a chave pública de B. Então, B usa a sua chave privada para desencriptar a mensagem recebida de A.

## Certificados Digitais

Um certificado digital autêntica as credenciais da web de um remetente e permite que o destinatário de uma mensagem encriptada saiba que os dados são de uma fonte confiável (ou de um remetente que afirma ser um deles).

Este tipo de certificado é usado para auto-assinatura e encriptação de mensagens e também pode ser chamado como certificado de chave pública ou certificado de identidade.

Seguindo o exemplo dado na definição de chave privada, o certificado digital é usado para garantir que A (remetente da mensagem) é o remetente original da mensagem. Para verificar essa situação, B (destinatário da mensagem) usa a chave pública de A para desencriptar o certificado, já que A deve usar previamente a sua chave privada para encriptar o certificado digital. Se for legível, o certificado digital será autenticado com uma autoridade de certificação (CA).

# Parte Prática

## Gerar par de Chaves

Nesta fase do projeto é pedido que cada elemento do grupo crie um par de chaves, para tal foi utilizada a ferramenta OpenSSL. Para tal é necessário correr os comandos demonstrados a seguir:

**Luís Araújo:**

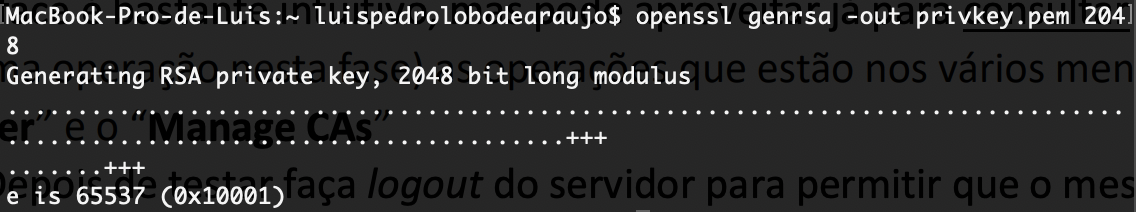


Figura - Gerar chave privada.



Figura - Verificar chave gerada.

**José Pedro Rocha:**

Figura -gerar chave privada.

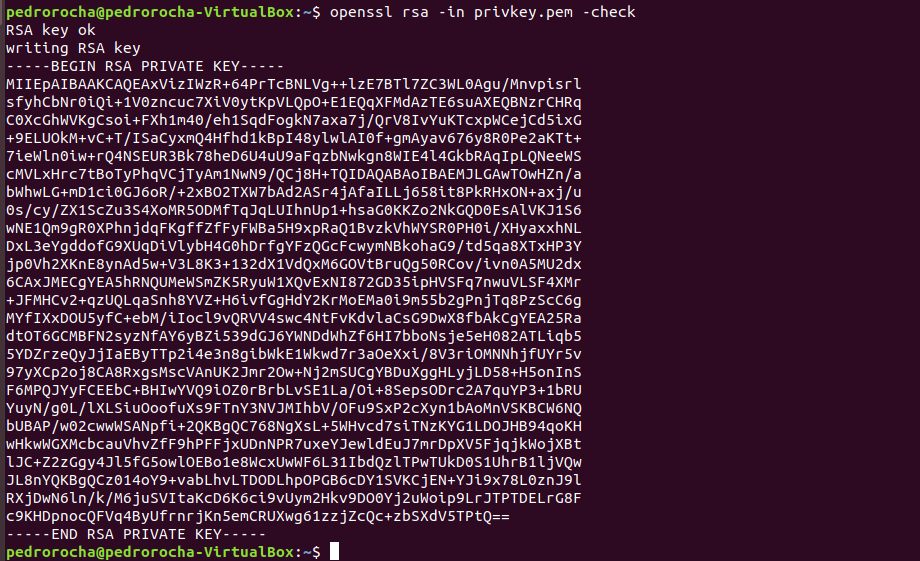


Figura - verificar chave privada.

## Criar Certificado do grupo

De seguida estão descritos os passos realizados para a criação do Certificado do grupo.

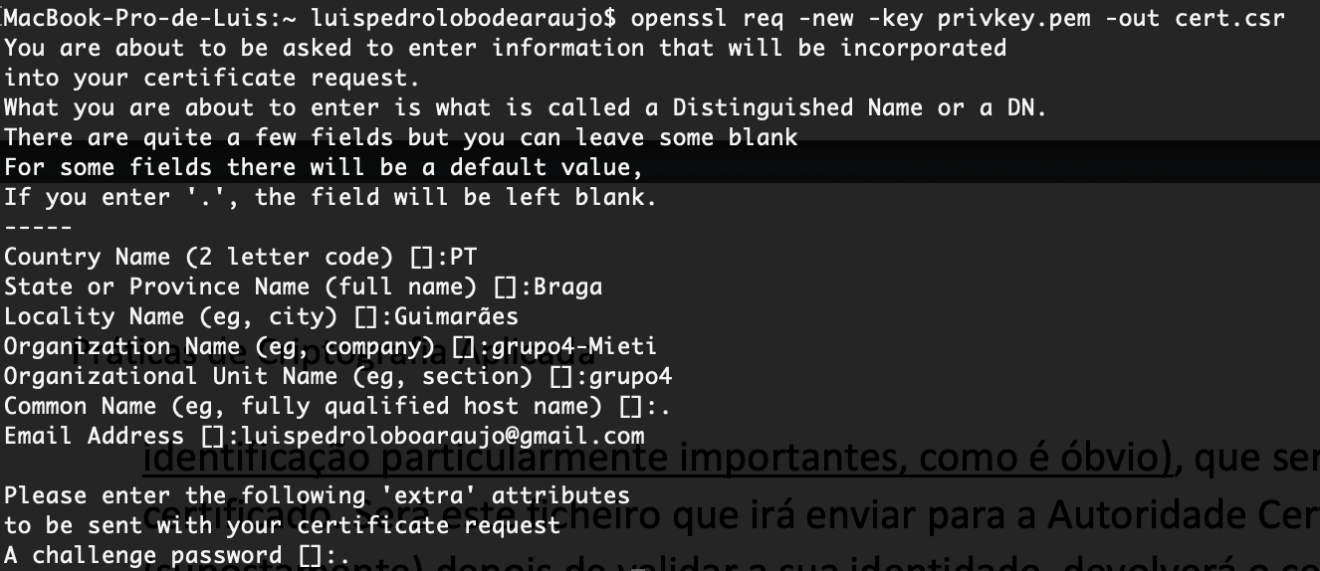


Figura - Pedido de certificado.

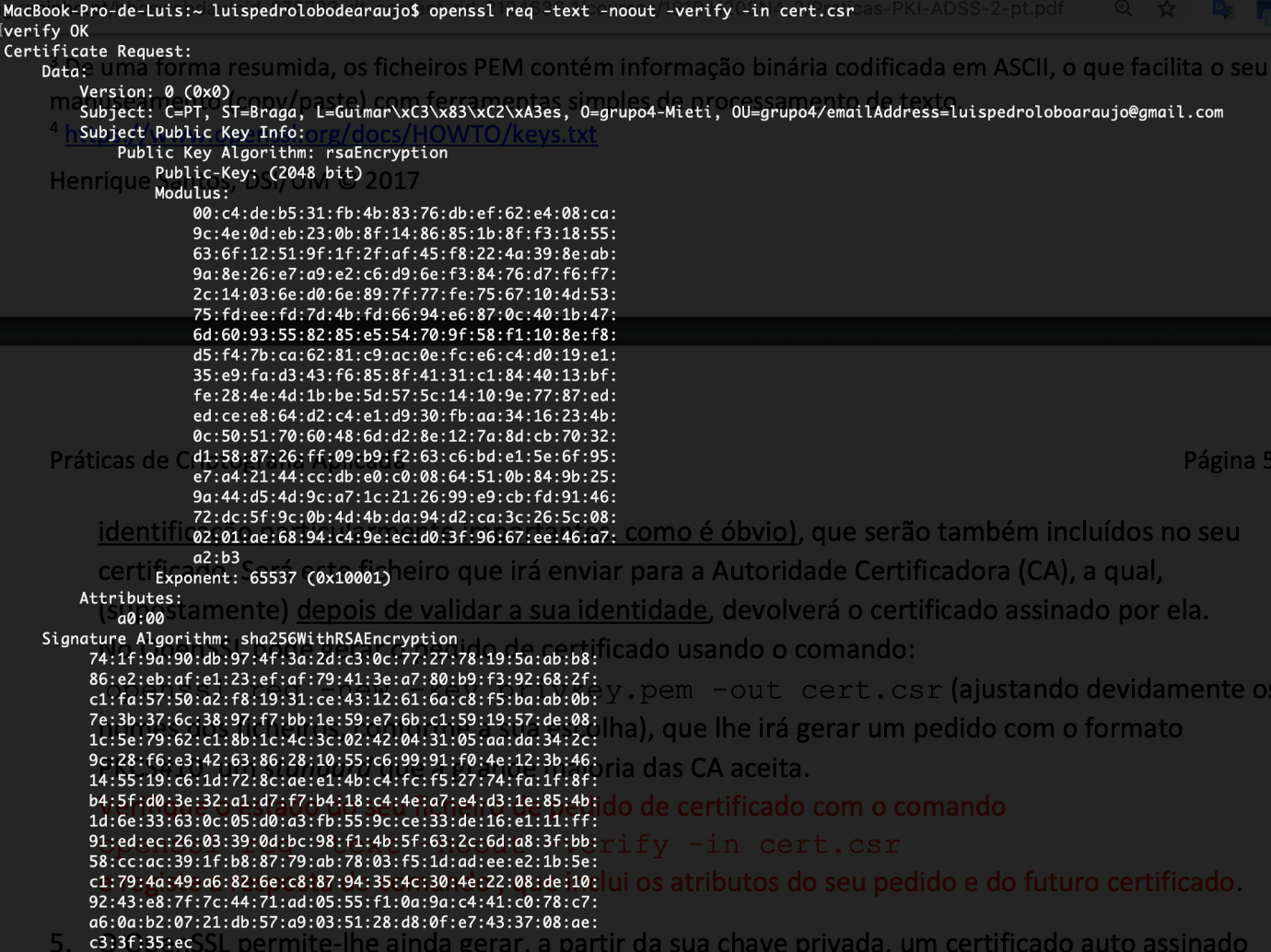


Figura - Verificar estado de pedido de certificados.

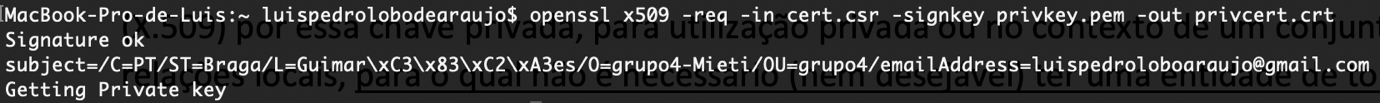


Figura - Gerar Pedido de certificado auto-assinado por Luís Araújo.

**José Pedro Rocha:**

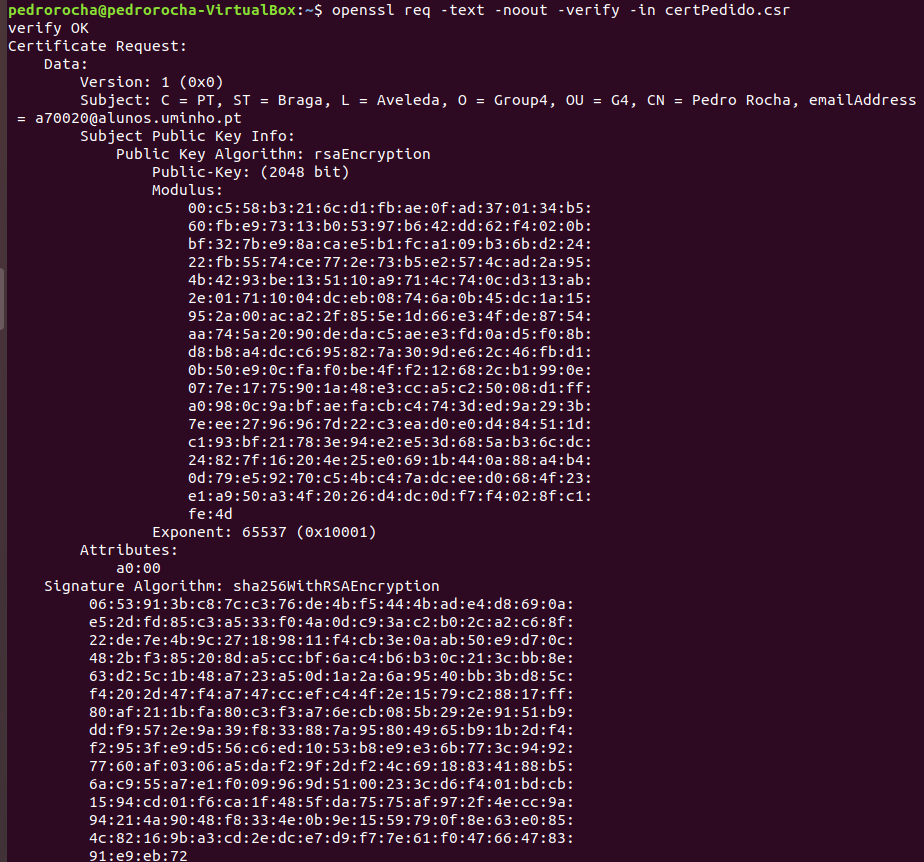


Figura - Verificar estado de pedido de certificados.



Figura -GERAR PEDIDO DE CERTIFICADO AUTO-ASSINADO POR José Pedro Rocha.

## Criar CA no ADSS

Em seguida são demonstrados os passos realizados para a criação da CA do grupo no ADSS.

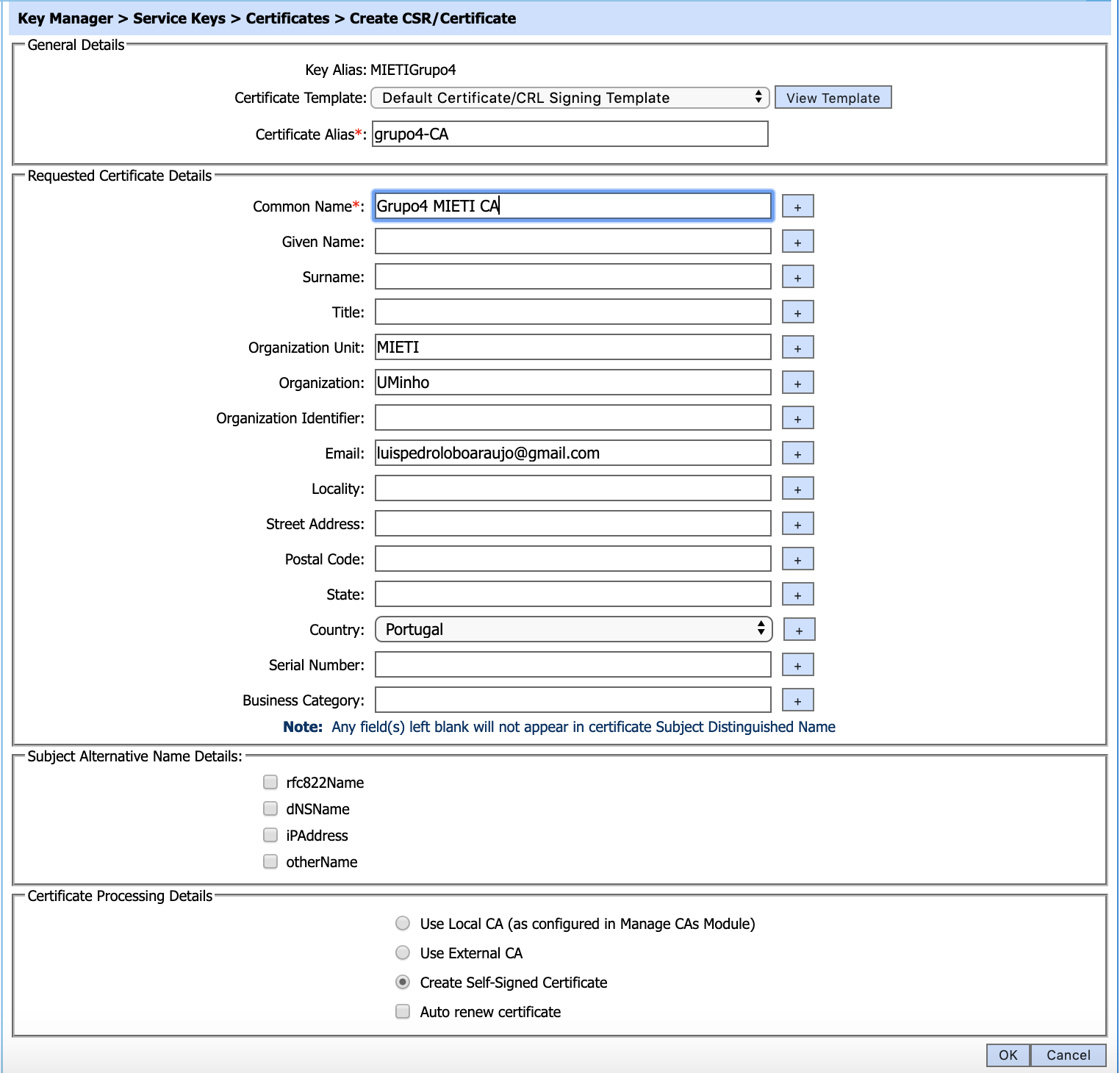


Figura - Criar certificado auto-assinado no ADSS.

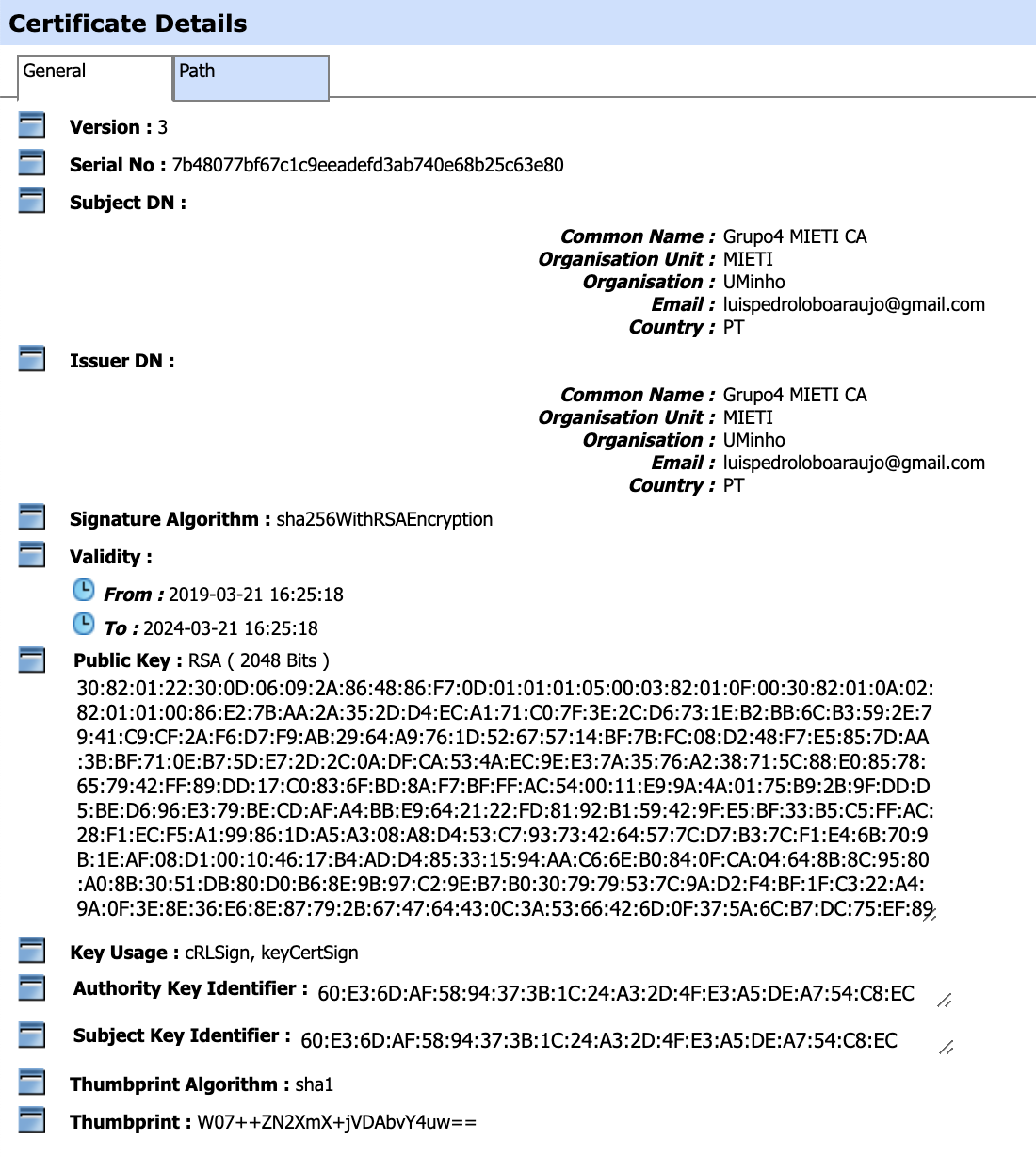


Figura - Certificado auto-assinado do grupo.

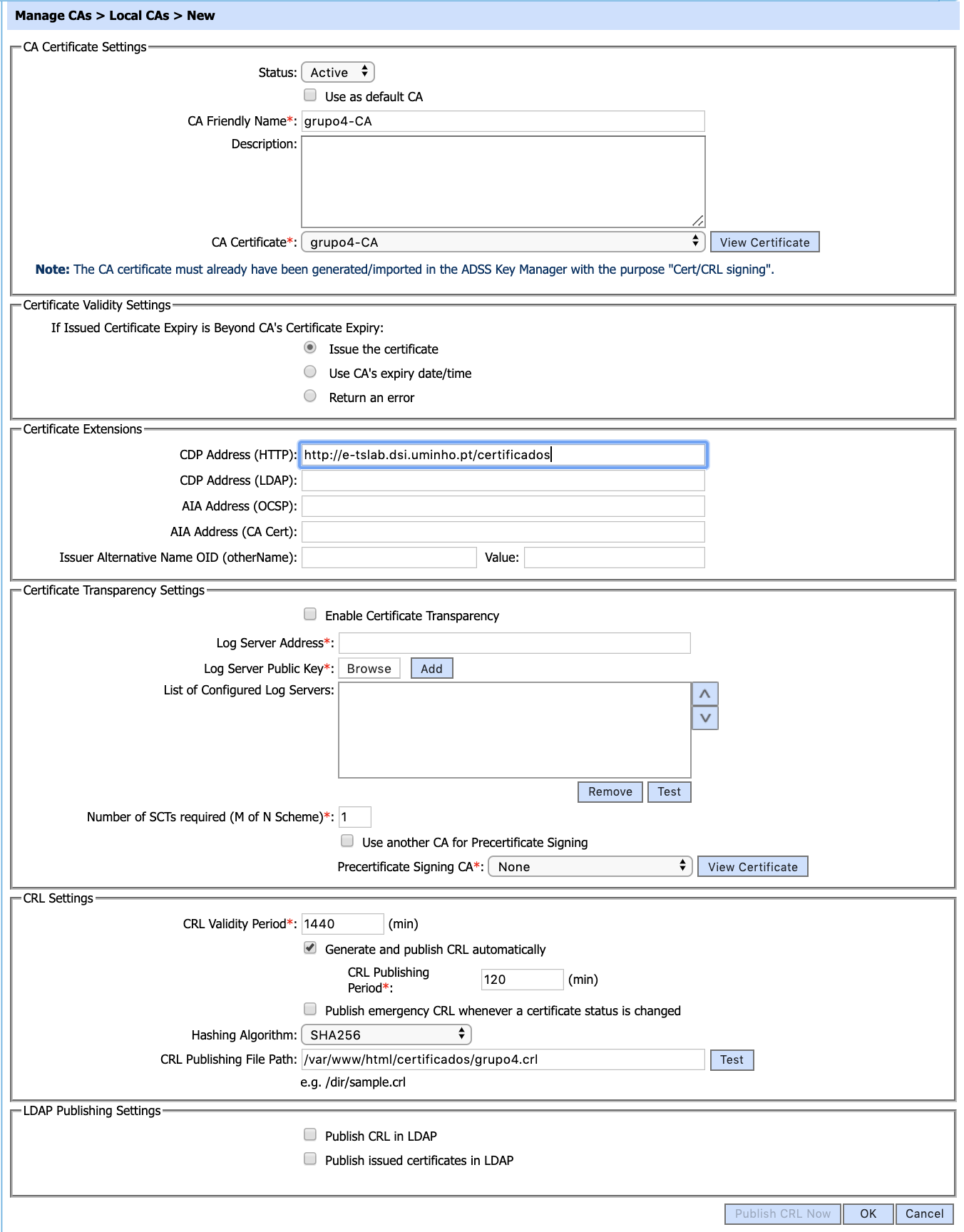


Figura – Criação do CA do Grupo.

## Criação de Certificados por elemento

**Luís Araújo:**

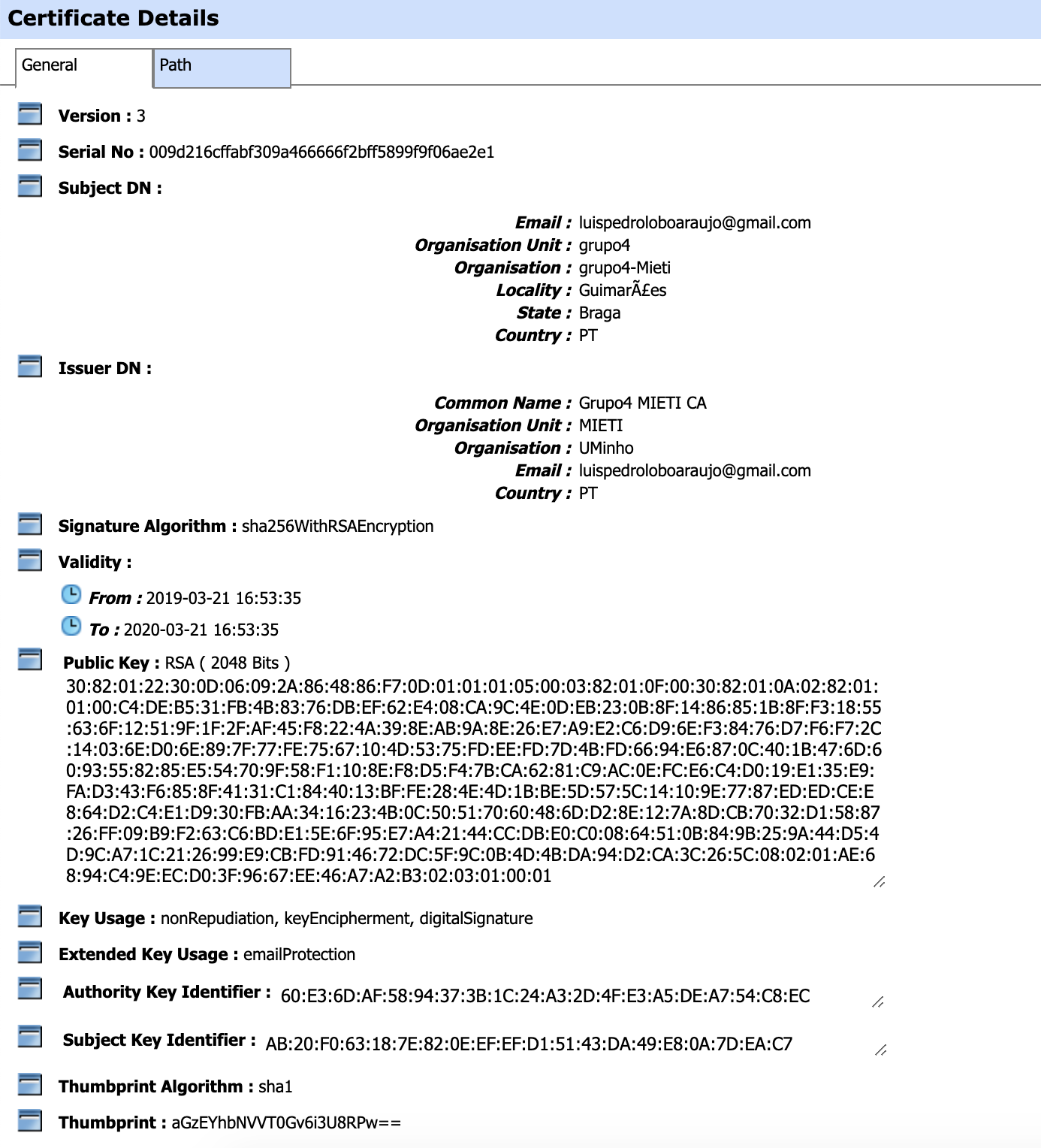


Figura - Certificado gerado para Luís Araújo.

**José Pedro Rocha:**

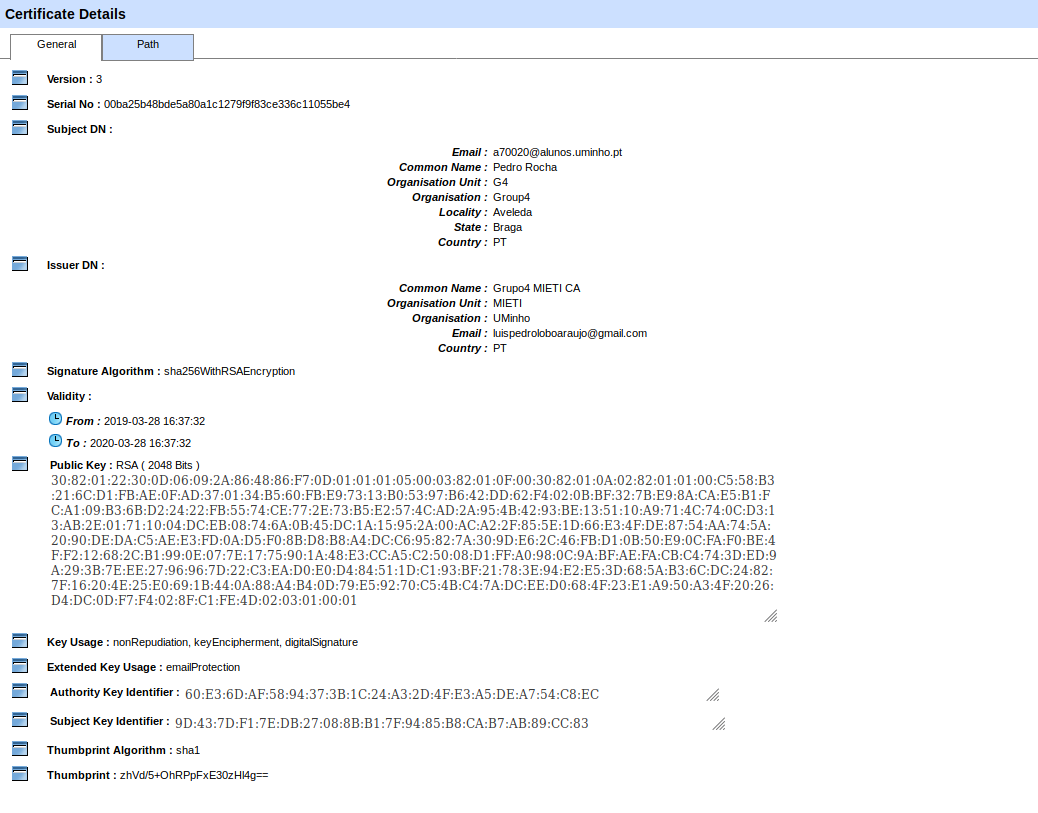


Figura - CERTIFICADO GERADO PARA josé pedro rocha.

Nesta fase, os elementos também guardaram os certificados assinados pelo CA criado para utilizar posteriormente.

## Importação de Certificados para o Sistema Operativo

Antes de se começar a importar os certificados gerados será preciso criar uma chave privada para cada elemento do grupo que irá conter o certificado público, assinado pelo CA, a chave privada e o certificado do CA.

**Luís Araújo:**

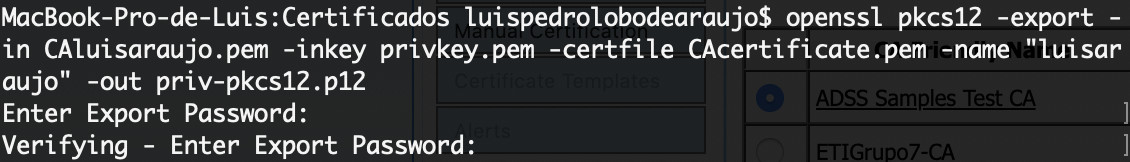


Figura - Criação do ficheiro PKCS#12 da chave-privada.

**José Pedro Rocha:**

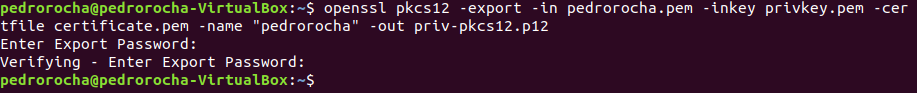


Figura - criação do ficheiro pkcs#12 da chave privada.

De seguida utilizou-se o ficheiro criado para instalar o certificado criado e ainda o CA.

**Luís Araújo:**



Figura - Inserir certificado.



Figura - Certificados Instalados.

**José Pedro Rocha:**

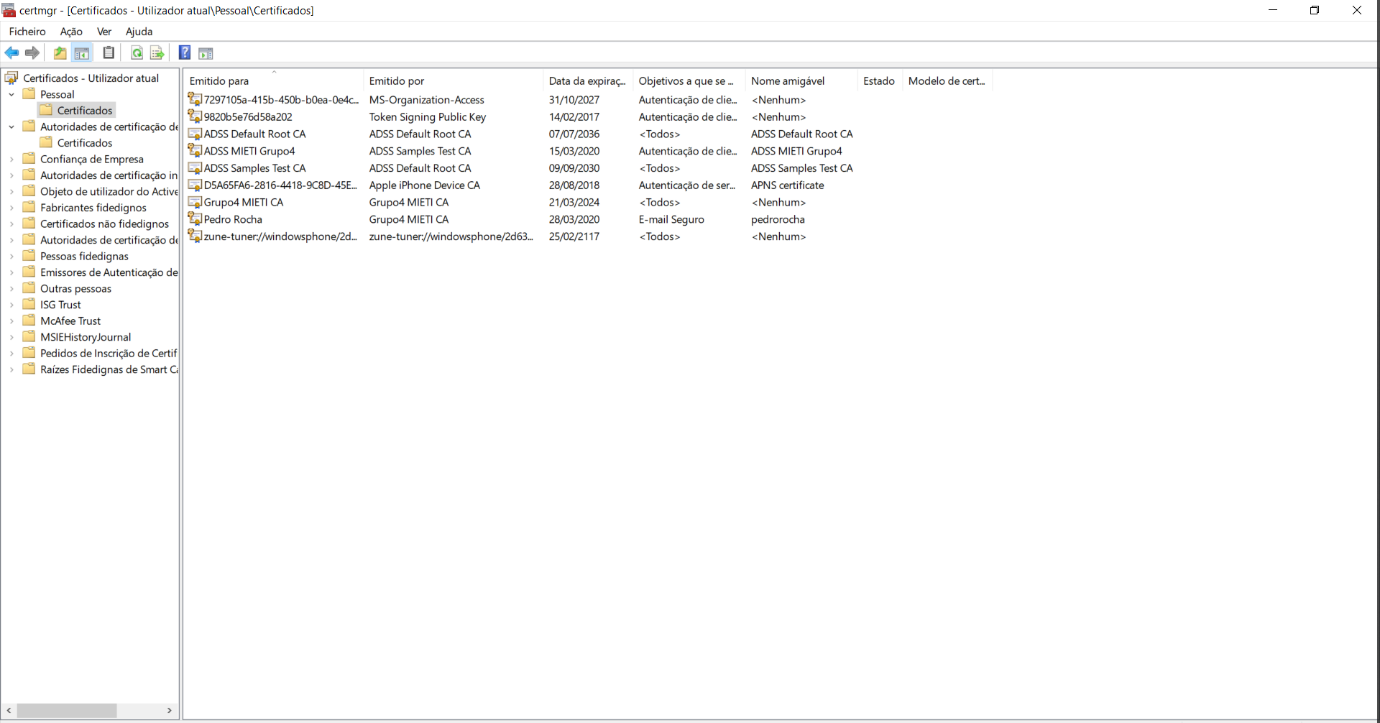
****

Figura - certificados instalados – pessoais

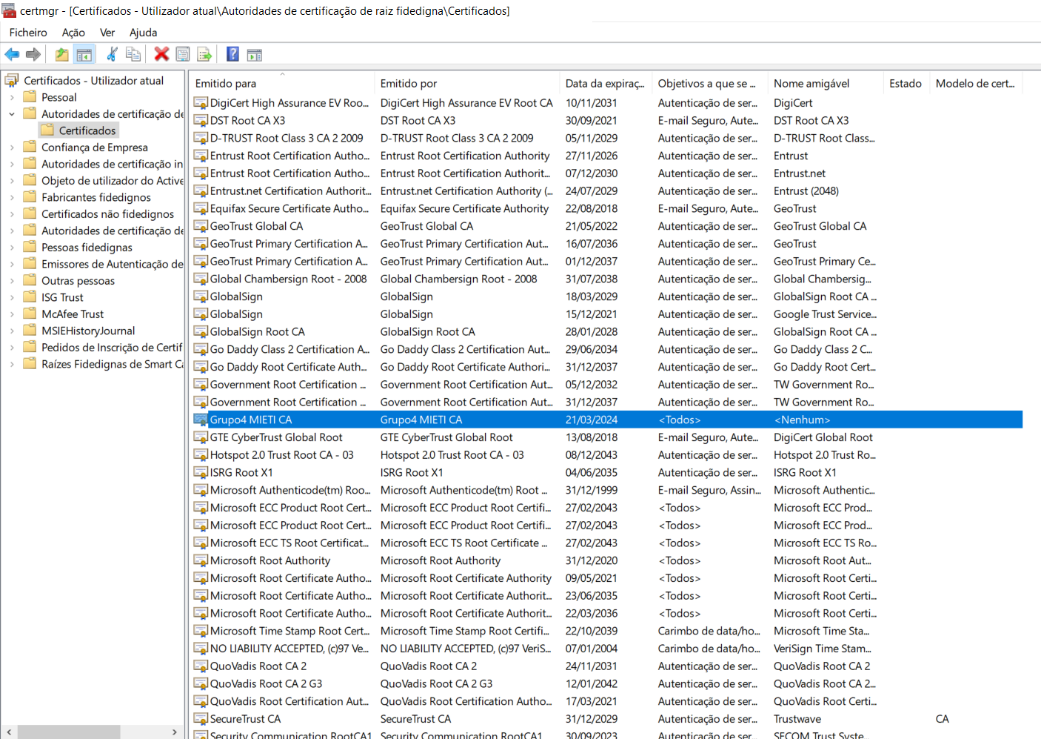


Figura - Certificados instalados – CA

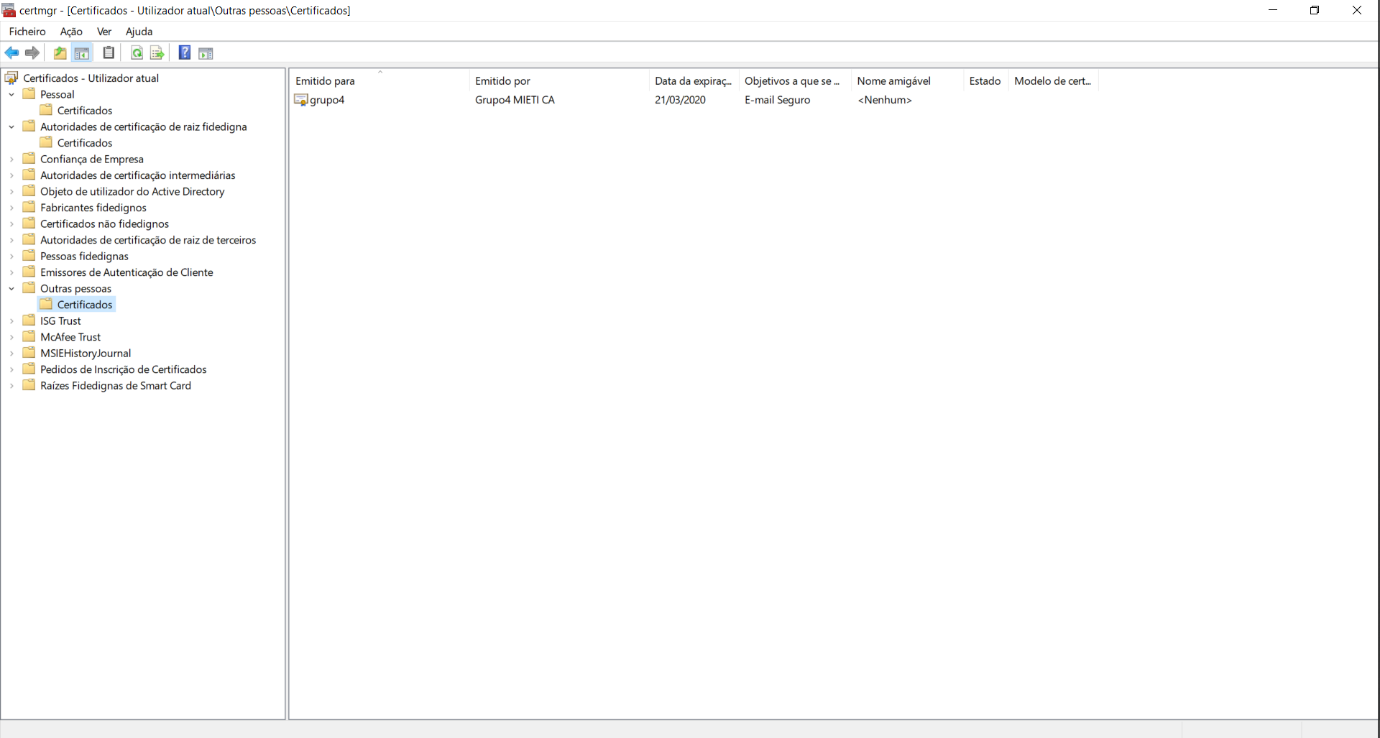


Figura - Certificados instalados - certificado público Luís araújo

## Envio de e-mails Assinados e Encriptados

Na sequência da criação e instalação dos certificados, foi-nos proposto enviar e receber mensagens seguras, ou seja, cada um dos elementos ser capaz de cifrar e assinar digitalmente e-mails. No entanto para a cifra de mensagens, é necessário ter acesso à chave publica do remetente.

**Luís Araújo:**

Para o envio de e-mails cifrados foi utilizada a aplicação de Mail proveniente do sistema operativo macOS. Uma vez que o certificado já está instalado no sistema operativo, este faz automaticamente a associação ao endereço de e-mail e ao endereço presente no certificado.

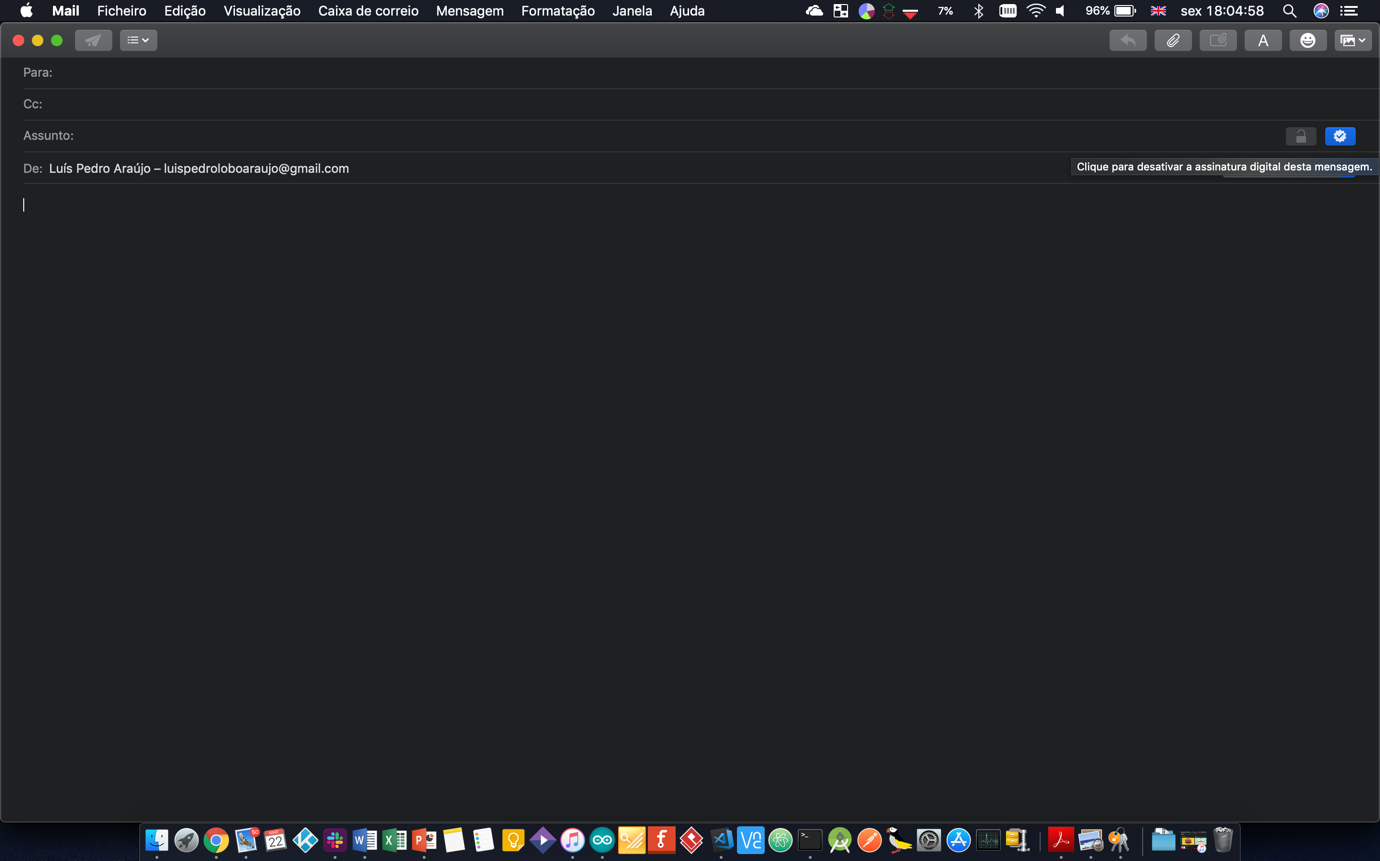


Figura - Assinatura de e-mail.

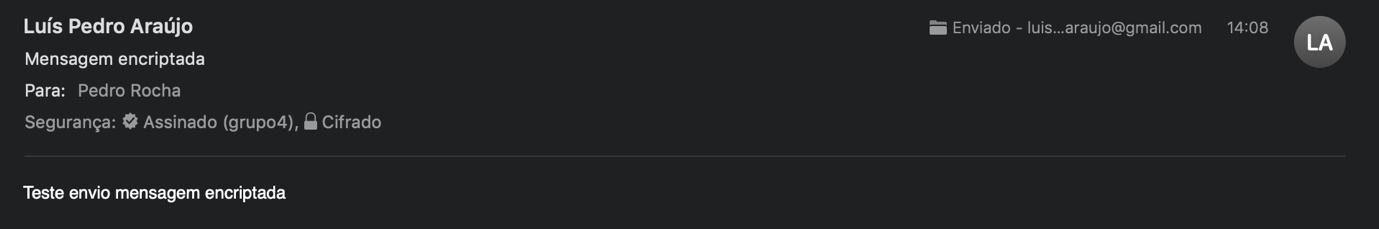


Figura - Envio de mensagem cifrada para José Pedro Rocha.

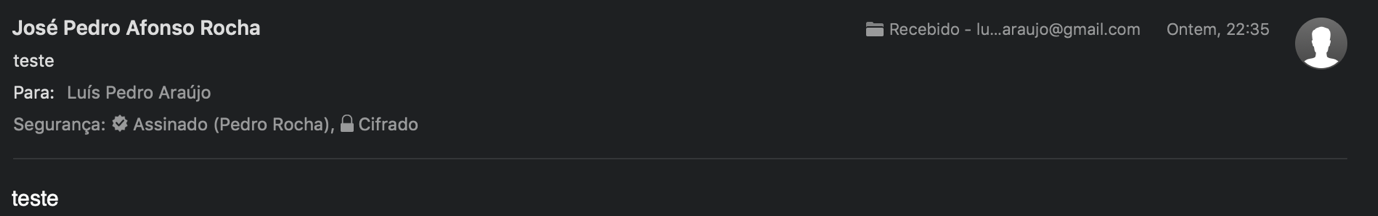


Figura - Mensagem cifrada recebida.

**José Pedro Rocha:**

No envio de e-mails cifrados, foi utilizado a aplicação Outlook, proveniente do Office365 instalado no sistema operativo Windows 10.

Neste caso, foi preciso importar os certificados já existentes para a conta mail associada ao Outlook e que estava definida nos certificados gerados.

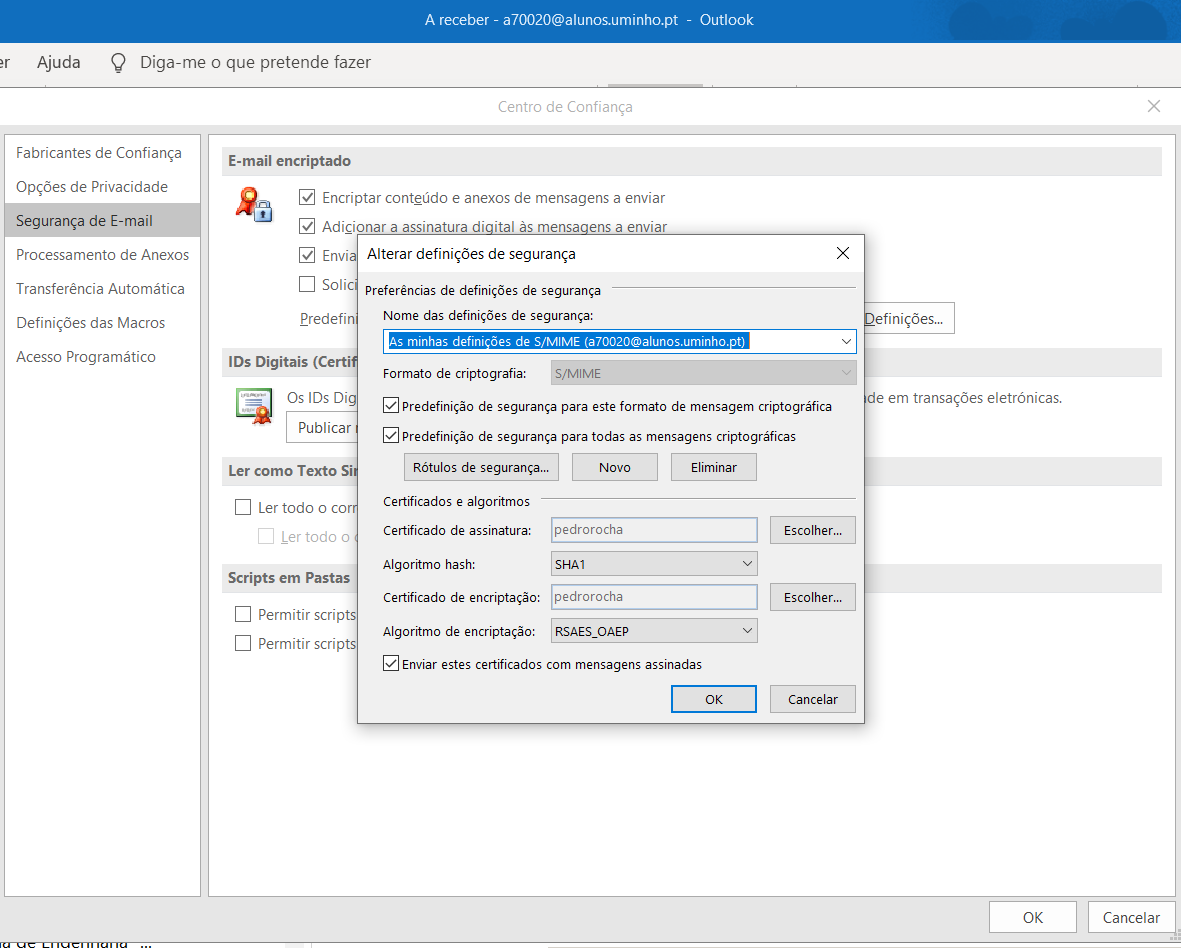


Figura - importação do certificado privado

Para o certificado público do destino, foi preciso adicionar o contacto e-mail e importar esse contacto específico.

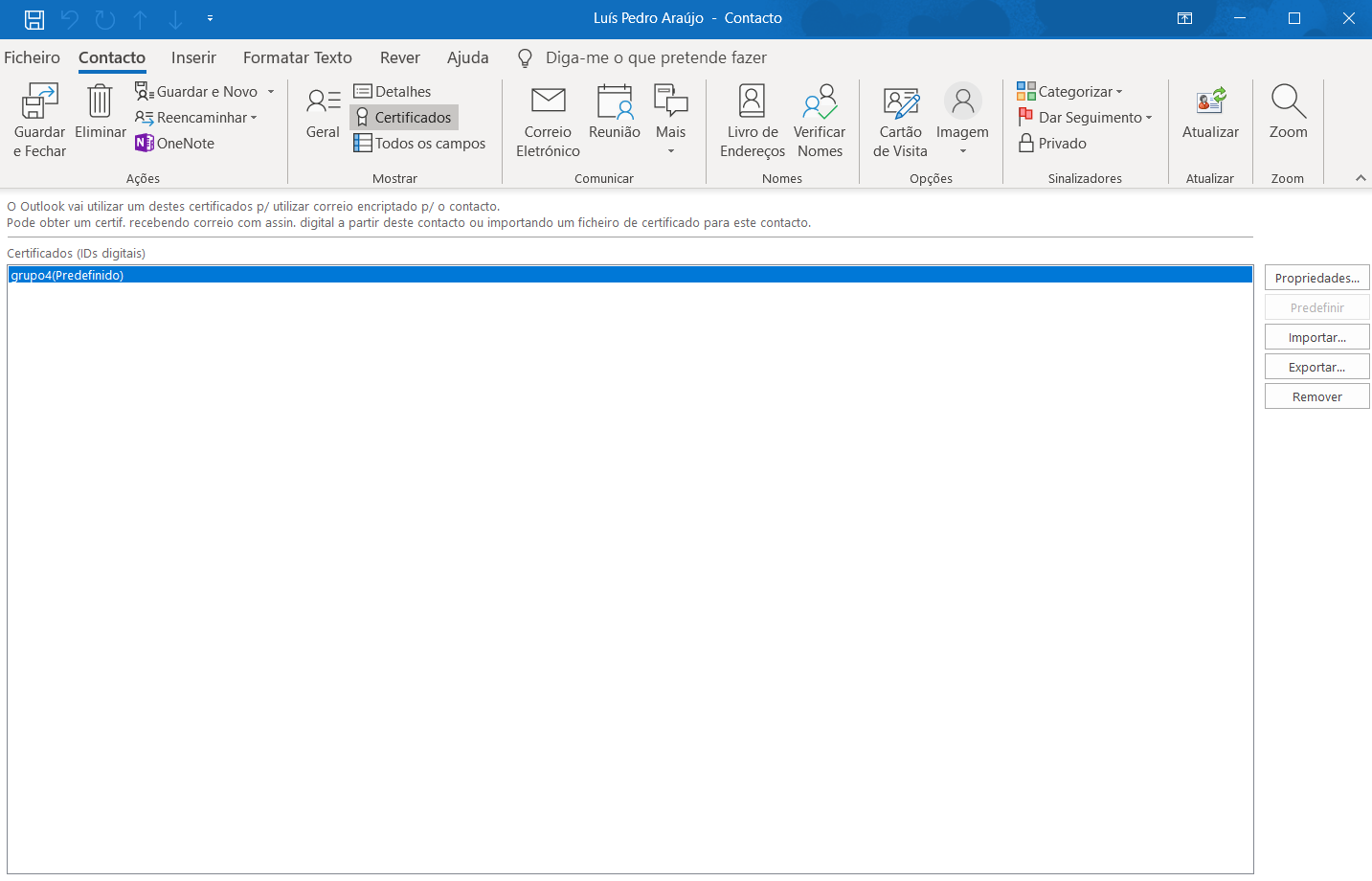


Figura – Importação do certificado público de luís araújo.

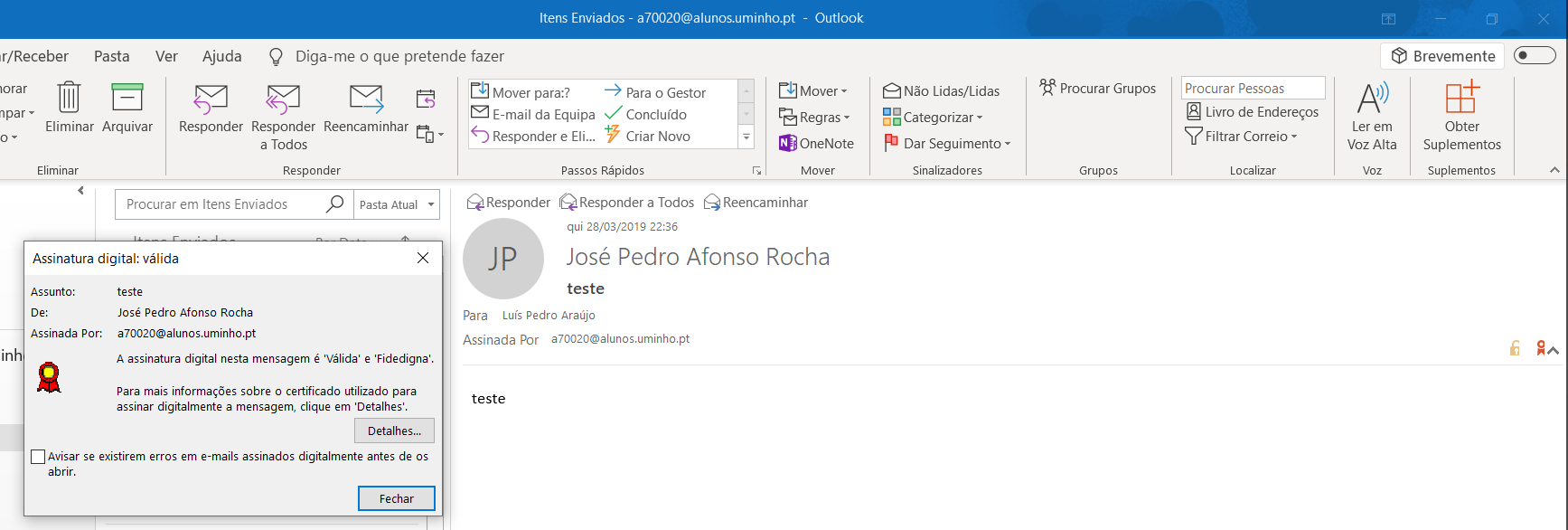


Figura – Email enviado - assinatura digital.

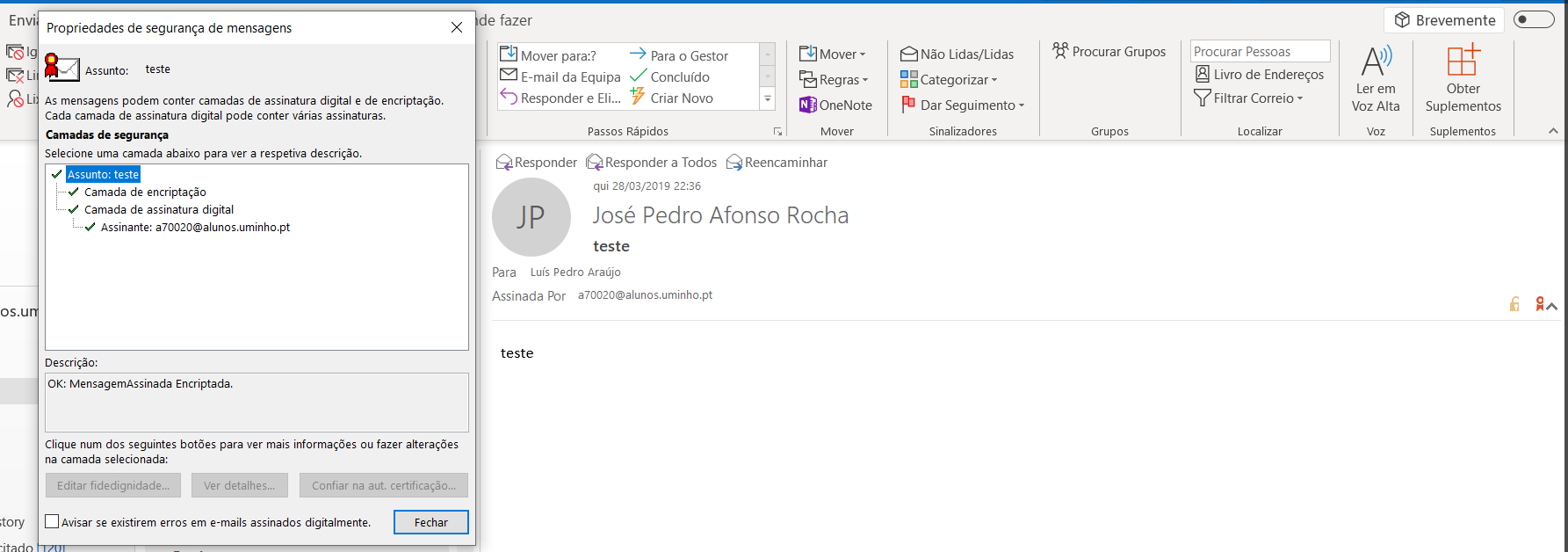


Figura - Email enviado - encriptação

### Mensagem entre grupos

Foi-nos ainda pedido que fossem estabelecidas relações de confiança entre CAs de colegas. Para tal, foram inseridos os certificados do colega para enviar a mensagem cifrada.

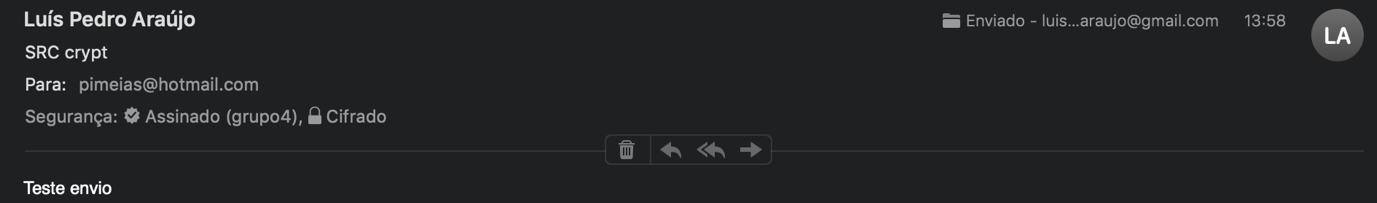


Figura - Mensagem enviada a outro colega.

## Revogação de um certificado

Nesta fase foi revogado o certificado do Luís Araújo, como é possível verificar nas figuras abaixo.

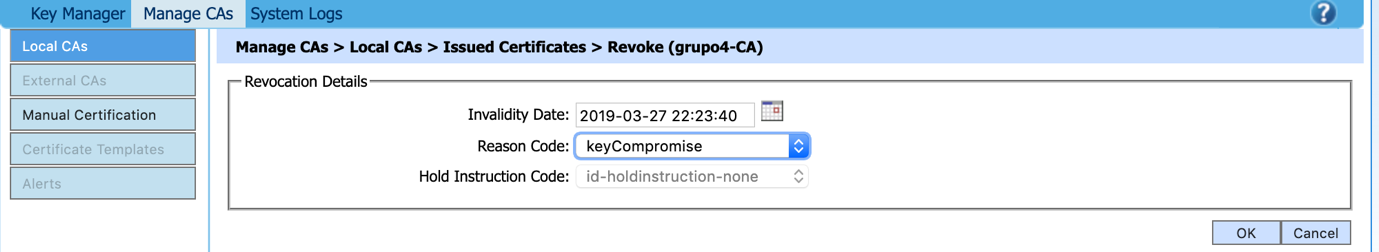


Figura - Revogação de certificado.



Figura - Lista de certificados e respetivos estados.

De seguida, foi retirada a CRL (Certificates Revogation List) atualizada do ADSS e inserida no Gestor de Certificados. Após a inserção da CRL atualizada, as mensagens recebidas já aparecem com uma assinatura inválida ou não-fidedigna, como podemos ver na figura abaixo.

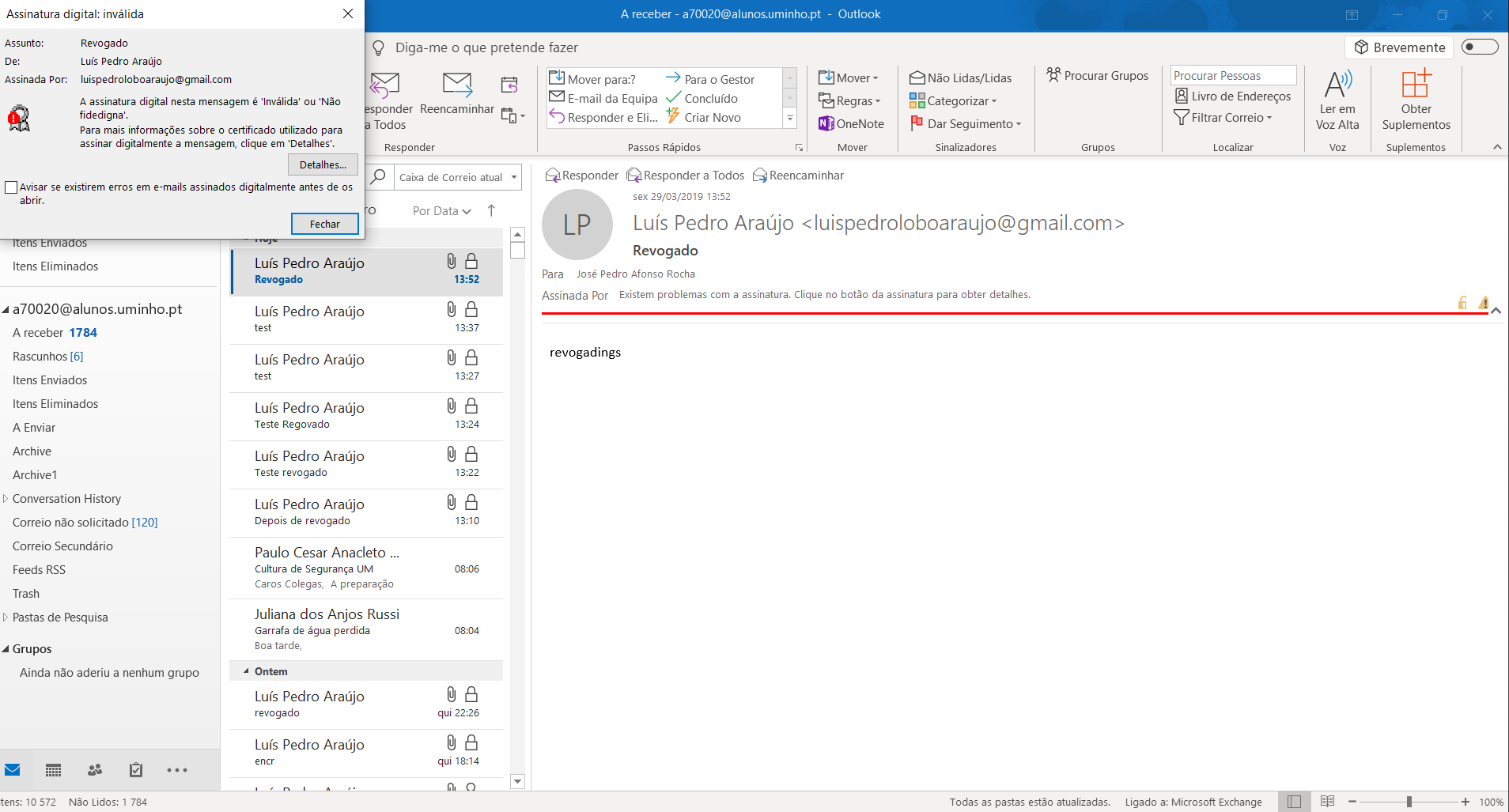
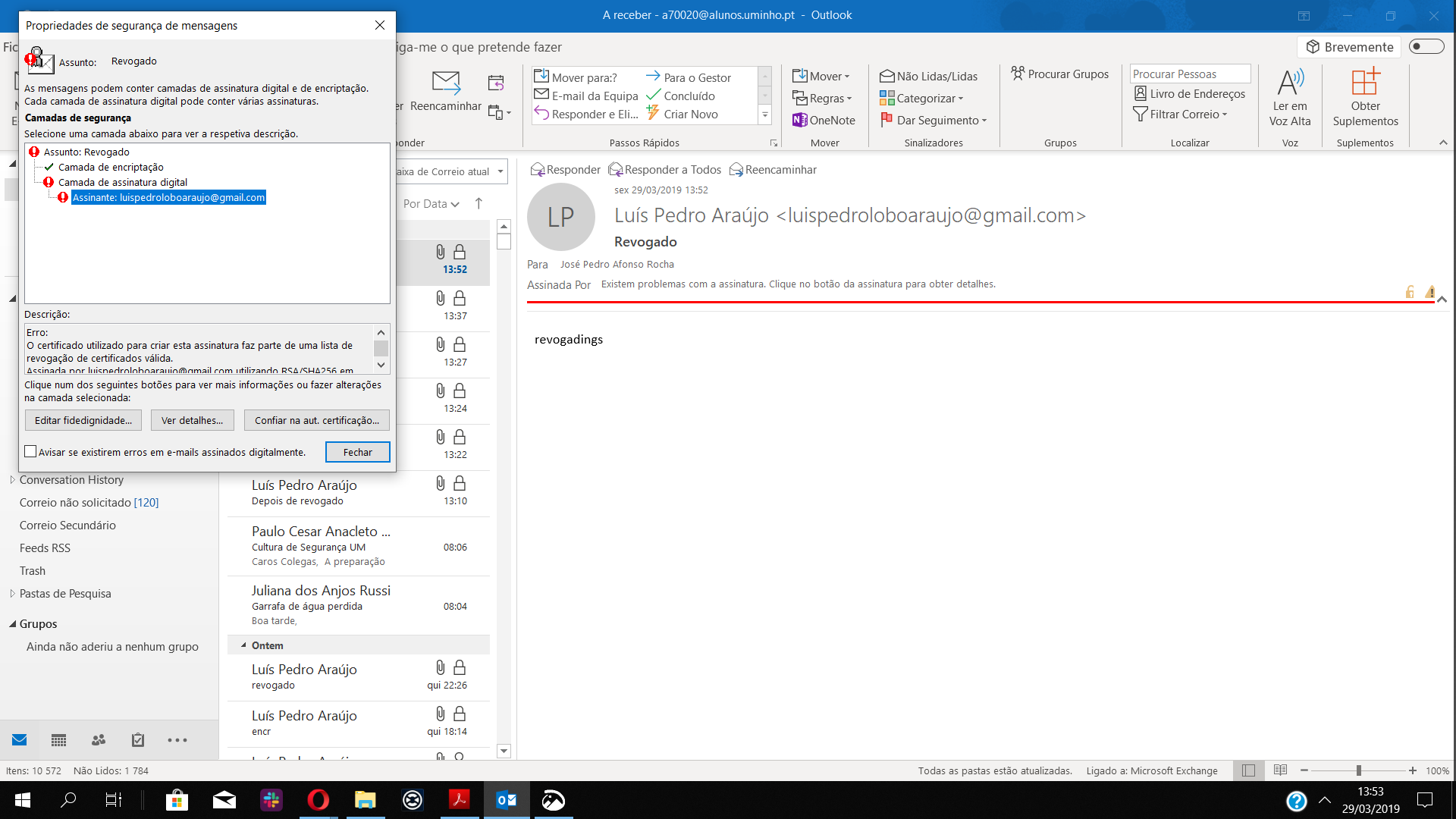


Figura - Mensagem depois da revogação do certificado.

# Conclusão

Com a realização deste trabalho, o grupo ficou com uma melhor noção das possibilidades e funcionalidades do uso de certificados digitais. Foi também compreendido o funcionamento das chaves privadas e chaves públicas, permitindo uma melhor utilização das ferramentas utilizadas no âmbito do projeto, OpenSSL e ADSS.

Com isto, o grupo verifica que todos os objetivos propostos no âmbito deste trabalho foram cumpridos. Como tal, foi compreendido e descrito o conceito de chave publica e privada e como estas são tipicamente implementadas e o reconhecimento das operações associadas à gestão das chaves.

Também foram ainda desenvolvidas competências na utilização do servidor ADSS, e como se utiliza certificados digitais para assinar e enviar mensagens com segurança.

Para além disto, foi compreendido o conceito e funcionamento das listas de certificados revogados, tendo o grupo experienciado o seu funcionamento quando revogou o certificado de um dos elementos.