Mac OS User Manual

Kit de Middleware Universal Bit4id

Índice

1. introdução

Este manual serve como um guia para concluir com êxito o processo de instalação do Bit4id Kit para o uso de cartões criptográficos e o procedimento para acessar e usar o aplicativo de gerenciamento. O Kit Bit4id consiste nos seguintes componentes:

- **Bit4id Middleware:** bibliotecas que permitem que qualquer aplicativo do sistema operacional opere com cartões criptográficos.

- **Bit4id PIN Manager:** aplicativo para gerenciamento de cartões, que permite operações como alterar PIN ou PUK, desbloquear PIN, obter informações sobre o cartão, importar ou exportar certificados ...

Este manual o guiará de maneira simples no processo de instalação e uso do Kit Bit4id.

1.1 Para quem é este documento?

Usuários finais, que vão usar cartões com chip em ambientes MacOS.

2. Antes de começar

Verifique se você tem:

- Um **leitor de cartão padrão** compatível com PC / SC que está conectado, instalado e configurado corretamente. Siga as instruções fornecidas pelo fabricante do leitor para verificar sua instalação e operação corretas.

- Tenha a **versão mais recente do Bit4id Kit** . Link para baixar a versão mais recente (http://cdn.bit4id.com/es/middleware.htm)
- Para poder instalar, é essencial ter **permissões de administrador** . Caso não os possua, a instalação será negada.

3. Instalação

Se necessário, você deve baixar e instalar os drivers para que o seu computador reconheça o leitor que você comprou. Para fazer isso, vá para a página oficial do fabricante do leitor.

Siga as instruções fornecidas pelo fabricante do leitor para verificar sua instalação e operação corretas.

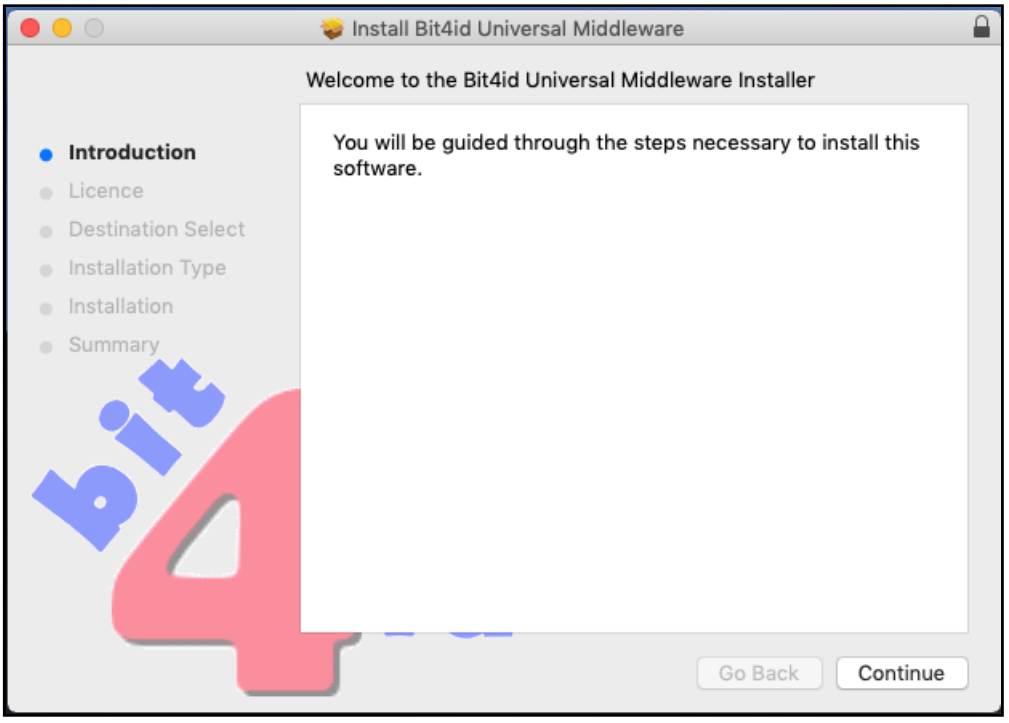
No caso de adquirir um leitor bit4id, se a sua versão do Mac OS tiver drivers PCSC instalados por padrão, não será necessário baixar nenhum driver. Caso contrário, devemos baixar e instalar os drivers do leitor (https://resources.bit4id.com/#/).

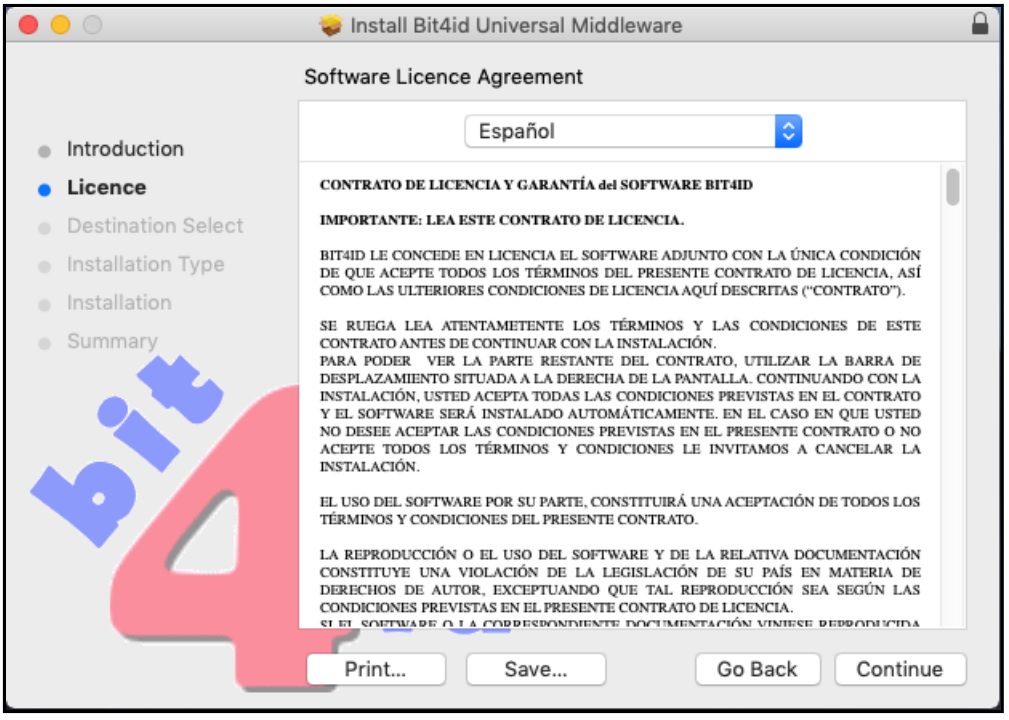
3.1 Assistente de Instalação do Gerenciador PKI

1. Vá para a pasta em que você baixou o arquivo

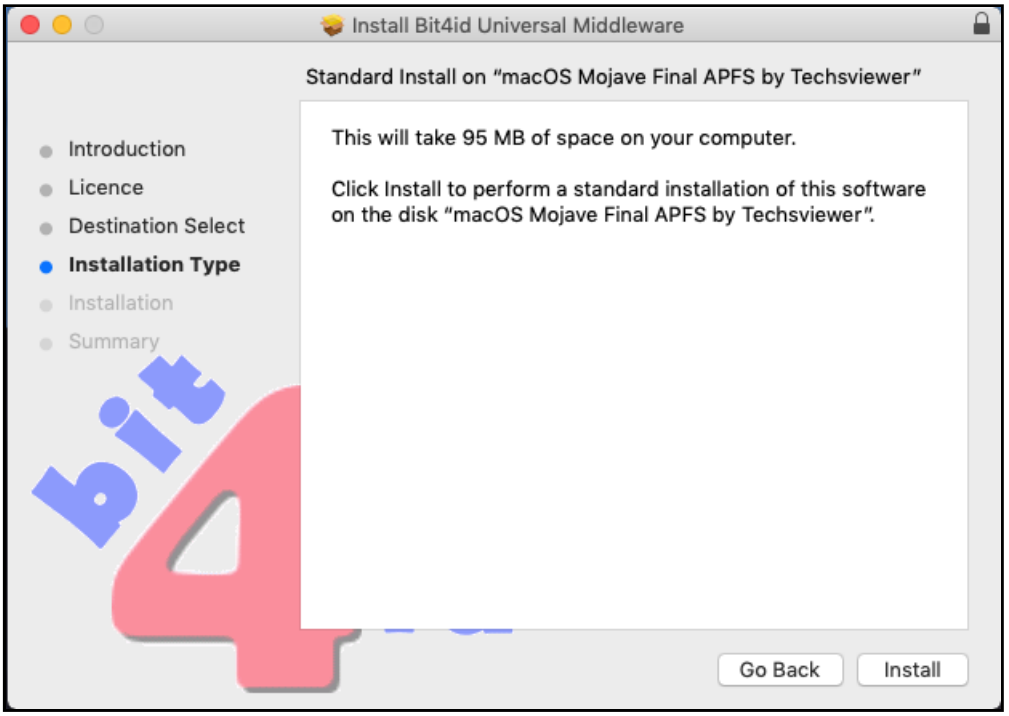
2. Execute o aplicativo

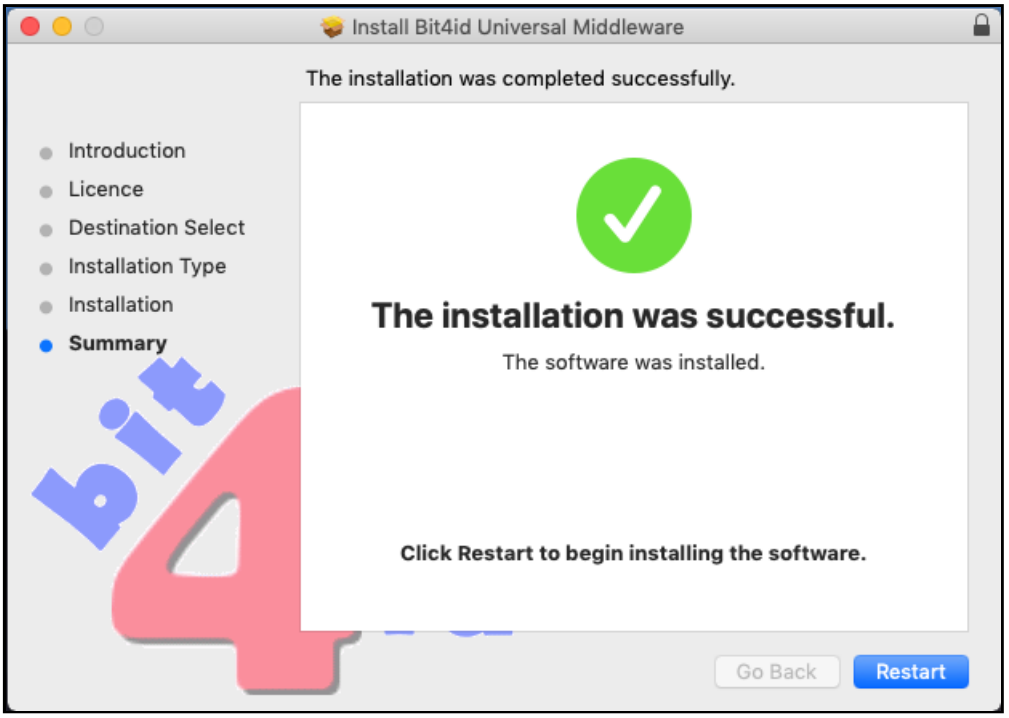
3. Siga as etapas do instalador.


Install Bit4id Universal Middleware
Welcome to the Bit4id Universal Middleware Installer
Introduction
Licence
Destination Select
Installation Type
Installation
Summary
You will be guided through the steps necessary to install this software.
Go Back
Continue


Install Bit4id Universal Middleware
Software Licence Agreement
Introduction
Licence
Destination Select
Installation Type
Installation
Summary
Español
CONTRATO DE LICENCIA Y GARANTÍA del SOFTWARE BIT4ID
IMPORTANTE: LEA ESTE CONTRATO DE LICENCIA.
BIT4ID LE CONCEDE EN LICENCIA EL SOFTWARE ADJUNTO CON LA ÚNICA CONDICIÓN DE QUE ACEPTE TODOS LOS TÉRMINOS DEL PRESENTE CONTRATO DE LICENCIA, ASÍ COMO LAS ULTERIORES CONDICIONES DE LICENCIA AQUÍ DESCRITAS ("CONTRATO").
SE RUEGA LEA ATENTAMETENTE LOS TÉRMINOS Y LAS CONDICIONES DE ESTE CONTRATO ANTES DE CONTINUAR CON LA INSTALACIÓN.
PARA PODER VER LA PARTE RESTANTE DEL CONTRATO, UTILIZAR LA BARRA DE DESPLAZAMIENTO SITUADA A LA DERECHA DE LA PANTALLA. CONTINUANDO CON LA INSTALACIÓN, USTED ACEPTA TODAS LAS CONDICIONES PREVISTAS EN EL CONTRATO Y EL SOFTWARE SERÁ INSTALADO AUTOMÁTICAMENTE. EN EL CASO EN QUE USTED NO DESEE ACEPTAR LAS CONDICIONES PREVISTAS EN EL PRESENTE CONTRATO O NO ACEPTE TODOS LOS TÉRMINOS Y CONDICIONES LE INVITAMOS A CANCELAR LA INSTALACIÓN.
EL USO DEL SOFTWARE POR SU PARTE, CONSTITUIRÁ UNA ACEPTACIÓN DE TODOS LOS TÉRMINOS Y CONDICIONES DEL PRESENTE CONTRATO.
LA REPRODUCCIÓN O EL USO DEL SOFTWARE Y DE LA RELATIVA DOCUMENTACIÓN CONSTITUYE UNA VIOLACIÓN DE LA LEGISLACIÓN DE SU PAÍS EN MATERIA DE DERECHOS DE AUTOR, EXCEPTUANDO QUE TAL REPRODUCCIÓN SEA SEGÚN LAS CONDICIONES PREVISTAS EN EL PRESENTE CONTRATO DE LICENCIA.
Print...
Save...
Go Back
Continue

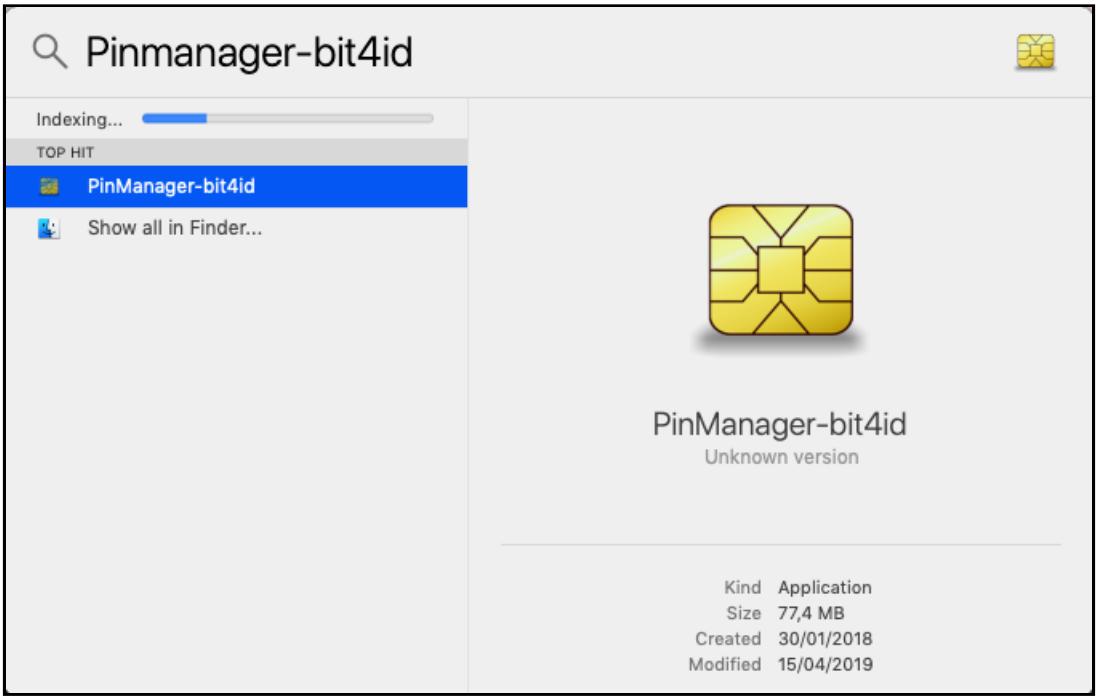

To continue installing the software you must agree to the terms of the software licence agreement.
Click Agree to continue or click Disagree to cancel the installation and quit the Installer.
Read Licence
Disagree
Agree



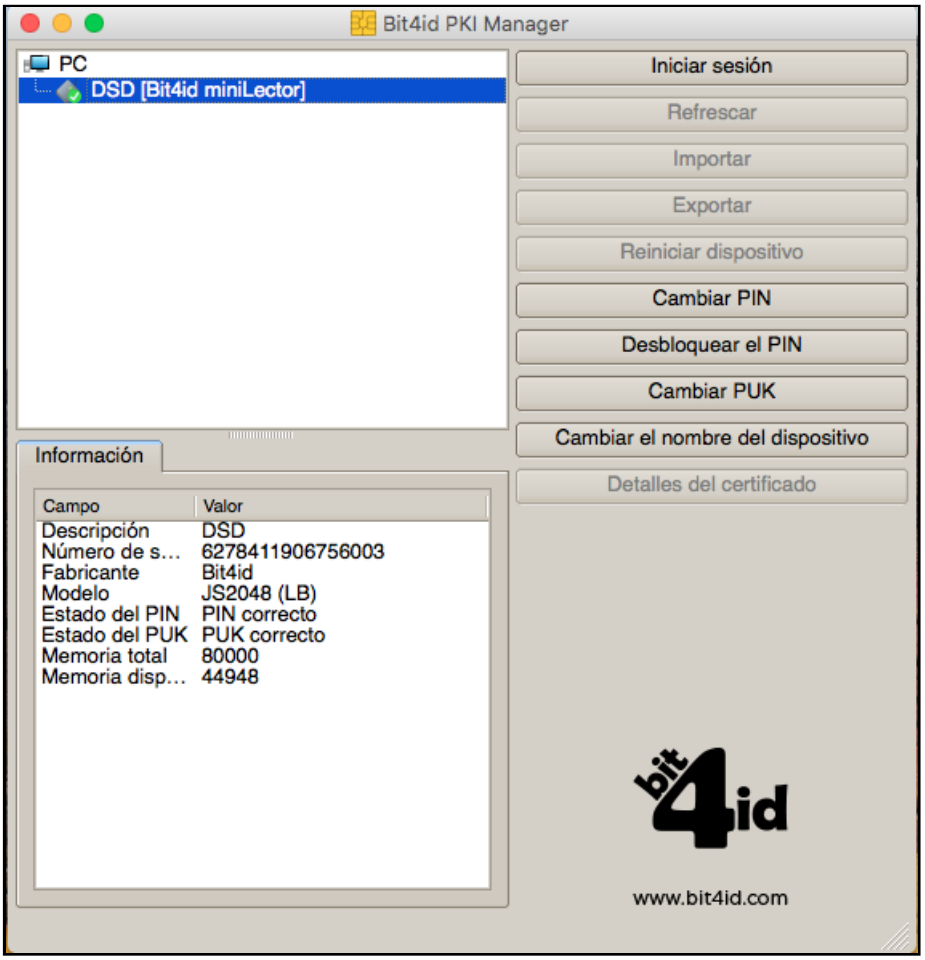


4. Quando a instalação do PKI Manager estiver concluída, reiniciaremos o computador.

5. Após o reinício, abrimos o aplicativo.



6. Com o aplicativo aberto, conectamos o leitor a uma porta USB e inserimos o cartão. Também podemos fazer esse processo, conectando o token em uma porta USB.



4. Problemas durante a instalação

Você pode ter versões mais antigas do aplicativo Card Management (Bit4id PKI Manager) instaladas no seu computador, portanto, você será solicitado a remover versões mais antigas antes de executar o instalador. Exclua essas versões e execute o instalador novamente.

Como desinstalar uma versão anterior do PKI Manager?

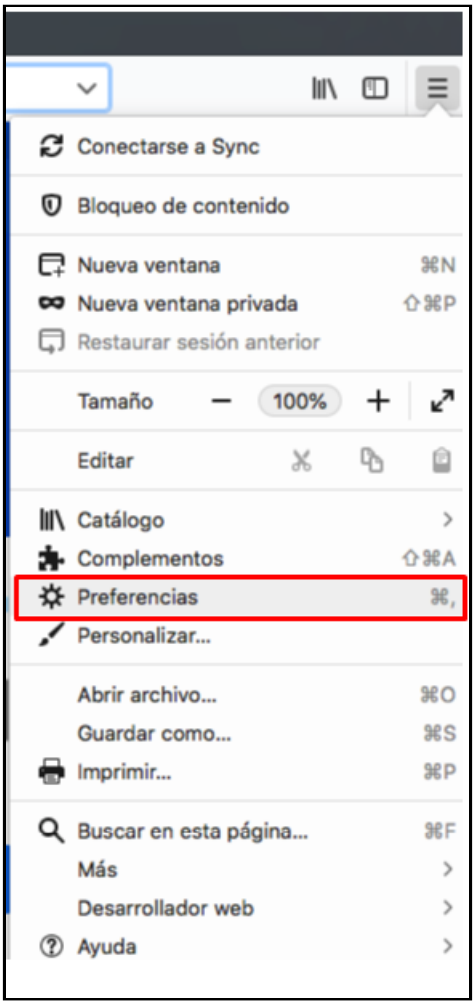
1. Abra o **Finder**
2. Vá para a guia **Aplicativos**
3. **Selecione o aplicativo** para desinstalar com um clique
4. Vá para **Arquivo** na parte superior da tela
5. Clique em: **Transferir para o lixo**

5. Configuração no Firefox

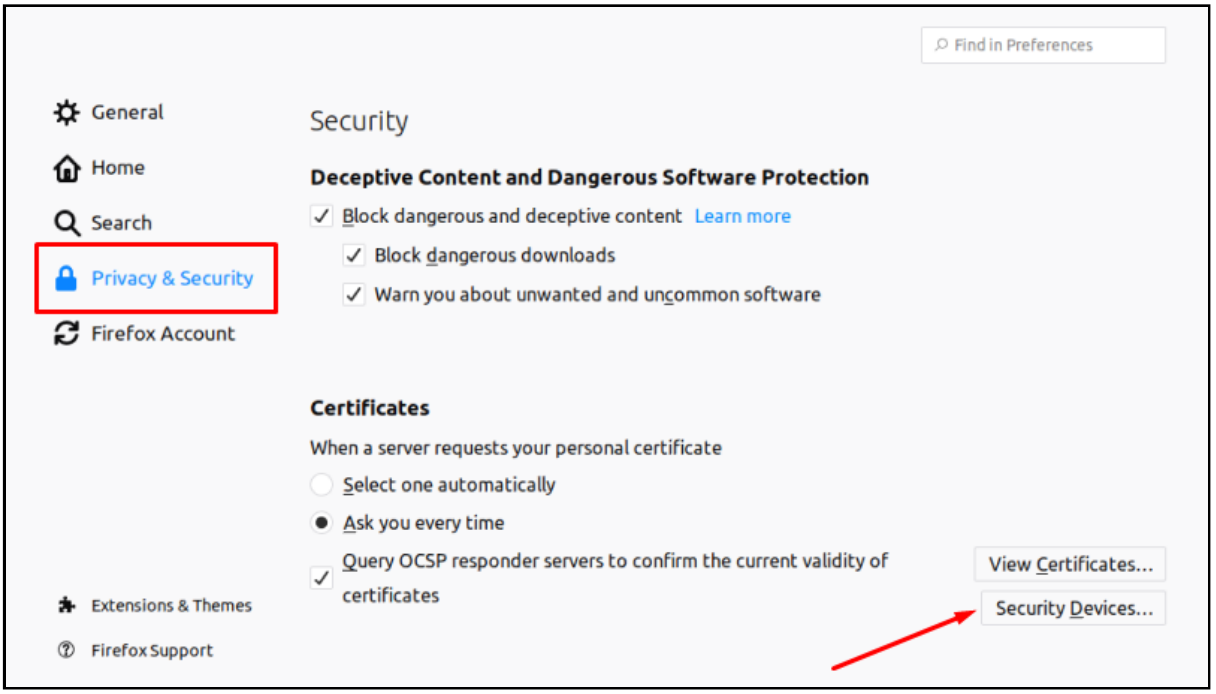
Para usar os certificados contidos no cartão inteligente no navegador Mozilla Firefox, é necessário incorporar as bibliotecas Bit4id Universal Middleware manualmente.

A incorporação automatizada de dispositivos de segurança no Firefox foi desativada desde a versão 3.5 como medida de segurança.

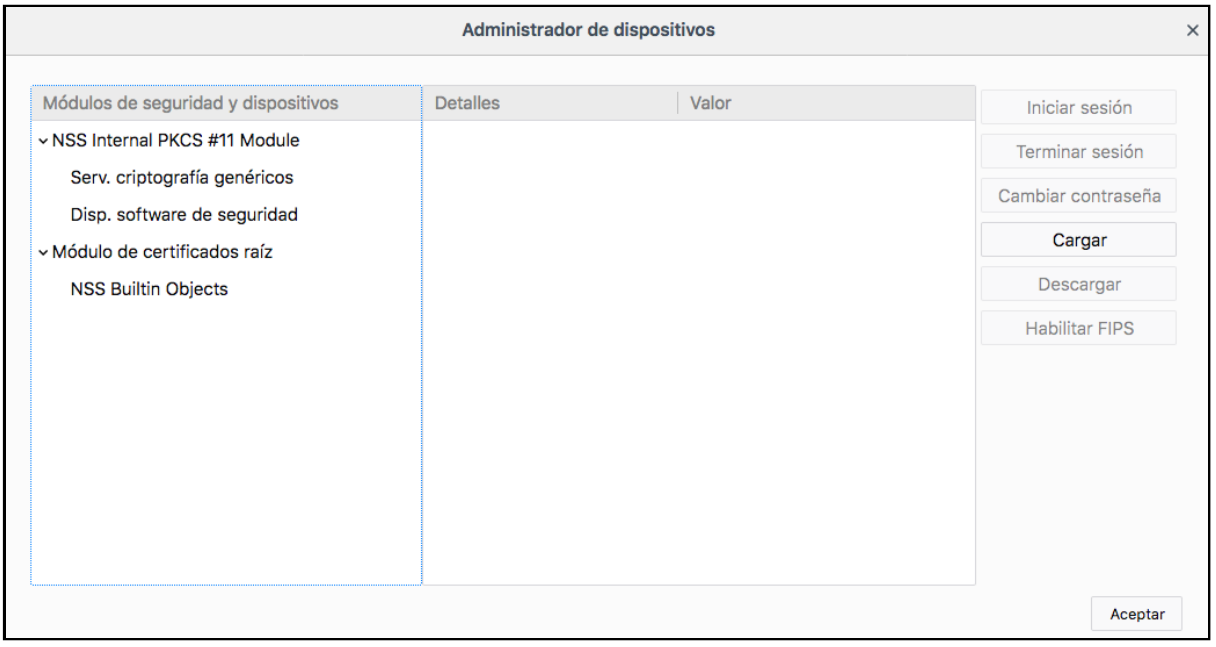
1. Abrimos o Mozilla Firefox, vamos para → Preferências ( )



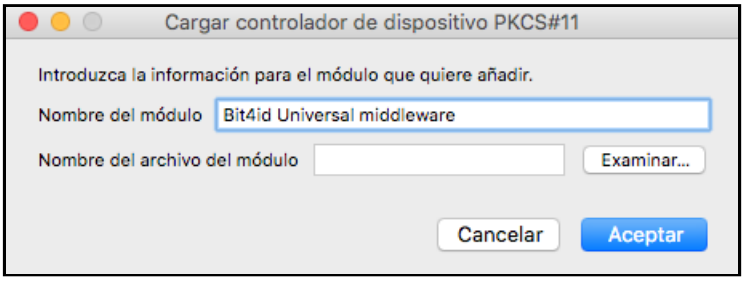
2. Na seção Privacidade e segurança, procuramos a seção de certificados e clicamos em Dispositivos de segurança



3. O Gerenciador de dispositivos será aberto. Clique em **Upload**



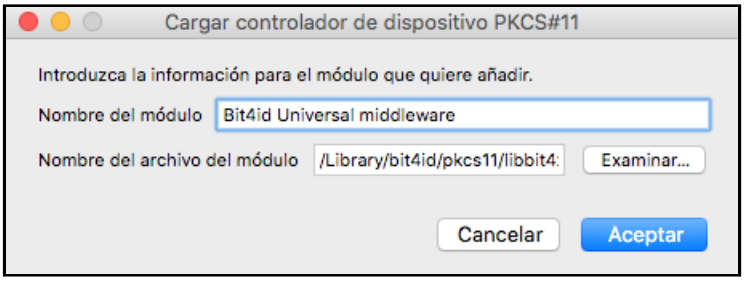
4. Quando essa janela é aberta, devemos procurar o driver de dispositivo PKCS # 11. Clicamos em **Procurar ...** para procurá-lo em nossa equipe.



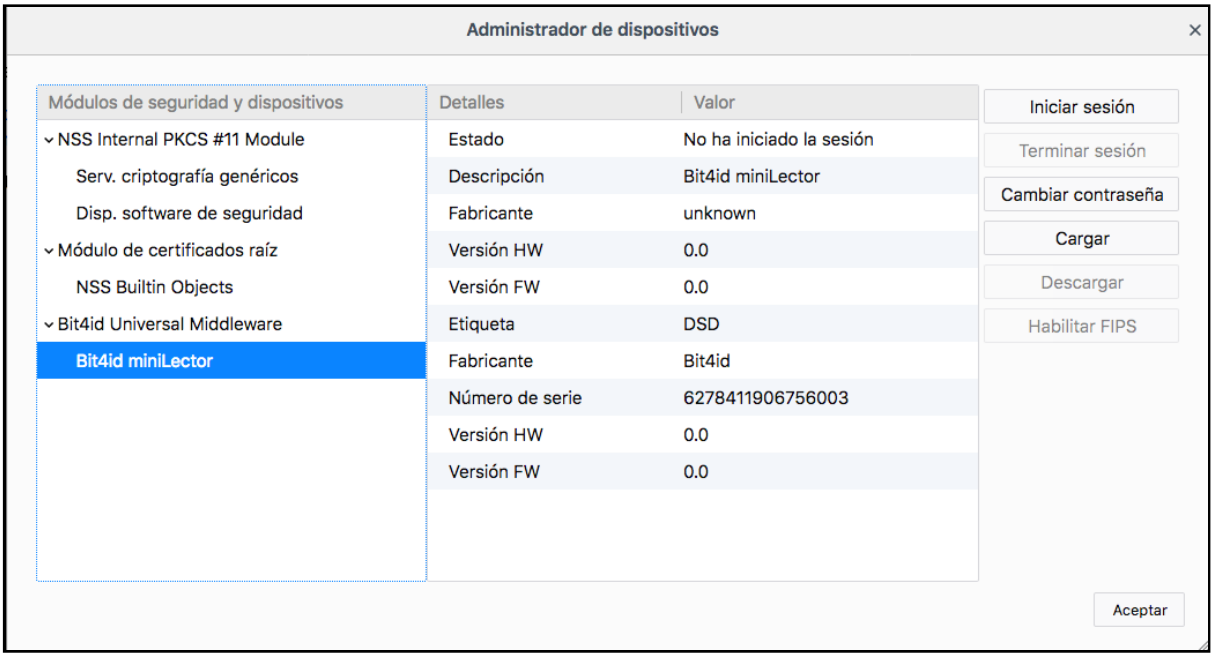
Na janela anterior, os seguintes dados devem ser inseridos:

- **Nome do módulo:** *Bit4id Universal Middleware*

- **Nome do arquivo do módulo:** /System/Library/Bit4id/pkcs11/libbit4ipki.dylib



Depois clique em OK. O módulo será incorporado com sucesso e a instalação no Firefox estará concluída.



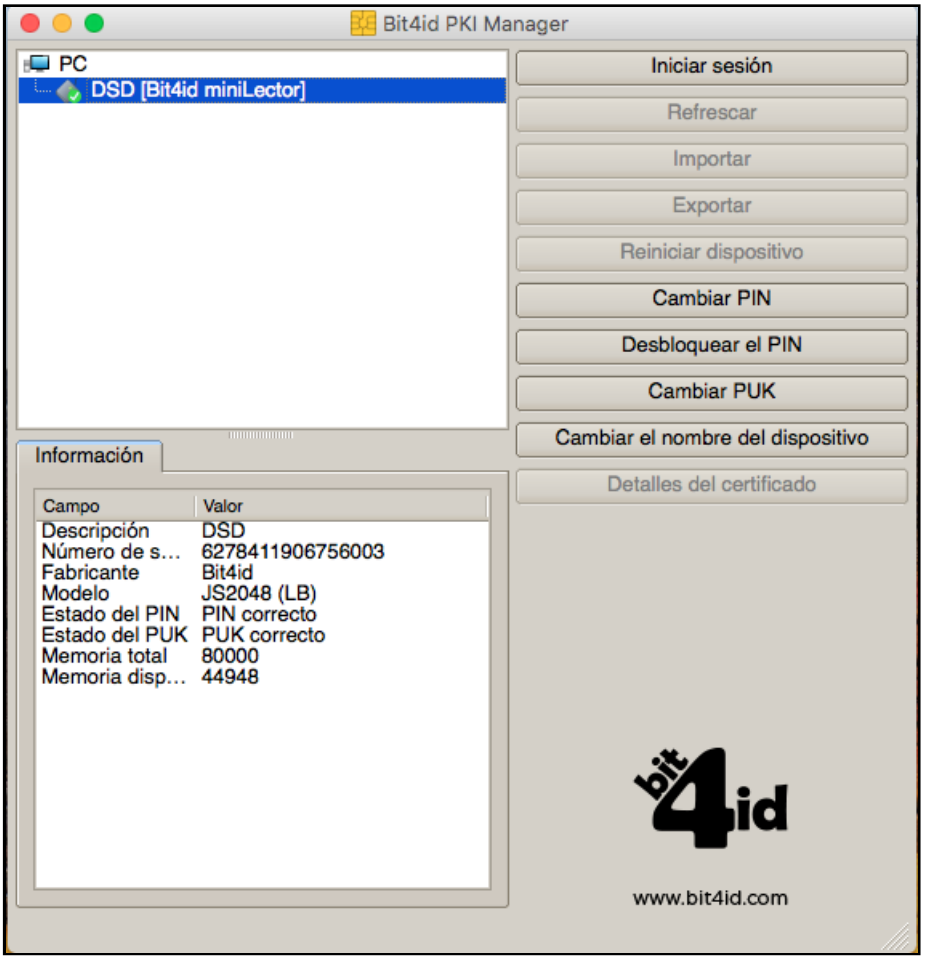
6. Antes de começar a usar o Kit Bit4id

O Bit4id PIN Manager requer um leitor de cartão inteligente compatível com PC / SC padrão que esteja conectado, instalado e configurado corretamente antes de começar.

Siga as instruções fornecidas pelo fabricante do leitor para verificar sua instalação e operação corretas.

7. Recursos

O aplicativo Bit4id PKI Manager possui várias funcionalidades disponíveis na tela principal.



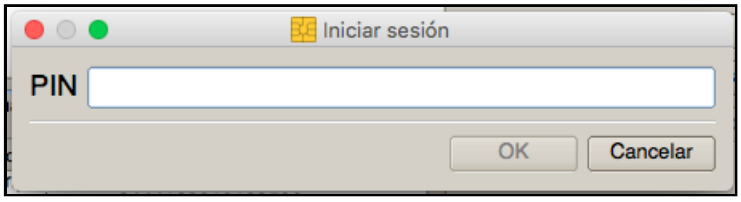
7.1 Tabela de recursos

Função	Descrição do produto
Iniciar sessão	Solicitação de PIN para acessar o conteúdo do cartão
Atualizar	Atualize o conteúdo do token / cartão para ver novos certificados
Importação / Exportação	Função para importar / exportar certificados no cartão
Reiniciar dispositivo	Função para deixar o cartão sem certificados ou chaves
Alterar PIN / PUK	Função para alterar o PIN / PUK do cartão
Desbloquear PIN	Função para desbloquear o PIN do cartão através do PUK do cartão
Renomear dispositivo	Defina o nome sob o qual o dispositivo aparece
Detalhes do certificado	Janela pop-up exibindo informações sobre certificados e sua cadeia de confiança

Função	Descrição do produto
Informações	Janela localizada na parte inferior do aplicativo que mostra informações sobre o cartão (modelo, número de série, identificação do fabricante e etiqueta)
Copiar certificados	Copie os certificados no Windows CSP

- **Iniciar sessão**

Para acessar qualquer funcionalidade oferecida pelo software, você deve inserir o PIN do cartão

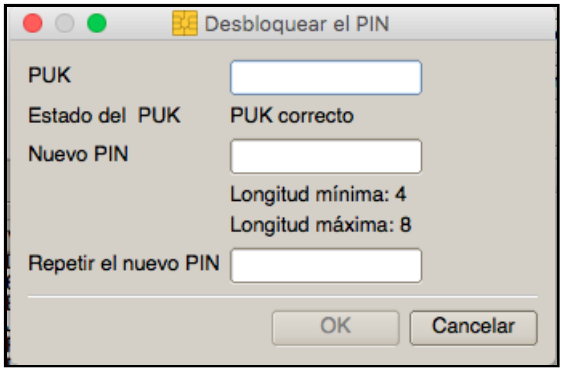


- **Alterar PIN**

Para alterar o PIN, digite o PIN do cartão e insira o novo PIN. O novo PIN deve ter entre 4 e 8 dígitos alfanuméricos.

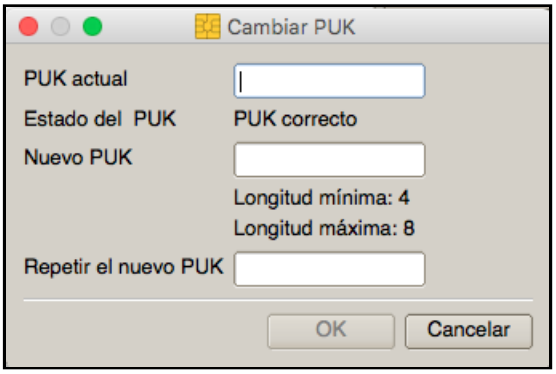
- **Desbloquear PIN**

Para desbloquear o PIN, insira o PUK do cartão e insira o novo PIN. O novo PIN deve ter entre 4 e 8 dígitos alfanuméricos.



- **Alterar o PUK**

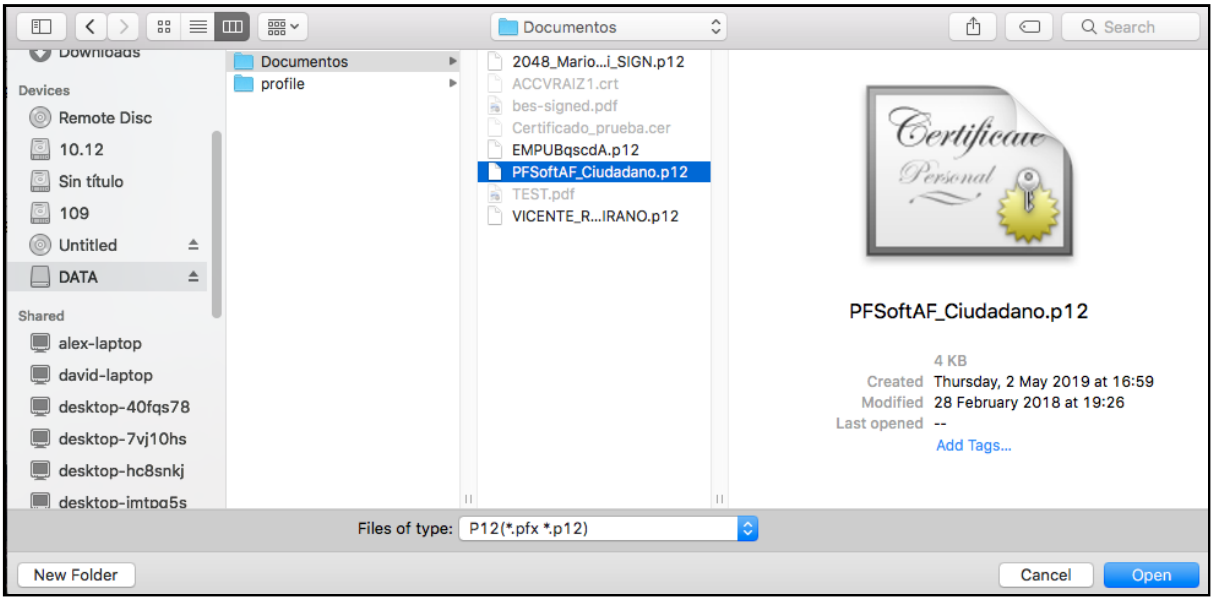
Digite o PUK antigo no cartão e o novo PUK. O novo PUK deve ter entre 4 e 8 dígitos alfanuméricos.



- **Importar**

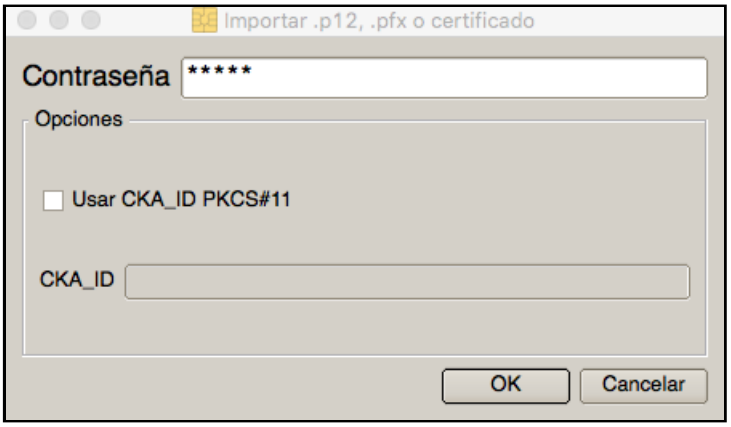
Esta opção permite a importação de certificados no cartão. Os formatos aceitos para importar certificados em cartões .p12 ou .pfx, pois esses formatos incluem a chave privada do certificado, essencial para a execução de operações criptográficas.

Para iniciar a importação, primeiro selecione o certificado em seu local, conforme mostrado na imagem a seguir:



Depois que o certificado for selecionado, pressione "Abrir":

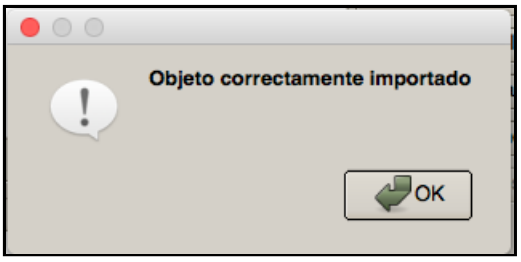
O sistema solicitará a senha do arquivo PFX ou P12 (certificado e chave privada do mesmo) que você deseja importar e que contém seu certificado e par de chaves. Insira-o e conclua as opções de importação conforme sua conveniência, onde:



- Importar certificados sem par de chaves associado: permite importar toda a hierarquia de certificação incluída no arquivo PFX ou P12. Recomendamos NÃO VERIFICAR esta opção.

- Defina CKA_ID do PKCS # 11: identificador que certos aplicativos usam ao exibir o certificado. Recomendamos inserir um valor de identificação útil, por exemplo, pedro_firma, pedro_acceso, pedro_ciprado, etc.

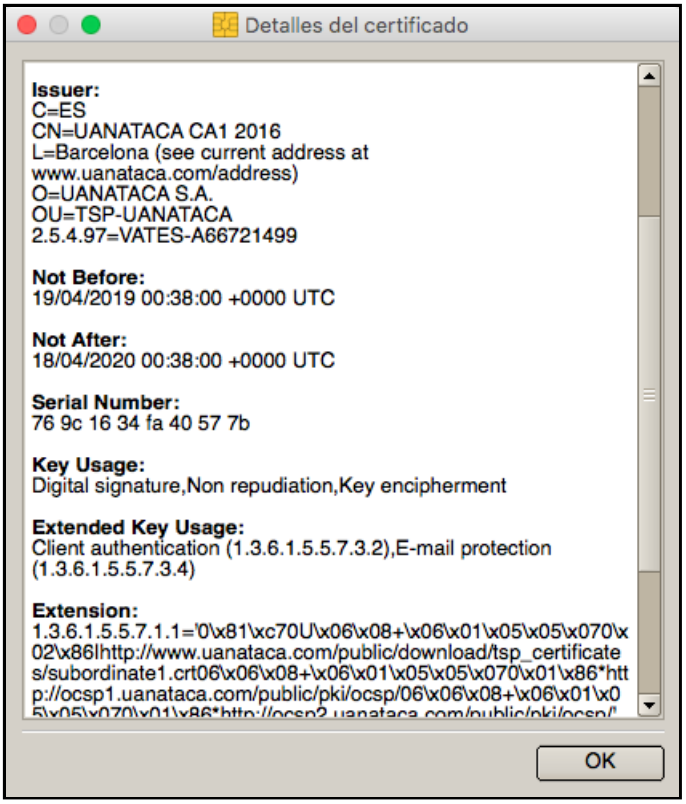
E a importação do certificado está concluída:



Caso deseje verificar se o certificado foi salvo corretamente, lembre-se de que você pode revisar todos os certificados armazenados no cartão através da opção "Visualizar" do Bit4id PKI Manager.

- **Detalhes do certificado**

Depois que o PIN do cartão é inserido, podemos ver os certificados que estão dentro dele. Na janela pop-up que mostra o aplicativo, podemos ver informações



- **Informações do cartão**

Fornece informações detalhadas do cartão: modelo, número de série, fabricante e etiqueta.
O suporte (support@bit4id.com) pode solicitar essas informações para saber o tipo de cartão que você está usando.

8. Perguntas frequentes

Posso combinar números e letras para o número PIN do cartão?
Sim, não há problema, desde que o novo PIN tenha entre 4 e 8 dígitos.

Existe um número máximo de entradas de PIN, caso você tenha alguma dúvida e não se lembre do meu número PIN? Quando o cartão pode ser bloqueado?
Se você digitar o código PIN mais de três vezes incorretamente, ele será bloqueado. Entre em contato com o Bit4id para desbloqueá-lo.

Existe um máximo de inserções PUK para tentar desbloquear o PIN? O que acontece se o cartão estiver bloqueado?
Se você inserir o código PUK mais de três vezes com erro, ele bloqueará. Por razões de segurança, o cartão está completamente bloqueado. Entre em contato com Bit4id.

9. Glossário

Autoridade de Certificação: É a entidade confiável, responsável por emitir e revogar os certificados eletrônicos usados na assinatura eletrônica. A Autoridade de Certificação, por si só ou através da intervenção de uma Autoridade de Registro, verifica a identidade do requerente de um certificado antes de sua emissão ou, no caso de certificados emitidos com a condição de revogada, elimina a revogação dos certificados por verifique essa identidade.

Expiração do certificado digital: O certificado digital tem um período de validade indicado no mesmo certificado. Geralmente são 2 anos, embora por lei uma validade de até 5 anos seja permitida. Depois que o certificado expirar, os serviços oferecidos pela Administração que exigem uma assinatura eletrônica não poderão ser utilizados, e qualquer assinatura eletrônica feita a partir desse momento não será válida.

Certificado digital: documento em mídia de computador emitida e assinada pela Autoridade de Certificação, que garante a identidade de seu proprietário.

Certificado reconhecido: certificado emitido por um provedor de serviços de certificação que atende aos requisitos estabelecidos na lei em relação à verificação da identidade e de outras circunstâncias dos solicitantes e à confiabilidade e garantias dos serviços de certificação que prestam, de acordo com com o disposto no Capítulo II do Título II da Lei 59/2003, de 19 de dezembro, sobre Assinatura Eletrônica.

Assinatura eletrônica: conjunto de dados, em formato eletrônico, anexado a outros dados eletrônicos ou funcionalmente associados a eles, usado como um meio para identificar formalmente o autor ou autores do documento que os coleta. Existem 3 tipos de assinatura eletrônica: assinatura eletrônica simples, avançada e reconhecida.

Assinatura eletrônica simples: conjunto de dados, em formato eletrônico, anexado a outros dados.

Assinatura eletrônica avançada: assinatura eletrônica que permite que o assinante seja identificado e qualquer alteração subseqüente nos dados assinados seja detectada, que é vinculada exclusivamente ao signatário e aos dados a que se refere e que foram criados por meio de que o signatário pode manter seu controle. controle exclusivo.

Assinatura eletrônica reconhecida: uma assinatura eletrônica reconhecida é uma assinatura eletrônica avançada baseada em um certificado reconhecido e gerada por um dispositivo de criação de assinatura segura. A assinatura eletrônica reconhecida terá o mesmo valor em relação aos dados gravados em formato eletrônico que a assinatura manuscrita em relação aos registrados em papel.

Função hash: é uma operação executada em um conjunto de dados de qualquer tamanho, para que o resultado obtido seja outro conjunto de dados de tamanho fixo, independentemente do tamanho original, e que tenha a propriedade de ser associado exclusivamente aos dados iniciais, ou seja, é impossível encontrar duas mensagens diferentes que geram o mesmo resultado ao aplicar a Função Hash.

Hash ou impressão digital: resultado de tamanho fixo obtido após a aplicação de uma função de hash em uma mensagem e que tem a propriedade de ser associado exclusivamente aos dados iniciais.

Integridade: Integridade é a qualidade que um documento ou arquivo possui que não foi alterado e que também permite verificar que nenhuma manipulação ocorreu no documento original.

Listas de revogação de certificados ou listas de certificados revogadas: lista que contém exclusivamente os relacionamentos de certificados revogados ou suspensos (não expirados).

Não repúdio: O emissor que assina eletronicamente um documento não pode negar que enviou a mensagem original, pois é atribuível ao emissor por meio da chave privada que somente ele conhece e é obrigado a guardar. O não repúdio também permite verificar quem participou de uma transação.

O não repúdio ou inalienabilidade é um serviço de segurança intimamente relacionado à autenticação e que permite provar a participação das partes em uma comunicação. A diferença essencial com a autenticação é que a primeira ocorre entre as partes que estabelecem a comunicação e o serviço de não repúdio ocorre na frente de uma terceira parte

Fornecedor de serviços de certificação ou PSC: pessoa singular ou coletiva que emite certificados eletrônicos ou presta outros serviços em relação à assinatura eletrônica. Consulte Autoridade de Certificação.

PIN: sequência de caracteres que permitem acesso aos certificados. Número de identificação pessoal, às vezes chamado de PIN.

PUK: sequência de caracteres que permitem alterar ou desbloquear o PIN. Chave de desbloqueio pessoal.

Renovação: a renovação consiste em solicitar um novo certificado por meio de um certificado atual que está prestes a expirar. Dessa forma, antes da expiração de um certificado, a renovação pode ser solicitada e isso implica que um novo certificado válido seja emitido.

Revogação: cancelamento definitivo de um certificado digital a pedido do assinante ou por iniciativa da Autoridade de Certificação em caso de dúvida sobre a segurança das chaves. A revogação é um estado irreversível. Você pode solicitar a revogação de um certificado após uma situação de suspensão ou por vontade das pessoas autorizadas a solicitá-lo. Da mesma forma, no caso de um certificado suspenso, se o período máximo de suspensão tiver passado, se o certificado não tiver sido ativado, ele será revogado permanentemente. Quando o organismo de certificação revoga ou suspende um certificado, deve declará-lo nas Listas de certificados revogados (CRL), para tornar esse fato público. Essas listas são públicas e devem estar sempre disponíveis.

Cartão inteligente: qualquer cartão com circuitos integrados que permitem a execução de certa lógica programada.