**KIT DE EXEMPLOS WCF – ANBIMA**

**DOCUMENTAÇÃO DE APOIO – INSTALAÇÃO DE CERTIFICADOS DIGITAIS**

Logo Desenvolvimento**Controle de Revisão e Aprovação**

Registro de Alterações

| **Data** | **Autor** | **Versão** | **Referência da Alteração** |
| --- | --- | --- | --- |
| 26/07/2010 | Leandro Cardoso | 1.0 | Versão Inicial |
|  |  |  |  |

Revisão

| **Data** | **Nome** | **Cargo** | **Versão Aprovada** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

Propriedades do Documento

| **Item** | **Descrição** |
| --- | --- |
| **Título** | ANBIMA - Kit de exemplos WCF – Documentação de Apoio – Instalação de Certificados Digitais |
| **Autor** | Leandro Cardoso de Almeida |
| **Data de Criação** | 26/07/2010 |
| **Última Atualização** |  |

# Índice

[Introdução 4](#_Toc268518875)

[Certificados Digitais 4](#_Toc268518876)

[Instalação do Certificado Digital 5](#_Toc268518877)

[Verificação do Certificado Digital 8](#_Toc268518878)

[Utilização do Certificado Digital 10](#_Toc268518879)

[Referências Bibliográficas 10](#_Toc268518880)

# Introdução

Este documento tem por objetivo descrever os principais passos para a instalação de um certificado digital X509 para utilização em uma aplicação Windows, de forma que sirva como fonte de consulta para desenvolvedores e analistas.

Por se tratar de um tema muito extenso e complexo, este documento não pretende esgotar as alternativas, definições e caminhos para a utilização de certificados, mas sim de fornecer uma maneira segura para este fim.

# Certificados Digitais

A certificação digital é um tipo de tecnologia de identificação que permite que transações eletrônicas dos mais diversos tipos sejam feitas considerando sua integridade, sua autenticidade e sua confidencialidade, de forma a evitar que adulterações, interceptações ou outros tipos de fraude ocorram.

Um certificado digital é um documento eletrônico com assinatura digital que contêm dados como nome do utilizador (que pode ser uma pessoa, uma empresa, uma instituição, etc.), entidade emissora, prazo de validade e chave pública.

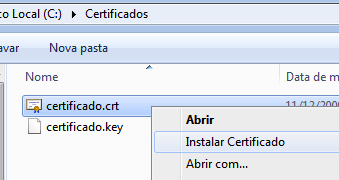
Para poder ser utilizado, o certificado digital deve estar instalado no repositório de certificados do Windows – local que mantém todos os certificados do computador e do usuário, e deve ser e ter sua cadeia de certificados adjacentes válida.

O processo para importar e validar o certificado digital será descrito na próxima sessão.

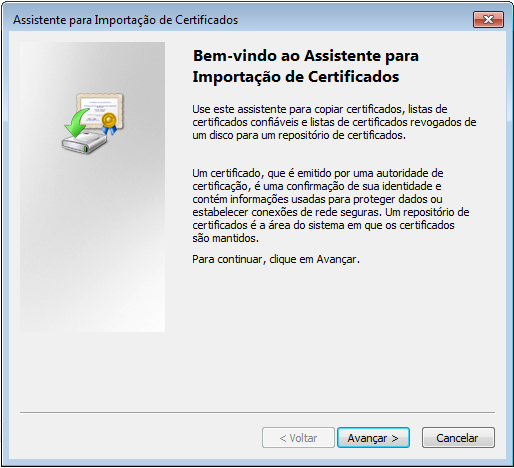
# Instalação do Certificado Digital

Para instalar um certificado no repositório de certificados do Windows, realize os passos descritos abaixo:

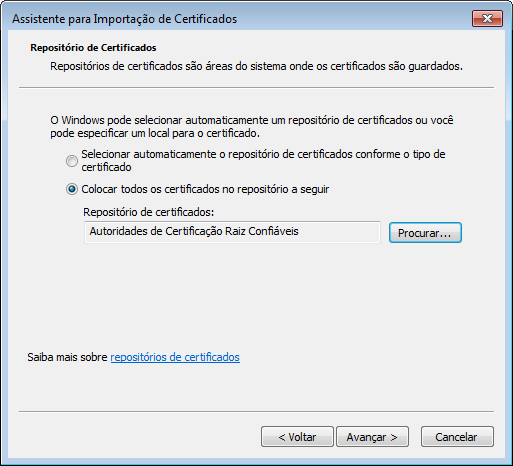
1. Localize, no Windows Explorer o arquivo do certificado desejado, clique com o botão direito sobre o arquivo e selecione a opção Instalar Certificado;



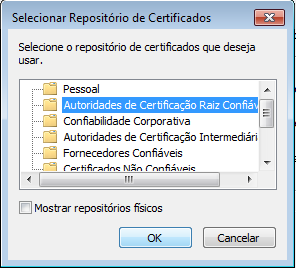
1. Na janela a seguir, clique em Avançar;



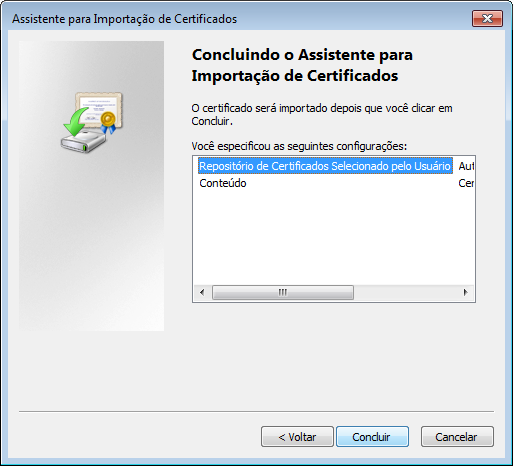
1. Dependendo do tipo do certificado, ele poderá ser instalado para a conta de Usuário (CurrentUser) ou para o Computador (LocalMachine) automaticamente, e sua localização pode ser definida através da opção “Colocar todos os certificados no repositório a seguir”.



1. Clique no botão Procurar e, em seguida selecione o repositório “Autoridades de Certificação Raiz Confiáveis”.



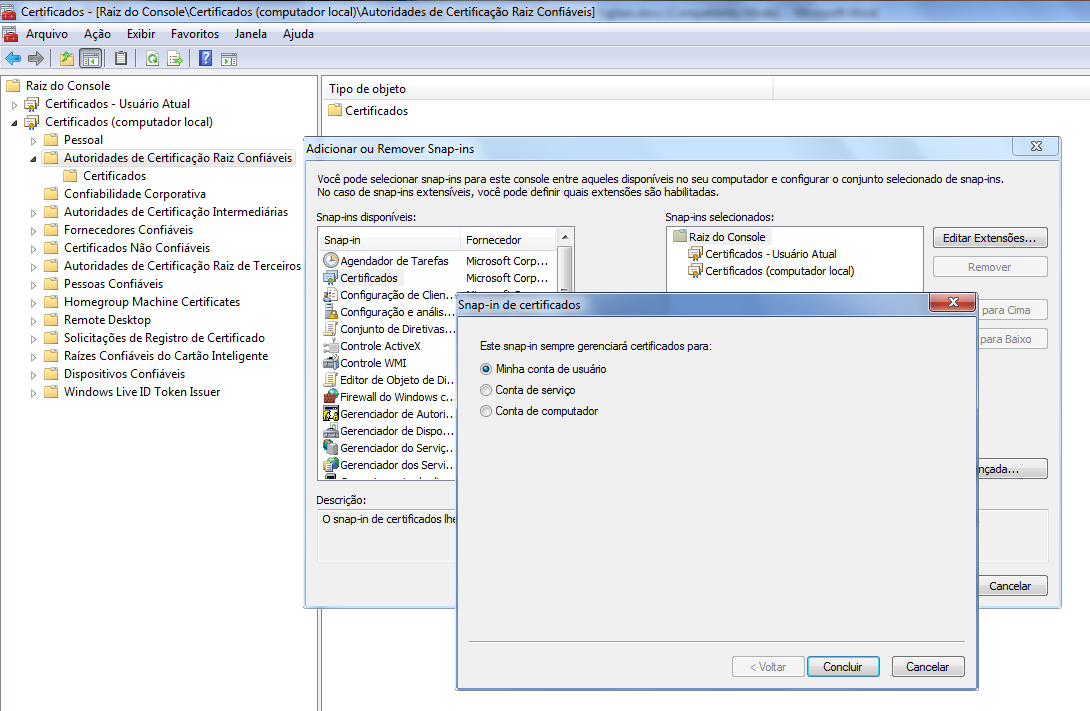
1. Conclua a instalação



# Verificação do Certificado Digital

Para a utilização do certificado, é necessário verificar se o caminho da cadeia do certificado é válido. Se o certificado não possuir em sua cadeia toda a extensão válida, o certificado não será válido.

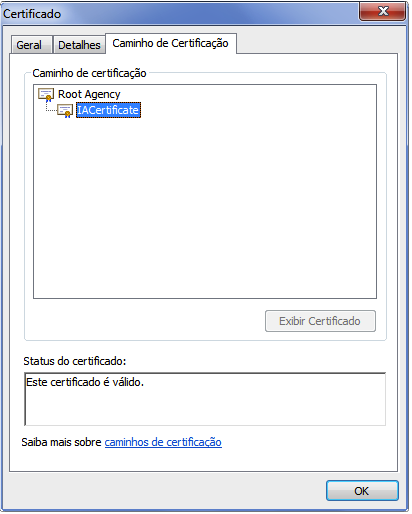
Para isso, é necessário o uso do Console de Gerenciamento (mmc.exe), e adicionar os snap-in de Certificados para contas pessoais e contas de computador, como na imagem abaixo:



O certificado digital instalado anteriormente pode ser localizado no snap-in Certificados – Usuário Atual, repositório Autoridades de Certificação Raíz Confiáveis.

Depois de localizado, suas propriedades podem ser visualizadas com um duplo-clique sobre o certificado.

Para verificar a validade da cadeia de emissão do certificado, clique na guia Caminho de Certificação e veja se todos os emissores de certificados são válidos na cadeia, como na imagem abaixo:



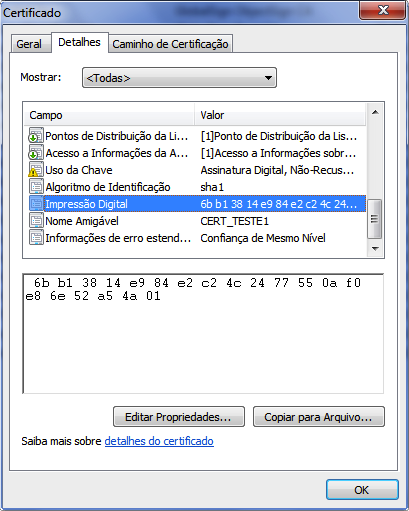
Se o certificado e/ou sua cadeia adjacente não for válida, o certificado pode ser instalado novamente – como no procedimento já descrito – no repositório para “Pessoas Confiáveis”, ou apenas copiando e colando o certificado do repositório “Autoridades de Certificação Raiz Confiáveis” para o repositório “Pessoas Confiáveis”.

# Utilização do Certificado Digital

Para utilizar um certificado instalado no computador em um aplicativo, é necessária a sua correta identificação.

Problemas de identificação de certificado podem gerar transtornos desnecessários, como utilização do certificado errado ou a não identificação.

Certificados são localizados através do tipo de conta onde ele foi instalado (Usuário ou Computador) e pelo seu repositório, e pode ser pesquisado de diversas maneiras. Por este motivo, recomendamos a pesquisa de certificado pela sua impressão digital (thumbprint), encontrado na figura abaixo:



# Referências Bibliográficas

<http://www.iti.gov.br>