

# Tag "retConsStatServ" não encontrado pela função "Load CDSFrom XML"

## **Tag "retConsStatServ" não encontrado pela função "Load CDSFrom XML"**

Essa rejeição irá ocorrer quando alguma informação genérica do XML não foi preenchida corretamente. Existe um conjunto de regras básicas para o preenchimento dos campos da NF-e que devem ser compreendidos, portanto conhecer a estrutura básica da NF-e e os campos existentes vai ajudar a identificar essas falhas e sanar os erros de preenchimento das tags. Estudar o leiaute da NF-e é um requisito essencial!

### **Ação sugerida:**

1 - Em Opções da Internet, aba Avançadas, desmarcar as 5 últimas opções

2 - Instalação da Cadeia dos Certificados

a) Fazer o download e instalar a cadeia de certificados abaixo:

<http://acraiz.icpbrasil.gov.br/credenciadas/RAIZ/ICP-Brasilv5.crt>

b) Executar o comando certmgr.msc, o gerenciador do certificados será aberto;

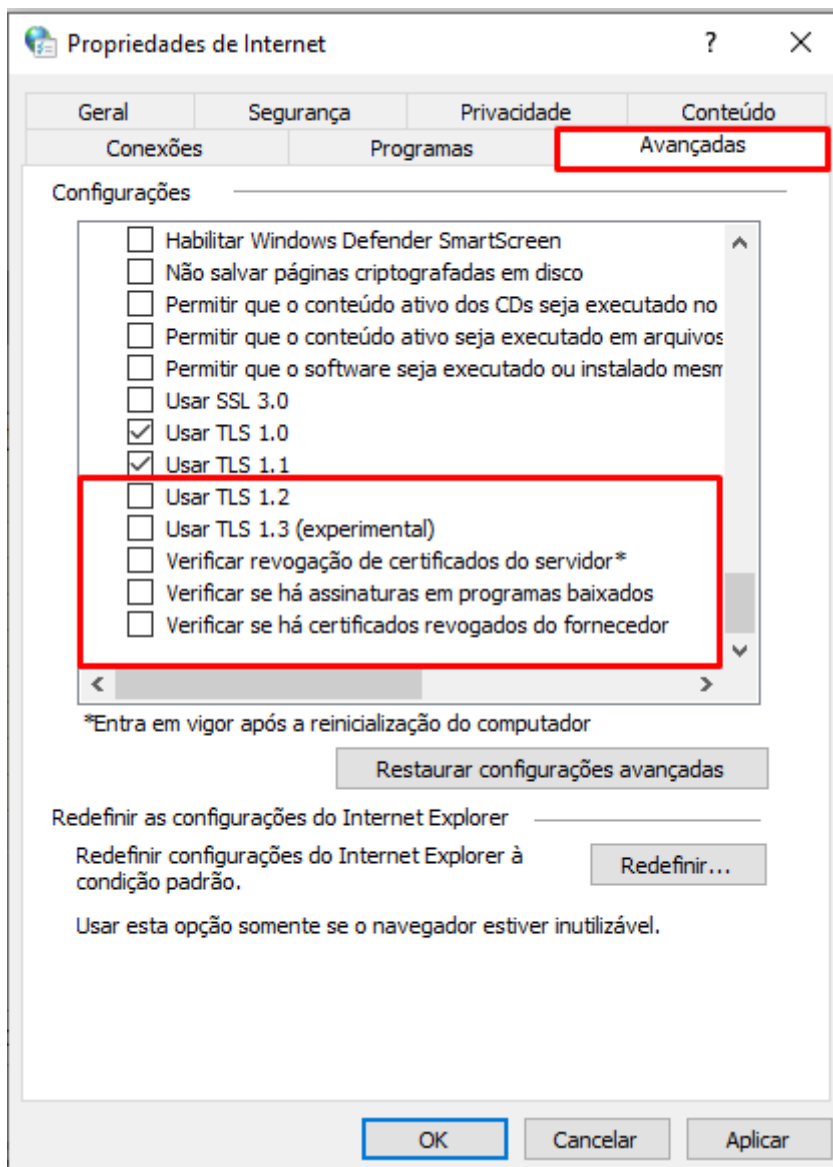
c) Clicar na pasta "Autoridades de Certificação Raiz Confiáveis", irá abrir a pasta "certificados" do lado esquerdo, clique nesta pasta "certificados" com o botão direito ir em todas as tarefas e clicar em importar, e faça o processo de instalação.

d) Abrir a pasta "certificados", clicar no certificado que você baixou no passo a passo 1 com o botão direito, ir em propriedades, e clicar na opção "ativar todas as finalidades deste certificado", aplicar e dar ok.

Pronto.

### **Correção:**

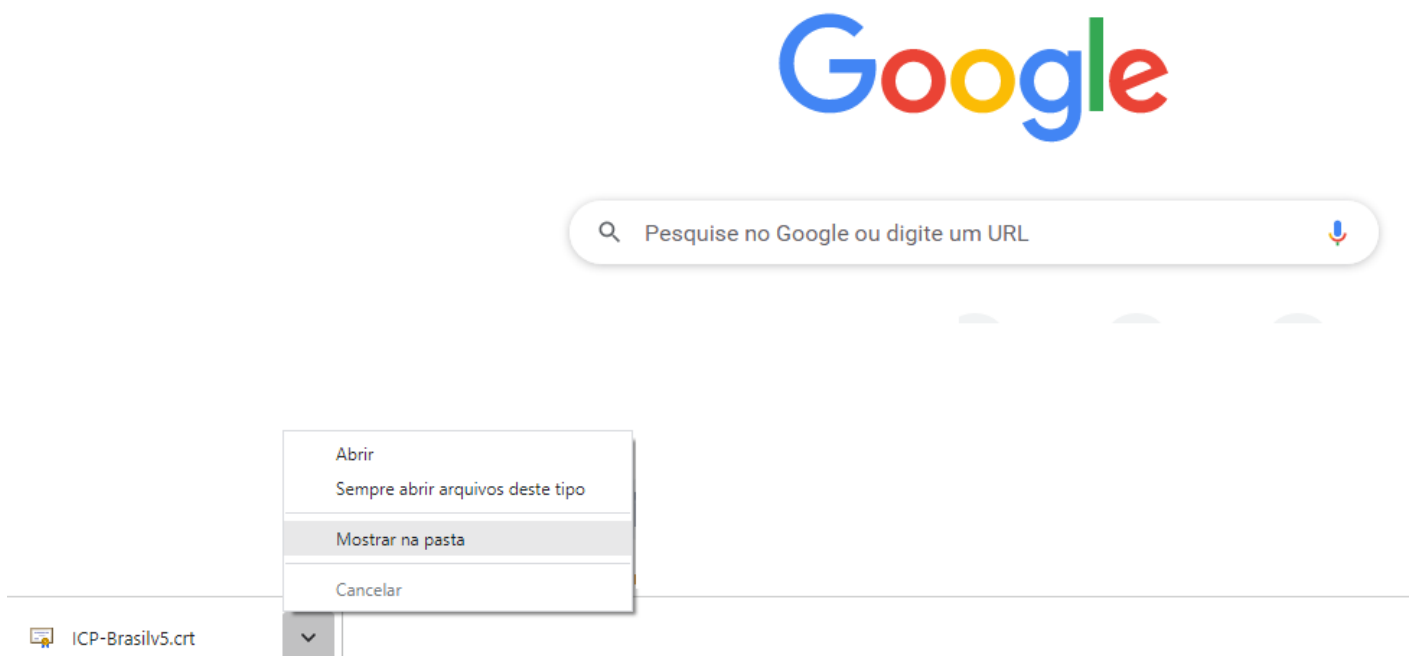
1 - Em Opções da Internet, aba Avançadas, desmarcar as 5 últimas opções



## 2 - Instalação da Cadeia dos Certificados

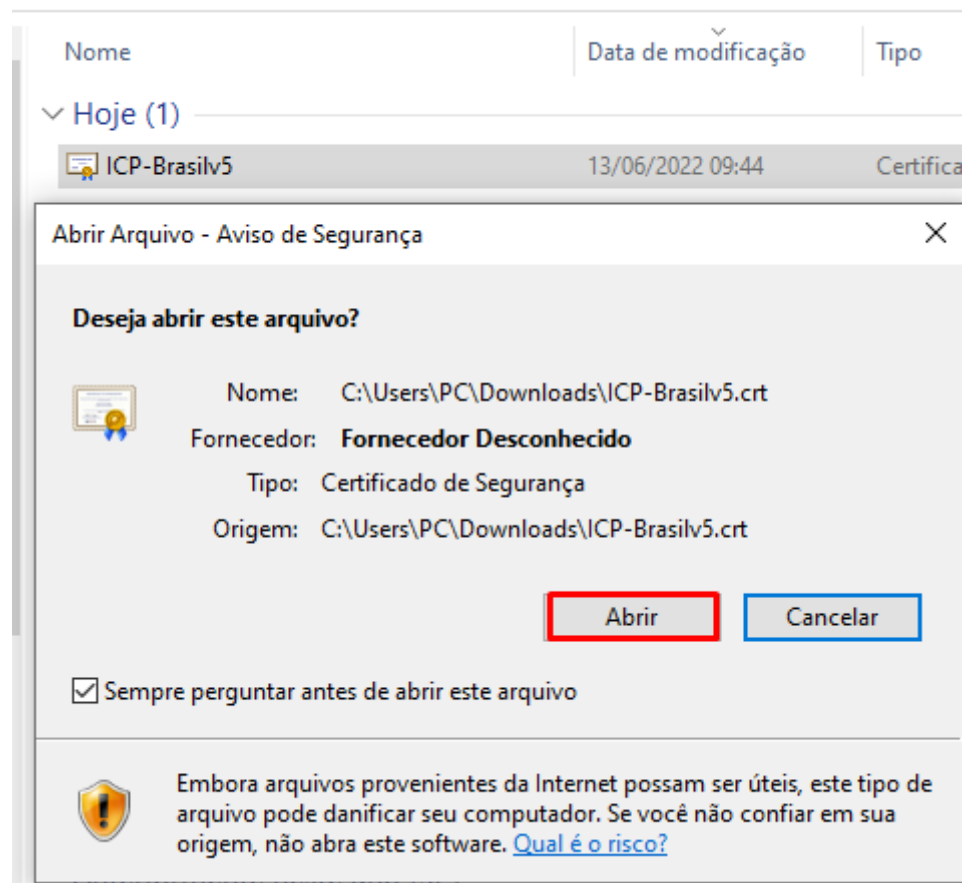
a) Fazer o download e instalar a cadeia de certificados abaixo:

<http://acraiz.icpbrasil.gov.br/credenciadas/RAIZ/ICP-Brasilv5.crt>

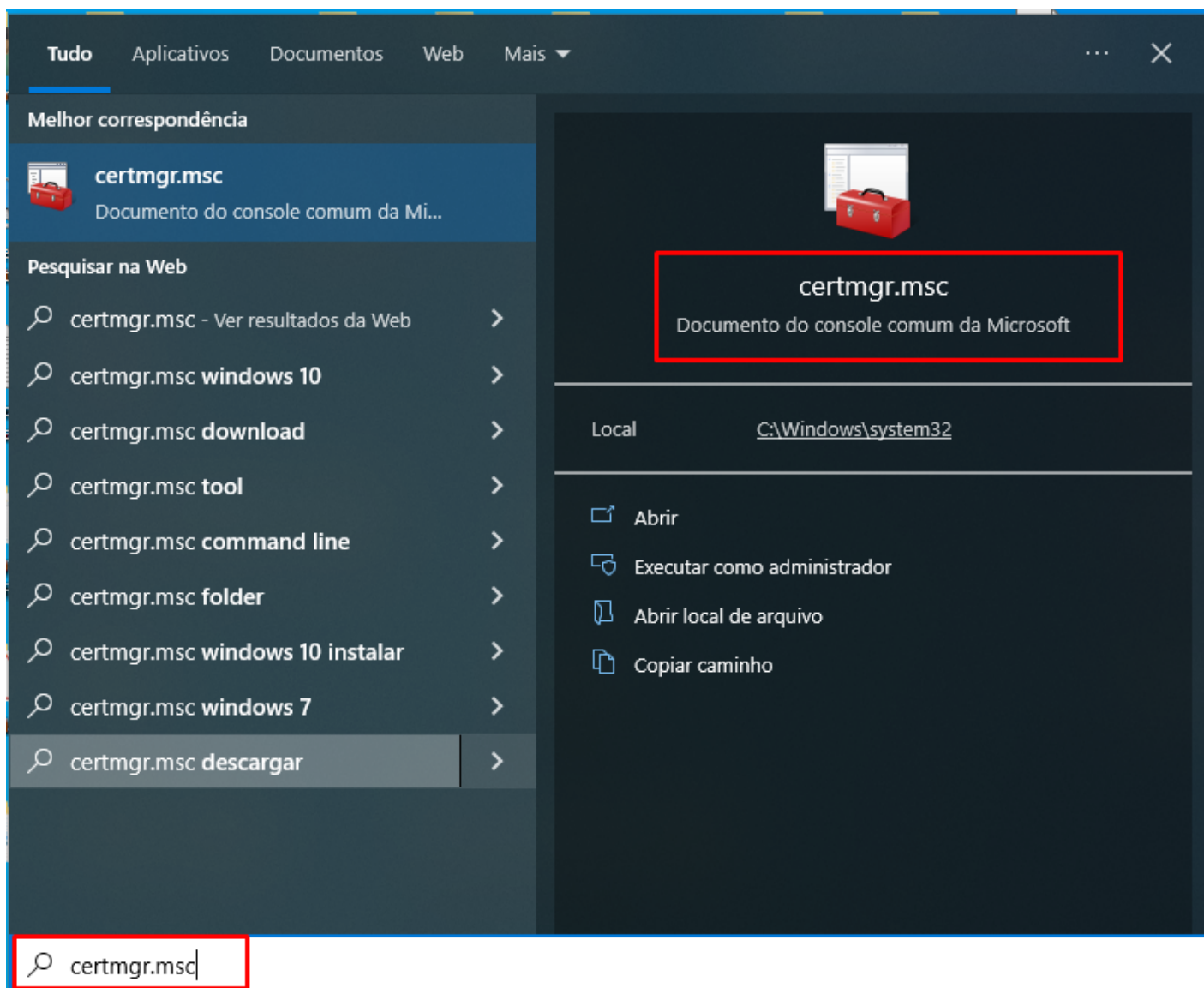


Execute o ICP-Brasilv5

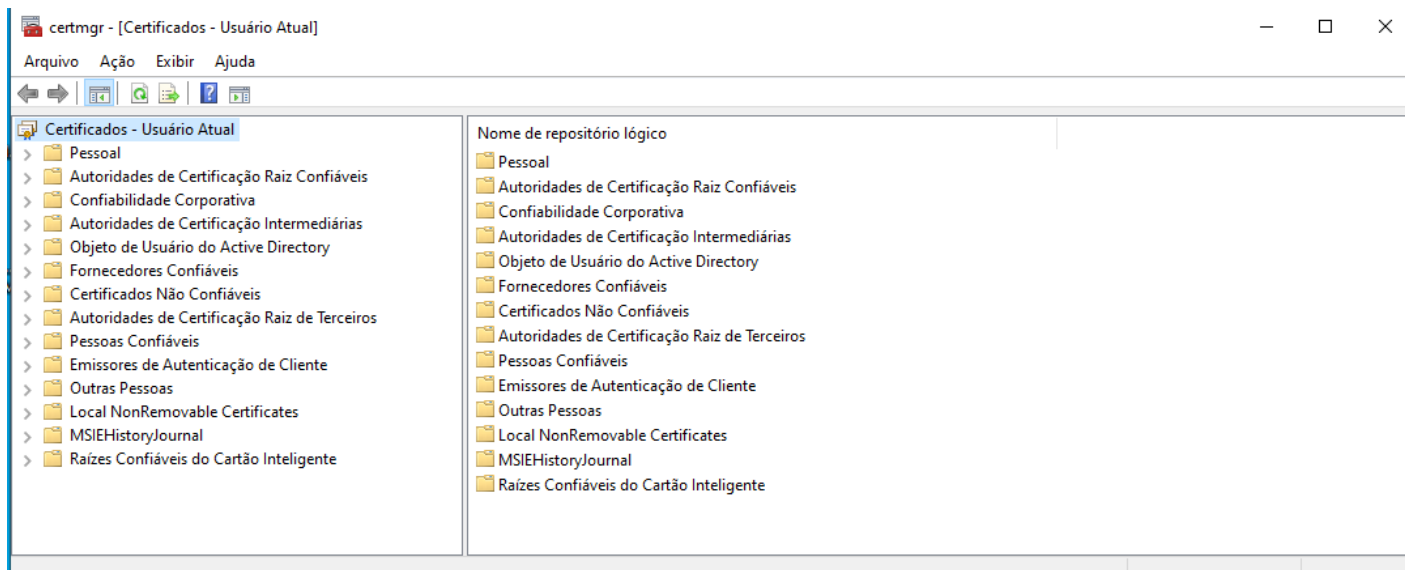
lor > Disco Local (C:) > Usuários > PC > Downloads



b) Clique na pesquisa do windows e digite certmgr.msc,

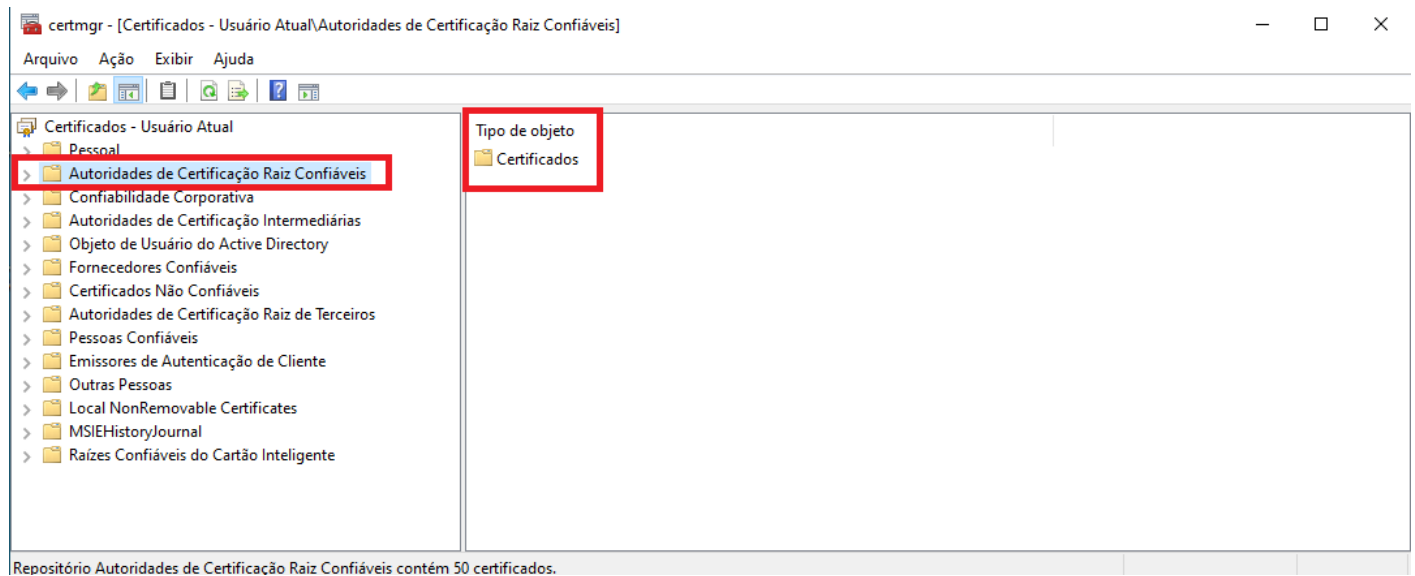


Será aberto o Gerenciador de Certificados Digitais.

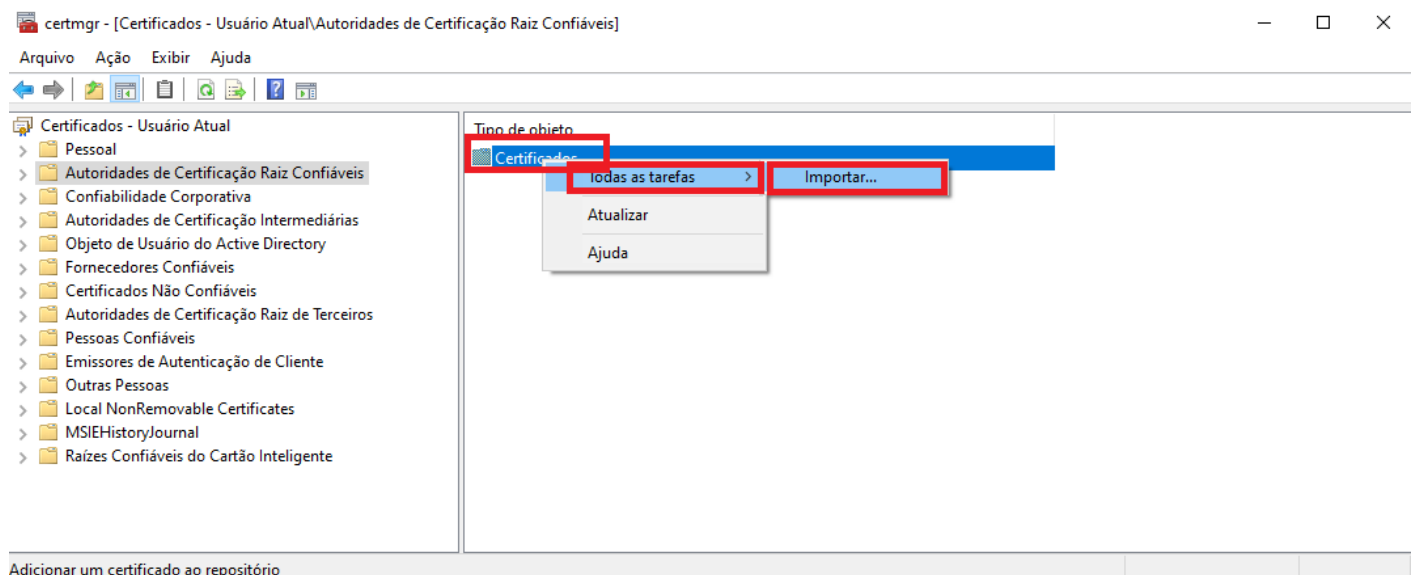


c) Clique na pasta "Autoridades de Certificação Raiz Confiáveis", irá abrir a pasta "certificados" do

lado esquerdo,



clique na pasta " certificados" com o botão direito ir em todas as tarefas e clicar em importar,



Faça o processo de instalação clicando em Avançar.



## Bem-vindo ao Assistente para Importação de Certificados

Use este assistente para copiar certificados, listas de certificados confiáveis e listas de certificados revogados de um disco para um repositório de certificados.

Um certificado, que é emitido por uma autoridade de certificação, é uma confirmação de sua identidade e contém informações usadas para proteger dados ou estabelecer conexões de rede seguras. Um repositório de certificados é a área do sistema em que os certificados são mantidos.

### Local do Repositório

☒ Usuário Atual

☐ Máquina Local

Para continuar, clique em Avançar.

Avançar

Cancelar

Procure pelo Arquivo do Certificado Digital e clique em Avançar



## Assistente para Importação de Certificados

### Arquivo a Ser Importado

Especifique o arquivo que você deseja importar.

Nome do arquivo:

Procurar...

Observação: mais de um certificado pode ser armazenado em um único arquivo nos seguintes formatos:

Troca de Informações Pessoais - PKCS nº 12 (.PFX,.P12)

Padrão de Sintaxe de Mensagem Criptografada - PKCS nº7 (.P7B)

Repositório de Certificados Serializado da Microsoft (.SST)

Avançar

Cancelar

d) Ainda no certmgr.msc, expanda a pasta Autoridades de Certificação Raiz confiáveis, será apresentada a pasta Certificados

certmgr - [Certificados - Usuário Atual\Autoridades de Certificação Raiz Confiáveis\Certificados]

Arquivo Ação Exibir Ajuda

Certificados - Usuário Atual

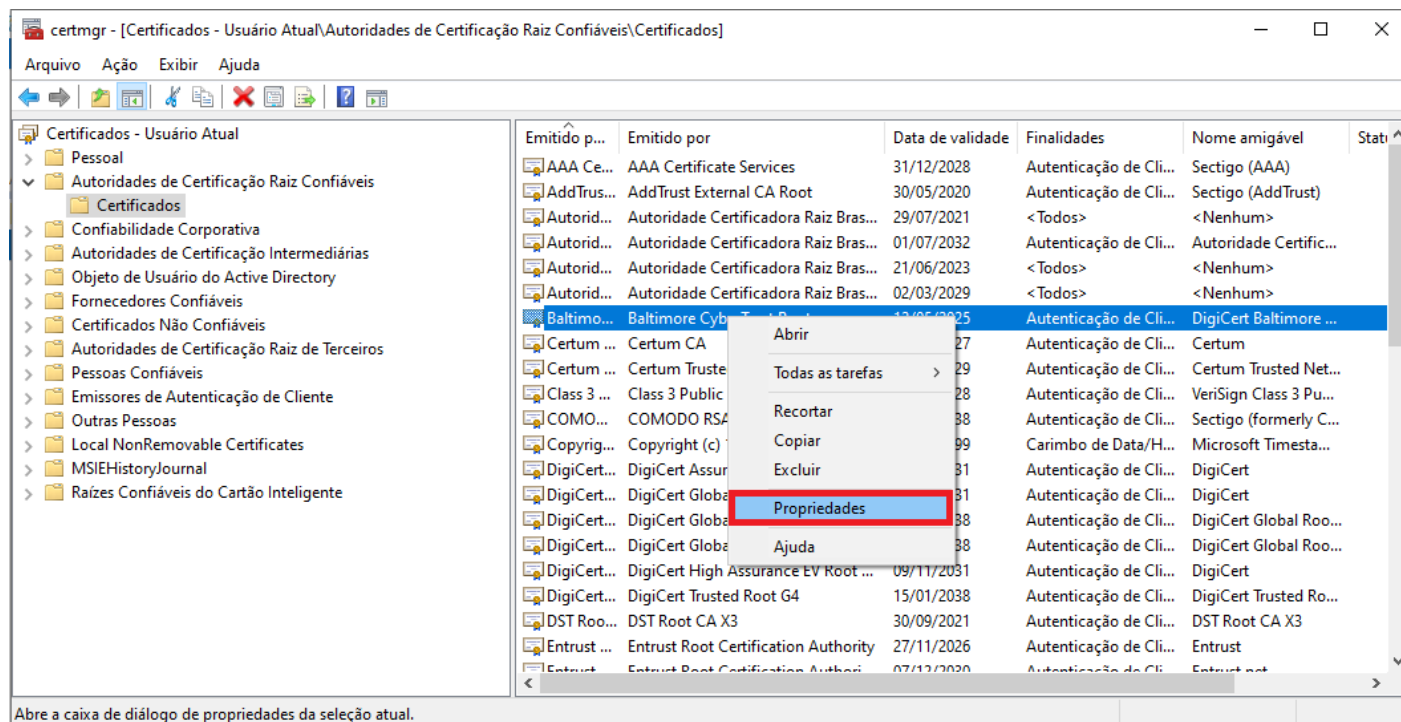
- Pessoal
- Autoridades de Certificação Raiz Confiáveis
  - Certificados**
- Confiabilidade Corporativa
- Autoridades de Certificação Intermediárias
- Objeto de Usuário do Active Directory
- Fornecedores Confiáveis
- Certificados Não Confiáveis
- Autoridades de Certificação Raiz de Terceiros
- Pessoas Confiáveis
- Emissores de Autenticação de Cliente
- Outras Pessoas
- Local NonRemovable Certificates
- MSIEHistoryJournal
- Raízes Confiáveis do Cartão Inteligente

Emitido para	Emitido por	Data de validade	Finalidades	Nome
AAA Certificate Services	AAA Certificate Services	31/12/2028	Autenticação de Cli...	Secti
AddTrust External CA Root	AddTrust External CA Root	30/05/2020	Autenticação de Cli...	Secti
Autoridade Certificadora Raiz B...	Autoridade Certificadora Raiz Bras...	29/07/2021	<Todos>	<Ne
Autoridade Certificadora Raiz B...	Autoridade Certificadora Raiz Bras...	01/07/2032	Autenticação de Cli...	Autc
Autoridade Certificadora Raiz B...	Autoridade Certificadora Raiz Bras...	21/06/2023	<Todos>	<Ne
Autoridade Certificadora Raiz B...	Autoridade Certificadora Raiz Bras...	02/03/2029	<Todos>	<Ne
Baltimore CyberTrust Root	Baltimore CyberTrust Root	12/05/2025	Autenticação de Cli...	Digi
Certum CA	Certum CA	11/06/2027	Autenticação de Cli...	Certi
Certum Trusted Network CA	Certum Trusted Network CA	31/12/2029	Autenticação de Cli...	Certi
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	01/08/2028	Autenticação de Cli...	VeriS
COMODO RSA Certification Au...	COMODO RSA Certification Auth...	18/01/2038	Autenticação de Cli...	Secti
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	30/12/1999	Carimbo de Data/H...	Micr
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	09/11/2031	Autenticação de Cli...	Digi
DigiCert Global Root CA	DigiCert Global Root CA	09/11/2031	Autenticação de Cli...	Digi
DigiCert Global Root G2	DigiCert Global Root G2	15/01/2038	Autenticação de Cli...	Digi
DigiCert Global Root G3	DigiCert Global Root G3	15/01/2038	Autenticação de Cli...	Digi
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	09/11/2031	Autenticação de Cli...	Digi
DigiCert Trusted Root G4	DigiCert Trusted Root G4	15/01/2038	Autenticação de Cli...	Digi
DST Root CA X3	DST Root CA X3	30/09/2021	Autenticação de Cli...	DST
Entrust Root Certification Auth...	Entrust Root Certification Authority	27/11/2026	Autenticação de Cli...	Entr
Entrust Root Certification Auth...	Entrust Root Certification Authori...	07/12/2020	Autenticação de Cli...	Ente

Repositório Autoridades de Certificação Raiz Confiáveis contém 50 certificados.



Procure do lado direito da tela o Certificado Digital instalado e clique com o botão direito do mouse, em seguida clique em Propriedades.



Em seguida selecione a opção "ativar todas as finalidades deste certificado", clique em Aplicar e em seguida em OK.

Propriedades de Baltimore CyberTrust Root

Gerar Certificados Cruzados OCSP Validação Estendida

Nome amigável: DigiCert Baltimore Root

Descrição:

Finalidades do certificado

☒ Ativar todas as finalidades deste certificado

☐ Desativar todas as finalidades deste certificado

☐ Ativar somente as seguintes finalidades

Observação: você pode editar somente as finalidades de certificados aceitas pelo caminho de certificação.

<input checked="" type="checkbox"/>	Autenticação do Servidor
<input checked="" type="checkbox"/>	Autenticação de Cliente
<input checked="" type="checkbox"/>	Assinatura do Código
<input checked="" type="checkbox"/>	Email Seguro
<input checked="" type="checkbox"/>	Carimbo de Data/Hora
<input type="checkbox"/>	Assinatura da Lista de Confiabilidade da Microsoft
<input type="checkbox"/>	Carimbo de Data/Hora da Microsoft

Adicionar Finalidade...

OK Cancelar Aplicar

Revision #1

Created 3 August 2022 08:15:16 by DesenvolR

Updated 2 June 2023 10:00:09 by DesenvolR