Erro 403 – Forbidden: Access is denied.

Há diversas causas possíveis para o erro 403 (Proibido). A Microsoft tem uma lista de todos os códigos que o IIS pode retornar:
https://support.microsoft.com/pt-br/kb/943891

A lista dos navegadores que são suportados pelo Sefaz Identity (utilizado para a autenticação dos usuários) não inclui o Edge Legacy, disponível no Windows 10. Os requisitos para a autenticação por certificado digital no Sefaz Identity são similares aos requisitos para o acesso remoto, com exceção do plugin da Citrix e do Citrix Receiver, que não são necessários. As instruções para os servidores da Sefaz configurarem o acesso remoto estão em:
https://portal.fazenda.sp.gov.br/servicos/teletrabalho/Paginas/Acesso-Remoto.aspx

No caso específico da autenticação por certificado digital, supondo que seja utilizado um navegador compatível (Chrome, Firefox, o novo Edge Chromium, etc), que a leitora de cartão esteja corretamente instalada e que o cartão esteja inserido corretamente, os 4 erros mais prováveis são:

- **403.7 - Certificado de cliente necessário.**

  Indica apenas que o navegador do cliente não entregou o certificado digital do usuário para os nossos servidores.
  Possíveis causas:
  - Usuário cancelou a seleção do certificado digital a ser utilizado.
  - Usuário cancelou a digitação do PIN do certificado digital.
  - Usuário está usando o Microsoft Edge Legacy.
  - Usuário está usando o Internet Explorer em um computador desatualizado.
  - Usuário está usando o Internet Explorer em um dos poucos computadores com Windows 10 que apresentam o problema.

  Possíveis soluções:
  - Reiniciar o navegador (fechando **todas** as janelas).
  - Limpar cache e estado SSL do navegador:
    https://support.microsoft.com/pt-br/help/17438/windows-internet-explorer-view-delete-browsing-history
    https://www.a2hosting.com/kb/getting-started-guide/internet-and-networking/clearing-a-web-browsers-ssl-state
  - Utilizar outro navegador, como o Internet Explorer ou o Chrome, por exemplo.
  - Atualizar o computador:
    https://support.microsoft.com/pt-br/help/12373/windows-update-faq
    Obs: Se for Windows 7, favor verificar se KB3020369 e KB3125574 realmente já estão instalados.
  - Desabilitar a utilização do protocolo TLS 1.2 pelo Internet Explorer:
    Ver instruções na última página.
    Obs: Solução de contorno **somente** para o uso do Internet Explorer (que não tem mais suporte) nos poucos computadores com Windows 10 que apresentam o problema.
  - Reiniciar o computador.
    Obs: Raramente é necessário, mas os passos anteriores nem sempre são suficientes.

- **403.13 - Certificado de cliente revogado.**

  Indica que o navegador do cliente entregou um certificado digital revogado ou que não pôde ser validado por nossos servidores.
  Possíveis causas:
  - Falhas temporárias de rede/comunicação.
    Obs: Falha na obtenção das informações de revogação (CRL/OCSP).
  - O certificado digital do usuário foi revogado pela autoridade certificadora que o emitiu.

  Possíveis soluções:
  - Tentar novamente mais tarde.
  - Utilizar outro certificado digital.
    Obs: Caso haja dúvidas sobre o motivo da revogação, entrar em contato com a autoridade certificadora que emitiu o certificado.

- **403.16 - Certificado do cliente não é confiável ou é inválido.**

  Indica que o navegador do cliente entregou um certificado digital inválido ou que não pôde ser validado por nossos servidores.
  Causa:
  - Emissor do certificado não é reconhecido por nossos servidores.

  Possíveis soluções:
  - Verificar se todos os certificados da cadeia de certificados do usuário estão ok: Ver instruções na próxima página.
  - Enviar a parte **pública** do certificado (sem a chave privada) para que possamos verificar se o emissor do certificado deveria ser reconhecido por nossos servidores:
    Instruções para exportar certificados estão disponíveis em https://ads.intra.fazenda.sp.gov.br/tfs/ADMIN/Wiki_Arquitetura/_wiki/wikis/Wiki_Arquitetura.wiki/413/ ou https://support.office.com/pt-br/article/exibir-certificados-b73abe88-9f85-48a1-b00f-7ade1c0ec49f
    Obs: Utilizar, preferencialmente, o padrão PKCS nº7. Selecionar "Incluir todos os certificados no caminho de certificação, se possível". Vale a pena reforçar que, mesmo que a opção esteja disponível, **nunca** se deve selecionar "Sim, exportar a chave privada".

- **403.17 - Certificado do cliente expirado ou ainda não está válido.**

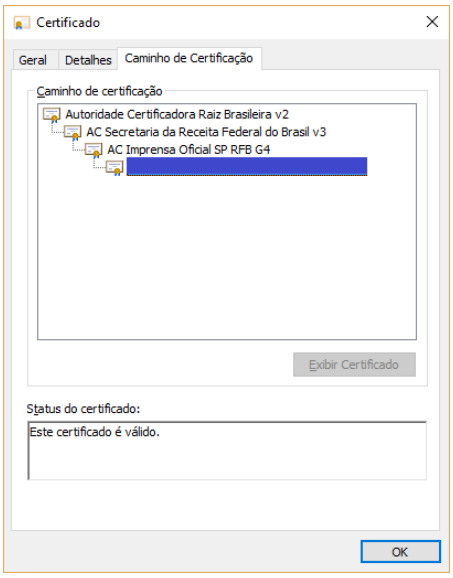
  Indica que o navegador do cliente entregou para os nossos servidores um certificado digital que está fora do período de validade.
  Causas:
  - O certificado digital já expirou.
  - O certificado digital ainda não é válido.

  Solução:
  - Utilizar outro certificado digital.
    Obs: Caso haja dúvidas sobre o período de validade, entrar em contato com a autoridade certificadora que emitiu o certificado.

Obs: Mesmo que a informação do subtipo do erro 403 (por exemplo, 403**.7**) não apareça no navegador do usuário, ela é gravada no log do IIS do servidor que retornou o erro.

Verificar o caminho de certificação do certificado do usuário

Examinar a aba “Caminho de Certificação” do certificado do usuário:



Usar a aplicação de exemplo do Sefaz Identity:
https://www.identityprd.fazenda.sp.gov.br/Sefaz.Identity.STS.Exemplo/ACs.aspx

Verificar que o primeiro certificado do caminho de certificação aparece na lista de certificados raiz e que o resultado da verificação é “Ok”:

Certificados de Autoridades Certificadoras Raiz:

Subject	Thumbprint	Resultado da Verificação
AC Raiz da Secretaria da Fazenda-SP V1	EEE797E2ABECA31B518336E3D4700F5BA9E79CA0	Ok
Autoridade Certificadora Raiz Brasileira v1	705D2B4565C7047A540694A79AF7ABB842BDC161	Ok
Autoridade Certificadora Raiz Brasileira v2	A9822E6C6933C63C148C2DCAA44A5CF1AAD2C42E	Ok
Autoridade Certificadora Raiz Brasileira v5	4ACADAB14B74BF4FBA7BACE64B91801C44B8CC66	Ok
CA Raiz Corporativa SEFAZ	DF8197317AE7E24860F20CD63A7B1A448A47E3F4	Ok
DigiCert Global Root CA	A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436	Ok
VeriSign Class 3 Public Primary Certification Authority - G5	4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5	Ok

Verificar que todos os outros certificados do caminho de certificação aparecem na lista de certificados intermediários e que o resultado da verificação também é “Ok”:

Certificados de Autoridades Certificadoras Intermediárias:

Subject	Thumbprint	Resultado da Verificação
AC BOA VISTA	1EA69AFAC7FAA78E8B4C882CCD4176371F29E526	Ok
AC BOA VISTA CERTIFICADORA	8B0D5AEC03BBA5C24DB8830D1C85C7483B7A6577	The revocation function was unable to check revocation for the certificate.
...		
AC Imprensa Oficial SP G3	E530BA1DA1B6400626982DA39DB56FABF1B1A9FF	Ok
AC Imprensa Oficial SP G4	6861B849837C7A3F99A67B1B118AC8DA688C1903	Ok
AC Imprensa Oficial SP RFB G3	26F9A0C6E8A840C9F6DF2FE8B6690AEB8DBF80DF	The certificate is revoked.
AC Imprensa Oficial SP RFB G4	6BBC3C434F6C9D90D2F26AE5C59C51A49832885C	Ok
...		
AC SAFEWEB RFB v5	A338B1007EE682B6D90BB7CBFC82F1838879462F	Ok
AC SAT SEFAZ SP	57433CD786EC15B2465B9A8435D4C7AAF16C91A9	A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.
AC Secretaria da Receita Federal do Brasil	1F97AE58A3C25358187A7D9BF071ADB176F0932F	Ok
AC Secretaria da Receita Federal do Brasil v3	ECDCC493FDF4F1D40ADE2F8E26C5AECEF172D475	Ok
AC Secretaria da Receita Federal do Brasil v4	0E182E25504C1C6EDFE9598900F5D173055DE696	Ok
AC SEFAZ-SP Sistemas V1	5AF92E3401E3234F5621133157FC034BE5C43161	Ok

Se todos os certificados do caminho de certificação estiverem ok, e o certificado do usuário também (ou seja, dentro da validade, não revogado, etc.), o usuário deveria conseguir usar o certificado dele sem problemas.

Se qualquer certificado do caminho de certificação não for encontrado nas listas acima (lista de certificados raiz e lista de certificados intermediários) ou se a verificação falhar para qualquer um desses certificados, o certificado do usuário será recusado pelo Sefaz Identity e o usuário não vai conseguir fazer login. As falhas mais prováveis são:

- **The certificate is revoked.**

  Indica que o certificado da autoridade certificadora foi revogado. Com isso, todo e qualquer certificado assinado por esse mesmo certificado de AC é considerado não confiável e será recusado pelo Sefaz Identity.
  Qualquer aplicação que aceite esse certificado de AC (ou qualquer certificado assinado por esse mesmo certificado de AC) tem problemas de segurança, portanto não se pode aceitar argumentos do tipo “Esse mesmo certificado funciona na aplicação X”.
  Solução:
  - Utilizar outro certificado digital.
    Obs: Caso haja dúvidas sobre o motivo da revogação, entrar em contato com a autoridade certificadora que emitiu o certificado de AC.

- **A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file.**

  Indica que o certificado da autoridade certificadora está fora do período de validade.
  Qualquer aplicação que aceite esse certificado de AC (ou qualquer certificado assinado por esse mesmo certificado de AC) tem problemas de segurança, portanto não se pode aceitar argumentos do tipo “Esse mesmo certificado funciona na aplicação X”.
  Possíveis causas:
  - Certificado ainda não é válido.
  - Certificado já expirou.

  Possíveis soluções:
  - Utilizar outro certificado digital.
    Obs: Caso haja dúvidas sobre a validade do certificado, entrar em contato com a autoridade certificadora que emitiu o certificado de AC.

- **A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.**

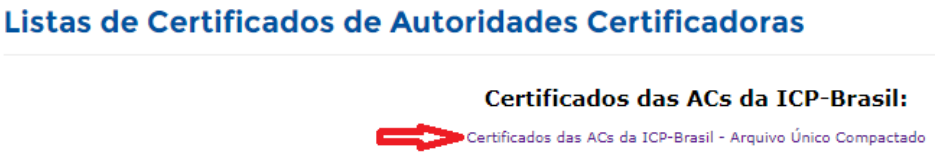
  Indica que o certificado raiz correspondente não é aceito pelo Sefaz Identity.
  Qualquer aplicação que aceite esse certificado de AC (ou qualquer certificado assinado por esse mesmo certificado de AC) tem problemas de segurança, portanto não se pode aceitar argumentos do tipo “Esse mesmo certificado funciona na aplicação X”.
  Possíveis causas:
  - O certificado raiz correspondente está na lista de certificados rejeitados pelo Sefaz Identity.
    Obs: É o caso do certificado da “AC SAT SEFAZ SP”, que é distribuído para todos os servidores da Sefaz, mas não é aceito pelo Sefaz Identity porque o certificado raiz correspondente está na lista de certificados rejeitados por nossos servidores.

  Possíveis soluções:
  - Utilizar outro certificado digital.
    Obs: Caso haja dúvidas sobre a lista de certificados rejeitados pelo Sefaz Identity, solicitar para a equipe técnica responsável pelo sistema com problemas que entre em contato com a equipe do Sefaz Identity.

- **The revocation function was unable to check revocation for the certificate.**

  Indica que o certificado da autoridade certificadora não pôde ser validado por nossos servidores ou é inválido.
  Qualquer aplicação que aceite esse certificado de AC (ou qualquer certificado assinado por esse mesmo certificado de AC) tem problemas de segurança, portanto não se pode aceitar argumentos do tipo “Esse mesmo certificado funciona na aplicação X”.
  Possíveis causas:
  - Falhas temporárias de rede/comunicação ou na AC emissora do certificado.
    Obs: Falha na obtenção das informações de revogação (CRL/OCSP).
    Ex: “AC BOA VISTA CERTIFICADORA” durante todo o 1º semestre de 2018.
  - Algum certificado do caminho de certificação do certificado da AC não está instalado em nossos servidores.

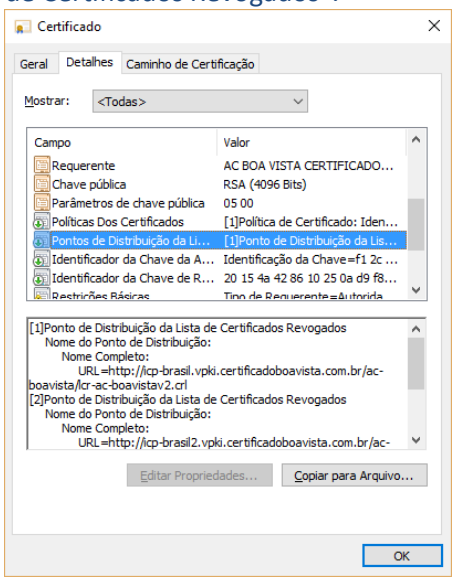
  Possíveis soluções:
  - Tentar novamente mais tarde.
    Obs: Se as informações de revogação disponibilizadas por alguma AC expiraram, pode-se tentar entrar em contato com a AC para comunicar o problema. Neste caso não há o que fazer na Sefaz.
    Ver instruções na próxima página.
  - Verificar, utilizando o link no topo da página da aplicação de exemplo do Sefaz Identity, se algum certificado do caminho de certificação do certificado da AC foi inserido recentemente na lista de certificados divulgada pelo ITI:

    Obs: Neste caso é possível que o processo de instalação desses certificados de AC ainda não tenha sido concluído pelas equipes responsáveis. Também é possível que o processo de distribuição desses certificados para os servidores do Sefaz Identity ainda esteja em andamento.

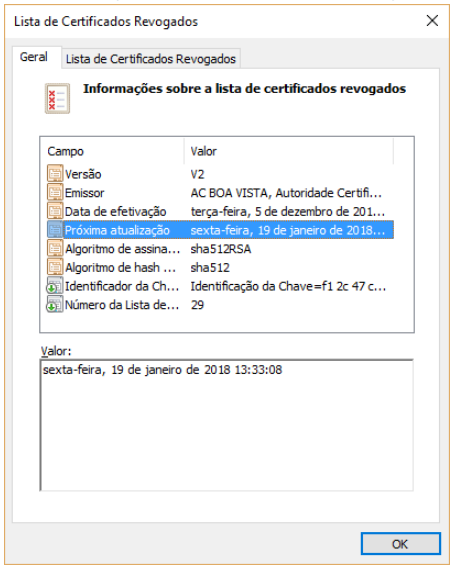
Verificar informações de revogação de certificados

Examinar, na aba “Detalhes” do certificado, os endereços dos “Pontos de Distribuição da Lista de Certificados Revogados”:



Usar um navegador Web para fazer download da Lista de Certificados Revogados (LCR). No caso específico do exemplo acima:
http://icp-brasil.vpki.certificadoboavista.com.br/ac-boavista/lcr-ac-boavistav2.crl

Examinar, na aba “Geral” da LCR, o campo “Próxima atualização”:



No caso do exemplo acima, a LCR disponibilizada pela “AC BOA VISTA” (emissora do certificado da “AC BOA VISTA CERTIFICADORA”) não é válida na data atual:

Horário da Verificação:

11/10/2018 17:20:34.142 a 11/10/2018 17:20:34.970

Para determinar se um certificado é válido, esta verificação tem que ser feita para todos os certificados do caminho de certificação, desde o certificado do usuário até o certificado raiz.
Obs: Certificados raiz sem endereços de LCR são considerados válidos se estiverem instalados.

Verificar se há problemas no sistema usuário

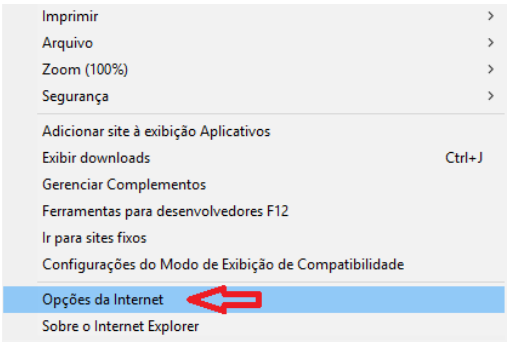
Usar a aplicação de exemplo do Sefaz Identity (clicar no certificado):
https://www.identityprd.fazenda.sp.gov.br/Sefaz.Identity.STS.Exemplo/Default.aspx

Se a aplicação de exemplo funcionar, o Sefaz Identity está ok e a autenticação no sistema usuário também deveria estar funcionando. Caso não esteja, solicitar para a equipe técnica responsável pelo sistema com problemas que entre em contato com a equipe do Sefaz Identity.

Desabilitar a utilização do protocolo TLS 1.2 pelo Internet Explorer

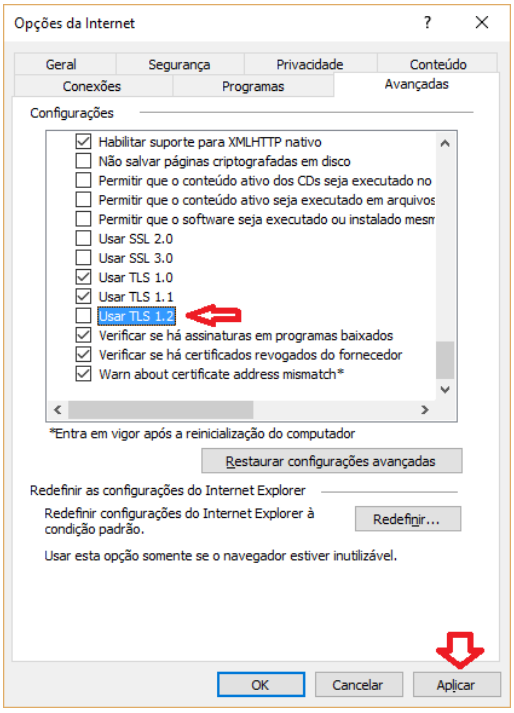
Selecionar “Ferramentas” no canto superior direito do Internet Explorer:

Em seguida, selecionar “Opções da Internet”:



Na janela que abrir, selecionar a aba “Avançadas”:

Desabilitar “Usar TLS 1.2” e clicar em “Aplicar”:



Fechar a janela clicando em “OK”.