

Projeto ACBr



Dúvidas sobre a NFe 4.0 Certificado e TLS 1.2

Daniel Simões de Almeida

Certificado e TLS 1.2

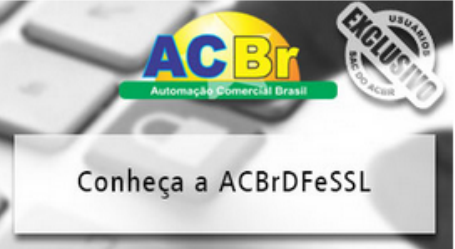


- Nova exigência. TLS 1.2
- Como configurar o ACBrNFe?
- TLS1.2 não funciona, o que tentar ?
- Dúvidas Frequentes
- Bibliotecas externas
- Certificado A1 ou A3, qual o melhor ?

Vídeo completo:

Conheça a ACBrDFeSSL (exclusivo SAC)





Conheça a ACBrDFeSSL

Ver agora

Informações

Ver agora

Conheça a ACBrDFeSSL.

- Saiba como tirar o máximo de proveito dos componentes de Documentos Fiscais Eletrônicos do ACBr
- Fique livre da CAPICOM
- Compile em 64 bits e em Linux
- Aumente a performance da sua aplicação
- Conheça as tecnologias disponíveis (OpenSSL, libXML2, XMLSec, WinCrypt, etc)
- Compreenda como o ACBr, Cria, Assina, Verifica e envia os Documentos Eletrônicos

Baixe o PDF em anexo

Nota: Vídeo dividido em 2 partes... clique em "Parte1" e "Parte2"

Apresentação - Conheça a ACBrDFeSSL.pdf

Gerenciar Relatário

7 5

EMBarbosa, Kiko Fernandes, datahotel e 9 outros reagiu para isto

ssl x wincrypt x openssl x https x tls1.2 x capicom x msxml x sign x digest x canonical x +

Iniciado por **Daniel Simoes**
3 Janeiro

Coleções Suporte Pago - SAC

Atualizado 3 Janeiro

Exibições 1.116

Comentário 0

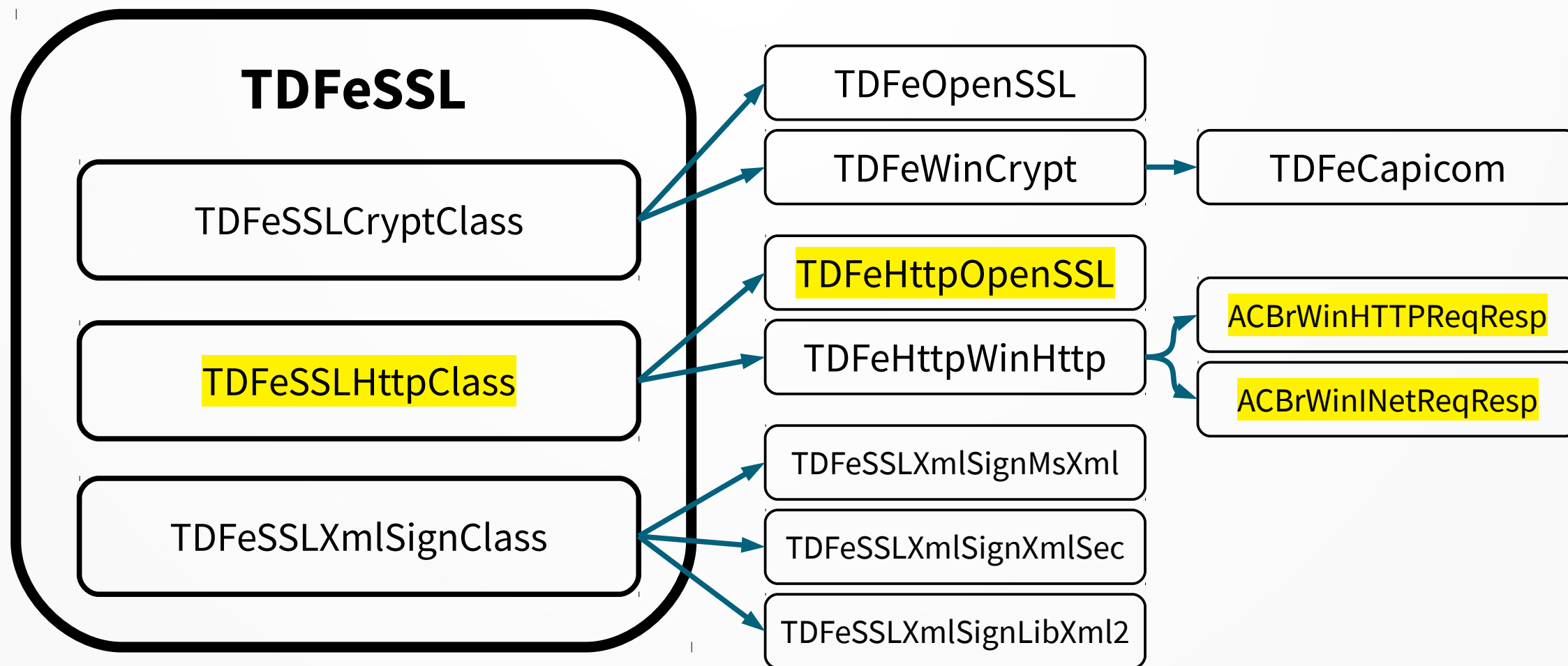
Avaliação ★★★★★ (13 análises)

Nova exigência. TLS 1.2

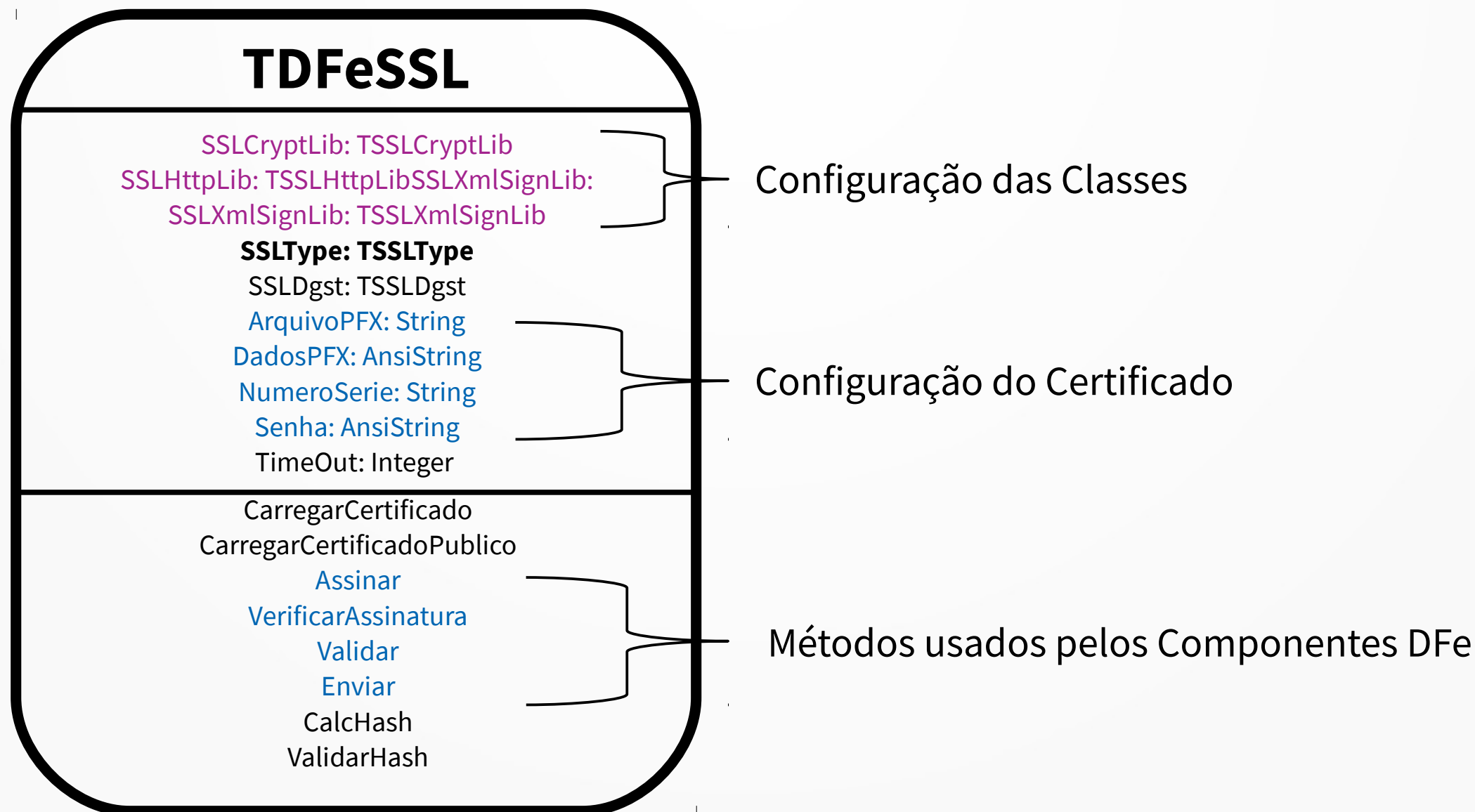


- O que é SSL/TLS ?
 - São protocolos de segurança que protegem a comunicação via internet
- NFe 3.10
 - Utiliza SSL3
 - Secure Sockets Layer
 - Depreciado (inseguro)
 - Algumas UFs aceitam TLS1.2
- NFe 4.00
 - Aceita apenas TLS1.2
 - Transport Layer Security

Como a TDFeSSL é organizada ?



Métodos e Propriedades de TDFeSSL



Como configurar a TDFeSSL

TDFeSSL

SSLCryptLib: TSSLCryptLib
SSLHttpLib: TSSLHttpLib
SSLXmlSignLib: TSSLXmlSignLib
SSLType: TSSLType
SSLDgst: TSSLDgst
ArquivoPFX: String
DadosPFX: AnsiString
NumeroSerie: String
Senha: AnsiString
Timeout: Integer

CarregarCertificado
CarregarCertificadoPublico
Assinar
VerificarAssinatura
Validar
Enviar
CalcHash
ValidarHash

- **ArquivoPFX:** Permite definir um caminho (path), para carregar o Certificado diretamente do Arquivo PFX (A1)
- **DadosPFX:** Permite informar o Conteúdo binário, do Certificado, no formato PFX (A1)
- **NumeroSerie:** Procura pelo Certificado previamente instalado no Windows, com o Num.Série informado. (A1 ou A3)
- **Senha:** Senha para acesso ao certificado.

Dica: ArquivoPFX, DadosPFX e NumeroSerie, são mutuamente exclusivos.
(Defina valor apenas para um deles)

Como configurar a TDFeSSLHttpClient

TDFeSSL

SSLCryptLib: TSSLCryptLib

SSLHttpLib: TSSLHttpLib

SSLXmlSignLib: TSSLXmlSignLib

SSLType: TSSLType

SSLDgst: TSSLDgst

ArquivoPFX: String

DadosPFX: AnsiString

NumeroSerie: String

Senha: AnsiString

Timeout: Integer

CarregarCertificado

CarregarCertificadoPublico

Assinar

VerificarAssinatura

Validar

Enviar

CalcHash

ValidarHash

- **SSLHttpLib:**

- Permite definir qual será a API de comunicação Segura (HTTPS)
 - HttpNone,
 - HttpWinINet,
 - **HttpWinHttp,**
 - HttpOpenSSL,
 - httpIndy

- **SSLType:**

- LT_all,
- LT_SSLv2,
- LT_SSLv3,
- LT_TLSv1,
- LT_TLSv1_1,
- **LT_TLSv1_2,**
- LT_SSHv2

- **Timeout:**

- Tempo máximo (em milissegundos) de espera pela conexão ou resposta do WebService

httpOpenSSL



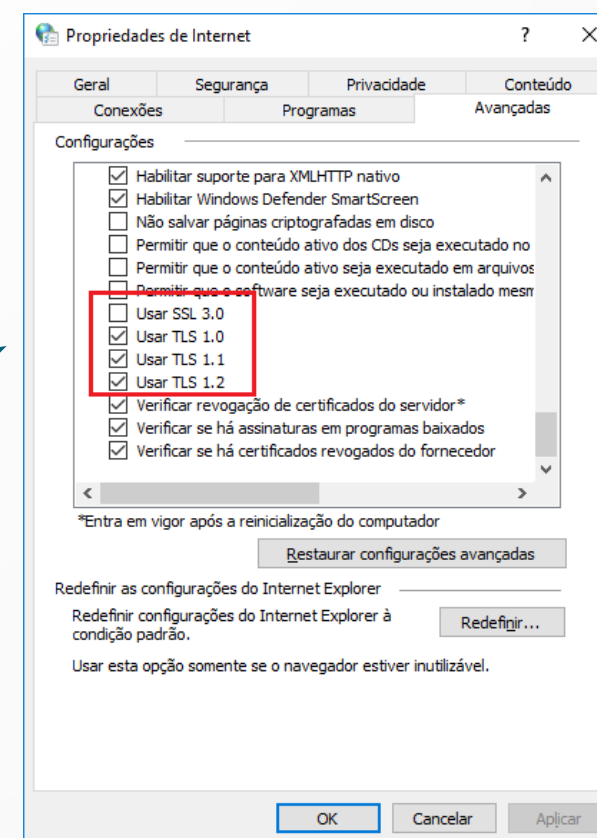
- Configuração
 - TDFeSSL.SSLHttpLib := httpOpenSSL;
- Bibliotecas Externas:
 - libeay32.dll, ssleay32.dll
- Vantagens:
 - Não Depende de configurações no Windows
 - Não depende de outras bibliotecas (exceto Run Time do compilador. Ex: msvcr120.dll – MS VS2013)
 - Não requer registro da biblioteca (regsvr32)
 - **Roda em Linux, Windows e WinXP**
 - Roda em 32 e 64 bits
 - Certificados não precisam ser instalados no Windows
- Desvantagens:
 - Suporta apenas Certificados A1
 - **Apenas versões superiores a 1.0 da OpenSSL suportam TLS 1.2**
 - ACBr não é compatível com série 1.1

httpWinHttp

- Usa a API do Windows **WinHTTP**, para comunicação com HTTPS.
- Configuração
 - TDFeSSL.SSLHttpLib := **httpWinHttp**;
- Bibliotecas Externas:
 - 32 bits: C:\Windows\SysWOW64\winhttp.dll
 - 64 bits C:\Windows\System32\winhttp.dll
- Vantagens:
 - **Não Depende de configurações no Windows**
 - Não requer registro da biblioteca (regsvr32)
 - Roda em 32 e 64 bits
 - Suporta Certificados A1 e A3
 - Nativa do Windows
- Desvantagens:
 - **Depende de atualizações do Windows**
 - Roda apenas em Windows,

httpWinINet

- Usa a API do Windows, **WinINet**, para comunicação com HTTPS. (Internet Explorer)
- Configuração
 - TDFeSSL.SSLHttpLib := **httpWinINet**;
- Bibliotecas Externas:
 - 32 bits: C:\Windows\SysWOW64\wininet.dll
 - 64 bits C:\Windows\System32\wininet.dll
- Vantagens:
 - Não requer registro da biblioteca (regsvr32)
 - Roda em 32 e 64 bits
 - Suporta Certificados A1 e A3
 - Nativa do Windows
- Desvantagens:
 - **Depende de configurações no Windows**
 - **Depende de atualizações do Windows**
 - Roda apenas em Windows,



Nossa sugestão de configuração

Windows

```
SSLCryptLib := cryWinCrypt;  
SSLHttpLib := httpWinHttp;  
SSLXmlSignLib := xsLibXml2;  
SSLType := LT_TLSv1_2;
```

- Vantagens
 - Suporta Certificados A1 e A3
 - Não requer a instalação de DLLs externas
 - Não requer registro de DLLs
 - Não requer ajustes nas configurações do Internet Explorer
 - Certificado A1 não precisa ser instalado no Windows
 - Suporta TLS1.2 e SHA256
- Desvantagens
 - Depende de Windows atualizado
 - Depende das DLLs da libXML2
 - Pode não funcionar em WinXP

Linux/WinXP

```
SSLCryptLib := cryOpenSSL;  
SSLHttpLib := httpOpenSSL;  
SSLXmlSignLib := xsLibXml2;  
SSLType := LT_TLSv1_2
```

- Vantagens
 - Não requer registro de DLLs
 - Não requer ajustes nas configurações do Internet Explorer
 - Certificado A1 não precisa ser instalado no Windows
 - Suporta TLS1.2 e SHA256
 - Funciona no WinXP
- Desvantagens
 - Depende das DLLs do OpenSSL e libXML2
 - Suporta Apenas Certificados A1

TLS1.2 não funciona, o que tentar ?



- WinCrypt (A1/A3)
 - Verifique se o seu Windows funciona com TLS1.2
 - Funciona apenas em Windows acima da Versão 7 (com SP1 instalado)
 - Não roda em sistemas antigos:
 - Windows XP
 - Windows Server 2008
 - Atualizar o Windows
 - Use o Windows Update, e rode todas atualizações disponíveis
- OpenSSL (A1)
 - Utilizar versão superior a 1.0
 - Série 1.1 ainda não é compatível com o ACBr

Duvidas frequentes



- A versão CAPICOM funcionará com a versão 4.0 da NF-e, e TLS1.2 ?
 - SIM
 - Não é recomendado, depreciado
- Meu certificado da versão 3.10 é compatível com a versão 4.0?
 - SIM, é o mesmo certificado

Bibliotecas externas



- Onde posso achar as DLLs necessárias ?
 - **OpenSSL:** \ACBr\DLLs\OpenSSL\1.0.2.13
 - **LibXML2:** \ACBr\DLLs\LibXml2
 - **MinGW:** \ACBr\DLLs\XMLSec\MinGW (toda a pasta)
- Qual usar, 32 ou 64 bit ?
 - Você deve usar DLLs compatíveis com a versão do seu Compilador.
 - Compilador 32 bits: Use todas DLLs em 32 bits (independente do Sistema Operacional ser 64 bits)
 - Compilador 64 bits: Seu programa exigirá um Sistema Operacional de 64 bits e portanto todas DLLs devem ser 64 bits
- Para onde copiar ?
 - Copie as DLLs para a mesma pasta da sua aplicação .EXE (**recomendado**) ou
 - De forma alternativa, você pode copiar as DLLs para o "System" do Windows
 - Para DLLs 32 bits
 - Windows 32 bits: copie para a pasta: C:\Windows\System32
 - Windows 64 bits: copie para a pasta: C:\Windows\SysWOW64
 - Para DLLs de 64 bits
 - Windows 32 bits: Não é compatível, não use
 - Windows 64 bits: copie para a pasta: C:\Windows\System32 (sim isso mesmo System32)

Certificado A1 x A3

• Vantagens

- Baixo suporte
- Fácil instalação
- O mesmo certificado, pode ser instalado em várias máquinas.
- No ACBr, ele não precisa ser instalado no Windows, para ser utilizado.
 - Pode ser “baixado” na estação por BD, Webservice, etc
- Compatível com Linux
- Compatível com todas as Bibliotecas de SSL do ACBr

A1

• Desvantagens

- Menos seguro que o A3
- Renovação anual
- Um pouco mais caro que o A3

• Vantagens

- Mais seguro que o A1
- Duração de 3 anos
- Um pouco mais barato que o A1 (custo por ano)

A3

• Desvantagens

- Alto nível de suporte
- Instalação complexa e diferente para cada Fornecedor ou Driver
- Precisa ser instalado no Windows, para ser utilizado.
- Não pode ser instalado em várias máquinas.
- Dificuldade de instalação no Linux
- Não é Compatível com todas as Bibliotecas de SSL do ACBr

• **Prefira certificados A1**

- Defina como “requisito de funcionamento” para o seu sistema o certificado A1.
- A pequena economia que o certificado A3 gera (custo por ano), não cobrem os custos com o Suporte

Dicas

Links úteis



- Bye Bye CAPICOM
- ACBrDFe OpenSSL e TLS1.2
- Biblioteca OpenSSL
- Transport Layer Security
- Vídeo completo: Conheça a ACBrDFeSSL (exclusivo SAC)
- Atualização para ativar o TLS 1.1 e o TLS 1.2 como um protocolos de segurança padrão no WinHTTP no Windows

Daniel Simões de Almeida

Fundador do Projeto ACBr
daniel@projetoacbr.com.br

<https://www.projetoacbr.com.br/forum/>