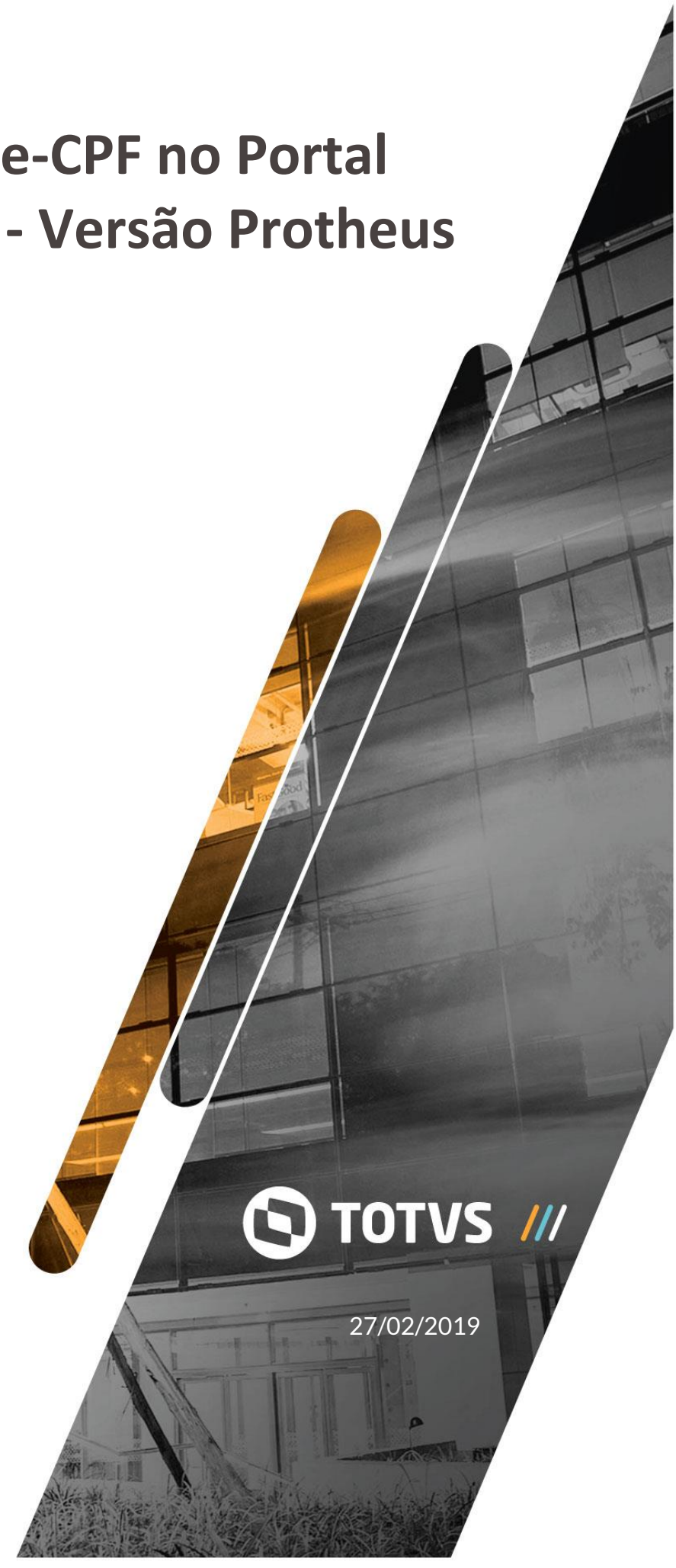
Configurando e-CPF no Portal Web do SARA - Versão Protheus



27/02/2019

Sumário

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

SARA – Portal Web

Este documento descreve como configurar e-CPF para conexão segura em modo APR.
O Portal *Web* do SARA foi desenvolvido dentro do Protheus e é emulado para *Web* pelo *SmartClient HTML* que roda em um servidor *Apache Tomcat*.
Para uso de autenticação via E-CPF, o servidor deve estar habilitado para conexão segura *SSL* e a maquina Cliente deve ter o E-CPF instalado assim como todas as cadeias de certificados do fornecedor para seu E-CPF.

1. Instale o Openssl

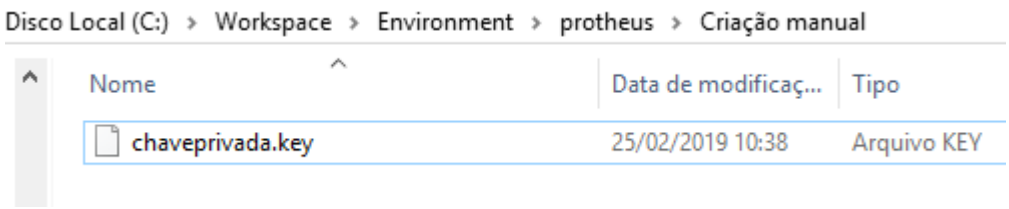
Siga a instrução de instalação conforme o fornecedor.

2. Geração do CSR

Digite no *prompt* de comando a instrução para gerar a chave privada, será solicitado uma senha que deve ser guardada, aqui usaremos 1234.

```
openssl genrsa -des3 2048 > chaveprivada.key
```

Será gerado um arquivo contendo a chave privada conforme a imagem, esta chave não pode ser recriada ela é única, guarde-a.



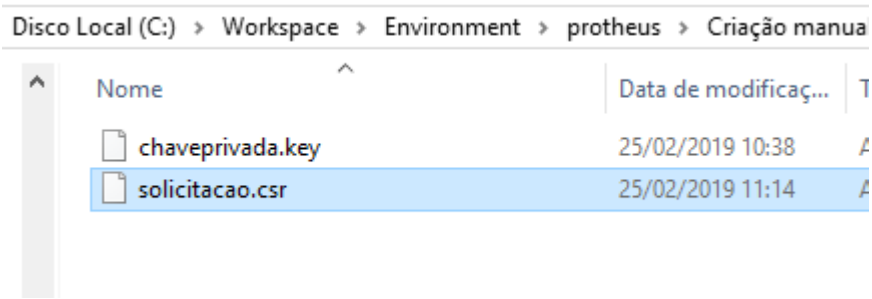
Digite no *prompt* de comando a instrução para gerar o CSR, algumas informações serão solicitadas:

```
openssl req -new -key chaveprivada.key > solicitacao.csr
```

- ***Country Name*** *(e letter code)*: Nome do país com duas letras, aqui usaremos o BR referente ao Brasil;
- ***State or Province Name*** *(full name) (Some-State):* Nome do estado, usaremos Santa Catarina;
- ***Locality name*** *(eg, city):* Nome da cidade, usaremos Joinville;
- ***Organization Name*** *(eg, company) (Intermet Widgits Pty Ptl):* Nome da Empresa usaremos TOTVS S/A;
- ***Organization Unit Name*** *(eg, section):* Nome da unidade da empresa, caso só tenho uma coloque o mesmo da anterior, usarei TOVTVS Joinville SC;
- ***Common Name*** *(e.g. server FQDN or YOUR name):* O nome comum é o seu nome na *WEB* seu endereço(Domínio), usaremos portalweb.com.br;
- ***Email Adress***: e-mail da empresa yuri@totvs.com.br;
- ***A challenge password***: uma senha, este campo é opcional e eu deixaremos em branco neste exemplo;
- ***An optional company name***: uma nova identificação de nome da empresa, este campo é opcional e eu deixarei em branco.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Será gerado o um arquivo que é o CSR, solicitação da assinatura:



3. Comprar um certificado digital

Após a geração do CSR você precisa comprar um certificado digital para o domínio descrito no passo acima, entre em contato a sua certificadora de preferencia informado o CSR, algumas certificadora permitirão a inclusão do arquivo ou o conteúdo dele no formulário, após o tramite da compra você receberá o certificado que deverá estar em formato **.pfx**. Caso seu certificado não venha no formato **.pfx**. Veja como converter no item 4.

4. Transformar arquivo PFX em PEM

A partir dessa etapa estamos no processo de configuração que não depende mais dos processos de compra, e o cliente irá fornecer este arquivo.
Para configurar o consumo do e-CPF no *Tomcat* iremos converter o arquivo **PFX** em **PEM**, separar o certificado da chave privada, também será necessário baixar a cadeia de certificados que será aceita, no item 6 deste manual falaremos sobre o E-CPF que será usado no Cliente e a cadeia configurada aqui deverá ser a mesma que o cliente irá comprar o e-CPF.
Digite no *prompt* de comando a instrução para extrair a chave em formato **PEM**. Será solicitado a chave do certificado que você comprou:

```
openssl pkcs12 -in PORTAL_WEB.PFX -nocerts -out key.pem
```

Digite no *prompt* de comando a instrução para extrair o Cerificado em formato **PEM**:

```
openssl pkcs12 -in MULTILOG_SUL_ARMAZENS_GERAIS_LTDA.pfx -clcerts -nokeys -out cert.pem
```

Baixe a cadeia de certificados **Raiz** da certificadora que irá fornecer o certificado do Cliente que será instalado no navegador este arquivo costuma vir com extensão **.cer** arqui vamos assumir que o nome dele é **TrustCACerts.cer**

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

5. Configurar o Tomcat

Dentro da instalação do *SmartClient Html* existe um *Tomcat*, abra o diretório **server\conf** e encontre o arquivo **server.xml** procure pela *tag* ***<Connector***, haverá um previamente configurado na instalação, você pode modificar esta configuração ou simplesmente criar uma nova utilizando portas diferentes, neste caso vamos criar uma nova *tag* ***<Connector***.
Veja como ficou no exemplo e modifique os campos que estão em vermelho para o nome e local dos arquivos correspondentes no seu ambiente:

```
<Connector
        protocol="org.apache.coyote.http11.Http11AprProtocol"
        port="9443"
        maxThreads="200"
        scheme="https"
        secure="true"
        SSLEnabled="true"
        SSLCertificateFile="C:\Temp\cert.pem"
        SSLCertificateKeyFile="C:\temp\key.pem"
        SSLCACertificateFile="C:\Temp\TrustCACerts.cer"
        SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
        SSLVerifyClient="required" />
```

A propriedade *SSLVerifyClient* está configurada como *required* o que significa que sempre será solicitado a autenticação via e-CPF ele pode também também assumir a opção *optional* caso desejar que a autenticação também possa ser utilizada a partir de usuário e senha, pode assumir *none* ou simplesmente não inclui-la caso não seja necessário a autenticação via e-CPF, os demais campos são a chave e certificados gerados nos passos anteriores e a porta que será usada para conexão.
Reinicie o *SmartClient Html*.

6. Instalar certificado e-CPF no cliente

Após a compra do certificado e-CPF pelo cliente instale o certificado na maquina que será usada para o acesso, instale as cadeias de certificado **Raiz** fornecida pela certificadora, fique atendo ao passo descrito no item 4 pois o certificado e-CPF usado pelo cliente tem que pertencer a certificadora **Raiz** que foi configurada no item 4.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Conteúdo de exemplos

- Conteúdo de exemplo da chave privada em formato PEM

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,9FF0349B2DEDA3AC

E9DeZSI6OIUN+s6NAokzgPxtgqZJWLMAWdqzWLL7uERVgDSXvuGugYFW11WKCktd
pcyUuhF+KboOkeWbRI4LfhblnChw8YFEAipWmSs/X2i9XKLmR+yaeICjFms5h+In
ER26Qsa6cbHEOeiyvreSI9H7uSbt6tzYVRHkf4Hi01tvB9JEc+cASvcyzQMyzRFy
H8Ukf9BNFVim/aRbb8ymCu3I+mRB+me5Eqw7U1Zbc29SBMeIIsG9OyRHxWBUxQkY
7UXI2RqvFuiNtJk8v/I5Ja19/1N8WEKE3W+YnbI0Fzm6YIjydQhZPQEW9wS1/7gh
8AFf34okFVzVnLuIrJC970yhMNB3aiYLAKPlWgj+QHRPWgXcYp5jI1c41KOtXOLS
EjU41SUPeowN0KmSoXqyo1M+y0AwMWHkjxeCGuKyIVsro9qq4WpJSNHy65cIoFoR
Ng+D1iBqbFA+lxMKKgOmMMsgnovBEq/zZrNLzeplHUjUbBW626dfgoaumTh0lWkV
Rs2RWQ6m8av/JnU4TBaU1hZ46BoFWSV/Du22TxGQm2cN9aPFcNDu7B7cgQff+DqV
a4vGbyJSA3YA6Vrm4RncCEdrVk3W+puKjk+CGrNPtQLwFu8s62s3SeiWQ39TZLvK
cq/Ocy1fS0/mXvW5jdAHSbalhHUAWferz1BTZPT/GJ/ZHWIqJ6HBSMWIYf8Dunbi
VwoXliTwYu82t7AgML7+vpouC4IwNnJ1z5Grli+Bp9LZipQbN9W/Duhsji8rI4oj
tssl5kZygxhC2bPhdJRXRI1QK+I9c22VSLrQ5OU3VpTYSdlFHIpCoz474i59/fH5
IObzc5EqnfySVzgK7HfshCm69xulr3ed1neZW5hjOOE5vj1yG1hbK9kLksr22baD
jzh0GCgF81CiYrknztmw0BIz8PeS3obysI29pHsWN+o/dvOMp4kzq3f0lC4ClDGI
RuCqPFXScviDPfxAh9k0c4ZU94c+4HIlxt0vFRpufn9RPAWN+f/iil7nIXZHKWsq
zKjomUqV+R6W7bLjbNBYWfsXmjqI4csm6YFmnIrrQDXbocfzi+7NTEJJl0+z6GBS
WqmBdymaW4OUWrcSvWxb2nAdGb/OsEa1qgqYlMnBiLy+pgfr1wfp4VjMKUaEXg7O
aoDuvUi5a6u7/p0lalqrBfLRYmIggdK+DJK6CnfsPXeFRFjHwvLjSF2p54nZ3+Mq
g8L9JhOVvlOhESCF/H47xVF6/fmOIMI114MMRZPJ3xp5kGIPW+dWG7I1qYxqcXAK
1WIrfv341pc7WuagnbGWrkltzb5sZxVmykMj4TJgS6iuGdB+ISPOetmGf3n6vcNH
6hUuvcw0/AxFGCDoqz5CgMXKy+Agp3VLPN3kDJO6nVqQpIkCYgviW5rv2NHYIUCJ
sgWrGOTwcYXLTZQNnPLLz4APZp9IanU4PuUUeW3tNNuAmfzbUcL1zDrbGWANZNVW
0jDVI5kJImkdz2c5tn7dadgZMgvp/F3NMSFFm2Na2s5f0fMuhJHH/LLh0uGX9C0N
Fjjjx/WFfJ3IG0NpGUd8Q+xrg9oEqCksHFIFU1qmHDYQCwq1c7SfWQh/B98gkdBf
-----END RSA PRIVATE KEY-----

- Conteúdo de exemplo do solicitação de assinatura.

-----BEGIN CERTIFICATE REQUEST-----
MIIC7jCCAdYCAQAwgagxCzAJBgNVBAYTAkJSMRcwFQYDVQQIDA5TYW50YSBDYXRh
cmluYTESMBAGA1UEBwwJSm9pbnZpbGxlMRIwEAYDVQQKDAlUT1RWUyBTL0ExGzAZ
BgNVBAsMElRPVFZTIEpvaW52aWxsZSBTQzEZMBcGA1UEAwwQcG9ydGFsd2ViLmNv
bS5icjEgMB4GCSqGSIb3DQEJARYReXVyaUB0b3R2cy5jb20uYnIwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDjIuIKe97mT6Za57Nkkh6DSYSVwR+g2Qem
kQdHjWG9p57Bi4adJNCwxPeGVpZzOUGHg6KvBJQ0gsNADqVnin8aobgWqJmgbFla
lGlDKoPv9+WVN7ScMw1DL9K2aIIo4ZHsY8lk+SXq4gLlHyxZfukBQb77hh9dadpT
P88HLswpYDbnQ5abazeCtxiF8GrjrbZ91VyyTFcByYQkc7jsTCD/VY8a2rLRUocQ
RiFkJ8ZcV8lcMLHvZ/1Q6WVsEVF0ShMPBsMJzdGv+QjwQlPWT7TD7TzfXwx8OfPs
f6Zzk8tve2nP4aSHDZwnY3nwWtWCBXF4UkH+B7NzxJimidsuYtzjAgMBAAGgADAN
BgkqhkiG9w0BAQsFAAOCAQEAYc5IlgZvP9GHdkSBqrfrGtm7gfL91AnejvAumuGc
MI6p1GktWWKRxsIe3vTH7AjRwAxdfjygz2YTTxfQyechGv3RgsiNk6+0ixxSAxPr
x3WZtSlZnV8SeW1fEcz+K3SyftaLWyD0bwLucKaNcaAhPCJl9qkbF3dNZDeyFzuv
7jtR4alWrcG5nkDJKE6Ir22uw4J0WPJG7aRX1rbJkYHlvA8VhcTczx03TVlqQn3Y
bnqdU7idnRIRtRdnC4DS00gFZEDpClzU/PV42JOXlQNzFR4LcP3SbJCcC8qZIoEY
tjTchNQh4Ctceqwy2vrOPaYDz4cMJ6eKILImbC1QVcTNyA==
-----END CERTIFICATE REQUEST-----

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©