

MANUAL DE INTEGRAÇÃO DE SOFTWARE

e-Fatura - Comunicação por webservice - Aspetos genéricos

Versão 1.0

Outubro 2025

HISTÓRICO DE ALTERAÇÕES

Data	Versão	Descrição
29-10-2025	V2.0	Separação entre aspetos gerais e específicos
		Ajustamento consoante o feedback recebido

Índice

1. INTRODUÇÃO 4

2. COMUNICAÇÃO POR *WEBSERVICE* 6
2.1. Fases de implementação 9
2.1.1 Desenvolvimento 9
2.1.2 Testes 11
2.1.3 Distribuição 12
2.1.4 Produção 13
2.2. Estrutura do envio ou da consulta de dados (SOAP) 14
2.2.1 SOAP: Header 15
2.3. Assinatura certificado SSL (CSR) 17
2.3.1 Gerar um certificado SSL 19
2.3.2 Verificar conteúdo do CSR gerado 20
2.3.3 Integrar certificado com a chave privada 20

3. ENDEREÇOS ÚTEIS 21
3.1. Página de produtores de software 21
3.2. Certificação de software de faturação 21
3.3. SAF-T (PT) - Versão portuguesa 21
3.4. Gestão de subutilizadores no PF 21
3.5. WSDL do envio de dados à AT por webservice 21
3.6. WSDL de consulta de documentos à AT por webservice 21
3.7. Para envio de dados por webservice 21
3.8. Para consultar dados por webservice 22

4. TESTE DE CONECTIVIDADE DO *WEBSERVICE* EM TESTES 23

5. GLOSSÁRIO 24

1. Introdução

O “Manual de Integração de Software – e-Fatura: Comunicação por webservice” tem como principal objetivo disponibilizar informação sobre os procedimentos a considerar na transmissão eletrónica, em tempo real, à Autoridade Tributária e Aduaneira (AT), dos elementos dos documentos de faturação emitidos (faturas, documentos de conferência e recibos).

Ciente de que o processo de aperfeiçoamento deve nortear a sua atuação, a AT promoveu melhorias refletidas neste documento, destinado a apoiar empresas ou indivíduos que desenvolvam e/ou comercializem programas de faturação, doravante designados por produtores de software.

Para além dos serviços já disponibilizados por webservice — comunicação em tempo real dos elementos dos documentos emitidos, alteração de estado e correção de erros na comunicação —, foi introduzida a possibilidade de consulta das faturas registadas no sistema e-Fatura, nas quais o NIF do sujeito passivo figure como transmitente ou adquirente.

Este novo desenvolvimento permite integrar, nos softwares de faturação, funcionalidades para obter, por webservice, os elementos das faturas registadas no sistema e-Fatura, associadas a um determinado sujeito passivo, mediante autenticação com as credenciais de acesso ao Portal das Finanças desse sujeito passivo.

Na comunicação por webservice, cada programa de faturação é identificado perante a AT através de um Certificado Digital, emitido pelo produtor de software e assinado digitalmente pela AT.

A comunicação de dados apenas será estabelecida se o programa de faturação enviar o Certificado Digital correspondente. Este certificado garante exclusivamente o estabelecimento da ligação, sendo da responsabilidade do programa a correta transmissão da informação relativa aos documentos emitidos pelos sujeitos passivos.

O desenho do webservice é muito semelhante ao de outros serviços disponibilizados pela AT. Dada esta similitude — resultado da preocupação em reduzir o esforço de desenvolvimento exigido aos produtores de software —, optou-se por dividir este Manual de Integração em dois documentos:

O presente “Manual de Integração de Software – e-Fatura: Comunicação por Webservice, Aspetos Genéricos”, que descreve a fase de implementação, a estrutura do envio de dados (SOAP: header) e os aspetos relacionados com a assinatura e o certificado SSL (CSR);

O documento complementar “Manual de Integração de Software – e-Fatura: Comunicação por Webservice, Aspetos Específicos”, que descreve e exemplifica as estruturas de envio de dados (SOAP: body).

2. Comunicação por *webservice*

A comunicação da informação dos documentos por *webservice* à AT pressupõe o envio à medida que os documentos são emitidos nos programas de faturação, estando associado ao conceito de comunicação em tempo real, ou seja, assim que o sujeito passivo emite um documento comercial, um documento de conferência ou um recibo, os elementos de comunicação obrigatória são de imediato transmitidos à AT.

Cada produtor de software é responsável por implementar um módulo que permita o envio da informação dos documentos à AT, devendo respeitar os seguintes passos:

1. O sujeito passivo emite o documento no programa informático;

2. O programa informático utiliza as credenciais do sujeito passivo, tal como definidas no Portal das Finanças e na gestão de subutilizadores (Nº de Contribuinte e Senha de acesso):

    a) Cada sujeito passivo deve criar um subutilizador para o envio dos dados dos documentos em **Portal das Finanças > Cidadãos > Serviços > Autenticação de Contribuintes > Gestão de Utilizadores**;

    b) A este subutilizador deve ser atribuído o perfil "WFA – Webservice de Comunicação de dados de faturas".

        - A comunicação dos elementos da fatura via web service é efetuada por utilizadores devidamente qualificados para esse efeito. A respetiva habilitação é efetuada no Portal das Finanças e consiste na criação de um subutilizador de perfíl "WFA-Comunicação de dados de faturas" do NIF da entidade emitente do documento a comunicar.

3. Com base nos dados do documento criado no **passo n.º 1** e nas credenciais referidas no **passo n.º 2**, deve construir o pedido SOAP, de acordo com o definido:

    a) No WSDL para **comunicação dos dados** disponível em:

    https://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/Faturacao/Fatcorews/Documents/Fatcorews.wsdl

    b) No WSDL para **consulta de informação** disponível em: **(falta adicionar o WSDL – FATSHARE - INVOICES**):

    A disponibilizar em breve.

Este pedido SOAP (webservice) é composto pelas seguintes secções, que se resumem a:

- SOAP: Header (descrito na secção 2.2 deste documento) - onde se incluem os campos de autenticação do utilizador que vai ser responsável pela invocação do webservice (a senha que vai nesta secção tem que ser cifrada, recorrendo à chave pública do sistema de autenticação do Portal das Finanças);

- SOAP: Body (descrito no manual complementar "Manual de Integração de Software de Comunicação de documentos à AT por webservice, Aspetos Específicos") contém os dados do registo, alteração de estado, eliminação de documentos ou resultado da consulta.

4. Estabelecer uma ligação segura em HTTPS com o Portal das Finanças (utilizando o certificado SSL previamente submetido e assinado pela AT, através do processo de adesão ao envio de dados dos documentos por parte dos produtores de software) ao seguinte endereço:

    a) Para envio de dados de faturas:
    https://servicos.portaldasfinancas.gov.pt:723/fatcorews/ws/

    b) Para consulta de dados de faturas:
    https://servicos.portaldasfinancas.gov.pt:725/fatshare/ws/fatshareFaturas

5. Processar corretamente a resposta devolvida pelo webservice, que pode ser de quatro tipos:

    a) Mensagens de autenticação inválida;

    b) Mensagens de processamento inválido dos dados do pedido;

    c) Registo com sucesso dos dados do documento.

    d) Lista dos documentos consultados.

Para adaptar os programas de faturação, é recomendada a execução das seguintes fases implementação:

- Desenvolvimento

- Testes

- Distribuição
- Produção

2.1. Fases de implementação

2.1.1 Desenvolvimento

Para poder iniciar o desenvolvimento, cada produtor de software deve obter, junto da AT, os elementos necessários para o efeito, designadamente:

1. Criar um subutilizador do próprio produtor de software, em **Portal das Finanças > Cidadãos > Serviços > Autenticação de Contribuintes > Gestão de Utilizadores**;

2. Obter a chave pública do Sistema de Autenticação do Portal das Finanças para cifrar a senha do utilizador;

3. Obter certificado SSL para comunicação com o endereço de testes;

4. Obter o WSDL que define a estrutura do pedido SOAP a construir para enviar os dados de documentos, disponível em:

   Portal das Finanças > Cidadãos > Serviços > e-Fatura > página **Produtores de Software >** opção **Testar Webservice**

Ao criar o subutilizador no Portal das Finanças (1º passo), deve atribuir a autorização WFA disponível para a comunicação de dados de documentos. Para criar este utilizador, é necessário indicar um Nome, uma senha (e respetiva confirmação) e um endereço de email para utilização em contactos por parte da AT. No final, obtém a identificação do subutilizador (e.g., 555555555/55) e a respetiva senha deve ser comunicada à equipa de desenvolvimento.

O envio de dados de documentos tem de respeitar o WSDL definido para o efeito e disponível na página de produtores de software:

Portal das Finanças > Cidadãos > Serviços > e-Fatura > página **Produtores de Software >** opção **Testar Webservice**

Para obter a chave pública do Sistema de Autenticação e o certificado SSL de comunicação em testes é necessário enviar um email à AT a solicitar o envio dos mesmos. A mensagem a enviar por email deve respeitar o seguinte modelo:

TO:	asi-cd@at.gov.pt
Subject:	Obtenção do certificado SSL para testes e chave pública do sistema de Autenticação – NIF <NIF>

Exmos. Senhores,

O Produtor de Software <NOME> (NIF <NIF>) vem por este meio solicitar o envio dos seguintes elementos para desenvolvimento e testes de envio de documentos por webservice:

- Chave pública do Sistema de Autenticação do Portal das Finanças;
- Certificado SSL para comunicação com o endereço de testes de webservices.

Estes elementos serão utilizados por este produtor de software para incluir nos seguintes programas de faturação:

Designação Software	**Certificado AT / DGCI**
<SOFTWARE 1>	<CERTIFICADO 1>
…	...
<SOFTWARE N>	<CERTIFICADO N>

Aguardamos a vossa resposta.

Na comunicação, cada produtor de software deve substituir os seguintes elementos pelos seus dados:

<NIF> - Substituir pelo NIF do produtor de software;

<NOME> - Substituir pelo Nome do produtor de software;

<SOFTWARE N> - Designação do software N;

<CERTIFICADO N> - Nº de certificado da AT (DGCI se ainda for o caso).

Para a correta construção do pedido SOAP (invocação do webservice), deve utilizar a informação complementar, disponível neste documento na secção 2.2 e no documento complementar “Manual de Integração de Software – e-Fatura: Comunicação por Webservice,

Aspetos Específicos", onde se detalha a informação que deve constar dos campos do pedido SOAP, bem como a sua forma de construção

2.1.2 Testes

A AT disponibiliza um endereço de testes para verificação da comunicação de dados à AT, de forma a apoiar cada produtor de software na correta disponibilização dos seus programas aos sujeitos passivos, seus clientes.

Para este efeito, cada produtor de software deve seguir o seguinte procedimento:

1. Solicitar as credenciais de subutilizador e senha criada para os testes de comunicação de documentos (e.g., 555555555/55 + SENHA);

2. Cifrar a senha e compor o SOAP: Header de acordo com o definido na **secção 2.2.1**;

3. Com base na operação pretendida (envio, alteração de estado ou eliminação de documento, ou consulta), construir o SOAP: Body de acordo com o definido no documento complementar "Manual de Integração de Software – e-Fatura: Comunicação por Webservice, Aspetos Específicos",

4. Estabelecer uma ligação HTTPS com o seguinte endereço disponibilizado apenas para testes:

    a) https://servicos.portaldasfinancas.gov.pt:723/fatcorews/ws

    b) https://servicos.portaldasfinancas.gov.pt:725/fatshare/ws/fatshareFaturas

    c) Estes endereços só aceitam ligações com o certificado SSL disponibilizado para testes (vide **secção 2.1.1**);

5. Submeter o pedido SOAP construído no ponto 3;

6. Processar a resposta que o serviço lhe devolve de acordo com as várias hipóteses definidas no documento complementar "Manual de Integração de Software – e-Fatura: Comunicação por Webservice, Aspetos Específicos". As respostas são dos seguintes tipos:

    a) Erros de autenticação referentes aos campos do SOAP: Header;

    b) Erros nos dados dos pedidos referentes aos campos preenchidos no SOAP: Body.

    c) Código de sucesso;

d) Lista dos documentos consultados;

Para efeitos de despiste, é disponibilizada uma página de testes de conectividade na **secção 4** deste documento. Também foram disponibilizados exemplos de pedido e resposta SOAP para comparação com o programa do produtor de software na **secção 1.1** do documento complementar "Manual de Integração de Software – e-Fatura: Comunicação por Webservice, Aspetos Específicos".

2.1.3 Distribuição

Depois de confirmarem a correta adaptação dos programas informáticos e antes de os distribuir, é necessário proceder da seguinte forma:

1. Efetuar a adesão ao envio de dados de documentos, através do formulário disponível em:

   Portal das Finanças > Cidadãos > Serviços > e-Fatura > página **Produtores de Software >** opção **Aderir ao Serviço**

   a) É necessário aceitar os termos e condições do serviço, disponíveis para consulta no formulário;

   b) Para completar o pedido de adesão, é necessário gerar um certificado SSL de acordo com as instruções disponíveis na **secção 2.3.1**;

   c) A AT responde a este pedido por mensagem de email, contendo o certificado assinado com o certificado digital da AT;

2. Alterar o endereço de comunicação para o endereço de comunicação de dados à AT em ambiente de produção:

   https://servicos.portaldasfinancas.gov.pt:423/fatcorews/ws

3. Alterar o endereço de comunicação para o endereço de consulta de dados à AT em ambiente de produção:

   https://servicos.portaldasfinancas.gov.pt:425/fatshare/ws/fatshareFaturas

4. Substituir o certificado utilizado em testes (ponto 4 da Fase de Testes) pelo certificado de produção emitido no ponto 1 alínea c) desta fase.

Depois de concluído este procedimento, o programa informático está pronto para ser distribuído aos clientes (sujeitos passivos).

2.1.4 Produção

Depois de instalado o programa de faturação nos computadores dos utilizadores (sujeitos passivos), estão criadas as condições para a comunicação dos elementos dos documentos de faturação emitidos por esta via.

Cada sujeito passivo deve criar um subutilizador para a comunicação de dados dos documentos, de forma em tudo idêntica ao definido no ponto 1 da Fase de Desenvolvimento (vide **secção 2.1.1**) e com permissões WFA, ou seja, para a comunicação de documentos à AT.

Depois de criado este subutilizador, o sujeito passivo, responsável pelas credenciais emitidas (utilizador e senha), deve configurar no programa informático com estas credenciais, através de opção própria.

Por regra, o envio prossegue da seguinte forma:

1. O sujeito passivo emite o documento no programa informático;
2. São obtidas as credenciais do sujeito passivo configuradas no programa informático;
3. É construído o pedido SOAP e invocado o *webservice* em produção com os dados do ponto 1 e ponto 2;
4. O programa processa a resposta do serviço e informa o utilizador do sucesso ou solicita uma ação do utilizador, para o caso de erro no envio.

2.2. Estrutura do envio ou da consulta de dados (SOAP)

O serviço de comunicação de dados de documentos em tempo real disponibiliza as seguintes operações, que possibilita o envio dos elementos previstos no n.º 4 do Artigo 3.º do Decreto-Lei n.º 198/2012, de 24 de agosto:

- Registo de Documento Comercial;
- Alteração de estado do Documento Comercial;
- Eliminação da comunicação do Documento Comercial;[1]
- Registo de Documento de Conferência;
- Alteração de estado do Documento de Conferência;
- Eliminação da comunicação do Documento de Conferência;[2]
- Registo de Recibo emitido no âmbito do regime de IVA de Caixa;
- Alteração de estado do Recibo emitido no âmbito do regime de IVA de Caixa;
- Eliminação da comunicação do Recibo emitido no âmbito do regime de IVA de Caixa.[3]

Paralelamente o serviço de comunicação disponibiliza uma operação que permite a consulta de informação:

- Consulta de documentos Comerciais (exceto os comunicados ao abrigo do n.º 6 do art. 3º do Decreto-Lei n.º 198/2012, de 24 de agosto).

O pedido é efetuado segundo o protocolo SOAP e é constituído por duas secções:

a) SOAP: Header;

b) SOAP: Body.

A primeira secção, o Header, inclui todos os campos de autenticação do utilizador que vai ser responsável pela invocação do *webservice*. Este utilizador será um subutilizador do NIF do sujeito passivo (emitente) com perfil WFA.

Para criar o subutilizador, deve aceder ao **Portal das Finanças > Cidadãos > Serviços > Autenticação de Contribuintes > Gestão de Utilizadores**.

A segunda secção, dependendo da operação que está a ser realizada, contém elementos de registo de documentos, alteração de estado, eliminação da comunicação ou informação referente às faturas consultadas, os quais se detalham no tópico SOAP: Body.

[1] **Se o período de comunicação do documento ainda estiver dentro do prazo o processo é automático, caso contrário o pedido de eliminação deve ser acompanhado no portal do e-Fatura.**
[2] **Idem.**

2.2.1 SOAP: Header

O desenho do Header tem como requisito garantir a confidencialidade dos dados de autenticação e a impossibilidade de reutilização dos mesmos em ataques Man-in-the-middle (MITM). Por este motivo, só serão aceites invocações que respeitem os procedimentos de encriptação infra descritos.

O SOAP: Header é construído de acordo com o standard WS-Security, definido pela OASIS e recorrendo à definição do Username Token Profile 1.1, também definido pela mesma organização. Todas as cadeias de caracteres (strings) aqui referidas devem ser codificadas em UTF-8.

Na seguinte tabela, detalha-se a forma de construção de cada campo, de acordo com as necessidades de segurança específicas do sistema de autenticação do Portal das Finanças.

Parâmetro	Descrição	Obrig.[4]	Tipo Dados[5]
H.1 - Utilizador (Username)	Identificação do utilizador que vai submeter os dados, composto da seguinte forma e de acordo com a autenticação do portal das finanças: <NIF do emitente>/<UserId> Exemplos possíveis: 1. 555555555/1 (subutilizador n.º 1) 2. 555555555/0002 (subutilizador n.º 2) 3. 555555555/1234 (subutilizador n.º 1234)	S	String
H.2 - Password	O campo Password deverá conter a senha do utilizador / subutilizador, a mesma que é utilizada para entrar no Portal das Finanças. Esta senha tem de ser cifrada através da chave simétrica do pedido (ver campo Nonce) e codificado em Base64. $Password := Base64(C_{K_s}^{AES,ECB,PKCS5Padding}(SenhaPF))$ **SenhaPF** := Senha do utilizador definido no campo H.1 - Username; $C_{K_s}^{AES,ECB,PKCS5Padding}$:= Função de cifra utilizando o algoritmo AES, Modelo ECB, PKCS5Padding e a	S	String (base64)

[3] **Idem.**
[4] Obrigatório: S – Sim; N – Não.
[5] A validar na especificação WSDL (*Web Service Definition Language*) do serviço

	chave simétrica do pedido (K_S). **Base64** := Codificação em Base 64 do resultado.		
H.3 - Nonce	Chave simétrica gerada a cada pedido e para cifrar o conteúdo dos campos H.2 - Password e H.4 - Created. Cada invocação do *webservice* deverá conter esta chave gerada aleatoriamente e a qual não pode ser repetida. Para garantir a confidencialidade, a chave simétrica tem de ser cifrada com a chave pública do Sistema de Autenticação de acordo com o algoritmo RSA e codificada em Base 64. A chave pública do sistema de autenticação do Portal das Finanças deve ser obtida de acordo com o definido no ponto 2.1.1 deste manual. O campo é construído de acordo com o seguinte procedimento $$Nonce := Base64(C_{RSA,Kpub_{SA}}(K_s))$$ **K_S** := array de bytes com a chave simétrica de 128 bits, produzida de acordo com a norma AES. **$C_{RSA,KpubSA}$** := Função de cifra da chave simétrica com o algoritmo RSA utilizando a chave pública do sistema de autenticação (K_{pubSA}). **Base64** := Codificação em Base 64 do resultado.	S	String (base64)
H.4 - Data de sistema (Created)	O campo Created deverá conter a data e hora de sistema da aplicação que está a invocar o *webservice*. Esta data é usada para validação temporal do pedido, pelo que é crucial que o sistema da aplicação cliente tenha o seu relógio certo. Sugere-se a sincronização com o Observatório Astronómico de Lisboa: http://www.oal.ul.pt/index.php?link=acerto A zona temporal deste campo deverá estar definida para UTC e formatado de acordo com a norma ISO 8601 tal como é definido pelo W3C: http://www.w3.org/QA/Tips/iso-date http://www.w3.org/TR/NOTE-datetime	S	String (base64)

	e.g.: 2013-01-01T19:20:30.45Z Este campo é cifrado com a chave de pedido (K_S) e codificada em Base 64. $Created := Base64(C_{K_s}^{AES,ECB,PKCS5Padding}(Timestamp))$ **Timestamp** := data hora do sistema (UTC); $C_{K_s}^{AES,ECB,PKCS5Padding}$:= Função de cifra utilizando o algoritmo AES, Modelo ECB, PKCS5Padding e a chave simétrica do pedido (K_S). **Base64** := Codificação em Base 64 do resultado.		

2.2.1.1 Exemplo SOAP:Header

Como resultado da aplicação das regras de construção anteriores será produzido um header de pedido SOAP tal como o seguinte:

```
<S:Header>
   <wss:Security xmlns:wss="http://schemas.xmlsoap.org/ws/2002/12/secext">
      <wss:UsernameToken>
         <wss:Username>599999993/37</wss:Username>
         <wss:Password>ikCyRV+SWfvZ5c6Q0bhrBQ==</wss:Password>
         <wss:Nonce>
            fkAHne7cqurxpImCfBC8EEc2vskyUyNofWi0ptIijYg4gYCxir++unzfPVPpusloEtmLkcZjf+E6
            T9/76tsCqdupUkxOhWtkRH5IrNwmfEW1ZGFQgYTF21iyKBRzMdsJMhhHrofYYV/YhSPdT4dlgG0t
            k9Z736jFuw061mP2TNqHcR/mQR0yW/AEOC6RPumqO8OAfc9/b4KFBSfbpY9HRzbD8bKiTo20n0Pt
            amZevCSVHht4yt/Xwgd+KV70WFzyesGVMOgFRTWZyXyXBVaBrkJS8b6PojxADLcpWRnw5+YeOs3c
            PU2o1H/YgAam1QuEHioCT2YTdRt+9p6ARNElFg==
         </wss:Nonce>
         <wss:Created>YEWoIoqIY5DOD11SeXz+0i4b/AJg1/RgNcOHOYpSxGk</wss:Created>
      </wss:UsernameToken>
   </wss:Security>
</S:Header>
```

2.3. Assinatura certificado SSL (CSR)

A invocação dos serviços web pressupõe um processo de autenticação mediante a validação da chave privada da aplicação, do conhecimento exclusivo do produtor de software (entidade aderente), sendo a respetiva chave pública comunicada e assinada pela AT.

O certificado a ser utilizado na operação é assinado pela AT, a pedido da entidade aderente. Para este efeito, a empresa aderente deve efetuar um pedido de certificado (CSR – Certificate Signing Request).

O CSR é um pequeno ficheiro de texto cifrado que contém o certificado SSL e toda a informação necessária para que a AT possa assinar e devolver o certificado assinado digitalmente, para que possa ser utilizado no processo de autenticação na invocação do serviço web de apoio à submissão de documentos de faturação.

Os procedimentos para geração do CSR são simples, mas variam de acordo com a tecnologia web utilizada pela entidade aderente, razão pela qual devem ser consultados os respetivos manuais de apoio de cada ferramenta.

A informação que o CSR deve conter é a que segue *infra*, não podendo ultrapassar os tamanhos máximos indicados, pois vai ultrapassar o tamanho total aceite para o campo CSR, e onde todos os campos têm de estar preenchidos com informação relevante ou de acordo com a descrição abaixo:

Campo CSR	Descrição	Tamanho Máximo
C = Country	O código de dois caracteres (alfa2) segundo a norma ISO 3166-1referente ao local da sede. Por exemplo, no caso de Portugal é “PT”.	2 (chars)
ST = Province, Region, County or State	Distrito da sede.	32 (chars)
L = Town/City	Local da sede.	32 (chars)
O = Business Name / Organisation	Designação legal da entidade aderente.	180 (chars)
OU = Department Name /Organisational Unit	Departamento para contacto.	180 (chars)
CN = Common Name	Neste campo deve ser indicado o número de identificação fiscal da entidade aderente.	9 (chars)
E = An email address	O endereço de correio eletrónico para contacto, geralmente do responsável pela emissão do CSR ou do departamento de informática. Tem que ser um endereço de email válido.	80 (chars)
Key bit length	Chave pública do certificado SSL criado pelo produtor de software tem de ser gerada com 2048 bits.	2048 (bits)

A utilização de caracteres especiais (e.g., portugueses, línguas latinas, etc.) não é aceite em nenhum dos campos acima indicados, uma vez que a utilização desses caracteres vai invalidar a assinatura digital do certificado SSL.

Como resultado deste processo, a AT procederá à assinatura do certificado e remete em resposta ao pedido o certificado assinado para integração na chave privada do produtor de software.

O certificado terá a validade de 12 meses a contar da data da assinatura.

2.3.1 Gerar um certificado SSL

Um certificado SSL é uma chave RSA composta por duas partes: chave privada e chave pública.

Como a chave privada deve ser apenas do conhecimento do produtor de software, a emissão da mesma tem sempre de ser efetuada pelo próprio, em computador próprio, e nunca num sítio ou serviço web que encontre para o efeito.

Existem diversas ferramentas para geração de certificados SSL, proprietárias e Opensource. Para efeitos de exemplo, a AT utiliza a ferramenta OpenSSL, que é a ferramenta Opensource de referência, livre de custos de utilização.

Para gerar um certificado SSL, cada produtor de software deve fazê-lo no seu próprio computador, utilizando o seguinte comando:

- **openssl req -new -subj** "**/C=**PT**/ST=**Distrito da Sede**/L=**Local da Sede**/O=**Empresa **/OU=**Departamento de Informatica**/CN=**555555555**/E=**informatica@empresa.pt" **-newkey rsa:2048 -nodes -out** 555555555.csr **-keyout** 555555555.key

Cada produtor de software deve substituir a informação específica no comando anterior pelos seus dados, uma vez que os apresentados são apenas exemplificativos, e não deve alterar a informação indicada a **Negrito**.

Como resultado, do comando anterior será gerado o certificado SSL e serão produzidos dois ficheiros:

- 555555555.csr - Ficheiro com o pedido CSR a enviar à AT;
- 555555555.key - Ficheiro com a chave privada gerada.

2.3.2 Verificar conteúdo do CSR gerado

Antes de enviar o CSR para assinatura digital pela AT, pode e deve ser verificado o conteúdo do ficheiro para garantir que toda a informação está como pretendido. Para tal, deve ser usado o seguinte comando:

- **openssl req -text -noout -in** 555555555.csr

Onde cada produtor de software deve substituir os parâmetros que não estão a **Negrito** pelos nomes dos ficheiros corretos.

2.3.3 Integrar certificado com a chave privada

Depois de receber o certificado SSL assinado pela chave digital da AT, é necessário integrar esse certificado com a chave privada gerada no passo anterior (555555555.key). Para tal, deve ser usado o seguinte comando:

- **openssl pkcs12 -export -in** 555555555.crt **-inkey** 555555555.key **-out** 555555555.pfx

Onde cada produtor de software deve substituir os parâmetros que não estão a **Negrito** pelos nomes dos ficheiros corretos.

Como resultado, o certificado SSL assinado pela AT é integrado com a chave privada e gravada com uma senha de acesso que cada produtor de software deve definir na execução do comando.

3. Endereços Úteis

3.1. Página de produtores de software

https://faturas.portaldasfinancas.gov.pt/painelInicialProdSoftware.action

3.2. Certificação de software de faturação

https://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/Faturacao/Paginas/certificacao-de-software.aspx

3.3. SAF-T (PT) - Versão portuguesa

https://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/SAFT_PT/Paginas/news-saf-t-pt.aspx

3.4. Gestão de subutilizadores no PF

https://www.acesso.gov.pt/gestaoDeUtilizadores/consulta?partID=PFAP

3.5. WSDL do envio de dados à AT por webservice

https://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/Faturacao/Fatcorews/Documents/Fatcorews.wsdl

3.6. WSDL de consulta de documentos à AT por webservice

A disponibilizar em breve.

3.7. Para envio de dados por webservice

Ambiente de testes

https://servicos.portaldasfinancas.gov.pt:723/fatcorews/ws/

Ambiente de produção

https://servicos.portaldasfinancas.gov.pt:423/fatcorews/ws/

3.8. Para consultar dados por webservice

Ambiente de testes

https://servicos.portaldasfinancas.gov.pt:725/fatshare/ws/fatshareFaturas

Ambiente de produção

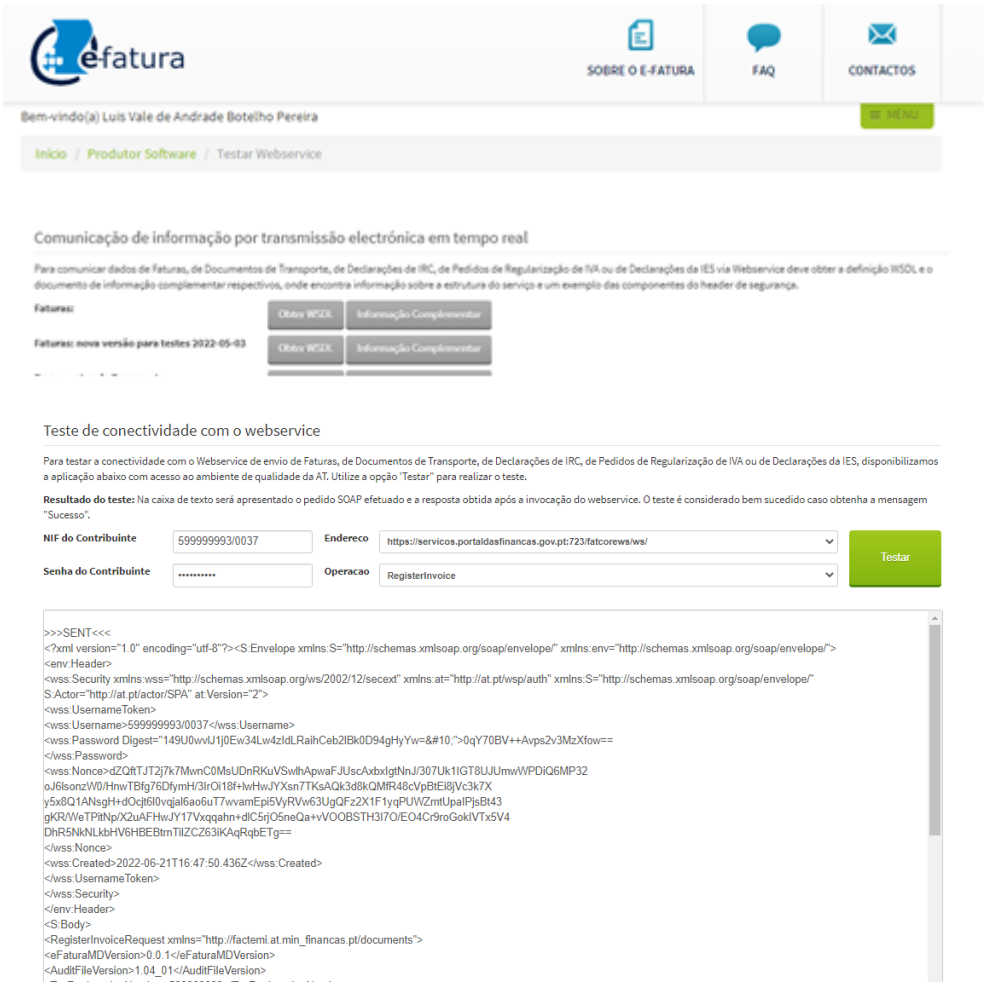
https://servicos.portaldasfinancas.gov.pt:425/fatshare/ws/fatshareFaturas

4. Teste de conectividade do *webservice* em testes

Na página de apoio aos produtores de software, também, é disponibilizado um formulário para testar a conetividade com o *webservice* do ambiente de testes:

https://faturas.portaldasfinancas.gov.pt/testarLigacaoWebService.action

Este formulário simula o envio de dados à AT para o ambiente de testes, com base em credenciais e dados de documentos pré-definidos no formulário. É disponibilizado um campo de texto onde pode ser obtido o pedido SOAP e a resposta do *webservice* em ambiente de testes.



Também, nesta página de teste de conectividade, é disponibilizado o respetivo código fonte para consulta dos produtores de software, como forma de apoio ao desenvolvimento das adaptações que devem efetuar aos seus programas informáticos, de modo a que estes estejam em condições de procederem ao envio de dados por *webservice*, com sucesso.

5. Glossário

Tabela de acrónimos, abreviaturas e definições de conceitos utilizados neste documento, ordenados alfabeticamente por termo.

Termo	Definição
AES	http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
Chave Pública do SA	http://wsautentica.segautenticacaodev.ritta.local/certificates/SA.cer
ECB	Referência do ECB: http://www.itl.nist.gov/fipspubs/fip81.htm Explicação do ECB: http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation#Electronic_codebook_.28ECB.29
OAL	Observatório Astronómico de Lisboa: http://www.oal.ul.pt/ Para acertar a hora do computador seguindo as instruções do Observatório: http://www.oal.ul.pt/index.php?link=acerto
OpenSSL	http://www.openssl.org/
PF	Portal das Finanças: www.portaldasfinancas.gov.pt
PKCS#5	Referência do PKCS #5: http://tools.ietf.org/html/rfc2898 Explicação do PKCS #5: http://en.wikipedia.org/wiki/PKCS
SA	Sistema de autenticação do Portal das Finanças: https://www.acesso.gov.pt/v2/loginForm?partID=PFAP&path=/geral/dashboard. Sistema responsável por validar as credenciais de um utilizador registado no Portal das Finanças.
SAF-T (PT)	https://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/SAFT_PT/Paginas/news-saf-t-pt.aspx
SOAP	http://www.w3.org/TR/soap/
Standard Date Format ISO 8601	http://www.w3.org/TR/NOTE-datetime http://www.w3.org/QA/Tips/iso-date
Username Token Profile	https://www.oasis-open.org/committees/download.php/16782/wss-v1.1-spec-os-UsernameTokenProfile.pdf
Webservice	http://www.w3.org/TR/ws-arch/

WS-Security	https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
WSDL	http://www.w3.org/TR/wsdl