



# MANUAL

## STADAEXPCAU - Webservices

Documentação Técnica

10-01-2023

<b>Classificação</b>	100.10.600
<b>Segurança</b>	Pública
<b>Versão</b>	1.0

#### CIRCUITO DE APROVAÇÃO

<b>Elaborado:</b>	AT-ASA
<b>Verificado:</b>	AT-ASA
<b>Aprovado:</b>	AT-ASA
<b>Data:</b>	16-02-2023

#### HISTÓRICO DE VERSÕES

Versão Anterior	Data de Aprovação	Síntese de Alterações

Otimizado para impressão frente e verso

## Índice

1. Introdução .....	4
2. Estrutura do envio de dados à AT (SOAP) .....	5
3. SOAP:Header .....	6
3.1 Exemplo de SOAP:Header.....	10
4. SOAP:Body.....	11
4.1 Serviço processaMensagem .....	12
4.1.1 Exemplo de SOAP:Body.....	12
4.2 Serviço obterDocumentosPDFNaoEntregues.....	13
4.2.1 Exemplo de SOAP:Body.....	14
4.3 Serviço obterDocumentosPDFEntregues .....	16
4.3.1 Exemplo de SOAP:Body.....	16
4.4 Serviço obterMensagensNaoEntregues .....	18
4.4.1 Exemplo de SOAP:Body.....	18
4.5 Serviço obterMensagensEntregues .....	20
4.5.1 Exemplo de SOAP:Body.....	21
4.6 Serviço entregarDocumentos.....	22
4.6.1 Exemplo de SOAP:Body.....	22
4.7 Código Resultado .....	24
5. Tipos de PDF/Mensagem .....	25
6. Assinatura certificado SSL (CSR).....	25
6.1 Gerar um certificado SSL .....	26
6.2 Verificar conteúdo do CSR gerado.....	27
6.3 Integrar certificado com a chave privada .....	27
7. Endereços Úteis .....	29
7.1 Página de produtores de software .....	29
7.2 Gestão de subutilizadores no Portal das Finanças.....	29
7.3 WSDL do envio de dados à AT por Webservice.....	29
7.4 Endereços para envio de dados à AT por Webservice.....	29

## 1. Introdução

O presente manual contém as especificações técnicas do canal *Webservice* que será disponibilizado aos Operadores Económicos no âmbito do novo sistema de Exportação para a tramitação da Declaração Aduaneira de Exportação (DAE).

Os destinatários deste manual são os Operadores Económicos autorizados pela AT a comunicar eletronicamente com as Estâncias Aduaneiras, utilizando o canal *Webservice*.

Para este canal de comunicação serão disponibilizados serviços para:

- processamento da mensagem enviada pelo operador económico;
- obtenção dos documentos PDF gerados pelo sistema;
- obtenção das notificações/mensagens geradas pelo sistema;
- envio de documentos digitalizados.

A estrutura dos tipos de mensagens enviadas pelo operador económico bem como das mensagens geradas pelo sistema para notificação dos mesmos no âmbito do processo de tramitação da declaração é apresentada no documento **STADAEXPCAU- Guia XML - Definições Gerais** pelo que não serão abordadas neste manual.

## 2. Estrutura do envio de dados à AT (SOAP)

Neste ponto pretende-se descrever a metodologia do *Webservice* do STADAEXPCAU.

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

- **SOAP:Header:**

- Esta secção inclui todos os campos de autenticação do utilizador que vai ser responsável pela invocação do *Webservice*;
- Para aderir ao envio de mensagens de exportação por webservices, o utilizador deverá aceder ao sistema Gestão de Utilizadores Externos (GUE) e seleccionar o sistema automático de exportação (STDEXP);
- O utilizador poderá ser um subutilizador do NIF/EORI do sujeito passivo devendo este ser inscrito também no GUE com acesso ao sistema STDEXP.

- **SOAP:Body:**

- Esta secção contém os dados referentes ao sistema STADAEXPCAU, os quais se detalham no ponto SOAP:Body.

### 3. 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.

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.

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	Obrigatório (S/N)	Tipo de Dados
<b>H.1 – Utilizador (Username)</b>	<p>Identificação do utilizador que vai submeter os dados, composto da seguinte forma e de acordo com a autenticação do Portal das Finanças:</p> <p style="text-align: center;"><b>&lt;NIF&gt;/&lt;SUBUTILIZADOR&gt;</b></p> <p>Exemplos:</p> <ul style="list-style-type: none"> <li>• 1111111111</li> <li>• 55555555/1 (subutilizador n.º 1)</li> <li>• 55555555/0002 (subutilizador n.º 2)</li> <li>• 55555555/1234 (subutilizador n.º 1234)</li> </ul>	S	String

Parâmetro	Descrição	Obrigatório (S/N)	Tipo de Dados
<b>H.2 – Password</b>	<p>O campo Password deverá conter a senha do utilizador/subutilizador, a mesma que é utilizada para entrar no Portal das Finanças.</p> <p>Esta Password tem de ser cifrada através da chave simétrica do pedido (ver <b>H.3 – Nonce</b>) e codificado em Base64.</p> <p style="text-align: center;"><b>Password</b></p> <p><math>:= \text{Base64}(C_{K_S}^{\text{AES,ECB,PKCS5Padding}}(\text{Senha}))</math></p> <p><b>SenhaPF</b> := Senha do utilizador definido no campo</p> <p>H.1 – Username;</p> <p><math>C_{K_S}^{\text{AES,ECB,PKCS5Padding}}</math> := Função de cifra utilizando o algoritmo AES, Modelo ECB, PKCS5Padding e a chave simétrica do pedido (<math>K_S</math>).</p> <p><b>Base64</b> := Codificação em Base 64 do resultado.</p>	S	string (base64)

Parâmetro	Descrição	Obrigatório (S/N)	Tipo de Dados
<b>H.3 – Nonce</b>	<p>Chave simétrica gerada a cada pedido e para cifrar o conteúdo dos campos H.3 - Password e H.4 - Created.</p> <p>Cada invocação do <i>Webservice</i> deverá conter esta chave gerada aleatoriamente e a qual não pode ser repetida.</p> <p>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.</p> <p>A chave pública do sistema de autenticação do Portal das Finanças deve ser obtida por solicitação própria e através do endereço de email <a href="mailto:asi-cd@at.gov.pt">asi-cd@at.gov.pt</a>.</p> <p>O campo é construído de acordo com o seguinte procedimento:</p> $\mathbf{Nonce} := \mathbf{Base64}(C_{RSA, K_{pub_{SA}}}(K_s))$ <p><math>K_s</math> := array de bytes com a chave simétrica de 128 bits, produzida de acordo com a norma AES.</p> <p><math>C_{RSA, K_{pub_{SA}}}</math> := Função de cifra da chave simétrica com o algoritmo RSA utilizando a chave pública do sistema de autenticação (<math>K_{pub_{SA}}</math>).</p> <p><b>Base64</b> := Codificação em Base 64 do resultado.</p>	S	String (base64)



Parâmetro	Descrição	Obrigatório (S/N)	Tipo de Dados
<b>H.4 – Data de sistema (Created)</b>	<p>O campo <b>Created</b> deverá conter a data e hora de sistema da aplicação que está a invocar o <i>webservice</i>.</p> <p>Esta data é usada para validação temporal do pedido, pelo que é crucial que o sistema da aplicação cliente tenha o seu relógio certo.</p> <p>Sugere-se a sincronização com o Observatório Astronómico de Lisboa:  <a href="http://www.oal.ul.pt/index.php?link=acerto">http://www.oal.ul.pt/index.php?link=acerto</a></p> <p>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:  <a href="http://www.w3.org/QA/Tips/iso-date">http://www.w3.org/QA/Tips/iso-date</a>  <a href="http://www.w3.org/TR/NOTE-datetime">http://www.w3.org/TR/NOTE-datetime</a></p> <p>Exemplo: 2017-01-01T19:20:30.45Z</p> <p>Este campo é cifrado com a chave de pedido (KS) e codificada em Base 64.</p> <p><b>Created</b>  <math>:= \text{Base64}(C_{K_S}^{\text{AES,ECB,PKCS5Padding}}(\text{Time}))</math></p> <p><b>Timestamp</b> := data hora do sistema (UTC);</p> <p><math>C_{K_S}^{\text{AES,ECB,PKCS5Padding}}</math> := Função de cifra utilizando o algoritmo AES, Modelo ECB, PKCS5Padding e a chave simétrica do pedido (K<sub>S</sub>).</p> <p><b>Base64</b> := Codificação em Base 64 do resultado.</p>	S	string (base64)

### 3.1 Exemplo de SOAP:Header

Como resultado da aplicação das regras de construção anteriores será produzido um *header* de pedido SOAP tal como se apresenta no seguinte exemplo:

```
<S:Header>
  <wss:Security xmlns:wss="http://schemas.xmlsoap.org/ws/2002/12/secext">
    <wss:UsernameToken>
      <wss:Username>500000016/15</wss:Username>
      <wss:Password>ikCyRV+SWfvZ5c6Q0bhrBQ==</wss:Password>
      <wss:Nonce>
        fkAHne7cquxplmCfBC8EEc2vskyUyNofWi0ptlijYg4gYCxir++unzfPVPpusloEtmLkcZjf+E6T9/7
        6tsCqdupUkxOhWtkRH5lrNwmfEW1ZGFQgYTF21iyKBRzMdsJMhhHrofYYV/YhSPdT4dlgG0tk
        9Z736jFuw061mP2TNqHcR/mQR0yW/AEOC6RPumqO8Oafc9/b4KFBSfbpY9HRzbD8bKiTo20
        n0PtamZevCSVHht4yt/Xwgd+KV70WFzyesGVMOGFRTWZyXyXBVaBrkJS8b6PoixADLcpWRnw
        5+YeOs3cPU2o1H/YgAam1QuEHioCT2YTdRt+9p6ARNEIFg==
      </wss:Nonce>
      <wss:Created>>YEWoloqIY5DOD11SeXz+0i4b/AJg1/RgNcOH0YpSxGk</wss:Created>
    </wss:UsernameToken>
  </wss:Security>
</S:Header>
```

## 4. SOAP:Body

Nesta secção são definidos os serviços para a criação, anulação ou alteração de declarações, bem como a obtenção de documentos ou mensagens.

Os métodos definidos para este *Webservice* são:

Método	Descrição
<b>processaMensagem</b>	<p>Serviço que permite processar os tipos de mensagens:</p> <ul style="list-style-type: none"> <li>• <b>PT507C</b> – Comunicação de chegada à saída;</li> <li>• <b>PT511C</b> – Notificação de apresentação das mercadorias;</li> <li>• <b>PT513C</b> – Pedido de Alteração da DAE;</li> <li>• <b>PT514C</b> – Pedido de Anulação da DAE;</li> <li>• <b>PT515C</b> – Declaração aduaneira de exportação (DAE);</li> <li>• <b>PT583C</b> – Resposta ao pedido de informação sobre exportação sem saída (Procedimento de inquérito);</li> </ul>
<b>obterDocumentosPDFEntregues</b>	<p>Serviço que permite a um operador obter os documentos PDF já entregues anteriormente para uma determinada DAE.</p> <p>Este serviço permite pesquisar por NRL e Tipo de PDF, para um único NRL.</p>
<b>obterDocumentosPDFNaoEntregues</b>	<p>Serviço que permite a um operador obter os documentos PDF que ainda não lhe foram entregues para uma determinada DAE.</p> <p>Este serviço permite pesquisar por NRL e Tipo de PDF, até um máximo de 5 NRL.</p> <p>O serviço retorna ainda um indicador que diz se após esta resposta ainda há mais informação por transmitir (1).</p>
<b>obterMensagensEntregues</b>	<p>Serviço que permite a um operador obter as mensagens XML já entregues anteriormente para uma determinada DAE.</p> <p>Este serviço permite pesquisar por NRL e Tipo de XML, para um único NRL.</p>
<b>obterMensagensNaoEntregues</b>	<p>Serviço que permite a um operador obter as mensagens XML que ainda não lhe foram entregues para uma determinada DAE.</p> <p>Este serviço permite pesquisar por NRL e Tipo de XML, até um máximo de 5 NRL.</p> <p>O serviço retorna ainda um indicador que diz se após esta resposta ainda há mais informação por transmitir (1).</p>
<b>entregarDocumentos</b>	<p>Serviço que permite a um operador enviar até um máximo de 20 documentos digitalizados para 1 NRL.</p> <p>Só serão aceites documentos no formato PDF ou PNG.</p> <p>Corresponde à mensagem PTE46C.</p>

- (1) Com o intuito de restringir a dimensão da resposta aos serviços **obterDocumentosPDFNaoEntregues** e **obterMensagensNaoEntregues**, a resposta a estes serviços está limitada a 10 PDFs ou 10 mensagens por DAE (ou seja, por NRL), respetivamente. Assim, caso existam mais dados a transmitir isso será sinalizado na resposta através dum atributo **existeMaisInformacao** e nesse caso o Operador deverá invocar novamente o serviço para obter o resto da informação.

## 4.1 Serviço processaMensagem

### Input

Parâmetros de entrada	Tipo de dados	Tamanho	Mín/Máx	Descrição
<b>processaMensagemInput</b>	<b>Objeto</b>		<b>1..1</b>	<b>Objeto de input.</b>
mensagem	byte[]		1..1	Mensagem em base64.
tipo	String		1..1	Tipo de mensagem.

### Output

Parâmetros de saída	Tipo de dados	Mín/Máx	Descrição
<b>resultadoProcessamento</b>	<b>Objeto</b>	<b>1..1</b>	<b>Objeto de output.</b>
codigoResultado	String	1..1	Código de resultado.
descricaoResultado	String	1..1	Descrição do resultado.
dataEnvio	String	1..1	Data e hora de envio da resposta.

#### 4.1.1 Exemplo de SOAP:Body

Como resultado da aplicação do serviço **processaMensagem** será produzido um *body* de pedido SOAP tal como se apresenta no seguinte exemplo:

```

<soapenv:Body>
  <web:processaMensagem>
    <processaMensagemInput>
      <mensagem>Mensagem do tipo PT507C em base64</mensagem>
      <tipo>PT507C</tipo>
    </processaMensagemInput>
  </web:processaMensagem>
</soapenv:Body>
  
```

A este pedido o sistema responde da seguinte forma:

```
<env:Body>
  <m:processaMensagemResponse>
    <return>
      <resultadoProcessamento>
        <codigoResultado>0</codigoResultado>
        <descricaoResultado> Mensagem submetida com sucesso.</descricaoResultado>
      </resultadoProcessamento>
      <dataEnvio>2020-12-12 19:30</dataEnvio>
    </return>
  </m:processaMensagemResponse>
</env:Body>
```

## 4.2 Serviço obterDocumentosPDFNaoEntregues

### Input

Parâmetros de entrada	Tipo de dados	Tamanho	Mín/Máx	Descrição
<b>obterDocumentosPDFNaoEntreguesInput</b>	<b>Objeto</b>		<b>1..1</b>	<b>Objeto de Input.</b>
<b>listaNRLs</b>	<b>ArrayList</b>		<b>1..5</b>	<b>Lista de Números de Referência Local.</b>
numeroReferenciaLocal	String	22	1..1	Número de Referência Local da declaração.
tipo	String	3	0..1	Tipo de PDF.

### Output

Parâmetros de saída	Tipo de dados	Mín/Máx	Descrição
<b>resultadoProcessamento</b>	<b>Objeto</b>	<b>1..1</b>	<b>Resultado do processamento da mensagem.</b>
codigoResultado	String	1..1	Código de resultado.
descricaoResultado	String	1..1	Descrição do resultado.
<b>declaracao</b>	<b>Objeto</b>	<b>0..5</b>	
numeroReferenciaLocal	String	1..1	Número de referência local que identifica a declaração.
codigoResultado	String	0..1	Código de resultado do NRL (caso existam erros).
descricaoResultado	String	0..1	Descrição do resultado.
<b>ficheiroResposta</b>	<b>Objeto</b>	<b>0..n</b>	<b>Lista de resultados dos documentos PDF não entregues.</b>
nomeFicheiro	String	1..1	Nome do ficheiro.
ficheiro	String	1..1	Documento em base64.
existeMaisInformacao	String	1..1	Indicador da existência de mais PDFs.

			Se existirem mais PDFs será devolvido <b>true</b> , caso contrário será devolvido <b>false</b> .
dataEnvio	String	1..1	Data e hora de envio da resposta.

#### 4.2.1 Exemplo de SOAP:Body

Como resultado da aplicação do serviço **obterDocumentosPDFNaoEntregues** será produzido um *body* de pedido SOAP tal como se apresenta no seguinte exemplo:

```

<soapenv:Body>
  <web:obterDocumentosPDFNaoEntregues>
    <obterDocumentosPDFNaoEntreguesInput>
      <listaNRLs>
        <numeroReferenciaLocal>20PT999999999000000001</numeroReferenciaLocal>
        <numeroReferenciaLocal>20PT999999999000000002</numeroReferenciaLocal>
        <numeroReferenciaLocal>20PT999999999000000003</numeroReferenciaLocal>
        <numeroReferenciaLocal>20PT999999999000000004</numeroReferenciaLocal>
        <numeroReferenciaLocal>20PT999999999000000005</numeroReferenciaLocal>
      </listaNRLs>
      <tipo>VAL</tipo>
    </obterDocumentosPDFNaoEntreguesInput>
  </web:obterDocumentosPDFNaoEntregues>
</soapenv:Body>
  
```

Como resultado desta invocação será devolvido o seguinte:

```

<env:Body>
  <m:obterDocumentosPDFNaoEntreguesResponse>
    <return>
      <resultadoProcessamento>
        <codigoResultado>0</codigoResultado>
        <descricaoResultado> Mensagem processada com sucesso.</descricaoResultado>
      </resultadoProcessamento>
      <declaracao>
        <numeroReferenciaLocal>20PT999999999000000001</numeroReferenciaLocal>
      </declaracao>
    </return>
  </m:obterDocumentosPDFNaoEntreguesResponse>
</env:Body>
  
```

```
<codigoResultado>100</codigoResultado>
<descricaoResultado>Dados encontrados.</descricaoResultado>
<ficheiroResposta>
  <nomeFicheiro> Documento A </nomeFicheiro>
  <ficheiro> Documento em base64</ficheiro>
</ficheiroResposta>
<ficheiroResposta>
  <nomeFicheiro> Documento B </nomeFicheiro>
  <ficheiro> Documento em base64</ficheiro>
</ficheiroResposta>
<existeMaisInformacao>true</existeMaisInformacao>
</declaracao>
<declaracao>
  <numeroReferenciaLocal>20PT999999999000000002</numeroReferenciaLocal>
  <codigoResultado>102</codigoResultado>
  <descricaoResultado>Número de Referência Local inexistente.</descricaoResultado>
  <existeMaisInformacao>false</existeMaisInformacao>
</declaracao>
<dataEnvio>2020-12-12 19:30</dataEnvio>
</return>
</m:obterDocumentosPDFNaoEntreguesResponse>
</env:Body>
```

### 4.3 Serviço obterDocumentosPDFEntregues

#### Input

Parâmetros de entrada	Tipo de dados	Tamanho	Mín/Máx	Descrição
<b>obterDocumentosInput</b>	<b>Objeto</b>		<b>1..1</b>	<b>Objeto de Input.</b>
numeroReferenciaLocal	String	22	1..1	Número de Referência Local da declaração.
tipo	String	3	0..1	Tipo de PDF.

#### Output

Parâmetros de saída	Tipo de dados	Mín/Máx	Descrição
<b>resultadoProcessamento</b>	<b>Objeto</b>	<b>1..1</b>	<b>Resultado do processamento da mensagem.</b>
codigoResultado	String	1..1	Código de resultado.
descricaoResultado	String	1..1	Descrição do resultado.
<b>declaracao</b>	<b>Objeto</b>	<b>0..1</b>	
numeroReferenciaLocal	String	1..1	Número de referência local que identifica a declaração
codigoResultado	String	0..1	Código de resultado do NRL (caso existam erros).
descricaoResultado	String	0..1	Descrição do resultado.
<b>ficheiroResposta</b>	<b>Objeto</b>	<b>0..n</b>	<b>Lista de resultados dos documentos PDF entregues.</b>
nomeFicheiro	String	1..1	Nome do ficheiro.
ficheiro	String	1..1	Documento em base64.
dataEnvio	String	1..1	Data e hora de envio da resposta.

#### 4.3.1 Exemplo de SOAP:Body

Como resultado da aplicação do serviço **obterDocumentosPDFEntregues** será produzido um *body* de pedido SOAP tal como se apresenta no seguinte exemplo:

```
<soapenv:Body>
  <web:obterDocumentosPDFEntregues>
    <obterDocumentosInput>
      <numeroReferenciaLocal>20PT999999999000000001</numeroReferenciaLocal>
      < tipo>VAL</tipo>
    </obterDocumentosInput>
  </web:obterDocumentosPDFEntregues>
</soapenv:Body>
```



A este pedido o sistema responde da seguinte forma:

```
<env:Body>
  <m:obterDocumentosPDFEntreguesResponse>
    <return>
      <resultadoProcessamento>
        <codigoResultado>0</codigoResultado>
        <descricaoResultado> Mensagem processada com sucesso.</descricaoResultado>
      </resultadoProcessamento>
      <declaracao>
        <numeroReferenciaLocal>20PT999999999000000001</numeroReferenciaLocal>
        <codigoResultado>100</codigoResultado>
        <descricaoResultado> Dados encontrados.</descricaoResultado>
        <ficheiroResposta>
          <nomeFicheiro> Documento A </nomeFicheiro>
          <ficheiro> Documento em base64</ficheiro>
        </ficheiroResposta>
        <ficheiroResposta>
          <nomeFicheiro> Documento B </nomeFicheiro>
          <ficheiro> Documento em base64</ficheiro>
        </ficheiroResposta>
      </declaracao>
      <dataEnvio>2020-12-12 19:30</dataEnvio>
    </return>
  </m:obterDocumentosPDFEntreguesResponse>
</env:Body>
```

## 4.4 Serviço obterMensagensNaoEntregues

### Input

Parâmetros de entrada	Tipo de dados	Tamanho	Mín/Máx	Descrição
<b>obterMensagensInput</b>	<b>Objeto</b>		<b>1..1</b>	<b>Objeto de Input.</b>
<b>listaNRLs</b>	<b>ArrayList</b>		<b>1..5</b>	<b>Lista de Números de Referência Local.</b>
numeroReferenciaLocal	String	22	1..1	Número de Referência Local da declaração.
tipo	String	3	0..1	Tipo de Mensagem.

### Output

Parâmetros de saída	Tipo de dados	Mín/Máx	Descrição
<b>resultadoProcessamento</b>	<b>Objeto</b>	<b>1..1</b>	<b>Resultado do processamento da mensagem.</b>
codigoResultado	String	1..1	Código de resultado.
descricaoResultado	String	1..1	Descrição do resultado.
<b>declaracao</b>	<b>Objeto</b>	<b>0..5</b>	
numeroReferenciaLocal	String	1..1	Número de referência local que identifica a declaração
codigoResultado	String	0..1	Código do resultado para o NRL (caso existam erros).
descricaoResultado	String	0..1	Descrição do resultado.
<b>ficheiroResposta</b>	<b>Objeto</b>	<b>0..n</b>	<b>Lista de resultados das mensagens XML não entregues.</b>
nomeFicheiro	String	1..1	Nome do ficheiro.
ficheiro	String	1..1	Documento em base64.
existeMaisInformacao	String	1..1	Indicador da existência de mais mensagens XML. Se existirem mais mensagens XML será devolvido <b>true</b> , caso contrário será devolvido <b>false</b> .
dataEnvio	String	1..1	Data e hora de envio da resposta.

### 4.4.1 Exemplo de SOAP:Body

Como resultado da aplicação do serviço **obterMensagensNaoEntregues** será produzido um *body* de pedido SOAP tal como se apresenta no seguinte exemplo:

```
<soapenv:Body>
  <web:obterMensagensNaoEntregues>
    <obterMensagensNaoEntreguesInput>
      <listaNRLs>
        <numeroReferenciaLocal>20PT999999999000000001</numeroReferenciaLocal>
        <numeroReferenciaLocal>20PT999999999000000002</numeroReferenciaLocal>
      </listaNRLs>
    </obterMensagensNaoEntreguesInput>
  </web:obterMensagensNaoEntregues>
</soapenv:Body>
```

```
<numeroReferenciaLocal>20PT99999999000000003</numeroReferenciaLocal>  
<numeroReferenciaLocal>20PT99999999000000004</numeroReferenciaLocal>  
<numeroReferenciaLocal>20PT99999999000000005</numeroReferenciaLocal>  
</listaNRLs>  
< tipo>VAL</tipo>  
</obterMensagensNaoEntreguesInput>  
</web:obterMensagensNaoEntregues>  
</soapenv:Body>
```

A este pedido o sistema responde da seguinte forma:

```
<env:Body>  
<m:obterMensagensNaoEntreguesResponse>  
<return>  
<resultadoProcessamento>  
<codigoResultado>0</codigoResultado>  
<descricaoResultado> Mensagem processada com sucesso.</descricaoResultado>  
</resultadoProcessamento>  
<declaracao>  
<numeroReferenciaLocal>20PT99999999000000001</numeroReferenciaLocal>  
<codigoResultado>100</codigoResultado>  
<descricaoResultado> Dados encontrados.</descricaoResultado>  
<ficheiroResposta>  
<nomeFicheiro> Documento A </nomeFicheiro>  
<ficheiro> Documento em base64</ficheiro>  
</ficheiroResposta>  
<ficheiroResposta>  
<nomeFicheiro> Documento B </nomeFicheiro>  
<ficheiro> Documento em base64</ficheiro>  
</ficheiroResposta>  
<existeMaisInformacao>true</existeMaisInformacao>  
</declaracao>
```

```

<declaracao>
  <numeroReferenciaLocal>20PT999999999000000002</numeroReferenciaLocal>
  <codigoResultado>100</codigoResultado>
  <descricaoResultado> Dados encontrados.</descricaoResultado>
  <ficheiroResposta>
    <nomeFicheiro> Documento C </nomeFicheiro>
    <ficheiro> Documento em base64</ficheiro>
  </ficheiroResposta>
  <existeMaisInformacao>true</existeMaisInformacao>
</declaracao>
<dataEnvio>2020-12-12 19:30</dataEnvio>
</return>
</m:obterMensagensNaoEntreguesResponse>
</env:Body>

```

## 4.5 Serviço obterMensagensEntregues

### Input

Parâmetros de entrada	Tipo de dados	Tamanho	Mín/Máx	Descrição
<b>obterMensagensInput</b>	<b>Objeto</b>		<b>1..1</b>	<b>Objeto de Input.</b>
numeroReferenciaLocal	String	22	1..1	Número de Referência Local da declaração.
tipo	String	3	0..1	Tipo de Mensagem.

### Output

Parâmetros de saída	Tipo de dados	Mín/Máx	Descrição
<b>ResultadoProcessamento</b>	<b>Objeto</b>	<b>1..1</b>	Resultado do processamento da mensagem.
codigoResultado	String	1..1	Código de resultado.
descricaoResultado	String	1..1	Descrição do resultado.
<b>declaracao</b>	<b>Objeto</b>	<b>0..1</b>	
numeroReferenciaLocal	String	1..1	Número de referência local que identifica a declaração
codigoResultado	String	0..1	Código do resultado para o NRL (caso existam erros).
descricaoResultado	String	0..1	Descrição do resultado.
<b>ficheiroResposta</b>	<b>Objeto</b>	<b>0..n</b>	Lista de resultados das mensagens XML entregues.
nomeFicheiro	String	1..1	Nome do ficheiro.

ficheiro	String	1..1	Documento em base64.
dataEnvio	String	1..1	Data e hora de envio da resposta.

#### 4.5.1 Exemplo de SOAP:Body

Como resultado da aplicação do serviço **obterMensagensEntregues** será produzido um *body* de pedido SOAP tal como se apresenta no seguinte exemplo:

```
<soapenv:Body>
  <web:obterMensagensEntregues>
    <obterMensagensEntreguesInput>
      <numeroReferenciaLocal>20PT999999999000000001</numeroReferenciaLocal>
      <tipo>VAL</tipo>
    </obterMensagensEntreguesInput>
  </web:obterMensagensEntregues>
</soapenv:Body>
```

A este pedido o sistema responde da seguinte forma:

```
<env:Body>
  <m:obterMensagensEntreguesResponse>
    <return>
      <resultadoProcessamento>
        <codigoResultado>0</codigoResultado>
        <descricaoResultado> Mensagem processada com sucesso.</descricaoResultado>
      </resultadoProcessamento>
      <declaracao>
        <numeroReferenciaLocal>20PT999999999000000001</numeroReferenciaLocal>
        <codigoResultado>100</codigoResultado>
        <descricaoResultado> Dados encontrados.</descricaoResultado>
        <ficheiroResposta>
          <nomeFicheiro> Documento A </nomeFicheiro>
          <ficheiro> Documento em base64</ficheiro>
        </ficheiroResposta>
      </declaracao>
    </return>
  </m:obterMensagensEntreguesResponse>
</env:Body>
```

```

    <ficheiroResposta>
      <nomeFicheiro> Documento B </nomeFicheiro>
      <ficheiro> Documento em base64</ficheiro>
    </ficheiroResposta>
  </declaracao>
  <dataEnvio>2020-12-12 19:30</dataEnvio>
</return>
</m:obterMensagensEntreguesResponse>
</env:Body>
  
```

## 4.6 Serviço entregarDocumentos

### Input

Parâmetros de entrada	Tipo de dados	Tamanho	Mín/Máx	Descrição
<b>identificacaoDeclaracao</b>	<b>Objeto</b>		<b>1..1</b>	<b>Identificação da declaração.</b>
numeroReferenciaLocal	String	22	1..1	Número de Referência Local da declaração.
mrn	String	20	1..1	MRN da declaração.
<b>documento</b>	<b>Objeto</b>		<b>1..20</b>	<b>Lista de documentos a enviar.</b>
codigoDocumento	String	15	1..1	Código do documento.
numAdicao	Short	1	1..1	Número de Adição. Se se tratar de um documento declarado ao nível da declaração então deve ser indicado '0'.
nomeFicheiro	String	22	1..1	Nome do ficheiro a enviar.
conteudoFicheiro	byte[]		1..1	Documento em base64.

### Output

Parâmetros de saída	Tipo de dados	Mín/Máx	Descrição
<b>resultadoProcessamento</b>	<b>Objeto</b>	<b>1..1</b>	<b>Resultado do processamento da mensagem.</b>
codigoResultado	String	1..1	Código de resultado.
descricaoResultado	String	1..1	Descrição do resultado.
<b>documento</b>	<b>Objeto</b>	<b>1..n</b>	<b>Lista dos documentos enviados com o resultado do processamento de cada documento.</b>
codigoDocumento	String	1..1	Código do documento com erro.
nomeFicheiro	String	1..1	Nome do ficheiro com erro.
codigoResultado	String	1..1	Código do resultado para o documento.
descricaoResultado	String	1..1	Descrição do resultado.
dataEnvio	String	1..1	Data e hora de envio da resposta.

#### 4.6.1 Exemplo de SOAP:Body

Como resultado da aplicação do serviço **entregarDocumentos** será produzido um *body* de pedido SOAP tal como se apresenta no seguinte exemplo:

```
<soapenv:Body>
  <web:entregarDocumentos>
    <entregarDocumentosInput>
      <identificacaoDeclaracao>
        <numeroReferenciaLocal>20PT123456987963258741</numeroReferenciaLocal>
        <mrn>20PT1234567889123R1</mrn>
        <numeroProvisorio>899/2020</ numeroProvisorio>

      </identificacaoDeclaracao>
      <documento>
        <codigoDocumento>N380</tipoDocumento>
        <numAdicao>3</ numAdicao>
        <nomeFicheiro>documento_digitalizado1.pdf</nomeFicheiro>
        <conteudoFicheiro> Documento em base64</conteudoFicheiro>
      </documento>
      <documento>
        <codigoDocumento>N750</tipoDocumento>
        <numAdicao>C</ numAdicao>
        <nomeFicheiro>documento_digitalizado2.doc</nomeFicheiro>
        <conteudoFicheiro> Documento em base64</conteudoFicheiro>
      </documento>
    </entregarDocumentosInput>
  </web:entregarDocumentos>
</soapenv:Body>
```

Como resultado desta invocação será devolvido o seguinte:

```
<env:Body>
  <m:entregarDocumentosResponse>
    <return>
      <resultadoProcessamento>
        <codigoResultado>0</codigoResultado>
        <descricaoResultado> Mensagem processada com sucesso.</descricaoResultado>
      </resultadoProcessamento>
    </return>
  </m:entregarDocumentosResponse>
</env:Body>
```

```

</resultadoProcessamento>

<documento>

  <codigoDocumento>N380</codigoDocumento>

  <nomeFicheiro> documento_digitalizado1.pdf </nomeFicheiro>

  <codigoResultado>200</codigoResultado>

  <descricaoResultado>Documento submetido com sucesso.</descricaoResultado>

</documento>

<documento>

  <codigoDocumento>N750</codigoDocumento>

  <nomeFicheiro> documento_digitalizado2.doc </nomeFicheiro>

  <codigoResultado>201</codigoResultado>

  <descricaoResultado>Formato do documento não suportado.</descricaoResultado>

</documento>

<dataEnvio>2020-12-12 19:30</dataEnvio>

</return>

</m:entregarDocumentosResponse>

</env:Body>

```

## 4.7 Código Resultado

A cada invocação, o sistema poderá responder com as mensagens abaixo descritas:

Código	Descrição
<b>Códigos de Resultado genéricos</b>	
0	Mensagem processada com sucesso. / Mensagem submetida com sucesso.
1	Ultrapassado o limite máximo de documentos por pedido.
2	Mensagem inválida.
3	Tipo de mensagem inválido.
9xx	Ocorreu um erro interno. Por favor contacte a AT indicando o identificador: <i>identificador</i>.
<b>Códigos de Resultado específicos – obter PDFs/Mensagens</b>	
100	Dados encontrados.
101	Não foram encontrados resultados para a operação pretendida.
102	Número de Referência Local inexistente.



<b>Códigos de Resultado específicos – enviar Documentos</b>	
200	Documento submetido com sucesso.
201	Formato do documento não suportado.
202	Tamanho máximo ultrapassado.
203	Número da Adição inexistente.
204	Código de documento inválido.

## 5. Tipos de PDF/Mensagem

Nos serviços *obterDocumentosPDFNaoEntregues*, *obterDocumentosPDFEntregues*, *obterMensagensNaoEntregues* e *obterMensagensEntregues*, pode ser especificado o tipo de PDF ou mensagem que se pretende obter.

A lista de valores possíveis encontra-se abaixo descrita:

<b>Código</b>	<b>Descrição</b>
<b>VAL</b>	Devolve os PDFs/mensagens geradas durante a fase de Validação da declaração.
<b>ACE</b>	Devolve os PDFs/mensagens geradas na Aceitação da declaração.
<b>CTR</b>	Devolve os PDFs/mensagens geradas no âmbito de um processo de Controlo da declaração.
<b>RLQ</b>	Devolve os PDFs/mensagens associadas ao registo e notificação da dívida.
<b>AUT</b>	Devolve os PDFs/mensagens geradas no âmbito da Autorização de Saída.
<b>ALT</b>	Devolve os PDFs/mensagens geradas no âmbito de um processo de alteração da declaração.
<b>ANU</b>	Devolve os PDFs/mensagens geradas no âmbito de um processo de anulação da declaração.

## 6. 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 da 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 entidade 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.

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 não pode ultrapassar os tamanhos máximos, conforme a descrição seguinte:

Campo CSR	Descrição	Tamanho Máximo
<b>C = Country</b>	O código ISO de 2 letras referente ao local da sede. Por exemplo, no caso de Portugal é "PT".	2 (chars)
<b>ST = Province, Region, County or State</b>	Distrito da sede.	32 (chars)
<b>L = Town/City</b>	Local da sede.	32 (chars)
<b>CN = Common Name</b>	Neste campo deve ser indicado o número de identificação fiscal da entidade aderente.	9 (chars)
<b>O = Business Name / Organisation</b>	Designação legal da empresa.	180 (chars)
<b>OU = Department Name / Organisational Unit</b>	Departamento para contacto.	180 (chars)
<b>E = An email address</b>	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)
<b>Key bit length</b>	Chave pública do certificado SSL 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 da entidade aderente.

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

## 6.1 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 da entidade aderente, a emissão da mesma tem sempre de ser efetuada pelo próprio, em computador próprio, e nunca num *site* ou serviço web que encontre para o efeito.

Existem diversas ferramentas para geração de certificados SSL, proprietárias e *OpenSource*. A AT utiliza a ferramenta OpenSSL, que é a ferramenta *OpenSource* de referência, livre de custos de utilização.

Para gerar um certificado SSL, cada entidade aderente 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/emailAddress=informatica@empresa.pt" -newkey rsa:2048 -nodes -out 555555555.csr -keyout 555555555.key
```

Cada entidade aderente 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 **Bold**.

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.

## 6.2 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 entidade aderente deve substituir os parâmetros que não estão a **Bold** pelos nomes dos ficheiros corretos.

## 6.3 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 entidade aderente deve substituir os parâmetros que não estão a **Bold** pelos nomes dos ficheiros corretos.

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



## 7. Endereços Úteis

### 7.1 Página de produtores de software

<https://www.portaldasfinancas.gov.pt/pt/external/factemipf/painellInicialProdSoftware.action>

### 7.2 Gestão de subutilizadores no Portal das Finanças

<https://www.acesso.gov.pt/gestaoDeUtilizadores/consulta?partID=PFIN>

### 7.3 WSDL do envio de dados à AT por Webservice

“A definir”

### 7.4 Endereços para envio de dados à AT por Webservice

**Ambiente de desenvolvimento:**

“A definir”

**Ambiente de qualidade:**

“A definir”

**Ambiente de produção:**

“A definir”