



AT
autoridade
tributária e aduaneira



MANUAL DE INTEGRAÇÃO DE SOFTWARE

Comunicação da Declaração Recapitulativa do IVA à AT

HISTÓRICO DE ALTERAÇÕES

VERSÃO	DATA	ALTERAÇÕES
1.0	12-12-2025	Criação do documento.

ÍNDICE

1 INTRODUÇÃO	4
1.1 Namespaces usados	4
2 ENQUADRAMENTO	6
2.1 Comunicação das Declarações por Webservice	6
3 ADAPTAÇÃO DO SOFTWARE	7
3.1 Comunicação por Webservice	7
4 ESTRUTURA DO SERVIÇO DE SUBMISSÃO DE DECLARAÇÕES À AT (SOAP).....	13
4.1 Pedido SOAP.....	13
4.2 Resposta ao pedido SOAP	19
4.3 Tipos Acessórios	23
5 ASSINATURA CERTIFICADO SSL (CSR)	29
5.1 Gerar um certificado SSL.....	30
5.2 Verificar conteúdo do CSR gerado	31
5.3 Integrar certificado SSL com a chave privada	31
6 ENDEREÇOS ÚTEIS.....	32
6.1 Página de produtores de software	32
6.2 Suporte informático da Declaração	Error! Bookmark not defined.
6.3 Página de apoio ao contribuinte	32
6.4 Página de gestão de utilizadores	32
6.5 Endereços para envio de dados à AT por Webservice	32
7 GLOSSÁRIO	33

1 Introdução

O presente documento descreve os procedimentos e requisitos necessários ao cumprimento de serviços para a comunicação da Declaração Recapitulativa do IVA à Autoridade Tributária e Aduaneira (AT).

Este documento destina-se a apoiar as entidades ou indivíduos, doravante designados por produtores de software, que desenvolvam e/ou comercializem software para os Contabilistas Certificados e Contribuintes (seus clientes utilizadores do software produzido).

Os produtores de software são responsáveis por desenvolver programas que cumpram com os requisitos legais da comunicação da Declaração Recapitulativa do IVA e para este efeito devem guiar-se pelas especificações produzidas pela AT.

O Contabilista Certificado (CC) é responsável pelo envio e dados do pedido (credenciais e declaração), uma vez que utiliza as suas credenciais no Portal das Finanças (Utilizador e Senha). Estas credenciais só podem ser conhecidas pelo CC devendo o software produzido estar preparado para solicitar estas credenciais, sempre que necessário à comunicação dos dados.

Complementarmente às credenciais solicitadas do CC, o software deve também estar preparado para solicitar as credenciais do Contribuinte, podendo ser apenas o NIF, se foram conferidos ao CC plenos poderes declarativos, ou as credenciais no Portal das Finanças (Utilizador e Senha), se não tiverem sido conferidos ao CC plenos poderes.

Existe ainda a possibilidade do Contribuinte proceder à entrega da Declaração Recapitulativa do IVA, sendo que, nesses casos, deve apenas indicar as suas credenciais.

Cada software é identificado perante a AT através de um Certificado SSL emitido pelo produtor de software e assinado digitalmente pela AT através de processo de adesão disponível no site e-fatura [\[6.1\]](#).

A AT só aceita estabelecimento de comunicação de dados se for enviado no processo de comunicação, o Certificado SSL emitido para este efeito. Este certificado apenas garante o estabelecimento da comunicação sendo responsabilidade do produtor de software transmitir corretamente os dados dos seus clientes (CC e Contribuinte).

1.1 Namespaces usados

Por uma questão de síntese, a declaração dos namespaces foi omitida dos exemplos e da referência nos capítulos seguintes.

São listados na seguinte tabela, para referência, todos os prefixos de *namespaces* utilizados.

Prefixo	Namespace	Descrição
at	http://at.pt/wsp/auth	AT Authentication Extension
soapenv	http://schemas.xmlsoap.org/soap/envelope/	SOAP Envelope Specification
wss	http://schemas.xmlsoap.org/ws/2002/12/secext	Web Services Security Policy Language
tns	https://servicos.portaldasfinancas.gov.pt/drivaWebservice/2025	Target namespace atribuído aos elementos do DRIVA-WS

2 Enquadramento

A solução disponibilizada no Portal das Finanças permite o cumprimento de obrigação de submissão da Declaração Recapitulativa do IVA, por diferentes modos:

- Formulário web
- Webservice

O cumprimento desta obrigação legal fica ao encargo do Contabilista Certificado, ou do próprio Sujeito Passivo.

2.1 Comunicação das Declarações por Webservice

Para efetuar a comunicação de declarações por Webservice os programas informáticos têm que estar adaptados de forma a:

1. Respeitar o modelo de dados tal como definido em formato WSDL publicado no site Portal das Finanças, na secção *Apoio ao Contribuinte* » *Outras Entidades* » *Produtores de Software / Integradores de Sistemas* » *Comunicações / Webservices* » *Declaração Recapitulativa*.
2. Utilizar os protocolos de comunicação definidos para a transmissão de dados utilizando este serviço, designadamente o protocolo SOAP.
3. Implementar os mecanismos de segurança na transmissão de dados que visam garantir a confidencialidade dos dados, designadamente:
 - a) Comunicação de dados através de canal HTTPS, com utilização de certificado SSL que identifica o produtor de software e que foi previamente assinado pela AT;
 - b) Encriptação da senha dos utilizadores no Portal das Finanças (CC e/ou Sujeito Passivo) recorrendo a chave pública (RSA) do Sistema de Autenticação;
 - c) Demais mecanismos, definidos em detalhe neste documento para garantir a segurança da transmissão dos dados para a AT.

3 Adaptação do software

Nesta secção a AT apresenta as suas recomendações aos produtores de *software* de forma a alterarem os seus programas informáticos para incluírem o envio da Declaração Recapitulativa do IVA, via *Webservice*.

3.1 Comunicação por Webservice

Cada produtor de software é responsável por implementar o módulo que vai enviar a Declaração Recapitulativa do IVA, que deverá respeitar os seguintes passos:

1. Se ainda não tiver efetuado a adesão ao serviço, deverá realizar o processo da Declaração Recapitulativa do IVA - (ver [secção 6.1](#)):
 - a) É necessário utilizar o certificado SSL e submetê-lo para ser assinado pela AT, através do processo de adesão ao envio da Declaração Recapitulativa do IVA por parte dos produtores de software.
2. O utilizador (CC ou Sujeito Passivo) preenche a declaração no programa informático próprio;
 - a) O programa informático solicita as credenciais dos intervenientes nesta submissão (CC e/ou Sujeito Passivo) tal como definidas no Portal das Finanças.
3. Com base nos dados da declaração criada no passo n.º 1 e nas credenciais solicitadas no passo n.º 2 deve construir o pedido SOAP:
 - a) Seguindo o WSDL;
 - b) Estes pedidos SOAP (*Webservice*) são compostos pelas seguinte secções, descritas no capítulo [4 - Estrutura do serviço de submissão de declarações à AT \(SOAP\)](#), e que se resumem a:
 - SOAP:Header – onde se incluem os campos de autenticação dos utilizadores que vão ser responsáveis pela invocação do *Webservice* (as senhas que vão nesta secção têm que ser cifradas recorrendo à chave pública do sistema de autenticação do portal das finanças);
 - SOAP:Body – contém os dados da declaração Recapitulativa do IVA;
 - SOAP:Fault – contém a exceção de autenticação ocorrida efetuar o pedido.
4. Estabelecer uma ligação segura em HTTPS com o portal das finanças utilizando o seguinte endereço para as várias operações:
<https://servicos.portaldasfinancas.gov.pt:426/driva/ws>

5. Processar corretamente o código de resposta devolvido pelo Webservice, que pode ser de três tipos:
 - a) Mensagens de autenticação inválida;
 - b) Mensagens de processamento inválido da declaração;
 - c) Registo com sucesso da declaração.

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

- Desenvolvimento
- Testes
- Distribuição
- Produção

Fase de Desenvolvimento

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

1. Criar sub-utilizador do próprio produtor de software fazendo-o no Portal das Finanças (ver [secção 6.4](#)):

[Site Portal das Finanças » Serviços » Autenticação de Contribuintes » Gestão de Utilizadores](#)

Ao criar o sub-utilizador no Portal das Finanças (1º passo) deve atribuir o perfil WDR, disponível para a comunicação da Declaração Recapitulativa do IVA.

Para criar este utilizador é necessário indicar um:

- Nome,
- Senha (e respetiva confirmação),
- Endereço de e-mail para utilização em contactos por parte da AT.

No final é obtida a identificação do sub-utilizador (e.g., 555555555/55) e a respetiva senha, que deve ser comunicada à equipa de desenvolvimento.

2. Obter a chave pública do Sistema de Autenticação do Portal das Finanças para cifrar a senha do utilizador e certificado SSL assinado para comunicação com o endereço de testes:

É necessário enviar um email à AT a solicitar o envio dos mesmos. A mensagem a enviar por email deve respeitar o seguinte *template*:

TO:	asi-cd@at.gov.pt								
Subject:	Obtenção do certificado SSL para testes e chave pública do sistema de Autenticação - NIF <NIF>								
<p>Exmos. Senhores,</p> <p>O Produtor de Software <NOME> (NIF <NIF>) vem por este meio solicitar o envio dos seguintes elementos para desenvolvimento e testes de envio da Declaração Recapitulativa do IVA:</p> <ul style="list-style-type: none">• Chave pública do Sistema de Autenticação do PF;• Certificado SSL para comunicação com o endereço de testes de Webservices. <p>Estes elementos serão utilizados por este produtor de software para incluir nos seguintes programas:</p> <table border="1"><thead><tr><th>Designação Software</th><th>Certificado AT / DGCI</th></tr></thead><tbody><tr><td><SOFTWARE 1></td><td><CERTIFICADO 1></td></tr><tr><td>...</td><td>...</td></tr><tr><td><SOFTWARE N></td><td><CERTIFICADO N></td></tr></tbody></table> <p>Aguardamos a vossa resposta.</p>		Designação Software	Certificado AT / DGCI	<SOFTWARE 1>	<CERTIFICADO 1>	<SOFTWARE N>	<CERTIFICADO N>
Designação Software	Certificado AT / DGCI								
<SOFTWARE 1>	<CERTIFICADO 1>								
...	...								
<SOFTWARE N>	<CERTIFICADO N>								

No *template* anterior, 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)

3. Obter o WSDL que define a estrutura do pedido SOAP a construir para enviar a Declaração Recapitulativa do IVA.

Para a correta construção do pedido SOAP (invocação do Webservice) deve utilizar a informação complementar disponível no capítulo [4 - Estrutura do serviço de submissão de declarações à AT \(SOAP\)](#), onde se detalha a informação que deve constar dos campos do pedido SOAP bem como a sua forma de construção.

Fase de 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 Contribuintes, seus clientes (ver [secção 6.1](#), opção Testar webservice).

Para este efeito, a aplicação desenvolvida para a submissão da Declaração Recapitulativa do IVA deverá seguir o seguinte procedimento:

1. Utilizar credenciais de sub-utilizador e senha criada para efeito de testes de comunicação da Declaração Recapitulativa do IVA, com o perfil WDR (e.g., 555555555/55 + SENHA);
2. Construir o SOAP:Body de acordo com o definido no capítulo [4.1 - Pedido SOAP](#);
3. Cifrar a senha e compor o SOAP:Header de acordo com o definido na secção **Error! Reference source not found.** do capítulo [4.1 - Pedido SOAP](#);
4. Estabelecer uma ligação HTTPS com o seguinte endereço disponibilizado apenas para testes;

Endereço: <https://servicos.portaldasfinancas.gov.pt:726/driva/ws>

- a) Este endereço apenas aceita ligações com o certificado SSL disponibilizado para testes.
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 capítulo [4.2 - Resposta ao pedido SOAP](#). As respostas são dos seguintes tipos:
 - a) Código de sucesso;
 - b) Erros de autenticação referentes aos campos do SOAP:Header;
 - c) Erros nos dados da declaração referentes aos campos preenchidos no SOAP:Body.

Para efeitos de despiste, é disponibilizada uma página de testes de conectividade e exemplos de pedido e resposta SOAP para comparação com o programa do produtor de software.

Na página de testes também se encontra disponibilizado um exemplo de código fonte da aplicação java para apoiar no desenvolvimento do cliente *webservice*

Tendo em consideração que se trata do ambiente de testes, existe a possibilidade de os dados existentes neste ambiente poderem ser apagados periodicamente.

Fase de Distribuição

Depois de confirmarem a correta adaptação do programa informático e antes de distribuir os programas aos clientes é necessário proceder da seguinte forma:

1. Efetuar a adesão ao envio de dados através do formulário disponível em:
[Site 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 no capítulo [5 - Assinatura certificado SSL \(CSR\)](#);
 - c) A AT responde a este pedido por mensagem de e-mail contendo o certificado SSL assinado digitalmente pela 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:426/driva/ws>
3. Substituir o certificado SSL utilizado em testes (ponto 4 da **Error! Reference source not found.**) pelo certificado SSL de produção emitido no ponto 1 alínea c) desta fase.

Depois de concluído este procedimento o(s) vosso(s) programas informáticos estão prontos para serem distribuídos aos vossos clientes.

Fase de produção

Depois de instalado o programa informático nos computadores dos vossos clientes (Contribuintes) estão em condições para iniciar o envio de declarações da Declaração Recapitulativa do IVA via *Webservice*.

Por regra, o envio procede da seguinte forma:

1. O utilizador (CC ou Sujeito Passivo) preenche a declaração no programa informático;
2. São obtidas as credenciais dos intervenientes na submissão da declaração (CC e/ou 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. Programa processa a resposta do serviço e informa o utilizador do sucesso ou solicita ação do utilizador para o caso de erro no envio.

4 Estrutura do serviço de submissão de declarações à AT (SOAP)

Nesta secção descreve-se informação complementar ao definido no WSDL do serviço de submissão da Declaração Recapitulativa do IVA.

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 dos utilizadores que vão ser responsáveis pela invocação do Webservice. Estes utilizadores podem ser o NIF do CC, sub-utilizador do CC com perfil WDR, o NIF do Contribuinte declarante, ou sub-utilizador do Contribuinte declarante com perfil WDR.

Para criar o sub-utilizador deve ser utilizada a opção:

[Portal das Finanças » Aceda aos Serviços Tributários » Serviços » Autenticação de Contribuintes » Gestão de Utilizadores \[6.3\]](#)

A segunda secção contém os dados da Declaração Recapitulativa do IVA, os quais se detalham no tópico SOAP:Body.

O serviço de submissão de Declarações de Obrigações Acessórias prevê as seguintes operações:

- a) **submeterDeclaracao**, que permite a validação e registo de uma Declaração Recapitulativa do IVA à AT;

Mais à frente neste capítulo serão explicados os campos envolvidos na invocação de cada uma das operações deste serviço.

4.1 Pedido SOAP

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 seguintes 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 do *WS-Security*, e de acordo com as necessidades de segurança específicas do sistema de autenticação do Portal das Finanças.

Parâmetro	Descrição	Obrig. ¹	Tipo Dados ²
H.1 - Utilizador (Username)	<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;"><NIF do emitente>/<UserId></p> <p>Exemplos possíveis:</p> <ol style="list-style-type: none"> 1. 555555555/0000 (utilizador principal) 2. 555555555/1 (sub-utilizador n.º 1) 3. 555555555/0002 (sub-utilizador n.º 2) 4. 555555555/1234 (sub-utilizador n.º 1234) 	S	string
H.2 - Nonce	<p>Chave simétrica gerada por autenticação para cifrar o conteúdo do campo H.3 - Password e do seu atributo Digest.</p> <p>Cada autenticação deverá conter esta chave gerada aleatoriamente e a qual não pode ser repetida entre <i>headers</i> de autenticação (wss:Security) e entre pedidos.</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 e-mail asi-cd@at.gov.pt conforme o descrito na secção Fase de Desenvolvimento do capítulo 3.1.</p> <p>O campo é construído de acordo com o seguinte procedimento</p> $\text{Nonce} := \text{Base64}(C_{RSA, K_{pubSA}}(K_s))$ <p>K_s := array de bytes com a chave simétrica de 128 bits, produzida de acordo com a norma AES.</p> <p>C_{RSA, K_{pubSA}} := Função de cifra da chave simétrica com o algoritmo RSA utilizando a chave pública do sistema de autenticação (K_{pubSA}).</p> <p>Base64 := Codificação em Base 64 do resultado.</p>	S	string (base64)

¹ Obrigatório: S – Sim; N – Não.

² A validar na especificação WSDL (*Web Service Definition Language*) do serviço

Parâmetro	Descrição	Obrig. ¹	Tipo Dados ²
H.3 - Password	<p>O campo Password deverá conter a senha do utilizador / sub-utilizador, a mesma que é utilizada para entrar no Portal das Finanças.</p> <p>Esta senha tem de ser cifrada através da chave simétrica do pedido (ver campo Nonce) e codificado em Base64.</p> $\text{Password} := \text{Base64}(C_{K_s}^{AES, ECB, PKCS5Padding}(\text{SenhaPF}))$ <p>SenhaPF := Senha do utilizador definido no campo H.1 - Username;</p> $C_{K_s}^{AES, ECB, PKCS5Padding} := \text{Função de cifra utilizando o algoritmo AES, Modelo ECB, PKCS5Padding e a chave simétrica do pedido (K}_S).$ <p>Base64 := Codificação em Base 64 do resultado.</p> <p>Adicionalmente este campo deverá conter o atributo Digest. Este atributo deverá conter um digest da password, seguindo a seguinte fórmula:</p> $\text{Digest} := \text{Base64}(C_{K_s}^{AES, ECB, PKCS5Padding}($ $\text{SHA-1}(K_s + \text{Created} + \text{SenhaPF})))$ <p>K_s+Created+SenhaPF := São os bytes dos três campos concatenados;</p> <p>SHA-1 := Função de cálculo de digest usando o algoritmo SHA-1;</p> $C_{K_s}^{AES, ECB, PKCS5Padding} := \text{Função de cifra utilizando o algoritmo AES, Modelo ECB, PKCS5Padding e a chave simétrica do pedido (K}_S).$ <p>Base64 := Codificação em Base 64 do resultado.</p>	S	string (base64)

Parâmetro	Descrição	Obrig. ¹	Tipo Dados ²
H.4 - Data de sistema (Created)	<p>O campo Created deverá conter a data e hora de sistema da aplicação que está a invocar o webservice.</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 de acordo com a hora legal.</p> <p>Sugere-se a sincronização com o Observatório Astronómico de Lisboa:</p> <p style="text-align: center;">http://www.oal.ul.pt/index.php?link=acerto</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:</p> <p style="text-align: center;">http://www.w3.org/QA/Tips/iso-date</p> <p style="text-align: center;">http://www.w3.org/TR/NOTE-datetime</p> <p>e.g.: 2013-01-01T19:20:30.45Z</p> <p>Este campo não deve ser cifrado.</p> <p><i>Created := Timestamp</i></p> <p>Timestamp := data hora do sistema (UTC).</p>		string (base64)

Autenticação com vários contribuintes

O sistema de autenticação do Portal das Finanças estendeu o protocolo de autenticação atual para permitir a autenticação de mais de um contribuinte. Esta nova versão, versão “2”, é compatível com o uso da versão anterior. Isto é, existindo a necessidade de autenticação de apenas um utilizador, é aceite o uso de qualquer uma das versões de autenticação.

Uma vez que a submissão de declarações de Obrigações Acessórias exige que todos os intervenientes nesta submissão sejam autenticados perante a AT, na invocação deste serviço deverá ser utilizado o atributo */wss:Security/@S:Actor* por forma a identificar em que qualidade o utilizador a ser autenticado está a atuar.

/wss:Security/@S:Actor	Valor semântico
http://at.pt/actor/SPA	Contribuinte
http://at.pt/actor/TOC	Contabilista Certificado

O valor utilizado por omissão é o “<http://at.pt/actor/SPA>”.

Para a utilização desta versão, necessária para a invocação do serviço de submissão de declarações de Obrigações Acessórias, deverá ser utilizado o atributo */wss:Security/@Version* com o valor “2”, tal como os exemplos que se seguem o demonstram.

Exemplos SOAP:Header

Como resultado da aplicação das regras de construção anteriores será produzido um *header* de pedido SOAP tal como os seguintes exemplos:

Autenticação do CC com plenos poderes declarativos para o Contribuinte:

Neste exemplo, como o CC tem plenos poderes declarativos para o Contribuinte não é necessário indicar a senha deste. De notar que os *Actors* de todos os elementos de autenticação são definidos explicitamente. O número de versão é incluído no atributo *Version*, com o valor “2”.

```
<S:Header>
  <wss:Security xmlns:wss="http://schemas.xmlsoap.org/ws/2002/12/secext"
    S:Actor="http://at.pt/actor/SPA" at:Version="2">
    <wss:UsernameToken>
      <wss:Username>555555555</wss:Username>
    </wss:UsernameToken>
  </wss:Security>
  <wss:Security xmlns:wss="http://schemas.xmlsoap.org/ws/2002/12/secext"
    S:Actor="http://at.pt/actor/TOC" at:Version="2">
    <wss:UsernameToken>
      <wss:Username>111111111</wss:Username>
      <wss:Password Digest="TTTTTT==>TTTTTTTTTTTTTTT=</wss:Password>
      <wss:Nonce>
        TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
        TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
        TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
      </wss:Nonce>
      <wss:Created>2015-03-09T20:45:05.424Z</wss:Created>
    </wss:UsernameToken>
  </wss:Security>
</S:Header>
```

Autenticação do CC sem plenos poderes declarativos para o Contribuinte:

Neste exemplo, é necessário indicar as credenciais de acesso do Contribuinte, uma vez que o CC não tem plenos poderes. De notar que os *Actors* de todos os elementos de autenticação são definidos explicitamente. O número de versão é incluído no atributo *Version*, com o valor “2”.

```
<S:Header>
  <wss:Security xmlns:wss="http://schemas.xmlsoap.org/ws/2002/12/secext"
    S:Actor="http://at.pt/actor/SPA" at:Version="2">
    <wss:UsernameToken>
      <wss:Username>555555555</wss:Username>
      <wss:Password Digest="AAAAAA==">AAAAAAAAAAAAAAA=</wss:Password>
      <wss:Nonce>
        AAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAA
      </wss:Nonce>
      <wss:Created>2015-03-09T20:45:05.424Z</wss:Created>
    </wss:UsernameToken>
  </wss:Security>
  <wss:Security xmlns:wss="http://schemas.xmlsoap.org/ws/2002/12/secext"
    S:Actor="http://at.pt/actor/TOC" at:Version="2">
    <wss:UsernameToken>
      <wss:Username>111111111</wss:Username>
      <wss:Password Digest="TTTTTT==>TTTTTTTTTTTTTTT=</wss:Password>
      <wss:Nonce>
        TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
```

```
        TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT  
        TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT  
</wss:Nonce>  
<wss:Created>2015-03-09T20:45:05.424Z</wss:Created>  
</wss:UsernameToken>  
</wss:Security>  
</S:Header>
```

Autenticação do Contribuinte:

Neste exemplo, o *Actor* é definido explicitamente. O número de versão é incluído no atributo *Version*, com o valor “2”.

```
<S:Header>
  <wss:Security xmlns:wss="http://schemas.xmlsoap.org/ws/2002/12/secext"
    S:Actor="http://at.pt/actor/SPA" at:Version="2">
    <wss:UsernameToken>
      <wss:Username>555555555</wss:Username>
      <wss:Password Digest="AAAAAA==">AAAAAAAAAAAAAAAAA=</wss:Password>
      <wss:Nonce>
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      </wss:Nonce>
      <wss:Created>2015-03-09T20:45:05.424Z</wss:Created>
    </wss:UsernameToken>
  </wss:Security>
</S:Header>
```

Autenticação do Contribuinte sem definir o Actor explicitamente:

Neste caso, o *Actor* a ter em conta é o “<http://at.pt/actor/SPA>”, sendo este o *Actor* por omissão. O número de versão é incluído no atributo *Version*, com o valor “2”.

```
<S:Header>
  <wss:Security xmlns:wss="http://schemas.xmlsoap.org/ws/2002/12/secext"
    at:Version="2">
    <wss:UsernameToken>
      <wss:Username>555555555</wss:Username>
      <wss:Password Digest="AAAAAA==">AAAAAAAAAAAAAAAAA=</wss:Password>
      <wss:Nonce>
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      </wss:Nonce>
      <wss:Created>2015-03-09T20:45:05.424Z</wss:Created>
    </wss:UsernameToken>
  </wss:Security>
</S:Header>
```

SOAP:Body

O corpo do pedido é distinto conforme a operação que foi solicitada. As secções seguintes apresentam os diferentes SOAP:Body.

Operação *submeterDeclaracao* – dados do elemento *submeterDeclaracaoRequest*

De seguida são apresentados os campos para a operação de submissão de uma Declaração Recapitulativa do IVA, e que compõem o elemento *submeterDeclaracaoRequest*.

Parâmetro	Descrição	Obrig. ³	Tipo Dados ⁴
1.1 - Declaração (declaracao)	Elemento que representa a declaração.	S	DeclaracaoTy pe
1.2 - Versão da declaração (version)	Preencher com a versão da declaração a que se destina. Este campo está diretamente ligado com as versões do webservice que impliquem alterações à operação de submissão. Versão em vigor: 1.0	S	string
1.3 - Indicador se aceita alertas (aceitaAlertas)	Indica se a submissão da declaração deve continuar apesar de ter alertas. Este campo só deve ser preenchido numa segunda submissão após a primeira ter sido retornada com a apresentação de alertas.	N	boolean

4.2 Resposta ao pedido SOAP

SOAP:Body

O corpo da resposta ao pedido é distinto conforme a operação que foi solicitada. As secções seguintes apresentam os diferentes SOAP:Body.

Operação *submeterDeclaracao* – dados do elemento *submeterDeclaracaoResponse*

Nesta secção são apresentados os campos que compõem o elemento *submeterDeclaracaoResponse*. Este campo define a resposta ao pedido à operação de submissão de uma declaração de Obrigação Acessória (*submeterDeclaracao*).

Parâmetro	Descrição	Obrig. ⁵	Tipo Dados ⁶

³ Obrigatório: S – Sim; N – Não.

⁴ A validar na especificação WSDL (Web Service Definition Language) do serviço

⁵ Obrigatório: S – Sim; N – Não.

⁶ A validar na especificação WSDL (Web Service Definition Language) do serviço

Parâmetro	Descrição	Obrig. ⁵	Tipo Dados ⁶
1.1 - Código Resposta (codigo)	<p>Código do resultado da invocação desta interface. Se a resposta for zero, a operação foi bem-sucedida. Se for um número diferente de zero, significa que a operação não foi bem-sucedida.</p> <p>Código de sucesso:</p> <ul style="list-style-type: none"> 0 - Declaração submetida com sucesso; <p>Códigos de resposta (autenticação):</p> <ul style="list-style-type: none"> 1 - Utilizador não preenchido; 2 - Tamanho do utilizador incorreto; 3 - NIF inválido; 4 - Utilizador com formato inválido; 5 - Sub-utilizador com formato inválido; 6 - Senha não preenchida; 7 - Codificação Base64 inválida; 8 - Cifra da chave pública inválida; 9 - Formato do campo Created inválido; 10 - Validade da credencial expirada; 11 - Chave simétrica inválida; 12 - Chave simétrica repetida; 13 - Estrutura da senha inválida; 16 - Chave de sessão inválida. Não foi possível decifrar o campo Created; 17 - Chave de sessão inválida. Não foi possível decifrar o campo Password; 19 - Data de criação do pedido não preenchida; 20 - Chave do pedido não preenchida; 33 - Pedido SOAP inválido; 50 - Header inexistente ou vazio; 51 - O NIF não está preenchido no Header; 52 - Não foi possível verificar se o utilizador tem permissões para aceder a esta operação; 99 - Erro na validação da senha (Senha errada, acesso suspenso, etc.). 	S	int

Parâmetro	Descrição	Obrig. ⁵	Tipo Dados ⁶
	<p>Código de resposta (serviço):</p> <ul style="list-style-type: none"> -1 - Nem todos os utilizadores estão identificados. A mensagem de erro identificará qual o Actor em falta; -4 - Existem dois Security Headers sem o atributo Actor definido; -5 - O Actor definido está repetido. Será apresentado no campo 1.2 a mensagem de erro com o Actor repetido; -6 - O Actor indicado não é conhecido. Será apresentado no campo 1.2 qual é o Actor erróneo; -7 - Versão do Header do pedido deve ser igual a 2; -9 - Parâmetro da versão da declaração é diferente da atual; -10 - A declaração não tem campos preenchidos; -99 - Erro interno; -100 - A declaração apresenta um ou mais erros; -102 - O Header do pedido inexistente ou vazio; -103 - O utilizador autenticado no Security Header não tem permissões para aceder a uma determinada operação; -105 - O NIF autenticado é diferente do NIF da declaração. -106 - O NIF do CC autenticado não pode efetuar a operação para o SP indicado. 		
1.2 - Mensagem Resposta (mensagem)	Mensagem do resultado da invocação desta interface.	N	string
1.3 - Dados de Submissão		N	SubmeterDeclaracaoRespondeType
1.3.1 - Identificação da Declaração (idDeclaracao)	Identificação única da declaração submetida.	N	long

Parâmetro	Descrição	Obrig. ⁵	Tipo Dados ⁶
1.3.2 – Erros	Erros que ocorreram na submissão.	N	ErrosType
1.3.3 – Alertas	Alertas que ocorreram na submissão.	N	WarningsType

SOAP:Fault – dados do elemento *AutenticationException*

Nesta secção são definidos os campos de exceção à autenticação do pedido de registo de uma declaração de Obrigação Acessória.

Parâmetro	Descrição	Obrig. ⁷	Tipo Dados ⁸
1.1 – Lista de erros de autenticação (<i>AuthenticationFailed</i>) – campo repetitivo	S		
1.1.1 – Código de erro (Code)	<p>Código do erro ocorrido aquando da submissão da declaração.</p> <p>Códigos de resposta:</p> <ul style="list-style-type: none"> -1 – Ocorreu um erro no processamento e não foi possível concluir a operação. Por favor tente mais tarde; 0 – A operação decorreu com sucesso e o contribuinte foi autenticado corretamente; 1 – Utilizador não preenchido; 2 – Tamanho do utilizador (14) incorreto; 3 – NIF inválido; 4 – Utilizador com formato inválido; 5 – Sub-Utilizador com formato inválido; 6 – Senha não preenchida; 7 – Codificação Base64 inválida; 8 – Cifra inválida; 9 – Timestamp não preenchido; 10 – Formato do timestamp inválido; 11 – Validade da credencial expirada; 12 – Chave simétrica não preenchida; 13 – Chave simétrica repetida; 14 – Digest da senha não preenchido; 15 – O Digest não corresponde ao esperado; 16 – Dois ou mais Actors definidos por omissão. Existem dois Security Headers sem o atributo Actor definido; 17 – O Actor definido está repetido. A mensagem de erro deverá identificar qual o Actor repetido. As situações em que este erro poderá ocorrer incluem também a situação em que um Actor definido colide 	S	int

⁷ Obrigatório: S – Sim; N – Não.

⁸ A validar na especificação WSDL (*Web Service Definition Language*) do serviço

Parâmetro	Descrição	Obrig. ⁷	Tipo Dados ⁸
	com o valor por omissão de um Actor não especificado; 99 – Erro na validação da senha (Senha errada, acesso suspenso, etc.).		
1.1.2 – Mensagem de erro (Message)	Mensagem do erro ocorrido aquando da autenticação.	S	string
1.1.3 – Número de tentativas de autenticação disponíveis (NumberOfTriesRemaining)	Número de tentativas de autenticação ainda disponíveis. Este campo representa o número de vezes que o contribuinte pode tentar efetuar a autenticação. É decrementado sempre que a autenticação é falhada, levando à suspensão do acesso caso chegue a 0. Se o erro for relacionado com a estrutura e este campo não tiver sido afetado, o seu valor será -1.	S	int
1.1.4 – Ator (Actor)	Identificação do Actor cuja Autenticação falhou. Os valores constantes neste campo são os mesmos dos declarados no atributo /wss:Security@S:Actor.	N	string

4.3 Tipos Acessórios

DeclaracaoType

Parâmetro	Descrição	Obrig. ⁹	Tipo Dados ¹⁰
1.1 – Quadro01	Contém os campos referentes ao quadro 1 da declaração	S	RostoQuadro0 1SectionType
1.1.1 – Campo 1 (f1)	Representa o campo 1 do quadro 1.	N	long
1.2 – Quadro02	Contém os campos referentes ao quadro 2 da declaração	S	RostoQuadro0 2SectionType
1.2.1 – Campo 1 (f1)	Representa o campo 1 do quadro 2.	N	string

⁹ Obrigatório: S – Sim; N – Não.

¹⁰ A validar na especificação WSDL (*Web Service Definition Language*) do serviço

Parâmetro	Descrição	Obrig. ⁹	Tipo Dados ¹⁰
1.2.2 – Campo 3 (f3)	Representa o campo 3 do quadro 2.	N	string
1.2.3 – Campo 4 (f4)	Representa o campo 4 do quadro 2.	N	boolean
1.2.4 – Campo 5 (f5)	Representa o campo 5 do quadro 2.	N	string
1.2.5 – Campo 6 (f6)	Representa o campo 6 do quadro 2.	N	boolean
1.2.6 – Campo 7 (f7)	Representa o campo 7 do quadro 2.	N	boolean
1.2.7 – Campo 8 (f8)	Representa o campo 8 do quadro 2.	N	boolean
1.2.8 – Campo 9 (f9)	Representa o campo 9 do quadro 2.	N	boolean
1.2.9 – Campo 10 (f10)	Representa o campo 10 do quadro 2.	N	boolean
1.2.10 – Campo 11 (f11)	Representa o campo 11 do quadro 2.	N	boolean
1.2.11 – Campo 12 (f12)	Representa o campo 12 do quadro 2.	N	boolean
1.2.12 – Campo 13 (f13)	Representa o campo 13 do quadro 2.	N	boolean

Parâmetro	Descrição	Obrig. ⁹	Tipo Dados ¹⁰
1.3 – Quadro03	Contém os campos referentes ao quadro 3 da declaração	S	RostoQuadro0 3SectionType
1.3.1 – Campo 1 (f1)	Representa o campo 1 do quadro 3.	N	string
1.3.2 – Campo 2 (f2)	Representa o campo 2 do quadro 3.	N	string
1.3.3 – Campo 3 (f3)	Representa o campo 3 do quadro 3.	N	string
1.3.4 – Campo 4 (f4)	Representa o campo 4 do quadro 3.	N	string
1.3.5 – Campo 5 (f5)	Representa o campo 5 do quadro 3.	N	string
1.4 – Quadro0405	Contém os campos referentes aos quadros 4 e 5 da declaração		RostoQuadro0 405SectionType
1.4.1 – Campo 10 (f10)	Representa o campo 10 do quadro 4 e 5.	N	long
1.4.2 – Campo 11 (f11)	Representa o campo 11 do quadro 4 e 5.	N	long
1.4.3 – Campo 17 (f17)	Representa o campo 17 do quadro 4 e 5.	N	long
1.4.4 – Campo 18 (f18)	Representa o campo 18 do quadro 4 e 5.	N	long

Parâmetro	Descrição	Obrig. ⁹	Tipo Dados ¹⁰
1.4.5 – Campo 19 (f19)	Representa o campo 19 do quadro 4 e 5.	N	long
1.4.6 - Tabela (rostoQuadro0405TableItem Type)	Representa a tabela dos quadros 4 e 5.	N	RostoQuadro0405TableItem Type
1.4.6.1 – Campo 2 (f2)	Representa o campo 2 da tabela dos quadros 4 e 5.	N	string
1.4.6.2 – Campo 3 (f3)	Representa o campo 3 da tabela dos quadros 4 e 5.	N	string
1.4.6.3 – Campo 4 (f4)	Representa o campo 4 da tabela dos quadros 4 e 5.	N	long
1.4.6.4 – Campo 5 (f5)	Representa o campo 5 da tabela dos quadros 4 e 5.	N	string
1.5 – Quadro06	Contém os campos referentes ao quadro 6 da declaração		RostoQuadro06SectionType
1.5.1 - Tabela (rostoQuadro06TableItem Type)	Representa a tabela do quadro 6.	N	RostoQuadro06TableItem Type
1.5.1.1 – Campo 2 (f2)	Representa o campo 2 da tabela do quadro 6.	N	string
1.5.1.2 – Campo 3 (f3)	Representa o campo 3 da tabela do quadro 6.	N	string
1.5.1.3 – Campo 4 (f4)	Representa o campo 4 da tabela do quadro 6.	N	string

Parâmetro	Descrição	Obrig. ⁹	Tipo Dados ¹⁰
1.5.1.4 – Campo 5 (f5)	Representa o campo 5 da tabela do quadro 6.	N	string
1.6 – Quadro07	Contém os campos referentes ao quadro 7 da declaração	S	RostoQuadro07SectionType
1.6.1 – Campo 1	Representa o campo 1 da tabela do quadro 7.	N	long

ErrosType

Parâmetro	Descrição	Obrig. ¹¹	Tipo Dados ¹²
1.1 - Erro	Lista de erros.	N	ErroType
1.1.1 - Campo	Caminho no ficheiro XML até ao elemento do erro.	S	string
1.1.2 - Mensagem	Mensagem associada ao erro.	S	string
1.1.3 – Ligações (ligacoes)	Lista de ligações associadas ao erro.	N	LinksType
1.1.3.1 – Ligação (ligacao)	Ligação para o campo da declaração onde se encontra o erro.	N	string

¹¹ Obrigatório: S – Sim; N – Não.

¹² A validar na especificação WSDL (*Web Service Definition Language*) do serviço

WarningsType

Parâmetro	Descrição	Obrig. ¹³	Tipo Dados ¹⁴
1.1 - Alerta	Lista de alertas.	N	WarningType
1.1.1 - Campo	Caminho no ficheiro XML até ao elemento do alerta.	S	string
1.1.2 - Mensagem	Mensagem associada ao alerta.	S	string

¹³ Obrigatório: S – Sim; N – Não.

¹⁴ A validar na especificação WSDL (*Web Service Definition Language*) do serviço

5 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 SSL 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 assinatura de certificado SSL (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 digitalmente esse certificado. Posto isto, o certificado SSL assinado é devolvido para que possa ser utilizado no processo de autenticação na invocação do serviço web de apoio à submissão da Declaração Recapitulativa do IVA.

Os procedimentos para geração do CSR são simples mas variam de acordo com a tecnologia 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 seguinte, 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 ISO de 2 letras referente 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)
CN = Common Name	Neste campo deve ser indicado o número de identificação fiscal da entidade aderente.	9 (chars)
O = Business Name / Organisation	Designação legal da empresa.	180 (chars)
OU = Department Name /Organisational Unit	Departamento para contacto.	180 (chars)

Campo CSR	Descrição	Tamanho Máximo
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 gerado pelo produtor de software tem de ser gerado 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 SSL e remete em resposta ao pedido o certificado SSL assinado para integração na chave privada do produtor de software.

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

5.1 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 site 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=5555555555/emailAddress=informatica@empresa.pt" -newkey
rsa:2048 -nodes -out 5555555555.csr -keyout 5555555555.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 **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.

5.2 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 **BOLD** pelos nomes dos ficheiros corretos.

5.3 Integrar certificado SSL 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 **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 produtor de software deve definir na execução do comando.

6 Endereços Úteis

6.1 Página de produtores de software

Adesão ao serviço:

<https://faturas.portaldasfinancas.gov.pt/consultarPedidosAdesao.action>

Testar webservice:

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

6.2 Página de apoio ao contribuinte

http://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/

6.3 Página de gestão de utilizadores

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

6.4 Endereços para envio de dados à AT por Webservice

Ambiente de testes

<https://servicos.portaldasfinancas.gov.pt:726/driva/ws>

Ambiente de produção

<https://servicos.portaldasfinancas.gov.pt:426/driva/ws>

7 Glossário

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

Termo	Definição
Webservice	http://www.w3.org/TR/ws-arch/
WS-Security	https://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.pdf
WSDL	http://www.w3.org/TR/wsdl
WDR	Perfil para acesso via Webservice a operações da Declaração Recapitulativa