AT autoridade tributária e aduaneira

MANUAL DE INTEGRAÇÃO DE SOFTWARE

Comunicação de Declarações Periódicas de IVA à AT

HISTÓRICO DE ALTERAÇÕES

VERSÃO	DATA	ALTERAÇÕES
1.0	2015-04-29	Criação do documento.
1.1	2016-03-28	Correção das instruções de autenticação de contribuintes no SOAP:Header. Atualizado o endereço do ambiente de testes.
1.2	2019-11-21	Atualização dos valores possíveis para o campo “versaoDeclaracao” nos pedidos das operações de validação e submissão. Atualização dos endereços úteis.

ÍNDICE

1 Introdução

O presente documento descreve os procedimentos e requisitos necessários à comunicação de declarações periódicas de 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 das declarações periódicas de 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 sua própria declaração periódica de 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
S	http://schemas.xmlsoap.org/soap/envelope/	SOAP Envelope Specification
wss	http://schemas.xmlsoap.org/ws/2002/12/secext	Web Services Security Policy Language

2 Enquadramento

A solução apresentada permite a submissão deste tipo de declarações por diferentes modos:

- Formulário web
- Aplicação desktop instalável
- Webservice

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

2.1 Comunicação das Declarações por Webservice

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

1. Respeitar o modelo de dados tal como definido em formato WSDL.
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 Contribuinte) 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 de declarações periódicas de IVA via Webservice.

3.1 Comunicação por Webservice

Cada produtor de software é responsável por implementar o módulo que vai enviar as declarações periódicas de IVA, que deverá respeitar os seguintes passos:

1. Se ainda não tiver efetuado a adesão ao serviço, deverá realizar o processo de adesão à comunicação de declarações periódicas de IVA:
    a) É necessário utilizar o certificado SSL e submetê-lo para ser assinado pela AT, através do processo de adesão ao envio de declarações periódicas de IVA por parte dos produtores de software.
2. O utilizador (CC ou Contribuinte) preenche a declaração no programa informático próprio;
    a) O programa informático solicita as credenciais dos intervenientes nesta submissão (CC e/ou Contribuinte) 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 periódica de 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 de submissão da declaração:

https://servicos.portaldasfinancas.gov.pt:406/dpivaws/DeclaracaoPeriodicaIVAWebService

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 periódica de IVA;
    c) Registo com sucesso da declaração periódica de IVA.

Para adaptar os programas informáticos é recomendada 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:

    Site Portal das Finanças » Outros Serviços » Gestão de utilizadores

    Ao criar o sub-utilizador no Portal das Finanças (1º passo) deve atribuir a autorização IVA, disponível para a comunicação de declarações periódicas de 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>

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 declarações periódicas de IVA via Webservice:

- Chave pública do Sistema de Autenticação do PF;
- 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:

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

Aguardamos a vossa resposta.

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 as declarações periódicas de 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.

Para este efeito, a aplicação desenvolvida para a submissão de declarações periódicas de IVA deverá seguir o seguinte procedimento:

1. Solicitar as credenciais de sub-utilizador e senha criada para os testes de comunicação de declarações periódicas de IVA (e.g., 555555555/55 + SENHA);
2. Com base na declaração periódica de IVA preenchida, 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 SOAP:Header do capítulo 4.1 - Pedido SOAP;
4. Estabelecer uma ligação HTTPS com o seguinte endereço disponibilizado apenas para testes;

   https://servicos.portaldasfinancas.gov.pt:706/dpivaws/DeclaracaoPeriodicaIVAWebService

   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 periódica de IVA 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.

Tendo em consideração que se trata do ambiente de testes, existe a possibilidade dos 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 vossos programas aos vossos 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

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

   a) 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);

   b) 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:406/dpivaws/DeclaracaoPeriodicaIVAWebService

3. Substituir o certificado SSL utilizado em testes (ponto 4 da Fase de Testes) 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 periódicas de IVA via Webservice.

Por regra, o envio procede da seguinte forma:

1. O utilizador (CC ou Contribuintes) preenche a declaração no programa informático;
2. São obtidas as credenciais dos intervenientes na submissão da declaração (CC e/ou Contribuinte) 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 de declarações periódicas de 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, o NIF do Contribuinte declarante, ou sub-utilizador do Contribuinte declarante com as respetivas permissões.

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

Site Portal das Finanças » página *Serviços tributários* » secção *Outros serviços* » opção *Gestão de utilizadores* [6.4]

A segunda secção contém os dados da declaração periódica de IVA, os quais se detalham no tópico SOAP:Body.

O serviço de submissão de Declarações Periódicas de IVA prevê três operações:

a) **submeterDeclaracao**, que permite a comunicação e registo de uma declaração periódica de IVA à AT;

b) **validarDeclaracao**, que permite a validação de uma declaração periódica de IVA perante as regras definidas pela a AT (não é feito qualquer registo da declaração).

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)	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. 555555555/0000 (utilizador principal) 2. 555555555/1 (subutilizador n.º 1) 3. 555555555/0002 (subutilizador n.º 2) 4. 555555555/1234 (subutilizador n.º 1234)	S	string
H.2 - Nonce	Chave simétrica gerada por autenticação para cifrar o conteúdo dos campos H.3 - Password e H.4 - Created. Cada autenticação deverá conter esta chave gerada aleatoriamente e a qual não pode ser repetida entre headers de autenticação (wss:Security) e entre pedidos. 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 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.	S	string (base64)

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

	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.		
H.3 - 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 chave simétrica do pedido (K_S). **Base64** := Codificação em Base 64 do resultado. Adicionalmente este campo deverá conter o atributo Digest. Este atributo deverá conter um digest da password, seguindo a seguinte fórmula: $$Digest := Base64(C_{K_s}^{AES,ECB,PKCS5Padding}(SHA-1(K_s + Created + SenhaPF)))$$ **K_s+Created+SenhaPF** := São os bytes dos três campos concatenados; **SHA**-1 := Função de cáluculo de digest usando o algoritmo SHA-1; $C_{K_s}^{AES,ECB,PKCS5Padding}$:= 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.	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		string (base64)

	crucial que o sistema da aplicação cliente tenha o seu relógio de acordo com a hora legal. 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 e.g.: 2013-01-01T19:20:30.45Z Este campo não deve ser cifrado. $Created := Timestamp$ **Timestamp** := data hora do sistema (UTC).		

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 periódicas de IVA exige que 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 utilizador por omissão é o *"http://at.pt/actor/SPA"*.

Para a utilização desta versão, necessária para a invocação do serviço de submissão de declarações periódica de IVA, 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>111111111</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>333333333</wss:Username>
         <wss:Password Digest=”TTTTTTT==”>TTTTTTTTTTTTTTTT=</wss:Password>
         <wss:Nonce>
            TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
            TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
         </wss:Nonce>
         <wss:Created>20152015-03-09T20:45:05.424Z</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>111111111</wss:Username>
         <wss:Password Digest=”AAAAAA==”>AAAAAAAAAAAAAAAA=</wss:Password>
         <wss:Nonce>
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
         </wss:Nonce>
         <wss:Created>20152015-03-09T20:45:05.424Z</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>333333333</wss:Username>
         <wss:Password Digest=”TTTTTTT==”>TTTTTTTTTTTTTTTT=</wss:Password>
         <wss:Nonce>
            TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
            TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
```

```
         </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>111111111</wss:Username>
         <wss:Password Digest=”AAAAAA==”>AAAAAAAAAAAAAAAA=</wss:Password>
         <wss:Nonce>
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
         </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>111111111</wss:Username>
         <wss:Password Digest=”AAAAAA==”>AAAAAAAAAAAAAAAA=</wss:Password>
         <wss:Nonce>
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
         </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 conforma a operação que foi solicitada. As secções seguintes apresentam os diferentes SOAP:Body.

Operação *submeterDeclaracao* - elemento *submeterDeclaracaoIVARequest*

De seguida são apresentados os campos para a operação de submissão de uma declaração periódica de IVA, e que compõem o elemento *submeterDeclaracaoIVARequest*.

Parâmetro	Descrição	Obrig.[3]	Tipo Dados[4]
1.1 – Versão da Declaração (*versaoDeclaracao*)	Versão da Declaração • Preencher com a versão da declaração a que se destina. Para a submissão de declarações no formato em vigor (formato XML) a versão deverá ser “2016”. Para a submissão de declarações no formato anterior, a versão deverá ser "2013".	S	string
1.2 – Declaração (*declaracao*)	Declaração • Declaração a ser submetida no formato publicado.	S	base64Binary
1.3 – Aceita Alertas (aceitaAlertas)	Aceita Alertas • Indica se a submissão da declaração deve continuar apesar de ter alertas.	N	boolean

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

Operação *validarDeclaracao* – elemento *validarDeclaracaoIVARequest*

Nesta secção são definidos os campos para a operação de validação de uma declaração periódica de IVA, e que compõem o elemento *validarDeclaracaoIVARequest*.

Parâmetro	Descrição	Obrig.[5]	Tipo Dados[6]
1.1 – Versão da Declaração (*versaoDeclaracao*)	Versão da Declaração • Preencher com a versão da declaração a que se destina. Para a submissão de declarações no formato em vigor (formato XML) a versão deverá ser “2016”. Para a submissão de declarações no formato anterior, a versão deverá ser "2013".	S	string
1.2 – Declaração (*declaracao*)	Declaração • Declaração a ser submetida no formato publicado.	S	base64Binary

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

4.2 Resposta ao pedido SOAP

SOAP:Body

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

Operação *submeterDeclaracao* – dados do elemento *submeterDeclaracaoIVAResponse*

Nesta secção são apresentados os campos que compõem o elemento *submeterDeclaracaoIVAResponse*. Este campo define a resposta ao pedido à operação de submissão de uma declaração periódica de IVA.

Parâmetro	Descrição	Obrig.[7]	Tipo Dados[8]
1.1 - Código de resposta (*codigo*)	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. **Código de resposta (serviço):** **-12 - "**A declaração enviada está duplicada e não foi processada.**"** **-11 - "**A declaração apresenta um ou mais erros e/ou alertas.**"** **-10 - "**Erro no preenchimento dos dados da declaração.**"** **-7 - "**Não foi possível verificar se o CC está autorizado a submeter declarações em nome do Sujeito Passivo.**"** **-6 - "**O CC não está autorizado a submeter declarações em nome do Sujeito Passivo e deve indicar a senha do mesmo.**"** **-5 - "**Parâmetro da declaração não está preenchido ou está vazio.**"** **-4 - "**Parâmetro da versão da declaração é diferente da atual.**"** **-3 - "**O utilizador autenticado no Security Header não corresponde ao Sujeito Passivo constante dos dados declarados.**"** **-2 - "**Existem utilizadores autenticados que não pertencem aos dados do serviço.**"** **-1 - "**Nem todos os utilizadores estão identificados.**"** **0 - "**Declaração submetida com sucesso.**"/"**A Declaração não apresenta Erros e/ou Alertas.**"** **50 - "**Header inexistente ou vazio.**"** **51 - "**Actor não é único no Header.**"** **52 - "**O NIF não está preenchido no Header.**"** **53 - "**Não foi possível verificar se o utilizador tem permissões para aceder a esta operação.**"** **54 - "**Não tem permissões para aceder a esta operação.**"** **99 - "**Erro interno.**"**	S	int

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

1.2 – Mensagem de resposta (mensagem)	Mensagem do resultado da invocação desta interface.	S	string
1.3 – Dados de submissão (dadosSubmissao)		N	
1.3.1 – Data de submissão (*data*)	Data de efetivação da submissão da declaração.	S	dateTime
1.3.2 – Ano da declaração (*ano*)	Ano a que se destina a declaração submetida.	S	short
1.3.3 - Período da declaração (periodo)	Período a que se destina a declaração submetida.	S	string
1.3.4 – Identificador da declaração (*idDeclaracao*)	Identificação única da declaração submetida.	S	long
1.3.5 – Contribuinte (contribuinte) – campo repetitivo		S	
1.3.5.1 – Actor do contribuinte (actor)	O Actor que representa cada um dos contribuintes envolvidos na declaração submetida (ver secção Autenticação com vários contribuintes do capítulo 4.1 que descreve os valores esperados).	S	string
1.3.5.2 – NIF do contribuinte (nif)	Número de identificação fiscal que representa cada um dos contribuintes envolvidos na declaração submetida.	S	long
1.4 – Alertas que ocorreram na submissão (alertas)		N	
1.4.1 – Tem mais alertas (temMaisAlertas)	Campo que indica se existe mais alertas que aqueles apresentados.	S	boolean
1.4.2 – Alerta (alerta) – campo repetitivo		S	
1.4.2.1 – Anexo (anexo)	Identificação do anexo em que ocorre cada um dos alertas.	N	string
1.4.2.2 – Quadro (quadro)	Identificação do quadro em que ocorre cada um dos alertas.	N	string

1.4.2.3 – Código (codigo)	Código de cada um dos alertas identificados.	N	string
1.4.2.4 – Mensagem (mensagem)	Mensagem de cada um dos alertas identificados.	S	string
1.5 – Erros que ocorreram na submissão (erros)		N	
1.5.1 – Tem mais erros (temMaisErros)	Campo que indica se existe mais erros que aqueles apresentados.	S	boolean
1.5.2 – Erro (erro) – campo repetitivo		S	
1.5.2.1 – Anexo (anexo)	Identificação do anexo em que ocorre cada um dos erros.	N	string
1.5.2.2 – Quadro (quadro)	Identificação do quadro em que ocorre cada um dos erros.	N	string
1.5.2.3 – Código (codigo)	Código de cada um dos erros identificados.	N	string
1.5.2.4 – Mensagem (mensagem)	Mensagem de cada um dos erros identificados.	S	string

Operação *validarDeclaracao* – dados do elemento *validarDeclaracaoIVAResponse*

De seguida são apresentados os campos que compõem o elemento *validarDeclaracaoIVAResponse*. Este campo define a resposta ao pedido à operação de validação de uma declaração periódica de IVA.

Parâmetro	Descrição	Obrig.[9]	Tipo Dados[10]
1.1 - Código de resposta (*codigo*)	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. **Código de resposta (serviço):** **-11 - "**A declaração apresenta um ou mais erros e/ou alertas.**"** **-10 - "**Erro no preenchimento dos dados da declaração.**"** **-5 - "**Parâmetro da declaração não está preenchido ou está vazio.**"** **-4 - "**Parâmetro da versão da declaração é diferente da atual.**"** **-3 - "**O utilizador autenticado no Security Header não corresponde ao Sujeito Passivo constante dos dados declarados.**"** **-2 - "**Existem utilizadores autenticados que não pertencem aos dados do serviço.**"** **-1 - "**Nem todos os utilizadores estão identificados.**"** **0 - "**A Declaração não apresenta Erros e/ou Alertas.**"** **50 - "**Header inexistente ou vazio.**"** **51 - "**Actor não é único no Header.**"** **52 - "**O NIF não está preenchido no Header.**"** **53 - "**Não foi possível verificar se o utilizador tem permissões para aceder a esta operação.**"** **54 - "**Não tem permissões para aceder a esta operação.**"** **99 - "**Erro interno.**"**	S	int
1.2 – Mensagem de resposta (mensagem)	Mensagem do resultado da invocação desta interface.	S	string
1.3 – Alertas que ocorreram na submissão (alertas)		N	
1.3.1 – Tem mais alertas (temMaisAlertas)	Campo que indica se existe mais alertas que aqueles apresentados.	S	boolean
1.3.2 – Alerta (alerta) – campo repetitivo		S	

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

1.3.2.1 – Anexo (anexo)	Identificação do anexo em que ocorre cada um dos alertas.	N	string
1.3.2.2 – Quadro (quadro)	Identificação do quadro em que ocorre cada um dos alertas.	N	string
1.3.2.3 – Código (codigo)	Código de cada um dos alertas identificados.	N	string
1.3.2.4 – Mensagem (mensagem)	Mensagem de cada um dos alertas identificados.	S	string
1.4 – Erros que ocorreram na submissão (erros)		N	
1.4.1 – Tem mais erros (temMaisErros)	Campo que indica se existe mais erros que aqueles apresentados.	S	boolean
1.4.2 – Erro (erro) – campo repetitivo		S	
1.4.2.1 – Anexo (anexo)	Identificação do anexo em que ocorre cada um dos erros.	N	string
1.4.2.2 – Quadro (quadro)	Identificação do quadro em que ocorre cada um dos erros.	N	string
1.4.2.3 – Código (codigo)	Código de cada um dos erros identificados.	N	string
1.4.2.4 – Mensagem (mensagem)	Mensagem de cada um dos erros identificados.	S	string

SOAP:Fault – dados do elemento *AutenticationException*

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

Parâmetro	Descrição	Obrig.[11]	Tipo Dados[12]
1.1 – Lista de erros de autenticação (*AuthenticationFailed*) – campo repetitivo		S	
1.1.1 – Código de erro (*Code*)	Código do erro ocorrido aquando da submissão da declaração. **Códigos de resposta:** **-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 com o valor por omissão de um Actor não especificado; **99** – Erro na validação da senha (Senha errada, acesso suspenso, etc.).	S	int
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

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

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

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 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 de declarações periódicas de IVA.

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 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 /Organizational Unit	Departamento para contacto.	180 (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 gerado pelo produtor de software tem de ser gerado com 2048 bits.	2048 (bits)

A utilização de carateres especiais (e.g., portugueses, línguas latinas, etc.) não é aceite em nenhum dos campos acima indicados, uma vez que a utilização desses carateres 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=**555555555**/emailAddress=**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 **BOLD**.

Como resultado o 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 Suporte informático da Declaração Periódica de IVA

http://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/Suporte_Informatico_Formato_ficheiros/Pages/default.aspx#IVA

6.3 Página de apoio ao contribuinte

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

6.4 Página de gestão de utilizadores

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

6.5 Endereços para envio de dados à AT por Webservice

Ambiente de testes

https://servicos.portaldasfinancas.gov.pt:706/dpivaws/DeclaracaoPeriodicaIVAWebService

Ambiente de produção

https://servicos.portaldasfinancas.gov.pt:406/dpivaws/DeclaracaoPeriodicaIVAWebService

7 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_mode_of_operation
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: www.acesso.gov.pt. Sistema responsável por validar as credenciais de um utilizador registado no Portal das Finanças.
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