AT autoridade tributária e aduaneira



MANUAL DE INTEGRAÇÃO DE SOFTWARE

Entrega da Declaração Mensal de Imposto do Selo

HISTÓRICO DE ALTERAÇÕES

DATA	ALTERAÇÕES
03-12-2019	Criação do documento.
23-12-2019	Adiciona elemento AlreadyPaidTaxAmount.
17-01-2020	Introdução de novos códigos de erro.
04-02-2020	Endpoint de invocação de testes.
15-12-2020	Endpoint de invocação de produção.
29-01-2021	Altera restrição minInclusive do elemento TaxPeriod para 2021-01, e altera tipo do elemento TaxableEntityTaxOfficeCode para string.
17-02-2021	Introdução de novos códigos de erro.
17-08-2021	Atualização dos códigos de resposta dados durante o processo de autenticação.
14-12-2021	Acrescenta novos elementos FairImpediment e RepresentedEntity (ambos de preenchimento opcional), que serão aceites para submissões realizadas após 2022-01-31. Acrescenta novos códigos de erro.
30-01-2023	Altera a parametrização do elemento OperationTypeCode (Código de Tipo de Operação). Adiciona um novo valor ao elemento TerritorialityCode (Territorialidade). Adiciona novo elemento do XML: “Data da Cessação do Facto” (FairImpedimentCloseDate). Acrescenta os códigos de erro -1056 e -1057. Altera o descritivo do elemento Facto que Determinou o Impedimento (FairImpedimentFact) relativamente ao valor ‘03’.
06-07-2023	Altera as regras de aplicabilidade das validações correspondentes aos códigos de erro -1056 e -1057.
22-08-2023	Altera a validação com o código de erro -1030. Acrescenta o código de erro -1058

DATA	ALTERAÇÕES
17-07-2024	Adiciona novo elemento do XML: “Facto que Determinou o Impedimento de Prolongado” (LongTermFairImpedimentFact). Altera o descritivo do elemento “Facto que Determinou o Impedimento de Curta Duração” (FairImpedimentFact) Altera as regras da validação correspondente aos códigos de erro -1030, -1049, -1052 e -1053
31-07-2025	Atualização da hiperligação da página de Apoio ao Contribuinte.
08-06-2026	Adiciona validação relativamente as Combinações do Código de Tipo de Operação e Código de Circunscrição Territorial, com código de erro -1065; Adiciona validação, impedindo a submissão da declaração quando está a decorrer um procedimento inspetivo, com código de erro -1066.

ÍNDICE

1 INTRODUÇÃO 5

2 ENQUADRAMENTO 6
2.1 Comunicação por Webservice 6

3 ADAPTAÇÃO DO SOFTWARE 7
3.1 Comunicação por Webservice 7

4 ESTRUTURA DO ENVIO DE DADOS À AT (SOAP) 12
4.1 SOAP:Header 12
4.2 SOAP:Body – Submissão da declaração DMIS 14

5 ASSINATURA CERTIFICADO SSL (CSR) 32
5.1 Gerar um certificado SSL 33
5.2 Verificar conteúdo do CSR gerado 34
5.3 Integrar certificado SSL com a chave privada 34

6 ENDEREÇOS ÚTEIS 35
6.1 Página de produtores de software 35
6.2 Apoio ao Contribuinte no Portal das Finanças 35
6.3 Endereços para envio de dados à AT por Webservice 35

7 GLOSSÁRIO 36

1 Introdução

O presente documento descreve os procedimentos e requisitos necessários à entrega da declaração mensal de Imposto do Selo (DMIS) à Autoridade Tributária e Aduaneira, adiante designada por AT.

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

Os produtores de software são responsáveis por desenvolver programas que cumpram com os requisitos legais da entrega das declarações e, para este efeito, devem guiar-se pelas especificações produzidas pela AT para este efeito de comunicação.

O Sujeito Passivo é responsável pelo envio e conteúdo da mensagem, uma vez que utiliza as suas credenciais no Portal das Finanças (Utilizador e Senha). Estas credenciais só podem ser conhecidas pelo Sujeito Passivo devendo o software produzido estar preparado para solicitar estas credencias, sempre que necessário à comunicação dos dados.

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.

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 Sujeitos Passivos, seus clientes.

2 Enquadramento

De acordo com o disposto no Código do Imposto do Selo (CIS) e de acordo com o modelo estabelecido pela Portaria n.º 339/2019 de 1 de outubro, os sujeitos passivos referidos no nº. 1 do artigo 2.º. do CIS têm de entregar à AT a declaração a que se refere o n.º 2 do artigo 52.º -A do CIS, exclusivamente por transmissão eletrónica de dados:

- Por transmissão eletrónica integrada em programa informático, utilizando o Webservice disponibilizado pela AT;
- No Portal das Finanças, com o upload do ficheiro ou através do preenchimento manual da declaração diretamente no formulário disponibilizado para o efeito.

2.1 Comunicação 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 previsto na Portaria nº 339/2019 de 1 de outubro e definidos em formato WSDL/XSD publicados no site Portal das Finanças na secção Apoio ao Contribuinte em IS – Imposto do Selo.
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 tal como disposto no Artigo 6.º do Decreto-Lei n.º 198/2012 de 24 de agosto, 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 do utilizador do sujeito passivo no portal das finanças recorrendo a chave pública (RS) do sistema de autenticação utilizado pelo Portal das Finanças na identificação dos seus utilizadores;
    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 mudarem os seus programas informáticos para incluírem a entrega da DMIS.

3.1 Comunicação por Webservice

O envio da declaração da DMIS por Webservice pressupõe os seguintes passos:

1. Se ainda não tiver efetuado a adesão ao serviço, deverá realizar o processo de adesão à comunicação por webservice:
    a) É necessário utilizar o certificado SSL e submetê-lo para ser assinado pela AT, através do processo de adesão análogo ao envio de dados de documentos de transporte e e-fatura por parte dos produtores de software;
2. O sujeito passivo estrutura a informação a ser comunicada no programa informático próprio;
3. O programa informático solicita as credenciais do sujeito passivo tal como definidas no portal das finanças e na gestão de subutilizadores:
    a) Cada sujeito passivo deve criar um subutilizador para o envio de dados relativos aos documentos de transporte na opção disponível no Portal das Finanças na secção “Serviços tributários/Outros serviços/Gestão de utilizadores”;
    b) A este subutilizador deve ser atribuída a operação “DIS – Entrega da Declaração Mensal de Imposto do Selo”;
4. Com base nos dados a preencher na declaração, criados no passo n.º 1 e nas credenciais solicitadas no passo n.º 2 deve construir o pedido SOAP tal como definido:
    a) No WSDL e XSD disponíveis na secção Apoio ao Contribuinte em IS – Imposto do Selo.
    b) Estes pedidos SOAP (Webservice) são compostos pelas seguintes secções descritas na secção 4 deste documento e que se resumem a:
        - SOAP:Header - onde se incluem os campos de autenticação do utilizador que vai ser responsável pela invocação do Webservice (a senha que vai nesta secção tem que ser cifrada recorrendo à chave pública do sistema de autenticação do portal das finanças);
        - SOAP:Body - contém os dados da declaração DMIS;
5. Estabelecer uma ligação segura em HTTPS com o portal das finanças e utilizando o seguinte endereço de envio da declaração:

https://servicos.portaldasfinancas.gov.pt:721/DmisServiceImplService

6. 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 dos dados da declaração DMIS;
    c) Registo com sucesso dos dados da declaração DMIS.

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

- Desenvolvimento
- Testes
- Distribuição
- Produção

3.1.1 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 subutilizador do próprio produtor de software fazendo-o no Portal das Finanças:

    Portal das Finanças > Autenticação de Contribuintes > Gestão de utilizadores

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

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 devem 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 comunicação por webservice com a AT:
>
> - Chave pública do Sistema de Autenticação do PF;
> - Certificado SSL para comunicação com o endereço de testes de Webservices.
>
> Aguardamos a vossa resposta.

3. Construir o pedido SOAP de acordo com o WSDL/XSD do webservice.

Para a correta construção do pedido SOAP (invocação do Webservice) deve utilizar a informação complementar disponível neste documento na secção 4, onde se detalha a informação que deve constar dos campos do pedido SOAP bem como a sua forma de construção.

3.1.2 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 sujeitos passivos, seus clientes.

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

1. Solicitar as credenciais de subutilizador e senha criada para os testes de comunicação dos documentos de transporte ou de guias de aquisição a produtores agrícolas (e.g., 555555555/55 + SENHA);
2. Cifrar a senha e compor o SOAP:Header de acordo com o definido na secção 0;
3. Com base na declaração DMIS, construir o SOAP:Body de acordo com o definido na secção 4.2;
4. Estabelecer uma ligação HTTPS com o seguinte endereço disponibilizado apenas para testes.

   https://servicos.portaldasfinancas.gov.pt:721/DmisServiceImplService

5. Submeter o pedido SOAP construído no ponto 3;
6. Processar a resposta que o serviço lhe devolve de acordo com os seguintes tipos:

a) Código de sucesso;

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

c) Erros nos dados da declaração DMIS 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. Mais informação na secção 4.1.1 deste documento.

3.1.3 Fase de Distribuição

Depois de confirmarem a correta adaptação do programa informático e antes de distribuir os vossos programas aos vossos clientes (sujeitos passivos) 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 na secção 5;

   c) A AT responde a este pedido por mensagem de email 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:421/DmisServiceImplService.

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 concluída este procedimento o(s) vosso(s) programas informáticos estão prontos para serem distribuídos aos vossos clientes (sujeitos passivos).

3.1.4 Fase de produção

Depois de instalado o programa informático nos computadores dos vossos clientes (sujeitos passivos) está tudo pronto para começar a entrega das declarações DMIS por Webservice.

Cada sujeito passivo deve criar um subutilizador para a comunicação de dados.

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

Por regra, o envio procede da seguinte forma:

1. Sujeito passivo estrutura a informação a ser comunicada no programa informático;
2. São obtidas as credenciais do sujeito passivo configuradas no programa informático;
3. É construído o pedido SOAP e invocado o Webservice em produção com os dados do ponto 1 e ponto 2;
4. 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 envio de dados à AT (SOAP)

Nesta secção descreve-se informação complementar ao definido no WSDL/XSD do serviço de entrega da declaração DMIS.

4.1 SOAP:Header

O desenho do Header tem como requisito garantir a confidencialidade dos dados de autenticação e a impossibilidade de reutilização dos mesmos em ataques Man-in-the-middle (MITM). Por este motivo, só serão aceites invocações que respeitem os 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 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. 555555555/1 (subutilizador n.º 1) 2. 555555555/0002 (subutilizador n.º 2) 3. 555555555/1234 (subutilizador n.º 1234)	S	String
H.2 - Nonce	Chave simétrica gerada a cada pedido e para cifrar o conteúdo dos campos H.3 - Password e H.4 - Created. Cada invocação do Webservice deverá conter esta chave gerada aleatoriamente e a qual não pode ser repetida. Para garantir a confidencialidade, a chave simétrica tem de ser cifrada com a chave pública do Sistema de Autenticação de acordo com o algoritmo RSA e codificada em Base 64.	S	String (base64)

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

	A chave pública do sistema de autenticação do portal das finanças deve ser obtida por solicitação própria e através do endereço de email asi-cd@at.gov.pt. O campo é construído de acordo com o seguinte procedimento $Nonce := Base64(C_{RSA,Kpub_{SA}}(K_s))$ **Ks** := 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 Password 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.	S	string (base64)
H.4 - Data de sistema (Created)	O campo Created deverá conter a data e hora de sistema da aplicação que está a invocar o webservice. Esta data é usada para validação temporal do pedido, pelo que é crucial que o sistema da aplicação cliente tenha o seu relógio certo. Sugere-se a sincronização com o Observatório Astronómico de Lisboa: http://www.oal.ul.pt/index.php?link=acerto A zona temporal deste campo deverá estar definida para UTC e formatado de acordo com a norma ISO 8601 tal como é definido pelo W3C: http://www.w3.org/QA/Tips/iso-date		string (base64)

	http://www.w3.org/TR/NOTE-datetime e.g.: 2013-01-01T19:20:30.45Z Este campo é cifrado com a chave de pedido (K_S) e codificada em Base 64. $Created := Base64(C_{K_s}^{AES,ECB,PKCS5Padding}(Timestamp))$ **Timestamp** := data hora do sistema (UTC); $C_{K_s}^{AES,ECB,PKCS5Padding}$:= Função de cifra utilizando o algoritmo AES, Modelo ECB, PKCS5Padding e a chave simétrica do pedido (K_S). **Base64** := Codificação em Base 64 do resultado.		

4.1.1 Exemplo SOAP:Header

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

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

4.2 SOAP:Body – Submissão da declaração DMIS

Nesta secção são definidos os campos para o registo de uma nova declaração DMIS.

4.2.1 Descrição da Operação

Esta operação possibilita o envio, por um sujeito passivo, de todos os elementos de uma DMIS, de modo a que esta seja validada localmente e registada na AT, sendo devolvido um Identificador unívoco para a declaração submetida, bem como uma correspondente Referência para Pagamento.

4.2.2 Submissão "por Blocos de Linhas"

De modo a assegurar a escalabilidade da operação de submissão, sempre que a quantidade de linhas contidas na declaração seja muito elevada (> 5.000 linhas), a transmissão eletrónica da declaração deverá realizar-se através de invocações sucessivas ao Web Service, enviando-se, em cada invocação, um Bloco de Linhas da declaração (e sendo retornado o Identificador da declaração submetida, e a Referência para Pagamento, apenas após o envio da totalidade das linhas da declaração). Por exemplo, para uma declaração que contenha 12.400 linhas, deverão ser realizadas 3 invocações sucessivas para submissão dessa declaração:

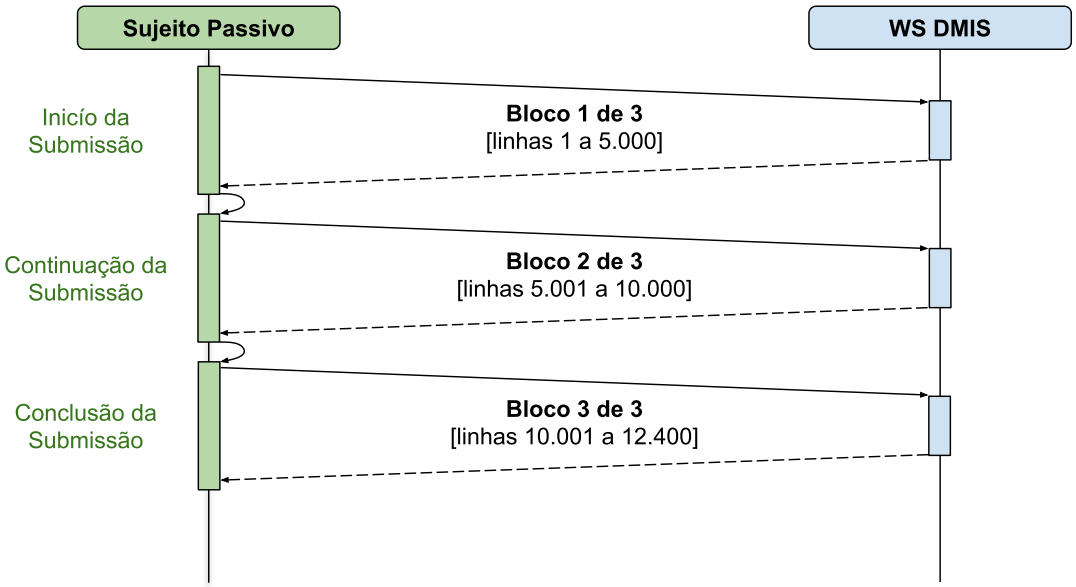


Figura 1 – Exemplo de Submissão de Declaração "por Blocos de Linhas"

4.2.3 Substituição de Blocos de Linhas

Caso surja a necessidade de substituir um determinado Bloco de Linhas *n* (por exemplo, porque o sujeito passivo detetou a existência de erros nos dados previamente transmitidos nesse bloco *n*):

- Se ainda estiver incompleta a transmissão de todos os Blocos de Linhas da declaração relativa a esse período (e, portanto, ainda não tiver sido atribuído um Identificador de declaração submetida), deverá ser reenviado o Bloco de Linhas *n* (com os dados corrigidos), e, nesse caso, o sistema irá validar os novos dados, e em caso de validação com sucesso, irá substituir todos os dados do Bloco de Linhas *n* (registando-se os dados corrigidos) e irá eliminar eventuais Blocos de Linhas *n+1*, *n+2* etc., que deverão ser posteriormente retransmitidos.
- Se já estiver concluída a transmissão da declaração relativa a esse período (e, portanto, já tiver sido atribuído um Identificador de declaração submetida), deverá

proceder-se ao envio integral (ou seja, de todos os Blocos de Linhas) de uma declaração de substituição referente ao mesmo período de imposto.

Por razões de segurança e escalabilidade, caso ainda esteja incompleta a transmissão de todos os Blocos de Linhas da declaração, o sistema apenas permite a substituição, em cada invocação, de até 50 Blocos de Linhas dessa declaração. Por exemplo, caso surja a necessidade de substituir o Bloco de Linhas número 33, quando, anteriormente, já tenha sido submetido o Bloco de Linhas número 92, deverá substituir-se primeiro o Bloco de Linhas número 42 e só depois o Bloco de Linhas número 33.

4.2.4 Substituição de Declarações

A transmissão eletrónica de uma DMIS de substituição, para um determinado período, deverá realizar-se através dos mesmos procedimentos aplicados para transmissão eletrónica da primeira declaração para esse mesmo período, com exceção:

- Do elemento SubstitutionDeclaration, que, nesse caso, deverá ser preenchido com o valor “true” (de modo a indicar que se trata de uma Declaração de Substituição para o correspondente Período Mensal);
- Da “Lista de Linhas da Declaração” (DeclarationLinesList), que, nesse caso, poderá estar vazia (de modo a anular simplesmente a declaração anterior para o correspondente Período Mensal).

4.2.5 Parâmetros

A estrutura de dados XML a incluir na secção SOAP:Body do SOAP:Envelope relativo aos parâmetros de entrada da operação é a seguinte:

Cardinalidade	Elemento XML	Descrição	Tipo	
1	DmisWsSubmissionRequest			
1	TaxableEntityTaxOfficeCode	Código do Serviço de Finanças do Sujeito Passivo	xsd:string	pattern=\d{4}
1	TaxableEntityTaxID	Número de Identificação Fiscal do Sujeito Passivo	xsd:int	pattern=[1-9]\d{8}
1	TaxPeriod	Período Mensal de Imposto	xsd:gYearMonth	pattern=\d{4}-\d{2} minInclusive=2021-01
1	SubstitutionDeclaration	Indica se se trata de uma Declaração de Substituição para o correspondente Período Mensal (deve ser preenchido com "false" no caso de ser a 1.ª Declaração)	xsd:boolean	
0..1	TaxRepresentativeTaxID	Número de Identificação Fiscal do Representante Legal	xsd:int	pattern=[1-9]\d{8}
0..1	CertifiedAccountantTaxID	Número de Identificação Fiscal do Contabilista Certificado	xsd:int	pattern=[1-9]\d{8}
0..1	FairImpediment	Justo Impedimento		
0..1[xsd:choice]	FairImpedimentFact	Facto que determinou o Justo Impedimento de Curta Duração: 01 - Falecimento de cônjuge não separado de pessoas e bens, de pessoa com quem vivam em condições análogas às dos cônjuges, ou de parente ou afim no 1.º grau da linha reta 02 - Falecimento de outro parente ou afim na linha reta ou no 2.º grau da linha colateral 03 - Doença grave e súbita ou internamento hospitalar do contabilista, que o impossibilite em absoluto de cumprir as suas obrigações ou em situações de parto ou de assistência 04 - Situações de parentalidade **[xsd:choice]** Obrigatório se **LongTermFairImpedimentFact** não estiver definido	xsd:string	01 02 03 04
0..1[xsd:choice]	FairImpedimentDate	Data da ocorrência do facto que determinou o Justo Impedimento de Curta Duração.	xsd:date	

		[xsd:choice] Obrigatório se **FairImpedimentFact** estiver definido.		
0..1[xsd:choice]	FairImpedimentCloseDate	Data da cessação do facto que determinou o Justo Impedimento de Curta Duração **[xsd:choice]** Opcional que só pode ser preenchido se **FairImpedimentFact** estiver definido.	xsd:date	
0..1[xsd:choice]	LongTermFairImpedimentFact	Facto que determinou o Justo Impedimento Prolongado: 04 - Situações de parentalidade 05 - Doença prolongada do contabilista, que o impossibilite em absoluto de cumprir as suas obrigações 06 - Nomeação de novo contabilista (falecimento do anterior contabilista) **[xsd:choice]** Obrigatório se **FairImpedimentFact** não estiver definido.	xsd:string	04 05 06
1	DeclarationLinesQuantity	Quantidade (total) de Linhas da Declaração	xsd:int	pattern=\d{1,9}
1	DeclarationLinesBlocksQuantity	Quantidade (total) de Blocos de Linhas da Declaração	xsd:int	pattern=[1-9]\d{0,4}
1	DeclarationLinesBlock	Bloco de Linhas da Declaração		
1	BlockId	Número Identificador do Bloco de Linhas	xsd:int	pattern=[1-9]\d{0,4}
1	DeclarationLinesList	Lista de Linhas da Declaração		
0..5000	DeclarationLine	Linha da Declaração		
1	LineId	Número Identificador de Linha (sequencial)	xsd:int	pattern=[1-9]\d{0,8}
0..1	TaxChargeHolder	Titular do Encargo Fiscal		
0..1 [xsd:choice]	PortugueseTaxID	Número de Identificação Fiscal Português **[xsd:choice]** Obrigatório se **ForeignTaxID** não estiver definido	xsd:int	pattern=[1-9]\d{8}
0..1 [xsd:choice]	ForeignTaxID	Número de Identificação Fiscal Estrangeiro **[xsd:choice]** Obrigatório se **PortugueseTaxID** não estiver definido		
1	CountryCode	Código de País (código numérico ISO 3166-1, diferente de 620 - Portugal)	xsd:string	pattern=\d{3}

1	TaxID	Número de Identificação Fiscal	xsd:string	minLength=1 maxLength=30 pattern=\S(.*\S)?
1	TaxCode	Código correspondente à verba constante na Tabela Geral do Imposto do Selo	xsd:string	minLength=1 maxLength=10 pattern=\S(.*\S)?
1	TerritorialConstituencyCode	Código de Circunscrição Territorial: C - Continente A - Açores M - Madeira	xsd:string	 C A M
1	TerritorialityCode	Código de Territorialidade: 1 - Art.º 4.º, n.º 1 CIS 2 - Art.º 4.º, n.º 2 CIS 3 - Art.º 4.º, n.º 7 CIS 4 - Art.º 4.º, n.º 8 CIS 5 - Art.º 4.º, n.º 9 CIS	xsd:string	 1 2 3 4 5
1	OperationTypeCode	Código de Tipo de Operação sujeita a Imposto (isenta ou não)	xsd:short	pattern=\d{1,3}
1	OperationPerformedByRepresentative	Indica se a Operação foi realizada por um Representante obrigatoriamente nomeado em Portugal, ao abrigo das alíneas i) a l) do n.º 1 do Art.º 2.º CIS	xsd:boolean	
0..1	RepresentedEntity	Entidade Representada		
0..1 **[xsd:choice]**	PortugueseTaxID	Número de Identificação Fiscal Português **[xsd:choice]** Obrigatório se **ForeignTaxID** não estiver definido	xsd:int	pattern=[1-9]\d{8}
0..1 **[xsd:choice]**	ForeignTaxID	Número de Identificação Fiscal Estrangeiro **[xsd:choice]** Obrigatório se **PortugueseTaxID** não estiver definido		
1	CountryCode	Código de País (código numérico ISO 3166-1, diferente de 620 - Portugal)	xsd:string	pattern=\d{3}
1	TaxID	Número de Identificação Fiscal	xsd:string	minLength=1 maxLength=30 pattern=\S(.*\S)?
1	TaxBase	Base Tributável		

0..1 **[xsd:choice]**	BankCheckQuantity	Quantidade de Cheques Bancários atribuídos **[xsd:choice]** Obrigatório se **TaxBaseAmount** não estiver definido	xsd:int	pattern=[1-9]\d{0,5}
0..1 **[xsd:choice]**	TaxBaseAmount	Montante da Base Tributável, incluindo a relativa a operações isentas **[xsd:choice]** Obrigatório se **BankCheckQuantity** não estiver definido	xsd:decimal	fractionDigits=2 totalDigits=15 minInclusive=0.01
0..1	TaxAmount	Montante correspondente ao valor do imposto liquidado	xsd:decimal	fractionDigits=2 totalDigits=15 minInclusive=0.00
0..1	AlreadyPaidTaxAmount	Montante de Imposto já Pago, para o Período Mensal de Imposto (a preencher, opcionalmente, apenas em Declaração de Substituição)	xsd:decimal	fractionDigits=2 totalDigits=15 minInclusive=0.01

4.2.6 Resultados

A estrutura de dados XML da secção SOAP:Body do SOAP:Envelope relativo aos resultados devolvidos pela operação é a seguinte:

Cardinalidade	Elemento XML	Descrição	Tipo	
1	DmisWsSubmissionResponse			
1	ReturnInfo	Informação de Controlo do Resultado da Operação		
1	ReturnCode	Código de Resultado da invocação (código de sucesso ou de erro)	xsd:short	
1	ReturnMessage	Descrição do Código de Resultado da invocação	xsd:string	
0..1	DmisRegistrationData	Dados de Registo da Declaração		
1	SubmittedDeclarationLinesBlocksQuantity	Quantidade de Blocos de Linhas da Declaração que já foram submetidos (com sucesso)	xsd:int	pattern=[1-9]\d{0,4}
0..1	NotSubmittedDeclarationLinesBlocksQuantity	Quantidade de Blocos de Linhas da Declaração que ainda não foram submetidos (com sucesso)	xsd:int	pattern=[1-9]\d{0,4}
0..1	DmisRegistrationID	Identificador da Declaração submetida (apenas disponível após a submissão, com sucesso, de todos os Blocos de Linhas da Declaração)	xsd:long	pattern=[1-9]\d{0,12}
0..1	DmisRegistrationTimeStamp	Data/Hora de Registo da Declaração submetida (apenas disponível após a submissão, com sucesso, de todos os Blocos de Linhas da Declaração)	xsd:dateTime	
0..1	TaxPaymentReference	Referência para Pagamento do Imposto (apenas disponível após a submissão, com sucesso, de todos os Blocos de Linhas da Declaração)	xsd:long	pattern=\d{15}
0..1	TaxPaymentAmount	Montante de Imposto a Pagar (apenas disponível após a submissão, com sucesso, de todos os Blocos de Linhas da Declaração)	xsd:decimal	fractionDigits=2 totalDigits=15 minInclusive=0.01

4.2.7 Códigos de Resultado

Estão previstos os seguintes erros, transmitidos como elementos SOAP:Fault, resultantes de validações sobre os dados XML incluídos na secção SOAP:Header do SOAP:Envelope:

- 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 – Chave de sessão inválida. Não foi possível decifrar o campo Created;
- 17 – Chave de sessão inválida. Não foi possível decifrar o campo Password;
- 18 – Chave de sessão inválida. Não foi possível decifrar o campo Digest;
- 19 – Data de criação do pedido não preenchida;
- 20 – Chave do pedido não preenchida;
- 33 - Pedido SOAP inválido;
- 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 na validação da senha (Senha errada, acesso suspenso, etc.).

Estão previstos os seguintes valores para o elemento “Código de Resultado da invocação” (ReturnCode):

- Códigos de Sucesso:
    - -8001 – Bloco de Linhas registado com sucesso nas bases de dados da AT;
    - -8002 – Bloco de Linhas registado com sucesso nas bases de dados da AT, substituindo Bloco de Linhas anteriormente transmitido;

- -8003 – Declaração registada com sucesso nas bases de dados da AT (último Bloco de Linhas transmitido e registado com sucesso).

- Códigos de Erro:
  - -1035 – Erro de validação da estrutura XML dos parâmetros de entrada;
  - -1036 - Erro técnico inespecífico;
  - -1028 – O valor de “Quantidade (total) de Blocos de Linhas da Declaração” (DeclarationLinesBlocksQuantity) deve corresponder ao resultado da divisão da “Quantidade (total) de Linhas da Declaração” (DeclarationLinesQuantity) por 5.000.
  - -1029 – O valor de “Número Identificador do Bloco de Linhas” (BlockId) não deve ser maior do que o valor da “Quantidade (total) de Blocos de Linhas da Declaração” (DeclarationLinesBlocksQuantity).
  - -1027 – Quando o valor de “Número Identificador do Bloco de Linhas” (BlockId) é igual a 1, e ainda não tenha sido concluída a transmissão de todos os Blocos de Linhas de uma declaração primeira relativa ao mesmo período, o valor de SubstitutionDeclaration deverá ser igual a “false”.
  - -1019 – Quando o valor de “Número Identificador do Bloco de Linhas” (BlockId) é igual a 1, e já tenha sido concluída a transmissão de todos os Blocos de Linhas de uma declaração primeira relativa ao mesmo período, o valor de SubstitutionDeclaration deverá ser igual a “true”.
  - -1030 – Os valores dos elementos TaxableEntityTaxOfficeCode, SubstitutionDeclaration, TaxRepresentativeTaxID, CertifiedAccountantTaxID, FairImpedimentFact, FairImpedimentDate, FairImpedimentCloseDate, LongTermFairImpedimentFact, DeclarationLinesQuantity, DeclarationLinesBlocksQuantity e AlreadyPaidTaxAmount deverão ser iguais aos inicialmente transmitidos (a quando da transmissão do Bloco de Linhas com BlockId igual a 1), considerando a mesma declaração.

- -1031 – Deve ter sido previamente transmitido um Bloco de Linhas identificado igual a “Número Identificador do Bloco de Linhas” (BlockId) -1, e ainda não deverá ter sido concluída a transmissão de todos os Blocos de Linhas da declaração.
- -1023 – Na linha x, o valor de “Número Identificador de Linha” (LineId) da primeira linha, deve ser igual à subtração de 4.999 ao resultado da multiplicação de 5.000 pelo valor de “Número Identificador do Bloco de Linhas” (BlockId).
- -1022 – Na linha x, o valor de “Número Identificador de Linha” (LineId) deve ser sequencial.
- -1024 – Na linha x, o valor de “Número Identificador de Linha” (LineId) da última linha, deve ser igual ao valor de “Quantidade (total) de Linhas da Declaração” (DeclarationLinesQuantity).
- -1009 – Na linha x, o valor do “Número de Identificação Fiscal do Sujeito Passivo” não é aplicável para o “Código de Tipo de Operação” (OperationTypeCode).
- -1010 – Na linha x, o valor do NIF português (TaxChargeHolder/PortugueseTaxID), relativo ao Titular do Encargo Fiscal, não é aplicável para o “Código de Tipo de Operação” (OperationTypeCode).
- -1011 – Na linha x, o valor de “Código de Verba” (TaxCode) não é aplicável para o “Código de Tipo de Operação” (OperationTypeCode).
- -9003 – O valor do elemento “Código do Serviço de Finanças do Sujeito Passivo” (TaxableEntityTaxOfficeCode) deve corresponder ao existente no Cadastro de Contribuintes da AT, para o “Número de Identificação Fiscal do Sujeito Passivo” (TaxableEntityTaxID).
- -9004 – O Utilizador ou Sub-Utilizador autenticado não corresponde ao “Número de Identificação Fiscal do Sujeito Passivo” (TaxableEntityTaxID).
- -9005 – O Utilizador ou Sub-Utilizador autenticado não tem permissões de acesso a esta funcionalidade.

- -1021 – O valor do “Número de Identificação Fiscal do Sujeito Passivo” (TaxableEntityTaxID) deve ser válido, de acordo como o algoritmo de validação do check-digit dos NIFs portugueses.
- -9006 – O valor do “Número de Identificação Fiscal do Sujeito Passivo” (TaxableEntityTaxID) deve existir e estar coerente no Cadastro de Contribuintes da AT.
- -1017 – O valor do “Número de Identificação Fiscal do Representante Legal” (TaxRepresentativeTaxID) deve ser válido, de acordo como o algoritmo de validação do check-digit dos NIFs portugueses.
- -9001 – O valor do “Número de Identificação Fiscal do Representante Legal” (TaxRepresentativeTaxID) deve existir e estar coerente no Cadastro de Contribuintes da AT.
- -1018 – O valor do “Número de Identificação Fiscal do Contabilista Certificado” (CertifiedAccountantTaxID) deve ser válido, de acordo como o algoritmo de validação do check-digit dos NIFs portugueses.
- -9002 – O valor do “Número de Identificação Fiscal do Contabilista Certificado” (CertifiedAccountantTaxID) deve existir e estar coerente no Cadastro de Contribuintes da AT.
- -1002 – Na linha x, o valor do “Número de Identificação Fiscal Português” (TaxChargeHolder/PortugueseTaxID), relativo ao Titular do Encargo Fiscal, deve ser válido, de acordo como o algoritmo de validação do check-digit dos NIFs portugueses.
- -1004 – Na linha x, o valor do “Código de País” (TaxChargeHolder/ForeignTaxID/CountryCode), relativo ao Titular do Encargo Fiscal, é inválido.
- -1025 – Na linha x, o valor do “Código de País” (TaxChargeHolder/ForeignTaxID/CountryCode), relativo ao Titular do Encargo Fiscal, deve ser diferente de “620”.
- -1007 – Na linha x, o valor do “Código de Verba” (TaxCode) é inválido.

- -1008 – Na linha x, o valor do “Código de Verba” (TaxCode) não é aplicável para o “Período Mensal de Imposto” (TaxPeriod).
- -1020 – Na linha x, o valor do “Código de Tipo de Operação” (OperationTypeCode) é inválido.
- -1014 – Na linha x, o “Montante da Base Tributável” (TaxBaseAmount) não deve estar preenchido para o “Código de Verba” (TaxCode).
- -1012 – Na linha x, a “Quantidade de Cheques Bancários” (BankCheckQuantity) não deve estar preenchida para o “Código de Verba” (TaxCode).
- -1013 – Na linha x, o “Montante imposto liquidado” (TaxAmount) deve estar preenchido para o “Código de Tipo de Operação” (OperationTypeCode).
- -1026 – Na linha x, o “Montante imposto liquidado” (TaxAmount) não deve estar preenchido para o “Código de Tipo de Operação”.
- -1032 – Na linha x, a combinação dos valores de TaxChargeHolder/PortugueseTaxID, TaxChargeHolder/ForeignTaxID/CountryCode, TaxChargeHolder/ForeignTaxID/TaxID, TaxCode, TerritorialConstituencyCode, TerritorialityCode, OperationTypeCode, OperationPerformedByRepresentative, RepresentedEntity/PortugueseTaxID, RepresentedEntity/ForeignTaxID/CountryCode e RepresentedEntity/ForeignTaxID/TaxID está repetida noutra linha da declaração.
- -1033 – Para uma declaração primeira, deve ser preenchida, pelo menos, uma linha na “Lista de Linhas da Declaração” (DeclarationLinesList).
- -1034 – Na linha x, o “Titular do Encargo Fiscal” (TaxChargeHolder) deve estar preenchido para o “Código de Verba” (TaxCode).
- -1037 – A data do último dia do “Período Mensal de Imposto” (TaxPeriod) deve ser anterior à data atual.

- -1038 – Na linha x, o valor do “Montante imposto liquidado” (TaxAmount) não deve ser inferior ao montante calculado pelo sistema, considerando o “Código de Verba” (TaxCode).
- -1039 – O “Montante de Imposto já Pago” (AlreadyPaidTaxAmount) não deve estar preenchido para uma declaração primeira.
- -1042 – Quando o valor de “Número Identificador do Bloco de Linhas” (BlockId) seja menor que o valor de “Quantidade (total) de Blocos de Linhas da Declaração“ (DeclarationLinesBlocksQuantity), o valor de “Número Identificador de Linha” (LineId) da última linha da “Lista de Linhas da Declaração” (DeclarationLinesList), deve ser igual ao resultado da multiplicação de 5.000 pelo valor de “Número Identificador do Bloco de Linhas” (BlockId).
- -1043 – O Bloco de Linhas a substituir não deve ter um “Número Identificador do Bloco de Linhas” (BlockId) menor do que o resultado da subtração de 50 ao Número Identificador do Bloco de Linhas previamente transmitido para a mesma declaração.
- -1046 – Na linha x, o valor do “Número de Identificação Fiscal Português” (RepresentedEntity/PortugueseTaxID), relativo à Entidade Representada, deve ser válido, de acordo como o algoritmo de validação do check-digit dos NIFs portugueses.
- -1047 – Na linha x, o valor do “Código de País” (RepresentedEntity/ForeignTaxID/CountryCode), relativo à Entidade Representada, é inválido.
- -1048 – Na linha x, estando preenchido o elemento “Entidade Representada” (RepresentedEntity), o valor do elemento “Operação foi realizada por um Representante” (OperationPerformedByRepresentative) deverá ser igual a “true”.
- -1049 – O elemento "Facto que Determinou o Justo Impedimento de Curta Duração" (FairImpedimentFact) ou "Facto que Determinou o Justo Impedimento Prolongado" (LongTermFairImpedimentFact) apenas deverá estar preenchido quando a declaração seja entregue após o prazo legalmente previsto.

- -1052 – Se algum dos elementos "Facto que Determinou o Justo Impedimento de Curta Duração" (FairImpedimentFact) ou "Facto que Determinou o Justo Impedimento Prolongado" (LongTermFairImpedimentFact) estiver preenchido, deve ser obrigatoriamente preenchido o “Número de Identificação Fiscal do Contabilista Certificado” (CertifiedAccountantTaxID).
- -1053 – O valor do elemento “Data da Ocorrência do Facto “ (FairImpedimentDate) é inválido para o "Facto que Determinou o Justo Impedimento de Curta Duração" (FairImpedimentFact) indicado.
- -1054 – Na linha x, o valor do elemento “Código de País” (RepresentedEntity/ForeignTaxID/CountryCode), relativo à Entidade Representada, deve ser diferente de “620”.
- -1055 - Quando a declaração mais recente, com o mesmo "Número de Identificação Fiscal do Sujeito Passivo" (TaxableEntityTaxID) e mesmo "Período Mensal de Imposto" (TaxPeriod), tenha uma “Quantidade (total) de Linhas da Declaração” (DeclarationLinesQuantity) igual a zero, deve estar preenchida (pelo menos) uma linha da “Lista de Linhas da Declaração” (DeclarationLinesList).
- -1056 - O elemento "Data da Cessação do Facto" (FairImpedimentCloseDate) apenas deverá estar preenchido quando o "Facto que Determinou o Justo Impedimento" (FairImpedimentFact) estiver preenchido com valor igual a '03', sendo, neste caso, de preenchimento obrigatório.
- -1057 - A data do elemento "Data da Cessação do Facto" (FairImpedimentCloseDate) deve estar compreendido entre a “Data da Ocorrência do Facto “ (FairImpedimentDate) e a data atual.
- -1058 - Na linha x, o valor do NIF português (TaxChargeHolder/PortugueseTaxID), relativo ao Titular do Encargo Fiscal, não é aplicável para o “Código de Verba” (TaxCode)"
- -1065 -Na linha x, o valor do “Código de Circunscrição Territorial” (TerritorialConstituencyCode) não é aplicável para o “Código de Tipo de Operação” (OperationTypeCode);

- -1066 -Por se encontrar em curso um procedimento inspetivo, está inibida a possibilidade de proceder à apresentação desta declaração, de acordo com o previsto no artigo 28.º, n.º 3 do RCPITA (Regime Complementar do Procedimento de Inspeção Tributária e Aduaneira).
- Outros códigos de erro, resultantes de validações sobre os dados XML incluídos na secção SOAP:Body do SOAP:Envelope, a definir futuramente.

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 e devolver o certificado SSL assinado digitalmente para que possa ser utilizado no processo de autenticação na invocação do serviço.

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 /Organisational Unit	Departamento para contacto.	180 (chars)
E = An email address	O endereço de correio eletrónico para contacto, geralmente do responsável pela	80 (chars)

	emissão do CSR ou do departamento de informática. Tem que ser um endereço de email válido.	
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 especifica 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 digita 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

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

6.2 Apoio ao Contribuinte no Portal das Finanças

https://info.portaldasfinancas.gov.pt/pt/apoio_ao_contribuinte/Pages/default.aspx

6.3 Endereços para envio de dados à AT por Webservice

Ambiente de testes:

https://servicos.portaldasfinancas.gov.pt:721/DmisServiceImplService

Ambiente de produção:

https://servicos.portaldasfinancas.gov.pt:421/DmisServiceImplService.

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_modes_of_operation#Electronic_codebook_.28ECB.29
OAL	Observatório Astronómico de Lisboa: http://www.oal.ul.pt/ Para acertar a hora do computador seguindo as instruções do Observatório: http://www.oal.ul.pt/index.php?link=acerto
OpenSSL	http://www.openssl.org/
PF	Portal das Finanças: www.portaldasfinancas.gov.pt
PKCS#5	Referência do PKCS #5: http://tools.ietf.org/html/rfc2898 Explicação do PKCS #5: http://en.wikipedia.org/wiki/PKCS
SA	Sistema de autenticação do Portal das Finanças: www.acesso.gov.pt. Sistema responsável por validar as credenciais de um utilizador registado no Portal das Finanças.
SAF-T (PT)	http://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/NEWS_SAF-T_PT.htm
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