

MANUAL DE INTEGRAÇÃO DE SOFTWARE

Entrega do pedido de certificado da isenção da declaração de exportação (IVAEXP)

Av. Eng.º Duarte Pacheco, 28 - 18.º, Lisboa
Email: portal-qt@at.gov.pt

www.portaldasfinancas.gov.pt **Tel: (+351) 21 383 4200 Fax: (+351) 21 383 4646**

HISTÓRICO DE ALTERAÇÕES

DATA	ALTERAÇÕES
12-06-2025	Criação do documento
17-07-2025	Adição dos parâmetros isInterveniente e tipoSubmissao à operação pedidoCertificadoIVAEXP e do parâmetro isInterveniente às operações obterCertificadoIVAEXP e anulaCertificadoIVAEXP e adição de código de erro
25-08-2025	Adição de endereço de qualidade

ÍNDICE

1 INTRODUÇÃO 4

2 ENQUADRAMENTO 5
2.1 Comunicação por Webservice 5

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 14

5 ASSINATURA CERTIFICADO SSL (CSR) 24
5.1 Gerar um certificado SSL 25
5.2 Verificar conteúdo do CSR gerado 25
5.3 Integrar certificado SSL com a chave privada 26

6 ENDEREÇOS ÚTEIS 27
6.1 Página de produtores de software 27
6.2 Apoio ao Contribuinte no Portal das Finanças 27
6.3 Endereços para envio de dados à AT por Webservice 27

1 Introdução

O presente documento descreve os procedimentos e requisitos necessários à entrega do pedido de certificado de isenção da declaração de exportação (IVAEXP) 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 transmitentes, e intervenientes em seu nome, com NIF português (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 Transmitente, ou Interveniente em seu nome, 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 Transmitente ou Interveniente 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

Com a entrada em vigor do n.º 8 do artigo 29.º do Código do IVA, as transmissões de bens isentas de IVA ao abrigo da alínea a) do n.º 1 do artigo 14.º do mesmo Código, expedidos ou transportados para país terceiro ou território terceiro, pelo transmitente ou por um interveniente por sua conta, devem ser comprovadas com a declaração aduaneira de sujeição dos bens ao regime aduaneiro da exportação, com a certificação da saída.

Nos termos do n.º 9 do mesmo artigo, a falta desse documento comprovativo determina a obrigação para o transmitente dos bens de liquidar o imposto correspondente.

A medida de simplificação do procedimento de exportação de remessas de bens de valor não superior a 1000 euros e que não sejam passíveis de direitos de exportação, visa dar resposta a esta necessidade. Esta medida assenta na comunicação dos elementos das faturas de suporte à exportação visando a obtenção de um número de registo e a subsequente emissão automática do formulário de exportação IVA que serve de comprovativo à aplicação da isenção nos termos do n.º 8 do artigo 29.º do Código do IVA, não sendo aplicável aos meios de transporte e, transitoriamente, aos bens sujeitos a impostos especiais de consumo.

O transmitente ou o interveniente por sua conta devem, no Portal das Finanças, submeter o formulário devidamente preenchido com os elementos da(s) fatura(s) que titula(m) a(s) operação(ões) de exportação:

- Por transmissão eletrónica integrada em programa informático, utilizando o Webservice disponibilizado pela AT;
- No Portal das Finanças, através do preenchimento do formulário em funcionalidade disponibilizada para o efeito.

2.1 Comunicação por Webservice

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

1. Respeitar o modelo de dados tal como definido em formato WSDL, publicado no site do Portal das finanças:

   https://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/IVAEXP/Documents/IVAEXPWS.wsdl <a disponibilizar brevemente>

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 do pedido de certificado de isenção da declaração de exportação (IVAEXP).

3.1 Comunicação por Webservice

A entrega do pedido de certificado de isenção da declaração de exportação (IVAEXP) 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 submete-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 às declarações mensais globais 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 "WEX – Entrega de pedidos de certificado de isenção da entrega da declaração de exportação (WebService)"
4. Com base nos dados a preencher no pedido de certificado, criados no passo n.º 2 e nas credenciais solicitada no passo n.º 3 deve construir o pedido SOAP tal como definido:
    a) No WSDL e XSD disponíveis na secção Apoio ao Contribuinte em IVAEXP – Certificado de isenção da entrega da declaração de exportação.
    b) Estes pedidos SOAP (Webservice) são composto pelas seguinte 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 do pedido de certificado de insenção;

5. Estabelecer uma ligação segura em HTTPS com o portal das finanças e utilizando o seguinte endereço de envio do pedido de certificado:

   https://servicos.portaldasfinancas.gov.pt:..... <a definir brevemente>

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 do pedido de certificado;

   c) Registo com sucesso dos dados do pedido de certificado de isenção.

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 IVAEXP. 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 das declarações mensais globais (e.g., 555555555/55 + SENHA);
2. Cifrar a senha e compor o SOAP:Header de acordo com o definido na secção 4.1;
3. Com base no pedido de certificado de isenção da entrega da declaração de exportação, construir o SOAP:Body de acordo com o definido na secção 0;
4. Estabelecer uma ligação HTTPS com o seguinte endereço disponibilizado apenas para testes.

   https://servicos.portaldasfinancas.gov.pt:706/ivaexp/CertificadoIsencaoWebService/
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 DMGIVA 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:..... <a definir brevemente>

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 (transmitentes).

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 dos pedidos de certificado de isenção da entrega da declaração de exportação 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 dos pedidos de certificado de isenção da entrega da declaração de exportação.

Nota importante: na comunicação por webservice todas as strings enviadas devem estar codificadas em UTF-8.

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>/<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. 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.	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 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 http://www.w3.org/TR/NOTE-datetime e.g.: 2025-01-01T19:20:30.45Z Este campo é cifrado com a chave de pedido (K_S) e codificada em Base 64.		string (base64)

	$Created := Base64(C_{K_s}^{AES,ECB,PKCS5Padding}(Timestamp))$ **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.		

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

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

Nesta secção são definidos os campos para o registo do pedido de certificado da isenção de declaração de exportação (IVAEXP).

4.2.1 Pedido SOAP

4.2.1.1 Entrega do pedido de Certificado IVAEXP – Operação *pedidoCertificadoIVAEXP*

Esta operação possibilita o envio, por um sujeito passivo, de todos os elementos de um pedido de certificado, de modo a que este seja validado localmente e registado na AT, sendo devolvido um identificador unívoco (NRM - Número de registo do movimento) para a declaração submetida.

De seguida são apresentados os campos para a operação de entrega de um pedido de certificado, e que compõem o elemento *pedidoCertificadoIVAEXPRequest*.

Parâmetro	Descrição	Obrig.[3]	Tipo Dados[4]
1.1 – Pedido de Certificado (*pedidoCertificado*)	Pedido de Certificado • Pedido de Certificado a ser entregue no formato publicado (xml)	S	base64Binary
1.2 – Indicador de interveniente (*isInterveniente*)	Indicador do tipo de sujeito a pedir o certificado: • True: entrega por interveniente • False: entrega por transmitente	S	boolean
1.3 – Tipo de submissão (*tipoSubmissao*)	Indicador do tipo de submissão, podendo ter os seguintes valores: • E - entrega • R - retificação	S	string
1.4 – Identificador do pedido de certificado (*nrm*)	Identificação única do pedido de Certificado (NRM - Número de registo do movimento).	N	string

4.2.1.2 Obtenção do certificado – Operação *obterCertificadoIVAEXP*

Esta operação possibilita a obtenção do certificado, quando emitido, através do seu identificador NRM - Número de registo do movimento e versão, se esta não for preenchida é retornada a última (vigente).

Caso não tenha sido emitido, é devolvida a respetiva prova de entrega.

De seguida são apresentados os campos que compõem o elemento *obterCertificadoIVAEXPRequest*.

Parâmetro	Descrição	Obrig.[5]	Tipo Dados[6]
1.1 – Identificador do pedido de Certificado (*nrm*)	Identificação única do pedido de Certificado (NRM - Número de registo do movimento)	S	long

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

1.2 – Versão (*nrm*)	Identificação da versão do certificado que se pretende consultar	N	long
1.3 - Indicador de interveniente (*isInterveniente*)	Indicador do tipo de sujeito a pedir o certificado: • True: entrega por interveniente • False: entrega por transmitente	S	String

4.2.1.3 Anulação do Pedido de certificado – Operação *anulaCertificadoIVAEXP*

Esta operação possibilita a anulação do pedido de certificado vigente, através do seu identificador NRM - Número de registo do movimento.

De seguida são apresentados os campos que compõem o elemento *anulaCertificadoIVAEXPRequest*.

Parâmetro	Descrição	Obrig.[7]	Tipo Dados[8]
1.1 – Identificador do pedido de Certificado (*nrm*)	Identificação única do pedido de Certificado (NRM - Número de registo do movimento)	S	long
1.2 - Indicador de interveniente (*isInterveniente*)	Indicador do tipo de sujeito a pedir o certificado: • True: entrega por interveniente • False: entrega por transmitente	S	String

4.2.2 Resposta ao pedido SOAP

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

4.2.2.1 Operação *pedidoCertificadoIVAEXP* – dados do elemento *pedidoCertificadoIVAEXPResponse*

Nesta secção são apresentados os campos que compõem o elemento *pedidoCertificadoIVAEXPResponse*. Este campo define a resposta ao pedido à operação de Entrega do pedido de Certificado IVAEXP.

Parâmetro	Descrição	Obrig.[9]	Tipo Dados[10]

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

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 sucesso:** **0** – Submissão com sucesso; **Códigos de resposta (autenticação):** **1** - Utilizador não preenchido; **2** - Tamanho do utilizador incorreto; **3** - NIF inválido; **4** - Utilizador com formato inválido; **5** - Sub-utilizador com formato inválido; **6** - Senha não preenchida; **7** - Codificação Base64 inválida; **8** - Cifra da chave pública inválida; **9** - Formato do campo Created inválido; **10** - Validade da credencial expirada; **11** - Chave simétrica inválida; **12** - Chave simétrica repetida; **13** - Estrutura da senha inválida; **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; **19** - Data de criação do pedido não preenchida; **20** - Chave do pedido não preenchida; **21** - Pedido SOAP inválido; **22** - Header inexistente ou vazio; **23** - O NIF não está preenchido no Header; **24** - Não foi possível verificar se o utilizador tem permissões para aceder a esta operação; **25** - Erro na validação da senha (Senha errada, acesso suspenso, etc.); **Código de resposta (serviço):** **-1** - Nem todos os utilizadores estão identificados.	S	int

	-2 - Existem utilizadores autenticados que não pertencem aos dados do serviço. **-3** - O utilizador autenticado no Security Header não corresponde ao transmitente constante dos dados do pedido de certificado. **-4** - Existem dois Security Headers sem o atributo Actor definido. **-5** - O Actor definido está repetido. **-6** - O Actor indicado não é conhecido. **-7** - O schema do pedido de certificado entregue é inválido **-8** - Não foi possível verificar se o utilizador tem permissões para aceder a esta operação. **-9** - O formato do ficheiro é inválido, tem que ser zip ou xml. **-10** - O nif indicado é inválido. **-15** - O utilizador indicado não tem permissões para aceder à operação pretendida. **-97** - Tipo de submissão inválido. **-98** - NRM preenchido. **-99** - Erro interno. **-100** – O pedido de certificado entregue tem erros de validação		
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 – Identificador do pedido de Certificado (*nrm*)	Identificação única do pedido de Certificado (NRM - Número de registo do movimento)	S	string
1.3.2 - Versão do certificado (versao)	Número de identificação da versão do certificado após solicitação.	S	long
1.3.3 – Data de submissão (*data*)	Data de efetivação da submissão do pedido de certificado.	S	dateTime
1.4 – Erros que ocorreram na entrega (erros)		N	
1.4.1 – Erro (erro) – campo repetitivo		S	

1.4.1.1 – Quadro (quadro)	Identificação do quadro em que ocorre cada um dos erros.	N	string
1.4.1.2 – Tabela (tabela)	Identificação da tabela em que ocorre cada um dos erros.	N	string
1.4.1.3 – Linha (linha)	Identificação da linha da tabela em que ocorre cada um dos erros.	N	string
1.4.1.4 – Campo (campo)	Identificação do campo em que ocorre cada um dos erros.	N	string
1.4.1.5 – Código (codigo)	Código de cada um dos erros identificados.	S	string
1.4.1.6 – Mensagem (mensagem)	Mensagem de cada um dos erros identificados.	S	string

4.2.2.2 Operação obterCertificadoIVAEXP – dados do elemento obterCertificadoIVAEXPResponse

Parâmetro	Descrição	Obrig.[11]	Tipo Dados[12]
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 sucesso:** **0** - Estado do certificado fornecido com sucesso. **Códigos de resposta (autenticação):** **1** - Utilizador não preenchido; **2** - Tamanho do utilizador incorreto; **3** - NIF inválido; **4** - Utilizador com formato inválido; **5** - Sub-utilizador com formato inválido; **6** - Senha não preenchida; **7** - Codificação Base64 inválida;	S	int

[11] Obrigatório: S – Sim; N – Não.

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

	8 - Cifra da chave pública inválida; **9** - Formato do campo Created inválido; **10** - Validade da credencial expirada; **11** - Chave simétrica inválida; **12** - Chave simétrica repetida; **13** - Estrutura da senha inválida; **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; **19** - Data de criação do pedido não preenchida; **20** - Chave do pedido não preenchida; **21** - Pedido SOAP inválido; **22** - Header inexistente ou vazio; **23** - O NIF não está preenchido no Header; **24** - Não foi possível verificar se o utilizador tem permissões para aceder a esta operação; **25** - Erro na validação da senha (Senha errada, acesso suspenso, etc.). **Código de resposta (serviço):** **-1** - Nem todos os utilizadores estão identificados. **-2** - Existem utilizadores autenticados que não pertencem aos dados do serviço. **-3** - O utilizador autenticado no Security Header não corresponde ao transmitente constante dos dados do pedido de certificado. **-4** - Existem dois Security Headers sem o atributo Actor definido. **-5** - O Actor definido está repetido. **-6** - O Actor indicado não é conhecido. **-7** - O schema da consulta de certificado entregue é inválido **-8** - Não foi possível verificar se o utilizador tem permissões para aceder a esta operação. **-9** - O formato do ficheiro é inválido, tem que ser zip ou xml. **-10** - O nif indicado é inválido.		

	-11 - O NRM é obrigatório. **-12** – Não existe certificado com o NRM indicado. **-13** – O certificado para o par NRM nif do sujeito passivo indicado não existe. **-14** – O certificado encontra-se anulado. **-15** - O utilizador indicado não tem permissões para aceder à operação pretendida. **-99** - Erro interno.		
1.2 – Mensagem de resposta (mensagem)	Mensagem do resultado da invocação desta interface.	S	string
1.3 – Dados do documento (infoDocumento)		N	
1.3.1 – Tipo do documento (tipoDoc)	Indica se é o certificado ou a prova de entrega: • 1 – certificado • 2 – prova de entrega	S	int
1.3.2 – Estado do Pedido (*estadoPedido*)	Estado do pedido do certificado	S	char
1.3.4 – Data de estado (*dataEstado*)	Data de estado do certificado.	S	dateTime
1.3.2 – Documento (documento)	Certificado ou prova de entrega em PDF do pedido entregue.	S	Base64Binary

4.2.2.3 *Operação anulaCertificadoIVAEXP – dados do elemento anulaCertificadoIVAEXP*Response

Parâmetro	**Descrição**	**Obrig.[13]**	**Tipo Dados[14]**
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 sucesso:**	S	int

[13] Obrigatório: S – Sim; N – Não.

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

	0 - Estado do certificado fornecido com sucesso. **Códigos de resposta (autenticação):** **1** - Utilizador não preenchido; **2** - Tamanho do utilizador incorreto; **3** - NIF inválido; **4** - Utilizador com formato inválido; **5** - Sub-utilizador com formato inválido; **6** - Senha não preenchida; **7** - Codificação Base64 inválida; **8** - Cifra da chave pública inválida; **9** - Formato do campo Created inválido; **10** - Validade da credencial expirada; **11** - Chave simétrica inválida; **12** - Chave simétrica repetida; **13** - Estrutura da senha inválida; **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; **19** - Data de criação do pedido não preenchida; **20** - Chave do pedido não preenchida; **21** - Pedido SOAP inválido; **22** - Header inexistente ou vazio; **23** - O NIF não está preenchido no Header; **24** - Não foi possível verificar se o utilizador tem permissões para aceder a esta operação; **25** - Erro na validação da senha (Senha errada, acesso suspenso, etc.). **Código de resposta (serviço):** **-1** - Nem todos os utilizadores estão identificados. **-2** - Existem utilizadores autenticados que não pertencem aos dados do serviço. **-3** - O utilizador autenticado no Security Header não corresponde ao transmitente constante dos dados do pedido de certificado. **-4** - Existem dois Security Headers sem o atributo Actor		

	definido. **-5** - O Actor definido está repetido. **-6** - O Actor indicado não é conhecido. **-7** - O schema da consulta de certificado entregue é inválido **-8** - Não foi possível verificar se o utilizador tem permissões para aceder a esta operação. **-9** - O formato do ficheiro é inválido, tem que ser zip ou xml. **-10** - O nif indicado é inválido. **-11** - O nrm é obrigatório. **-12** – Não existe certificado com o nrm indicado. **-13** – O certificado para o par nrm nif do sujeito passivo indicado não existe. **-14** – O certificado não reúne as condições para ser anulado. **-15** - O utilizador indicado não tem permissões para aceder à operação pretendida. **-99** - Erro interno.		
1.2 – Mensagem de resposta (mensagem)	Mensagem do resultado da invocação desta interface.	S	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 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 emissão do CSR ou do departamento de informática.	80 (chars)

	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

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

6.3 Endereços para envio de dados à AT por Webservice

Ambiente de testes:

https://servicos.portaldasfinancas.gov.pt:706/ivaexp/CertificadoIsencaoWebService/

Ambiente de produção:

https://servicos.portaldasfinancas.gov.pt:..... <a definir brevemente>