



MANUAL DE INTEGRAÇÃO DE SOFTWARE

Comunicação dos Documentos de Transporte à AT

HISTÓRICO DE ALTERAÇÕES

DATA	ALTERAÇÕES
19-02-2013	Criação do documento
21-02-2013	Alteração das descrições do SOAP:Body.
14-03-2013	<ul style="list-style-type: none">• Incluído código de resposta ao Webservice para pedidos SOAP inválidos.• Alterados os portos dos endereços de testes e de produção para 701 e 401, respetivamente.• Indicação da data de disponibilização dos Webservices nos respetivos ambientes: 2 de abril para testes; 1 de maio para produção.• Alteração do SOAP:Body.• Alteração do logotipo.
25-03-2013	<ul style="list-style-type: none">• Alteração do SOAP:Body com a inclusão de lista de referências para o documento de origem ao nível do bem e remoção da referência do documento de origem ao nível do documento de transporte.
02-04-2013	<ul style="list-style-type: none">• Inclusão do formato do ficheiro de resposta.• Alteração do SOAP:Body com a uniformização do wsdl para inglês.
04-04-2013	<ul style="list-style-type: none">• Alteração do Endereços para envio de dados à AT por Webservice (Ambiente de teste).

Í NDI CE

1	INTRODUÇÃO	4
2	ENQUADRAMENTO.....	5
2.1	Comunicação dos Documentos por Webservice	5
2.2	Comunicação dos Documentos de Transporte por SAF-T (PT)	6
2.3	Registo direto no Portal das Finanças	8
3	ADAPTAÇÃO DO SOFTWARE	9
3.1	Comunicação por Webservice	9
3.2	Comunicação por SAF-T (PT)	15
4	ESTRUTURA DO ENVIO DE DADOS À AT (SOAP).....	16
4.1	SOAP:Header	17
4.2	SOAP:Body.....	20
4.3	Resposta ao pedido SOAP	24
5	ASSINATURA CERTIFICADO SSL (CSR)	26
5.1	Gerar um certificado SSL.....	27
5.2	Verificar conteúdo do CSR gerado	28
5.3	Integrar certificado SSL com a chave privada	28
6	ENDEREÇOS ÚTEIS.....	29
6.1	Página de produtores de software	29
6.2	Certificação de software	29
6.3	SAF-T (PT) - Versão portuguesa	29
6.4	Gestão de subutilizadores no PF	29
6.5	WSDL do envio de dados à AT por Webservice.....	29
6.6	Endereços para envio de dados à AT por Webservice	29
7	GLOSSÁRIO	30

1 Introdução

O presente documento descreve os procedimentos e requisitos necessários à comunicação de dados dos documentos de transporte 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 comunicação dos documentos de transporte e, para este efeito, devem guiar-se pelas especificações produzidas pela AT para este efeito de comunicação.

O Sujeito Passivo (também designado por remetente) 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 Decreto-Lei n.º 198/2012 de 24 de agosto, os sujeitos passivos de IVA têm de comunicar os documentos de transporte emitidos à AT, por uma das seguintes vias:

- Por transmissão eletrónica em tempo real, integrada em programa informático, utilizando o Webservice disponibilizado pela AT;
- Através do envio do ficheiro SAF-T (PT), exportado pelo programa informático certificado e recorrendo a aplicação de envio de dados disponibilizada no site e-fatura no Portal das Finanças;
- Através da emissão direta no Portal das Finanças do documento de transporte utilizando as funcionalidades previstas para esta comunicação.

2.1 Comunicação dos Documentos por Webservice

Para efetuar a comunicação por Webservice, tal como disposto no Decreto-Lei n.º 198/2012 de 24 de agosto, os programas informáticos tem que estar adaptados de forma a:

1. Respeitar o modelo de dados tal como previsto no Decreto-Lei n.º 198/2012 de 24 de agosto e definido em formato WSDL publicado no site e-fatura, na página dedicada aos produtores de software, ou em alternativa através do endereço:

<http://info.portaldasfinancas.gov.pt/NR/rdonlyres/A75E1110-7EB8-479E-BC09-6D5B726F6A1C/0/documentosTransporte.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 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.

2.2 Comunicação dos Documentos de Transporte por SAF-T (PT)

Para comunicar os dados dos documentos de transporte por ficheiro SAF-T (PT), cada sujeito passivo (remetente) terá de proceder em dois passos:

1. Extração do ficheiro SAF-T (PT);
2. Envio do ficheiro no Portal das Finanças, site e-fatura.

2.2.1 Extração do Ficheiro SAF-T (PT)

O sujeito passivo (remetente) extrai do seu sistema informático o ficheiro SAF-T (PT) para o efeito de comunicação à AT dos documentos de transporte.

O ficheiro XML para este efeito deve conter as seguintes tabelas do SAF-T (PT) e os respetivos elementos definidos na estrutura de dados disponível no seguinte endereço:

http://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/NEWS_SAF-T_PT.htm

1 - Cabeçalho (Header);

2.2 - Tabela de clientes (Customer);

2.3 - Tabela de fornecedores (Supplier);

4.2 - Documentos de movimentação de mercadorias (MovementOfGoods) adiante também designados por documentos de transporte.

Para efeitos de otimização de envio do ficheiro, este deve conter apenas:

- Os documentos de transporte que ainda não tenham sido enviados - sem código de identificação do documento atribuído pela AT;
- Os documentos de transporte com data de início de transporte entre a data início e data fim de período de ficheiro (Ano, Mês, Dia);
- Os clientes e fornecedores que tenham referência nos Documentos de movimentos de mercadorias (deixando de fora os que não movimentaram mercadorias naquele período);

É recomendável que o envio de movimentos por ficheiro seja efetuado no dia ou dias imediatamente anteriores ao transporte, dependendo o número de dias do processo organizativo de cada sujeito passivo. Assim se vou fazer os movimentos na sexta-feira de manhã, devo comunicar os movimentos na quinta ao final do dia.

Apesar desta recomendação, serão processados todos os ficheiros e até contendo movimentos no próprio dia.

2.2.2 Envio do Ficheiro SAF-T (PT) extraído

Na posse do ficheiro extraído, o sujeito passivo (remetente) acede ao Portal das Finanças e ao site e-fatura:

- Escolhe a opção de “Comunicação por Ficheiro - Enviar” disponível na área dos remetentes;
- Ao escolher esta opção é-lhe disponibilizado um formulário para indicação do ficheiro a comunicar (caminho-da-diretoria-onde-está-guardado e nome.xml); note-se que a extensão do ficheiro será obrigatoriamente .xml.
- Após escolha do ficheiro este é automaticamente validado, apresentando mensagens de erro no caso de o ficheiro não estar em condições de ser submetido;
- Após a correta validação do ficheiro é apresentado um resumo estatístico do seu conteúdo e disponibilizada a opção de envio para a AT - Submeter;
- Ao submeter será necessário introduzir as credenciais (Utilizador e Senha) do Portal das Finanças referentes ao sujeito passivo (remetente) responsável pelo envio do ficheiro de documentos de transporte;
- Após a completa transmissão do ficheiro para a AT é mostrada uma mensagem de confirmação do envio.

Posteriormente, o ficheiro será processado pela AT e, se o conteúdo desse ficheiro for válido, serão processados todos os elementos dos documentos de Transporte, que serão integrados na base de dados de documentos de transporte para os efeitos determinados na lei. Como resposta receberá um ficheiro onde constarem os códigos de identificação AT atribuídos a cada documento válido e com mensagens de validação para os que não foram aceites indicado o motivo de rejeição.

2.2.3 Processamento do ficheiro de resposta

Como resultado do processamento do ficheiro, seja total ou parcialmente integrado, será gerado um ficheiro de resposta contendo:

- Um código de identificação de documento gerado pela AT para cada documento integrado com sucesso;
- Uma mensagem de rejeição de integração indicado o motivo da rejeição.

Quando receber este ficheiro o Sujeito passivo deverá importar os códigos de identificação de documento gerados pela AT para a sua aplicação de gestão de documentos de transporte, de onde originalmente extraiu o ficheiro enviado.

2.2.4 Consulta do processamento dos ficheiros

Para seguimento do tratamento do ficheiro comunicado, o remetente terá disponível uma opção de consulta aos ficheiros SAF-T (PT) por ele submetidos à AT. Sempre que comunique um ficheiro, o remetente deverá posteriormente aceder a essa consulta e verificar se o ficheiro foi processado com Sucesso.

As situações de processamento previstas são:

- **Pendente** - quando ainda espera processamento;
- **Integrado com sucesso** - quando o ficheiro foi totalmente processado e registado na base de dados da AT;
- **Integrado parcialmente** - quando só parte da informação foi processada, por exemplo a que difere da enviada anteriormente por este ou outro meio.
- **Rejeitado** - quando se detetou um problema a nível de conteúdo que impediu o respetivo processamento.

2.3 *Registo direto no Portal das Finanças*

De acordo com o Decreto-Lei n.º 198/2012 está prevista a disponibilização de funcionalidades para a emissão direta de documentos de transporte no portal das finanças, onde os sujeitos passivos devem introduzir todos os elementos obrigatórios para emissão do documento e de onde no final poderão obter o código de identificação atribuído pela AT.

Existirá uma funcionalidade de recolha de dados para o registo das informações dos documentos de transporte que foram parcialmente comunicados por via telefónica e para os quais há a obrigatoriedade de comunicar a totalidade dos dados até ao 5.º dia útil seguinte ao transporte.

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 o envio de documentos de transporte, um a um por Webservice ou para o envio de documentos de transporte por ficheiro SAF-T (PT).

3.1 Comunicação por Webservice

O envio de documentos de transporte por Webservice pressupõe que este é feito à medida que os documentos de transporte são registados no programa informático, estando associado ao conceito de comunicação em tempo real, ou seja, assim que o sujeito passivo regista um documento transporte no programa este é de imediato comunicada à AT por este canal.

Cada produtor de software é responsável por implementar o módulo que vai enviar os documentos de transporte que, para além dos requisitos gerais já enunciados na secção 2.1, deverá respeitar os seguintes passos:

1. Se ainda não tiver efetuado a adesão ao serviço, deverá realizar o processo de adesão à comunicação de documentos de transporte,
 - a) É necessário utilizar o certificado SSL e submetê-lo para ser assinado pela AT, através do processo de adesão ao envio de dados dos documentos de transporte por parte dos produtores de software;
2. O sujeito passivo (remetente) emite documento de transporte no programa informático próprio;
3. O programa informático solícita 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 “WDT - Comunicação de dados de documentos de transporte”;
4. Com base nos dados do documento de transporte criado no passo n.º 1 e nas credenciais solicitada no passo n.º 2 deve construir o pedido SOAP tal como definido:
 - a) No WSDL disponível no endereço:
<http://info.portaldasfinancas.gov.pt/NR/rdonlyres/A75E1110-7EB8-479E-BC09-6D5B726F6A1C/0/documentosTransporte.wsd!>
 - b) Este pedido SOAP (Webservice) é composto 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 do documento de transporte;
5. Estabelecer uma ligação segura em HTTPS com o portal das finanças e utilizando o seguinte endereço de envio de dados de documentos de transporte:

<https://servicos.portaldasfinancas.gov.pt:701/sgdtws/documentosTransporte>

NOTA: este endereço apenas estará disponível a partir do dia **1 de maio de 2013**.

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 documento de transporte;
 - c) Registo com sucesso dos dados do documento de transporte.

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 -> Outros Serviços -> Gestão de utilizadores](#)

Ao criar o subutilizador no Portal das Finanças (1º passo) deve atribuir a autorização WDT disponível para a comunicação de dados dos documentos de transporte. 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., 55555555/55) 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-psws@at.gov.pt								
Subject:	Obtenção do certificado SSL para testes e chave pública do sistema de Autenticação - NIF <NIF>								
<p>Exmos. Senhores,</p> <p>O Produtor de Software <NOME> (NIF <NIF>) vem por este meio solicitar o envio dos seguintes elementos para desenvolvimento e testes de envio de documentos de transporte por Webservice:</p> <ul style="list-style-type: none"> • Chave pública do Sistema de Autenticação do PF; • Certificado SSL para comunicação com o endereço de testes de Webservices. <p>Estes elementos serão utilizados por este produtor de software para incluir nos seguintes programas:</p> <table border="1"> <thead> <tr> <th>Designação Software</th> <th>Certificado AT / DGCI</th> </tr> </thead> <tbody> <tr> <td><SOFTWARE 1></td> <td><CERTIFICADO 1></td> </tr> <tr> <td>...</td> <td>...</td> </tr> <tr> <td><SOFTWARE N></td> <td><CERTIFICADO N></td> </tr> </tbody> </table> <p>Aguardamos a vossa resposta.</p>		Designação Software	Certificado AT / DGCI	<SOFTWARE 1>	<CERTIFICADO 1>	<SOFTWARE N>	<CERTIFICADO N>
Designação Software	Certificado AT / DGCI								
<SOFTWARE 1>	<CERTIFICADO 1>								
...	...								
<SOFTWARE N>	<CERTIFICADO N>								

No *template* anterior, cada produtor de software deve substituir os seguintes elementos pelos seus dados:

- <NIF> - Substituir pelo NIF do produtor de software;
- <NOME> - Substituir pelo NIF 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 os dados dos documentos de transporte, disponível em:

[Site e-fatura -> página Produtores de Software -> opção Testar 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 (e.g., 55555555/55 + SENHA);
2. Cifrar a senha e compor o SOAP:Header de acordo com o definido na secção 4.1;
3. Com base no documento de transporte inserido, 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:
 - a) <https://servicos.portaldasfinancas.gov.pt:701/sgdtws/documentosTransporte>

NOTA: este endereço apenas estará disponível a partir do dia 2 de abril de 2013.

- b) Este endereço só aceita ligações com o certificado SSL disponibilizado para testes (vide 3.1.1);
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 na secção 4.3. As respostas são dos seguintes tipos:
 - a) Código de sucesso;
 - b) Erros de autenticação referentes aos campos do SOAP:Header;
 - c) Erros nos dados dos documentos de transporte 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 dos documentos de transporte 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:401/sqdtws/documentosTransporte>

NOTA: este endereço apenas estará disponível a partir do dia **1 de maio de 2013**.

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 o envio de documentos de transporte por Webservice.

Cada sujeito passivo deve criar um subutilizador para a comunicação de dados dos documentos de transporte de forma em tudo idêntica ao definido no ponto 1 da Fase de Desenvolvimento (vide 3.1.1) e com permissões WDT para comunicação dos documentos de transporte à AT.

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 emite documento de transporte 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.

Uma vez que este serviço deve ser utilizado no envio de cada documento de transporte individualmente, sempre que o produtor de software identificar a necessidade de envio massivo de documentos transporte, deve indicar ao sujeito passivo que tem de utilizar o envio por ficheiro SAF-T (PT), tal como definido na secção 3.2 deste documento.

3.2 Comunicação por SAF-T (PT)

Tal como descrito na secção 2.2 o envio do ficheiro SAF-T (PT) é composto por dois passos: extração a partir do software próprio e posteriormente realizado o envio no site e-fatura.

Para otimização do envio, os produtores de software devem considerar implementar as seguintes características nos seus produtos:

1. Extrair a informação de documentos de transporte que não tenham código de identificação AT;
2. Extrair a informação com a indicação de um determinado período (datas, por dia, etc.);
3. Extrair apenas a informação da tabela de clientes e fornecedores que tenham referência em documentos comerciais desse ficheiro, não incluindo os restantes;

Estas otimizações têm dois efeitos: reduzem o tamanho do ficheiro e conseqüentemente ocupam menos espaço em disco; e conseqüentemente reduzem o tempo necessário para processar cada ficheiro.

Com redução do tamanho poupa-se espaço em disco e consumo de memória de cada processamento efetuado. Reduzindo a informação ao que é relevante em cada ficheiro, permite acelerar o tempo de extração, validação local e conseqüentemente o tempo total de comunicação dos documentos de transporte à AT.

3.2.1 Processamento do ficheiro de resposta

Como resultado do processamento do ficheiro, será gerado um ficheiro de resposta em formato normalizado, na linguagem XML, respeitando o esquema de validação "FicheiroResposta.xsd" disponível no endereço abaixo:

<http://info.portaldasfinancas.gov.pt/NR/rdonlyres/D5EC8326-8297-43AF-BCE6-1CE4B0EF344D/0/FicheiroResposta.xsd>

4 Estrutura do envio de dados à AT (SOAP)

Nesta secção descreve-se informação complementar ao definido no WSDL do serviço de comunicação de dados de documentos transporte em tempo real.

O serviço disponibiliza uma operação de registo de documento de transporte, que possibilita o envio dos elementos previstos no Decreto-Lei n.º 198/2012, documento de transporte a documento de transporte.

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

- d) SOAP:Header;
- e) SOAP:Body

A primeira secção, o Header, inclui todos os campos de autenticação do utilizador que vai ser responsável pela invocação do Webservice. Este utilizador será um subutilizador do NIF do sujeito passivo (remetente) com perfil WDT.

Para criar o subutilizador deve ser utilizada a opção Serviços tributários/Outros serviços/Gestão de utilizadores.

A segunda secção contém os dados do documento de transporte os quais se detalham no tópico SOAP:Body.

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)	<p>Identificação do utilizador que vai submeter os dados, composto da seguinte forma e de acordo com a autenticação do portal das finanças:</p> <p style="text-align: center;"><NIF do emitente>/<UserId></p> <p>Exemplos possíveis:</p> <ol style="list-style-type: none"> 1. 55555555/1 (subutilizador n.º 1) 2. 55555555/0002 (subutilizador n.º 2) 3. 55555555/1234 (subutilizador n.º 1234) 	S	String
H.2 - Nonce	<p>Chave simétrica gerada a cada pedido e para cifrar o conteúdo dos campos H.3 - Password e H.4 - Created.</p> <p>Cada invocação do Webservice deverá conter esta chave gerada aleatoriamente e a qual não pode ser repetida.</p> <p>Para garantir a confidencialidade, a chave simétrica tem de ser cifrada com a chave pública do Sistema de Autenticação de acordo com o algoritmo RSA e codificada em Base 64.</p> <p>A chave pública do sistema de autenticação do portal das finanças deve ser obtida por solicitação própria e através do endereço de email asi-psws@at.gov.pt.</p> <p>O campo é construído de acordo com o seguinte procedimento</p> $\text{Nonce} := \text{Base64}(C_{RSA, K_{pub}_{SA}}(K_s))$	S	String (base64)

¹ Obrigatório: S – Sim; N – Não.

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

	<p>K_S := array de bytes com a chave simétrica de 128 bits, produzida de acordo com a norma AES.</p> <p>$C_{RSA, K_{pubSA}}$:= Função de cifra da chave simétrica com o algoritmo RSA utilizando a chave pública do sistema de autenticação (K_{pubSA}).</p> <p>Base64 := Codificação em Base 64 do resultado.</p>		
<p>H.3 - Password</p>	<p>O campo Password deverá conter a senha do utilizador / subutilizador, a mesma que é utilizada para entrar no Portal das Finanças.</p> <p>Esta Password tem de ser cifrada através da chave simétrica do pedido (ver campo Nonce) e codificado em Base64.</p> <p><i>Password := Base64($C_{K_S}^{AES, ECB, PKCS5Padding}(SenhaPF)$)</i></p> <p>SenhaPF := Senha do utilizador definido no campo H.1 - Username;</p> <p>$C_{K_S}^{AES, ECB, PKCS5Padding}$:= Função de cifra utilizando o algoritmo AES, Modelo ECB, PKCS5Padding e a chave simétrica do pedido (K_S).</p> <p>Base64 := Codificação em Base 64 do resultado.</p>	<p>S</p>	<p>string (base64)</p>
<p>H.4 - Data de sistema (Created)</p>	<p>O campo Created deverá conter a data e hora de sistema da aplicação que está a invocar o webservice.</p> <p>Esta data é usada para validação temporal do pedido, pelo que é crucial que o sistema da aplicação cliente tenha o seu relógio certo.</p> <p>Sugere-se a sincronização com o Observatório Astronómico de Lisboa:</p> <p>http://www.oal.ul.pt/index.php?link=acerto</p> <p>A zona temporal deste campo deverá estar definida para UTC e formatado de acordo com a norma ISO 8601 tal como é definido pelo W3C:</p> <p>http://www.w3.org/QA/Tips/iso-date</p> <p>http://www.w3.org/TR/NOTE-datetime</p> <p>e.g.: 2013-01-01T19:20:30.45Z</p> <p>Este campo é cifrado com a chave de pedido (K_S) e codificada em Base 64.</p> <p><i>Created := Base64($C_{K_S}^{AES, ECB, PKCS5Padding}(Timestamp)$)</i></p>		<p>string (base64)</p>

	<p>Timestamp := data hora do sistema (UTC);</p> <p>$C_{K_s}^{AES, ECB, PKCS5Padding}$:= Função de cifra utilizando o algoritmo AES, Modelo ECB, PKCS5Padding e a chave simétrica do pedido (Ks).</p> <p>Base64 := Codificação em Base 64 do resultado.</p>		
--	--	--	--

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+9p6ARNE1Fg==
      </wss:Nonce>
      <wss:Created>>YEWoIoqIY5DOD11SeXz+0i4b/AJg1/RgNcOH0YpSxGk</wss:Created>
    </wss:UsernameToken>
  </wss:Security>
</S:Header>
```

4.2 SOAP:Body

Nesta secção são definidos os campos para o registo de um novo documento de transporte.

Os campos utilizados no pedido por Webservice derivam do definido na Portaria nº 382/2012 de 23 de novembro para os campos de SAF-T (PT).

Parâmetro	Descrição	Obrig. ³	Tipo Dados ⁴
1.1 – NIF Remetente (TaxRegistrationNumber)	NIF do remetente <ul style="list-style-type: none"> Preencher com o NIF português sem espaços e sem qualquer prefixo do país. 	S	int
1.2 – Nome da empresa (CompanyName)	Nome da empresa <ul style="list-style-type: none"> Denominação social da empresa ou nome do sujeito passivo. 	S	string
1.3 – Endereço da Empresa (CompanyAddress)		S	
1.3.1 – Morada detalhada (AddressDetail)	Deverá incluir o nome da rua, número de polícia e andar, se aplicável.	S	string
1.3.2 – Localidade (City)	Localidade.	S	string
1.3.3 - Código postal (PostalCode)	Código Postal.	S	string
1.3.4 – Pais (Country)	Preencher com <<PT>>.	S	string
1.4 – Identificação única do documento (DocumentNumber)	Identificação única do documento de transporte <ul style="list-style-type: none"> Deve ser idêntico ao que consta no ficheiro SAF-T (PT), quando gerado a partir sistema informático que emitiu este documento; Deve respeitar o formato definido na legislação relativa ao ficheiro SAF-T (PT), em vigor aquando da comunicação dos elementos dos documentos de transporte: <ul style="list-style-type: none"> É composto pelo código interno do documento, seguido de um espaço, seguido do identificador da série do 	S	string

³ Obrigatório: S – Sim; N – Não.

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

	<p>documento, seguido de uma barra (/), e de um número sequencial do documento dentro da série;</p> <ul style="list-style-type: none"> • Não podem existir registos com a mesma identificação. • Não podem ser utilizados o mesmo código interno de documento em tipos de documentos (InvoiceType) diferentes. 		
1.5 - Estado atual do documento <i>(MovementStatus)</i>	<p>Estado de documento. Pode assumir os seguintes valores:</p> <ul style="list-style-type: none"> • N – Normal; • T – Por conta de terceiros; • A – Anulada. 	S	string
1.7– Data do documento <i>(MovementDate)</i>	Data de emissão do documento de transporte.	S	date
1.8 – Tipo do documento <i>(MovementType)</i>	<p>Deve ser preenchido com:</p> <ul style="list-style-type: none"> • GR – Guia de remessa; • GT – Guia de transporte; • GA – Guia de movimentação de ativos próprios; • GC – Guia de consignação; • GD – Guia ou nota de devolução efetuada pelo cliente. 	S	string
1.9 – NIF Cliente <i>(CustomerTaxID)</i>	<p>NIF do cliente nacional</p> <ul style="list-style-type: none"> • Número de Identificação Fiscal português (sem qualquer prefixo do país); • No caso em que não se conhece o destinatário deverá ser preenchido com o NIF <<999999990>>; • Este campo também deve ser preenchido no caso das guias que titulam a transferência de bens do próprio remetente. 	N	string
1.10 – NIF fornecedor <i>(SupplierTaxID)</i>	<p>NIF do fornecedor nacional</p> <ul style="list-style-type: none"> • Número de Identificação Fiscal português (sem qualquer prefixo do país); 	N	string

	<ul style="list-style-type: none"> No caso em que não se conhece o destinatário deverá ser preenchido com NIF <<999999990>>; Este campo apenas deve ser utilizado no caso de guias de devolução ou guias de transporte de bens móveis produzidos ou montados sob encomenda com materiais que o dono da obra tenha fornecido para o efeito e se o campo anterior não estiver preenchido. 		
1.11 – Nome da Empresa Cliente (CustomerName)	<p>Nome da empresa Cliente</p> <ul style="list-style-type: none"> Denominação social da empresa ou nome do sujeito passivo. 	N	string
1.12 – Endereço da Empresa Cliente (CustomerAddress)		N	string
1.12.1 – Morada detalhada (AddressDetail)	Deverá incluir o nome da rua, número de polícia e andar, se aplicável.	N	string
1.12.2 - Localidade (City)	Localidade.	N	string
1.12.3 - Código postal (PostalCode)	Código Postal.	N	string
1.12.4 – Pais (Country)	Preencher com <<PT>>.	N	string
1.13 – Local de descarga (AddressTo)		N	
1.13.1 – Morada detalhada (AddressDetail)	Deverá incluir o nome da rua, número de polícia e andar, se aplicável.	N	string
1.13.2 - Localidade (City)	Localidade.	N	string
1.13.3 - Código postal (PostalCode)	Código Postal.	N	string
1.13.4 – Pais (Country)	Preencher com <<PT>>.	N	string
1.14 – Local de carga (AddressFrom)		S	
1.14.1 – Morada detalhada (AddressDetail)	Deverá incluir o nome da rua, número de polícia e andar, se aplicável.	S	string

1.14.2 - Localidade (City)	Localidade.	S	string
1.14.3 - Código postal (PostalCode)	Código Postal.	S	string
1.14.4 – Pais (Country)	Preencher com PT.	S	string
1.15 – Data hora fim de transporte (MovementEndTime)	Tipo de data e hora: <<AAAA-MM-DD Thh:mm:ss>> em que o <<ss>> pode ser <<00>>, na ausência de informação concreta.	N	dateTime
1.16 – Data hora início de transporte (MovementStartTime)	Tipo de data e hora: <<AAAA-MM-DD Thh:mm:ss>> em que o <<ss>> pode ser <<00>>, na ausência de informação concreta.	S	dateTime
1.17 – Identificador do veículo (VehicleID)	Matrícula do veículo.	N	string
1.18 – Linhas do Documento com os bens (Line)	Linhas de bens do documento de transporte.	S	
1.18.1 – Referência ao documento de origem (OrderReferences)	Existindo a necessidade de efetuar mais do que uma referência, este campo poderá ser gerado tantas vezes quantas as necessárias.	N	string
1.18.2 – Descrição do Produto ou Serviço (ProductDescription)	Descrição da linha da fatura, ligada à tabela de produtos e serviços.	S	string
1.18.3 – Quantidade (Quantity)	Quantidade.	S	decimal
1.18.4 – Unidade de medida (UnitOfMeasure)	Unidade de medida.	S	string
1.18.5 – Preço Unitário (UnitPrice)	Preço unitário sem imposto e deduzido dos descontos de linha e cabeçalho. Em documentos não valorizados deve ser preenchido com <<0.00>>.	S	decimal

4.3 Resposta ao pedido SOAP

Parâmetro	Descrição	Obrig. ⁵	Tipo Dados ⁶
1.1 - Código do resultado (ReturnCode)	<p>Código do resultado da invocação desta interface. Se a resposta for zero, a operação foi bem sucedida. Se for um número diferente de zero, significa que a operação não foi bem-sucedida.</p> <p>Código de sucesso:</p> <p style="padding-left: 40px;">0 – Documento registado com sucesso.</p> <p>Códigos de resposta (autenticação):</p> <p style="padding-left: 40px;">1 - Utilizador não preenchido;</p> <p style="padding-left: 40px;">2 - Tamanho do utilizador incorreto;</p> <p style="padding-left: 40px;">3 - NIF inválido;</p> <p style="padding-left: 40px;">4 - Utilizador com formato inválido;</p> <p style="padding-left: 40px;">5 - Subutilizador com formato inválido;</p> <p style="padding-left: 40px;">6 - Senha não preenchida;</p> <p style="padding-left: 40px;">7 - Codificação Base64 inválida;</p> <p style="padding-left: 40px;">8 - Cifra da chave pública inválida;</p> <p style="padding-left: 40px;">9 - Formato do Timestamp inválido;</p> <p style="padding-left: 40px;">10 - Validade da credencial expirada;</p> <p style="padding-left: 40px;">11 - Chave simétrica inválida;</p> <p style="padding-left: 40px;">12 - Chave simétrica repetida;</p> <p style="padding-left: 40px;">13 - Estrutura da senha inválida;</p> <p style="padding-left: 40px;">33 - Pedido SOAP inválido;</p> <p style="padding-left: 40px;">99 - Erro na validação da senha (Senha errada, acesso suspenso, etc.).</p> <p>Códigos de resposta (dados dos documentos de transporte):</p> <p style="padding-left: 40px;">-1 – Parâmetros de entrados inválidos;</p>	S	Int

⁵ Obrigatório: S – Sim; N – Não.

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

	<p>-2 – Data de emissão inválida;</p> <p>-3 – Documento duplicado;</p> <p>-4 – Entidade emissora não tem permissões para registar documentos com o NIF de emitente indicado;</p> <p>-98 – A integridade referencial, multiplicidade ou tipo de dados dos parâmetros de entrada são inválidos;</p> <p>-99 – Erro interno;</p>		
1.2 - Mensagem <i>(ReturnMessage)</i>	Mensagem descritiva da resposta.	N	string
1.4 – Identificação única do documento <i>(DocumentNumber)</i>	<p>Identificação única do documento de transporte</p> <ul style="list-style-type: none"> • Deve ser idêntico ao que consta no ficheiro SAF-T (PT), quando gerado a partir sistema informático que emitiu este documento; • Deve respeitar o formato definido na legislação relativa ao ficheiro SAF-T (PT), em vigor aquando da comunicação dos elementos dos documentos de transporte: <ul style="list-style-type: none"> ○ É composto pelo código interno do documento, seguido de um espaço, seguido do identificador da série do documento, seguido de uma barra (/), e de um número sequencial do documento dentro da série; • Não podem existir registos com a mesma identificação; 	N	string
1.5 – Código de Identificação do documento <i>(ATDocCodeID)</i>	Código de identificação atribuído pela AT ao documento, nos termos do decreto-lei nº 198/2012, de 24 de agosto.	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 e devolver o certificado SSL assinado digitalmente para que possa ser utilizado no processo de autenticação na invocação do serviço web de apoio à submissão dos documentos de transporte.

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. Tem que ser um endereço de email válido.	80 (chars)
Key bit length	Chave pública do certificado SSL gerado pelo produtor de software tem de ser gerado com 2048 bits.	2048 (bits)

A utilização de caracteres especiais (e.g., portugueses, línguas latinas, etc.) não é aceite em nenhum dos campos acima indicados, uma vez que a utilização desses caracteres vai invalidar a assinatura digital do certificado SSL.

Como resultado deste processo a AT procederá à assinatura do certificado SSL e remete em resposta ao pedido o certificado SSL assinado para integração na chave privada do produtor de software.

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

5.1 Gerar um certificado SSL

Um certificado SSL é uma chave RSA composta por duas partes: chave privada e chave pública.

Como a chave privada deve ser apenas do conhecimento do produtor de software a emissão da mesma tem sempre de ser efetuada pelo próprio, em computador próprio e nunca num site ou serviço web que encontre para o efeito.

Existem diversas ferramentas para geração de certificados SSL, proprietárias e Opensource. Para efeitos de exemplo a AT utiliza a ferramenta OpenSSL, que é a ferramenta Opensource de referência, livre de custos de utilização.

Para gerar um certificado SSL cada produtor de software deve fazê-lo no seu próprio computador utilizando o seguinte comando:

```
➤ openssl req -new -subj "/C=PT/ST=Distrito da Sede/L=Local da Sede/O=Empresa /OU=Departamento de Informatica/CN=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*

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

6.2 *Certificação de software*

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

6.3 *SAF-T (PT) - Versão portuguesa*

http://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/NEWS_SAF-T_PT.htm

6.4 *Gestão de subutilizadores no PF*

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

6.5 *WSDL do envio de dados à AT por Webservice*

<http://info.portaldasfinancas.gov.pt/NR/rdonlyres/A75E1110-7EB8-479E-BC09-6D5B726F6A1C/0/documentosTransporte.wsdl>

6.6 *Endereços para envio de dados à AT por Webservice*

Ambiente de testes

<https://servicos.portaldasfinancas.gov.pt:701/sqdtws/documentosTransporte>

NOTA: este endereço apenas estará disponível a partir do dia **2 de abril de 2013**.

Ambiente de produção

<https://servicos.portaldasfinancas.gov.pt:401/sqdtws/documentosTransporte>

NOTA: este endereço apenas estará disponível a partir do dia **1 de maio de 2013**.

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