AT autoridade tributária e aduaneira

MANUAL DE INTEGRAÇÃO DE SOFTWARE

Comunicação de Séries Documentais de Autofaturação com Acordo, Aspetos Genéricos

Portaria n.º 195/2020

Versão 1.0

Dezembro 2022

HISTÓRICO DE ALTERAÇÕES

DATA	VERSÃO	DESCRIÇÃO
07-12-2022	V1.0	Versão inicial

ÍNDICE

1. Introdução

O desenho do *webservice* do sistema de Gestão e Controlo de Séries de Autofaturação é muito semelhante ao dos *webservices* que a Autoridade Tributária e Aduaneira (AT) disponibiliza no quadro dos Documentos de Transporte e do e-Fatura. Dada esta similitude, que resultou da preocupação em reduzir o esforço de desenvolvimento exigido aos produtores de software, optou-se por dividir o Manual de Integração em dois documentos:

- O **Manual de Integração de Software de Comunicação de Séries Documentais de Autofaturação com Acordo, Aspetos Genéricos** que descreve aspetos técnicos do tratamento de séries documentais de autofaturação comuns a outros *webservices* da AT, como os indicados antes;
- O **Manual de Integração de Software de Comunicação de Séries Documentais de Autofaturação com Acordo, Aspetos Específicos** que descreve os aspetos particulares, específicos das operações realizadas através do *webservice*, caracterizando, nomeadamente, a estrutura técnica dos conteúdos XML necessários à invocação do *webservice* do Sistema de Gestão e Controlo de Séries.

A menos que especificado diferentemente, todas as referências feitas neste documento a comunicações com a AT ou a *webservices*, referem-se sempre a comunicações com a AT via *webservice* no âmbito da Comunicação de Séries Documentais de Autofaturação com Acordo.

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

A solução apresentada permite a realização de comunicações com a AT no âmbito do *webservice* de Comunicação de Séries Documentais de Autofaturação, prevista no Decreto-lei n.º 28/2019, de 15 de fevereiro. Para efetuar a comunicação por *webservice* os programas informáticos têm de estar adaptados de forma a:

1. Respeitar o modelo de dados tal como definido em formato WSDL;
2. Utilizar os protocolos de comunicação definidos para a transmissão de dados utilizando este serviço, designadamente o protocolo SOAP;
3. Implementar os mecanismos de segurança na transmissão de dados que visam garantir a confidencialidade dos dados, designadamente:

a) Comunicação de dados através de canal HTTPS, com utilização de certificado digital que autoriza a comunicação com a AT;
b) Encriptação da senha dos utilizadores no Portal das Finanças recorrendo a chave pública fornecida especificamente para este efeito pela AT;
c) Demais mecanismos, definidos em detalhe neste documento para garantir a segurança da transmissão dos dados para a AT.

2. Credenciais do operador económico (utilizador e senha)

Qualquer utilização do webservice exige a indicação das credenciais (nome do utilizador e senha do Portal das Finanças) de quem está a invocar o serviço. A responsabilidade de qualquer comunicação com a AT é sempre do detentor destas credenciais que aparecem na invocação do *webservice*.

Os métodos do *webservice* da Gestão e Controlo de Séries de Autofaturação foram desenhados para serem usados pelos autofaturantes. As credenciais (utilizador e senha do Portal das Finanças) a usar na invocação daqueles métodos do *webservice* têm de ser dos respetivos autofaturantes.

Dado que as credenciais do autofaturante só devem ser conhecidas do próprio, o *software* deve estar preparado para solicitar a sua introdução por este, quando necessário, não devendo as mesmas estar guardadas no programa.

2.1. Sub-utilizador e perfil

Por outro lado, para invocar o *webservice* é necessário que o utilizador que está a invocar o *webservice* esteja autorizado a fazê-lo, isto é, que tenha o perfil WSE - Comunicação de Séries Documentais por *Webservice*. O procedimento a seguir para obter as credenciais a usar na invocação é o seguinte:

Criar um sub-utilizador e atribuir-lhe o perfil WSE - Comunicação de Séries Documentais por *Webservice* em: https://www.acesso.gov.pt/gestaoDeUtilizadores/criarForm?partID=PFIN

2.2. Cifra da senha do utilizador

A senha do utilizador tem de ser cifrada recorrendo à chave pública do sistema de autenticação do Portal das Finanças. Não dispondo desta chave pública, o produtor de software deverá solicitá-la à AT (ver secção Chave pública do Sistema de Autenticação para cifra de credenciais e certificado digital).

2.3. Credenciais de Testes

Para a realização de testes, os produtores de *software* deverão utilizar um sub-utilizador do seu NIF, atribuindo-lhe também o perfil WSE - Comunicação de Séries Documentais por Webservice.

No ambiente de testes, a informação submetida/consultada fica residente em ambiente próprio para o efeito, no entanto, a autenticação é validada com os dados de produção do sub-utilizador mencionado acima.

3. Certificado digital

A AT só aceita o estabelecimento de comunicação de dados se o programa enviar, no processo de comunicação, o Certificado Digital emitido para este efeito. Este certificado digital apenas garante o estabelecimento da comunicação sendo responsabilidade do produtor de *software* transmitir corretamente os dados dos operadores económicos, seus clientes.

Para a comunicação de Séries Documentais de Autofaturação poderão ser usados certificados digitais que se encontrem em uso nos procedimentos do e-Fatura ou dos documentos de transporte.

Se o produtor de *software* não dispuser de um certificado digital emitido pela AT, é necessário efetuar a adesão ao serviço através do formulário disponível em:

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

Para completar o pedido de adesão, é necessário gerar um certificado digital de acordo com as instruções disponíveis (ver Gerar um certificado digital).

A AT responde ao pedido por mensagem de email, contendo o certificado assinado.

3.1. Certificado de testes

Para a realização de testes de comunicação deverá ser usado o certificado digital disponibilizado pela AT para ser usado apenas em testes. No caso de o produtor de *software* não dispor deste certificado da AT, poderá obtê-lo como indicado em Chave pública do Sistema de Autenticação para cifra de credenciais e certificado digital.

4. Estrutura das comunicações com a AT via *webservice* (SOAP)

A estrutura das comunicações (pedido SOAP) deve seguir o WSDL disponível no endereço:

> Portal das Finanças » Informação » Apoio » Faturação - Regras e mecanismos de comunicação » Comunicação de Séries à AT e ATCUD » Especificação de Webservice de Autofaturação (WSDL).

Este pedido SOAP (*Webservice*) é composto pelas seguintes secções:

- 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 de ser cifrada recorrendo à chave pública do sistema de autenticação do Portal das Finanças). Esta secção encontra-se detalhada neste documento;
- SOAP: *Body* - contém os dados comerciais. Esta secção encontra-se detalhada no Manual de Integração de Software de Comunicação de Séries Documentais de Autofaturação com Acordo, Aspetos Específicos;

Descreve-se a informação complementar ao definido no WSDL do serviço de comunicação de dados de Séries Documentais de Autofaturação com Acordo.

A secção *Header*, inclui todos os campos de autenticação do utilizador que vai ser responsável pela invocação do *webservice*. Como referido, este utilizador será um sub-utilizador do NIF do operador económico com perfil WSE - Comunicação de Séries Documentais por *Webservice* (ver Credenciais do operador económico (utilizador e senha).

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 procedimentos de encriptação infra descritos.

O SOAP:*Header* é construído de acordo com o *standard* WS-*Security* e recorrendo à definição do *Username Token Profile* 1.1, definidos pela OASIS.

Na seguinte tabela, detalha-se a forma de construção de cada campo, de acordo com as necessidades de segurança específicas do sistema de autenticação do Portal das Finanças.

Parâmetro	Descrição	Obrig.	Tipo de dados[1]
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: A. 555555555/1 (subutilizador n.º 1); B. 555555555/0002 (subutilizador n.º 2); C. 555555555/1234 (subutilizador n.º 1234);	Sim	string
H.2 - Password	O campo Password deverá conter a senha do utilizador / sub-utilizador, 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($C_K^{AES_S,ECB,PKCS\ 5Padding}$ (SenhaPF)) **SenhaPF** = Senha do utilizador definido no campo H.1 - Username; $C_K^{AES_S,ECB,PKCS\ 5Padding}$ = 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.	Sim	string (base64)

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

Parâmetro	Descrição	Obrig.	Tipo de dados[1]
H.3 - 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. O campo é construído de acordo com o seguinte procedimento: **Nonce** = Base64($C_{RSA,KpubSA}$ (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.	Sim	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.: 2013-01-01T19:20:30.45Z Este campo é cifrado com a chave de pedido (K_S) e codificada em Base64. Created = Base64($C_K^{AES_S,ECB,PKCS\ 5Padding}$ (Timestamp)) **Timestamp** = data hora do sistema (UTC); $C_K^{AES_S,ECB,PKCS\ 5Padding}$ = Função de cifra utilizando o algoritmo AES, Modelo ECB, PKCS5Padding e a chave simétrica do pedido (K_S); **Base64** = Codificação em Base64 do resultado.	Sim	string (base64)

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 (dados de autenticação meramente exemplificativos):

```
<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>
```

4.1.2. Tabela de erros de autenticação / autorização no Portal das Finanças

Código do erro	Descrição
104x	Formato do Pedido XML Incorreto (cabeçalho de segurança)
105x	Erro interno no processo de autenticação/autorização
11xx	Gama de erros no âmbito da autenticação
12xx	Gama de erros no âmbito da autorização
1200	Utilizador sem perfil adequado para aceder ao serviço

5. Assinatura certificado digital (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 digital a ser utilizado na operação é emitido pela AT, a pedido da entidade aderente. Para este efeito, a entidade aderente deve efetuar um pedido de certificado digital (CSR – *Certificate Signing Request*).

O CSR é um pequeno ficheiro de texto cifrado que contém o certificado digital e toda a informação necessária para que a AT possa assinar e devolver o certificado digital, para que possa ser utilizado na autorização da invocação do *webservice*.

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 que segue infra, 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 / Organization	Designação legal da empresa	180 (chars)
OU = Department Name / Organizational Unit	Departamento para contacto.	180 (chars)
E = An email address	O endereço de correio eletrónico para contacto, geralmente do responsável pela emissão do CSR ou do departamento de informática. Tem de ser um endereço de email válido.	80 (chars)
Key bit length	Chave pública do certificado digital 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 digital.

Como resultado deste processo, a AT procederá à assinatura/emissão do certificado digital e remete, em resposta ao pedido, o certificado digital para integração na chave privada do produtor de *software*.

5.1. Gerar um certificado digital

Um certificado digital 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 digitais, 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 digital, 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, do comando anterior será gerado o certificado digital 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 pretendida. 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 com a chave privada

Depois de receber o certificado digital emitido pela AT, é necessário integrar esse certificado com a chave privada gerada no passo anterior (555555555.key). Para tal, deve ser usado um dos seguintes comandos:

```
openssl pkcs12 -export -in 555555555.crt -inkey 555555555.key -out 555555555.pfx
openssl pkcs12 -export -in 555555555.cer -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 digital 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.

5.4. Renovação do certificado digital

O certificado emitido tem neste momento a validade de 24 meses, devendo ser renovado pelo menos um mês antes do fim da sua validade. A renovação processa-se de modo idêntico ao primeiro pedido.

6. Anexos

6.1. Endereços úteis

Página de produtores de *software*:

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

Certificação de *Software* de Faturação:

https://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/Faturacao/Paginas/certificacao-de-software.aspx

Gestão de sub-utilizadores no Portal das Finanças:

https://www.acesso.gov.pt/gestaoDeUtilizadores/criarForm?partID=PFIN

6.2. Chave pública do Sistema de Autenticação para cifra de credenciais e certificado digital

No caso de o produtor de *software* não dispor da chave pública do Sistema de Autenticação a utilizar na cifra das credencias do utilizador ou do certificado digital de comunicação em testes, poderá obtê-los por um dos seguintes meios:

a. Através do e-balcão, no Portal das Finanças;
b. Através da opção Testar *Webservice*, no e-Fatura, Produtores de *Software*;
c. Enviando um email como indicado a seguir:

To:	asi-cd@at.gov.pt
Subject:	Obtenção do certificado digital 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 digital para comunicação com o endereço de testes de *webservices*. Aguardamos a vossa resposta.	

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
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/ Pode 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: https://www.acesso.gov.pt/v2/loginForm?partID=PFAP Sistema responsável por validar as credenciais de um utilizador registado no Portal das Finanças.
SOAP	http://www.w3.org/TR/soap/
Standard Date Format ISO 8601	http://www.w3.org/TR/NOTE-datetime http://www.w3.org/QA/Tips/iso-date
Username Token Profile	http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-UsernameTokenProfile.pdf
Webservice	http://www.w3.org/TR/ws-arch/
WS-Security	http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
WSDL	http://www.w3.org/TR/wsdl