AT autoridade tributária e aduaneira



MANUAL DE INTEGRAÇÃO DE SOFTWARE

Comunicação de dados DAC9/GIR por WebService

HISTÓRICO DE ALTERAÇÕES

VERSÃO	DATA	ALTERAÇÕES
1.0	16-07-2026	Criação do documento.

ÍNDICE

1 INTRODUÇÃO 4
1.1 Namespaces usados 5

2 ENQUADRAMENTO 6

3 ADAPTAÇÃO DO SOFTWARE 7

4 ESTRUTURA DO SERVIÇO DE SUBMISSÃO DE DADOS DAC9/GIR À AT (SOAP) 13
4.1 Pedido SOAP 14
4.2 Resposta ao pedido SOAP 19
4.3 Tipos Acessórios 21

5 ASSINATURA CERTIFICADO SSL (CSR) 23
5.1 Gerar um certificado SSL 24
5.2 Verificar conteúdo do CSR gerado 25
5.3 Integrar certificado SSL com a chave privada 25

6 ENDEREÇOS ÚTEIS 26
6.1 Página de produtores de software 26
6.2 Página de apoio ao contribuinte 26
6.3 Página de gestão de utilizadores 26
6.4 Endereços para envio de dados DAC9/GIR à AT por Webservice 26

7 GLOSSÁRIO 27

1 Introdução

O presente documento descreve os procedimentos e requisitos necessários para a comunicação de dados DAC9/GIR à Autoridade Tributária e Aduaneira (AT).

Este documento destina-se a apoiar as entidades ou indivíduos, doravante designados por produtores de software, que desenvolvam e/ou comercializem software para as entidades reportantes (seus clientes utilizadores do software produzido). Os produtores de software são responsáveis por desenvolver programas que cumpram com os requisitos legais da comunicação de dados DAC9/GIR e para este efeito devem guiar-se pelas especificações produzidas pela AT.

A entidade reportante é responsável pelo envio e pelos dados do pedido, uma vez que utiliza as suas credenciais no Portal das Finanças (utilizador e senha). Estas credenciais só podem ser conhecidas pela própria devendo o software produzido estar preparado para solicitar estas credenciais, 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 [6.1].

A AT só aceita estabelecimento de comunicação de dados se for enviado no processo de comunicação, o certificado SSL emitido para este efeito. Este certificado apenas garante o estabelecimento da comunicação sendo responsabilidade do produtor de software transmitir corretamente os dados dos seus clientes.

1.1 Namespaces usados

Por uma questão de síntese, a declaração dos *namespaces* foi omitida dos exemplos e da referência nos capítulos seguintes.

São listados na seguinte tabela, para referência, todos os prefixos de *namespaces* utilizados.

Prefixo	*Namespace*	Descrição
at	http://at.pt/wsp/auth	AT Authentication Extension
S	http://www.w3.org/2003/05/soap-envelope	SOAP Envelope Specification
wss	http://schemas.xmlsoap.org/ws/2002/12/secext	Web Services Security Policy Language

2 Enquadramento

A solução disponibilizada no Portal das Finanças permite o cumprimento de obrigação de submissão de dados DAC9/GIR, por diferentes modos:

- *Upload* (directamente no Portal das Finanças)
- *Webservice*

O cumprimento desta obrigação legal fica ao encargo da entidade reportante.

Para efetuar a comunicação de dados 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 Portal das Finanças.
2. Utilizar os protocolos de comunicação definidos para a transmissão de dados utilizando este serviço, designadamente o protocolo SOAP.
3. Implementar os mecanismos de segurança na transmissão de dados que visam garantir a confidencialidade dos dados, designadamente:
    a) Comunicação de dados através de canal HTTPS, com utilização de certificado SSL que identifica o produtor de software e que foi previamente assinado pela AT;
    b) Encriptação da senha dos utilizadores no Portal das Finanças recorrendo à chave pública (RSA) do Sistema de Autenticação;
    c) Demais mecanismos, definidos em detalhe neste documento para garantir a segurança da transmissão dos dados para a AT.

3 Adaptação do software

Nesta secção a AT apresenta as suas recomendações aos produtores de *software* de forma a alterarem os seus programas informáticos para incluírem o envio de dados DAC9/GIR, via *Webservice*.

Cada produtor de software é responsável por implementar o módulo que vai enviar os dados DAC9/GIR, que deverá respeitar os seguintes passos:

1. Se ainda não tiver efetuado a adesão ao serviço, deverá realizar o processo de adesão ao envio de dados DAC9/GIR - (ver secção 6.1):
    a) É necessário utilizar o certificado SSL e submetê-lo para ser assinado pela AT, através do processo de adesão ao envio de dados DAC9/GIR por parte dos produtores de software.
2. A entidade reportante preenche o ficheiro no programa informático próprio;
    a) O programa informático solicita as credenciais dos intervenientes nesta submissão tal como definidas no Portal das Finanças.
3. Com base nos dados do ficheiro criado no passo n.º 1 e nas credenciais solicitadas no passo n.º 2 deve construir o pedido SOAP:
    a) Seguindo o WSDL;
    b) Estes pedidos SOAP (*Webservice*) são compostos pelas seguinte secções, descritas no capítulo 4 - Estrutura do serviço de submissão de dados DAC9/GIR à AT (SOAP), e que se resumem a:
        - SOAP:Header – onde se incluem os campos de autenticação dos utilizadores que vão ser responsáveis pela invocação do *Webservice* (as senhas que vão nesta secção têm que ser cifradas recorrendo à chave pública do sistema de autenticação do Portal das Finanças);
        - SOAP:Body – contém os dados DAC9/GIR;
        - SOAP:Fault – contém a exceção de autenticação ocorrida efetuar o pedido.
4. Estabelecer uma ligação segura em HTTPS com o Portal das Finanças utilizando o seguinte endereço para as várias operações:
    - https://servicos.portaldasfinancas.gov.pt:427/dac9gir/ws/ficheiro/enviar
5. Processar corretamente o código de resposta devolvido pelo *Webservice*, que pode ser de três tipos:
    a) Mensagens de autenticação inválida;

b) Mensagens de processamento inválido dos dados (DAC9/GIR);

c) Registo com sucesso dos dados (DAC9/GIR).

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

- Desenvolvimento
- Testes
- Distribuição
- Produção

Fase de Desenvolvimento

Para poder iniciar o desenvolvimento cada produtor de software deve obter junto da AT os elementos necessários para o efeito, designadamente:

1. Criar sub-utilizador do próprio produtor de *software* fazendo-o no Portal das Finanças (ver secção 6.4):

   Site Portal das Finanças » Serviços » Autenticação de Contribuintes » Gestão de Utilizadores

   Ao criar o sub-utilizador no Portal das Finanças (1º passo) deve atribuir a autorização WD9, disponível para a comunicação de dados DAC9/GIR.

   Para criar este utilizador é necessário indicar um:

   - Nome,
   - Senha (e respetiva confirmação),
   - Endereço de e-mail para utilização em contactos por parte da AT.

   No final é obtida a identificação do sub-utilizador (e.g., 555555555/55) e a respetiva senha, que deve ser comunicada à equipa de desenvolvimento.

2. Obter a chave pública do Sistema de Autenticação do Portal das Finanças para cifrar a senha do utilizador e certificado SSL assinado para comunicação com o endereço de testes:

   É necessário enviar um email à AT a solicitar o envio dos mesmos. A mensagem a enviar por email deve respeitar o seguinte *template*:

TO:	asi-cd@at.gov.pt
Subject:	Obtenção do certificado SSL para testes e chave pública do Sistema de Autenticação - NIF <NIF>

Exmos. Senhores,

O Produtor de Software <NOME> (NIF <NIF>) vem por este meio solicitar o envio dos seguintes elementos para desenvolvimento e testes de envio de dados DAC9/GIR:

- Chave pública do Sistema de Autenticação do PF;
- Certificado SSL para comunicação com o endereço de testes de *Webservices*.

Estes elementos serão utilizados por este produtor de software para incluir nos seguintes programas:

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

Aguardamos a vossa resposta.

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

<NIF> - Substituir pelo NIF do produtor de software;

<NOME> - Substituir pelo Nome do produtor de software.

<SOFTWARE N> - Designação do software N

<CERTIFICADO N> - Nº de certificado da AT (DGCI se ainda for o caso)

3. Obter o WSDL que define a estrutura do pedido SOAP a construir para enviar os dados DAC9/GIR.

   Para a correta construção do pedido SOAP (invocação do *Webservice*) deve utilizar a informação complementar disponível no capítulo 4 - Estrutura do serviço de submissão de dados DAC9/GIR à AT (SOAP), onde se detalha a informação que deve constar dos campos do pedido SOAP bem como a sua forma de construção.

Fase de Testes

A AT disponibiliza um endereço de testes para verificação da comunicação de dados à AT de forma a apoiar cada produtor de software na correta disponibilização dos seus programas aos seus clientes (ver secção 6.1, opção Testar *webservice*).

Para este efeito, a aplicação desenvolvida para a submissão de dados DAC9/GIR deverá seguir o seguinte procedimento:

1. Utilizar credenciais de sub-utilizador e senha criada para efeito de testes de comunicação de dados DAC9/GIR, com o perfil apropriado (e.g., 555555555/55 + SENHA);
2. Com base no ficheiro preenchido, construir o SOAP:Body de acordo com o definido no capítulo 4.1 - Pedido SOAP;
3. Cifrar a senha e compor o SOAP:Header de acordo com o definido na secção SOAP:Header do capítulo 4.1 - Pedido SOAP;
4. Estabelecer uma ligação HTTPS com o seguinte endereço disponibilizado apenas para testes;

   Endereço: https://servicos.portaldasfinancas.gov.pt:727/dac9gir/ws/ficheiro/enviar

   a) Este endereço apenas aceita ligações com o certificado SSL disponibilizado para testes.
5. Submeter o pedido SOAP construído no ponto 3;
6. Processar a resposta que o serviço lhe devolve de acordo com as várias hipóteses definidas no capítulo 4.2 - Resposta ao pedido SOAP. As respostas são dos seguintes tipos:

   a) Código de sucesso;

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

   c) Erros nos dados DAC9/GIR referentes aos campos preenchidos no SOAP:Body.

Tendo em consideração que se trata do ambiente de testes, existe a possibilidade de os dados existentes neste ambiente poderem ser apagados periodicamente.

Fase de Distribuição

Depois de confirmarem a correta adaptação do programa informático e antes de distribuir os programas aos clientes é necessário proceder da seguinte forma:

1. Efetuar a adesão ao envio de dados através do formulário disponível em:

   Site e-fatura » página Produtores de Software » opção Aderir ao Serviço

   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 no capítulo 5 - Assinatura certificado SSL (CSR);

   c) A AT responde a este pedido por mensagem de e-mail contendo o certificado SSL assinado digitalmente pela AT.

2. Alterar o endereço de comunicação para o endereço de comunicação de dados à AT em ambiente de produção:

   - https://servicos.portaldasfinancas.gov.pt:427/dac9gir/ws/ficheiro/enviar

3. Substituir o certificado SSL utilizado em testes (ponto 4 da Fase de Testes) pelo certificado SSL de produção emitido no ponto 1 alínea c) desta fase.

Depois de concluído este procedimento o(s) vosso(s) programas informáticos estão prontos para serem distribuídos aos vossos clientes.

Fase de produção

Depois de instalado o programa informático nos computadores dos vossos clientes (entidades reportantes) estão em condições para iniciar o envio de dados DAC9/GIR via *Webservice*.

Por regra, o envio procede da seguinte forma:

1. O utilizador (entidade reportante) preenche os dados no programa informático;
2. São obtidas as credenciais dos intervenientes na submissão configuradas no programa informático;
3. É construído o pedido SOAP e invocado o *Webservice*, em produção, com os dados do ponto 1 e ponto 2;
4. Programa processa a resposta do serviço e informa o utilizador do sucesso ou solicita ação do utilizador para o caso de erro no envio.

4 Estrutura do serviço de submissão de dados DAC9/GIR à AT (SOAP)

Nesta secção descreve-se informação complementar ao definido no WSDL do serviço de submissão de dados DAC9/GIR.

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

a) SOAP:Header;

b) SOAP:Body

A primeira secção, o *Header*, inclui todos os campos de autenticação dos utilizadores que vão ser responsáveis pela invocação do *Webservice*. Estes utilizadores podem ser o NIF da entidade reportante ou um sub-utilizador da mesma com as respetivas permissões.

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

Portal das Finanças » Aceda aos Serviços Tributários » Serviços » Autenticação de Contribuintes » Gestão de Utilizadores [6.3]

A segunda secção contém os dados DAC9/GIR, os quais se detalham no tópico SOAP:Body.

O serviço de submissão de dados DAC9/GIR prevê as seguintes operações:

a) SendDac9GirFile, que permite o registo de dados DAC9/GIR junto da AT;

Mais à frente neste capítulo serão explicados os campos envolvidos na invocação de cada uma das operações deste serviço.

4.1 Pedido SOAP

SOAP:Header

O desenho do *Header* tem como requisito garantir a confidencialidade dos dados de autenticação e a impossibilidade de reutilização dos mesmos em ataques *Man-in-the-middle* (MITM). Por este motivo, só serão aceites invocações que respeitem os seguintes procedimentos de encriptação.

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

Na seguinte tabela, detalha-se a forma de construção de cada campo do *WS-Security*, e de acordo com as necessidades de segurança específicas do Sistema de Autenticação do Portal das Finanças.

Parâmetro	Descrição	Obrig.[1]	Tipo Dados[2]
H.1 - Utilizador (Username)	Identificação do utilizador que vai submeter os dados, composto da seguinte forma e de acordo com a autenticação do portal das finanças: <NIF do emitente>/<UserId> Exemplos possíveis: 1. 555555555/0000 (utilizador principal) 2. 555555555/1 (sub-utilizador n.º 1) 3. 555555555/0002 (sub-utilizador n.º 2) 4. 555555555/1234 (sub-utilizador n.º 1234)	S	string
H.2 - Nonce	Chave simétrica gerada por autenticação para cifrar o conteúdo do campo H.3 - Password e do seu atributo Digest. Cada autenticação deverá conter esta chave gerada aleatoriamente e a qual não pode ser repetida entre *headers* de autenticação (wss:Security) e entre pedidos. Para garantir a confidencialidade, a chave simétrica tem de ser cifrada com a chave pública do Sistema de Autenticação de acordo com o algoritmo RSA e codificada em Base 64. A chave pública do Sistema de Autenticação do Portal das Finanças deve ser obtida por solicitação própria e através do endereço de e-mail asi-cd@at.gov.pt conforme o descrito na secção Fase de Desenvolvimento do capítulo 3.1. O campo é construído de acordo com o seguinte procedimento	S	string (base64)

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

Parâmetro	Descrição	Obrig.[1]	Tipo Dados[2]
	$$Nonce := Base64(C_{RSA,Kpub_{SA}}(K_s))$$ **Ks** := array de bytes com a chave simétrica de 128 bits, produzida de acordo com a norma AES. **$C_{RSA,KpubSA}$** := Função de cifra da chave simétrica com o algoritmo RSA utilizando a chave pública do Sistema de Autenticação (K_{pubSA}). **Base64** := Codificação em Base 64 do resultado.		
H.3 - Password	O campo Password deverá conter a senha do utilizador / sub-utilizador, a mesma que é utilizada para entrar no Portal das Finanças. Esta senha tem de ser cifrada através da chave simétrica do pedido (ver campo Nonce) e codificado em Base64. $$Password := Base64(C_{K_s}^{AES,ECB,PKCS5Padding}(SenhaPF))$$ **SenhaPF** := Senha do utilizador definido no campo H.1 - Username; $C_{K_s}^{AES,ECB,PKCS5Padding}$:= Função de cifra utilizando o algoritmo AES, Modelo ECB, PKCS5Padding e a chave simétrica do pedido (K_S). **Base64** := Codificação em Base 64 do resultado. Adicionalmente este campo deverá conter o atributo Digest. Este atributo deverá conter um digest da password, seguindo a seguinte fórmula: $$Digest := Base64(C_{K_s}^{AES,ECB,PKCS5Padding}(SHA-1(K_s + Created + SenhaPF)))$$ **K_s+Created+SenhaPF** := São os bytes dos três campos concatenados; **SHA**-1 := Função de cálculo de digest usando o algoritmo SHA-1; $C_{K_s}^{AES,ECB,PKCS5Padding}$:= Função de cifra utilizando o algoritmo AES, Modelo ECB, PKCS5Padding e a chave simétrica do pedido (K_S). **Base64** := Codificação em Base 64 do resultado.	S	string (base64)

Parâmetro	Descrição	Obrig.[1]	Tipo Dados[2]
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 de acordo com a hora legal. Sugere-se a sincronização com o Observatório Astronómico de Lisboa: http://www.oal.ul.pt/index.php?link=acerto A zona temporal deste campo deverá estar definida para UTC e formatado de acordo com a norma ISO 8601 tal como é definido pelo W3C: http://www.w3.org/QA/Tips/iso-date http://www.w3.org/TR/NOTE-datetime e.g.: 2013-01-01T19:20:30.45Z Este campo não deve ser cifrado. $Created := Timestamp$ **Timestamp** := data hora do sistema (UTC).		string (base64)

Autenticação de contribuintes

O Sistema de Autenticação do Portal das Finanças estendeu o protocolo de autenticação atual. Esta nova versão, versão "2", é compatível com o uso da versão anterior. Isto é, existindo a necessidade de autenticação de apenas um utilizador, é aceite o uso de qualquer uma das versões de autenticação.

Uma vez que a submissão de dados DAC9/GIR exige que todos os intervenientes nesta submissão sejam autenticados perante a AT, na invocação deste serviço deverá ser utilizado o atributo */wss:Security@S:Actor* por forma a identificar em que qualidade o utilizador a ser autenticado está a atuar.

/wss:Security/@S:Actor	Valor semântico
http://at.pt/actor/SPA	Contribuinte (entidade reportante)

O valor utilizador por omissão é o *"http://at.pt/actor/SPA"*.

Para a utilização desta versão, deverá ser utilizado o atributo */wss:Security/@Version* com o valor "2", tal como os exemplos que se seguem o demonstram.

Exemplos SOAP:Header

Como resultado da aplicação das regras de construção anteriores será produzido um *header* de pedido SOAP tal como os seguintes exemplos:

Autenticação do Contribuinte:

Neste exemplo, o *Actor* é definido explicitamente. O número de versão é incluído no atributo *Version*, com o valor "2".

```
<S:Header>
   <wss:Security xmlns:wss="http://schemas.xmlsoap.org/ws/2002/12/secext"
      S:Actor="http://at.pt/actor/SPA" at:Version="2">
      <wss:UsernameToken>
         <wss:Username>555555555</wss:Username>
         <wss:Password Digest="AAAAAA==">AAAAAAAAAAAAAAAA=</wss:Password>
         <wss:Nonce>
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
         </wss:Nonce>
         <wss:Created>2015-03-09T20:45:05.424Z</wss:Created>
      </wss:UsernameToken>
   </wss:Security>
</S:Header>
```

Autenticação do Contribuinte sem definir o Actor explicitamente:

Neste caso, o *Actor* a ter em conta é o *"http://at.pt/actor/SPA"*, sendo este o *Actor* por omissão. O número de versão é incluído no atributo *Version*, com o valor "2".

```
<S:Header>
   <wss:Security xmlns:wss="http://schemas.xmlsoap.org/ws/2002/12/secext"
      at:Version="2">
      <wss:UsernameToken>
         <wss:Username>555555555</wss:Username>
         <wss:Password Digest="AAAAAA==">AAAAAAAAAAAAAAAA=</wss:Password>
         <wss:Nonce>
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
         </wss:Nonce>
         <wss:Created>2015-03-09T20:45:05.424Z</wss:Created>
      </wss:UsernameToken>
   </wss:Security>
</S:Header>
```

SOAP:Body

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

Operação *SendDac9GirFile* – dados do elemento *SendDac9GirFileSoapRequest*

De seguida são apresentados os campos para a operação de submissão de dados DAC9/GIR (*SendDac9GirFile*), e que compõem o elemento *SendDac9GirFileSoapRequest*.

Parâmetro	Descrição	Obrig.[3]	Tipo Dados[4]
1.1 – Início do período de reporte **(reportingPeriodStart)**	Preencher com a data de início do período de reporte a que os dados dizem respeito.	S	date
1.2– Fim do período de reporte **(reportingPeriodEnd)**	Preencher com a data de fim do período de reporte a que os dados dizem respeito.	S	date
1.3 – Tipo de ficheiro **(fileType)**	Tipo de dados a ser enviado.	S	string
1.4 – Nome do ficheiro **(filename)**	Nome do ficheiro a ser enviado.	S	string
1.5 - Ficheiro **(file)**	Conteúdo do ficheiro a ser enviado, seguindo o standard MTOM (Message Transmission Optimization Mechanism).	S	base64Binary

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

Parâmetro	Descrição	Obrig.[3]	Tipo Dados[4]
1.6 – Perfil da entidade reportante **(reportingEntityRole)**	Perfil da entidade reportante responsável pelo envio do ficheiro.	S	string
1.7 – NIF's das entidades-mãe finais **(ultimateParentEntityTins)**	Lista de NIF's das entidades-mãe finais associadas à entidade reportante.	N	UltimateParentEntityTinList

4.2 Resposta ao pedido SOAP

SOAP:Body

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

Operação SendDac9GirFile – dados do elemento *SendDac9GirFileSoapResponse*

Nesta secção são apresentados os campos que compõem o elemento *SendDac9GirFileSoapResponse*. Este campo define a resposta ao pedido de submissão de dados DAC9/GIR (*SendDac9GirFile*).

Parâmetro	Descrição	Obrig.[5]	Tipo Dados[6]
1.1 - Resultado **(result)**	Indicador do resultado da invocação desta interface. Se a resposta for *true*, a operação foi bem-sucedida. Caso contrário, significa que a operação não foi bem-sucedida. **Indicador de sucesso:** true – Ficheiro submetido com sucesso;	S	boolean
1.2 - Identificador **(identifier)**	Identificador atribuído ao ficheiro submetido em caso de submissão com sucesso.	N	string

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

Parâmetro	Descrição	Obrig.[5]	Tipo Dados[6]
1.3 - Erros que ocorreram na submissão (errors)		N	ErrorList

SOAP:Fault – dados do elemento *AutenticationException*

Nesta secção são definidos os campos de exceção à autenticação do pedido de submissão de dados DAC9/GIR.

Parâmetro	Descrição	Obrig.[7]	Tipo Dados[8]
1.1 – Lista de erros de autenticação (*AuthenticationFailed*) – campo repetitivo		S	
1.1.1 – Código de erro (*Code*)	Código do erro ocorrido aquando da submissão do ficheiro. **Códigos de resposta:** -1 – Ocorreu um erro no processamento e não foi possível concluir a operação. Por favor tente mais tarde; 0 – A operação decorreu com sucesso e o contribuinte foi autenticado corretamente; 1 – Utilizador não preenchido; 2 – Tamanho do utilizador (14) incorreto; 3 – NIF inválido; 4 – Utilizador com formato inválido; 5 – Sub-Utilizador com formato inválido; 6 – Senha não preenchida; 7 – Codificação Base64 inválida; 8 – Cifra inválida; 9 – Timestamp não preenchido; 10 – Formato do timestamp inválido; 11 – Validade da credencial expirada; 12 – Chave simétrica não preenchida; 13 – Chave simétrica repetida; 14 – Digest da senha não preenchido; 15 – O Digest não corresponde ao esperado; 16 – Dois ou mais Actors definidos por omissão. Existem dois Security Headers sem o atributo Actor definido; 17 – O Actor definido está repetido. A mensagem de erro deverá identificar qual o Actor repetido. As situações em que este erro poderá ocorrer incluem também a situação em que um Actor definido colide com o valor por omissão de um Actor não especificado; 99 – Erro na validação da senha (Senha errada, acesso suspenso, etc.).	S	int

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

Parâmetro	Descrição	Obrig.[7]	Tipo Dados[8]
1.1.2 – Mensagem de erro (*Message*)	Mensagem do erro ocorrido aquando da autenticação.	S	string
1.1.3 – Número de tentativas de autenticação disponíveis (*NumberOfTriesRemaining*)	Número de tentativas de autenticação ainda disponíveis. Este campo representa o número de vezes que o contribuinte pode tentar efetuar a autenticação. É decrementado sempre que a autenticação é falhada, levando à suspensão do acesso caso chegue a 0. Se o erro for relacionado com a estrutura e este campo não tiver sido afetado, o seu valor será -1.	S	int
1.1.4 – Ator (*Actor*)	Identificação do Actor cuja Autenticação falhou. Os valores constantes neste campo são os mesmos dos declarados no atributo /wss:Security@S:Actor.	N	string

4.3 Tipos Acessórios

UltimateParentEntityTinList

Parâmetro	Descrição	Obrig.[9]	Tipo Dados[10]
1.1 – NIF da entidade-mãe final **(ultimateParentEntityTin)**	Contém os números de identificação fiscal das entidades-mãe finais.	S	UltimateParentEntityTinType

UltimateParentEntityTinType

Parâmetro	Descrição	Obrig.[11]	Tipo Dados[12]
1.1 - NIF **(tin)**	Número de identificação fiscal da entidade-mãe final.	S	string
1.2 – País emissor **(issuerCountry)**	Código de 2 caracteres (ISO-3166 Alpha 2) que identifica o país emissor do número de identificação fiscal.	S	string

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

ErrorList

Parâmetro	Descrição	Obrig.[13]	Tipo Dados[14]
1.1 - Erro (error)	Identificação dos erros ocorridos na operação.	S	ErrorType

ErrorType

Parâmetro	Descrição	Obrig.[15]	Tipo Dados[16]
1.1 – Código de erro (code)	Código identificativo do erro ocorrido.	S	string
1.2 – Descrição (description)	Descrição do erro ocorrido.	S	string

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

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 assinatura de certificado SSL (CSR – Certificate Signing Request).

O CSR é um pequeno ficheiro de texto cifrado que contém o certificado SSL e toda a informação necessária para que a AT possa assinar digitalmente esse certificado. Posto isto, o certificado SSL assinado é devolvido para que possa ser utilizado no processo de autenticação na invocação do serviço web de apoio à submissão de dados DAC9/GIR.

Os procedimentos para geração do CSR são simples mas variam de acordo com a tecnologia 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)

Campo CSR	Descrição	Tamanho Máximo
E = An email address	O endereço de correio eletrónico para contacto, geralmente do responsável pela emissão do CSR ou do departamento de informática. Tem que ser um endereço de email válido.	80 (chars)
Key bit length	Chave pública do certificado SSL gerado pelo produtor de software tem de ser gerado com 2048 bits.	2048 (bits)

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

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

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

5.1 Gerar um certificado SSL

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

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

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

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

- **openssl req -new -subj** "**/C=**PT**/ST=**Distrito da Sede**/L=**Local da Sede**/O=**Empresa **/OU=**Departamento de Informatica**/CN=**555555555**/emailAddress=**informatica@empresa.pt" **-newkey rsa:2048 -nodes -out** 555555555.csr **-keyout** 555555555.key

Cada produtor de software deve substituir a informação específica no comando anterior pelos seus dados, uma vez que os apresentados são apenas exemplificativos e não deve alterar a informação indicada a **BOLD**.

Como resultado do 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

Adesão ao serviço:

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

6.2 Página de apoio ao contribuinte

https://info.portaldasfinancas.gov.pt/pt/apoio_ao_contribuinte/Outras_entidades/Suporte_tecnologico/Trocas_Info_Internacionais/GIR-DAC9–RIMG-Pilar-2/Paginas/default.aspx

6.3 Página de gestão de utilizadores

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

6.4 Endereços para envio de dados DAC9/GIR à AT por Webservice

Ambiente de testes

- https://servicos.portaldasfinancas.gov.pt:727/dac9gir/ws/ficheiro/enviar

Ambiente de produção

- https://servicos.portaldasfinancas.gov.pt:427/dac9gir/ws/ficheiro/enviar

7 Glossário

Tabela de acrónimos, abreviaturas e definições de conceitos utilizados neste documento, ordenados alfabeticamente por termo.

Termo	Definição
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