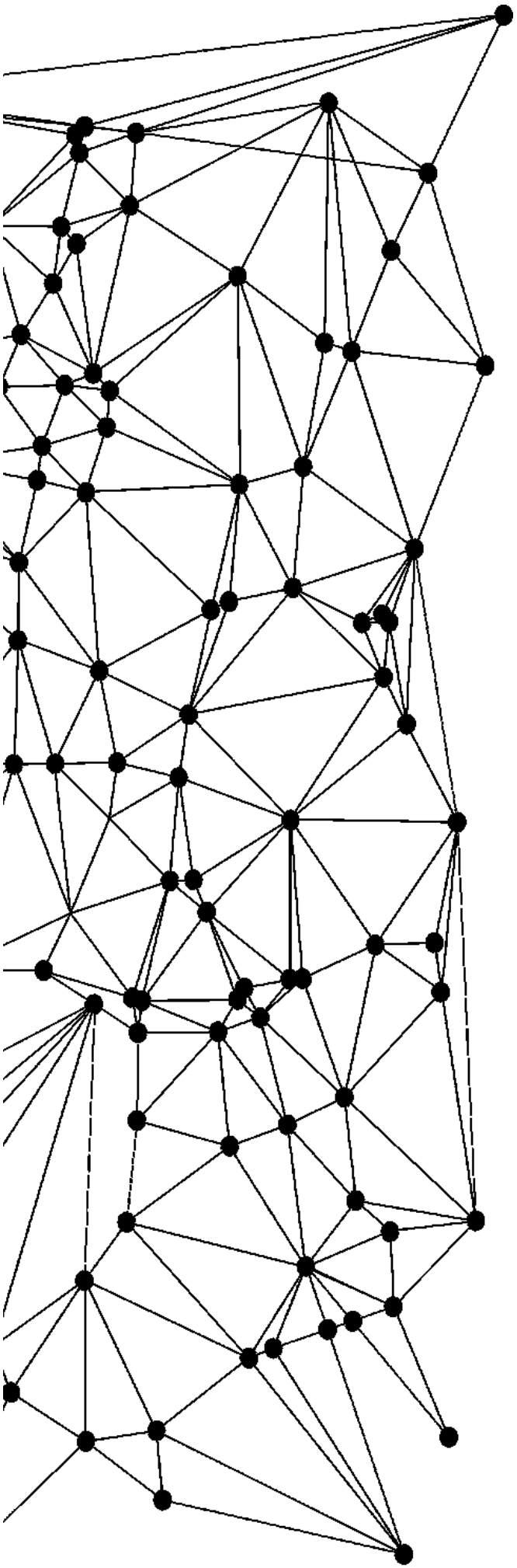

AT autoridade tributária e aduaneira

MANUAL

NR-CAU - Manual de WebServices - v1.0

Documentação Técnica

17-02-2023

Classificação	100.10.600
Segurança	Pública
Versão	1.0

CIRCUITO DE APROVAÇÃO	
Elaborado:	AT-ASA
Verificado:	AT-ASA
Aprovado:	AT-ASA
Data:	17-02-2023

HISTÓRICO DE VERSÕES

Versão Anterior	Data de Aprovação	Síntese de Alterações
1.0	17/02/2023	Versão Inicial

ÍNDICE

1. Introdução

O presente manual contém as especificações técnicas do *Web Service* de registo e consulta de Notificações de Reexportação (NR) que será disponibilizado aos Operadores Económicos (OE) no âmbito do sistema NR-CAU – Notificações de Reexportação no âmbito do Código Aduaneiro da União.
Para este canal de comunicação serão disponibilizados serviços para:

- Enviar mensagem da Notificação de Reexportação;
- Obter mensagens de resposta;
- Obter o estado de uma Notificação de Reexportação.

A comunicação entre a AT e os Operadores Económicos pressupõe a implementação de *Web Services*, devendo respeitar as seguintes regras:

1. O Operador Económico tem um utilizador credenciado na AT - caso as credenciais não sejam válidas, não conseguirá aceder ao *Web Service*;

2. Com base nas credenciais referidas no passo n.º 1, deve construir-se o pedido SOAP, descrito seguida e detalhadamente, neste documento.

2. Estrutura do envio de dados à AT (SOAP)

Neste ponto descreve-se a metodologia do *Web Service* do NR-CAU – parte integrante do SAE (Sistema Automático da Exportação).

O *Web Service* é efetuado segundo o protocolo SOAP e é constituído por duas secções:

2.1. SOAP:Header

Esta secção inclui todos os campos de autenticação do utilizador que vai ser responsável pela invocação do *Web Service*. O utilizador será um sub-utilizador do EORI do Operador Económico.

2.2. SOAP:Body

Esta secção contém os dados referentes às diferentes operações do sistema NR-CAU, os quais se detalham na secção SOAP:Body.

3. 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.

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. Todas as cadeias de caracteres (strings) aqui referidas devem ser codificadas em UTF-8.

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	Obrigatório (S/N)	Tipo de Dados
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: **<EORI>/<SUBTILIZADOR>** Exemplos: • PT555555555/1 (subtilizador n.º 1) • PT555555555/0002 (subtilizador n.º2) PT555555555/1234 (subtilizador n.º1234)	S	String
H.2 – Password	O campo **"Password"** deverá conter a senha do utilizador/subtilizador, amesma que é utilizada para entrar no Portal das Finanças. Esta password tem de ser cifrada através da chave simétrica do pedido(ver **H.3 – Nonce**) e codificado em Base64. $\boldsymbol{Password} := \boldsymbol{Base64}(\boldsymbol{C}_{\mathbf{KS}}^{\mathbf{AES,ECB,PKCS5Padding}}(\mathbf{SenhaPF}))$ **SenhaPF** := Senha do utilizador definido no campo H.1 – Username; $\boldsymbol{C}_{\mathbf{KS}}^{\mathbf{AES,ECB,PKCS5Padding}}$:=Função de cifra utilizando o algoritmo AES, ModeloECB, PKCS5Padding e a chave simétrica do pedido (K_S). **Base64** := Codificação em Base 64 do resultado.	S	String (base64)
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 *Web Service*deverá conter esta chave geradaaleatoriamente e a qual não pode serrepetida. Para garantir a confidencialidade, a chave simétrica tem de ser cifradacom a chave pública do Sistema de	S	String (base64)

Parâmetro	Descrição	Obrigatório (S/N)	Tipo de Dados
	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 própriae através do endereço de email asi-cd@at.gov.pt. O campo é construído de acordo como seguinte procedimento: $\boldsymbol{Nonce} := \boldsymbol{Base64}(\boldsymbol{C}_{\boldsymbol{RSA,Kpub_{SA}}}(\boldsymbol{K_s}))$ **K_S** := array de bytes com a chave simétrica de 128 bits, produzida de acordo com a norma AES. $\boldsymbol{C}_{\boldsymbol{RSA,Kpub_{SA}}}$:= Função de cifra da chave simétrica com o algoritmo RSA utilizando a chave pública do sistema de autenticação ($\boldsymbol{Kpub_{SA}}$). **Base64** := Codificação em Base 64 do resultado.		
H.4 – Data de sistema(Created)	O campo **"Created"** deverá conter adata e hora de sistema da aplicação que está a invocar o *Web Service*. Esta data é usada para validação temporal do pedido, pelo que é crucialque o sistema da aplicação clientetenha o seu relógio certo. Sugere-se a sincronização com o Observatório Astronómico de Lisboa: http://www.oal.ul.pt/index.php?link=ac erto 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 Exemplo: 2017-01-01T19:20:30.45Z	S	String (base64)

Parâmetro	Descrição	Obrigatório (S/N)	Tipo de Dados
	Este campo é cifrado com a chave de pedido (KS) e codificada em Base 64. $\boldsymbol{Created} := \boldsymbol{Base64}(\boldsymbol{C}_{\boldsymbol{K_S}}^{\boldsymbol{AES,ECB,PKCS5Padding}}(\boldsymbol{Time}$ **Timestamp** := data hora do sistema (UTC); $\boldsymbol{C}_{\boldsymbol{K_S}}^{\boldsymbol{AES,ECB,PKCS5Padding}}$:= Função de cifra utilizando o algoritmo AES, ModeloECB, PKCS5Padding e a chave simétrica do pedido (K_S). **Base64** := Codificação em Base 64 do resultado.		

3.1. Exemplo de SOAP:Header

Como resultado da aplicação das regras de construção anteriores será produzido um *header* de pedido SOAP tal como se apresenta no seguinte exemplo:

```
<S:Header>
    <wss:Security xmlns:wss="http://schemas.xmlsoap.org/ws/2002/12/secext">
        <wss:UsernameToken>
            <wss:Username>PT500000016/15</wss:Username>
            <wss:Password>ikCyRV+SWfvZ5c6Q0bhrBQ==</wss:Password>
            <wss:Nonce>
                fkAHne7cqurxpImCfBC8EEc2vskyUyNofWi0ptlijYg4gYCxir++unzfPVPpusloEtmLkcZjf+E6T9/76ts
                CqdupUkxOhWtkRH5IrNwmfEW1ZGFQgYTF21iyKBRzMdsJMhhHrofYYV/YhSPdT4dlgG0tk9Z73
                6jFuw061mP2TNqHcR/mQR0yW/AEOC6RPumqO8OAfc9/b4KFBSfbpY9HRzbD8bKiTo20n0Pta
                mZevCSVHht4yt/Xwgd+KV70WFzyesGVMOgFRTWZyXyXBVaBrkJS8b6PojxADLcpWRnw5+YeOs
                3cPU2o1H/YgAam1QuEHioCT2YTdRt+9p6ARNElFg==
            </wss:Nonce>
            <wss:Created>YEWoIoqIY5DOD11SeXz+0i4b/AJg1/RgNcOHOYpSxGk</wss:Created>
        </wss:UsernameToken>
    </wss:Security>
</S:Header>
```

3.2. Erro de autenticação

No caso de existirem erros de Autenticação para utilização do *Web Service* será devolvido um SOAP Fault com a estrutura do seguinte exemplo:

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
    <env:Header/>
    <env:Body>
        <env:Fault>
            <faultcode>2103</faultcode>
            <faultstring>Erro de Autenticação - Pedido do Cliente</faultstring>
            <detail>
                <transactionID>176675968</transactionID>
                <timestamp>2021-03-25 09:18:37</timestamp>
            </detail>
        </env:Fault>
    </env:Body>
</env:Envelope>
```

No entanto, o *faultcode* será específico para cada tipo de erro o que permitirá perceber se trata de um erro relacionado com a validação da Autenticação ou um erro relacionado com a validação da Autorização:

faultcode	Descrição
Erro na autenticação	
1<nnn>	Erro <nnn> na validação da Autenticação
1888	Formato do Pedido XML Incorreto: SecurityHeader vazio ou nulo
1999	Erro na invocação da Autenticação
Erro no sistema	
env:Client	Erro no pedido do cliente
env:Server	Erro na resposta do servidor

O campo *faultstring* permite distinguir se o erro tem origem no pedido do cliente ou na resposta do servidor.

faultstring	Descrição
Erro de Autenticação - Pedido do Cliente	Erro no pedido do cliente
Erro de Autenticação– Resposta do Servidor	Erro na resposta do Servidor

Sempre que seja necessário interagir com a AT no que diz respeito a uma situação de erro, o operador económico deve indicar toda a informação do *soapfault* que recebeu na invocação, em especial os campos:

- *faultcode;*
- *faultstring;*
- *transactionID;*
- *timestamp.*

4. SOAP: Body

Nesta secção serão indicadas todas as operações disponíveis para os Operadores Económicos e que deverão ser enviados na secção Body do pedido SOAP.

4.1. Serviço: Traders

Este serviço contém operações que permitem o envio de mensagens por parte dos Operadores Económicos e também a consulta de mensagens entregues e não entregues (no âmbito de Notificações de Reexportação), bem como o estado de Notificações de Reexportação.

4.1.1. Operação: *submitTradersMessageRequest*

Esta operação permite o envio de uma mensagem. O retorno da invocação desta operação não está relacionado com o processamento do conteúdo das mensagens que será efetuado num momento posterior.

Input

Parâmetro	Descrição	Min/Max	Tipo	Observações
sender	Eori do Operador Económico emissor da mensagem.	1..1	String	Pode, opcionalmente, ser concatenado no final o caracter "/" mais o utilizador orgânico (por ex: PT123456789/1). As mensagens de resposta e de notificação resultantes serão geradas contendo o receiver igual ao sender.
message	Mensagem que o Operador pretende enviar para o NR-CAU.	1..1	String	Esta mensagem deverá estar codificada em UTF8 e no formato base64.

Nota: Obrigatoriedade de preencher todos os critérios.

Exemplo de SOAP:Body - Request

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:trad="http://dssnrcau.at.gov.pt/WS/Traders">
  <soap:Header/>
  <soap:Body>
    <trad:submitTradersMessageRequest>
      <trad:sender>PT500077568</trad:sender>
    <trad:message>PHRyYWQ6UFQ1NzBDIHhtbG5zOnRyYWQ9Imh0dHA6Ly9kc3NucmNhdS5hdC5nb3YucHQvV1MvVHJhZG</trad:message>
    </trad:submitTradersMessageRequest>
  </soap:Body>
</soap:Envelope>
```

Output

Parâmetro	Descrição	Min/Max	Tipo	Observações
return	Resultado da receção da mensagem enviada.	1..1	String	

Exemplo de SOAP: Body – Response

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header/>
  <env:Body>
    <ns2:submitTradersMessageResponse xmlns:ns2="http://dssnrcau.at.gov.pt/WS/Traders">
      <ns2:return>0</ns2:return>
    </ns2:submitTradersMessageResponse>
  </env:Body>
</env:Envelope>
```

4.1.2. Operação: retrieveNewOutputMessagesIdsRequest

Esta operação retorna o ID da mensagem nova que o sistema NR-CAU gerou para o Operador Económico. Esse ID será passado na invocação da próxima operação *retrieveOutputMessagesByIdsRequest*.

Esta invocação não produz qualquer alteração de estado no sistema NR-CAU e deve ser invocada periodicamente (por ex: de 1 em 1 minuto) para que os Operadores tenham conhecimento de que têm novas mensagens para vir buscar ao sistema NR-CAU.

É da responsabilidade dos Operadores guardar o ID recebido no retorno desta invocação antes de efetuar a próxima operação *retrieveOutputMessagesByIdsRequest*, para que eventuais problemas de comunicações não resultem em perda de dados entre os sistemas.

Input

Parâmetro	Descrição	Min/Max	Tipo	Observações
receiver	Eori do Operador Económico recetor da mensagem.	1..1	String	Pode, opcionalmente, ser concatenado no final o caracter "/" mais o utilizador orgânico (por ex: PT123456789/1).

Exemplo de SOAP:Body – Request

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:trad="http://dssnrcau.at.gov.pt/WS/Traders">
  <soap:Header/>
  <soap:Body>
    <trad:retrieveNewOutputMessagesIdsRequest>
      <trad:receiver>PT500077568</trad:receiver>
    </trad:retrieveNewOutputMessagesIdsRequest>
  </soap:Body>
</soap:Envelope>
```

Output

Parâmetro	Descrição	Min/Max	Tipo	Observações
return	IDs das mensagens novas que estão disponíveis para serem obtidas.	0..1	**Lista**	Caso tenha sido indicado o utilizador orgânico no parâmetro receiver, só será retornado o ID destinado a esse utilizador orgânico. Caso tenha sido indicado só o EORI coletivo, será retornado o ID destinado a esse EORI (incluindo todos os utilizadores orgânicos).

Exemplo de SOAP: Body – Response

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header/>
  <env:Body>
    <ns2:retrieveNewOutputMessagesIdsResponse xmlns:ns2="http://dssnrcau.at.gov.pt/WS/Traders">
      <return>PT571C300123NR01</return>
      <return> PT571C300123NR02</return>
      <return> PT571C300123NR03</return>
      <return> PT571C300123NR04</return>
      <return> PT571C300123NR05</return>
      <return> PT571C300123NR06</return>
      <return> PT525C300123NR01</return>
```

```
      <return> PT525C300123NR02</return>
      <return> PT525C300123NR03</return>
      <return> PT525C300123NR04</return>
    </ns2:retrieveNewOutputMessagesIdsResponse >
  </env:Body>
</env:Envelope>
```

4.1.3. Operação: *retrieveOutputMessageByIdRequest*

Este método é responsável por devolver ao Operador a mensagem de saída identificada pelo ID indicado e marcar a mesma como já enviada (para deixar de constar no retorno do método *retrieveNewOutputMessagesIds*).

Caso haja problemas de comunicações no retorno das mensagens entre o sistema NR-CAU e os Operadores e as mesmas não cheguem ao destino, os referidos IDs já poderão ter sido marcados como enviados. De qualquer das formas, este método retornará sempre as mensagens com os IDs indicados, pelo que poderá ser invocado mais do que uma vez.

É da responsabilidade do Operador manter o ID retornado na invocação do método *retrieveNewOutputMessagesIdsRequest* e só o descartar quando realmente consegue receber com sucesso a respetiva mensagem XML.

Input

Parâmetro	Descrição	Min/Max	Tipo	Observações
receiver	Eori do Operador Económico que pretende obter as mensagens XML com os IDs indicados.	1..1	String	Pode, opcionalmente, ser concatenado no final o caracter "/" mais o utilizador orgânico (por ex: PT123456789/1).
outputMessagesId	ID da mensagem de saída que o Operador pretende obter.	1..1	String	

Nota: Obrigatoriedade de preencher todos os critérios.

Exemplo de SOAP:Body – Request

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:trad="http://dssnrcau.at.gov.pt/WS/Traders">
  <soap:Header/>
  <soap:Body>
    <trad:retrieveOutputMessageByIdRequest>
      <trad:receiver>PT500077568</trad:receiver>
      <trad:outputMessageId>PT571C300123NR01</trad:outputMessageId>
    </trad:retrieveOutputMessageByIdRequest>
  </soap:Body>
</soap:Envelope>
```

Output

Parâmetro	Descrição	Min/Max	Tipo	Observações
return	A mensagem XML de saída cujo ID foI indicado no input.	0..1	String	Resultado do processamento da mensagem. Esta mensagem encontra-se codificada em base64.

Exemplo de SOAP: Body – Response

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header/>
  <env:Body>
    <ns2:retrieveOutputMessagesByIdsResponse xmlns:ns2="http://dssnrcau.at.gov.pt/WS/Traders">
      <return>UEQ5NGJXd2dkbVZ5YzJsdmJqMGlNUzR3SWlCbGJtTnZaR2x1WnowaVZWUkdMVGdpSUhOMFlXNWtZV3h2Ym1VOU </return>
    </ns2:retrieveOutputMessagesByIdsResponse>
  </env:Body>
</env:Envelope>
```

4.1.4. Operação: *getDeclarationStateRequest*

Esta operação permite obter o estado da Notificação de Reexportação tendo por base os critérios de pesquisa dos parâmetros.

Input

Parâmetro	Descrição	Min/Max	Tipo	Observações
requester	Eori do declarante/representante que submeteu a declaração e pretende saber o seu estado.	1	String	Pode, opcionalmente, ser concatenado no final o caracter "/" mais o utilizador orgânico (por ex: PT123456789/1).
MRN	Número de referência principal da declaração (MRN).	1..1	String	

Nota: Obrigatoriedade de preencher ambos os critérios parametrizados.

Exemplo de SOAP:Body - Request

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:trad="http://dssnrcau.at.gov.pt/WS/Traders">
  <soap:Header/>
  <soap:Body>
    <trad:getDeclarationStateRequest >
      <trad:declarant>PT500077568</trad:declarant>
      <trad:MRN>21PT000000000001D9</trad:MRN>
    </trad: getDeclarationStateRequest >
  </soap:Body>
</soap:Envelope>
```

Output

Parâmetro	Descrição	Min/Max	Tipo	Observações
request	**Pedido de estado**	**1..1**	**Objecto**	**Contém o estado da declaração e o MRN associado que foi enviado no pedido.**
state	Estado atual da declaração.	1..1	String	
MRN	Número de referência principal (MRN) enviado no pedido.	1..1	String	

Exemplo de SOAP: Body - Response

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header/>
  <env:Body>
    <ns2:getDeclarationStateResponse xmlns:ns2="http://dssnrcau.at.gov.pt/WS/Traders">
      <ns2:declaration>
        <ns2:state>NR Registada</ns2:state>
        <ns2:MRN>21PT000000000001C9</ns2:MRN>
      </ns2:declaration>
    </ns2:getDeclarationStateResponse>
  </env:Body>
</env:Envelope>
```

5. Códigos de resultado

A cada invocação, o sistema poderá responder com as mensagens abaixo descritas:

Código	Descrição
Códigos de Resultado Genéricos	
0	Pedido processado com sucesso.
1	Mensagem inválida. Tipo de mensagem não reconhecido.
2	Preenchimento de campos obrigatórios em falta.
900	Ocorreu um erro interno. Por favor, envie o identificador do erro via sistema e-Balcão da AT (https://sitfiscal.portaldasfinancas.gov.pt/ebalcao/home)

6. 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 da entidade aderente, sendo a respetiva chave pública comunicada e assinada pela AT.

O certificado a ser utilizado na operação é assinado pela AT, a pedido da entidade aderente.

Para este efeito, a entidade aderente deve efetuar um pedido de certificado (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 assinado digitalmente, para que possa ser utilizado no processo de autenticação na invocação do serviço web.

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 não pode ultrapassar os tamanhos máximos, conforme a

descrição seguinte:

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 tem de ser gerada 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 e remete em resposta ao pedido o certificado assinado para integração na chave privada da entidade aderente.

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

6.1. 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 da entidade aderente, 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*. A AT utiliza a ferramenta *OpenSSL*, que é a ferramenta *Opensource* de referência, livre de custos de utilização.

Para gerar um certificado SSL, cada entidade aderente deve fazê-lo no seu próprio computador, utilizandoo 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 entidade aderente 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.

6.2. 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 entidade aderente deve substituir os parâmetros que não estão a **Bold** pelos nomes dos ficheiros corretos.

6.3. Integrar certificado com 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 entidade aderente 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 entidade aderente deve definir na execução do comando.

7. Endereços úteis

7.1. Página de produtor de software

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

7.2. Gestão de subtilizadores no Portal das Finanças

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

7.3. WSDL do envio de dados à AT por *web service*

O WSDL do *web service* está disponível em:

https://info-aduaneiro.portaldasfinancas.gov.pt/pt/informacao_aduaneira/Sistema_exportacao_e_saida/Sistema_Automatico_Exportacao/Paginas/default.aspx

7.4. Endereços para envio de dados à AT por *web service*

Ambiente de testes

A disponibilizar.

Ambiente de produção

A disponibilizar.