Declarações Electrónicas
DGAIEC

Web Services - Manual de Utilização

Versão 1.8

DECLARAÇÕES ELECTRÓNICAS DGAIEC

Web Services - Manual de Utilização

Título:	Declarações Electrónicas (DGAIEC) - Web Services - Manual de Utilização
Versão:	Versão 1.8
Data Criação:	2010-10-08 17:02
Data Revisão:	2011-03-31 12:51
Nome Ficheiro:	Portal DGAIEC - Webservices.doc
Tipo de Documento	Final

Versão	Data	Descrição	Capítulo
1.0	2010-05-19	Primeira versão do documento	-
1.1	2010-06-25	Inclusão da possibilidade de autenticação com identificadores EORI	3.2.2.2
1.2	2010-09-09	Actualização dos endereços de submissão	4
1.3	2010-10-13	Inclusão de secção sobre a obtenção do certificado das Declarações Electrónicas	2.1
1.4	2010-10-22	Actualização dos requisitos de segurança	3.2
1.5	2010-12-09	Actualização do formato da chave pública a enviar Instruções para exportar a chave pública de um certificado	2.2; 8
1.6	2010-12-28	Actualização dos endereços de Produção para o ICS e SDS	4.1; 4.2
1.7	2010-02-28	Criação do Capítulo com a secção de Testes	9
1.8	2011-03-16	Actualização dos endereços de submissão	4

Índice

1. Introdução

O presente documento visa descrever os procedimentos e requisitos necessários à utilização dos Web Services disponibilizados pelo sítio das Declarações Electrónicas (DGAIEC) [1] .

Este documento destina-se a empresas que pretendam desenvolver soluções que possibilitem, aos Utilizadores das Declarações Electrónicas, efectuar certas operações através dos Web Services já disponibilizados.

O Certificado Digital do fornecedor do Software assegura que a mensagem foi enviada através do software desse produtor, que é responsável por transmitir correctamente os dados dos Operadores (seus clientes). O Certificado a utilizar é o mesmo nos ambientes de Testes e Produção.

O Operador Económico é responsável pelo envio e conteúdo da mensagem, uma vez que utiliza as suas credenciais no Portal DGAIEC (Username e Password) que por sua vez são utilizadas pela Administração Aduaneira, para assegurar a não repudiação dos dados transmitidos. Estas credenciais só devem ser conhecidas pelo Operadior e devem ser diferentes nos ambientes de Testes e Produção.

2. Pré-requisitos para utilização do serviço

2.1. Certificado Servidor

O certificado SSL das Declarações Electrónicas pode ser obtido no seguinte endereço: https://www.e-financas.gov.pt/dgaiec/

2.2. Certificado Cliente

A utilização do serviço descrito neste documento pressupõe o envio prévio, para DGITA (ver 7. Contactos) de:

- Chave pública do certificado da Empresa e respectiva cadeia de certificação

  (a chave pública deve ser enviada para validação no formato: Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) - with the option: Include all certificates in the certification path if possible)

A chave pública deve ser enviada por email num ficheiro em formato .Zip.

O certificado a utilizar deve ter as seguintes propriedades (Key Usage):

- Digital Signature;
- Non Repudiation;
- Key Encipherment;
- Data Encipherment

A aplicação cliente deve ter acesso à chave privada do certificado.

2.3. Ambiente de testes

O ambiente de testes deve ser utilizado para validação do formato do pedido e dos dados submetidos.

Para obter acesso a este ambiente, devem ser solicitados NIF/Senhas válidos ou Números EORI/Senhas válidos no ambiente de testes para os casos que se pretendem testar.

3. Requisitos técnicos

3.1. Conexão ao sítio das Declarações Electrónicas

Os pedidos efectuados, via Web Service, ao sítio das Declarações Electrónicas devem respeitar os seguintes requisitos no que se refere à respectiva conexão:

- Método: **POST**
- Protocolo: **HTTPS**

3.2. Segurança

3.2.1. Autenticação da aplicação cliente

Conforme referido anteriormente, os pedidos devem ser efectuados via protocolo HTTPS, o que pressupõe a utilização de um certificado digital na autenticação da aplicação cliente perante o servidor.

3.2.2. Especificação de segurança dos Web Services

Os Web Services descritos neste documento foram implementados de acordo com o formato SOAP e seguem o standard **WS-Security 1.1** da **OASIS** [2], no que se refere à especificação de segurança para Web Services SOAP.

Na tabela que se segue, encontra-se definido quais os requisitos de segurança esperados na invocação de cada web service:

Identificação	Requisitos de segurança
Web Services do Sistema SDS e SDS Via Aérea	• Autenticação do utilizador
Web Services do Sistema ICS	• Autenticação do utilizador
Web Services do Sistema SIC-EU	• Autenticação do utilizador • Integridade e autenticidade da mensagem SOAP

	(assinatura digital)
Web Services do Sistema ECS	• Autenticação do utilizador • Integridade e autenticidade da mensagem SOAP (assinatura digital)

3.2.2.1. Integridade e autenticidade da mensagem SOAP

De modo a garantir a integridade e autenticidade das mensagens SOAP, os pedidos efectuados aos Web Services que apresentem esse requisito devem cumprir as seguintes especificações técnicas:

- Assinatura digital das mensagens SOAP: as mensagens enviadas devem incluir um *Security header* contendo uma assinatura digital gerada com base na chave privada do certificado cliente. Esta assinatura será validada no servidor através da chave pública do mesmo certificado.

  Exemplo de um SOAP Header contendo um *security header* com um elemento *Signature*:

```
<soapenv:Header>
  <wsse:Security xmlns:wsse="...">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="..."/>
          <ds:SignatureMethod Algorithm="..."/>
            <ds:Reference URI="...">
              <ds:Transforms>
                <ds:Transform Algorithm="..."/>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="..."/>
                <ds:DigestValue>
                  digestValue
                </ds:DigestValue>
            </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>
        signatureValue
      </ds:SignatureValue>
      <ds:KeyInfo Id="...">
        <wsse:SecurityTokenReference wsu:Id="..." xmlns:wsu="...">
          <ds:X509Data>
            <ds:X509IssuerSerial>
              <ds:X509IssuerName>
                certificateIssuerName
              </ds:X509IssuerName>
              <ds:X509SerialNumber>
                certificateSerialNumber
              </ds:X509SerialNumber>
            </ds:X509IssuerSerial>
          </ds:X509Data>
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>
    </ds:Signature>
  </wsse:Security>
</soapenv:Header>
```

- A assinatura digital deve ser criada de acordo com as seguintes indicações:
  - Elemento a assinar*:*

    SOAP Body

  - Algoritmo utilizado na canonicalização da mensagem (*Canonicalization Method*) :

    http://www.w3.org/2001/10/xml-exc-c14n#

  - Algoritmo utilizado na assinatura da mensagem (*Signature Method*):

    http://www.w3.org/2000/09/xmldsig#rsa-sha1

  - Tipo de identificação de chave (*Key Identifier Type*) utilizado:

X509IssuerSerial (certificate issuer name and serial number)

3.2.2.2. Autenticação do utilizador

Os utilizadores responsáveis pelos pedidos efectuados aos Web Services descritos neste documento devem ser autenticados perante o sítio das Declarações Electrónicas, pressupondo-se a utilização de credenciais válidas para esse efeito. Nesse sentido, todos os pedidos efectuados devem cumprir as seguintes especificações técnicas:

- As mensagens SOAP devem incluir um *Security header* contendo um *UsernameToken* constituído por *Username* e *Password* (coincidentes com as credenciais de acesso ao sítio das Declarações Electrónicas).

  Exemplo de um *SOAP Header* contendo um *security header* com *UsernameToken*:

```
<soapenv:Header>
  <wsse:Security>
    <wsse:UsernameToken wsu:Id="...">
      <wsse:Username>NIF ou identificador EORI</wsse:Username>
      <wsse:Password Type="...">Senha de acesso</wsse:Password>
    </wsse:UsernameToken>
  </wsse:Security>
</soapenv:Header>
```

- O tipo de password, especificado no atributo *Type* do elemento *Password*, deve ser:
  - **http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText**

- O conteúdo de *Username* pode ser:
  - Um NIF válido com acesso ao Portal DGAIEC:

    Exemplo: 123456789
  - Um NIF de um sub-utilizador válido com acesso ao Portal DGAIEC:

    Exemplo: 123456789/2 (sub-utilizador 2 do NIF: 123456789)
  - Um identificador EORI válido e com acesso prévio ao Portal DGAIEC:

    Exemplo: ES12345676.

- O conteúdo de *Password* deverá ser a senha respectiva do utilizador identificado em: *Username*.

4. Endereços de submissão

4.1. Web Services do Sistema SDS

Ambiente	Endereço
Qualidade/ Testes	https://www.e-financas.gov.pt:700/jsp-dgaiec/externalWebservice.jsp?external=sdsqualidadews
Produção	https://www.e-financas.gov.pt:400/jsp-dgaiec/externalWebservice.jsp?external=sdsws

4.2. Web Services do Sistema SDS Via Aérea

Environment	Address
Quality / Test	https://www.e-financas.gov.pt:700/jsp-dgaiec/externalWebservice.jsp?external=sdsdepqualidadews

4.3. Web Services do Sistema ICS

Ambiente	Endereço
Qualidade/ Testes	https://www.e-financas.gov.pt:700/jsp-dgaiec/externalWebservice.jsp?external=icsqualidadews
Produção	https://www.e-financas.gov.pt:400/jsp-dgaiec/externalWebservice.jsp?external=icsws

4.4. Web Services do Sistema SIC-EU

Ambiente	Endereço
Qualidade/ Testes	https://www.e-financas.gov.pt:700/jsp-dgaiec/externalWebservice.jsp?external=siceuws
Produção	https://www.e-financas.gov.pt:400/jsp-dgaiec/externalWebservice.jsp?external=siceuws

4.5. Webservices do Sistema ECS

Ambiente	Endereço
Qualidade/ Testes	https://www.e-financas.gov.pt:700/jsp-dgaiec/externalWebservice.jsp?external=ecsqualidadews
Produção	https://www.e-financas.gov.pt:400/jsp-dgaiec/externalWebservice.jsp?external=ecsws

4.6. Definição do WSDL dos Webservices

O WSDL de cada webservice deverá ser solicitado através do contacto definido em: 7 Contactos.

5. Referências

[1] Sítio das Declarações Electrónicas (DGAIEC):
http://www.e-financas.gov.pt/de/jsp-dgaiec/main.jsp

[2] OASIS
http://www.oasis-open.org

6. Definições, Acrónimos e Abreviaturas

DGAIEC	Direcção-Geral das Alfândegas e dos Impostos Especiais sobre o Consumo
Aplicação cliente	Aplicação desenvolvida e utilizada para aceder ao Web Service
Web Service	Serviço disponibilizado através de uma rede (Internet, Intranet ou outras) usado para a troca de dados entre aplicações e sistemas.
OASIS	Organization for the Advancement of Structured Information Standards
SOAP	Simple Object Access Protocol

7. Contactos

Telefone: 213820603

Email: SI - ASA - Área de Sistemas Aduaneiros (si-asa@dgita.min-financas.pt)

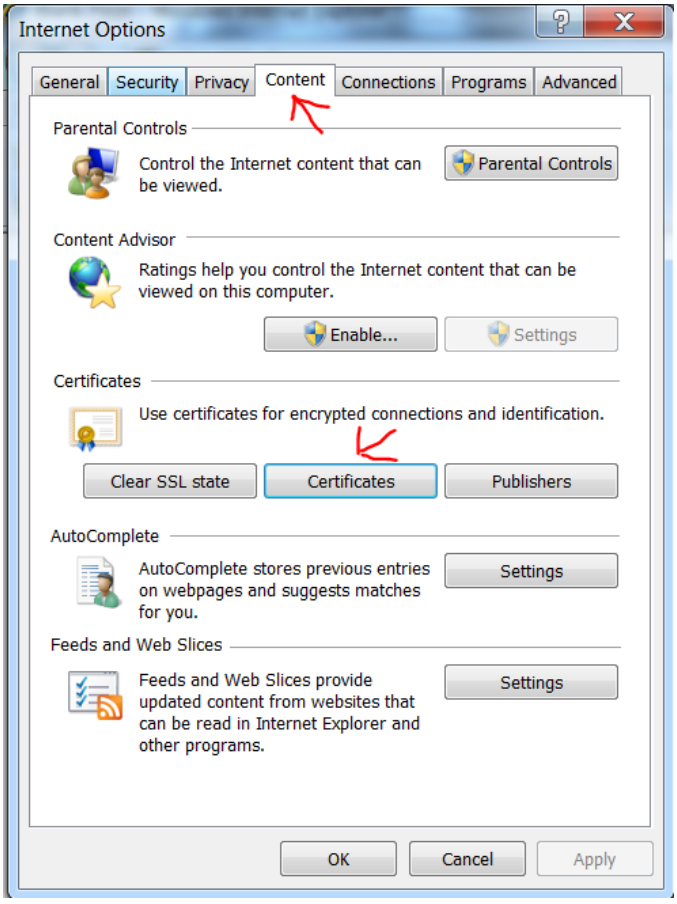
8. Como exportar a chave pública do certificado

Descrevem-se as instruções para obter a chave pública de um certificado instalado numa máquina Windows.

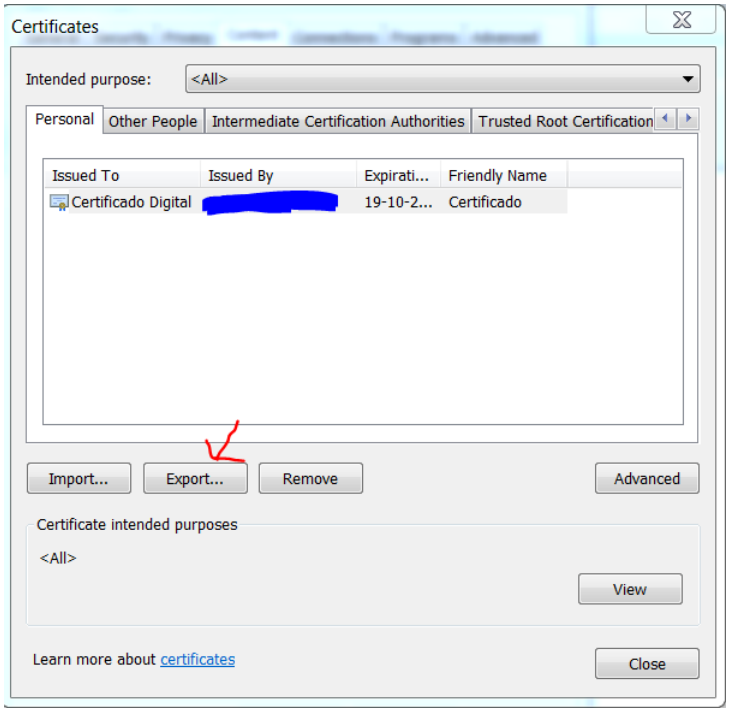
Assume-se que o certificado foi previamente importado no Sistema Operativo Windows e que está a ser utilizado o browser Internet Explorer 8, noutro sistema operativo ou browser, devem ser utilizadas as instruções em conformidade.

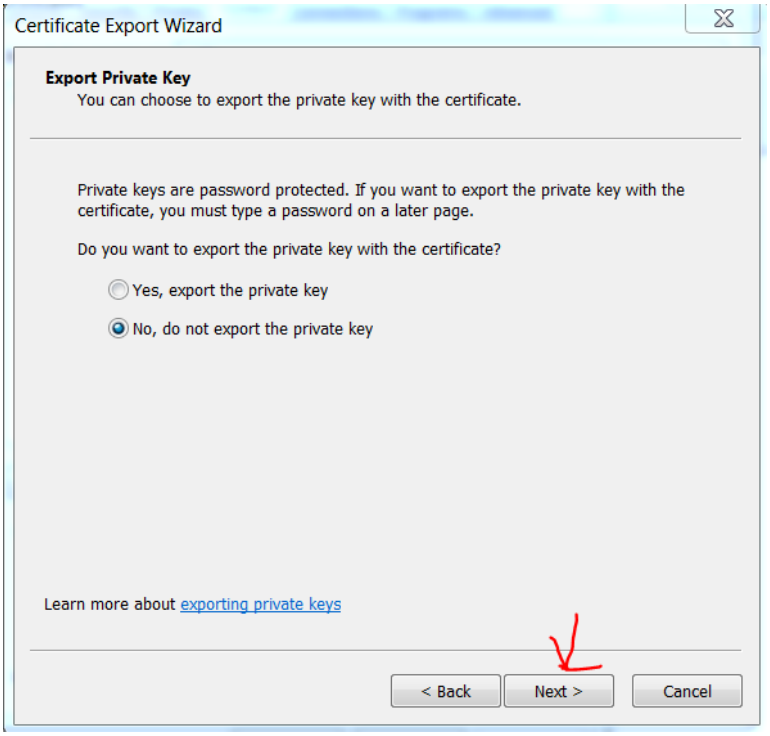
8.1. Localização do Certificado

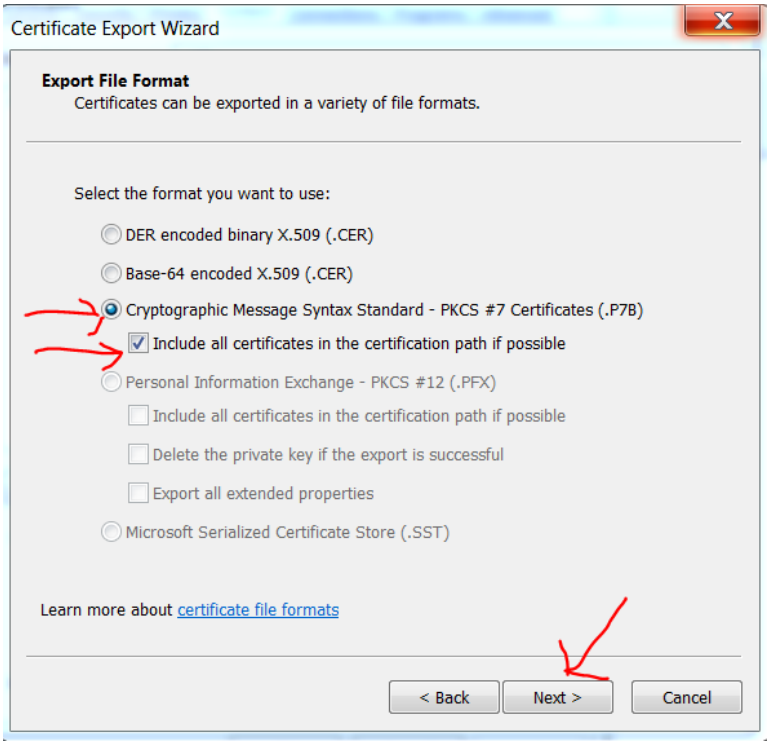
O certificado pode ser acedido no Browser: Internet Explorer em: Ferramentas -> Opções de Internet -> Conteúdo -> Certificados

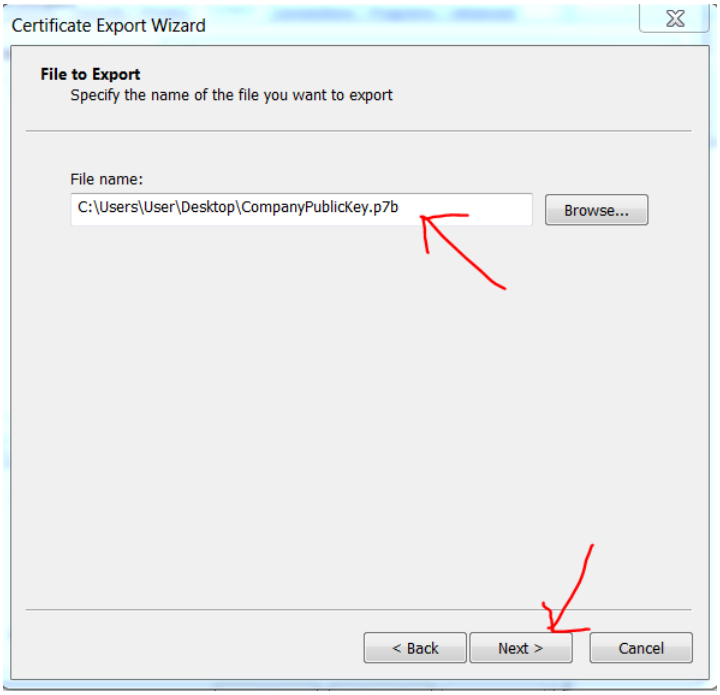


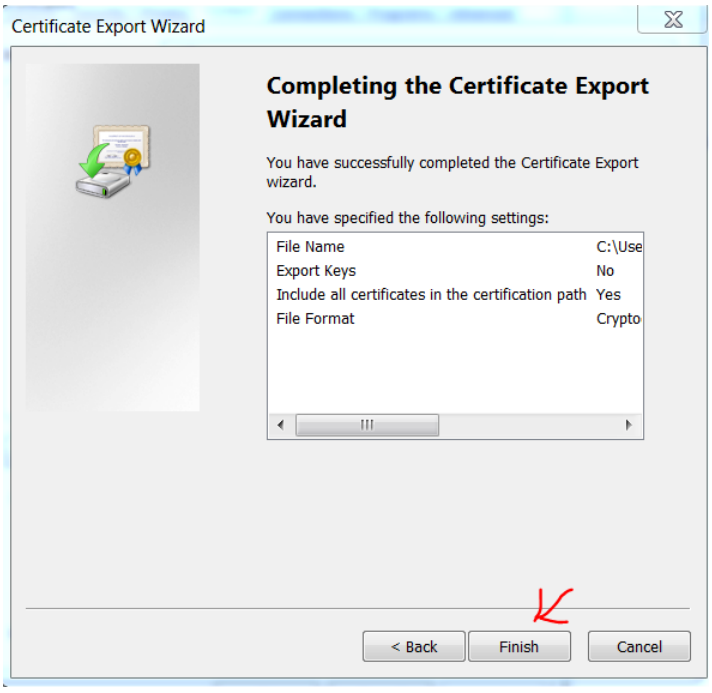
8.2. Exportar a Chave Pública




Certificate Export Wizard
Export Private Key
You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
Yes, export the private key
No, do not export the private key
Learn more about exporting private keys
< Back
Next >
Cancel

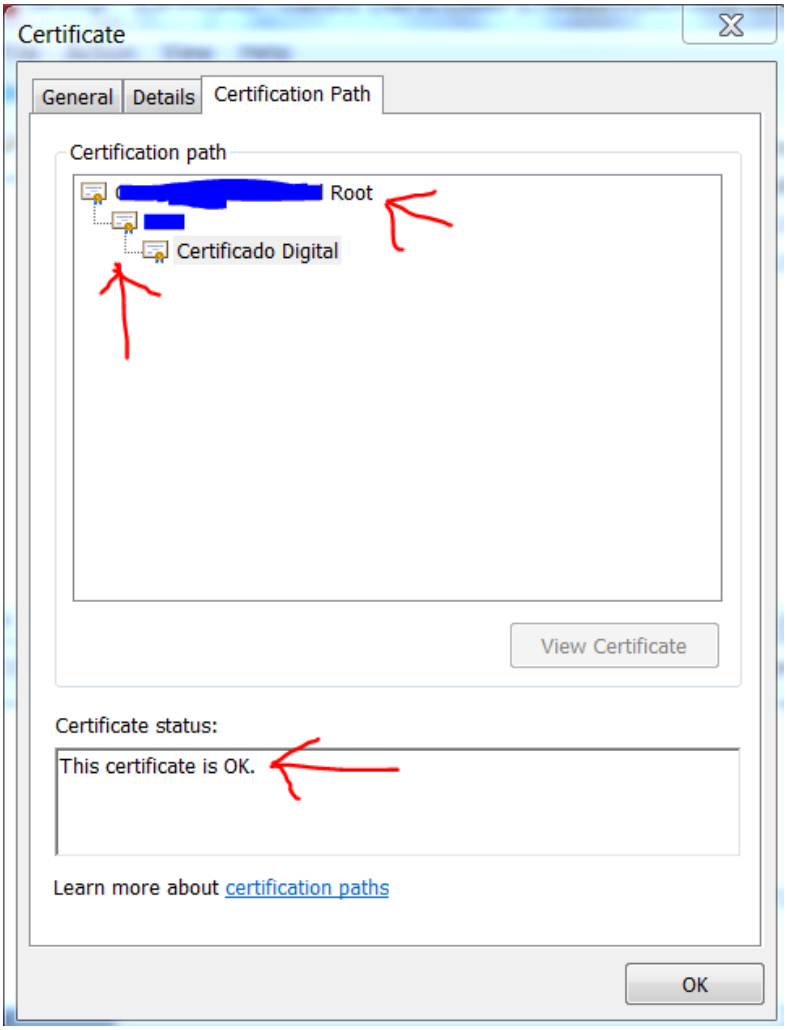

Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Delete the private key if the export is successful
Export all extended properties
Microsoft Serialized Certificate Store (.SST)
Learn more about certificate file formats
< Back
Next >
Cancel


Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
C:\Users\User\Desktop\CompanyPublicKey.p7b
Browse...
< Back
Next >
Cancel


Certificate Export Wizard
Completing the Certificate Export Wizard
You have successfully completed the Certificate Export wizard.
You have specified the following settings:
File Name C:\Use
Export Keys No
Include all certificates in the certification path Yes
File Format Crypto
< Back
Finish
Cancel

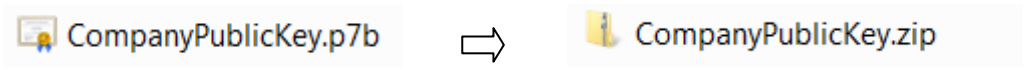
8.3. Verificar a Chave Pública

A chave pública deve conter uma cadeia de certificação válida, assinada por uma Root CA pública e reconhecida.



8.4. Enviar a Chave Pública

O ficheiro produzido em 8.2 deve ser "zipado" e enviado por email para validação.



9. Como testar Webservices com o SOAP-UI

Para testar os Webservices, sevem ser cumpridos os pré-requisitos definidos em: 3 `Requisitos técnicos`. Nomeadamente, deve ser produzido um pedido SOAP válido que deve ser enviado através do protocolo HTTPS , por um software cliente com um certificado cliente pré-validado e utilizando as credenciais válidas user/pass do ambiente de testes.

Nota: é um erro comum, a tentative de teste do Webservice, utilizando um pedido no Browser ou uma ferramenta como o "curl". Este tipo de pedidos são simplemesmente bloqueados pela infra-estrutura e não é fornecida informação útil à aplicação cliente.

9.1. Ferramenta SOAP-UI Tool

O SOAP-UI é uma ferramenta reconhecida, opensource, para o teste de Web-services através de interfaces SOAP. Esta ferramente pode ser configurada para cumprir com os requisitos anteriomente enunciados.

O SOAP-UI é opensource e a versão gratuita pode ser obtida em: http://www.soapui.org/

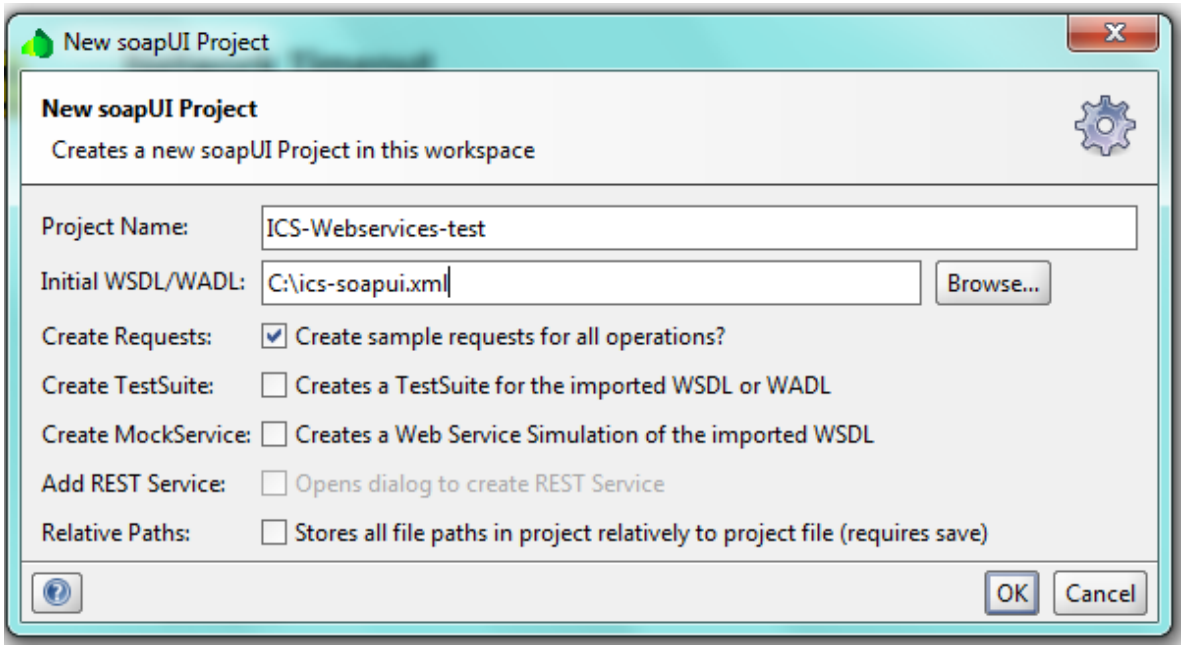
9.2. Instalação do SOAP-UI Instalação

Deverão ser seguidas as instruções de instalação da própria ferramenta.Follow the application installation instructions

9.3. Configuração do SOAP-UI

O exemplo seguinte, demonstra a configuração e chamada dos Webservices do Sistema ICS através do SOAP-UI.

1) **Create a new project**
   a) Menu File -> New soapUI Project
   b) Escolher um nome para o Projecto e o WSDL (o WSDL deve ser obtido atravé de: **Error! Reference source not found.**-`Contactos`).
   c) Assinalar a opção: Create sample requests for all operations



2) **Configurar a autenticação do Certificado Cliente**

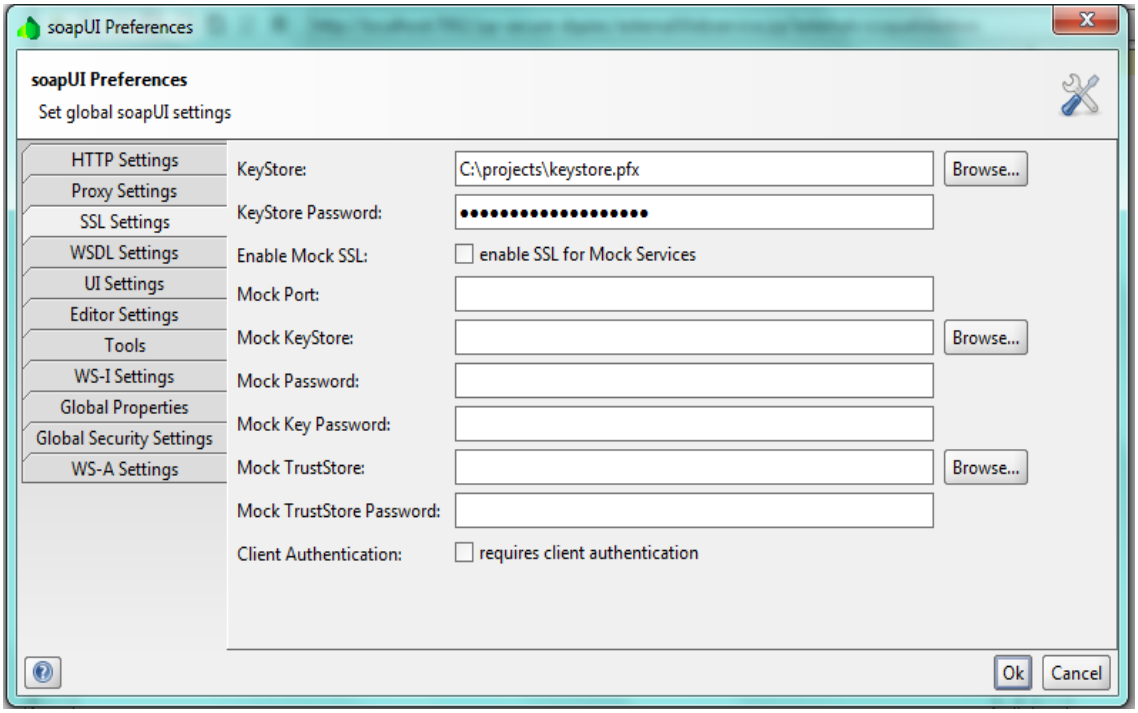
Para utilizar o certificado cliente na autenticação no Portal, deve ser selecionada a seguinte opção:

a) Menu File > Preferences > SSL Settings

b) Preencher a localização da Keystore onde está guardada a chave privada do certificado cliente.

c) Preencher a password de acesso à Keystore

d) Premir: OK



3) Configurar a autenticação do Utilizador (sem message digest)

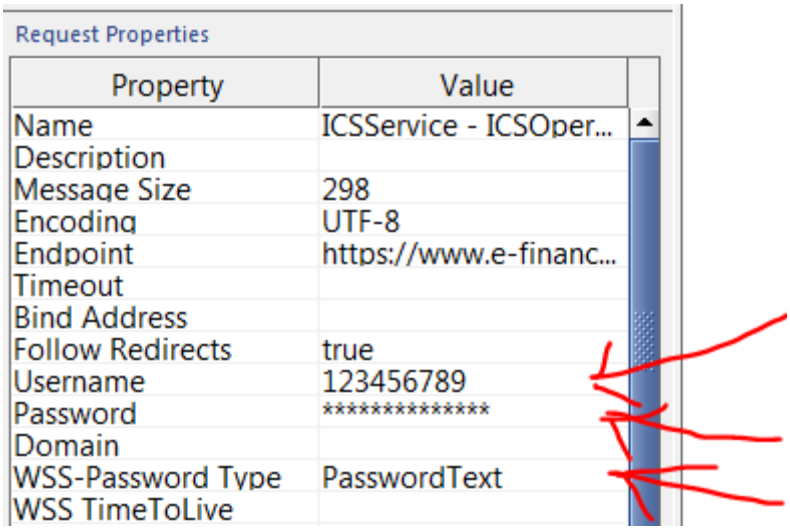
Esta configuração é uma abordagem simplista e aplica-se apenas a pedidos que não necessitem de "Message Digest"

No "Request Properties Panel", preencher as seguintes propriedades:

Username: com o Número EORI do Operador Económico (se o operador for um Operador Português, preencher o NIF -Número de Informação Fiscal) que foi registado no Portal DGAIEC.

Password: Preencher a Password que foi utilizada no processo de registo no Portal DGAIEC

WSS – Password Type: escolher "Password Text"



4) Configurar a autenticação utilizador (com message digest)

A opção: Message Digest, requer o acesso à Tab: Security Configurations –> Outgoing WS Security Configurations.

Criar uma nova Security Configuration e preencher os Tabs: Username and Signature Tabs.

Na TAB assinatura definir a Part:

Part: “Body”

Namespace: http://schemas.xmlsoap.org/soap/envelope/

Encode: Element

5) Efectuar uma operação

a) Aceder a uma operação na barra lateral esquerda e mudar o pedido para um conteúdo válido para a operação em causa.

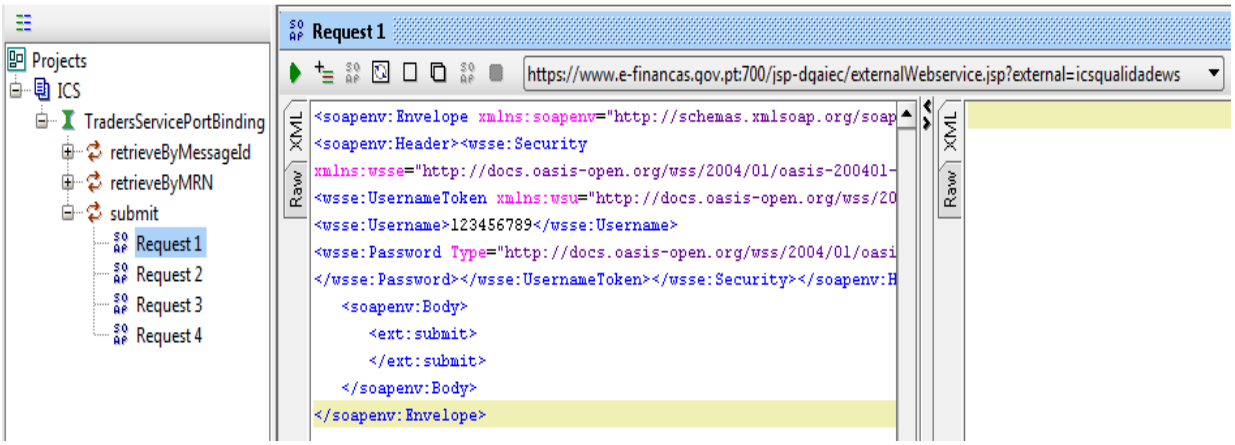
   a. O element <Body> deve ser preenchido com o XML apropriado para a operação que está a ser testada;

   b. O element <Username> deve ser preenchido automaticamente com o NIF ou Número EORI do operador económico definido anteriormente;

   c. O Elemento Password, deve ser preenchido automaticamente com a password definida anteriormente;

b) Definir o Endpoint (selecionar o endpoint descrito em: 4 `Endereços de submissão`)

c) Submeter o pedido (botão verde “play”) e verificar a resposta no quadro da direita, bem como o “error log”



9.4. Códigos de Erro e respostas comuns

9.4.1. Erros de Conexão

9.4.1.1. Error getting response; javax.net.ssl.SSLHanshakeException: Received fatal alert: handshake_failure

Este erro significa que a negociação SSL não foi completada com sucesso entre o SOAP UI e o Portal DGAIEC. Isto pode indicar que o Certificado Cliente que está a ser utilizado ainda não está registado no Portal DGAIEC.

Deve confirmar que recebeu uma configuração do registo do certificado pela Administração do Portal DGAIEC.

Verifique ainda que: está a usar a Key Store correcta e que a mesma contém o certificado cliente que espera utilizar, bem como está a preencher correctamente a chave de acesso à keystore.

9.4.1.2. ERROR:java.net.SocketTimeoutException: Read timed out

Verifique que existe conectividade HTTP entre a máquina cliente e a máquina servidor. O comando (Ex: `telnet www.e-financas.gov.pt 700`) deve retornar "`Connected to www.e-financas.gov.pt.`"

Isto pode significar também que o ambiente de testes do Portal DGAIEC está indisponível. Deve refazer o teste algumas vezes e se mesmo assim não obtiver resposta, deve contactar: 7 `Contactos`.

9.4.2. Erros de Autenticação

9.4.2.1. "No Username or Password in message!"

Significa que não foi preenchido um Username ou Password válidos referentes ao Operador Económico com que se está a efectuar o teste.

9.4.3. Erros Sintacticos

9.4.3.1. "Internal Error (from server)"

Este erro significa que provavelmente está a ser enviado um XML não concordante com o Schema do Webservice a testar.

Verifique o XML contra o schema do Webservice.

Se o erro persistir, contacte (**`Error! Reference source not found.`**-`Contactos`) e forneça: A Data/Hora do teste referente a GMO+0, o pedido completo que foi enviado e a resposta obtida.