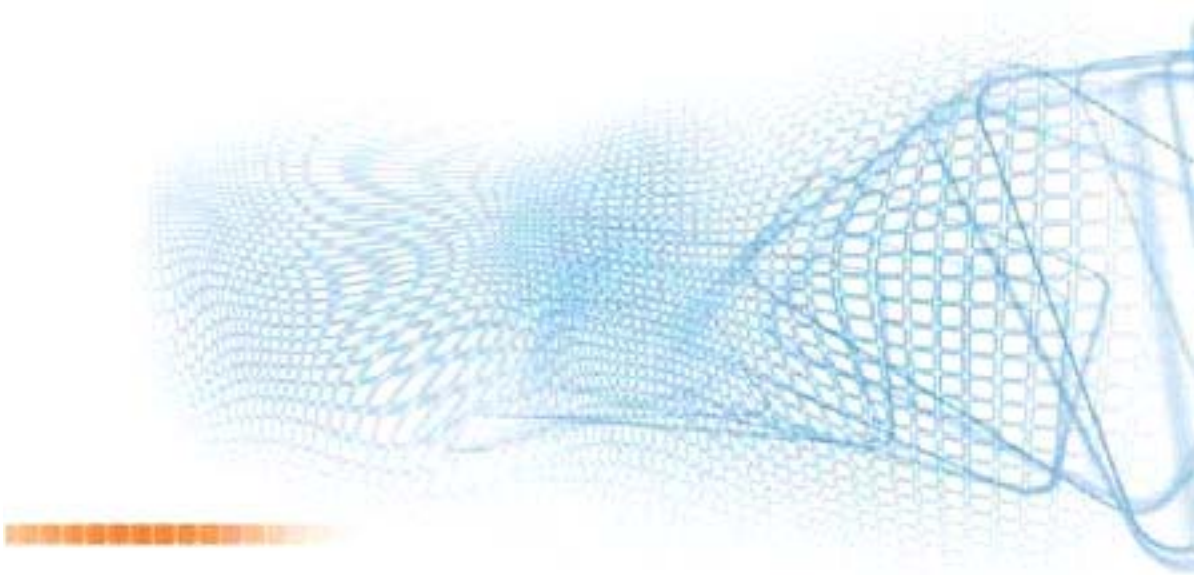
Declarações Electrónicas
DGAIEC

Web Services - Manual de Utilização

Versão 1.1



DECLARAÇÕES ELECTRÓNICAS DGAIEC

Web Services - Manual de Utilização

Opensoft – Soluções Informáticas, SA
Edifício Amoreiras Square
Rua Joshua Benoliel, 1 - 4ºC
1250 - 273 Lisboa, Portugal
Tel.: (+351) 21 380 44 10 • Fax: (+351) 21 380 44 19

Título:	Declarações Electrónicas (DGAIEC) - Web Services - Manual de Utilização
Versão:	Versão 1.1
Data Criação:	2010-05-19 9:44
Data Revisão:	2010-06-30 17:53
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

Índice

1. Introdução 5

2. Pré-requisitos para utilização do serviço 6

2.1. Certificado Cliente 6
2.2. Ambiente de testes 6

3. Requisitos técnicos 7

3.1. Conexão ao sítio das Declarações Electrónicas 7
3.2. Segurança 7
3.2.1. Autenticação da aplicação cliente 7
3.2.2. Autenticação do utilizador 7

4. Endereços de submissão 9

4.1. Web Services do Sistema ICS 9

5. Referências 10

6. Definições, Acrónimos e Abreviaturas 11

7. Contactos 12

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.

2. Pré-requisitos para utilização do serviço

2.1. 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 (formato: Base64 encoded X.509, extensão: .CER)

A chave pública deve ser enviada por email 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 da Empresa.

2.2. 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 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. Autenticação do utilizador

Os utilizadores responsáveis pelos pedidos efectuados devem ser autenticados perante o sítio das Declarações Electrónicas, pressupondo-se a utilização de credenciais válidas para esse efeito.

Nesse sentido, os Web Services descritos neste documento foram implementados de acordo com o formato SOAP e seguem a especificação da OASIS [2] no que se refere aos requisitos de segurança dos Web Services SOAP.

Concretamente, todos os pedidos efectuados devem cumprir os seguintes requisitos técnicos:

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

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

```
<soapenv:Header>
      <wsse:Security>
            <wsse:UsernameToken wsu:Id="UsernameToken-1">
                  <wsse:Username>nif ou identificador
            EORI</wsse:Username>
                  <wsse:Password Type=" http://docs.oasis-
            open.org/wss/2004/01/oasis-200401-wss-username-token-
            profile-1.0#PasswordText">senha</wsse:Password>
            </wsse:UsernameToken>
      </wsse:Security>
</soapenv:Header>
```

- O conteúdo de *Username* pode ser:
    - Um NIF válido com acesso ao Portal DGAIEC, Ex: 123456789
    - Um Nif de um sub-utilizador válido com acesso ao Portal DGAIEC, Ex: 123456789/2 (sub-utilizador 2 do NIF: 123456789).
    - Um identificador EORI válido e com acesso prévio ao Portal DGAIEC, Ex: ES12345676.

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

4. Endereços de submissão

4.1. Web Services do Sistema ICS

Ambiente	Endereço
Testes	https://www.e-financas.gov.pt:700/testes-dgaiec/services/de/jsp-dgaiec/externalWebservice.jsp?external=_icsdesenvolvimentows
Produção	https://www.e-financas.gov.pt:400/services/de/jsp-dgaiec/externalWebservice.jsp?external=ics

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)