



Electronic Declarations DGAIEC

Web Services - User Guide

Version 1.5

ELECTRONIC DECLARATIONS DGAIEC

Web Services - User Guide

Title: Electronic Declarations (DGAIEC) - Web Services - UserGuide
Version: Version 1.5
Date Created: 201010-08 17:04
Revision Name: 2010-12-09
File Name: Portal DGAIEC - Webservices.doc
Document Type Final

Version	Date	Comment	Chapter
1.0	2010-07-02	First Version	-
1.1	2010-06-25	Inclusion of the possibility of EORI authentication identifiers	3.2.2
1.2	2010-09-09	Submission address updates	4
1.3	2010-10-13	Included section about Electronic Declarations Server Certificate	2.1
1.4	2010-10-22	Security requirements update	3.2
1.5	2010-12-09	Updated public key format that is sent to validation	2.2
		Included Public Key export instructions	8

Index

1. Introduction.....	5
2. Prerequisites for using the service	6
2.1. Server Certificate	6
2.2. Client Certificate	6
2.3. Test Environment	6
3. Technical Requirements.....	7
3.1. Connection to Portal of Electronic Declarations	7
3.2. Security	7
3.2.1. Authentication of the client application	7
3.2.2. Web Services Security Specification	7
3.2.2.1. SOAP Message integrity and authenticity	8
3.2.2.2. User Authentication	9
4. Submissions URL's	11
4.1. SDS System Web Services.....	11
4.2. ICS System Web Services.....	11
4.3. SIC-EU System Web Services.....	11
4.4. Web Service WSDL definitions.....	12
5. References	13
6. Definitions, Acronyms and Abbreviations.....	14
7. Contacts.....	15

1. Introduction

This document describes the procedures and requirements necessary for the use of Web services provided by the DGAIEC - Electronic Declarations Portal [1] .

This document is intended for companies wishing to develop solutions which enable users to the Electronic Declarations, perform certain transactions through Web Services already available.

2. Prerequisites for using the service

2.1. Server Certificate

The SSL server certificate in use by Electronic Declarations can be reached at:
<https://www.e-financas.gov.pt/dgaiec/>

2.2. Client Certificate

The use of the service described in this document requires the prior submission to DGITA (see 7. Contacts) to:

- Company's Public Key Certificate its Certification Chain
(The certificate public key an certification chain must be sent to validation in the format: Cryptographic message Syntax Standard - PKCS #7 Certificates (.P7B) - with the option: Include all certificates in the certification path if possible)

The public key should be emailed in a Zip file.

The certificate must have the following properties (Key Usage):

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

The client application must have access to the private key of the this certificate.

2.3. Test Environment

The test environment should be used to validate the format of the application and submitted data.

To gain access to this environment, valid credentials should be requested in the form of a NIF / Password or EORI Number / Password valid in the test environment for scenarios to be tested.

3. Technical Requirements

3.1. Connection to Portal of Electronic Declarations

Requests via Web Service to the site of Electronic Declarations must meet the following requirements in regard to their connection:

- Method: **POST**
- Protocol: **HTTPS**

3.2. Security

3.2.1. Authentication of the client application

As mentioned before, applications must be made via HTTPS protocol, which requires the use of a digital certificate to authenticate the client application to the server.

3.2.2. Web Services Security Specification

Web services described in this document were implemented according to the SOAP specification and follow the WS-Security 1.1 OASIS Standard [2].

In the following table it is specified which security requirements are expected for each web service invocation:

Identificação	Requisitos de segurança
SDS System Web Services	<ul style="list-style-type: none">• User authentication
ICS System Web Services	<ul style="list-style-type: none">• User authentication
SIC-EU (EMCS) System Web Services	<ul style="list-style-type: none">• User authentication• SOAP message integrity and authenticity

3.2.2.1. SOAP Message integrity and authenticity

To ensure the integrity and authenticity of SOAP messages, requests made to Web Services that demand this requirement must meet the following technical specifications:

- Digital Signature of SOAP messages: messages sent by the client applications must include a *security header* containing a digital signature generated with the client certificate's private key. This signature will be validated on the server with the certificate's public key.

Example of a SOAP header containing a *security header* with a *signature* element:

```
<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>
```


- The digital signature must be created according with the following information:
 - SOAP element to sign:
SOAP Body
 - Canonicalization Method Algorithm:
<http://www.w3.org/2001/10/xml-exc-c14n#>
 - Signature Method Algorithm:
<http://www.w3.org/2000/09/xmldsig#rsa-sha1>
 - Key Identifier Type:
X509IssuerSerial (certificate issuer name and serial number)

3.2.2.2. User Authentication

All users responsible for submitting the requests must be authenticated on the Electronic Declarations site, assuming the use of valid credentials for this purpose. Thus, all requests must meet the following technical specifications:

- Messages must include a SOAP *security header* with *UsernameToken* containing *Username* and *Password* (matching access credentials to the Electronic Declarations website).

Example of a SOAP header containing a *security header* with *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>
```

- The type of password specified in the *Type* attribute of *Password* element, must be:
 - <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText>
- The *Username* content can be:
 - A valid NIF with access to Portal DGAIEC
Example: 123456789

- A sub-user NIF with valid Access to Portal DGAIEC,
Example: 123456789/2 (sub-user 2 of NIF: 123456789).
- A valid EORI identifier with prior access to Portal DGAIEC
Example: ES12345676.
- The password must match the password of the user identified by: *Username*.

4. Submissions URL's

4.1. SDS System Web Services

Environment	Address
Quality / Test	https://www.e-financas.gov.pt:700/jsp-dgaiec/externalWebservice.jsp?external=sdsqualidadews
Production	https://www.e-financas.gov.pt:400/jsp-dgaiec/externalWebservice.jsp?external=sds

4.2. ICS System Web Services

Environment	Endereço
Quality / Test	https://www.e-financas.gov.pt:700/jsp-dgaiec/externalWebservice.jsp?external=icsqualidadews
Production	https://www.e-financas.gov.pt:400/jsp-dgaiec/externalWebservice.jsp?external=ics

4.3. SIC-EU System Web Services

Ambiente	Endereço
Quality / Test	https://www.e-financas.gov.pt:700/jsp-dgaiec/externalWebservice.jsp?external=siceuws
Production	https://www.e-financas.gov.pt:400/jsp-dgaiec/externalWebservice.jsp?external=siceuws

4.4. Web Service WSDL definitions

To obtain a specific Web Service WSDL, please use contacts at Chapter 7 - *Contacts*.

5. References

[1] Electronic Declarations (DGAIEC):

<http://www.e-financas.gov.pt/de/jsp-dgaiec/main.jsp>

[2] OASIS

<http://www.oasis-open.org>

6. Definitions, Acronyms and Abbreviations

DGAIEC	Direcção-Geral das Alfândegas e dos Impostos Especiais sobre o Consumo
Client Application	Application developed and used to access Web Service
Web Service	Web Service available through a network (Internet, Intranet or other) used for exchanging data between applications and systems.
OASIS	Organization for the Advancement of Structured Information Standards
SOAP	Simple Object Access Protocol

7. Contacts

Phone: 213820603

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

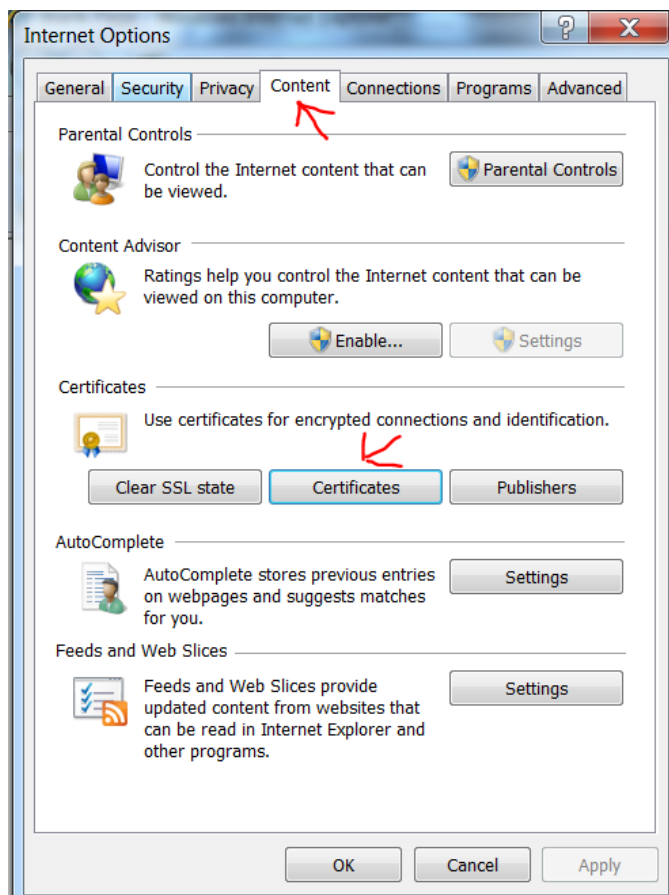
8. How to export the certificate public key

We describe the instructions to obtain a certificate public key in a Windows machine.

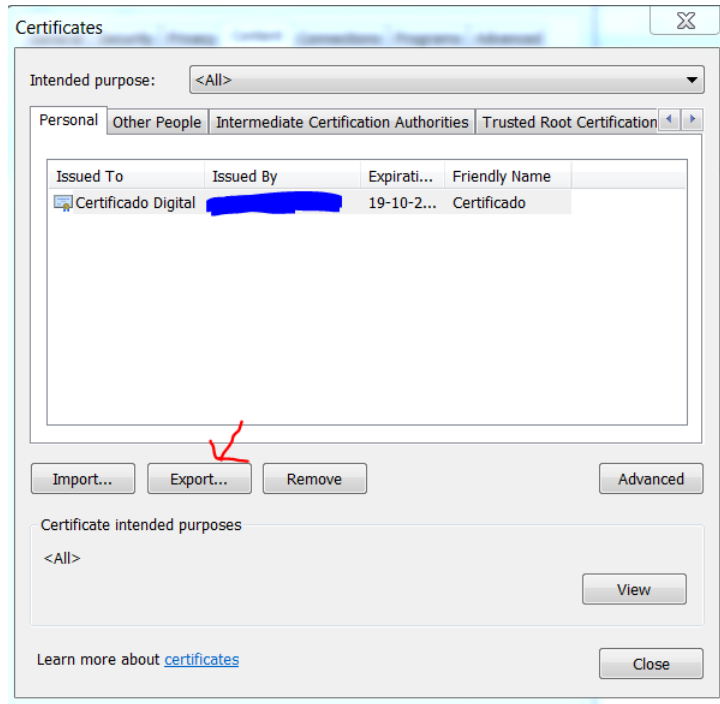
It is assumed that the certificate was previously imported in the Windows Operative System and an Internet Explorer 8 Browser is being used. For other combinations of OS an browser, the instructions should be adapted accordingly.

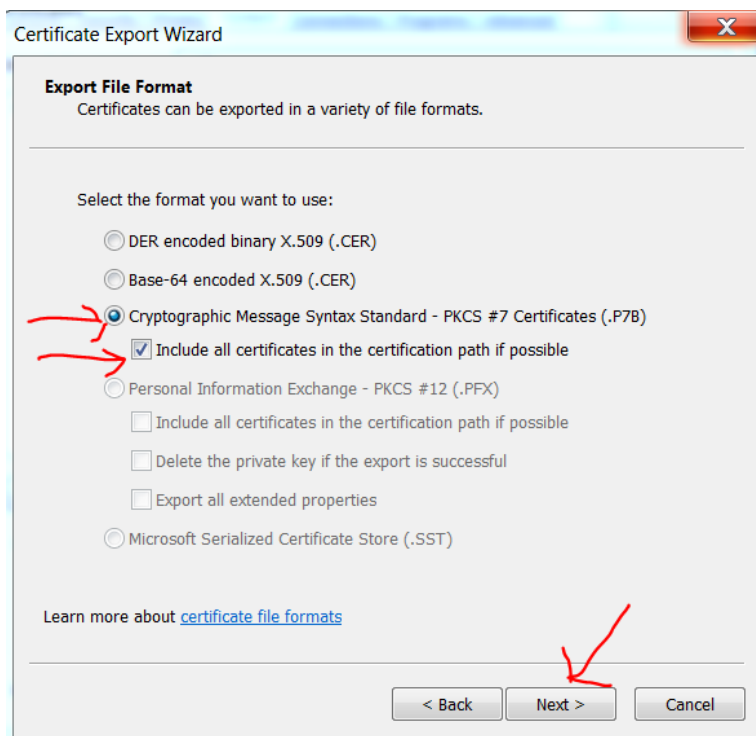
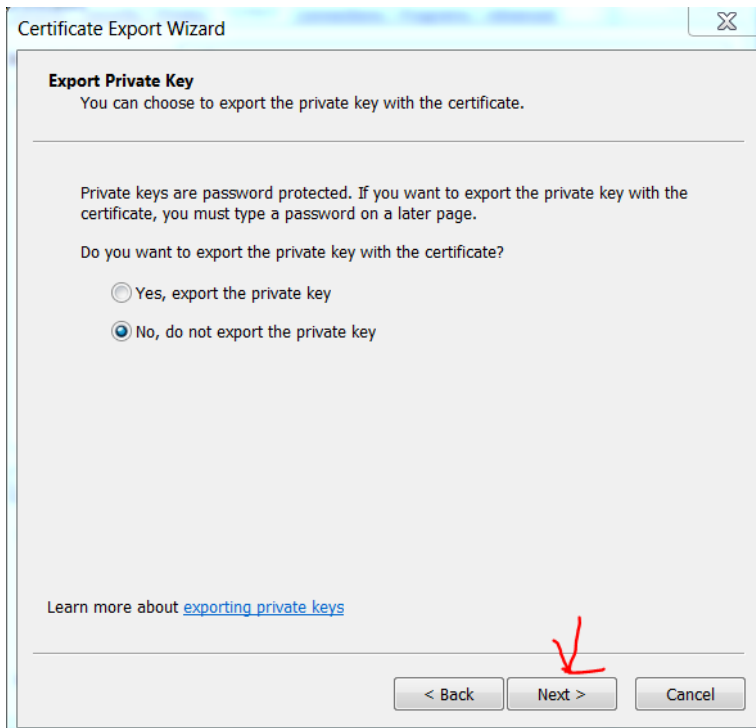
8.1. Certificate Location

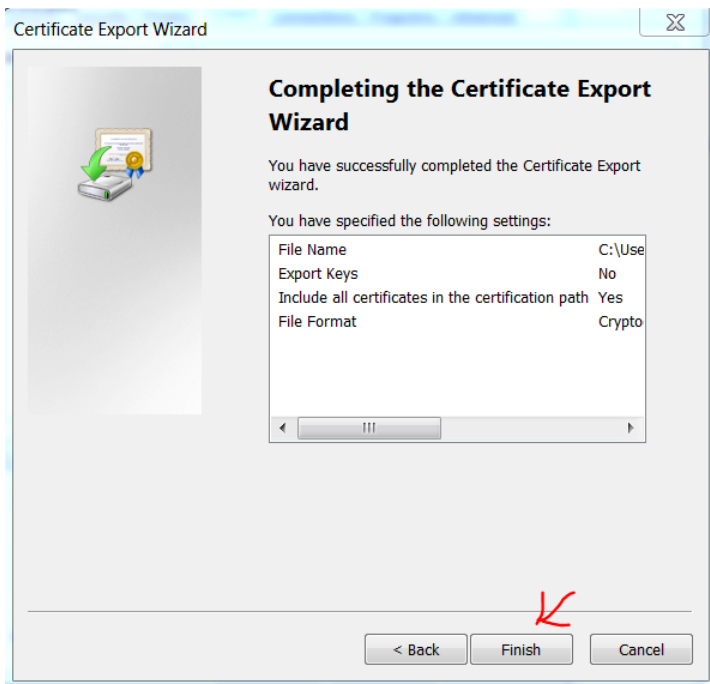
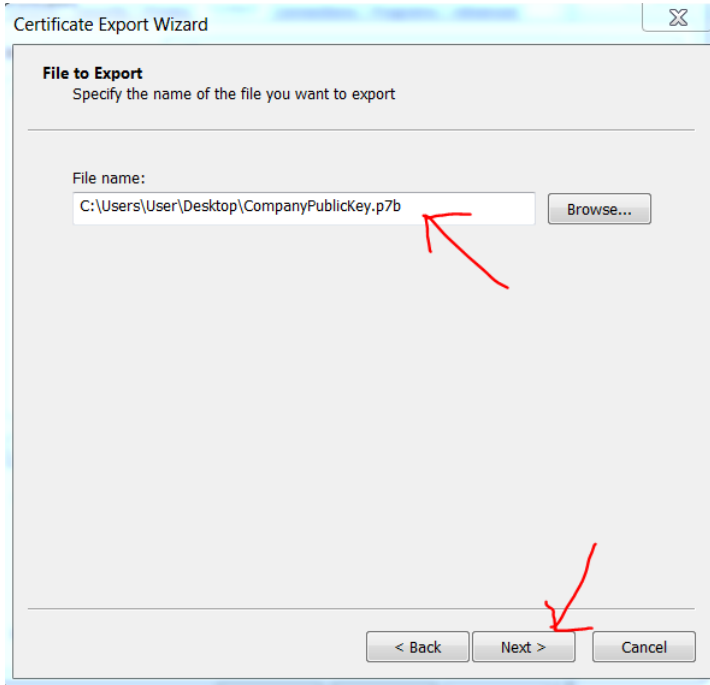
The certificate can be found in the Browser in the Menu: Tools -> Internet Options -> Content -> Certificates



8.2. Export the Public Key

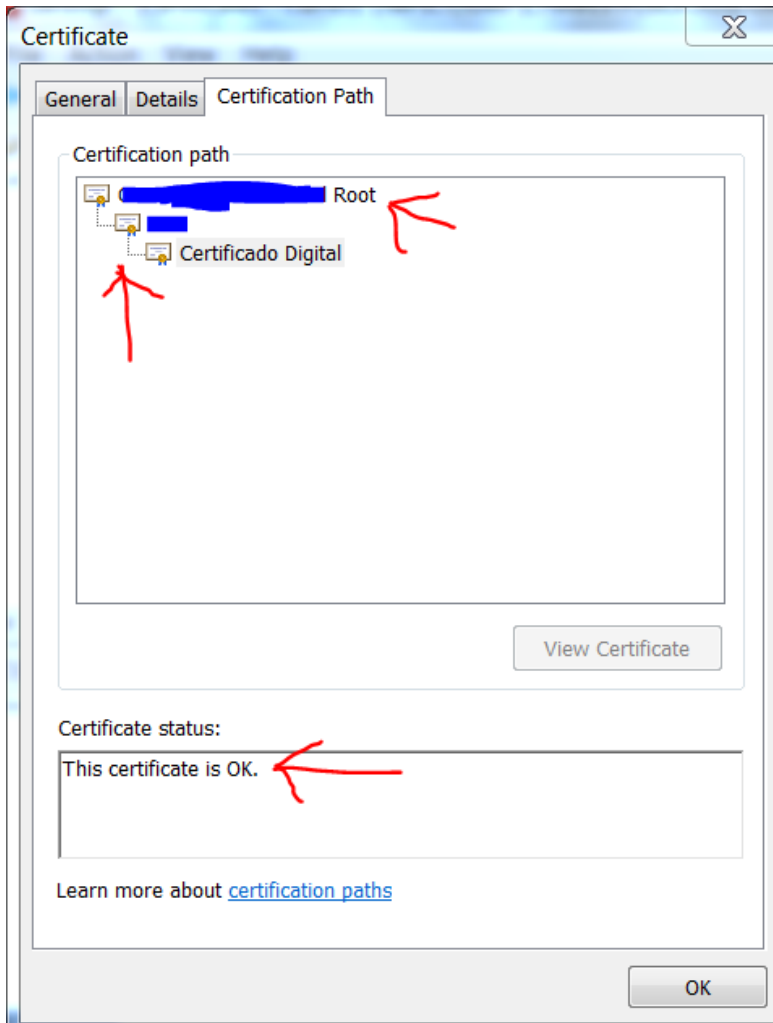






8.3. Check the Public Key

The public key must have a valid certification chain and it must be signed by a public and well known Root certification authority



8.4. Send the Public Key

The file that was obtained in **Error! Reference source not found.** must be “zipped” and sent by email to validation.

