AT
autoridade
tributária e aduaneira

Customs Electronic Declarations

Web Services - User Guide

Version 1.18

AT autoridade tributária e aduaneira

CUSTOMS ELECTRONIC DECLARATIONS

Web Services - User Guide

Title:	Customs Electronic Declarations - Web Services - User Guide
Version:	**1.18**
Date Created:	2016-08-19 15:06
Revision Name:	2019-01-11
File Name:	**Customs Electronic Declarations - Web Services - User Guide.docx**
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 Included Public Key export instructions	2.2 8
1.6	2010-12-28	Updated production addresses for ICS and SDS webservices	4.1; 4.2
1.7	2010-02-28	Included section about test Software	9
1.8	2011-03-16	Submission address updates (ECS and SDS Air Way Webservices)	4
1.9	2011-06-07	Submission address updates (Import Webservices)	4
1.10	2011-12-13	Included SDS - Air Way – Warehouse Keepers address Changed SDS – Air Way – Traders title	4.2 4.1
1.11	2012-03-28	Included AT Logo	-
1.12	2012-08-31	Included Java 7 related issue	8.4.1.2
1.13	2015-05-08	Updated quality assurance adresses	4
1.14	2015-06-23	Updated production adresses	4
1.15	2016-03-10	Removed deprecated info	**Erro! A origem da referência não foi encontrada.**
1.16	2016-08-19	Updated SICEX addresses	0
1.17	2018-12-05	Updated SDS WarehouseKeepers webservices	4.2
1.18	2019-01-09	Updated SDS WarehouseKeepers webservices	4.2

Index

1. Introduction

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

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

The software provider's digital certificate ensures that the message was sent by software produced by that software provider, which is responsible for correctly transmit the trader's (customer) messages. Digital certificates are different between Test and Production environment.

The trader is responsible for sending the message and message content, since it uses its own credentials in the AT – Customs Electronic Declarations Portal (Username/Password) that in turn are used by the Portuguese Customs Administration to assure non-repudiation of the transmitted data.

These credentials must only be known by Trader and should be different in Test and Production environments.

2. Prerequisites for using the service

2.1. Server Certificate

The SSL server certificate in use by AT – Customs Electronic Declarations Portal can be reached by reading the document "Digital Certificate Request EN" available here:

- https://aduaneiro.portaldasfinancas.gov.pt/

2.2. Client Certificate

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

- Company's Public Key Certificate its Certification Chain

  (The certificate public key a 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 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 test 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 AT – Customs Electronic Declarations Portal

Requests via Web Service to AT – Customs Electronic Declarations Portal 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:

System Identification	Security Requirements
SDS Air Way – Traders and SDS Air Way – Warehouse Keepers - System Web Services	• User authentication
ICS System Web Services	• User authentication
SIC-EU (EMCS) System Web Services	• User authentication • SOAP message integrity and authenticity

System Identification	Security Requirements
ECS System Web Services	- User authentication - SOAP message integrity and authenticity
Import System Web Services	- User authentication - SOAP message integrity and authenticity
SIC-EX Web services	- 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 AT – Customs Electronic Declarations Portal, 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 or EORI Number</wsse:Username>
      <wsse:Password Type="...">Password</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 a valid access to AT Portal:

    Example: 123456789
  - A sub-user NIF with a valid access to AT Portal:

    Example: 123456789/2 (sub-user number 2 of NIF: 123456789)
  - A valid EORI Number with prior access to AT Portal:

    Example: ES12345676

- The password must match the password of the user identified by: *Username*.

4. Submission URL's

4.1. SDS – Air Way – Traders – Web Services

Environment	Address
Quality / Test	https://servicos.portaldasfinancas.gov.pt:800/jsp/externalWebservice.jsp?external=sdsqualidadews
Production	https://servicos.portaldasfinancas.gov.pt:500/jsp/externalWebservice.jsp?external=sdsws

4.2. SDS WarehouseKeepers – Web Services

Environment	Address
Quality / Test	https://servicos.portaldasfinancas.gov.pt:807/jsp/externalWebservice.jsp?external=sdsdepws
Production	https://servicos.portaldasfinancas.gov.pt:507/jsp/externalWebservice.jsp?external=sdsdepws

4.3. ICS System – Web Services

Environment	Address
Quality / Test	https://servicos.portaldasfinancas.gov.pt:801/jsp/externalWebservice.jsp?external=icsqualidadews
Production	https://servicos.portaldasfinancas.gov.pt:501/jsp/externalWebservice.jsp?external=icsws

4.4. SIC-EU System – Web Services

Environment	Address
Quality / Test	https://servicos.portaldasfinancas.gov.pt:802/jsp/externalWebservice.jsp?external=siceuqualidadews
Production	https://servicos.portaldasfinancas.gov.pt:502/jsp/externalWebservice.jsp?external=siceuws

4.5. ECS System – Web Services

Environment	Address
Quality / Test	https://servicos.portaldasfinancas.gov.pt:803/jsp/externalWebservice.jsp?external=ecsqualidadews
Production	https://servicos.portaldasfinancas.gov.pt:503/jsp/externalWebservice.jsp?external=ecsws

4.6. SIC-EX System – Web services

Environment	Address
Quality / Test	https://servicos.portaldasfinancas.gov.pt:805/jsp/externalWebservice.jsp?external=sicexqualidadews
Production	https://servicos.portaldasfinancas.gov.pt:505/jsp/externalWebservice.jsp?external=sicexws

4.7. Import System – Web Services

Environment	Address
Quality / Test	https://servicos.portaldasfinancas.gov.pt:804/jsp/externalWebservice.jsp?external=impqualidadews
Production	To be defined.

4.8. Web Services WSDL definitions

All WSDL definitions are available in:

- https://aduaneiro.portaldasfinancas.gov.pt/

5. References

[1] AT - Customs Electronic Declarations Portal:
https://aduaneiro.portaldasfinancas.gov.pt/

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

6. Definitions, Acronyms and Abbreviations

AT	Autoridade Tributária e Aduaneira
Client Application	Application developed by a third party and used to access Web Service
EORI	Economic Operators Registration and Identification number
HTTPS	Hyper Text Transfer Protocol Secure
NIF	Número de Identificação Fiscal
OASIS	Organization for the Advancement of Structured Information Standards.
SOAP	Simple Object Access Protocol
Web Service	Web Service available through a network (Internet, Intranet or other) used for exchanging data between applications and systems

7. Contacts

Helpdesk e-mail:

- asa-pa@at.gov.pt

8. How to test the Web services with SOAP-UI

In order to test Web services the pre-requisites defined in point 3, Technical Requirements, must be met. Namely, one must produce a valid SOAP request that must be sent via the HTTPS protocol, by a Client Software with a pre-validated certificate and have the proper credentials user/pass for the test environment.

Note: It is a common mistake to test the web service with a simple browser request or using a tool like "curl". This kind of requests will simply be blocked by the infrastructure and no useful information will be given to the caller.

8.1. SOAP-UI Tool

SOAP-UI is a well-known open-source tool for testing Web services that enables testing SOAP interfaces and can be configured to meet the test requirements.

SOAP-UI is an open source tool and a free version can be obtained at http://www.soapui.org/.

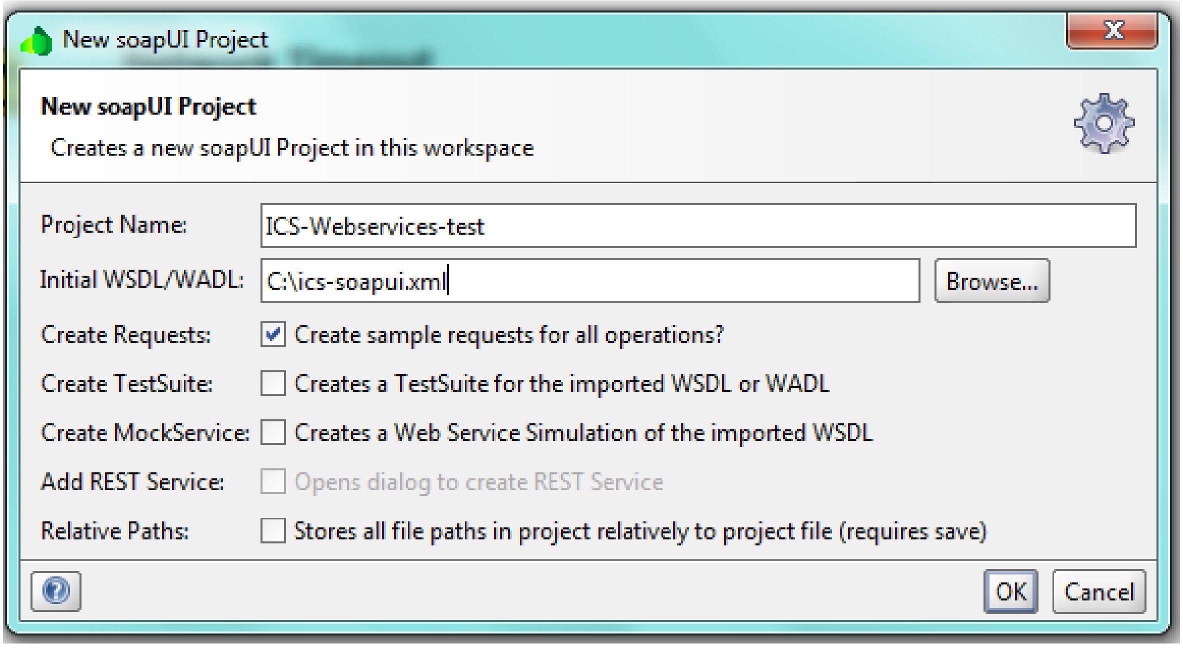
8.2. SOAP-UI Installation

Follow the application installation instructions.

8.3. SOAP-UI configuration

The following example illustrates the invocation of the ICS system Web service testing using SOAP-UI:

1) **Create a new project**
   a) Menu File -> New SOAP-UI Project
   b) Choose a name for the project and the WSDL (This WSDL is provided by: 7-Contacts).
   c) Check the option: Create sample requests for all operations.



New soapUI Project

New soapUI Project

Creates a new soapUI Project in this workspace

Project Name: ICS-Webservices-test

Initial WSDL/WADL: C:\ics-soapui.xml

Create Requests: ☑ Create sample requests for all operations?

Create TestSuite: □ Creates a TestSuite for the imported WSDL or WADL

Create MockService: □ Creates a Web Service Simulation of the imported WSDL

Add REST Service: □ Opens dialog to create REST Service

Relative Paths: □ Stores all file paths in project relatively to project file (requires save)

2) Configure client certificate authentication

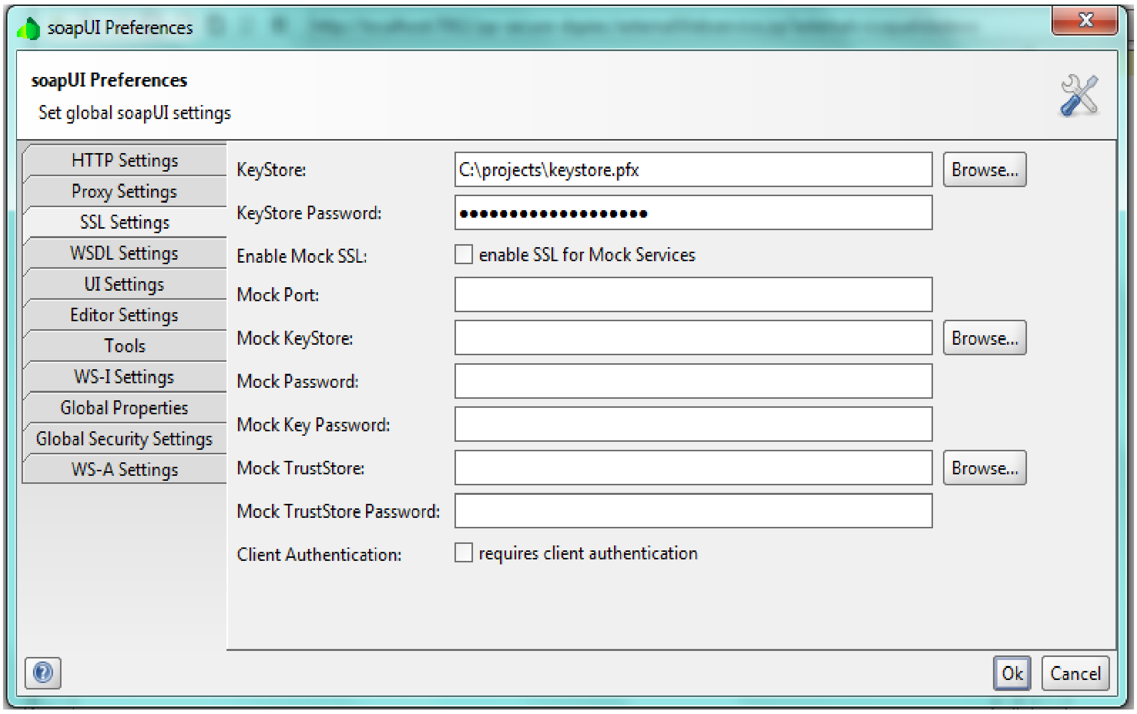
In order to use the client certificate to authenticate at the portal, the following option must be used.

a) Menu File > Preferences > SSL Settings

b) Enter the location of the KeyStore where the client certificate private key is stored

c) Enter the password of the KeyStore

d) Press: OK.



soapUI Preferences

Set global soapUI settings

KeyStore: C:\projects\keystore.pfx

KeyStore Password: ••••••••••••••••••

Enable Mock SSL: □ enable SSL for Mock Services

Mock Port:

Mock KeyStore:

Mock Password:

Mock Key Password:

Mock TrustStore:

Mock TrustStore Password:

Client Authentication: □ requires client authentication

3) Configure user authentication (without message digest)

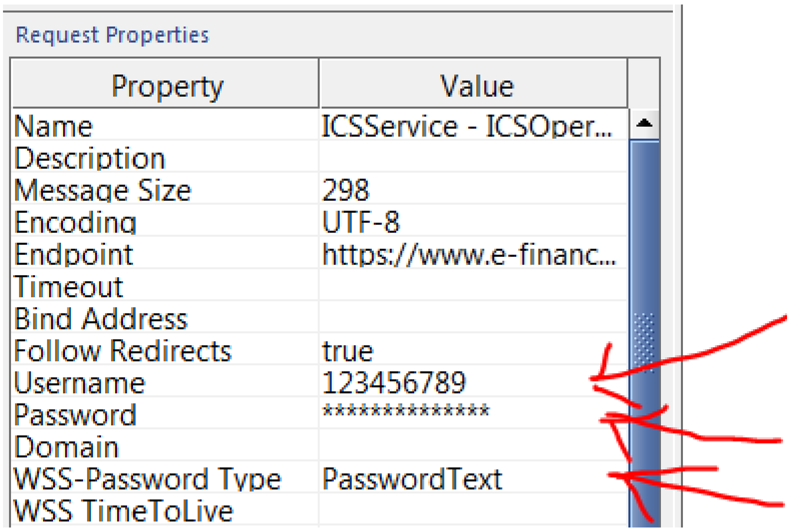
This configuration is a simplistic approach and applies only to requests without message digest.

In the request Properties Panel, fill the following properties:

Username: With the Economic Operator EORI Number (if the operator is a Portuguese Operator, fill with the NIF – Fiscal Number) that was registered in the AT Portal.

Password: Fill with the Password that was uses in the registration process in the AT Portal.

WSS – Password Type: choose “Password Text”.



Request Properties

Property	Value
Name	ICSService - ICSOper...
Description	
Message Size	298
Encoding	UTF-8
Endpoint	https://www.e-financ...
Timeout	
Bind Address	
Follow Redirects	true
Username	123456789
Password	**************
Domain	
WSS-Password Type	PasswordText
WSS TimeToLive	

4) Configure user authentication (with message digest)

Message Digest configuration requires access to the Tab: Security Configurations –> Outgoing WS Security Configurations.

Create a new Security Configuration and fill the: Username and Signature Tabs.

In the Signature Tab, define a Part:

- Part: "Body"
- Namespace: http://schemas.xmlsoap.org/soap/envelope/
- Encode: Element

5) Perform an operation

a) Access the one operation on the left sidebar and change the request with valid content:

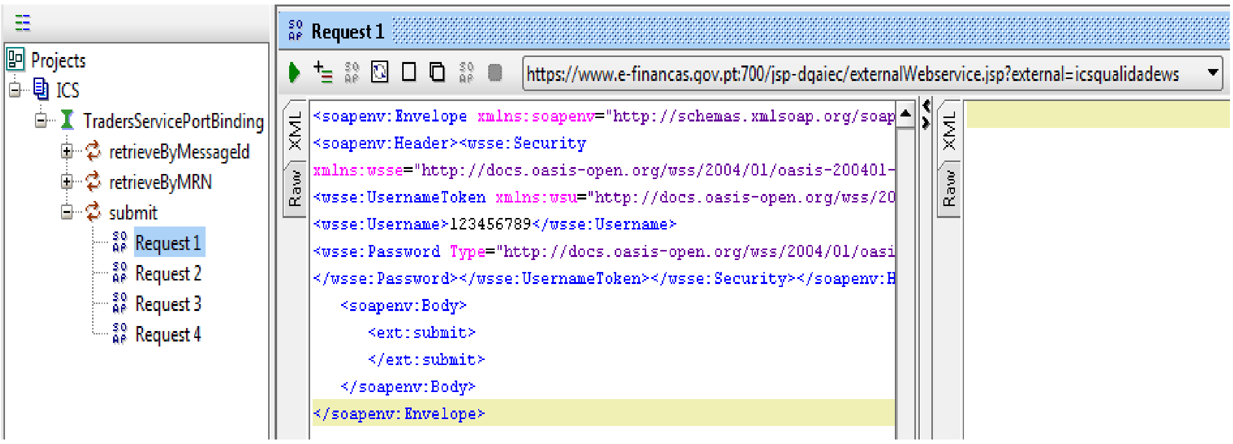
a. In the <Body> Fill with appropriate XML for the operation being tested

b. The <Username> should be automatically filled with the NIF or EORI number of the Economic Operator

c. The <Password> should be automatically filled with the password that was chosen for authentication at the AT Portal

b) Set the endpoint (select one of the endpoints described in: (4 Submission URL's)

c) Submit the request (the green play button) and check the response in the right frame or the error log.



https://www.e-financas.gov.pt:700/jsp-dqaiec/externalWebservice.jsp?external=icsqualidadews

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap
<soapenv:Header><wsse:Security
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
<wsse:UsernameToken xmlns:wsu="http://docs.oasis-open.org/wss/20
<wsse:Username>123456789</wsse:Username>
<wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasi
</wsse:Password></wsse:UsernameToken></wsse:Security></soapenv:H
   <soapenv:Body>
      <ext:submit>
      </ext:submit>
   </soapenv:Body>
</soapenv:Envelope>
```

8.4. Common errors and responses

8.4.1. Connection Errors

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

This means the handshake SSL handshake between SOAP UI and the AT Portal wasn't completed. This could mean the Client Certificate being used is not registered yet by the Portuguese Administration.

Please confirm that you received a confirmation of the registration by the Portuguese Administration.

Also check that: you are using the correct certificate store; that the store contains the client certificate that you are expecting to use and you are entering the correct key for that store.

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

Please make sure you have Http connectivity between the client machine and the server machine issue a (Ex: telnet servicos.portaldasfinancas.gov.pt 800 (see relevant port number)) should get a "Connected to servicos.portaldasfinancas.gov.pt".

This could also mean the test environment is unavailable, please redo the test a few more times and if still no response, please contact: 7 - Contacts.

8.4.2. Authentication Errors

8.4.2.1. “No Username or Password in message!”

This means a valid Username or Password was not provided in the UsernameToken, <Username> or <Password>.

8.4.3. Syntactic Errors

8.4.3.1. “Internal Error (from server)”

This probably means an invalid XML is being sent.

Please check the XML against the schema.

Contact (7 - Contacts) and provide: The Date/Time of the Test in GMO+0, the full request that is being sent and the response obtained.