Administration des Douanes et Accises du Luxembourg

eDouane

B2G INTERFACE PROTOCOL

Technical documentation

Version 1.2

Auteur	Administration des Douanes et Accises du Luxembourg (ADA)		
Version	1.2	Dernière mise à jour	24/02/2014

TABLE OF CONTENTS

1. Introduction

The purpose of this document is to specify the B2G interface protocol between the Luxembourg eDouane application and the economic operator systems.

The document will start with the technical specifications related to the data communication and security.

In addition to this document, all the technical specifications to design and build messages are available in the MIG specifications EMCS – ICS - IETA.

2. General architecture

The ‘Business to Government’ (B2G) approach of the eDouane project will use only:

Messages in **XML** format and the **AS2** communication protocol

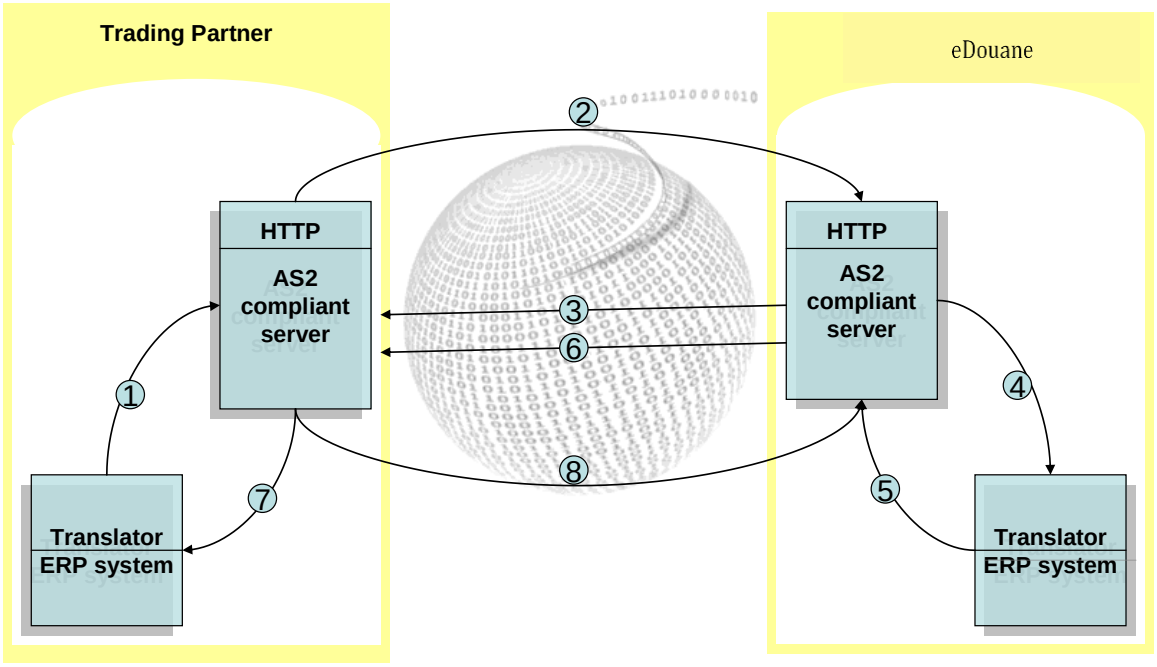
AS2 (standing for ‘Applicability Statement 2’) is a specification about how to transport data securely and reliably over the Internet. It is described in detail in RFC4130 (http://www.ietf.org/rfc/rfc4130.txt)

AS2 specifies how to connect, deliver, validate and acknowledge data. AS2 creates an envelope for a message which is then sent securely over the Internet. Security is achieved by using digital certificates and encryption.

An implementation of AS2 involves two machines, a client and a server, communicating with each other over the Internet. On the operating system level, the AS2 client may be a server, too, offering its communication services to application software. The client sends data to the server, e.g. a trading partner. On receipt of the message the receiving application sends an acknowledgement or MDN (Message Disposition Notification) back to the sender.

Through the use of AS2, efficient and secure machine-to-machine communication of XML data is achieved.

The general approach can be illustrated by the goods declaration of the Transit process:



1. Trading Partner's application generates the Declaration Data message that is mapped to XML data and is sent to AS2 compliant server.
2. Trading Partner's AS2 server encrypts, signs XML message and sends to eDouane via HTTP.
3. eDouane AS2 server sends MDN (Message Disposition Notification) to inform the Trading Partner that XML message has been received.
4. AS2 server uploads XML into eDouane ERP system.
5. The eDouane system generates a Movement Reference Number for identification of the Transit operation that is mapped to XML data and sends it to the eDouane AS2 server.
6. AS2 server encrypts, signs and forwards XML document to Trading Partner via HTTP.
7. The AS2 server of the Trading Partner decrypts XML and uploads the file to the Translator.
8. The AS2 server of the Trading Partner sends a MDN to eDouane to inform that XML message has been well received.

3. XML messages

The XML submitted to eDouane application must be compliant with the Luxembourg Customs standards.

The next part of this document will detail the different messages necessary for the different flows. All the 'XSD' schemas required for the XML messages are available for EMCS – ICS - IETA.

4. Communication Specifications

4.1 Protocol

AS2 provides an 'envelope' for the data, which is sent over the Internet using the standard HTTP protocol. Data is sent using a HTTP post (over TCP/IP) request to a static IP address.

The data it-self is encrypted and the description of the security aspect of the communication is described below.

4.2 AS2 identifier

The 'Administration des Douanes et Accises' is identified by its AS2 identifier: 'ADALUPLDA'

The AS2 Identifier from the message provider identifies the technical point from where and to where messages will be sent and received. This AS2 identifier is linked to the Luxtrust certificate. Only one Luxtrust certificate is necessary per AS2 identifier.

For message providers, one AS2 identifier is necessary, One Luxtrust certificate and multiple message sender.

4.3 Message sender identifier

The 'Administration des Douanes et Accises' message sender is: 'ADALUPLDA'

Each XML message that will be exchanged contains an Interchange Header, which identifies - besides other data types - the sender and recipient of the message. This is especially important for message providers to uniquely identify the final customer behind the message provider. One message provider can then have several final customers but each of these final customers must have a unique message sender identifier.

1. When the message is sent from service provider to ADA, the message sender is the final customer and message recipient is ADALUPLDA.
2. When the message is sent from ADA to service provider, the message sender is ADALUPLDA and message recipient is the final customer.

Note that the TEST and PROD Data of the message sender will be provided by the Luxembourg Customs.

4.4 IP address

All information regarding IP address and URL for connecting the test and production environments can be found inside the “AS2 Exchange Settings Document” received after successful registration as an “Economic Operator” with the Administration des Douanes & Accises.

4.5 Connection Info

Outgoing Message Security	Outgoing data needs to be signed and encrypted
Incoming Message Security	Incoming data requires signature and encryption
Compression	Data can be compressed

4.6 MDN receipts

Security	MDN receipts require a signature
Delivery	MDN receipts are exchanged preferably in an asynchronous way

4.7 Security

4.7.1 AS2 security concepts

The AS2 protocol provides two different levels of security for the exchange of messages.

The first level provides security at connection and data transport level. This means that the connection is secure and the communication protocol data is encrypted and authenticated. Technically, this is achieved by using SSL over HTTP (HTTPS).

An additional level of security offered by AS2 is the usage of S/MIME mechanisms to achieve end-to-end-security rather than transport layer security. S/MIME stands for “Secure Multipurpose Internet Mail Extensions” and is a standard for public key encryption and signing of electronic messages encapsulated in MIME. End-to-end-security means that the authenticity, integrity, confidentiality and non-repudiation of the message contents (IE messages in XML representation) are ensured at the application level rather than those of the “raw” data streams that are exchanged “on the wire” between the server and client . Technically, this is achieved by the usage of Public-Key-Infrastructure-mechanisms based on X.509 certificates at the level of the AS2 payload.

4.7.2 AS2 security in the eDouane B2G scenario

For AS2 communication between Trading Partners and the eDouane system, the HTTP protocol will be used. The usage of HTTPS is not necessary.

The payload of AS2 messages exchanged between Trading Partners and the eDouane system will be secured using S/MIME. Every message sent to and received from eDouane will be encrypted and signed. To this end, Trading Partners will have to purchase (a) S/MIME certificate(s) from one of the Certification Authorities accredited by eDouane. For more details about S/MIME message specification and certificate handling, please refer to RFC3850 and RFC3851.

Access to eDouane B2G functionality is restricted to authorized IP addresses. Trading Partners will have to register their IP address when applying for access to eDouane in order to be able to establish a B2G connection with eDouane.

4.7.3 SSL server/client authentication

This is the AS2 standard mechanism to ensure transport layer security. It is not used for eDouane B2G, which uses the standard HTTP protocol for data exchange.

4.7.4 IP address restriction

The eDouane B2G server will only accept and respond to HTTP requests coming from authorized IP addresses. Trading Partners will have to register their IP address in order to establish a B2G connection with eDouane.

4.7.5 Message Encryption

Every XML message sent or received by the eDouane B2G server will be encrypted to ensure the confidentiality of the message. The eDouane B2G server will not accept messages that are not encrypted.
Technically, this means that the payload of the AS2 HTTP-requests will be encrypted using S/MIME.
RFC 4130 “MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)” explains how S/MIME mechanisms are incorporated into the AS2 protocol.
The details about security formatting, encryption algorithm support and S/MIME message structure are set forth in RFC’s 3851/3852 "S/MIME Version 3.1 Message Specification; Cryptographic Message Syntax".
A trading partner encrypting a message to be sent to the eDouane B2G server will have to use the eDouane B2G public key. This key is contained in the eDouane B2G X.509 certificate of the Luxembourg Customs Administration. This is a S/MIME compliant certificate conforming to the provisions made in RFC 3850 “S/MIME Version 3.1 Certificate Handling”. Trading partners will receive this certificate as part of their registration process for eDouane B2G access and before any subsequent certificate change due to the expiration of the current certificate.
In order to be able to encrypt messages to be sent to the trading partner, eDouane will have to use the trading partner’s public key. For this reason, trading partners will transmit their S/MIME certificate to eDouane B2G authority, the Luxembourg Customs Administration, in advance, as part of the registration process for eDouane B2G access and before any subsequent expiration of the current certificate.
The trading partner’s certificate will ideally be a S/MIME compliant certificate which can be used for data encryption conforming to the provisions made in RFC 3850 “S/MIME Version 3.1 Certificate Handling”. It will be issued by a Certificate Authority (CA) that has previously been accredited for use with eDouane. Trading partners will use certificates issued by the Luxtrust CA.
Mandatory encryption does not apply to MDN receipts, which will be transmitted without encryption, but digitally signed. AS2 specifications do not provide for encrypted MDN exchange.

4.7.6 Message Signature

Every XML message sent or received by the eDouane B2G server will be digitally signed to ensure the integrity and authenticity of the message exchange. The eDouane B2G server will not accept messages that are not digitally signed.
Technically, this means that a digital signature of the payload of the AS2 HTTP-requests will be computed in compliance with S/MIME specifications.
RFC 4130 “MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)” explains how S/MIME mechanisms are incorporated into the AS2 protocol.
The details about security formatting, digest and signature algorithm support and S/MIME message structure are set forth in RFCs 3851/3852 "S/MIME Version 3.1 Message Specification; Cryptographic Message Syntax".
A trading partner verifying the digital signature of a message originating from the eDouane B2G

server will have to use the eDouane B2G public key. This key is contained in the eDouane B2G X.509 certificate of the Luxembourg Customs Administration. This is a S/MIME compliant certificate conform to the provisions made in RFC 3850 “S/MIME Version 3.1 Certificate Handling”. Trading partners will receive this certificate as part of their registration process for eDouane B2G access and before any subsequent certificate change due to the expiration of the current certificate.
In order to be able to verify the digital signature of messages received from the trading partner by eDouane, eDouane will have to use the trading partner’s public key. For this reason, trading partners will transmit their S/MIME certificate to eDouane B2G authority, the Luxembourg Customs Administration, in advance, as part of the registration process for eDouane B2G access and before any subsequent expiration of the current certificate.
The trading partner’s certificate will ideally be a S/MIME compliant certificate which can be used for digital signatures conforming to the provisions made in RFC 3850 “S/MIME Version 3.1 Certificate Handling”. It will be issued by a Certificate Authority (CA) that has previously been accredited for use with eDouane. Trading partners will use certificates issued by the Luxtrust CA.
Mandatory digital signature applies to MDN receipts as well, which will always have to be digitally signed.

4.7.7 Trading partner S/MIME certificate

Since the S/MIME security mechanisms used in the AS2 protocol are based on X.509 Since the S/MIME security mechanisms used in the AS2 protocol are based on X.509 certificates for public key management, trading partners will have to acquire such a certificate in order to access eDouane B2G functionality. This is a summary of the most important features regarding the certificate, some of which were already mentioned above:
The certificate must be issued by a Certification Authority that is accepted for use with eDouane. Ideally, the certificate is issued by the Luxtrust CA.
The certificate must be compliant to the provisions made in RFC 3850 “S/MIME Version 3.1 Certificate Handling”.
Trading partners must provide in advance the eDouane B2G authority, the Luxembourg Customs Administration, with their certificates. This applies to the registration process for eDouane B2G access as well as any subsequent change of the certificate due to expiration of the current one.

The certificate for message encryption can be the same as the one for message signature, since S/MIME provides certificates used for more than one purpose. (e.g. keyUsage extension with values digitalSignature and keyEncipherment set). Trading partners do not need to get two different certificates.

5. Contact

For more information, please contact the Helpdesk eDouane.

Helpdesk eDouane
Phone: +352 28 18 2000
Fax: + 352 28 18 92 01
E-mail: Helpdesk.Plda@do.etat.lu