Douane
Belastingdienst

Interface description HTG SMTP-MSA and POP3

Version 1.02

Date: 10-12-2019
Status: Definitive

Publisher’s imprint

Title	Interface description HTG SMTP-MSA and POP3
Organisation	National Helpdesk Dutch Customs T +31 88 156 66 55 nhd.apeldoorn@belastingdienst.nl

Table of contents

1 Introduction

1.1 Available interfaces

HTG, the "Handel en Transport Gateway" (Trade and Transport Gateway) (the successor of Digipoort Trade & Transport) is a generic electronic access service that allows the business community, active in the Trade and Transportation domain, to exchange electronic messages with public authorities. Whether or not HTG will function successfully depends heavily on the proper description of the interfaces to which the business community and the public authorities must be able to connect.

HTG offers the business community and the public authorities a number of interfaces based on electronic mail messages:

- SMTP-MTA (server-to-server)
- SMTP-MSA and POP3.

A description is available for each interface. This document sets out two of these interfaces, i.e. the SMTP-MSA (Simple Mail Transfer Protocol, Message Submission Agent) and POP3 (Post Office Protocol - Version 3) interfaces for the exchange of electronic messages between a mail client (business) and MTA mail server (HTG).

The following table indicates which interface descriptions apply to a specific message flow.

Message flow	Type of interface	Document
Logistic message flows for Customs and NVWA	SMTP-MTA	Interface description HTG SMTP-MTA
	SMTP-MSA/POP3	Interface description HTG SMTP-MSA and POP3
Single Window message flow for Rijkswaterstaat/NCA SSN, Border control and Customs	SMTP-MTA	Interface description HTG Single Window in addition to Interface description HTG SMTP-MTA
	SMTP-MSA/POP3	Interface description HTG Single Window in addition to Interface description HTG SMTP-MSA en POP3

Table 1: Message flows and interface descriptions

1.2 Target audience

This document is primarily intended for developers of system-to-system connections. In the business community two groups can be distinguished: reporting parties that have a legal obligation to communicate with a public authority, and dispatching organisations that offer services to help reporting parties with the communication. The term company is used in this document.

1.3 SMTP-MSA and POP3

These interfaces are intended for low frequency interaction (no more than 1 interaction per connection per minute) and are accessed ad-hoc over a TCP/IP (internet) connection. As soon as the transactions are completed using the interface, the connection is disconnected. For high frequency interaction, the interface SMTP-MTA must be used. For the time being, the SMTP-MSA and POP3 interfaces will not place any restrictions on the frequency of use.

With the interfaces SMTP-MSA and POP3 messages can be delivered to HTG and retrieved from a HTG mailbox. The SMTP-MSA interface is used for messages from a company to a public authority. For messages in the opposite direction the POP3 interface is used.

The SMTP-MSA and POP3 interfaces together offer an alternative for the SMTP-MTA (server-to-server) interface. For server-to-server connections, configuration of a Virtual Private Network (VPN) is necessary. The burden of setting up a VPN connection is too high for some companies. Together the SMTP-MSA and POP3 interfaces offer an alternative for which a VPN is not required.

1.4 Support

Support during connection setup and use is provided by the National Helpdesk Dutch Customs (NHD). See the publisher's imprint for contact details.

1.5 Outline of the document

The structure of this document is as follows. Chapter 1 contains general information. Chapter 2 contains a global process description. Chapter 3 describes the SMTP-MSA interface. Chapter 4 describes the POP3 interface. Chapter 5 describes the structure of the SMTP message. The document finishes with a list of abbreviations in chapter 6.

1.6 Version history

Version	Date	Changes (draft/definitive)
1.0	14-11-2019	Definitive version.
1.01	27-11-2019	Fixed typo in chapter 5, recipient address of preprod environment.
1.02	10-12-2019	Change of title page.

2 Process description

2.1 General

Messages are sent by companies to public authorities or from public authorities to companies. Trade and Transport Gateway (Dutch: Handel en Transport Gateway, HTG with internet domain htpoort.nl) provides the functionality required to exchange messages. Companies can be connected to the same message flow with several mail addresses. Communication between public authorities will usually occur via other interfaces.

In HTG no validation takes place on the (content of the) message, other than verification of the interface specifications as far as needed for routing and transportation (i.e. no syntax checks and no semantic checks of the payload).

HTG supports multiple message flows for several public authorities. An overview of the message flows is shown in Table 1.

Process/message flow	Public authority
Handling declarations (AGS declaration system)	Customs
Handling declarations, covenant partners (AGSC)	Customs
Handling declarations (DMS declaration system)	Customs
Handling declarations, covenant partners (DMSC)	Customs
EMCS	Customs
NCTS / Transit	Customs
CID Provision of Information	Customs
Single Window for Maritime and Aviation [1]	Rijkswaterstaat, Customs and Border Control
Pre-notification import animal products	NVWA
Pre-notification import plant products	NVWA
E-logbook fishing vessels	NVWA

Table 2: Message flows on HTG which can be delivered through SMTP

2.2 Message processing

Message processing by HTG starts with delivering the message. This results in a technical acceptance or rejection by HTG, according to the SMTP RFC's.

2.2.1 Delivery to HTG

When HTG receives a message, it will conduct checks to establish whether the message is safe to accept. HTG performs the necessary checks, such as valid authorisation, correct addressing, and maximum message length.

2.2.2 Confirmation of receipt

HTG accepts or rejects a message in accordance with the SMTP standards. This means that the message is technically accepted at the moment that the SMTP server (MTA) returns a "250 Ok" response in reaction to the SMTP DATA command. Additionally, a company can request during message transfer that it wants to receive a Delivery Status Notification (DSN). If the company also wants to receive a (positive) DSN in case of acceptance, this needs to be stated explicitly by means of the SMTP RCPT command, value NOTIFY (SUCCESS,FAILURE).

1 Single Window uses SMTP-MTA or SMTP-MSA and POP3 interfaces for message transfer , but it has additional requirements. Therefore there is an additional interface description for Single Window.

2.2.3 Delivery to recipient

HTG handles the delivery of messages. If the message is to be delivered to a public authority, HTG will connect to the server of the public authority and after authentication and additional checks, the message will be delivered. If the message is to be delivered to a company with a POP3 mailbox, HTG will store the message in the mailbox. The company must take the initiative to periodically connect via POP3 to HTG and retrieve the message from the mailbox.

2.3 Interface

HTG offers a basic service, which can be used by companies and public authorities. The SMTP-MSA and POP3 interfaces have been set up in such a way that they offer a platform for sending messages to HTG and receiving messages from HTG. The interface specifications indicate which specifications (RFCs) are used for sending and receiving messages and which standards are used to construct messages.

In these interface specifications, the actual content of the message that is forwarded by the interface ("the payload") is not described. There are separate Message Implementation Guides (MIGs) for each message flow, specified by the concerned public authority or authorities.

The interface specifications will be further explained in the next chapters.

3 Interaction through the SMTP-MSA interface (delivery of messages)

3.1 Use of Message Submission for mail instead of a standard MTA

For the delivery of SMTP traffic, a Message Transfer Agent (MTA) is usually used. To send a message, these MTAs can be accessed at port 25/tcp (TCP/IP protocol via port 25). However, many Internet Service Providers (ISPs) block this port, which means that for companies with a leased internet connection, it is not possible to connect to another party's MTA. ISPs offer a standard solution by directing all traffic through their own mail servers.

Blocking makes it impossible to set up a direct secure server-to-server connection between a company and HTG. That is why HTG offers a Message Submission Agent (MSA) which uses port 587/tcp. This allows companies to send their messages directly to HTG instead of using their own MTA or the ISP's MTA.

3.1.1 Principle of MSA

The principle of the MSA is described in "Message Submission for Mail" – Request for Comments (RFC) 6409. The RFC's point of view is as follows:

> The separation of message injection and message transmission, making it possible for the various services to focus on their own rules (for security, policy, etc.).

The role fulfilled by HTG as a service between business and government requires that aspects such as security and policy have to be interpreted in a specific way, which differs from a message submission chain offered by an internet service provider. The SMTP-MSA interface provides an opportunity for delivering messages to HTG by companies.

3.1.2 IANA considerations regarding SMTP-MSA

A big benefit of the use of the MSA is that it uses TCP port 587/tcp assigned by the Internet Assigned Numbers Authority (IANA), instead of port 25/tcp.

3.1.3 Authentication

Authentication at the session level has to take place based on SMTP Service Extension for Authentication (SMTP-AUTH). Chapter 4.3 of RFC 6409 sets out that the MSA returns an error message if the MAIL command is given and the session has not yet been authenticated. This is further elaborated in paragraph 3.3.2 of this document.

3.2 Contents

The contents of the message delivered to the MSA have to comply with the restrictions described in this interface description.

3.3 Security

The security requirements of the interface focus on the protection of the data between the sender and the recipient. Authenticity and integrity of the sent message is not guaranteed. The authenticity of the sender of the message is, however, to a certain degree safeguarded because authorised access is required.

3.3.1 Confidentiality of transport

The transport between the client and server of the interface is secured by using a so-called one-way Transport Layer Security (TLS). Only the TLS certificate of the HTG server is used to create a secure connection. After initiating the connection, the first thing to do is to establish a TLS connection (by means of the STARTTLS command). When the TLS connection is established the SMTP traffic can be exchanged. This principle is described in RFC 3207: ”SMTP Service Extension for Secure SMTP over TLS”. Authentication is possible (and required) after a TLS connection has been established.

3.3.2 Authentication and authorisation of the client

After establishing a TLS connection, the client must authenticate itself before it is authorised to deliver messages. Authentication is done by means of a username and password.

The interface uses the SMTP-AUTH and the Simple Authentication and Security Layer (SASL) – RFC 4422. These two standards together offer a framework for implementation of, amongst other things, username and password authentication methods. When the SASL is mentioned below, this actually refers to the combination SMTP-AUTH/SASL.

The interface supports the SASL mechanisms PLAIN and LOGIN[2]. Because use of a TLS connection is required, the password is protected against eavesdropping.

3.3.3 Recognised risks and measures

None of the existing SASL mechanisms is infallible and all warn for several types of attacks. When setting up the interface, extra attention should be paid to the following risks:

Risk	**Measure**
All commands given by the client that precede the STARTTLS command are in “plain text” and are at the expense of and for the responsibility of the client. The client has to give the STARTTLS command. If the client fails to do so, the connection is not secure. This risk applies in particular to the SASL mechanisms ‘PLAIN’ and ‘LOGIN’.	Until the STARTTLS command has been fully and properly completed, the MSA server may not honour any command at all that is given except for NOOP, EHLO, QUIT and STARTTLS. The server must respond to all other commands with a code 5xx.
A Man-In-The-Middle (MITM) attack is possible if the client spoofs the response from the STARTTLS command. The client now thinks that TLS is not possible and will continue with delivery of the mail in a plain text version, meaning the content of the message can be read by the MITM.	MITM attacks on SASL are almost impossible if the TLS connection has been established correctly. The condition is that the client must actually check the certificate provided by the server for validity and authenticity.

2 The HTG interface does not support SASL-mechanism DIGEST-MD5. To be able to support this mechanism, the SMTP server must be able to access the original password. The HTG server does not store the original passwords, but only a *one way hash* of the password. This makes it impossible to support DIGEST-MD5. Apart from that, DIGEST-MD5 is marked as obsolete by the IETF (see Moving DIGEST-MD5 to Historic – RFC 6331).

3.4 Example

The example below shows the interaction between the client and server when building up a SMTP MSA session and sending a message.

```
<server (S) is waiting for a TCP connection on port 587>
<client (C) opens a TCP connection on port 587>
S: 220 msa-smtp.htpoort.nl ESMTP
C: EHLO mycompany.nl
S: 250-msa-smtp.htpoort.nl
   250-STARTTLS
C: STARTTLS
S: 220 Ready to start TLS
S & C: <TLS connection between client and server is established>
C: AUTH PLAIN
S & C: <The PLAIN authentication scenario is carried out>
C: MAIL FROM:<me@mycompany.nl>
S: 250 2.1.0 Ok
C: RCPT TO:<douaneproces@htpoort.nl>
S: 250 2.1.5 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: <Enters SMTP headers and MIME message>
C: .
S: 250 2.0.0 Ok: queued as AE73753501E        <-- [3]
C: QUIT
<server closes the connection>
```

3.5 Standards

Standard	Reference
TCP/IP	https://tools.ietf.org/html/rfc793 https://tools.ietf.org/html/rfc1122 https://tools.ietf.org/html/rfc1958
Simple Message Transfer Protocol (SMTP)	https://tools.ietf.org/html/rfc5321
Message Submission for Mail (MSA)	https://tools.ietf.org/html/rfc6409
SMTP Service Extension for Authentication (SMTP-AUTH)	https://tools.ietf.org/html/rfc4954
Simple Authentication and Security Layer (SASL)	https://tools.ietf.org/html/rfc4422
Transport Layer Security v1.2 (TLS)	https://tools.ietf.org/html/rfc5246
PLAIN SASL Mechanism	https://tools.ietf.org/html/rfc4616
SMTP Service Extension for Secure SMTP over TLS	https://tools.ietf.org/html/rfc3207

3.6 Preconditions and agreements

These are already described in the RFC protocol standards and in this interface description.

RFC 6409 allows an MSA to rewrite email addresses. HTG expects that complete email addresses are offered by the client. It does not rewrite email addresses.

3.7 Email addresses, user name, and password

Email addresses are supplied after an account has been issued.

3 With this "250 OK" the SMTP-MSA server accepts the responsibility to deliver the message, or to report back by means of a DSN that delivery was not possible.

The user name and password are also supplied after an account has been issued. The user name is the fully qualified domain address of the mailbox, so including the domain. A new password can be requested by contacting National Helpdesk Dutch Customs (NHD).

3.8 Limitations

Technical limitations of the interface are supplied after an account has been issued.

4 Interaction through the POP3 interface (retrieving messages)

4.1 Use of POP3

The principle of POP3 is described in "Post Office Protocol 3" - RFC 1939. POP3 is intended as access to a message store[4]. This message store contains all messages that are addressed to a specific user. As soon as a user has authenticated himself and has gained access to his message store, messages can be retrieved.

4.1.1 Three states of a POP3 transaction

The POP3 protocol consists of three states during which it is active: AUTHORISATION, TRANSACTION and UPDATE. During the AUTHORISATION state, a client can only request the options from the server and log in. During the TRANSACTION state, messages from the user can be retrieved and/or deleted. After the TRANSACTION state, the server automatically switches to the UPDATE state.

AUTHORISATION state
During this state, the client has to authenticate himself to be authorised to access the message store. This is done through a combination of the USER and PASS command. Using the CAPA command, the client can request the options from the server. As soon as the authorisation has been given, the TRANSACTION state is entered. If the client gives a QUIT command here, the following states are omitted and the connection is closed.

TRANSACTION state
Once a client has obtained authorisation for a message store, the server will switch to this state. Here, messages can be retrieved and deleted. The RETR and DELE commands are used for this. Deletion does not actually take place during this state, but during the UPDATE state. As soon as the client has given a QUIT command, the TRANSACTION state ends and the UPDATE state starts.

HTG expects from a client that, after a RETR command and successful processing of the message, the deletion of the message from the message store will be done by means of a DELE command. It is explicitly not the intention to keep processed messages for a long time in the message store.

UPDATE state
During the UPDATE state, the server performs the requested deletions.

4.1.2 IANA considerations

POP3 operates on the TCP port assigned by the Internet Assigned Numbers Authority (IANA) which is 110/tcp.

4.2 Contents

The content of the messages retrieved from the POP3 postbox must comply with the restrictions described in this document.

4.3 Security

The security of the interface focuses on protecting the data between the sender and the recipient.

4 A message store is often referred to as mailbox.

4.3.1 Confidentiality of transport

The transport between the client and server is secured by using a so-called one-way Transport Layer Security (TLS). Only the TLS certificate of the server is used to create a secure connection. After initiating the connection, the first thing to do is to establish a TLS connection (by means of the STLS command). When the TLS connection is established the POP3 traffic can be exchanged. This principle is described in RFC 2595: ”Using TLS with IMAP, POP3 and ACAP”. Authentication is possible (and required) after a TLS connection has been established.

4.3.2 Authentication and authorisation of the client

After establishing a TLS connection, the client must authenticate itself before it is authorised to retrieve messages. Authentication is done by means of a username and password.

The interface uses the Simple Authentication and Security Layer (SASL) – RFC 4422. This standard offers a framework for implementation of, amongst other things, username and password authentication methods.

The interface supports the SASL mechanisms PLAIN and LOGIN[5]. Because the usage of a TLS connection is required, the password is protected against eavesdropping.

4.3.3 Recognised risks and measures

None of the existing SASL mechanisms is infallible and all warn for several types of attacks. When setting up the interface, extra attention should be paid to the following risks:

Risk	**Measure**
All commands given by the client that precede the STLS command are in “plain text” and are at the expense of and for the responsibility of the client. The client has to give the STLS command. If the client fails to do so, the connection is not secure. This risk applies in particular to the use of the SASL mechanisms ‘PLAIN’ and ‘LOGIN’.	Until the STLS command has been fully and properly completed, the POP3 server may not honour any command at all except for QUIT and STLS. The POP3 server may not leave the AUTHORISATION state until the STLS command has been given and a proper TLS connection has been established.
A Man-In-The-Middle (MITM) attack is possible if the client spoofs the response from the STLS command. The client now thinks that TLS is not possible and will continue with delivery of the mail in a plain text version, meaning the contents of the message can be read by the MITM.	MITM attacks on SASL are almost impossible if the TLS connection has been effected correctly. The condition is that the client must actually check the certificate provided by the server for validity and authenticity.

5 Also for the POP3 protocol, the HTG interface does not support SASL-mechanism DIGEST-MD5. See also paragraph 3.3.2.

4.4 Example

The example below shows the interaction between the client and server when building up a POP3 session and retrieving a message.

```
<server (S) is waiting for a TCP connection on port 110>
<client (C) opens a TCP connection on port 110>
S: +OK MDA Ready
C: CAPA
S: +OK Here's what I can do
TOP
STLS
C: STLS
S: +OK Begin TLS negotiation
S & C: <TLS connection between client and server is established>
C: AUTH PLAIN
S & C: <The PLAIN authentication scenario is carried out>
S: +OK Maildrop locked and ready
C: LIST
S: +OK
1 12288
2 31048713
C: RETR 1
S: +OK 12288 octets follow
<returns the message with ID 1 >
C: DELE 1
S: +OK Message 1 deleted
C: QUIT
<server deletes message with ID 1 and disconnects>
```

4.5 Standards

Standard	Reference
TCP/IP	https://tools.ietf.org/html/rfc793 https://tools.ietf.org/html/rfc1122 https://tools.ietf.org/html/rfc1958
Post Office Protocol – Version 3 (POP3)	https://tools.ietf.org/html/rfc1939
Simple Authentication and Security Layer (SASL)	https://tools.ietf.org/html/rfc4422
Transport Layer Security v1.2 (TLS)	https://tools.ietf.org/html/rfc5246
Using TLS with IMAP, POP3 and ACAP	https://tools.ietf.org/html/rfc2595
POP3 SASL Authentication Mechanism	https://tools.ietf.org/html/rfc5034
PLAIN SASL Mechanism	https://tools.ietf.org/html/rfc4616

4.6 Preconditions and agreements

These are already described in the RFC protocol standards and in this interface description.

4.7 Email addresses, user name, and password

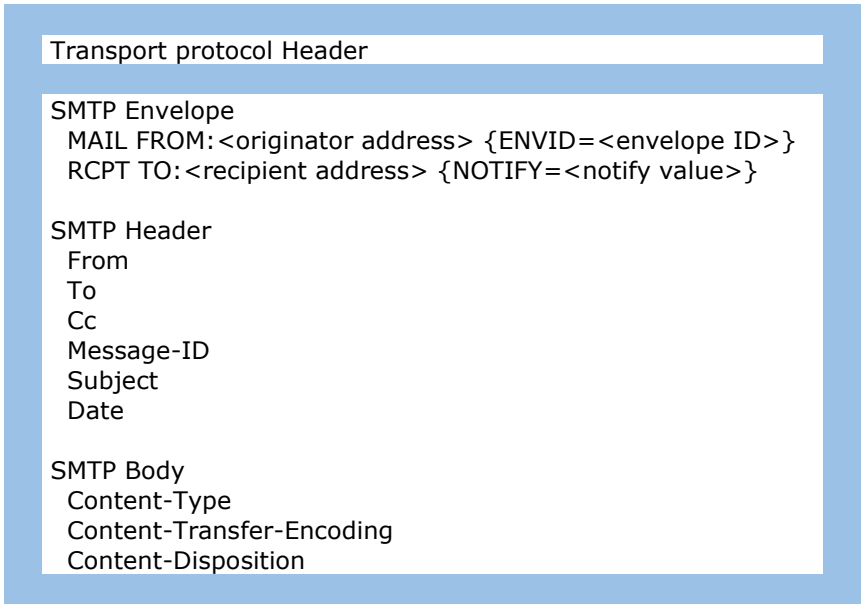
Email addresses are supplied after an account has been issued.

The user name and password are also supplied after an account has been issued. The user name is the fully qualified domain address of the mailbox, so including the domain. A new password can be requested by contacting National Helpdesk Dutch Customs (NHD).

4.8 Limitations

Technical limitations of the interface are supplied after an account has been issued.

5 Message specification



Element	**Specification**
MAIL FROM:<originator address> {ENVID=<envelope ID>}	The sender of the mail (originator address). Each mail has exactly one sender. If a receipt confirmation is requested a unique ID has to be included (envelope ID).
RCPT TO:<recipient address> {NOTIFY=SUCCCESS,FAILURE}	The recipient of the mail (recipient address). Each mail has exactly one recipient. The NOTIFY option can be used to indicate if the MSA must send a receipt confirmation and/or a delivery failure notification. Depending on the HTG environment the mail is being sent to, there are the following choices: <message type>@msa-smtp.htpoort.nl <message type>@msa-smtp.preprod.htpoort.nl
DATA [6]	The message content (SMTP headers and body).

Table 3: SMTP Envelope

6 See Table 4 and Table 5 for the definition of SMTP headers and body.

Element	Specification
From	Address of the sender of the message.
To	Address of the recipient of the message. Depending on the HTG environment the mail is being sent to, there are the following choices: <message type>@preprod.htpoort.nl <message type>@htpoort.nl
(Cc)	Since exactly one recipient is allowed, usage of Cc (and Bcc) is not allowed.
Message-ID	A unique identification of the message. The sender can set the message identification, provided that it is unique. If there is no message ID, HTG will add its own message ID.
Subject	A description of the subject of the message. This element is given to the recipient of the message.
Date	The transmission date of the message provided by the sender.

Table 4: SMTP Headers

Element	Value	Explanation
Content-Type	text/plain; charset=us-ascii	Preferred value for text-based messages. Other values are permitted for charset [7]. If there is no value, "us-ascii" is assumed. The supported values mentioned here are valid for the SMTP-MTA interface. In the Message Implementation Guide (MIG) of a message flow more strict requirements can occur. Windows Code Pages (CPxxxx) may not be referenced, because they cannot be interpreted on non-Windows systems.
	application/edifact	Alternative for messages in EDIFACT format.
	application/xml	Alternative for messages in XML format.
	application/octet-stream	application/octet-stream has to be used to transmit binary files.
Content-Transfer-Encoding	base64	Preferred value.
	quoted-printable	Alternative for base64.
	7bit	Permitted, but it is not recommended. Is unsuitable for binary data and text with ASCII values in excess of 127. CR/LF details can be lost upon conversion to base64. If the parameter Content-Transfer-Encoding is absent or the value is not entered, this is always interpreted as '7bit'.
Content-Disposition	attachment filename=<bestandsnaam>.<extensie>	HTG always replaces the filename with a unique ID. If the parameter is absent or the value is not entered, HTG generates a unique filename with extension .txt.

Table 5: SMTP Body

7 In any case, the following character sets are supported: "us-ascii", "UTF-8", "ISO-8859-1" (Latin1, West European), "ISO-8859-15" (Latin9, West European + Euro).

6 Abbreviations

Abbrev.	Meaning
AGS	Aangiftesysteem (Dutch abbreviation), declaration system
CID	Comfort Informatie Douane (Dutch), application provisioning information
DMS	Douaneaangiften Management Systeem (Dutch), further development of AGS
DSN	Delivery Status Notification, an automated message from a mail system
EMCS	Excise Movement and Control System
HTG	Handel en Transport Gateway (Dutch), Trade and Transport Gateway
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IP	Internet Protocol, a fundamental Internet standard
MIG	Message Implementation Guide
MSA	Message Submission Agent, software used when receiving email from client
MTA	Mail Transfer Agent, software that transfers e-mail between computers
NCTS	New Computerised Transit System
NHD	National Helpdesk Dutch Customs
NVWA	Netherlands Food and Consumer Product Safety Authority (Dutch abbreviation)
POP3	Post Office Protocol - Version 3
RFC	Request for Comments, technical and organisational notes about the internet
SASL	Simple Authentication and Security Layer, authentication framework
SMTP	Simple Mail Transfer Protocol
SW	Single Window, single reporting intended for multiple public authorities
TCP	Transmission Control Protocol, a fundamental Internet standard
TLS	Transport Layer Security, a protocol for secure computer network communication
VPN	Virtual Private Network, method to extend a private network across a public network