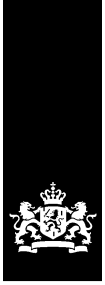

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Koppelvlakbeschrijving Digipoort
Berichtuitwisseling - SMTP-MSA

Versie 1.1.1

Datum 2 juni 2015
Status Concept

Publisher's imprint

Project name	Digipoort
Version number	1.1.1
Organization	Logius P.O. Box 96810 2509 JE The Hague servicecentrum@logius.nl
Appendix	0

Content

Introduction

Objective and target group
The aim of Digipoort (formerly the Government Gateway OTP) is to enable a generic electronic access service through which the business community can reach the entire government.
Whether or not Digipoort will function successfully is very dependent on the proper description of the interfaces to which the government and the business community have to be able to connect.

Digipoort offers the business community and the government various interfaces. A separate specification is available for each interface. This document sets out one of these interfaces, i.e. the SMTP-MSA interface. Based on this interface, messages can be delivered to Digipoort with the help of a mail client. This interface is intended for messages from the business community to the government. The POP-3 interface is available for the corresponding return messages.

This interface does not describe the standard for the exchange of messages between mail servers (MTAs). Information regarding this can be found in the document entitled "Interface Description Digipoort; Exchange of Messages - SMTP-MTA (server-to-server)".

This document is primarily intended for developers of system-to-system connections.

Outline of the report
The structure of the document is as follows. The first chapter contains general information. The second chapter contains the description of the functioning of the delivery. The third chapter provides a more detailed insight into the technical functioning of the interface. The document closes with an overview of all generally applicable standards and rules.

For more details about the structure of SMTP messages, you can read the message flow specifications and view the sample messages.

Status
The SMTP-MSA interface originated from a need to offer an alternative for the connection of businesses that provide information to Customs and currently do this by means of X.400 P7 postboxes.

Digipoort provided for the establishment of the SMTP-MSA/POP3 interfaces, however only in fixed connections through leased lines and VPNs. The expense of setting up a connection of this type is too high for both the businesses and the administrator of Digipoort. Along with the also new POP3 interface, SMTP-MSA offers an alternative, where leased lines and VPNs are not required.

Expectations are that the open standards that are used will develop further in the forthcoming years and that the communication demand will also be subject to change. As a consequence of this new releases of Digipoort will started to be used during the forthcoming years. That can have an impact on the interfaces.

1 Interaction through the interface

1.1 Transport

This interface is intended for low frequent interaction (less than 1 interaction per business per minute) and is 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 frequent interaction, the interface SMTP-MTA is used. For high frequent interaction, the interface SMTP-MTA is used. For the time being, the interface will not place any restrictions on the frequency of the use.

1.2 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. [1]To send a message, these MTAs can be accessed at 25/tcp. However, many Internet Service Providers (ISPs) block this port from the inside out, which means that for users of a leased internet connection, it is not possible to maintain SMTP traffic with another party. Providers offers a standard solution by directing all traffic through a message submission chain.

This means that it is difficult to set up a secure server-to-server connection between a business and Digipoort. That is why Digipoort takes on the role as a Message Submission Agent (MSA) for the government. This means that businesses inject their messages directly into Digipoort instead of their own MTA or by using the transmission of the ISP.

1.2.1 Principle of MSA

The principle of the MSA is described in full in "Message Submission for Mail" – Request for Comments (RFC) 4409. The RFC's point of view is as follows:

The separation of message injection and message transmission, because of which the various services can focus on their own rules. (for security, policy, etc.).

The role fulfilled by Digipoort at the edge of the government domain means that aspects such as security and policy have to be interpreted in a specific way, which differs from a message submission chain offered by a provider. The SMTP-MSA interface provides an opportunity for message injection to Digipoort by businesses.

1.2.2 IANA considerations in respect of MSA

A huge benefit from the use of the MSA is that this uses a TCP portal assigned by the Internet Assigned Numbers Authority (IANA) differently to 25/tcp, i.e. 587/tcp.

1.2.3 Authentication

Authentication at session level has to take place based on SMTP Service Extension for Authentication (SMTP-AUTH). Chapter 4.3 of the RFC sets out that the MSA standard returns an error message if the MAIL command

[1] *25/tcp means as much as TCP/IP port no. 25*

is given and the session has not yet been authenticated. This is elaborated on further in paragraph 1.4.2 of this document.

Figure1: Interaction with the MSA server when SASL is used

1.3 Contents

The content of the message injected in the MSA has to comply with the restrictions described in the document Message Flow Specifications - SMTP-MSAPOP3 Logistic Flows.

1.4 Security

The security of the interface focuses 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 access authorisation is given.

1.4.1 Confidentiality of transport

The transport between the client and server to the interface is secured using a so-called 1-way Transport Layer Security (TLS). Only the TLS certificate of the server is used to create a symmetrical secure connection. When initiating the connection, a TLS connection can immediately be created over which the SMTP traffic is exchanged.
Alternatively, an insecure connection can be created, after which the STARTTLS command is given by the client to initiate the TLS. This principle is described in RFC 2487: *"SMTP Service Extension for Secure SMTP over TLS*". This option is not preferable in terms of confidentiality and, if possible, should not be used (see 1.4.31.4.3.).

1.4.2 Authentication and authorisation of the client

After having created a TLS connection, the client has to authenticate itself before it is authorised to inject messages. Authentication is 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, the combination SMTP-AUTH/SASL is actually being referred to.

A list of the methods that are available is maintained by the IANA and can be viewed at http://www.iana.org/assignments/sasl-mechanisms.

The interface supports the SASL mechanisms DIGEST-MD5, PLAIN and LOGIN.

1.4.3 Recognised risks and measures

None of the existing SASL mechanisms is infallible and all warn of 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 use of the SASL mechanisms 'PLAIN' and 'LOGIN'.	Until the STARTTLS command has been fully and properly completed, the MSA server may not honour any commend at all that is given except for NOOP, EHLO, QUIT and STARTTLS. The server must respond to all other commands with a code 530 (Must issue a STARTTLS command First).
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 effected correctly. The condition is that the client must actually check the certificate provided by the server for validity and authenticity.

1.4.4 Possible scaling up of security

It is possible to scale up security by modifying authentication and authorisation. To this end, a 2-way TLS has to be transferred to. This means that the client must also supply a certificate to set up the secure connection. For the time being, this is not yet possible for this interface.

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

```
<server (S) is waiting for a TCP connection on
port 587>
<client (C) opens a TCP connection on port 587>
S: 220 msa.overheidstransactiepoort.nl ESMTP
  C: EHLO mijnbedrijf.nl
S: 250-msa.overheidstransactiepoort.nl
     250-PIPELINING
     250-SIZE 52428800
     250-STARTTLS
     250-8BITMIME
     250-AUTH DIGEST-MD5
  C: STARTTLS
S: 220 Ready to start TLS
S & C: <TLS connection between client and server
will be created>
  C: AUTH DIGEST-MD5
S & C: <The digest authentication scenario is
being played out>
  C: MAIL FROM:<ik@mijnbedrijf.nl>
S: 250 2.1.0 Ok
  C: RCPT TO:<belastingdienst@overheid.nl>
S: 250 2.1.5 Ok
  C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
  C: <Imports SMTP headers and MIME message>
S: 250 2.0.0 Ok: queued as EA37575310A
  C: QUIT
<server closes the connection>
```

2 General arrangements

2.1 Standards

Standard	Reference
TCP & TCP/IP	http://www.rfcsearch.org/rfcview/RFC/675.html, http://www.rfcsearch.org/rfcview/RFC/1958.html, http://www.rfcsearch.org/rfcview/RFC/1122.html
Simple Message Transfer Protocol (SMTP)	http://www.rfcsearch.org/rfcview/RFC/2821.html
Message Submission for Mail (MSA)	http://www.rfcsearch.org/rfcview/RFC/4409.html
SMTP Service Extension for Authentication (SMTP-AUTH)	http://www.rfcsearch.org/rfcview/RFC/2554.html
Simple Authentication and Security Layer (SASL)	http://www.rfcsearch.org/rfcview/RFC/4422.html
Transport Layer Security v1.1 (TLS)	http://www.rfcsearch.org/rfcview/RFC/4346.html
Digest Authentication for SASL (Digest-MD5)	http://www.rfcsearch.org/rfcview/RFC/2831.html
SMTP Service Extension for Secure SMTP over TLS	http://www.rfcsearch.org/rfcview/RFC/2487.html

2.2 Preconditions & Error messages

All applicable preconditions and error messages are already described in the prescriptive RFCs and the 'Interface specification document SMTP-MTA'.
RFC 4409 proposes that messages that are injected into the MSA are enhanced, as far as possible, if this is not done by the Mail User Agent (MUA). This is mainly about completing email addresses with the (local) domain part and rewriting From addresses. For injection, the Digipoort MSA expects full addresses and does not support the completion and rewriting of addresses.[2]

2.3 Addresses

These are supplied after an account is applied for.

2.4 Limits and restrictions

Technical restrictions of the interface are supplied after an account is applied for.

2.5 Support

Support during connection and use is provided by the Logius Service Centre. See the publisher's imprint for contact details.

[2] *Furthermore, addresses are rewritten by the Digipoort core functionality: from a logical address (xyz@otpnet.nl) a translation is made to the actual address (abc@xyz.nl) and the other way around.*