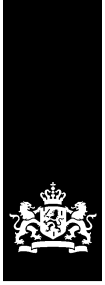

Logius
*Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*

# Koppelvlakbeschrijving Digipoort Berichtuitwisseling - POP3

Versie 1.1.1

Datum 2 juni 2015
Status Definitief

# Publisher's imprint


| | |
|---|---|
| Project name | Digipoort |
| Version number | 1.1.1 |
| Organization | Logius<br>P.O. Box 96810<br>2509 JE The Hague<br>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 POP3 interface. Based on this interface, message can be retrieved from Digipoort with the help of a mail client. This interface is intended for messages from the government to the business community. For electronic messaging in the opposite direction, the SMTP-MSA interface is available.

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 document is constructed 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 POP3 interface originated from a need to offer an alternative to the connection of businesses that provide information to Customs and currently do this using 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 SMTP-MSA interface, POP3 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. The consequence of this is that, during the forthcoming years, new releases of Digipoort will started to be used. 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 user 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.

## 1.2 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. 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, this will be locked by the POP3 server. As long as the POP3 server is active for message storage, no messages can be delivered to this message store. In addition, no messages can be retrieved by another government body from the POP3 server.

### *1.2.1 3 stages of a POP3 transaction*

The POP3 protocol consists of three stages during which it is active; AUTHORIZATION, TRANSACTION and UPDATE. During the AUTHORIZATION stage, a client can only request the options from the server and register. During the TRANSACTION stage, messages from the user can be retrieved and/or deleted. Following the TRANSACTION stage, the server automatically switches to the UPDATE stage. Figure1 provides an overview of the various stages.

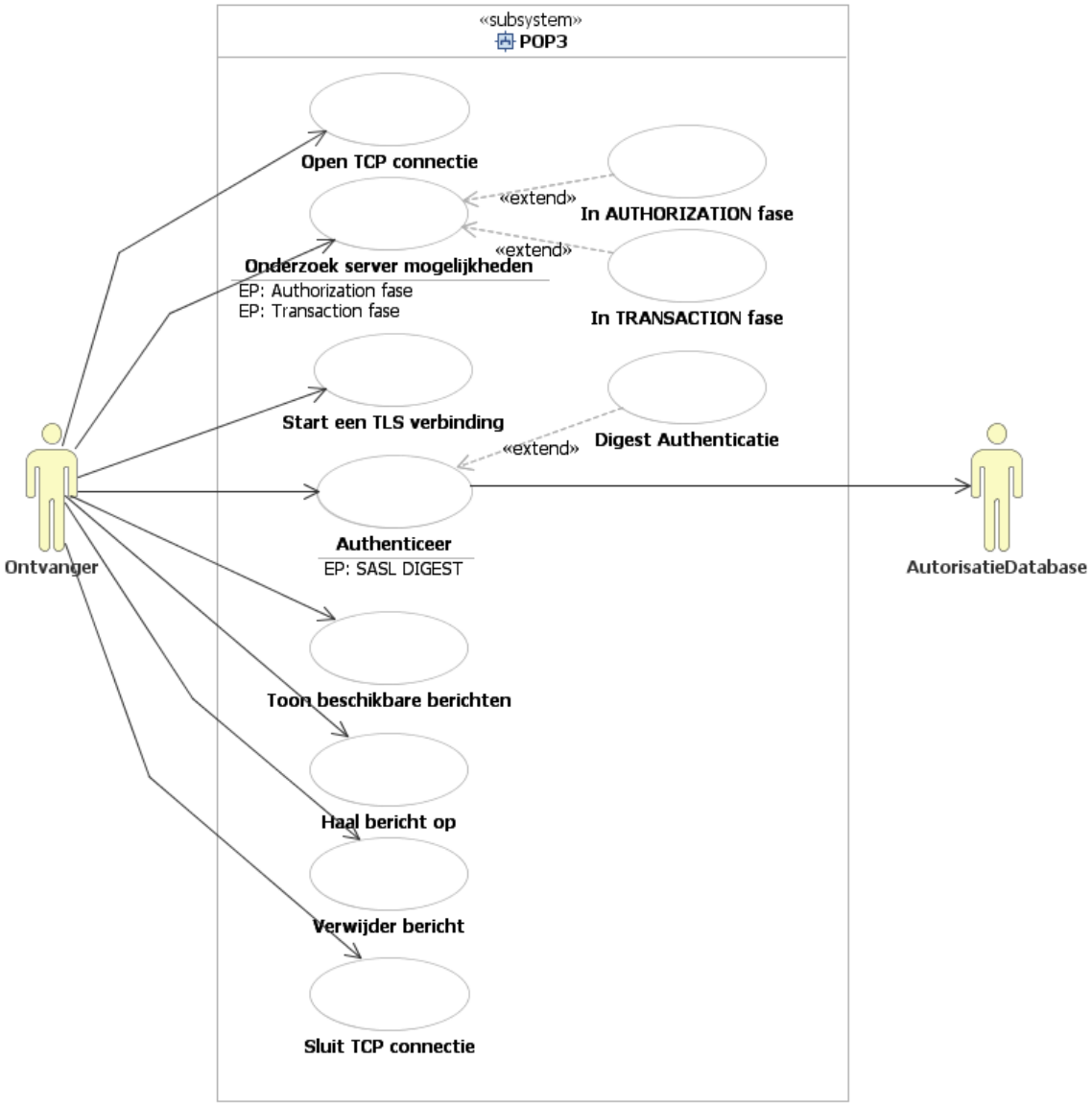


*Figure1: Interaction between the user and POP3 server when SASL is used*

1.2.1.1 AUTHORISATION stage

During this stage, the client has to authenticate himself and therefore gain authorisation 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 message store is locked to prevent further processing.
If the client gives a QUIT command here, the following stages are omitted and the connection is closed.

1.2.1.2 TRANSACTION stage

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

1.2.1.3 UPDATE stage
During the UPDATE stage, the server performs the requested deletions and unlocks the message store.

*1.2.2 IANA considerations*
POP3 operates on a TCP port assigned by the Internet Assigned Numbers Authority (IANA) which is 110/tcp.
NB: TCP port 995/ssl pop is not used. This port is 'discouraged' in RFC 2595.

## 1.3 Contents

The content of the messages retrieved from the POP3 postbox must comply with the restrictions described in the Message Flow Specifications - SMTP-MSAPOP3 Logistic Flows document.

## 1.4 Security

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

*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 STLS command is given by the client. This principle is described in RFC 2595: *"Using TLS with IMAP, POP3 and ACAP".* This option is not preferable in terms of confidentiality and, if possible, should not be used (see 1.4.3).

*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 retrieve messages. Authentication is 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.

A list of the available methods 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 STLS command are in "plain text" and are at the expense of and for the responsibility of the client.<br>The client has to give the STLS command. If the client fails to do so, the connection is not secure.<br>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 that is given except for QUIT and STLS.<br>The POP3 server may not leave the AUTHORISATION state until the STLS command has been given and a proper TLS connection has been achieved. |
| 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 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.

## 1.5 Example

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

```
<server (S) is waiting for a TCP connection on
port 110>
<client (C) opens a TCP connection on port 110>
S: +OK Hello there.
  C: CAPA
S: +OK Here's what I can do
     SASL DIGEST-MD5
     TOP
     PIPELINING
     STLS
  C: STLS
S: +OK Begin TLS negotiation
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>
S: +OK Maildrop locked and ready
  C: LIST
S: +OK
     1 12288
     2 31048713
  C: RETR 1
S: +OK 12288 octets follow
     <gives the MIME message with ID 1 back>
  C: DELE 1
S: +OK Message 1 deleted
  C: QUIT
<server deletes message with ID 1 and 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 |
| Post Office Protocol – Version 3 (POP3) | http://www.rfcsearch.org/rfcview/RFC/1939.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 |
| Using TLS with IMAP, POP3 and ACAP | http://www.rfcsearch.org/rfcview/RFC/2595.html |
| POP3 SASL Authentication Mechanism | http://www.rfcsearch.org/rfcview/RFC/5034.html |
| Digest Authentication for SASL (Digest-MD5) | http://www.rfcsearch.org/rfcview/RFC/2831.html |

## 2.2 Preconditions & Error messages

All applicable preconditions and error messages are already described in the standards listed above.

## 2.3 Addresses

These are supplied after an account is applied for.

## 2.4 Limits

These 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.