Mail-Server: ESMTP-Dialog (SMTP-Auth)

ESMTP-Dialog

Ein SMTP-Dialog wurde bereits vorgestellt. Heute erkläre ich einen ESMTP-Dialog mit verschiedenen Authentifizierungsmethoden.

Wir sehen uns drei Auth-Methods an:

- PLAIN
- LOGIN
- CRAM-MD5

PLAIN

Die Methode PLAIN wird von Netscape/Mozilla/Thunderbird bevorzugt. Dies Clients können zwar auch LOGIN, aber nutzten lieber dieses.

Hierbei werden ID, Username und Passwort in einen String zusammengefasst (mit &#65533; - also dem Null-Byte als Trenner) und dann Base64-Encodiert.

Sender
Text

client
```
telnet huschi.net 25
```

server
```
220 server1.consult-n.de ESMTP Postfix (Debian/GNU)
```

client
```
EHLO localhost
```

server
```
250 server1.consult-n.de
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
```

client

(c) 2025 huschi <huschi@huschi.net>

```
AUTH PLAIN dGVzdAB0ZXN0AHRlc3RwYXNz
```

server
```
235 go ahead
```

[...]

client
```
QUIT
```

server
```
221 Bye
```

LOGIN

Die Methode LOGIN wird vorallem von Outlook genutzt. (Es ist meist die einzige Methode, die Outlook beherscht.)

Hier werden Benuzternamen und Passwort einzeln abgefragt. Die Kommunikation dazu wird Base64 kodiert ('VXNlcm5hbWU6' => 'Username:').
Ensprechend wird der User und das Passwort Base64-kodiert übertragen.

Sender
Text

client
```
telnet huschi.net 25
```

server
```
220 server1.consult-n.de ESMTP Postfix (Debian/GNU)
```

client
```
EHLO localhost
```

server
```
250 server1.consult-n.de
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
```

client
```
AUTH LOGIN
```


(c) 2025 huschi <huschi@huschi.net>
URL: https://www.huschi.net/index.php?action=artikel&cat=11&id=108&artlang=de

server
```
334 VXNlcm5hbWU6
```

client
```
[username]
```

server
```
334 UGFzc3dvcmQ6
```

client
```
[userpw]
```

server
```
235 go ahead
```

[...]

client
```
QUIT
```

server
```
221 Bye
```

CRAM-MD5

Während bei den anderen zwei Methode das Passwort unverschlüsselt (Base64 ist keine Verschlüsselung!) über die Leitung geht, wird nun ein String erzeugt, welcher per MD5 kodiert ist.

Hierbei wird ein zufälliger String auf Server-Seite erzeugt (meist ein Timestamp), welcher zur Kodierung hinzugefügt wird. Dieser wird vom Server gesendet sobald CRAM-MD5 gewählt wurde.

Die Antwort enthält den User und das Passwort inkl. des Strings per MD5 encoded.

Sender
Text

client
```
telnet huschi.net 25
```

server
```
220 server1.consult-n.de ESMTP Postfix (Debian/GNU)
```


(c) 2025 huschi <huschi@huschi.net>
URL: https://www.huschi.net/index.php?action=artikel&cat=11&id=108&artlang=de

client
```
EHLO localhost
```

server
```
250 server1.consult-n.de
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
```

client
```
AUTH CRAM-MD5
```

server
```
334 PDI0NjA5LjEwNDc5MTQwNDZAcG9wbWFpbC5TcGFjZS5OZXQ+
```

client
```
USER NAME [username]
```

server
```
334
```

client
```
DIGEST [digest]
```

server
```
235 go ahead
```

[...]

client
```
QUIT
```

server
```
221 Bye
```

Verwandte Artikel:

- Eine typische SMTP-Sitzung

Eindeutige ID: #1107
huschi

(c) 2025 huschi <huschi@huschi.net>
URL: https://www.huschi.net/index.php?action=artikel&cat=11&id=108&artlang=de

2007-11-08 10:03

(c) 2025 huschi <huschi@huschi.net>
URL: https://www.huschi.net/index.php?action=artikel&cat=11&id=108&artlang=de