

## Re: Exchange 2003 SMTP nicht konform zu RFC?

**Source:**

<http://www.tech-archive.net/Archive/German/Exchange/microsoft.public.de.german.exchange2000.setup.installation/>

---

**From:** Thomas Krug (*no-spam\_at\_siw.de*)

**Date:** 03/29/04

Date: Mon, 29 Mar 2004 11:36:59 +0200

> "Thomas Krug" <no-spam@siw.de> schrieb  
>> Jens Mander <jens.mander@donotspam.com> wrote:  
>>> [Ex2003 SMTP nicht RFC-koform bei SMTP AUTH ?]  
>>> [Outlook Express erzeugt bei Kommunikation mit Smarthost  
>>> de Providers folgenden Dialog:]  
>>>  
>>> 220 mail.myprovider.com MYPROVIDER ESMTP MailService V2.00  
>>> EHLO myserver  
>>> 250-mail.myprovider.com  
>>> 250-PIPELINING  
>>> 250-SIZE 20971520  
>>> 250-ETRN  
>>> 250-AUTH CRAM-MD5 DIGEST-MD5 LOGIN PLAIN OTP  
>>> 250 8BITMIME  
>>> AUTH LOGIN  
>>> 334 VXNlcm5hbWU6  
>>> fhFDGf456GFGcc4fddFG==  
>>> 334 UGFzZc3dvcmQ6  
>>> bghfrDHGFFE=  
>>> 235 Authentication successful  
>>>  
>>> ....usw.  
>>>  
>>> Der Mailversand über Exchange 2003 auf dem gleichen System endet  
>>> allerdings mit dem Fehler "AUTH Failure" in der Warteschlange.  
>>> Snifft man hier den Netztraffic, sieht man, dass Exchange 2003 den  
>>> BASE64 verschlüsselten Login direkt hinter das "AUTH LOGIN" hängt,  
>>> ohne auf die Challenge des anderen SMTP Servers zu warten. Dies ist  
>>> aber laut RFC2554 nur für Authentifizierungsmethoden mit leeren  
>>> Challenges erlaubt. Diese hier ist aber nicht leer, wie man in der  
>>> Zeile "334 VXN..." sehen kann.  
>>>  
>>> Entspricht der Exchange 2003 hier nicht der RFC? Oder liegt hier der  
>>> Provider falsch?  
>>> Kann man Exchange 2003 zwingen, die lange Form der Authentifizierung  
>>> mit Base64-Credentials erst NACH Challenge zwingen?

>>>  
>>  
>>  
>> "Thomas Krug" <no-spam@siw.de> schrieb  
>> Das Challenge kommt doch erst nach dem AUTH LOGIN ... SMTP-Clients  
>> können durchaus ihren Benutzernamen gleich base64-codiert hinter das  
>> AUTH LOGIN schreiben.  
>>  
>> Ich hab in meinem Mailserver-Log sowohl solche als auch solche  
>> Authentifizierungsanfragen drin stehen – beides ist zulässig und  
>> abhängig vom Client.  
>>  
>> Laut RFC 2254 ist das zulässig, wenn eine Authentif.art gewählt  
>> wird, die kein Challenge mit Daten benötigt.  
>> "Login" gehört dazu – es wird lediglich Benutzername / Kennwort  
>> base64-kodiert und fertig; der Server muß also in seinem Challenge  
>> keinen String mitschicken, der Client weiter verwursten muß.  
>>  
>> Was Du als  
>>> 334 VXNlcm5hbWU6  
>> und  
>>> 334 UGFzZc3dycmQ6  
>> lesen kannst, heisst nur "Username:" und "Password:"  
>>  
>> [...]

Jens Mander <jens.mander@donotspam.com> wrote:

> Hallo Thomas.  
>  
> Erstmal danke für die Antwort. Hast Du eine Referenz, dass die  
> Methode LOGIN keinen Challenge erfordert?  
> Ich hab die Kommunikation zwischen Exchange und ISP gesniff't. Er  
> bricht nach dem AUTH LOGIN <base-64-username> ab, den Exchange im  
> Gegensatz zu OE sendet. Und zwar mit dem Fehler 353, der laut RFC  
> 2554 als Fehler bei "Methods that require a challenge" vorgesehen ist.  
> Ich müsste dem Provider jetzt klarmachen, dass AUTH LOGIN laut RFC den  
> Challenge "USERNAME:" nicht erfordert und daher ER das Problem  
> verursacht. Der Provider behauptet, MS wäre hier nicht RFC-konform  
> und ich solle mich an den MS Support wenden, wenn ich bei ihm keine  
> Mails absetzen kann.  
>

Hallo Jens,

also wie gesagt – auf meinen Mailservern kommen beide  
Authentifizierungsarten an. Als Clients wird querbeet alles eingesetzt, was  
Internetkunden eben so einsetzen.

Ich finde sowohl ein  
AUTH LOGIN  
als auch ein

AUTH LOGIN aGllcmtvZW5udGVJJaHJLZW5ud29ydHN0ZWlbg==  
in den Logdateien – beides wird von Clients verwendet und funktioniert.

Laut RFC 2554 ist das zusätzliche Argument erlaubt, wenn der Challenge nicht nötig ist:

---

The optional initial-response argument to the AUTH command is used to save a round trip when using authentication mechanisms that are defined to send no data in the initial challenge.

---

Bei "LOGIN" wäre das ein leerer Challenge, da der Server nur fragt: "Username:" -> der Client kann gleich mit der Tür ins Haus fallen und dem Server erklären: "Hallo, ich bin der-und-der-Benutzer und ich würde mich gerne authentifizieren". Im Gegensatz dazu wäre bei z.B. CRAM-MD5 Authentifizierung erstmal ein Challenge-String des Servers nötig, den der Client durch eine Hashfunktion jagen kann. Für ein SMTP-AUTH, das "LOGIN" als Authentifizierungsart unterstützt, sollte der Mailserver beide Arten drauf haben, sonst werden etliche Clients kein SMTP-AUTH machen können. Das geht vielleicht nur schwammig aus der RFC hervor, aber etliche Clients nutzen die sinnvolle Möglichkeit, gleich den Benutzernamen mitzusenden.

Abhilfe:

- + Provider konfiguriert seinen Mailserver vernünftig bzw. setzt einen ein, der auch bei anderen Anbietern rund läuft
- + anderen Provider suchen
- + andere Authentifizierungsart verwenden
  - > im dümmsten Fall z.B. pop-before-smtp, indem Du per Job alle n Minuten ein POP3-Postfach beim Provider abrufst.
  - (Ausser Standardauthentif. / "LOGIN" ist da leider nix Brauchbares für smtp auth dabei)

Viele Grüße

Thomas.