

RFC 7615 : The Hypertext Transfer Protocol (HTTP) Authentication-Info and Proxy-Authentication-Info Response Header Fields

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 octobre 2015

Date de publication du RFC : Septembre 2015

<https://www.bortzmeyer.org/7615.html>

Un très court RFC, probablement un des derniers du groupe de travail IETF qui a fait la réécriture de la norme HTTP 1.1 <<https://www.bortzmeyer.org/http-11-reecrit.html>>. Il normalise l'en-tête HTTP `Authentication-Info`, qui était précédemment dans le RFC 2617¹.

Cet en-tête, et son équivalent pour les relais, `Proxy-Authentication-Info`, sert au serveur HTTP à communiquer des informations après une authentification réussie.

Dans la nouvelle rédaction de la norme HTTP 1.1 <<https://www.bortzmeyer.org/http-11-reecrit.html>>, l'authentification est décrite par le RFC 7235. L'ancien RFC sur les méthodes d'authentification, le RFC 2617, est désormais abandonné et plusieurs RFC ont repris ses spécifications, comme notre RFC 7615 pour les deux en-têtes d'information `Authentication-Info` et `Proxy-Authentication-Info`.

La section 3 de notre RFC décrit en détail le premier en-tête. Envoyé par le serveur après une authentification réussie, il contient une liste de paires {nom, valeur}. Les noms possibles dépendent du mécanisme d'authentification utilisé. Par exemple, le mécanisme "*Digest*" du RFC 7617 utilise `Authentication-Info` pour des informations techniques nécessaires pour la prochaine authentification. Notre RFC 7615 ne normalise donc que la syntaxe, pas la sémantique. Voici un exemple :

```
Authentication-Info: rspauth="670ff3158cec20b73d7342932f8c40a1",  
  cnonce="1672b410efa182c061c2f0a58acaa17d", nc=00000001, qop=auth
```

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc2617.txt>

L'en-tête `Proxy-Authentication-Info`, décrit en section 4, est exactement le même, sauf qu'il est utilisé lors de l'authentification avec un relais intermédiaire et non pas avec le serveur HTTP final.

Les deux en-têtes peuvent être indiscrets, par les informations qu'ils donnent sur l'authentification (ne serait-ce que le simple fait qu'il y a eu authentification). La section 5 de notre RFC, consacrée à la sécurité, recommande donc l'utilisation de HTTPS.

Ces deux en-têtes HTTP sont enregistrés à l'IANA, dans le registre des en-têtes `<https://www.iana.org/assignments/message-headers>`.

Apparemment aucun changement significatif dans ces en-têtes n'est apparu depuis l'ancienne norme, le RFC 2617.