RFC 7372 : Email Authentication Status Codes

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 septembre 2014

Date de publication du RFC : Septembre 2014

https://www.bortzmeyer.org/7372.html

Il existe désormais plusieurs techniques d'authentification du courrier électronique, comme SPF ou DKIM. Elles permettent à un serveur de messagerie, s'il le désire, d'accepter ou de rejeter le courrier entrant s'il échoue à ces tests d'authentification. Mais il n'existait pas jusqu'à présent de moyen standard de prévenir l'expéditeur, lors de la session SMTP, de la raison de ce rejet. C'est désormais fait, avec ce nouveau RFC, qui permet de renvoyer des codes de retour SMTP explicites, si on veut.

J'ai bien dit « si on veut » car tous les administrateurs de serveurs ne sont pas d'accord pour indiquer à l'expéditeur les raisons exactes du rejet. Après tout, si l'authentification échoue, c'est peut-être que l'expéditeur était un méchant, un spammeur, par exemple, et, dans ce cas, on ne souhaite pas lui donner de l'information. L'utilisation de ces nouveaux codes de retour est donc optionnelle.

Ces codes sont de type « codes étendus », normalisés par le RFC 3463 [1] et dotés d'un registre IANA depuis le RFC 5248. Les codes « améliorés » du RFC 3463 comportent trois nombres, la **classe** (2 : tout va bien, 4 : erreur temporaire, 5 : erreur définitive, etc), le second le **sujet** (6 : problème avec le contenu du message, 7 : problème avec la politique de sécurité, etc) et le troisième le **détail**. Ils s'écrivent avec un point comme séparateur, contrairement aux codes de retour traditionnels, eux aussi à trois chiffres, mais sans séparateur.

La section 3 du RFC liste ces nouveaux codes. Ils figurent tous dans le registre IANA <https://www.iana.org/assignments/smtp-enhanced-status-codes/smtp-enhanced-status-codes.xhtml#smtp-enhanced-status-codes-3>. Dans quasiment tous les cas, le code de base (non étendu) associé sera 550, le code étendu donnant les détails.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3463.txt

D'abord, pour DKIM (RFC 6376). Il y a deux cas de succès, "*passing*", où la signature DKIM est valide et "*acceptable*", où non seulement la signature est valide mais où elle correspond aux règles locales du serveur récepteur (qui, par exemple, impose que tel ou tel en-tête soit couvert par la signature). Un cas particulier de "*acceptable*" (qui a son code spécifique) est celui où le serveur de réception impose que l'auteur du message (dans le champ `From:`) corresponde à une des identités DKIM utilisées pour signer le message. C'est donc la vérification la plus stricte.

Les codes sont respectivement :

— X.7.20 (où X indique la classe, qui sera 5 "*Permanent Failure*" dans la plupart des cas) : aucune signature DKIM "*passing*".
— X.7.21 : aucune signature DKIM "*acceptable*". Au moins une signature est valide ("*passing*"), autrement on utiliserait X.7.20 mais elle ne correspond pas aux exigences locales (rappelez-vous que la norme DKIM laisse une grande latitude à l'émetteur sur ce qu'il signe et notamment sur l'identité utilisée, voir entre autres la section 1.2 du RFC 6376).
— X.7.22 : il y a au moins une signature DKIM "*passing*" mais elle n'est pas "*acceptable*" car l'identité utilisée n'est pas celle contenue dans le champ `From:` (un cas particulier de X.7.21, donc).

Notez que DKIM permet d'avoir des signatures valides et des invalides sur le même message. En effet, certains logiciels modifient le message en route, invalidant les signatures. Le principe de DKIM est donc qu'on ignore les signatures invalides. On n'envoie les codes de retour indiquant un rejet que lorsqu'on n'a **aucune** signature valable. À noter aussi que tous ces codes indiquent que le serveur SMTP de réception s'est assis sur l'avis de la section 6.3 (et non pas 6.1 contrairement à ce que dit le nouveau RFC) du RFC 6376. Cet avis dit en effet « "*In general, modules that consume DKIM verification output SHOULD NOT determine message acceptability based solely on a lack of any signature or on an unverifiable signature ; such rejection would cause severe interoperability problems.*" » Le but est d'augmenter la robustesse de DKIM face à des intermédiaires qui massacreraient des signatures. Mais, bon, il y a des gens qui rejettent les messages juste pour une absence de signature valide, donc, autant leur fournir un code de retour adapté. (Voir aussi la section 4 qui discute ce point et insiste bien sur le fait que cela ne signifie pas une approbation de ce rejet violent par les auteurs du RFC. Cette question a été une des plus chaudement discutées dans le groupe de travail IETF.)

Ensuite, il y a des codes pour SPF (RFC 7208) :

— X.7.23 : message invalide selon SPF,
— X.7.24 : pas forcément invalide mais l'évaluation de SPF a entraîné une erreur (problème DNS, par exemple).

Voici à quoi pourrait ressembler une session SMTP avec rejet SPF :

```
% telnet mail.example.com smtp
220 myserver.example.com ESMTP Postfix (LibreBSD)
...
MAIL FROM:<me@foobar.fr>
550 5.7.23 Your server is not authorized to send mail from foobar.fr
```

Enfin, il y a un code pour le test dit "*reverse DNS*" décrit dans la section 3 du RFC 8601, qui consiste à traduire l'adresse IP de l'émetteur SMTP en nom(s) puis ce(s) nom(s) en adresses IP pour voir si l'adresse originale se trouve dans cet ensemble d'adresses. Il peut conduire au code SMTP X.7.25 en cas d'échec.

La section 4 de notre RFC mentionne un certain nombre de considérations générales sur ces codes de retour. Par exemple, les autres techniques d'authentification développées ultérieurement devront ajouter leur propre code SMTP étendu, sur le modèle de ceux-ci.

Autre point, SMTP ne permet de renvoyer qu'un seul code de retour étendu. Si on a plusieurs techniques d'authentification qui ont échoué, on peut toujours utiliser le code général X.7.26 qui indique que plusieurs tests ont échoué. Mais si on a une erreur d'authentification et une erreur d'un autre type, il n'y a pas de solution propre : il faut choisir une des causes de rejet et renvoyer le code correspondant.

Et la section 5, sur la sécurité, rappelle que l'utilisation de ces codes de retour étendus est **facultative**. Si vous ne voulez **pas** révéler à vos correspondants pourquoi vous rejetez leurs messages, vous êtes libre.