RFC 9991 : Domain-Based Message Authentication, Reporting, and Conformance (DMARC) Failure Reporting

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 mai 2026

Date de publication du RFC : Mai 2026

https://www.bortzmeyer.org/9991.html

DMARC (RFC 9989 [1]) permet de demander l'envoi, par les destinataires des messages, de rapports indiquant les éventuels problèmes notés, afin de diminuer le nombre de faux positifs (messages légitimes incorrectement considérés comme invalides). Cette demande de rapports se fait en ajoutant l'option `ruf` à l'enregistrement DMARC. Ce RFC décrit ces rapports.

Il y a au moins deux raisons de demander ces rapports :

— Comprendre pourquoi certains des messages qu'on envoie sont classés comme invalides alors qu'ils ne devraient pas l'être. On va donc analyser des rapports concernant des messages qu'on a réellement envoyés.
— Détecter les tentatives d'usurpation du domaine. On va donc analyser des rapports concernant des messages qu'on ne connaissait pas, et qu'un méchant a envoyés.

Notez qu'il existe aussi des rapports agrégés (RFC 9990, avec un format très différent, fondé sur XML) et qu'on demande parfois des rapports individuels parce qu'on note dans les rapports agrégés qu'il y a beaucoup d'erreurs et qu'on voudrait comprendre leur origine.

Le format normalisé ici dérive du format ARF ("*Abuse Reporting Format*", RFC 6591), qui décrivait les rapports pour les problèmes SPF et DKIM. L'option `ruf` dans l'enregistrement DMARC (RFC 9989, section 4.7) indique à quelle adresse de courrier le rapport doit être envoyé. Voici par exemple l'enregistrement DMARC de `afnic.fr` :

```
dig +short _dmarc.afnic.fr TXT
"v=DMARC1; p=quarantine; pct=100; ruf=mailto:dmarc-feedback@afnic.fr; rua=mailto:dmarc-feedback@afnic.fr; fo=1"
```

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc9989.txt`

Vous voyez le `ruf` ? Il indique que les rapports doivent être envoyés à `dmarc-feedback@afnic.fr`. Attention, j'ai écrit « doivent » mais, évidemment, les récepteurs de courrier ne sont **pas** obligés d'envoyer ces rapports, qui peuvent leur coûter des ressources et poser des problèmes de vie privée.

Pour DMARC, notre RFC ajoute au format du RFC 6591 les champs (section 4, ils sont listés dans un registre IANA <`https://www.iana.org/assignments/marf-parameters/marf-parameters.xml#marf-parameters-1`>) :

— `Identity-Alignment:`, qui liste les mécanismes d'authentification où il n'y a pas d'alignement avec l'expéditeur,
— `Delivery-Result:`,
— `DKIM-Domain:`, et quelques autres au sujet de DKIM,
— `SPF-DNS:`.

Il y a un autre piège avec les rapports, c'est la possibilité d'indiquer dans `ruf` l'adresse de quelqu'un d'autre, pour l'embêter avec beaucoup de rapports qui ne le concernent pas. La section 4 du RFC 9990 explique les précautions que devrait prendre un receveur de courrier avant d'envoyer un rapport vers une adresse qui n'est pas dans le domaine concerné, comme de tester le sous-domaine `_report._dmarc`. (Dans l'exemple `afnic.fr` plus haut, il n'y avait pas de problème, le destinataire des rapports est dans le domaine concerné.)

J'ai mentionné un peu plus haut la question de la vie privée. Les rapports détaillés, contrairement à leurs copains agrégés du RFC 9990, peuvent être très indiscrets, notamment parce qu'ils contiennent souvent des données personnelles, par exemple dans les champs indiquant l'expéditeur et le destinataire. Et il ne suffit pas de se dire « Bon, de toute façon, le gestionnaire du système envoyeur avait accès au message quand il est parti de son système » car le message a pu être transmis et re-transmis et le rapport donnera des informations sur des destinataires finaux. Une section 7, trés détaillée, couvre donc ce problème. Elle note par exemple que beaucoup de gros receveurs de courrier n'envoient pas du tout de rapport individuel, seulement des rapports agrégés. Et elle recommande que, même si on envoie les rapports, on en supprime les éléments les plus sensibles (voir le RFC 6590).

Enfin, à envoyer un rapport par message, on noiera l'expéditeur supposé sous des rapports qui concerneront des spams envoyés en nombre. Donc, prudence.

Un point amusant, que je vois pour la première fois dans un RFC : ce RFC 9991 recommande de modifier les URL présents dans les rapports en remplaçant `http` par `hxxp`. Cette convention est assez courante dans le monde de la sécurité Internet, pour éviter qu'un humain ne clique trop vite sur un lien malveillant.

L'annexe A du RFC donne un exemple de rapport, je ne montre ici que la partie MIME qui concerne le rapport proprement dit[Caractère Unicode non montré [2]] :

```
--=_mime_boundary_
Content-Type: message/feedback-report
Content-Transfer-Encoding: 7bit

Feedback-Type: auth-failure
Version: 1
User-Agent: DMARC-Filter/1.2.3
Auth-Failure: dmarc
Authentication-Results: gen.example;
  dmarc=fail header.from=consumer.example
Identity-Alignment: dkim
```

2. Car trop difficile à faire afficher par LaTeX

```
DKIM-Domain: consumer.example
DKIM-Identity: @consumer.example
DKIM-Selector: epsilon
Original-Envelope-Id: 65E1A3F0A0
Original-Mail-From: author=gen.example@forwarder.example
Source-IP: 192.0.2.2
Source-Port: 12345
Reported-Domain: consumer.example
```

Le message prétend venir de `consumer.example` mais aucune signature DKIM n'est valide, sans doute suite à des modifications chez `forwarder.example` ou bien parce que la clé DKIM n'a pu être récupérée dans le DNS.

Apparemment, OpenDKIM <`http://opendkim.org/`> est capable de générer ces rapports, mais je n'ai pas testé.