La délivrabilité e-mail

SPF, DKIM, DMARC, ??

François FREITAG

Les emplois de l'inclusion
GIP Inclusion

9 septembre 2024

Sommaire

Anatomie d'un e-mail - RFC 5322

```
Date: Tue, 3 Sep 2024 11:11:11 +0200
From: The Sender <sender@email.test>
To: me@beta.gouv.fr
Message-ID: <430617367.736715.1725348550243@uniq>
Subject: Mon message pour vous
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
Return-Path: <me@beta.gouv.fr>

Salutations de rigueur,

Le corps de l'email.

--
Moi
```

La circulation des emails

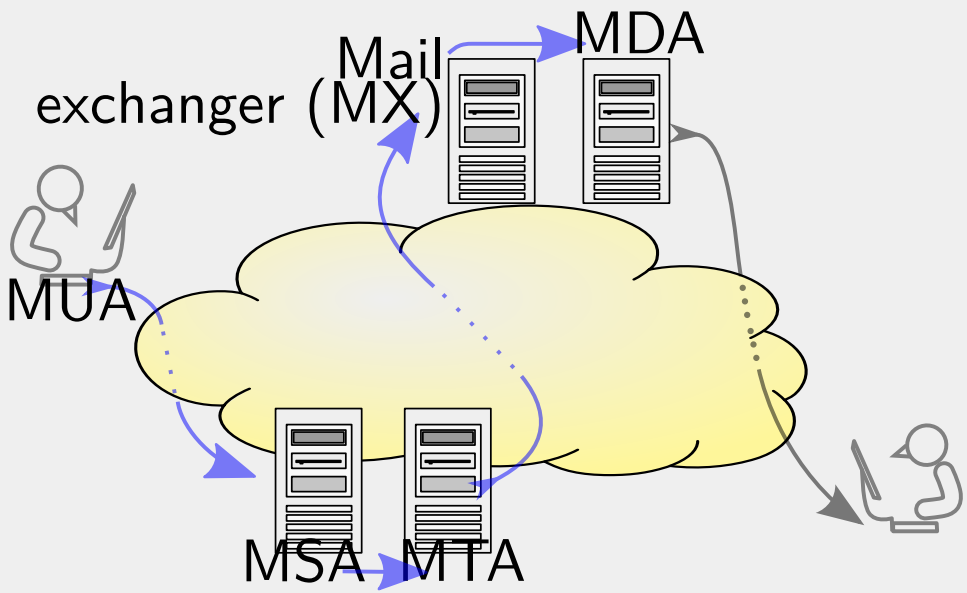

Figure – source : https://commons.wikimedia.org/wiki/File:SMTP-transfer-model.svg

MUA Mail User Agent

MSA Mail Submission Agent

MTA Mail Transfer Agent (Mail Relay)

MDA Mail Delivery Agent

MX : Mail eXchanger

Ensemble d'entrées DNS pour un domaine indiquant quels serveurs e-mail contacter, avec un ordre de priorité :

```
example.org.        MX      10 principal.example.org.
                    MX      50 secondaire.example.org.
```

Simple Mail Transfer Protocol

```
> telnet smtp.----.---- 25
< Connected to smtp.----.----.
< 220 smtp.----.---- SMTP Ready
> HELO yyyy.yyyy
< 250-smtp.----.----
< 250-PIPELINING
< 250 8BITMIME
> MAIL FROM: <auteur@yyyy.yyyy>
< 250 Sender ok
> RCPT TO: <destinataire@----.---->
< 250 Recipient ok.
> DATA
< 354 Enter mail, end with "." on a line by itself
> Subject: Test
>
> Corps du texte
> .
< 250 Ok
> QUIT
< 221 Closing connection
Connection closed by foreign host.
```

Sommaire

Histoire du spam

1978 : Email de publicité de Digital Equipment Corporation sur ARPANET par un membre du marketing

1993 : Accidentellement posté 200 messages sur Usenet, première utilisation du terme spam

1994 : Deux avocats (Canter & Siegel) embauchent un dev pour "spammer" (5 500 messages) Usenet avec une pub pour la lotterie pour l'obtention d'une green card.
$\Rightarrow$\$100-200K

Premier spam à succès

```
Path: gmd.de!urmel.informatik.rwth-aachen.de!newsserver.rrzn.uni-hannover.de!hrz-ws11.hrz.uni-kassel.de!news.th-darmstadt.de!fauern!zib
From: ni...@indirect.com (Laurence Canter)
Newsgroups: alt.bonehead.paul-hendry,alt.online-service.america-online
Subject: Green Card Lottery- Final One?
Date: 12 Apr 1994 07:40:23 GMT
Organization: Canter & Siegel
Lines: 34
Message-ID: <2odj97$25f@herald.indirect.com>
NNTP-Posting-Host: id1.indirect.com

Green Card Lottery 1994 May Be The Last One!
THE DEADLINE HAS BEEN ANNOUNCED.

The Green Card Lottery is a completely legal program giving away a
certain annual allotment of Green Cards to persons born in certain
countries. The lottery program was scheduled to continue on a
permanent basis.  However, recently, Senator Alan J Simpson
introduced a bill into the U. S. Congress which could end any future
lotteries. THE 1994 LOTTERY IS SCHEDULED TO TAKE PLACE
SOON, BUT IT MAY BE THE VERY LAST ONE.

PERSONS BORN IN MOST COUNTRIES QUALIFY, MANY FOR
FIRST TIME.

The only countries NOT qualifying  are: Mexico; India; P.R. China;
Taiwan, Philippines, North Korea, Canada, United Kingdom (except
Northern Ireland), Jamaica, Domican Republic, El Salvador and
Vietnam.

Lottery registration will take place soon.  55,000 Green Cards will be
given to those who register correctly.  NO JOB IS REQUIRED.

THERE IS A STRICT JUNE DEADLINE. THE TIME TO START IS
NOW!!

For FREE information via Email, send request to
cs...@indirect.com


--
*****************************************************************
Canter & Siegel, Immigration Attorneys
3333 E Camelback Road, Ste 250, Phoenix AZ  85018  USA
cs...@indirect.com    telephone (602)661-3911  Fax (602) 451-7617
```

Le nom spam

Un sketch des Monty Python

Lutter contre le spam

Impossible d'authentifier l'expéditeur :

Lutter contre le spam

Impossible d'authentifier l'expéditeur :

- Standards d'authentification non implémentés
- Les MTA font des erreurs très diverses
- Les MTA ne sont pas mis à jour

Lutter contre le spam

Impossible d'authentifier l'expéditeur :

- Standards d'authentification non implémentés
- Les MTA font des erreurs très diverses
- Les MTA ne sont pas mis à jour

$\Rightarrow$ **On abandonne ?**

Lutter contre le spam

Impossible d'authentifier l'expéditeur :

- Standards d'authentification non implémentés
- Les MTA font des erreurs très diverses
- Les MTA ne sont pas mis à jour

$\Rightarrow$ **On abandonne ?**

$\Rightarrow$ $\Rightarrow$ Mécanismes **optionnels** pour authentifier l'expéditeur.

Sommaire

RFC 7208 - Section 3

« An SPF record is a DNS record that declares which hosts are, and are not, authorized to use a domain name for the "HELO" and "MAIL FROM" identities. »

Enregistrement SPF

```
$ dig +short TXT inclusion.beta.gouv.fr
"v=spf1 include:spf.mailjet.com "
  "include:spf.sendinblue.com "
  "include:_spf.alwaysdata.com "
  "include:_spf.google.com "
  "include:mail.zendesk.com "
  "?all"
```

"+" **pass** (default, can be omitted), authorized

"-" **fail** not authorized (discouraged)

"~" **softfail** probably not authorized

"?" **neutral** not asserting whether the IP address is authorized

Exemples d'include

```
$ dig +short TXT spf.mailjet.com
"v=spf1 ip4:87.253.232.0/21 ip4:185.189.236.0/22 "
        "ip4:185.211.120.0/22 ip4:185.250.236.0/22 "
        "~all"
```

```
dig +short TXT _spf.alwaysdata.com
"v=spf1 ip4:185.31.40.0/22 ip4:188.72.70.0/24 "
    "ip4:78.142.219.0/24 "
    "ip6:2a00:b6e0::/32 ip6:2001:41d0:8:4734:1::1/64 "
    "ip4:176.31.58.20 ip4:176.31.58.21 "
    "ip4:176.31.58.22"
```

« If none of the mechanisms match [...] then [...] "neutral", just as if "?all" were specified as the last directive. »

Validation SPF (simplifiée)

1. Lire l'adresse IP de l'expéditeur
2. Lire `<DOMAIN>` depuis `MAIL FROM:`
3. `dig TXT <DOMAIN> | grep spf`
4. Vérifier la correspondance entre l'IP de l'étape 1. et la politique SPF

SPF bypass

« SPF uses the `rfc5321.MailFrom` address to determine the 'sender domain', which is where the SPF policy is fetched from.

However, the `rfc5321.MailFrom` address is not visible to the receiver, who only sees the `rfc5322.From` address as the sender. The flaw here is that the 'sender domain' and the domain used in the sender's email address do not have to match. »

```
telnet target.mailserver.com 25
helo attackerdomain.com
mail from: attacker@attackerdomain.com  <--- MAIL FROM matches HELO: OK
rcpt to: target@target.com
data  <--- Everything from here down is presented to the user.
from: "Sender, Legitimate" <Legitimate_Sender@spoofed.com>
to: target@target.com.au
subject: Presentation - Email Demo
This is a test

.
```

SPF lookup limit

Maximum 10 requêtes DNS pour une validation SPF.

```
$ dig +short TXT _spf.google.com
"v=spf1 include:_netblocks.google.com "
    "include:_netblocks2.google.com "
    "include:_netblocks3.google.com ~all"
```

SPF lookup limit

Maximum 10 requêtes DNS pour une validation SPF.

```
$ dig +short TXT _spf.google.com
"v=spf1 include:_netblocks.google.com "
    "include:_netblocks2.google.com "
    "include:_netblocks3.google.com ~all"
```

4 requêtes.

```
$ dig +short TXT bnc3.mailjet.com
"v=spf1 a include:spf.mailjet.com -all"
```

SPF lookup limit

Maximum 10 requêtes DNS pour une validation SPF.

```
$ dig +short TXT _spf.google.com
"v=spf1 include:_netblocks.google.com "
    "include:_netblocks2.google.com "
    "include:_netblocks3.google.com ~all"
```

4 requêtes.

```
$ dig +short TXT bnc3.mailjet.com
"v=spf1 a include:spf.mailjet.com -all"
```

2 requêtes.

SPF relaying

« A relaying SMTP service relays (forwards) all incoming email to a different domain. Relaying services are common for organizations that have multiple domains.

For example: all emails from `old-company-name.com` may automatically be relayed to `new-company-name.com`. »

Après un relai, toutes les vérifications SPF échouent.

Sommaire

DomainKey Identified Mail

« DomainKeys Identified Mail (DKIM) permits a person, role, or organization that owns the signing domain to claim some responsibility for a message by associating the domain with the message. »

[...]

« Assertion of responsibility is validated through a cryptographic signature and by querying the Signer's domain directly to retrieve the appropriate public key. »

Enregistrement DKIM

Selector : `name._domainkey.example.org`

```
$ dig +short TXT ovhex1077009-selector1._domainkey.beta.gouv.fr
"v=DKIM1; k=rsa; t=s; "
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3[...]wIDAQAB;"
```

- `v` Version
- `k` Key type
- `p` Public key
- `t` Flags

Header email DKIM

```
DKIM-Signature: v=1; a=rsa-sha256; d=beta.gouv.fr; s=ovhex1077009-selector1;
 c=relaxed/relaxed; t=1725378012; h=from:to:subject:date;
 bh=8MRBsVcw7gmBo1jQwq9N6SM3OuP0FrywUxo3X3oBDW0=;
    b=G3S65gh+sW52q/ryL/iHWlOjwp2MBxtA6LHier[...]Ug==
```

- `v` Version
- `a` Algorithm to compute the digital signature
- `d` Sender domain
- `s` Selector to lookup the public key
- `c` Canonicalization (`header/body`)
- `t` Signature timestamp
- `h` Signed header fields
- `bh` Hash of the canonicalized body
- `b` Signature data (generated from `h` and `bh`, signed with private key)

relaxed header canonicalization (simplifiée)

1. Convertir le nom des headers en minuscules
2. Joindre les lignes de continuation des headers
3. Remplacer les espaces consécutifs par un seul espace
4. Supprimer les espaces de fin de ligne
5. Supprimer les espaces autour du séparateur de header (:)

Validation DKIM (simplifiée)

1. Verifier que `From:` correspond au `domain (d=)`
2. `dig TXT <selector (s=)>.<domain (d=)>`
3. Canonicaliser, tronquer (`l=`, mailing lists) et hasher le body

3bis. `body-hash = hash-alg (canon-body, l-param)`

4. Collecter et canonicaliser les headers du mail (`h=`)
5. Vider le contenu du champ signature de `DKIM-Signature b=`

5bis. `data-hash = hash-alg (h-headers, D-SIG, body-hash)`

6. `signature = sig-alg (d-domain, selector, data-hash)`

Sommaire

DMARC

« Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a scalable mechanism by which a mail-originating organization can express domain-level policies and preferences for message validation, disposition, and reporting, that a mail-receiving organization can use to improve mail handling. »

Enregistrement DNS

```
$ dig +short TXT _dmarc.inclusion.beta.gouv.fr
"v=DMARC1;p=none;"
"rua=mailto:dmarc@inclusion.beta.gouv.fr,"
    "mailto:dmarc@mailinblue.com!10m;"
"ruf=mailto:dmarc+forensics@inclusion.beta.gouv.fr,"
    "mailto:dmarc@mailinblue.com!10m"
```

`v` Version

`p` Requested policy {`none`, `quarantine`, `reject`}

`pct` Apply policy to `pct` (%) messages

`rua` Send aggregated reports to these addresses

`ruf` Send failure reports to these addresses

`adkim` DKIM alignment {`strict`,`relaxed`}

`aspf` SPF alignment {`strict`,`relaxed`}

`fo` failure option (dans quel cas rapporter les erreurs ?)

Gestion des sous-domaines

- La politique DMARC est héritée du domaine parent
- Alignement SPF (`From:` et `Return-Path`)

  strict uniquement le domaine expéditeur
  relaxed autorise également les sous domaines
- Alignement DKIM (`From:` et `DKIM-signature: d=`)

  strict le `FQDN`
  relaxed l'`organizational domain`

SPF alignment ?

```
MAIL FROM: <sender@example.com>

From: sender@example.com
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.org
Subject: here's a sample
```

SPF alignment ?

```
MAIL FROM: <sender@example.com>

From: sender@example.com
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.org
Subject: here's a sample
```

OK

SPF alignment ?

```
MAIL FROM: <sender@example.com>

From: sender@sample.net
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.org
Subject: here's a sample
```

SPF alignment ?

```
MAIL FROM: <sender@example.com>

From: sender@sample.net
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.org
Subject: here's a sample
```

KO

$\Rightarrow$ C'est ce qui a été changé en juin sur Mailjet, pour aligner le `Return-Path:` avec le `From:`.

MAIL FROM vs Return-Path:

```
Date: Tue, 3 Sep 2024 11:11:11 +0200
From: The Sender <sender@email.test>
To: me@beta.gouv.fr
Subject: Mon message pour vous
Return-Path: <me@beta.gouv.fr>

BODY
```

MAIL FROM vs Return-Path:

```
Date: Tue, 3 Sep 2024 11:11:11 +0200
From: The Sender <sender@email.test>
To: me@beta.gouv.fr
Subject: Mon message pour vous
Return-Path: <me@beta.gouv.fr>

BODY
```

« When the delivery SMTP server makes the "final delivery" of a message, it inserts a return-path line at the beginning of the mail data. This use of return-path is required; mail systems MUST support it. The return-path line preserves the information in the <reverse-path> from the MAIL command. »

DKIM alignment ?

```
DKIM-Signature: v=1; ...; d=sample.net; ...
From: sender@child.example.com
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.org
Subject: here's a sample
```

DKIM alignment ?

```
DKIM-Signature: v=1; ...; d=sample.net; ...
From: sender@child.example.com
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.org
Subject: here's a sample
```

KO

DKIM alignment ?

```
DKIM-Signature: v=1; ...; d=example.com; ...
From: sender@example.com
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.org
Subject: here's a sample
```

DKIM alignment ?

```
DKIM-Signature: v=1; ...; d=example.com; ...
From: sender@example.com
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.org
Subject: here's a sample
```

OK

Rapport DMARC RUA - header

```
<?xml version="1.0"?>
<feedback xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <version>1.0</version>
  <report_metadata>
    <org_name>Enterprise Outlook</org_name>
    <email>dmarcreport@microsoft.com</email>
    <report_id>6e504d1d4cf846868ff04235dc7e4799</report_id>
    <date_range>
      <begin>1721692800</begin>
      <end>1721779200</end>
    </date_range>
  </report_metadata>
```

Rapport DMARC RUA - Policy published

```
<policy_published>
  <domain>inclusion.beta.gouv.fr</domain>
  <adkim>r</adkim>
  <aspf>r</aspf>
  <p>none</p>
  <sp>none</sp>
  <pct>100</pct>
  <fo>1</fo>
</policy_published>
```

fo=0 report if all fail (Default)

fo=1 report if any fail (Recommended)

fo=d only DKIM failures (regardless of alignment)

fo=s only SPF failures (regarless of alignment)

Rapport DMARC RUA - OK

```
<!-- dig TXT spf.mailjet.com
    "v=spf1 ip4:87.253.232.0/21 ip4:185.189.236.0/22 "
    "ip4:185.211.120.0/22 ip4:185.250.236.0/22 ~all" -->
<row>
  <source_ip>87.253.239.91</source_ip>
  <count>10</count>
  <policy_evaluated>
    <disposition>none</disposition>
    <dkim>pass</dkim>
    <spf>pass</spf>
  </policy_evaluated>
</row>
<identifiers>
  <envelope_to>are33.com</envelope_to>
  <envelope_from>bnc3.inclusion.beta.gouv.fr</envelope_from>
  <header_from>inclusion.beta.gouv.fr</header_from>
</identifiers>
<auth_results>
  <dkim>
    <domain>inclusion.beta.gouv.fr</domain>
    <selector>mailjet</selector>
    <result>pass</result>
  </dkim>
  <spf>
    <domain>bnc3.inclusion.beta.gouv.fr</domain>
    <scope>mfrom</scope>
    <result>pass</result>
  </spf>
</auth_results>
```

Rapport DMARC RUA - SPF fail

```
<!-- dig TXT spf.mailjet.com
    "v=spf1 ip4:87.253.232.0/21 ip4:185.189.236.0/22 "
    "ip4:185.211.120.0/22 ip4:185.250.236.0/22 ~all" -->
<row>
  <source_ip>40.93.69.3</source_ip>
  <count>1</count>
  <policy_evaluated>
    <disposition>none</disposition>
    <dkim>pass</dkim>
    <spf>fail</spf>
  </policy_evaluated>
</row>
<identifiers>
  <envelope_to>adef-emploi.fr</envelope_to>
  <envelope_from>bnc3.inclusion.beta.gouv.fr</envelope_from>
  <header_from>inclusion.beta.gouv.fr</header_from>
</identifiers>
<auth_results>
  <dkim>
    <domain>inclusion.beta.gouv.fr</domain>
    <selector>mailjet</selector>
    <result>pass</result>
  </dkim>
  <spf>
    <domain>bnc3.inclusion.beta.gouv.fr</domain>
    <scope>mfrom</scope>
    <result>fail</result>
  </spf>
</auth_results>
```

Attention à la politique SPF

Les `fail` (ex. `-all`) de SPF peuvent causer l'échec d'authentification d'un email et l'arrêt immédiat de l'évaluation, **avant d'envoyer un rapport DMARC !**

Rapport DMARC - RUF

Résultats de l'authentification résultats SPF et DKIM

En-têtes de message

Contenu du message permet d'identifier l'origine du message

Détails de cryptage *optionnel*

Rapport DMARC - RUF

Résultats de l'authentification résultats SPF et DKIM

En-têtes de message

Contenu du message permet d'identifier l'origine du message

Détails de cryptage *optionnel*

Mais presque pas utilisé :

- **Confidentialité** l'administrateur du domaine suit les messages
- **Sécurité** un acteur malveillant peut inonder la boîte RUF (1 rapport/erreur)

Sommaire

Réputation

Chacun pour soi... souvent basé sur les adresses IP émettrices.
Un exemple de service : https://emailrep.io

- Data breach
- First seen
- Last seen
- Domain exists
- Domain reputation
- Days since domain creation
- Suspicious TLD
- Free provider
- Malicious activity
- SPF record
- DKIM record
- DMARC record

Réputation inclusion.beta.gouv.fr


```
{
    "email": "tech@inclusion.beta.gouv.fr",
    "reputation": "low",
    "suspicious": true,
    "references": 0,
    "details": {
        "blacklisted": false,
        "malicious_activity": false,
        "malicious_activity_recent": false,
        "credentials_leaked": false,
        "credentials_leaked_recent": false,
        "data_breach": false,
        "first_seen": "never",
        "last_seen": "never",
        "domain_exists": true,
        "domain_reputation": "low",
        "new_domain": false,
        "days_since_domain_creation": 3115,
        "suspicious_tld": false,
        "spam": false,
        "free_provider": false,
        "disposable": false,
        "deliverable": true,
        "accept_all": false,
        "valid_mx": true,
        "primary_mx": "mx1.alwaysdata.com",
        "spoofable": true,
        "spf_strict": false,
        "dmarc_enforced": false,
        "profiles": []
    }
}
```

Amélioration effectuées

04 juillet 2024 Envoi des rapports DMARC à tech@inclusion.beta.gouv.fr (source)

04 juillet 2024 Demande à Mailjet d'envoyer avec bnc3.inclusion.beta.gouv.fr (source)

05 juillet 2024 Envoi depuis bnc3.inclusion.beta.gouv.fr (source)

24 juillet 2024 Envoi des rapports DMARC à une boîte mail dédiée (source)

25 juillet 2024 Ajout de include:spf.mailinblue.com au SPF (source)

30 juillet 2024 Ajout des ruf à la politique DMARC (source)

30 juillet 2024 Ajout du sélecteur Zendesk à la politique DKIM (source)

02 octobre 2024 Ajout de include:bnc3.inclusion.beta.gouv.fr au SPF (source)

08 octobre 2024 Remplacement de include:spf.sendinblue.com dans le SPF par include:spf.brevo.com (source)

09 octobre 2024 Retrait des ruf de la politique DMARC (source)

14 octobre 2024 Ajout de include:spf.sendinblue.com au SPF (source)

14 octobre 2024 Ajout de include:spf.tipimail.com au SPF (source)

15 octobre 2024 Ajout de include:spf.brevo.com au SPF de mon-recap, data-inclusion.

Améliorer cette réputation ?

Améliorer cette réputation ?

1. SPF :

```
$ dig +short TXT inclusion.beta.gouv.fr
"v=spf1 include:spf.mailjet.com [...] ?all"
```

Améliorer cette réputation ?

1. SPF :

```
$ dig +short TXT inclusion.beta.gouv.fr
"v=spf1 include:spf.mailjet.com [...] ?all"
```

2. DMARC :

```
$ dig +short TXT _dmarc.inclusion.beta.gouv.fr
"v=DMARC1;p=none;rua=[...]"
```

Merci de votre attention

Avez-vous des questions ?