L'email

(vaste sujet)

L'email (vaste sujet)

Wishlist

Formats
(mime, mbox, maildir,
quoted-printable, base64
s-mime, openpgp)

Protocoles
(smtp, imap,
pop, sieve, ssl/tls)

Interactions
(wrapper, dkim,
spf, arf, bounce, dns)

Acteurs
(caramail, microsoft,
ibm, yahoo,
IETF, mandrill, emailvision,
return-path, spamhaus ...)

Logiciels
(sendmail, procmail,
Postfix, thunderbird,
roundcube, mail, outlook...)

La base : l'adresse email

qqchose @ domaine

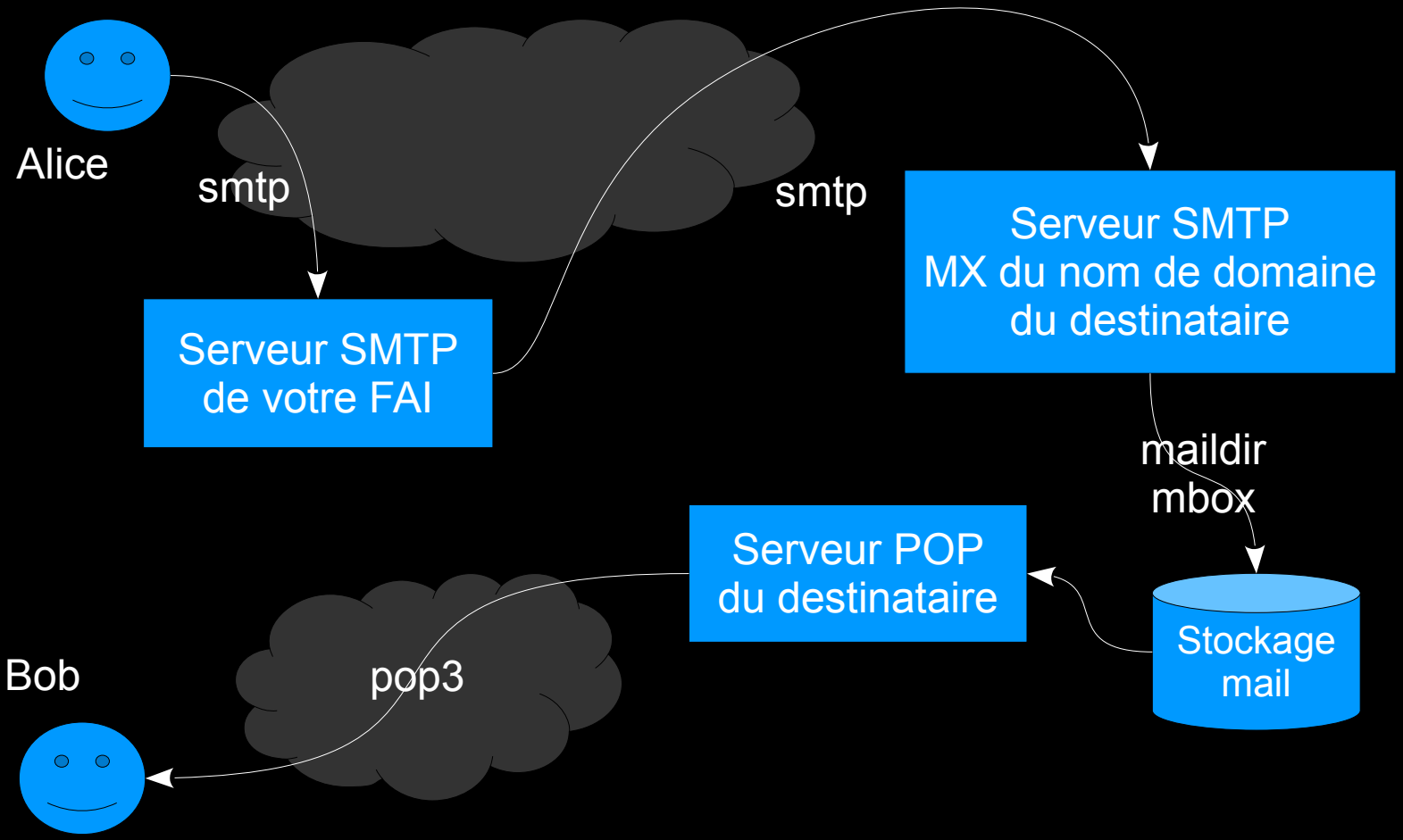
Exemple :

benjamin@sonntag.fr

noc@museum

"félix le [chat]"@eu.org

La base : SMTP / POP3



Exemple de session SMTP simple

```
benjamin@mg:~$ telnet alice  smtp     (25)
Trying 2001:67c:288::6...
Connected to alice.sonntag.fr.
Escape character is '^]'.
     220 alice.sonntag.fr ESMTP
HELO mg.sonntag.fr
     250 alice.sonntag.fr
MAIL FROM: benjamin@sonntag.fr
     250 2.1.0 Ok
RCPT TO: skhaen@cyphercat.eu
     250 2.1.5 Ok
DATA
     354 End data with <CR><LF>.<CR><LF>
From: <benjamin@sonntag.fr>
To: <skhaen@cyphercat.eu>
Subject: Test de mail pour la conférence du 7/02/2014

Salut Guillaume,
ce n'est qu'un test, merci de l'ignorer.
@+
Benjamin
.
     250 2.0.0 Ok: queued as 2E73F9A508C62
QUIT
     221 2.0.0 Bye
Connection closed by foreign host.
```

IMPORTANT
Apprendre la différence

Entre FROM d'enveloppe
Et FROM MIME

Ainsi que RCPT TO
Et TO/CC MIME

RFC 2821

Exemple de session POP3 simple

```
benjamin@mg:~$ telnet alice  pop3      (110)
Trying 2001:67c:288::6...
Connected to alice.sonntag.fr.
Escape character is '^]'.
+OK Hello there.
USER test@sonntag.fr
+OK Password required.
PASS test
+OK logged in.
UIDL
+OK
1 UID305-1224498663
2 UID306-1224498663
.
RETR 1
+OK 1879 octets follow.
  ** blablabla **
Subject: test de mail
From: benjamin@sonntag.fr
To: test@sonntag.fr
Message-Id: <20131112190435.C68325A4310@mg.sonntag.fr>
Date: Tue, 12 Nov 2013 20:04:28 +0100 (CET)

Bonjour test !
.
QUIT
+OK Bye-bye.
Connection closed by foreign host.
```

RFC 1939

Après POP3,
IMAPv4, pour synchroniser sa boite

IMAPv4 port TCP/143 (et TCP/SSL/993)

- synchronisation de dossiers de boite mail

- modulaire, extensible

- gestion d'abonnement aux dossiers

- permet la recherche côté serveur

- meilleure compatibilité avec les webmails (roundcube, mailpile...)

- permet l'envoi de mail (que personne n'utilise ;))

RFC 3501

Filtrage côté serveur avec Sieve & ManageSieve

RFC 5228

```
require ["vacation"];
require ["fileinto"];
# rule:[absence]
if true
{
vacation :days 15 :subject "Absence du bureau" text:
Bonjour,
Je serai en congé maternité jusqu'à la mi-septembre.
En mon absence, vous pouvez contacter ma collègue Ève
À bientôt,
Alice
.
;
}

# rule:[spammeur]
if header :contains "From" "mailingpro.fr"
{
     fileinto "Junk";
}
```

Filtrage côté serveur avec Sieve & ManageSieve

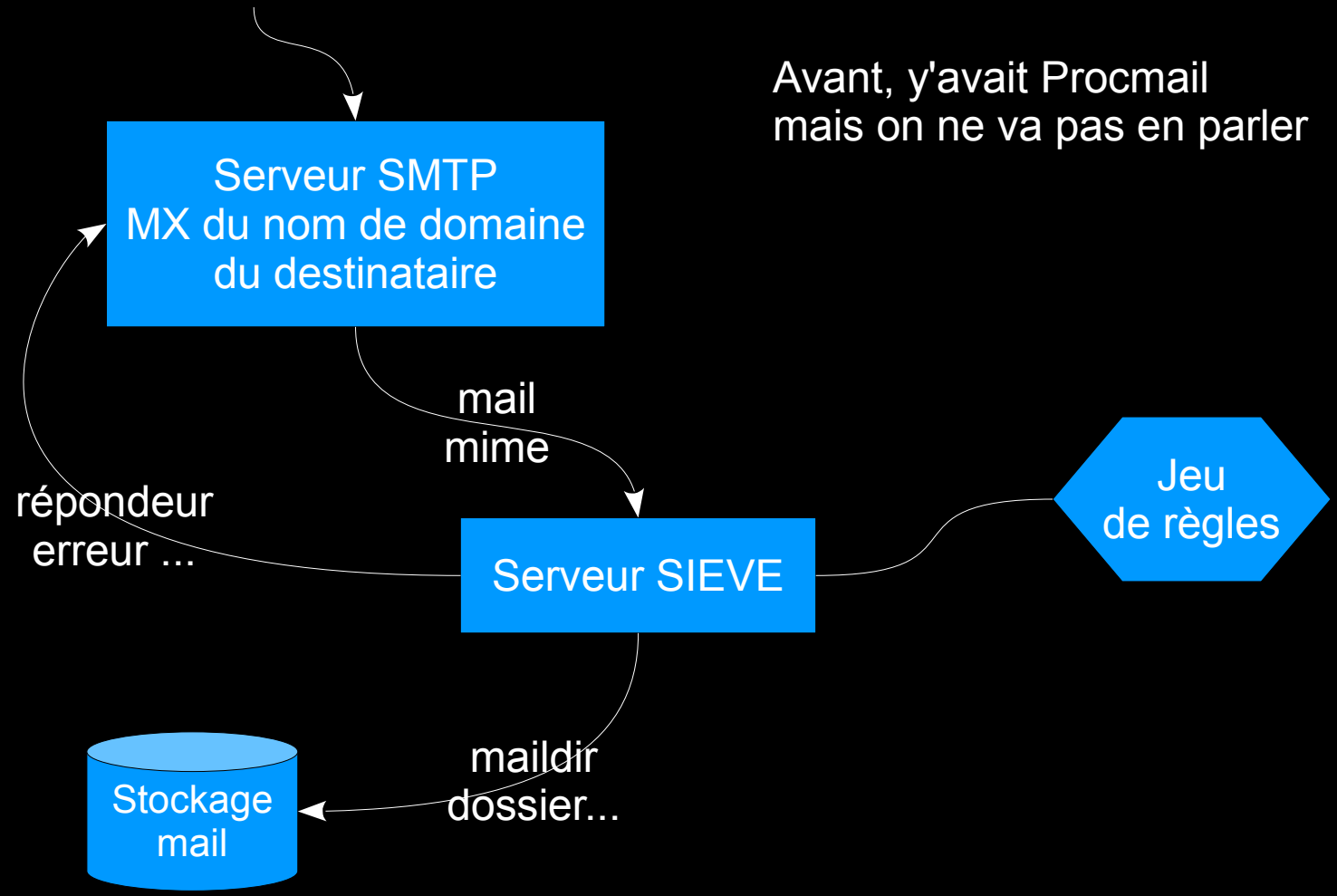
```
benjamin@mg:~# telnet localhost sieve
(4190)
Trying ::1...
Connected to localhost.
Escape character is '^]'.
"IMPLEMENTATION" "Dovecot Pigeonhole"
"SIEVE" "fileinto reject envelope encoded-
character vacation subaddress comparator-
i;ascii-numeric relational regex
imap4flags copy include variables body
enotify environment mailbox date ihave"
"NOTIFY" "mailto"
"SASL" "PLAIN LOGIN"
"STARTTLS"
"VERSION" "1.0"
OK "Dovecot ready."
```

```
AUTHENTICATE "PLAIN" "dGVzdEBvY3RvcHVjZS5mciB0ZXN0Cg=="
OK "Logged in."
LISTSCRIPTS
"managesieve" ACTIVE
OK "Listscripts completed."
GETSCRIPT "managesieve"
{105}
require ["fileinto"];
# rule:[spammeur]
if header :contains "From" "mailingpro.fr"
{
     fileinto "Junk";
}

OK "Getscript completed."
LOGOUT
OK "Logout completed."
Connection closed by foreign host.
```

RFC 5804

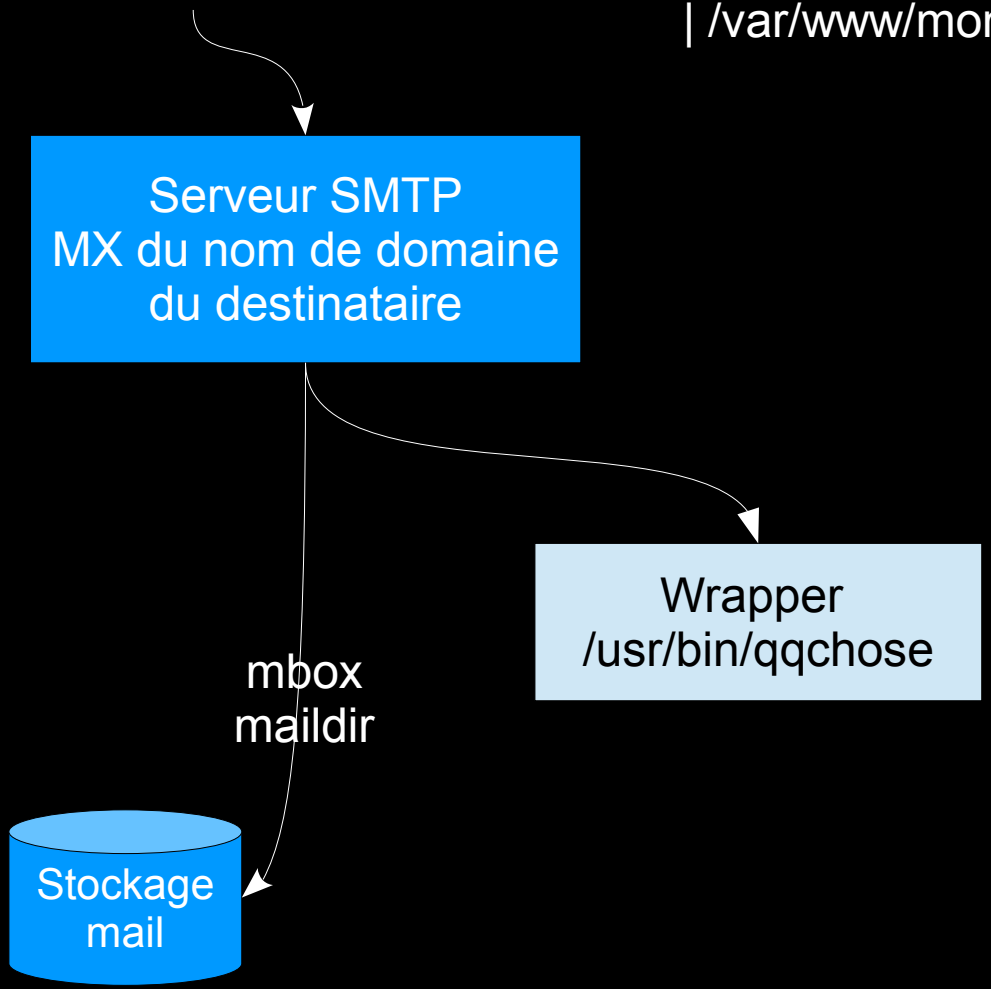
Filtrage côté serveur avec Sieve & ManageSieve



Avant, y'avait Procmail
mais on ne va pas en parler

Les Wrappers

| /usr/bin/procmail
| /usr/lib/mailman/bin/send
| /var/www/monsite/support.php



Et SSL/TLS dans tout ça ?!

- SMTP +SSL existe (port 465) mais n'est pas utilisé

- SMTP +TLS existe (sur port 25 ou 587) et est **très** utilisé et vivement conseillé

- POP (TCP/110) & IMAP (TCP/443) existent en SSL
  - POP3ssl sur le port TCP 995
  - IMAP4ssl sur le port TCP 993

  Ont été très utilisé (notamment disponible sous Outlook & Express depuis toujours)
  Le sont de moins en moins au profit de STARTTLS sur port standard (110/143)

- ManageSieve (4190) supporte STARTTLS nativement

→ **Il est important de bien configurer ses serveurs ! (SSL Labs-style)** ←

Et PGP ?

- inventé pour être utilisé avec le mail
- initialement utilisé « inline » avec en-têtes et pied de mail signalant le bloc PGP
  > ne chiffre / signe donc ni le sujet ni les pièces jointes

- depuis, OpenPGP est une RFC qui normalise PGP pour Internet
  > définit donc PGP/MIME pour protéger aussi sujet et pièce jointes

- utilisable ?
  Thundebird avec enigmail,
  Mutt nativement (mais sans règle « par destinataire »)
  Kmail, Claws mail nativement
  Outlook avec greffon (libre ou propriétaire) (rappel crypto sur os non libre ;))

→ exemple de mail pgp inline ←
→ exemple de mail pgp/mime ←

L'email (vaste sujet)

Et PGP ?

```
From - Wed Feb 05 22:00:40 2014
Message-ID: <52F2A676.4020705@laquadrature.net>
Date: Wed, 05 Feb 2014 22:00:38 +0100
From: "Benjamin Sonntag" <bs@laquadrature.net>
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:17.0) Gecko/20131103 Icedove/17.0.10
MIME-Version: 1.0
To: Guillaume Lecoquierre <skhaen@cyphercat.eu>
Subject: test mail pgp inline
X-Enigmail-Version: 1.5.1
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: quoted-printable

-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG v1.4.12 (GNU/Linux)
Comment: Using GnuPG with Icedove - http://www.enigmail.net/
hQIMA7h6jDeoZw5SAQ//ULWui4pTahOXOb38EwIdMGkWECx1AhYmjEaY9FVg7AT/
8Njfx/K80yAqvnXLe8aOakIhaldZEHxZbGgEJVZglBypfuhGDHB9ruWUcHppKdlw
5mr0mZxmaWkKnEblmV7LtEy35ZFegBdY+fBfGnxCYoYpvl2EnJfI539gcgm6cMRI
lVO3s4C4RUPhe0RaRxg8OGOEBkIY7/oA+X7PgDASd55sEZEYDXYbCLMVu2ULGtvZ
ZLFZ4fGQeHWPuVXOa95hI5aIskRq+D/FvxR6Du+wAuN60FmtfD3ZIZdp/Ld3I4o6
drKdbudA1MU2WRKmlOAXlkZwEFQWFVvixdQpVZX30sDKAe9F7OJ72V3xwwoFoXoU
QUJoe6rNXR9ZBZZ+ZBcOwsnOD+nyLzq8uH25OQvAmF834n1yzjTjzzSq7iviPp51
rYyJgdGBbz00bnX00zySeNozmSWXKPtDg8kRHDs6sPoNjqHRMh+lGiemzLZbFKtb
uMnF69XYXOS9OSZauK8ttwXXaKVNxya1Dj6tdeHTLVBskesoTsP6WN8WiSL1QLQm
piHw4inI/KpFx9B3cAcdqiVAuTDz4AIVD7rxL/ni7Bgza9mlCn9I6/q1jqkhw+u0
lNqIHl5OwOU/WW18xlie8Q5u1X+YmX3HTCnVnr7RWsr9ek7EEuaJKPxK8MmHMYXS
9ek7KjRQx8GUO2y6gRiYGjHngDwqfNuB6vLJg2T81Chsb3h35uxpNhNHWuwJa5r7
6qxgrFZXhe9EwFdk8bdG6j/01By3PtwCgjQdsDecaQTFZD1v2ZPh9rY9He99jQ5+
jdyIIUKpt6fN183tGH2mM602LH2dYx/GdAgMWOPUWBsCO0+qm1nsX66V/Q=3D=3D
=3DagHk
-----END PGP MESSAGE-----
```

L'email (vaste sujet)

Et PGP ?

```
From - Wed Feb 05 22:00:56 2014
Message-ID: <52F2A687.5090401@laquadrature.net>
Date: Wed, 05 Feb 2014 22:00:55 +0100
From: "Benjamin Sonntag (La Quadrature du Net)" <bs@laquadrature.net>
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:17.0) Gecko/20131103 Icedove/17.0.10
MIME-Version: 1.0
To: Guillaume Lecoquierre <skhaen@cyphercat.eu>
Subject: test mail pgp mime
X-Enigmail-Version: 1.5.1
Content-Type: multipart/encrypted;
 protocol="application/pgp-encrypted";
 boundary="----enig2GTRFPXDDOSULBNNLFMXH"

This is an OpenPGP/MIME encrypted message (RFC 4880 and 3156)
------enig2GTRFPXDDOSULBNNLFMXH
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identification

Version: 1

------enig2GTRFPXDDOSULBNNLFMXH
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.12 (GNU/Linux)
Comment: Using GnuPG with Icedove - http://www.enigmail.net/

hQIMA7h6jDeoZw5SARAAqd+5YHqOXt2uBYCGVrTAyKVtd3eVB5jmpS04Glx++0pp
yuOUd11qNKpoSRWwMHgXAnvObFMskAChky94awoYEJk6EFsbjqNvzz+egS6j0tBe
...
X9CZkIv2+WUysaiS3VIx1giFRRcOhnk96YaClJ7mILp0RYfB0L+3lE6p6THSveEe
h10OmWb3y21JYp6hWHEruO+Btp6GAJJ++y5s0rMKCyYsiyvT7AQpFbccTrnLsfjy
H6YCuSPdASigu6kEvpQC7yGigLCHW47XJ+QiRAG9RAcRLmTXONKoukX4pIN3CS4d
T+I=
=d4lL
-----END PGP MESSAGE-----

------enig2GTRFPXDDOSULBNNLFMXH--
```

Et PGP ?

```
From - Wed Feb 05 22:01:11 2014
Message-ID: <52F2A696.9010403@laquadrature.net>
Date: Wed, 05 Feb 2014 22:01:10 +0100
From: "Benjamin Sonntag (La Quadrature du Net)" <bs@laquadrature.net>
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:17.0) Gecko/20131103 Icedove/17.0.10
MIME-Version: 1.0
To: Guillaume Lecoquierre <skhaen@cyphercat.eu>
Subject: test mail signature only
X-Enigmail-Version: 1.5.1
Content-Type: multipart/signed; micalg=pgp-sha256;
 protocol="application/pgp-signature";
 boundary="----enig2KMHGRCXGSUCIPLWEXTQC"

This is an OpenPGP/MIME signed message (RFC 4880 and 3156)
------enig2KMHGRCXGSUCIPLWEXTQC
Content-Type: text/plain; charset=windows-1252
Content-Transfer-Encoding: quoted-printable

contenu du mail pgp signature only

------enig2KMHGRCXGSUCIPLWEXTQC
Content-Type: application/pgp-signature; name="signature.asc"
Content-Description: OpenPGP digital signature
Content-Disposition: attachment; filename="signature.asc"

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.12 (GNU/Linux)

iQEcBAEBCAAGBQJS8qaWAAoJEP6CnA9YYHPmAIwIAKwDwETVhkzFj47EA3RRNkmi
pGVjmdLt8K+5KyTEcaLoQf81N0B1x5TXsE6JeweQuS6padqu4ARfrc+ryFixhYfG
+i2kcic5wHBrlIy/+00sGrqhdT+JKgMdkM/8rz/XB72J8KUgkj6NTp4ELj6zmSsq
NUvzRyg+HJq/k5J24/wbK/4EGn1H3rqwofihcz0iZ2wIXCjTOMjYw7B4uOizZlvT
MFXDi2d1Ykf6f7B8NH0LvygsppO58qMIAq57JE6Wg7VHpwvVEBa7PbP/4ypnu8oB
+Hov+yZIzo7dvyRyDnDS9Cl1fMY4ZcUQQRTN7g/DOcLmVs4BXrOgEVlybjn6YkY=
=3dAC
-----END PGP SIGNATURE-----

------enig2KMHGRCXGSUCIPLWEXTQC--
```

RFC 4880

Pourquoi mon FAI bloque-t-il le port 25 SMTP ?

- À cause des virus et malware qui envoient du SPAM au MX des domaines concernés

- C'est tolérable si désactivable sans frais par l'abonné (ex free)

- Dans tous les cas, on peut utiliser le port Submission (SMTP sur port TCP/587)
  Pour relayer ses mails à travers son fournisseur de mail (+ STARTTLS)

- Le détournement du port 25 n'est **jamais** tolérable et doit être dénoncé comme une atteinte à la neutralité du net, au secret de la correspondance...

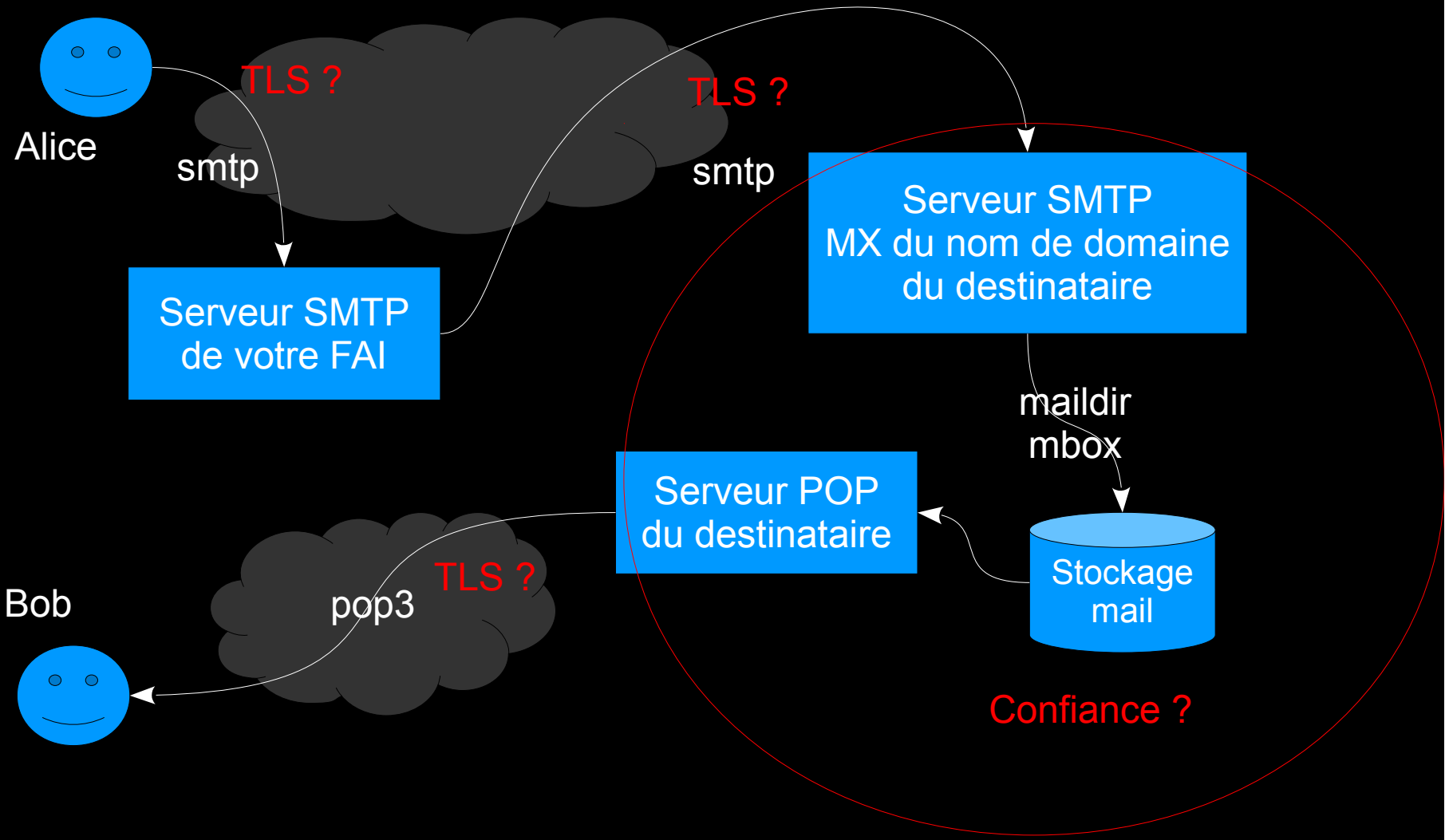
Quelles niveau de confidentialité ?

- si SSL ou STARTTLS, tout passe chiffré sur le réseau
  - mais les 2 extrémités : vous et votre fournisseur de mail savent qui écrit à qui
  - et le SMTP de votre fournisseur envoyant au SMTP du destinataire
  peut faire passer le mail en clair

- sinon si authentification sécurisée (cram-md5) le mot de passe passe chiffré
  Mais tous les mails passent en clair !!

- dans tous les cas, une confiance forte dans les fournisseurs est requise (bof ;( )
  Et même PGP ne protège pas l'écoute des metadonnées :
  - qui écrit à qui
  - quand
  - quel volume

Quelles niveau de confidentialité ? (dessin en pratique)



Quels formats de stockage du mail sur les serveurs ?

(Le format MIME est « un mail », on l'étudiera plus loin.)

- Le format Mailbox ou Mbox est un ensemble de mails MIME mis bout à bout,
Comme suit :

```
From <expéditeur> <date> \r\n
<le mail MIME>
...
```

(exemple sur ma machine locale : less /var/mail/benjamin)

- Le format Maildir est un dossier dans lequel on stocke un fichier par mail
  - avec 3 sous-dossiers tmp cur et new (les nouveaux dans new, les lus dans cur)
  - généralement nommé avec un GUUID + les attributs imap (lu, répondu etc.)

(exemple sur ma machine locale : find ~/Maildir/)

Quels formats de stockage du mail sur les serveurs ?

→ **Avantages et inconvénients des 2 structures** ←

→ **qui utilise quoi ?** ←

Autres formats spécifiques voire propriétaires :
- PST outlook
- Storage Zimbra, Exchange, Lotus
- Maildirs spécifiques avec index (dovecot, cyrus...)

Le format MIME (warning : nightmare ahead !)

- format texte historiquement encodé en ASCII 7 bits (?!)
- contient des en-têtes sous la forme
  Header-name : Content \n (et pas \n !)
- puis une ligne vide
- puis le contenu

```
Subject: test d' mail
From: benjamin@sonntag.f
To: tes nntag.fr
Messag Id: 20131112190435.C68325A431 @m s nntag.fr>
Date: Tue, 12 N v 2013 20:04:28 +0 0 (CE )

Bonjour test
.
```

RFC 2045
RFC 2046
RFC 2047
RFC 2048

Le format MIME (suite)

- en-têtes spécifique pour du contenu encodé en 8 bits
  Content-Type: text/plain; charset=UTF-8

- gestion des structures complexes via multipart :

  - pièces jointes
    Content-Type: multipart/mixed; boundary="WIyZ46R2i8wDzkSu"
    Et plus bas
    --WIyZ46R2i8wDzkSu
    Content-Type: application/pdf
    Content-Disposition: attachment; filename="acta-leak.pdf"

  - formats alternatifs (html + text)
    Content-Type: multipart/alternative; boundary="WIyZ46R2i8wDzkSu"

  - cas technique (gestion des retour en erreur « bounce »)
    Content-Type: multipart/report; report-type=delivery-status; boundary="toto"

Le format MIME (fin ?)

- encodage spécifiques pour les vieux MTA/Milters & autres incapable d'UTF-8

Content-Type: text/plain
Content-Disposition: inline
Content-Transfer-Encoding: quoted-printable

- et pour les modernes :

Content-Type: text/plain; charset=utf-8
Content-Disposition: inline
Content-Transfer-Encoding: 8bit

→ **de véritables exemples** ←

SPF, la lutte contre le SPAM, premier pas d'authentification des expéditeurs

- première tentative de validation des expéditeurs
- utilisation de RR DNS pour préciser qui est autorisé à envoyer du mail

- exemple de configuration

```
$ dig txt sonntag.fr
sonntag.fr.    IN   TXT  "v=spf1 a mx a:brassens.heberge.info a:z1.sonntag.fr ?all"
```

- la chose à ne pas faire (spf strict « -all » si pas sûr)
- mettez un SPF même large si besoin

RFC 4408

(et 6686 pour les trolls)

http://www.openspf.org/SPF_Record_Syntax

DKIM, lutte contre le spam
signature numérique par les MTA

- utilisation de RR DNS pour publier les clés publiques qui signent certains en-tête des mails émis

- exemple de configuration

```
$ dig txt default._domainkey.cairn.info
;; ANSWER SECTION:
default._domainkey.cairn.info. 1800 IN TXT  "v=DKIM1\; k=rsa\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC7lmzOaaojx4ppHCIoaqX5CP92tVCij36eFh+FscPyoTQ5CimLSFAyD
hDEp0hDYA/8EZoqWvF/z3rZKp+JrypKoqpPSI3QpaJGp+ZuqJabcKjE5rgk7bUUfm9gVUnOehIM185n7xpbWkQFxmCufpJu
3wu4eqNc2YPJ5A9H9AldyQIDAQAB"
```

- les choses à ne pas faire
  - signer si DNS pas à jour (+ TTL)
  - mal signer
  - utiliser une clé RSA de 1024 bits

DKIM, lutte contre le spam
signature numérique par les MTA

Exemple de mail signé par OpenDKIM :

```
Received: from z1.sonntag.fr (LHLO z1.sonntag.fr) (91.194.60.127) by
 z1.sonntag.fr with LMTP; Tue, 4 Feb 2014 11:21:32 +0100 (CET)
Received: from localhost (localhost [127.0.0.1])
          by z1.sonntag.fr (Postfix) with ESMTP id 1814D367CFE
          for <benjamin@sonntag.fr>; Tue,  4 Feb 2014 11:21:32 +0100 (CET)
Authentication-Results: z1.sonntag.fr (amavisd-new); dkim=pass header.i=@cairn.info
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=cairn.info; s=default;
                t=1391509288; bh=HH5tAaE9VHiRV4P0LkFCUYXTnavRvFDGVoLC8aKmgnQ=;
                h=Date:From:To:CC:Subject:From;
                b=MAaQC+PRMvxUY4IMbyj20i8FOYZRKqwwNAf1YXqCaQaDVG5WGypojalULKIDVRbhM
                 +cKZ3RR0h5KojQRlSGTkIkLXQWUY12AmXRWvzYhnZvCLoq12gYUr5dwBPAT86H1lnc
                  HKSOUAbx/sBqWpWnV/8vAWzWAD/VTv9Q/NGYJvVo=
Message-ID: <52F0BF28.90192901@cairn.info>
Date: Tue, 04 Feb 2014 11:21:28 +0100
From: =?ISO-8859-1?Q?Fran=E7ois?= <francois@cairn.info>
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20100101 Thunderbird/24.2.0
MIME-Version: 1.0
To: Support Octopuce <support@sonntag.fr>
CC: Un collègue <lautre@cairn.info>
Subject: question dkim
X-Enigmail-Version: 1.6
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 8bit

Bonjour,
```

Il existe aussi sender-id
Créé par Microsoft

DMARC, synthèse de DKIM SPF & Spam feedback loop

- utilisation de RR DNS pour publier les règles applicables à un domaine

- exemple de configuration

```
$ dig txt cairn.info
;; ANSWER SECTION:
cairn.info. 1800 IN TXT  "v=DMARC1; p=reject; rua=mailto:postmaster@cairn.info;
ruf=mailto:noc@cairn.info; adkim=r; aspf=r; rf=afrf; sp=reject"
```

- les choses à ne pas faire
    - imposer des règles sans certitudes

http://www.kitterman.com/dmarc/assistant.html

http://www.dmarc.org/overview.html

DMARC, Spam feedback loop : Le format ARF

- utilisation d'un rapport par mail utilisant un type Mime particulier

```
Content-Transfer-Encoding: binary
Content-Type: multipart/report;
        boundary="_----------=_1115257449152010";
        report-type="feedback-report"
MIME-Version: 1.0
X-Mailer: MIME::Lite 3.01 (F2.73; B3.01; Q3.01)
Date: Thu, 5 May 2005 01:44:09 UT
Subject: Spammy subject
To: recipient@example.com
From: sender@example.com

This is a multi-part message in MIME format.

--_----------=_1115257449152010
Content-Disposition: inline
Content-Transfer-Encoding: 7bit
Content-Type: text/plain

This is an automated report from a badly configured system
```

RFC 5965

```
--_----------=_1115257449152010
Content-Disposition: inline
Content-Transfer-Encoding: 7bit
Content-Type: message/feedback-report

Feedback-Type: abuse
Version: 1
Source-IP: 192.168.0.1
Feedback-Agent: Just some test code (MIME::ARF V0.01)
Received-Date: Wed, 4 May 2005 18:12:41 -0700

--_----------=_1115257449152010
Content-Disposition: inline
Content-Length: 93
Content-Transfer-Encoding: binary
Content-Type: message/rfc822

To: spamrecipient@example.com
Subject: Spammy subject
From: spammer@example.com

Spammy body

--_----------=_1115257449152010--
```

Autoconfiguration des clients pop/imap/smtp ? Les bons et mauvais élèves

Outlook & Thunderbird sont dans les bons élèves :

```
$ dig txt sonntag.fr
sonntag.fr.    IN   TXT  "mailconf=https://autodiscover.sonntag.fr/mail/mailautoconfig.xml"
```

Le XML retourné permet de configurer son mail :

```
Content-type: text/xml

<?xml version='1.0' encoding='UTF-8'?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
<Response xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a">
      <Account>
      <AccountType>email</AccountType>
      <Action>settings</Action>
      <Protocol>
            <Type>IMAP</Type>       <Server>alice.sonntag.fr</Server>
            <Port>993</Port>        <LoginName><?php echo $matches[0];?></LoginName>
            <DomainName><?php echo $emailDomain[1];?></DomainName>
            <SPA>off</SPA>          <SSL>on</SSL>           <AuthRequired>on</AuthRequired>
      </Protocol>
      <Protocol>
            <Type>SMTP</Type>
            <Server>alice.sonntag.fr</Server>
            <Port>465</Port>        <SPA>off</SPA>          <SSL>on</SSL>
            <AuthRequired>on</AuthRequired>          <UsePOPAuth>on</UsePOPAuth>        <SMTPLast>off</SMTPLast>
      </Protocol>
      </Account>
</Response>
</Autodiscover>
```

Autoconfiguration des clients pop/imap/smtp ?
La norme

Une RFC précise qu'on doit utiliser des enregistrements SRV pour préciser les serveurs pop, imap, pops, imaps, smtp, submission d'un service d'email

RFC 6186

```
dig srv _imap._tcp.sonntag.fr.

; ANSWER SECTION
_imap._tcp.sonntag.fr.   SRV   5 1 143 alice.sonntag.fr.

...

_pop3._tcp.sonntag.fr.    SRV  0 0   0 .
_imaps._tcp.sonntag.fr.   SRV  0 1 993 alice.sonntag.fr.
_pop3s._tcp.sonntag.fr.   SRV  2 1 995 alice.sonntag.fr.
```

Comment remonter les traces d'un mail ?

- Received-from est notre ami \o/

- Return-Path aussi

- on retrouve souvent l'adresse IP d'un émetteur
  (parfois dans un en-tête spécifique)

- ou pas (gmail & mta anonymiseurs)

Comment remonter les traces d'un mail ?

```
Authentication-Results: z1.sonntag.fr (amavisd-new); dkim=pass
     header.i=@twitter.com
Received: from z1.sonntag.fr ([127.0.0.1])
     by localhost (z1.sonntag.fr [127.0.0.1]) (amavisd-new, port 10024)
     with ESMTP id d3KgTE1qm5p0 for <benjamin@z1.sonntag.fr>;
     Wed,  5 Feb 2014 22:24:13 +0100 (CET)
Received: from brassens.heberge.info (unknown [91.194.60.2])
     by z1.sonntag.fr (Postfix) with ESMTPS id 831ED368F23
     for <benjamin@z1.sonntag.fr>; Wed,  5 Feb 2014 22:24:13 +0100 (CET)
Received: from localhost (localhost [127.0.0.1])
     by brassens.heberge.info (Postfix) with ESMTP id 648402CE6AD99;
     Wed,  5 Feb 2014 22:24:13 +0100 (CET)
Authentication-Results: brassens.heberge.info; dkim=pass
     (1024-bit key; insecure key) header.i=@twitter.com; dkim-adsp=pass
Received: from brassens.heberge.info ([91.194.60.2])
     by localhost (brassens.heberge.info [127.0.0.1]) (amavisd-new, port 10024)
     with ESMTP id aXZpjPcJnXdO; Wed,  5 Feb 2014 22:24:12 +0100 (CET)
Received: from spruce-goose-ae.twitter.com (spruce-goose-ae.twitter.com [199.59.150.74])
     (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
     (No client certificate requested)
     by brassens.heberge.info (Postfix) with ESMTPS id 80FFF2CE6AD95
     for <twitter@sonntag.fr>; Wed,  5 Feb 2014 22:24:11 +0100 (CET)
DKIM-Signature: v=1; a=rsa-sha1; d=twitter.com; s=dkim-201303; c=relaxed/relaxed;
     q=dns/txt; i=@twitter.com; t=1391635449;
     h=From:Subject:Date:To;
     bh=Wi9DC3AbuCIkVjxsxp/xlwJ7gT8=;
     b=FIEN6l8DJ/fLaed0WYDDmAcyWYDgPrW4ueQgbL/1B+vL7VMVQH+pp5FcoE3oe/WD
     vgSl5qj+as2SLLAIlwkzELjeECfeTzFBrixe92VZNt7Pk0GanEH4/tMyRJyaHKfq
     kagX9HePdgdh8YOM4/S3xjRxmh9dXIfwkecJRQ7vCOI=;
```

Qu'est-ce qu'une RBL ? À quoi cela sert ? Est-ce utile ?

- Service (généralement basé sur le DNS) de blacklist en temps réel
« R »ealtime « B »lack « L »ist

- Notent les serveur SMTP open-relay, IP dynamique, reverse pourri, spammeurs notoires etc.

- Très utile pour la notation antispam
- peu être utile en blackliste « dure » si on sait passer outre ou comment la liste est constituée
- vérifiez vos IPs sur Mxtoolbox pour éviter d'être considéré comme un spammeur !

RFC 5782

```
dig ANY  69.95.170.112.zen.spamhaus.org
;; ANSWER SECTION:
69.95.170.112.zen.spamhaus.org.     900 IN      TXT   "http://www.spamhaus.org/query/bl?ip=112.170.95.69"
69.95.170.112.zen.spamhaus.org.     900 IN      A     127.0.0.4
```

http://spamhaus.org

http://mxtoolbox.com/

Qu'est-ce qu'un bounce, comment apparait-il
Comment l'interpréter, le problème des alias,
Les emails VERP...

- un bounce = un retour de mail en erreur

- généralement envoyé au From: sinon au Errors-To:
- idéalement dans un format mime multipart/report compréhensible à un humain et à une machine (en-têtes spécifiques)

- Si vous avez une liste de diffusion ou de discussion, il FAUT traiter les bounces Automatiquement, pour désabonner vos abonnés en erreur !
  > Sinon risque d'être blacklisté par les gros domaines

- Certains logiciels de ML utilisent VERP pour envoyer un From: permettant de gérer les bounces non reconnus (retournés par Exchange, Lotus ou autre horreur)
Exemple : mailinglist-owner+recipient=domain.org@sender.net
news-owner+benjamin=sonntag.fr@mediapart.fr

Qu'est-ce qu'un bounce, comment apparait-il
Comment l'interpréter ?

```
...
Auto-Submitted: auto-replied
MIME-Version: 1.0
Content-Type: multipart/report; report-type=delivery-status;
        boundary="C5AC150F5D5.1391520505/gerard.sonntag.fr"
Content-Transfer-Encoding: 8bit
Message-Id: <20140204132825.E03A750F5D6@gerard.sonntag.fr>
This is a MIME-encapsulated message.
--C5AC150F5D5.1391520505/gerard.sonntag.fr
Content-Description: Notification
Content-Type: text/plain; charset=us-ascii

This is the mail system at host gerard.sonntag.fr.
I'm sorry to have to inform you that your message could not
be delivered to one or more recipients. It's attached below.
For further assistance, please send mail to postmaster.
If you do so, please include this problem report. You can
delete your own text from the attached returned message.
                   The mail system
<test@libertysurf.fr>: host mx1.free.fr[212.27.48.7] said: 550
5.1.1 user
    unknown (UserSearch) (in reply to RCPT TO command)
--C5AC150F5D5.1391520505/gerard.sonntag.fr
Content-Description: Delivery report
Content-Type: message/delivery-status
Reporting-MTA: dns; gerard.sonntag.fr
X-Postfix-Queue-ID: C5AC150F5D5
X-Postfix-Sender: rfc822; support@sonntag.fr
Arrival-Date: Tue,  4 Feb 2014 14:28:25 +0100 (CET)
Final-Recipient: rfc822; tlsp@libertysurf.fr
Original-Recipient: rfc822;tlsp@libertysurf.fr
Action: failed
Status: 5.1.1
Remote-MTA: dns; mx1.free.fr
Diagnostic-Code: smtp; 550 5.1.1 user unknown (UserSearch)
```

```
--C5AC150F5D5.1391520505/gerard.sonntag.fr
Content-Description: Undelivered Message Headers
Content-Type: text/rfc822-headers
Content-Transfer-Encoding: 8bit
Return-Path: <support@sonntag.fr>
Received: from localhost (localhost [127.0.0.1])
        by gerard.sonntag.fr (Postfix) with ESMTP id C5AC150F5D5
        for <test@libertysurf.fr>; Tue,  4 Feb 2014 14:28:25
+0100 (CET)
Date: Tue, 4 Feb 2014 14:26:49 +0100
To: tlsp@libertysurf.fr
From: Support Octopuce <support@sonntag.fr>
Subject: =?UTF-8?Q?important,_r=C3=A9ponse_demand=C3=A9e
Message-ID:
<ba0e9693bb4ba2c147582c674ff0473e@localhost.localdomain>
X-Priority: 3
X-Mailer: PHPMailer 5.1 (phpmailer.sourceforge.net)
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="b1_ba0e9693bb4ba2c147582c674ff0473e"
--C5AC150F5D5.1391520505/gerard.sonntag.fr--
```

RFC 3464

Méthodes de lutte contre le spam

- blacklisting (rbl, home-made bl/wl)
- greylisting (évincer les spammeurs sans file d'attente)
- bases baysiennes
- règles techniques complexes (mélange de contenu html+text, etc.)
- RPD (recurrent pattern detection)
- règles DNS à la réception (from & to [illegible], helo, dns & reverse ...)

(greylisting)

RFC 6647

Logiciels de lutte contre le SPAM

- opendkim milter
- amavis & spamassassin (+ auto-learning)
- règles postfix + header check + body check
- clamav ou d'autres antivirus
- dspam (bayes-based + auto-learning)

Et les acteurs du mail ?

- mail providers
  gmail, yahoo, microsoft (live, outlook etc) ISP (free, orange...)

- mail OUT providers
  mailchimp, smartfocus (was : emailvision) ...

- mail IN providers
  mailinblack, barracuda, norton, spamhaus, return-path …

- et des milliers de petits
  No-log, riseup, gandi, mailoo, lautre net …

Comment bien configurer son serveur de mail ?

- DNS propre :
  - le FQDN du serveur a pour A son IPv4, pour AAAA son IPv6

- Reverse DNS propre :
  - les PTR de l'IPv4 et de l'IPv6 sont le FQDN du serveur

- SPF proprement configuré
  - si besoin mettre ?all à la fin

- DKIM proprement configuré
  - clé RSA dans le DNS (2048 bits !)
  - tous mails sortant signés numériquement

- si on ne contrôle pas les mails sortant :
  - antispam / antivirus sortant (amavis/clamav expliqués plus bas)

- serveur pas relai ouvert, MX primaire et secondaire non load-balancés

Exemple de configuration DNS avec OpenDKIM, SPF & autodiscover

```
zone sonntag.fr.
@ IN TXT   "v=spf1 a mx a:brassens.heberge.info a:z1.sonntag.fr ?all"
@ IN TXT   "mailconf=https://autodiscover.sonntag.fr/mail/mailautoconfig.xml"
@ IN MX 5  alice.sonntag.fr.
@ IN MX 10 secondary.sonntag.fr.
alternc._domainkey  IN  TXT "v=DKIM1\; k=rsa\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC7lmzOaaojx4ppHCIoaqX5CP92tVCij36eFh+FscPyoTQ5CimLSFA
yDhDEp0hDYA/8EZoqWvF/z3rZKp+JrypKoqpPSI3QpaJGp+ZuqJabcKjE5rgk7bUUfm9gVUnOehIM185n7xpbWkQFxmCu
fpJu3wu4eqNc2YPJ5A9H9AldyQIDAQAB"
mail IN CNAME alice
webmail IN CNAME alice
pop IN CNAME alice
imap IN CNAME alice
smtp IN CNAME alice

alice IN A    91.194.60.6
alice IN AAAA 2001:67c:288::6

zone 60.194.91.in-addr.arpa.
6     IN PTR alice.sonntag.fr.

zone 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.8.2.0.C.7.6.0.1.0.0.2.ip6.arpa.
6.0.0.0   IN PTR alice.sonntag.fr.
```

Exemple d'extrait de configuration pour Postfix

/etc/postfix/main.cf

```
# TLS parameters
smtpd_tls_cert_file = /etc/ssl/certs/alice.crt+chain
smtpd_tls_key_file = /etc/ssl/private/alice.key
smtpd_use_tls = yes  # idem avec smtp

# Generic settings
myhostname = alice.sonntag.fr
alias_maps = hash:/etc/aliases
mydestination = alice.sonntag.Fr, localhost.sonntag.fr, localhost
# relayhost = 10.2.0.1
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
recipient_delimiter = +
inet_interfaces = all

# Filtres DKIM
milter_default_action = accept
milter_protocol = 6
smtpd_milters = inet:127.0.0.1:8891
non_smtpd_milters = inet:127.0.0.1:8891

# Filtres maison
header_checks = regexp:/etc/postfix/header_checks
body_checks = regexp:/etc/postfix/body_checks
message_size_limit = 502400000
mailbox_size_limit = 1024000000

# Secondary MX configuration
relay_domains = $mydestination hash:/etc/postfix/secondary
disable_vrfy_command = yes
smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated, reject_invalid_hostname,
  reject_non_fqdn_hostname, reject_non_fqdn_sender, reject_rbl_client zen.spamhaus.org,
  reject_non_fqdn_recipient, reject_unknown_sender_domain, reject_unknown_recipient_domain,
  reject_unauth_pipelining, reject_unlisted_recipient, reject_unauth_destination
```

Exemple d'extrait de configuration pour Postfix

/etc/postfix/master.cf

```
smtp      inet  n       -       y       -       20       smtpd
  -o content_filter=smtp-amavis:[127.0.0.1]:10024

smtps      inet  n       -       y       -       20       smtpd
  -o smtpd_tls_wrappermode=yes -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_mynetworks,permit_sasl_authenticated,reject

submission      inet  n       -       y       -       20       smtpd
  -o header_checks=regexp:/etc/postfix/receivedanonymous
  -o smtpd_recipient_restrictions=permit_mynetworks,permit_sasl_authenticated,reject
```

/etc/postfix/receivedanonymous

```
/^received: /     IGNORE
/^X-Sender: /     IGNORE
/^User-agent: /   IGNORE
```

Au travail

https://en.wikipedia.org/wiki/Variable_envelope_return_path

https://en.wikipedia.org/wiki/Abuse_Reporting_Format

https://en.wikipedia.org/wiki/Feedback_Loop_(email)

...

des questions ?

mailto : benjamin@sonntag.fr
xmpp : benjamin@mailfr.com
pgp : 0x586073e6

et... surfez couvert ;)