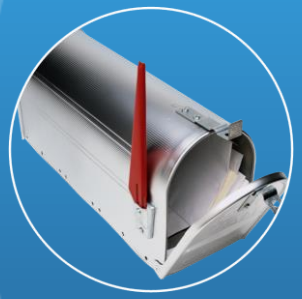
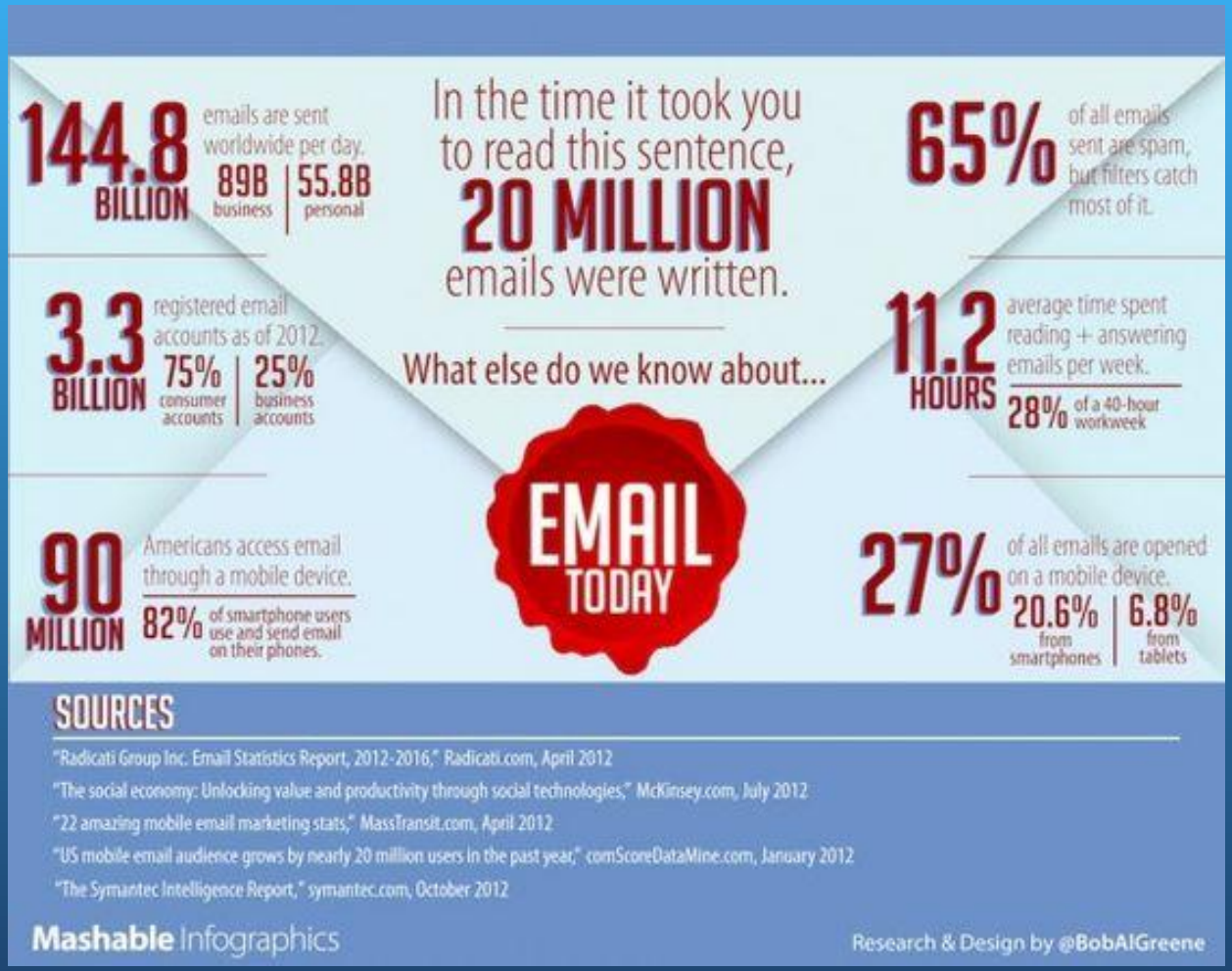
Présentation de la messagerie



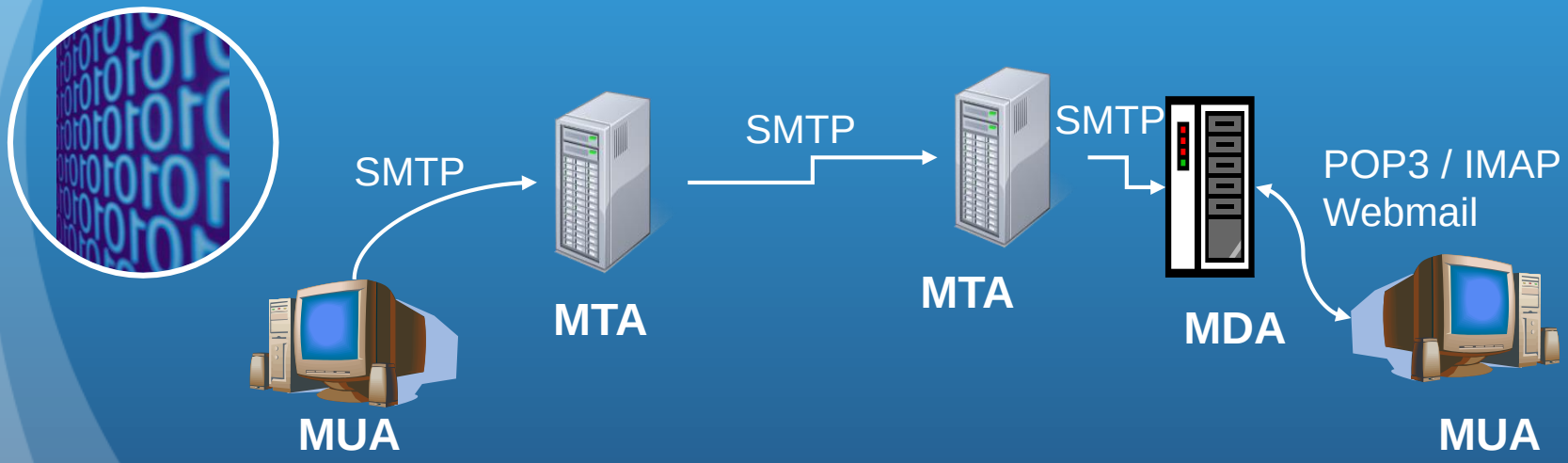
- Présentation des messageries
- Structure des messages et normes
- Intégrité et traçabilité des messages
- Particularités de SPF, DKIM et DMARC

Présentation de la messagerie



Présentation de la messagerie fonctionnement

Fonctionnement (MTA - MDA - MUA)



- MUA : Mail User Agent
- MTA : Mail Transfer Agent
- MDA : Mail Delivery Agent

Présentation de la messagerie

MUA (clients / Webmail)

Trois fonctionnements distincts :

- **Messagerie d'entreprise :**
  - **Exchange ; Lotus Domino ; Zimbra**
- **Client de messagerie :**
  - **Outlook ; Lotus Notes ; Thunderbird ; Eudora**
- **Webmail :**
  - **Orange ; yahoo ; hotmail ; gmail**

Présentation de la messagerie

Structure des messages et normes

- Structure :
  - En-tête de trace des mails
  - Corps du message
  - Pièces attachées
- Normes :
  - RFC 2822 (anciennement 822) format mails
  - RFC 5322 (en-têtes messages)
  - RFC 2821 (SMTP) RFC 3401 (IMAP) et RFC 1939 (POP3)
  - MIME ; UTF8 pour le contenu et pièces jointes
  - RFC 7208 SPF
  - RFC 6376 DKIM
  - RFC 7489 DMARC

Sender Policy Framework (SPF)

SPF

Limitations, dans un domaine, des adresses IP pouvant émettre un message.

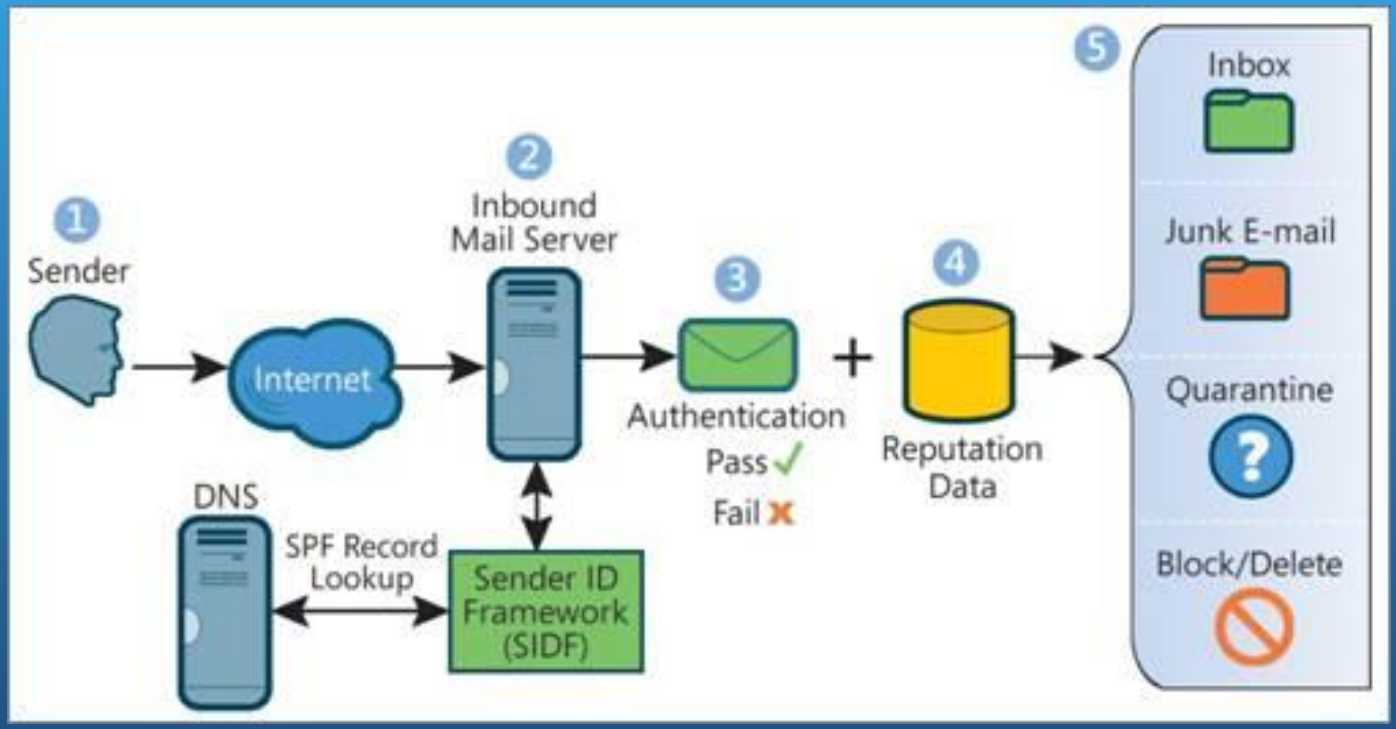
Enregistrées dans le DNS

“v=spf1 a ipv4:10.0.3.0/23 ipv4:192.168.55.0/26 -all”

MAIS : pas d’information de signature, ni d’identification de l’émetteur (personne).

N’empêche pas d’envoyer un email avec un faux nom lié à ce domaine à partir d’un autre serveur.

Schéma SPF


1
Sender
2
Inbound
Mail Server
Internet
3
Authentication
Pass
Fail
4
Reputation
Data
5
Inbox
Junk E-mail
Quarantine
Block/Delete
DNS
SPF Record
Lookup
Sender ID
Framework
(SIDF)

DomainKeys Identified Mail (DKIM)

DKIM (1)

Le serveur d'un domaine donné signe les messages envoyés avec sa clé privée.

La clé publique est enregistrées dans le DNS :

1537513012.experact._domainkey.experact.com. IN TXT (
"v=DKIM1;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC9NyiFNpd3sCTT7LjQRYeQdihU"
"/EdTQQNZcTrJS+Sg29mgcQkD6dVBpXsPu9YKmkTJJTq70zVLvucpwA0Htb7rGeBw"
"Yy5Xd/GbtQkbJM9hrysLeZ5NlDMc0+fXE/Mq+Ez3UdEcK6Fe62T7wq6+RrUjqPg2«
"wDaSNSTLtMHAqm0cSQIDAQAB")

DomainKeys Identified Mail (DKIM)

DKIM (2)

Le serveur d'émission calcule l'empreinte du message émis, indique la date de signature (optionnelle) et signe avec sa clé privée.

Le message reçu contient dans ses en-têtes :

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=experact.onmicrosoft.com; s=selector1-experact-onmicrosoft-com;
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;
bh=0qtqjQLyXpnigypkxmxAhXtYQaQMh02P7X+X/Hp2H1Y=;

b=Lwwbpv1Dro57Fd1PqhfNgsU00m5CObWdUEyopdLtGHNFpqwYc/gm5DZyF/qLHr/QS+SbTaH54R00u3y11mclvEp7jQ5fuOBXIH+goByDoHzlAfDzDeZl+dkbV74BilDC31zDa09XxbVm4XsltH60xCIPUkYo40pZQAgUFE61vvM=

d : domaine émetteur / a : algorithme de hash / h: en-têtes prises en compte dans la signature t (optionnel) : timestamp / b : données de signature / bh : hash du corps du message (incluant les attachements)

DomainKeys Identified Mail (DKIM)

DKIM (3)

Comment vérifier ?

1. *La signature du domaine*
2. *L'empreinte du message*

La signature est facile à valider avec une requête DNS

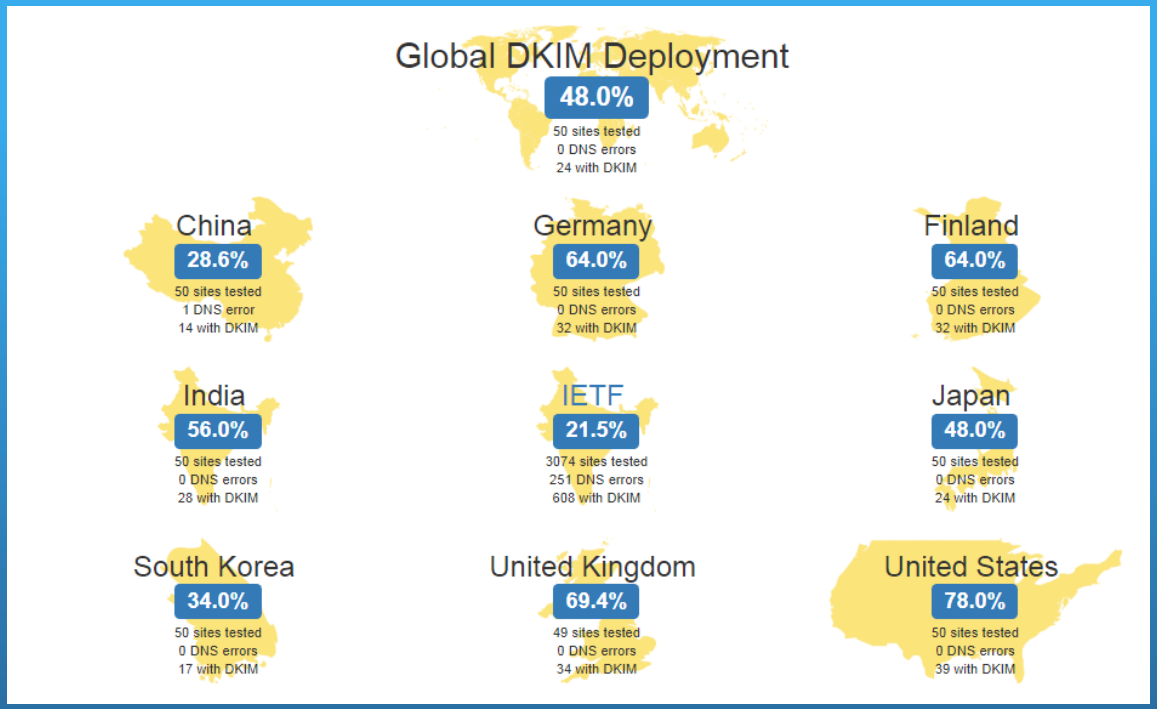
En revanche l'empreinte est sujette à difficultés :

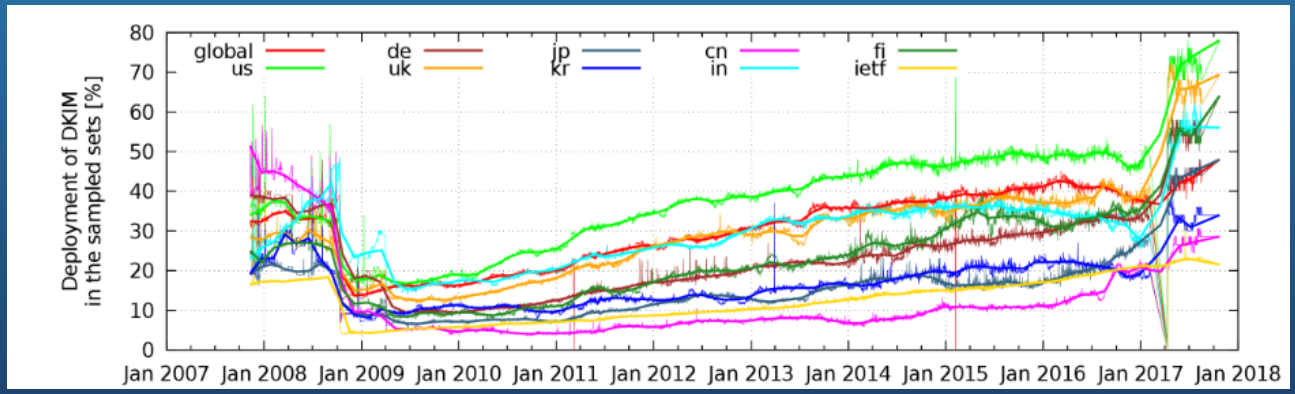
- Transformation du message en 7bits « quoted printable » avec les pièces jointes

- *Cannonisation du message (suppression des lignes vides en fin de message par exemple)*

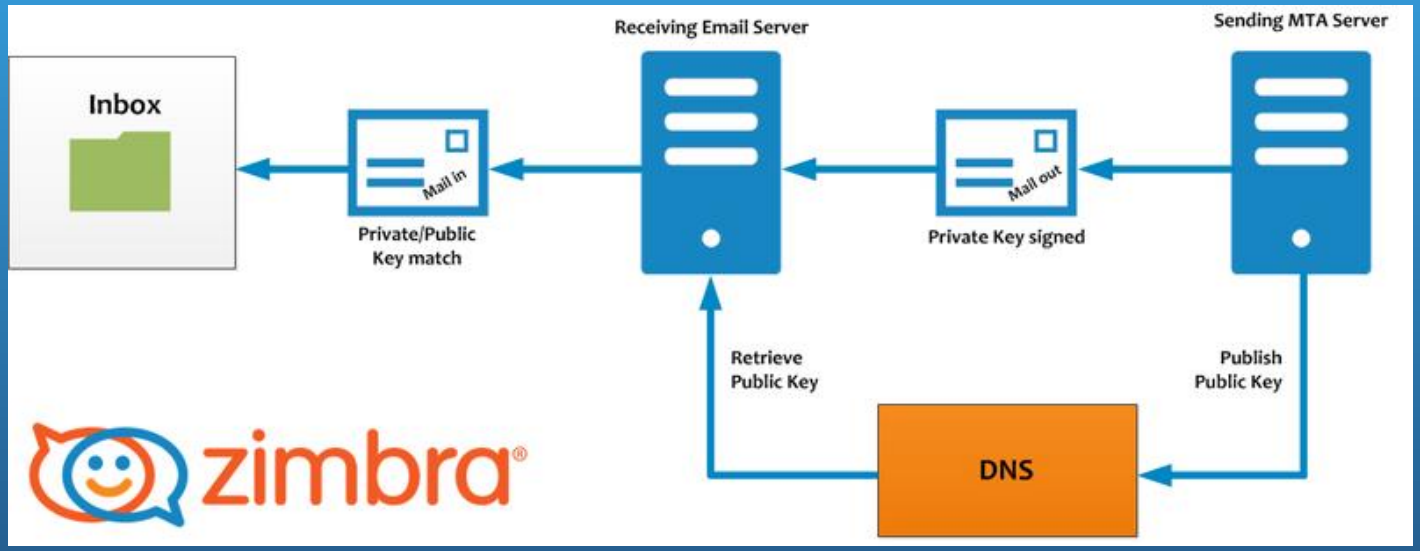
- modification du message lors des transferts (listes de diffusion, modification des en-têtes par les anti-SPAM…) (cf ARC)

DKIM progression

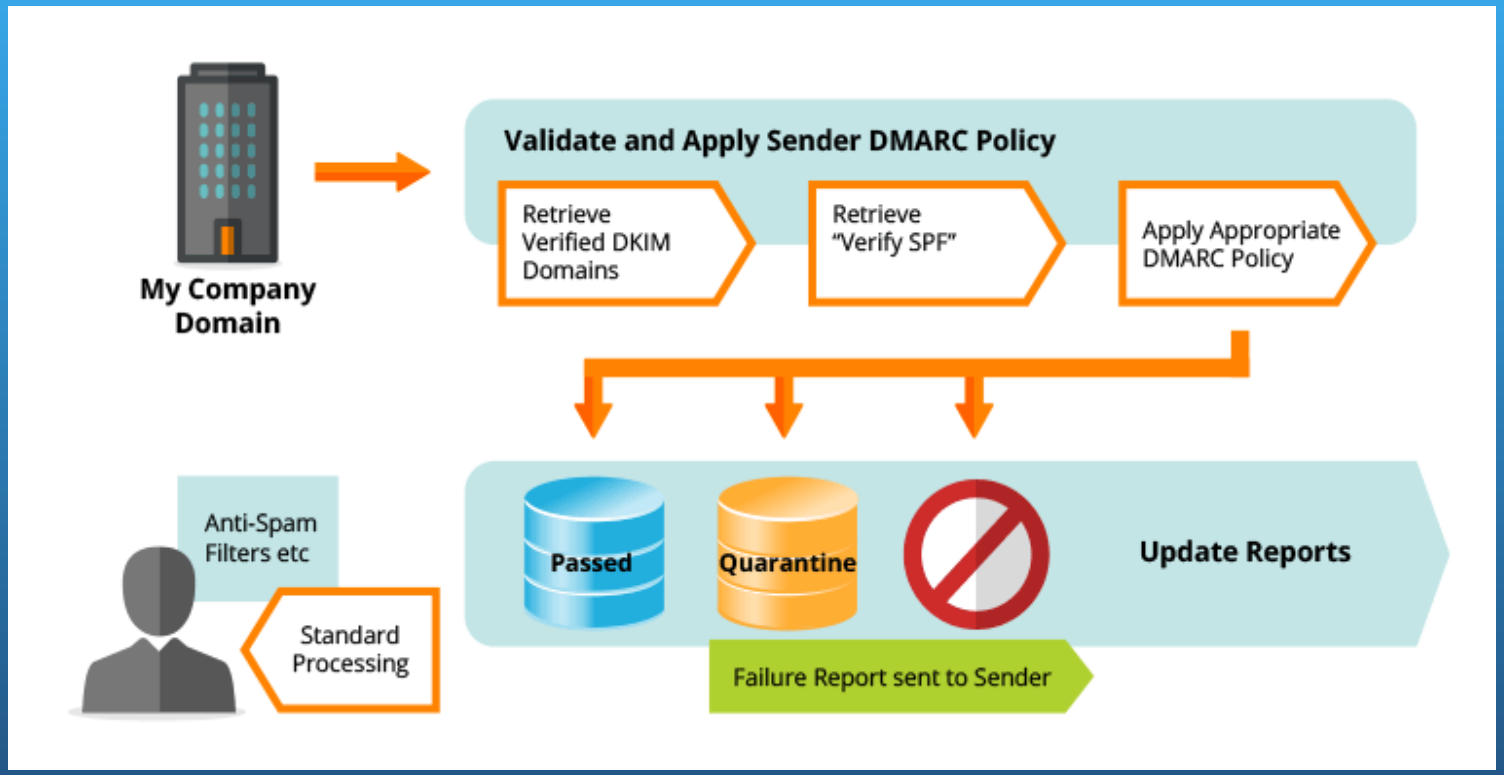




DKIM

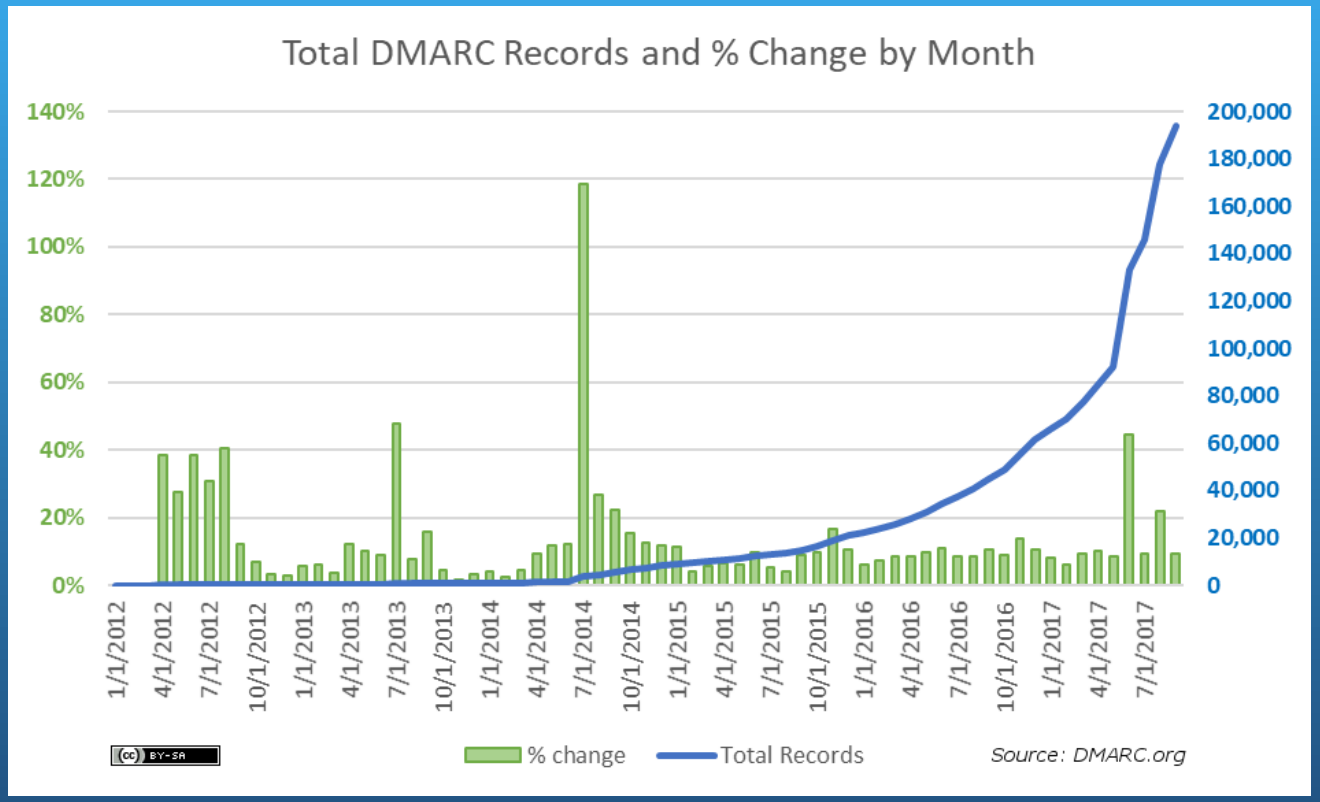

Receiving Email Server
Sending MTA Server
Inbox
Mail in
Private/Public
Key match
Mail out
Private Key signed
Retrieve
Public Key
Publish
Public Key
DNS
zimbra

Domain-based Message Authentication, Reporting and Conformance (DMARC)



Utile si les émetteurs utilisent DKIM et SPF

DMARC progression



200,000 domaines sur plus de 330 Millions !

Limites (from dmarc.org)

- Domains with strict DMARC policies (`p=reject`) may see legitimate messages blocked if they go through *indirect mailflows* such as mailing lists, forwarding, or filtering services
- Forwarding causes SPF to fail even if origin was legit
- Forwarders often alter messages, breaking DKIM
  - Disclaimers and footers
  - Virus scan results
  - Removed attachments
  - Mailing list subject tags

Analyse d'exemples

- Avec DKIM Valide
- Avec SPF et DKIM
- Avec ARC
- Non valides

Points de faiblesses actuels

- Absence de sécurisation des liens
- Pas d'authentification
- Absence d'horodatage fiable (sauf usage de 't' dans DKIM)
- Manque d'intégrité : DKIM aide en partie
- Faible traçabilité : si DKIM + SPF alors OK
- Mails anonymes : toujours vrai

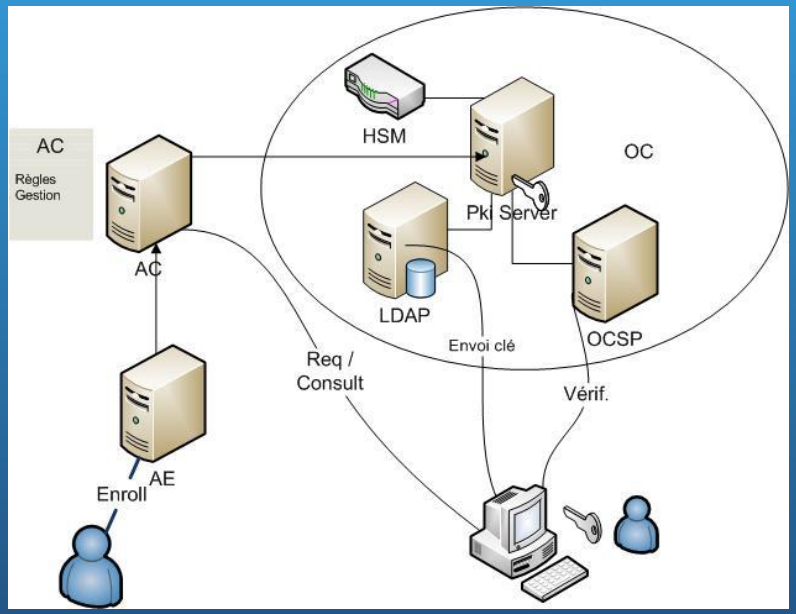
Nouvelle architecture de confiance

- Identification de la source (DKIM + IP)
- Authentification de l'émetteur (Sigelec)
- Sécurisation des échanges (TLS (SSL))
- Intégrité des messages (empreintes)
- Traçabilité et Horodatage (TSS + sigserv)
- Modification du protocole SMTP

QUESTIONS ?

Eric LAURENT-RICARD – Experact – eric@experact.com

PKI


AC
Règles
Gestion
AC
HSM
OC
Pki Server
LDAP
OCSP
Envoi clé
Req /
Consult
Vérif.
AE
Enroll