RENATER
CONNECTEUR DE SAVOIRS

JRES DIJON 2019

Tordons le cou au phishing !

Damien Mascré
Laurent Aublet-Cuvelier
David Verdin

Vous avez un message...

From: Jeanine Legall <legallj@live.fr>
To: undisclosed recipients: ;
Reply-to: legallj@live.fr
Subject: URGENT MR/MME
Date: Fri, 30 Nov 2012 01:31:57 +0000 (GMT)
X-Mailer: YahooMailClassic/15.0.8 YahooMailWebService/0.8.127.475

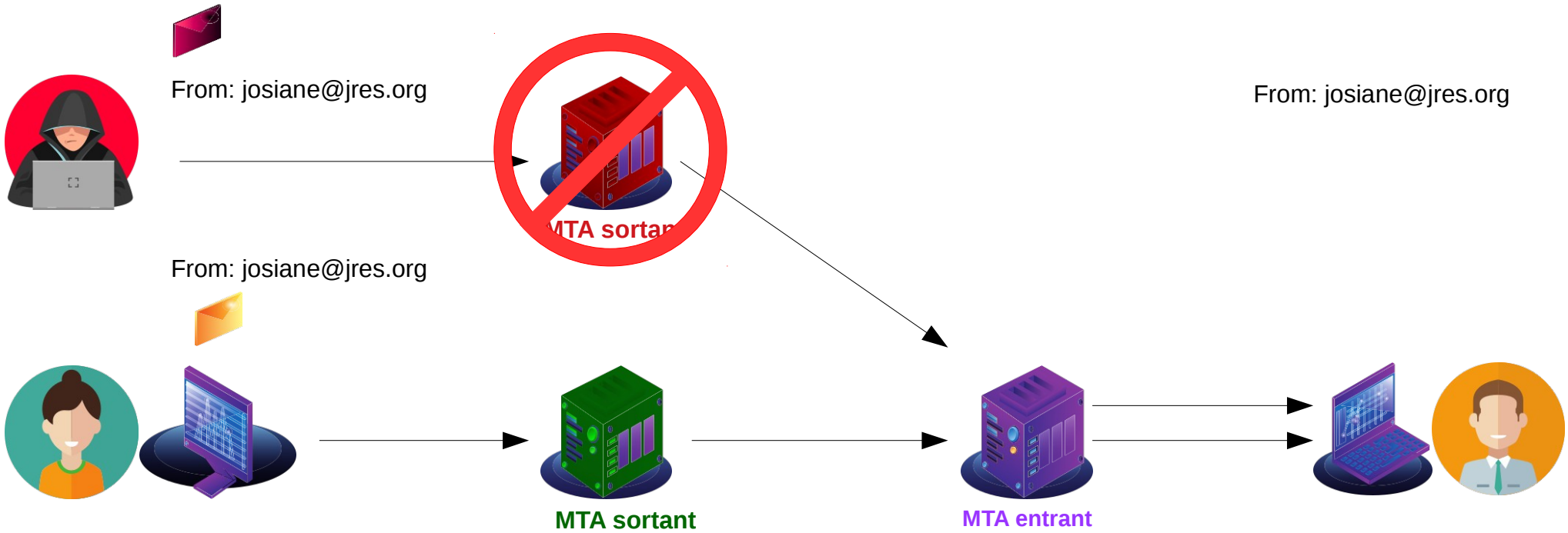
Excusez-moi de ce que mon mail peut causer cela faire deux (2)
jours que j'ai envoyé ce mail à une association qui s'occupe des enfants démunis,
et par de réponse, mais j'ai obtenu votre mail par le logiciel contact Express v2012 France
le moteur de recherche des adresses emails en France. Si vous recevez mon mail je vous prie de me répondre car ceci n'est pas une blague.
Je me nomme Le Gall Jeanine et cela fait quelques mois que j'ai été atteint d'un cancer de gorge selon les dits de mon docteur, une boule est installée présentement dans ma vessie. Par négligence de cette maladie, j'ai appris ces derniers temps que mon état s'est aggravé et même devenu incurable, j'ai fait recours à des spécialistes de cette maladie mais malheureusement je n'ai pu obtenir que des soins pour le ralentissement de l'avancée de ma maladie et non un traitement complet pour mon rétablissement. En ce moment je Me trouve à la clinique toutes Aures - Groupe Kapa Santé, en France pour un traitement.
C'est dans ce sens que je vous faire savoir avec beaucoup d'hésitation que je dispose de 350 000 euros dans ma banque SG (Société Générale), je souhaiterais faire don de la somme à une personne de confiance et d'honnête qui pourra en faire bon usage vu que mes jours sont désormais comptés et comme je n'ai toujours
pas de réponse de cette association c'est pour cela je vous contacte.
Je vous contacte car ce matin j'ai reçu un message de ma banque me disant que l'État Français
aimerait récupérer ces fonds après ma mort vu que je n'ai pas d'héritier. Je vous apporterais
le contact de mon gestionnaire si vous être à mesure de recevoir cette somme.

Merci de me répondre.
Mme Le Gall Jeanine .

Phishing ?

- Un mail dont l'auteur n'est pas la personne identifiée par le champ « From »
- Le but : vous voler vos identifiants
- Le moyen : vous amener sur un site où vous saisirez vos identifiants
- Souvent mal rédigés (effet de masse), parfois très bien ciblés

Comment ça marche ?



De quoi on parle ?

- Des RFC anti-phishing : authentification serveur !
  - SPF : Sender Policy Framework (2006 puis 2014)
  - DKIM : Domainkeys Identified Mail (2011)
  - DMARC : Domain-based Message Authentication, Reporting and Conformance (2015)
  - ARC : Authenticated Received Chain (2019)
- Les objectifs :
  - Expliquer comment elles fonctionnent : le principe ici, les détails dans l'article
  - Rechercher une organisation collective autour de ces RFC
- Attention ! Elles ne suffiront pas à elles seules !

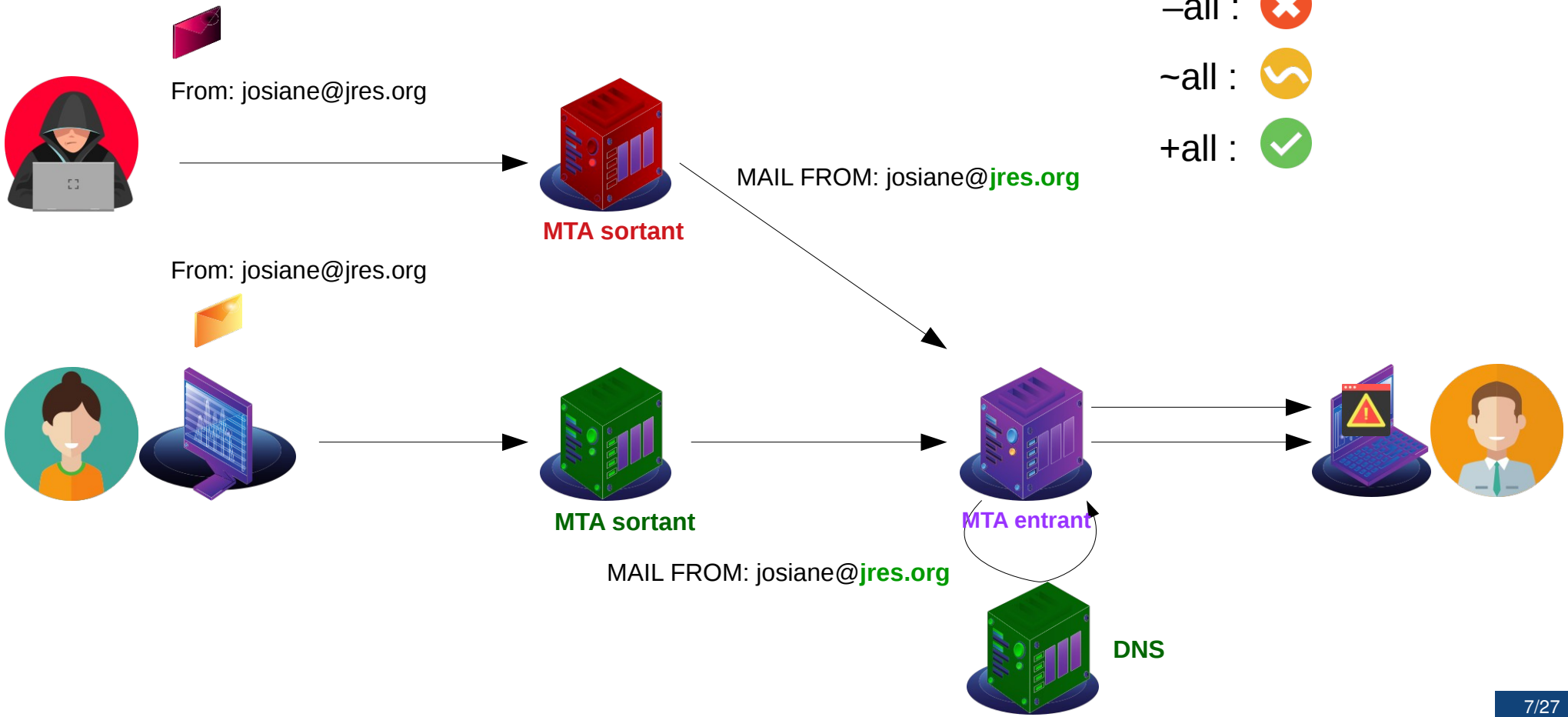
SPF

Enregistrement DNS (TXT) : quel serveur a le droit de poster ?

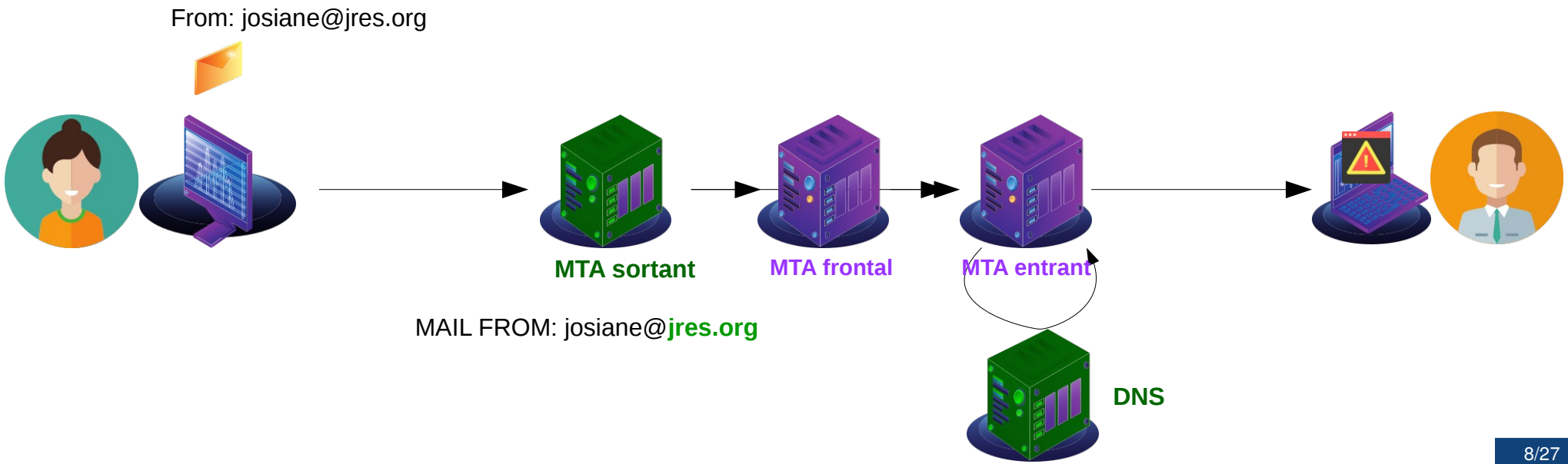
Exemple :

emetteur.tld. 14400 IN TXT "v=spf1 ip4:192.168.0.0 mx -all"

SPF


–all :
~all :
+all :
From: josiane@jres.org
MTA sortant
MAIL FROM: josiane@jres.org
From: josiane@jres.org
MTA sortant
MTA entrant
MAIL FROM: josiane@jres.org
DNS

SPF : limites


From: josiane@jres.org
MTA sortant
MTA frontal
MTA entrant
MAIL FROM: josiane@jres.org
DNS

DKIM

Signature du message et de ses entêtes

Clé privée sur le serveur

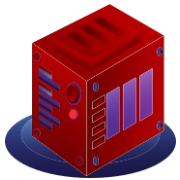
Enregistrement DNS (TXT) : clé publique et règles de signature

Exemple :

dkim._domainkey.emetteur.tld. 1779 IN TXT "v=DKIM1; k=rsa;p=MIGfMA0GCS
qGSIb3DQEBAQUAA4GNADCBiQKBgQDI6mZ3PHIbGNtNruAsbF/wNcqyNiD
T0CReSZQc9yVp6i24MxfLlOg++RhVJ0r8V0bpBLr34yVOGbsjK0VLbN9Xjusrs9
qRlvOoAXaOTRZSiIFBXgbp7AY0nwmOoFYkjmf/2FUq5szjl8rom8bXM7TlAcLm
vxWOi0e+jn5T0z888QIDAQAB ; t=s'

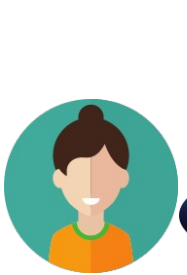
DKIM

From: josiane@jres.org



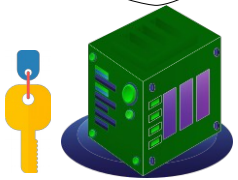
MTA sortant

From: josiane@jres.org



MTA sortant

MTA entrant



DNS

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
d=jres.org; s=lists; t=1253606545;
bh=OlpSJ5JchtJ2CadL8LtZ4wmoqGhpXKmpd54T9aeD6fY=; h=Message-ID:Date:From:MIME-Version:To:CC:Subject:References:In-Reply-To:Content-Type:Content-Transfer-Encoding;
b=aOxThCfbgV0Za82dFYHca0SZtqmQ8Ey2KMyzQ5NN0frwGkhXpJ/46jvIddQyuHU
T/U6UllkEV/062Lnf9gcGjgWgQwKw93CTqUvUAIVh2eenTy5rVmlLeK8J/N6DkFPDVd
qGWakjJCNWarvP3wn9+hjyc4bEEV8mV877aY=

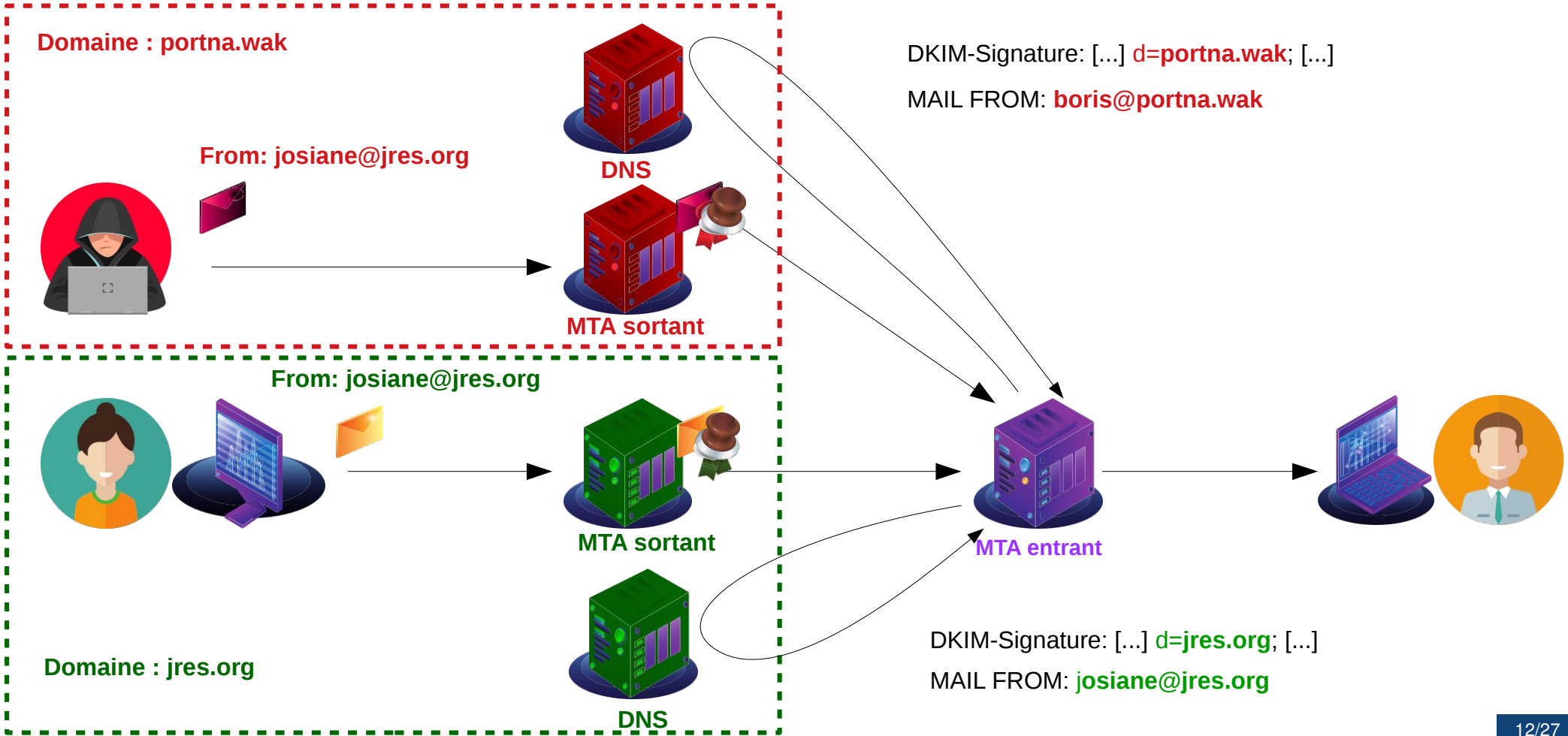
: Clé privée

: Clé publique

Alors, ça suffit ?

- Ben non, sinon y aurait pas d'histoire…
- Les limites :
  - SPF : cassé au premier relai, même légitime
  - Les deux : aucune obligation pour le domaine destinataire.
- Ça n'aide pas l'utilisateur :
  - En général, aucun affichage dans les clients,
  - Si c'était affiché, pourrait être confondu avec une vérification de l'identité de l'expéditeur

Limites de SPF et DKIM



DMARC

Politique de sécurité en fonction du respect de SPF et DKIM

Au moins un des deux (SPF ou DKIM) doit être valide !

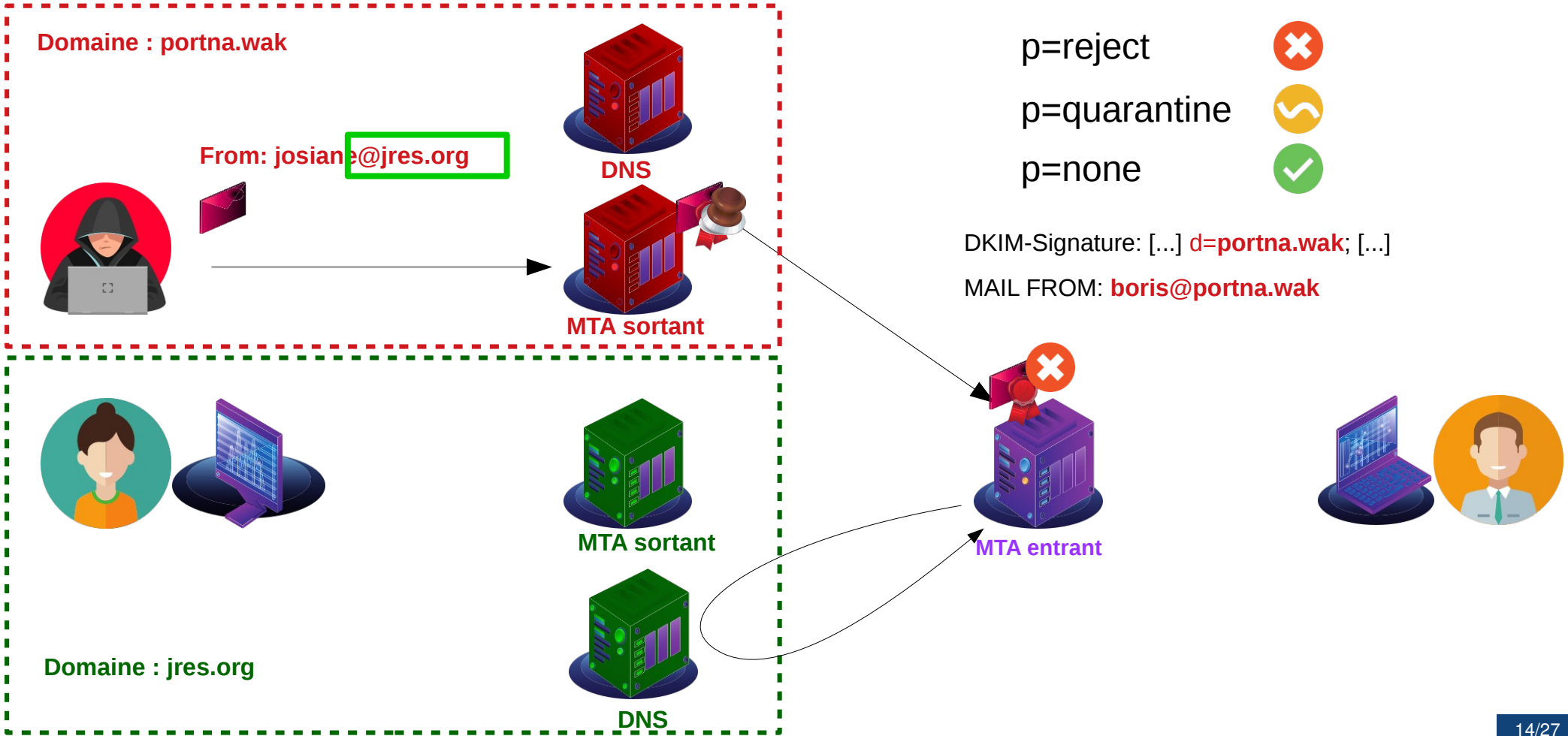
Alignement : seuls les SPF et DKIM du domaine du champ « From » sont pris en compte

Enregistrement DNS (TXT) : politique de sécurité

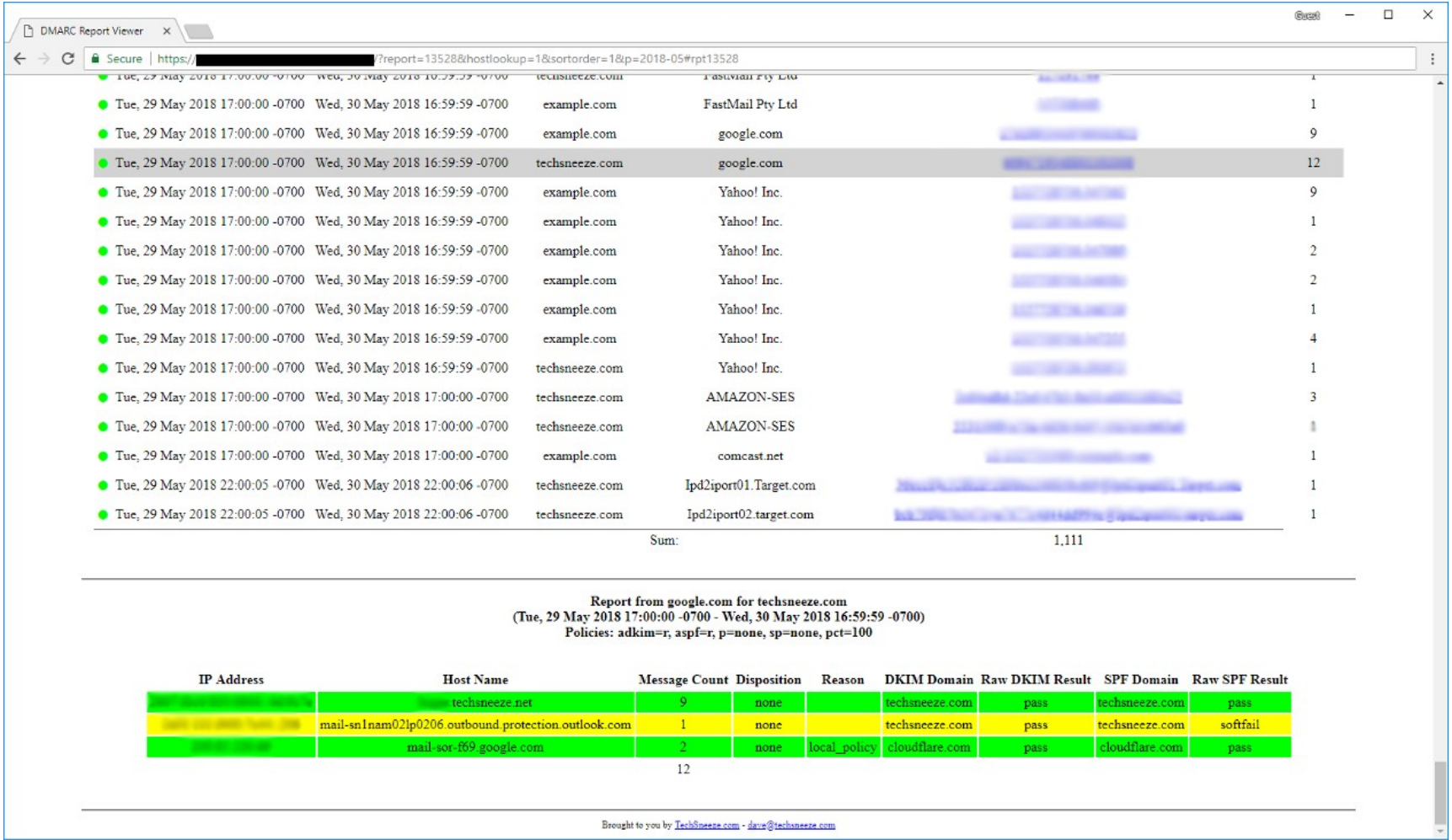
Exemple :

_dmarc.<emetteur.tld> 1800 INTXT"v=DMARC1; p=reject;
rua=mailto:local@emetteur.tld; ruf=mailto:local@emetteur.tld; fo=1; pct=100
adkim=strict; aspf=strict"

DMARC et l'alignement



DMARC : on voit le rapport



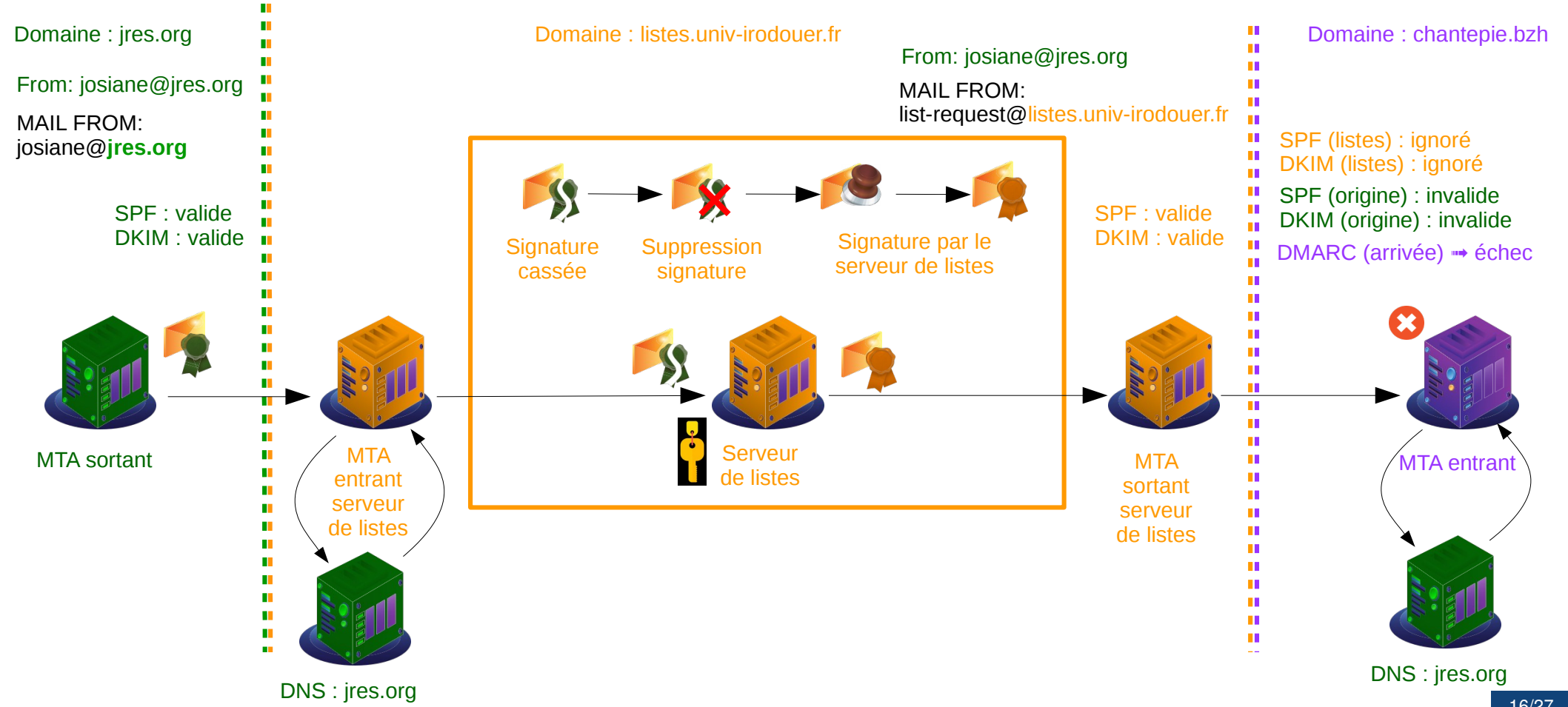
Tue, 29 May 2018 17:00:00 -0700	Wed, 30 May 2018 16:59:59 -0700	example.com	FastMail Pty Ltd	[redacted]	1
Tue, 29 May 2018 17:00:00 -0700	Wed, 30 May 2018 16:59:59 -0700	example.com	google.com	[redacted]	9
Tue, 29 May 2018 17:00:00 -0700	Wed, 30 May 2018 16:59:59 -0700	techsneeze.com	google.com	[redacted]	12
Tue, 29 May 2018 17:00:00 -0700	Wed, 30 May 2018 16:59:59 -0700	example.com	Yahoo! Inc.	[redacted]	9
Tue, 29 May 2018 17:00:00 -0700	Wed, 30 May 2018 16:59:59 -0700	example.com	Yahoo! Inc.	[redacted]	1
Tue, 29 May 2018 17:00:00 -0700	Wed, 30 May 2018 16:59:59 -0700	example.com	Yahoo! Inc.	[redacted]	2
Tue, 29 May 2018 17:00:00 -0700	Wed, 30 May 2018 16:59:59 -0700	example.com	Yahoo! Inc.	[redacted]	2
Tue, 29 May 2018 17:00:00 -0700	Wed, 30 May 2018 16:59:59 -0700	example.com	Yahoo! Inc.	[redacted]	1
Tue, 29 May 2018 17:00:00 -0700	Wed, 30 May 2018 16:59:59 -0700	example.com	Yahoo! Inc.	[redacted]	4
Tue, 29 May 2018 17:00:00 -0700	Wed, 30 May 2018 16:59:59 -0700	techsneeze.com	Yahoo! Inc.	[redacted]	1
Tue, 29 May 2018 17:00:00 -0700	Wed, 30 May 2018 17:00:00 -0700	techsneeze.com	AMAZON-SES	[redacted]	3
Tue, 29 May 2018 17:00:00 -0700	Wed, 30 May 2018 17:00:00 -0700	techsneeze.com	AMAZON-SES	[redacted]	1
Tue, 29 May 2018 17:00:00 -0700	Wed, 30 May 2018 17:00:00 -0700	example.com	comcast.net	[redacted]	1
Tue, 29 May 2018 22:00:05 -0700	Wed, 30 May 2018 22:00:06 -0700	techsneeze.com	Ipd2iport01.Target.com	[redacted]	1
Tue, 29 May 2018 22:00:05 -0700	Wed, 30 May 2018 22:00:06 -0700	techsneeze.com	Ipd2iport02.target.com	[redacted]	1
			Sum:		1,111

Report from google.com for techsneeze.com
(Tue, 29 May 2018 17:00:00 -0700 - Wed, 30 May 2018 16:59:59 -0700)
Policies: adkim=r, aspf=r, p=none, sp=none, pct=100

IP Address	Host Name	Message Count	Disposition	Reason	DKIM Domain	Raw DKIM Result	SPF Domain	Raw SPF Result
[redacted]	techsneeze.net	9	none		techsneeze.com	pass	techsneeze.com	pass
[redacted]	mail-sn1nam02lp0206.outbound.protection.outlook.com	1	none		techsneeze.com	pass	techsneeze.com	softfail
[redacted]	mail-sor-f69.google.com	2	none	local_policy	cloudflare.com	pass	cloudflare.com	pass
		12						

Brought to you by TechSneeze.com - dave@techsneeze.com

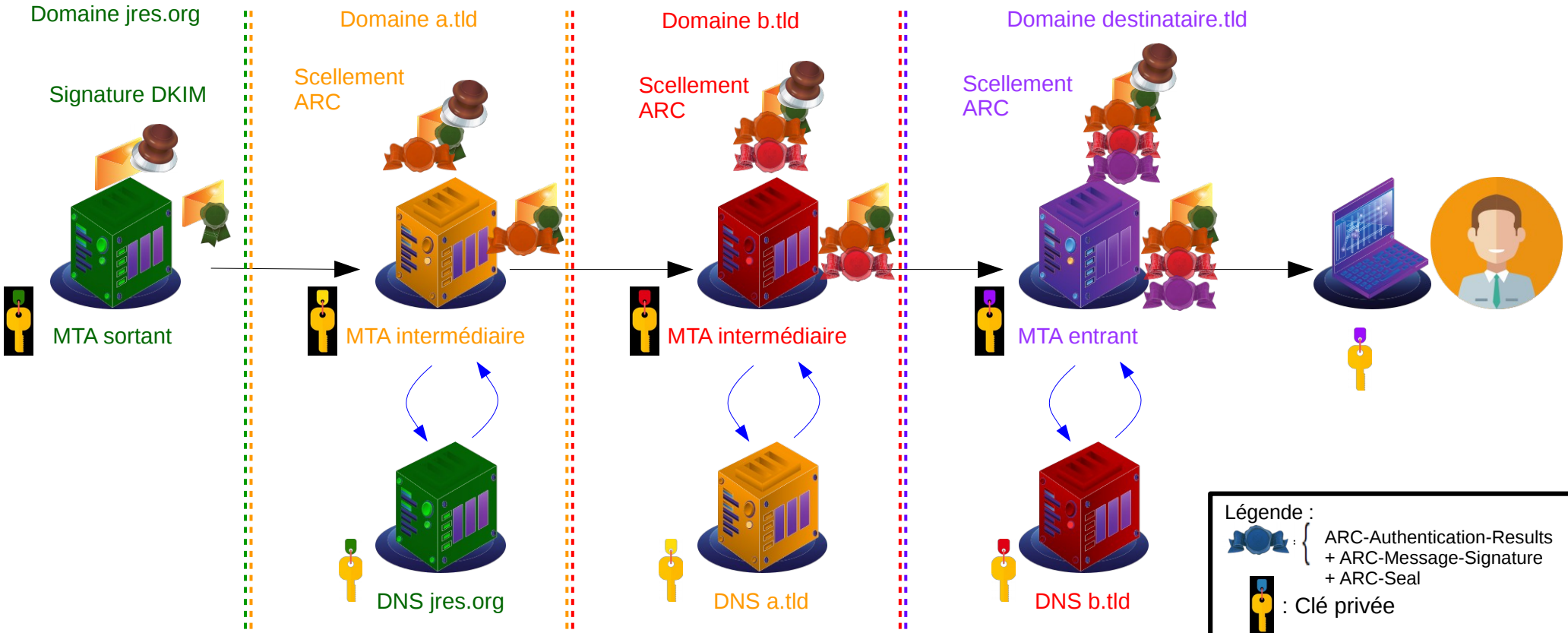
DMARC, l'alignement et les systèmes de ré-envoi



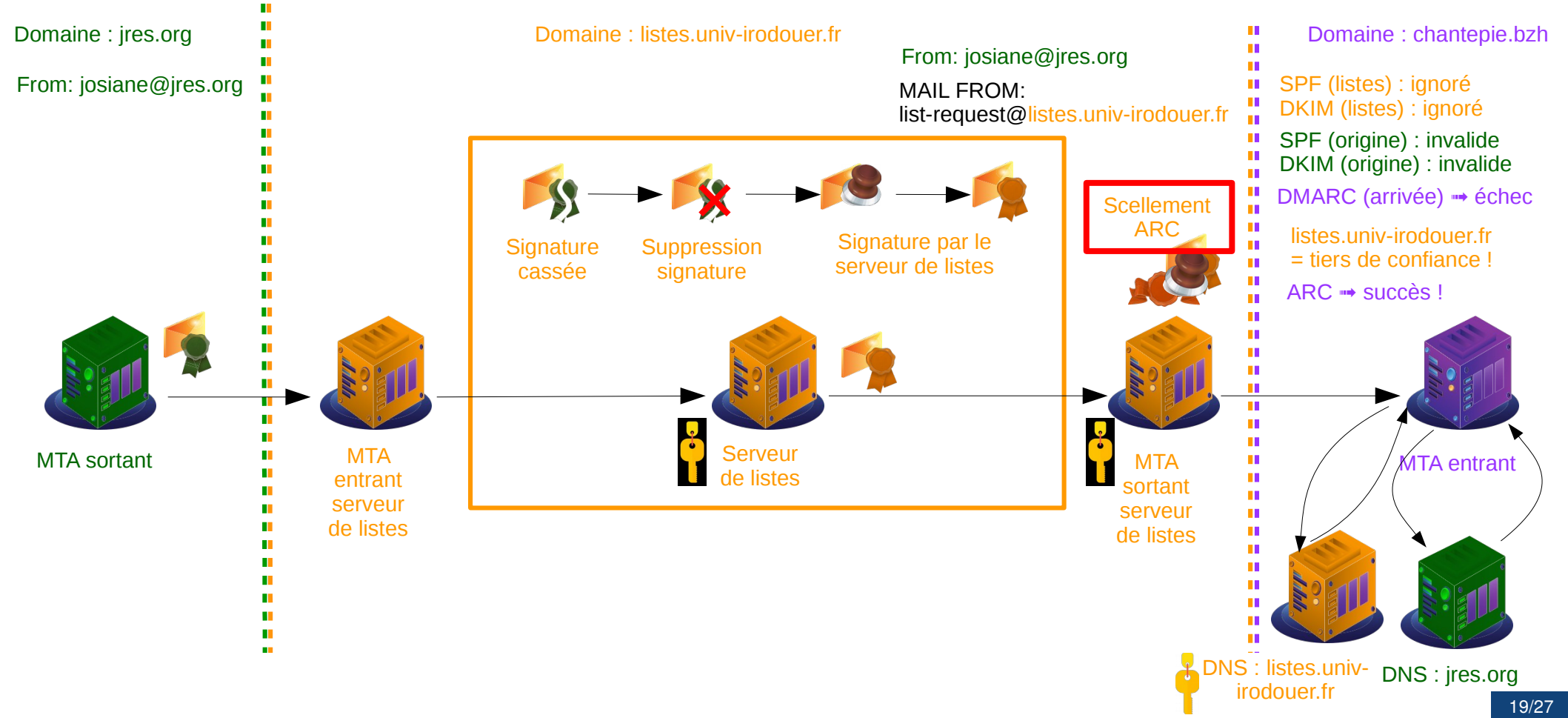
ARC

- Enregistrement DNS (TXT) : le même que DKIM !
- On peut donc le réutiliser
- Surtout des entêtes qui forment le **triplet ARC** :
  - *ARC-Authentication-Results* : état d'authentification du message à la réception
  - *ARC-Message-Signature* : Signature du message par le tiers courant
  - *ARC-Seal* : Sceau = Signature de toute la chaîne d'authentification
- « Sceller ARC » c'est ajouter un triplet ARC. Numéroté (1..n)
- Chaque intermédiaire peut poser un triplet ARC.
  L'ensemble forme la **chaîne d'authentification**.

ARC


Domaine jres.org
Signature DKIM
MTA sortant
Domaine a.tld
Scellement ARC
MTA intermédiaire
DNS jres.org
Domaine b.tld
Scellement ARC
MTA intermédiaire
DNS a.tld
Domaine destinataire.tld
Scellement ARC
MTA entrant
DNS b.tld
Légende :
ARC-Authentication-Results
+ ARC-Message-Signature
+ ARC-Seal
: Clé privée
: Clé publique

ARC et la confiance



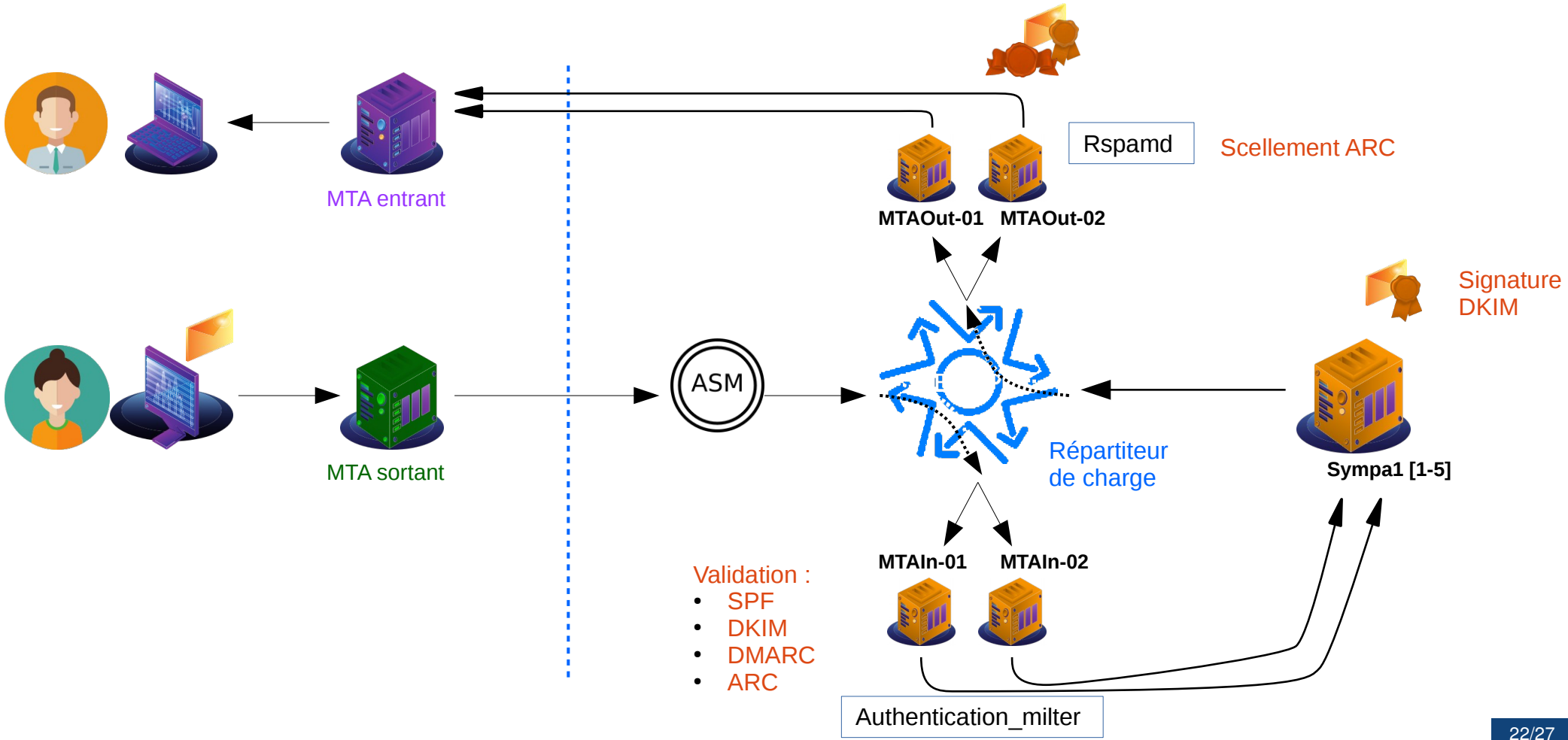
Bilan sur les 4 RFC

- SPF et DKIM : authentification serveur émetteur
- DMARC : politique de sécurité
- ARC : assouplissement de la politique pour les sources de confiance

Implémentations existantes

	OpenDKIM	OpenDMARC	OpenARC	authheaders	Amavis	SpamAssassin	Authentication_milter	Rspamd	Antispam RENATER
Vérifie SPF		≈		✔	✔	≈	✔	✔	✔
Vérifie DKIM	✔	✔		✔	✔	≈	✔	✔	✔
Signe DKIM	✔				✔	≈		✔	
Vérifie DMARC		✔		✔		≈	✔	✔	≈
Scelle ARC			✔			≈	✔	✔	≈
Vérifie ARC		≈	✔			≈	✔	✔	≈
ARC permet d'ignorer DMARC		≈				≈	✔	≈	≈

Implémentation expérimentale



Les limites

- Pas de protection contre un serveur piraté,
- Pas de protection contre un compte piraté,
- Pas de protection contre les domaines « presque comme les vrais ». « retaner.fr » par exemple,
- Pas d'affichage dans les clients utilisateurs.
- Ah oui, quand même...

Les arguments pour

- Protection contre les pirates qui n'ont pas suivi le mouvement,
- Mieux connaître l'utilisation de sa messagerie (le « R » de DMARC),
- Création d'un réseau de serveurs de confiance.

Bon. Et après ?

- Nos propositions :
  - Tout le monde signe DKIM
  - Tout le monde positionne un enregistrement SPF fini par « -all »
  - Tout le monde positionne une politique DMARC « p=reject »
  - Tout le monde empêche l'emploi de sous-domaines non déclarés (« t=s » dans DKIM, « adkim=strict » et « aspf=strict » dans DMARC)

→ Un bon paquet de phishings en moins

Quoi, là ? Tout de suite ?

- Non.
- D'abord, « p=none » sur DMARC => pas de rejets.
- Mettre en place un groupe de travail sur les outils et les méthodes,
- Suivre les rapports et mettre au carré l'infrastructure sortante,
- Essayer d'essaimer

RENATER
CONNECTEUR DE SAVOIRS

JRES DIJON 2019

Merci à tous !

Et maintenant : dites-nous où on se plante…

« J'ai tellement appris de mes erreurs que j'envisage d'en faire quelques-unes de plus. »