

**DIGITAL**  
**TECHNOLOGY**  
**INSIGHTS**

Comment le **protocole ARC** améliore-t-il la délivrabilité de vos emails ?

**Hugo BRUNET**  
Consultant Cyber Tech & Transformation

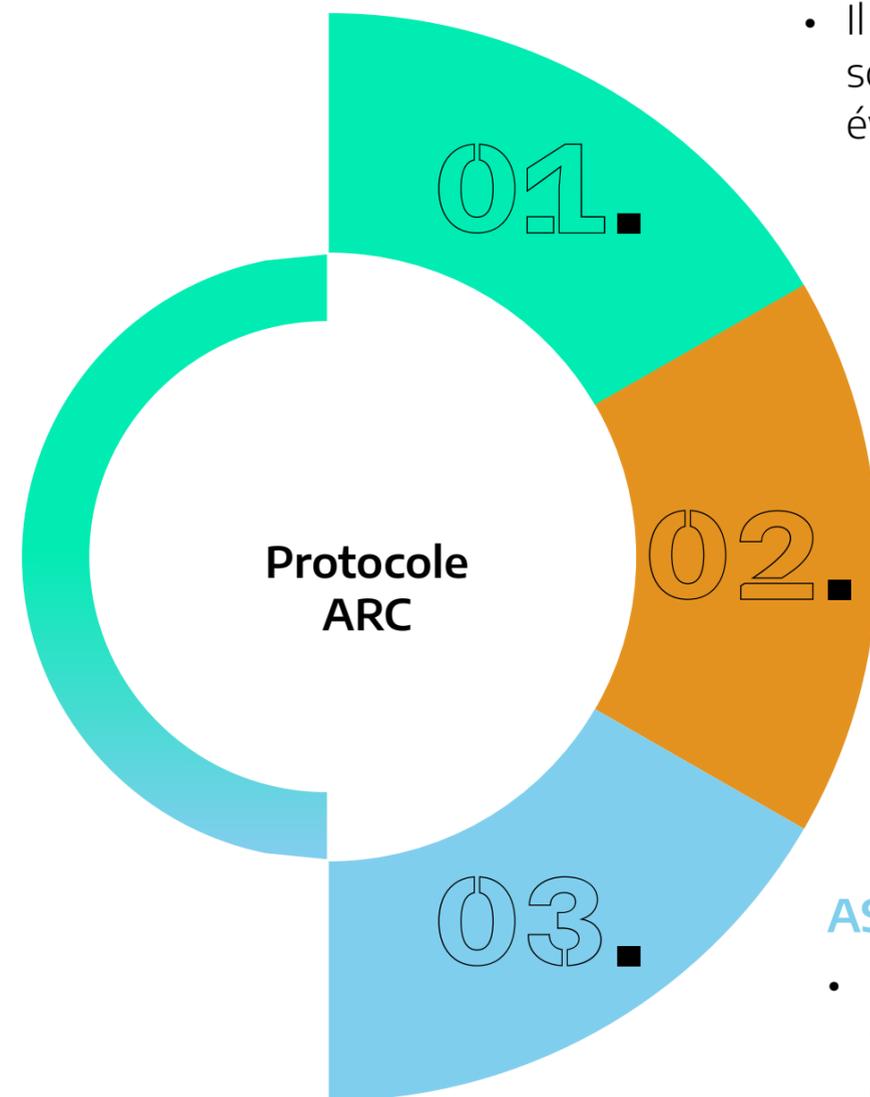


# LE PROTOCOLE ARC, C'EST QUOI ?

Le protocole ARC (Authenticated Received Chain) est un protocole qui permet de **renforcer la vérification et la traçabilité de vos courriels**, en particulier lorsqu'ils passent par plusieurs intermédiaires.

Il permet **d'améliorer la délivrabilité de vos courriels** en maintenant l'authentification des messages de bout en bout afin d'éviter les quarantaines ou les spams.

Le protocole ARC vient **consolider les protocoles d'authentification** existants tels que SPF, DKIM ou DMARC en ajoutant des sceaux pour garantir l'authenticité du courriel. Le maintien de la chaîne d'authentification ARC repose sur l'ajout de 3 en-têtes :



## AAR (ARC-Résultats d'authentification)

- Il contient les résultats d'authentification du mail au moment de son passage sur un serveur. Il indique comment le mail a été évalué en termes de SPF, DKIM et DMARC

## AMS (ARC-Message-Signature)

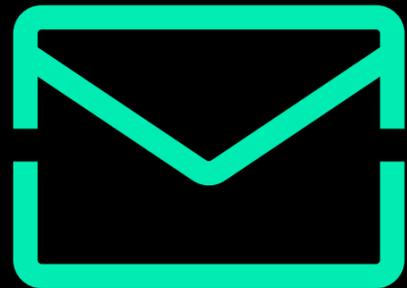
- Il contient la signature cryptographique du message, qui est similaire à celle de DKIM. Il garantit l'intégrité des informations d'authentification fournies par les intermédiaires

## AS (ARC-Seal)

- Il contient également une signature cryptographique, qui est semblable à celle du DKIM mais qui ne prend pas en compte le corps, il permet de valider tous les en-têtes ARC précédemment ajoutés, ainsi que le nouvel en-tête AMS

# POURQUOI METTRE EN PLACE LE PROTOCOLE ARC (GAINS ENVISAGÉS)

## Réduction des faux positifs



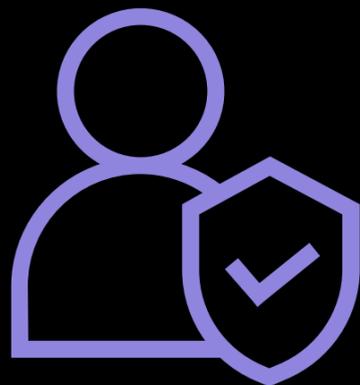
Les filtres anti-spam des serveurs de messagerie sont moins sollicités et la validation des courriels transférés est facilitée, réduisant ainsi le risque de faux positifs

## Alignement aux standards de sécurité



ARC permet d'aligner le service de messagerie aux standards de sécurité à la suite du durcissement des politiques DMARC de Google et de Yahoo

## Protection contre l'usurpation d'identité



Une baisse du phishing qui limite le risque d'utilisation malveillante des domaines de messagerie

## Amélioration de la réputation du domaine



Les domaines qui adoptent ARC bénéficient d'une reconnaissance accrue et d'une réputation renforcée notamment auprès des principaux fournisseurs de messagerie tels que Microsoft, Yahoo qui intègrent ARC

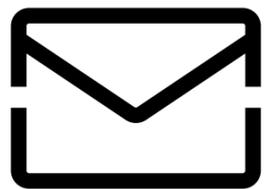
# FONCTIONNEMENT DU PROTOCOLE ARC

Pour garantir l'authentification à chaque transit, c'est-à-dire de serveurs en serveurs, le protocole ARC ajoute une chaîne de signatures numériques aux en-têtes des courriels.



## Fonctionnement d'une chaîne de mail sans le protocole ARC :

Envoi du courriel



1<sup>er</sup> serveur



Vérification et authentification du mail via les protocoles SPF, DKIM et DMARC

- Succès



Serveur intermédiaire



Le serveur change une partie de l'en-tête du mail et relais le courriel avec un autre DNS



Serveur de réception



Vérification et authentification du mail via les protocoles SPF, DKIM et DMARC

- Echec



Rejet du message ou passage en spam

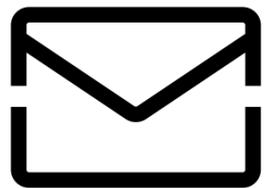


Le courriel est rejeté par le serveur du destinataire ou il passe directement dans les spams



## Fonctionnement d'une chaîne de mail avec la mise en œuvre du protocole ARC :

Envoi du courriel



1<sup>er</sup> serveur



Vérification et authentification du mail via les protocoles SPF, DKIM et DMARC

- Succès



Serveur intermédiaire



Le serveur change une partie de l'en-tête du mail et relais le courriel avec un autre DNS

- Ajout d'une signature numérique (ARC)



Serveur de réception



Vérification et authentification du mail via les protocoles SPF, DKIM et DMARC

- Validé



Acceptation du message



Le courriel est correctement transmis même après plusieurs transferts

Mise en place d'une chaîne d'authentification (ARC)

# COMMENT METTRE EN ŒUVRE LE PROTOCOLE ARC ?

Bien qu'aujourd'hui, le protocole ARC est principalement mis en place par les grands services de messagerie et les grandes entreprises, il tend à se démocratiser au sein de ETI et PME.

Pour faciliter la mise en œuvre d'ARC, il convient de respecter certaines pratiques :

## Configuration SPF et DKIM

Il faut vous assurer que ces protocoles soient correctement configurés pour votre domaine. En effet, le protocole ARC est basé sur ces mécanismes existants pour assurer l'authentification.

## Choix du fournisseur de services de messagerie

Si la mise en place de protocoles d'authentification de messagerie n'est pas votre cœur de métier, assurez-vous de faire appel à un fournisseur de services qui prend en charge le protocole ARC et qui puisse vous accompagner tout au long du processus de configuration

## Surveillance et tests

Une surveillance régulière du trafic est recommandée pour tout problème lié à la mise en œuvre d'ARC. Les tests sont essentiels pour identifier et résoudre les problèmes rapidement.

## Gardez les politiques à jour

A mesure que votre infrastructure de messagerie évolue, mettez à jour vos politiques ARC pour refléter ces changements. Des politiques obsolètes peuvent entraîner des échecs d'authentification.