**Sécuriser de la messagerie de votre organisation**

**Prévenir les attaques de phishing, usurpation d’identité et autres abus**

[Prérequis 3](#_Toc138505045)

[Recommandation 3](#_Toc138505046)

[Outils de vérification de sécurité 4](#_Toc138505047)

[**Avoir un reporting sur la sécurité** 4](#_Toc138505048)

[**Exemple** 4](#_Toc138505049)

[**Vérifier l’état de l’enregistrement DKIM (outil gratuit)** 4](#_Toc138505050)

[**Générateur de DKIM** 4](#_Toc138505051)

[Mode de fonctionnement et sécurité 5](#_Toc138505052)

[Explication 5](#_Toc138505053)

[Cheminement simplifié 5](#_Toc138505054)

[Définition 6](#_Toc138505055)

[Créer un enregistrement DMARC pour Microsoft 365 et fournisseur de nom de domaine 7](#_Toc138505056)

[**Exemple sur IONOS** 7](#_Toc138505057)

[**Les tags DMARC** 7](#_Toc138505058)

[Créer un enregistrement SPF pour Office 365 et fournisseur de nom de domaine 8](#_Toc138505059)

[Remarque 8](#_Toc138505060)

[Création des clés DKIM Office365 et fournisseur de nom de domaine 9](#_Toc138505061)

[Office365 9](#_Toc138505062)

[Fournisseur de nom de domaine 9](#_Toc138505063)

## **Prérequis**

Un compte administrateur permettant l’accès à la console d’administration Office 365 ou votre fournisseur de nom de domaine.

Générer une paire de clés RSA (Il est généralement proposé et conseillé par le registar, de sauvegarder la clé privée, lors de la création du nom de domaine)

## **Recommandation**

Le SPF peut et doit être créer lors de l’ajout du domaine après la vérification de la propriété du domaine.  
Il est de même recommandé de créer l’enregistrement DMARC avant de configurer les serveurs de courriel.

## **Outils de vérification de sécurité**

### **Avoir un reporting sur la sécurité**

Rendez-vous sur l’url [MXToolbox](https://mxtoolbox.com/) afin de tester le nom de domaine, le service est gratuit et permet d’améliorer grandement la sécurité de votre serveur de messagerie.

**Exemple**

*Retour sur mon domaine personnel, (je ne crains pas de faire apparaitre mon IP publique puisqu’elle est dynamique et ancienne.)*

**Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement**

### **Vérifier l’état de l’enregistrement DKIM (outil gratuit)**

[DKIM Record Lookup par EasyDMARC](https://easydmarc.com/tools/dkim-lookup)

Ou en vous envoyant un courriel à vous-même et en consultant l’en-tête, puis rechercher « DKIM-Signature

### **Générateur de DKIM**

[Encore une fois DKIM Record Generator par EasyDMARC](https://easydmarc.com/tools/DKIM-record-generator)

# **Mode de fonctionnement et sécurité**

## **Explication**

Le **DMARC,** utilise **deux protocoles** de sécurité de courriel :

Sender Policy Framework (**SPF**) et me DomainKeys Identified Mail (**DKIM**).

Le **SPF** permet aux organisations de **spécifier les adresses IP autorisées à envoyer des messages** pour leur domaine.

Le **DKIM** utilise des **signatures numériques** pour **vérifier** que le **message** n’a pas été **altéré** lors du transit.

Ainsi lors le fournisseur de messagerie réceptionne un courriel, il en vérifie la provenance en identifiant l’adresse IP et vérifie que celle-ci est autorisée à envoyer des courriels pour le domaine destinataire en utilisant SPF.

La **seconde vérification** est se fait via la **clé DKIM**, si celle-ci n’est pas **valide** ou ne répond pas aux exigences, le fournisseur de messagerie peut prendre les **mesures nécessaires** en fonction des **instructions** définies dans le **DMARC** configurait par l’organisation.

## **Cheminement simplifié**

L’expéditeur **envoi** un courriel, celui-ci à un **DMARC valide**, le fournisseur **vérifie** l’adresse dans l’**entête** du courriel **Mail From** et le **Recipient To**, si tout est **ok** il laisse **passer** celui-ci. Pour cela il utilise le couple SPF et DKIM, si **SPF** ou **DKIM** **échouent** lors de la vérification le serveur suit les instructions de la **politique DMARC**.

## **Définition**

**SPF (Sender Policy Framework) :** est une méthode de vérification qui permet de valider l'authenticité d'un courriel en vérifiant l'adresse IP de l'expéditeur. Lorsqu'un serveur de messagerie reçoit un courriel, il vérifie si l'adresse IP de l'expéditeur (serveur SMTP) est autorisée à envoyer des courriels pour le domaine (sous-) indiqué dans l'adresse de l'expéditeur. Si l'adresse IP est autorisée, le serveur de messagerie accepte l'email. Sinon, il peut le marquer comme spam ou le rejeter.

**DKIM (DomainKeys Identified Mail) :** DKIM est une autre méthode de vérification utilisée pour valider l'authenticité d'un courriel en vérifiant l'intégrité du contenu du courriel. Lorsqu'un courriel est envoyé, une signature numérique est ajoutée à l'en-tête du courriel. Cette signature est générée à l'aide d'une clé privée qui est associée au domaine de l'expéditeur. Lorsque le serveur de messagerie reçoit le courriel, il peut vérifier la signature en utilisant la clé publique du domaine de l'expéditeur. Si la signature est valide, cela signifie que le contenu du courriel n'a pas été modifié depuis son envoi, et le courriel est considéré comme authentique. Il s’agit d’un chiffrement asymétrique (paire de clé)

**DMARC (Domain-based Message Authentication, Reporting, and Conformance) :** DMARC est un protocole de vérification qui utilise à la fois SPF et DKIM pour améliorer la sécurité des courriels.

**Office 365**

Identifiez-vous sur <https://www.office.com/> et sélectionnez dans la partie gauche de l’interface :

« Paramètres > Domaines > Ajouter un domaine »

Sinon, rendez-vous dans la console de gestion des DNS afin d’ajouter l’entrée « TXT ».

**Fournisseur de nom de domaine**

Via l’interface de gestion, sélectionner le rouage à côté du nom de domaine (sous-) ou sur l’onglet dédié à la configuration du DNS (tout dépend du fournisseur).

## **Créer un enregistrement DMARC pour Microsoft 365 et fournisseur de nom de domaine**

1. Ajouter un **nouvel enregistrement**
2. Sélectionner **TXT** comme type
3. Définissez le nom sur **\_dmarc**
4. Définissez le contenu en l’adaptant à votre domaine et vos besoins, voici un exemple :

*v=DMARC1; p=none; rua=mailto:dmarc@mondomaine.fr; ruf=mailto:dmarc@mondomaine.fr; sp=none; aspf=r; adkim=s; fo=1*

### **Exemple sur IONOS**

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

### **Les tags DMARC**

|  |  |  |
| --- | --- | --- |
| **TAG** | **OPTIONS** | **DESCRIPTION** |
| P | none, quarantine, reject | Cette option spécifie la politique de traitement des messages. « none » pour la collecte de données initiale, « quarantine » pour marquer les messages suspects comme spam, ou « reject » pour rejeter les messages suspects. |
| sp | none, quarantine, reject | Cette option spécifie la politique de traitement des messages pour les sous-domaines. Si elle est absente, elle hérite de la politique définie pour le domaine parent. |
| rua | adresse email | Cette option spécifie l’adresse électronique pour les rapports d’activité. Elle doit être une adresse email valide et recevra les rapports de conformité DMARC. |
| ruf | adresse email | Cette option spécifie l’adresse email pour les rapports d’échec. Elle doit être une adresse email valide et recevra les rapports d’échec DMARC. |
| adkim | r, s | Cette option spécifie la méthode d’identification des clés DKIM (DomainKeys Identified Mail) utilisées pour signer les messages. « r » pour relâcher la contrainte de l’identificateur DKIM, ou « s » pour strict. |
| aspf | r , s | Cette option spécifie la politique de traitement des échecs d’identification des clés SPF (Sender Policy Framework). « r » pour relâcher la contrainte d’identification SPF, ou « s » pour strict. |
| fo | 0, 1, d, s | Cette option spécifie les rapports DMARC à générer en cas de non-conformité. « 0 » pour ne générer aucun rapport, « 1 » pour générer des rapports si l’identificateur DKIM a échoué, « d » pour générer des rapports si l’identificateur DKIM ou SPF a échoué, ou « s » pour générer des rapports pour tous les messages. |

***Afin de ne pas perdre les courriels, il est recommandé de configurer le DMARC sur p=quarantaine, ils seront déplacés dans le dossier spam.***

## **Créer un enregistrement SPF pour Office 365 et fournisseur de nom de domaine**

1. Ajouter un **nouvel enregistrement**
2. Sélectionner **TXT** comme type (ne pas confondre avec le type SPF)
3. Définissez le nom sur **\_dmarc**
4. Définissez le contenu en l’adaptant à votre domaine et vos besoins, voici quelques exemples :

***Microsoft 365***

*v=spf1 include:spf.protection.outlook.com -all*

***Google Workspace***

*v=spf1 include:\_spf.google.com -all*

Serveur Exchange on-premise

v=spf1 ip4:90.89.42.192 -all

***Si utilisation de newsletter combiner les optins pour les différents services***

*v=spf1 include:spf.protection.outlook.com include:spf.e-mailing.com -all*

## **Remarque**

Il ne peut y avoir qu’un seul enregistrement SPF par domaine

## **Création des clés DKIM Office365 et fournisseur de nom de domaine**

## **Office365**

Rendez-vous dans la console de gestion [Microsoft365 Defender](https://security.microsoft.com/)

Sélectionner dans la partie gauche

Stratégies et règles > Stratégies de menace > Paramètres d’authentification des courriels

Sélectionnez le domaine depuis lequel vous souhaitez envoyer les courriels

Sélectionnez « Créer des clés DKIM »

Copiez / collez, la valeur de la clé publique dans l’enregistrement

## **Fournisseur de nom de domaine**

Sélectionnez le rouage à côté du nom de domaine (sous-) afin de modifier les paramètres (tout dépend du fournisseur, l’interface peut être, plus ou moins explicite)

Sélectionnez ajouter un enregistrement de type CNAME

Copiez / Collez, la valeur de la clé publique dans l’enregistrement  
  
Remarque

En fonction du fournisseur de nom de domaine, il est nécessaire de désactiver le proxy pour ces entrées.

La clé privée doit être stockée sur le serveur de messagerie