

HCL Domino 12 : DKIM

Avec la version 12 de Domino, nous pouvons utiliser DKIM (DomainKeys Identified Mail) pour signer les messages envoyés par les utilisateurs internes vers des domaines internet externes. Nous allons dans cet article décrire brièvement ce que le DKIM, comment il fonctionne et comment le configurer sur un serveur HCL Domino 12.0.2.

Le DKIM, qu'est ce que c'est ?

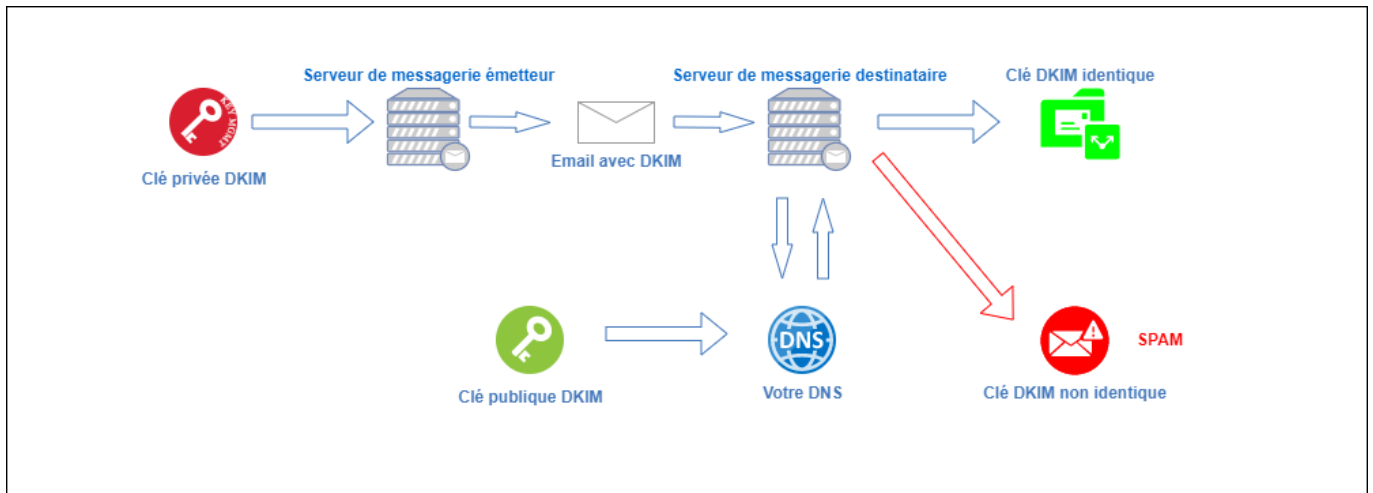
C'est une méthode d'authentification qui permet d'éviter l'usurpation d'adresses électroniques, renforce la sécurité du courrier électronique en permettant au serveur de messagerie du destinataire de vérifier l'authenticité du domaine de l'expéditeur.

Comment le DKIM fonctionne t il ?

Le concept de DKIM fonctionne avec deux clés DKIM. La clé publique de l'enregistrement DNS pour vérifier l'authenticité du message par le serveur destinataire et la clé privée pour votre serveur de messagerie dans le cadre de l'authentification.

- Envoi d'un message avec un en-tête DKIM généré par une clé privée
- Vérification de l'authenticité du DKIM de l'expéditeur
- A la réception du message par le serveur destinataire, vérification de la signature DKIM grâce à la clé publique se trouvant dans l'enregistrement DNS de l'expéditeur
- Si la clé publique correspond à la signature DKIM, le message est distribué

- Si la clé publique ne correspond pas à la signature DKIM, il est fort probable que le message soit envoyé dans les spams ou bloqué par l'antispam



DKIM et Domino

DKIM est disponible pour les serveurs Domino depuis la version 12 que ce soit sur Linux ou Windows. Voici les différentes étapes à suivre pour configurer DKIM sur votre serveur Domino.

- Création des clés de signature DKIM dans le magasin de données d'identification.
- Création d'un enregistrement TXT DNS contenant la clé et ajoutez-le à vos paramètres de domaine DNS.
- Spécification de la clé à utiliser pour la signature DKIM (via notes.ini) sur le serveur.
- Activation de la signature DKIM (via notes.ini) sur le serveur.

Création des clés de signature DKIM

```
keymgmt create DKIM domain selector RSA [keySize]
```

Avec

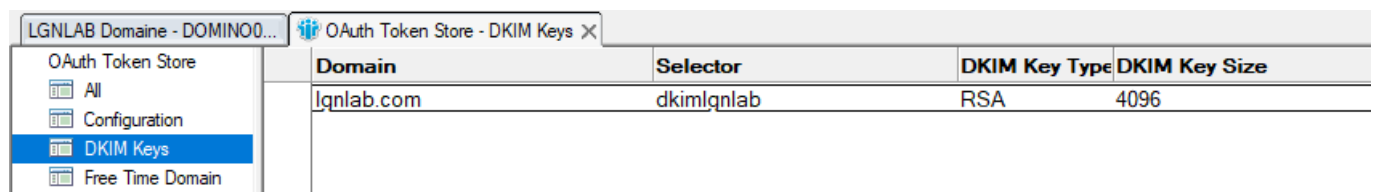
- *domain* est le nom du domaine internet
- *selector* est le nom du sélecteur que vous choisissez
- *keySize* est la taille de la clé DKIM. les tailles possibles sont 1024, 2048 et 4096

Dans notre exemple on prendre les valeurs suivantes

- *domain* : lgnlab.com
- *selector* : dkimlgnlab
- *keySize* : 4096

```
keymgmt create DKIM lgnlab.com dkimlgnlab RSA 4096
Created DKIM key dkimlgnlab._domainkey.lgnlab.com
```

La clé créé se trouve dans la base credstore.nsf dans le répertoire IBM_CredStore.



Domain	Selector	DKIM Key Type	DKIM Key Size
lgnlab.com	dkimlgnlab	RSA	4096

Création un enregistrement TXT DNS dans un fichier .txt

```
keymgmt export DKIM DNS domain selector dkimdnsfile
```

Avec

- *domain* est le nom du domaine internet
- *selector* est le nom du sélecteur que vous choisissez
- *dkimdnsfile* est le nom du fichier .txt qui contient l'enregistrement TXT DNS

Dans notre exemple on prendre les valeurs suivantes

- *domain* : lgnlab.com
- *selector* : dkimlgnlab
- *dkimdnsfile* : dkimdns.txt

```
keymgmt export DKIM DNS lgnlab.com dkimlgnlab dkimdns.txt
Parse domain lgnlab.com
Parse selector dkimlgnlab
Parse filename dkimdns.txt
Get DKIM key d=lgnlab.com, s=dkimlgnlab, No error
Get Key as PEM No error
Get Key as DNSKey v=DKIM1; k=rsa; p=<clé publique>;
Exported DKIM key to DNS file /local/notesdata/dkimdns.txt, No
error
```

Spécification de la clé à utiliser pour la signature DKIM (via notes.ini) sur le serveur.

Ajouter les informations DKIM dans la zone DNS de votre domaine.

Dans notre cas, nous allons ajouter les informations suivantes :

```
Name = dkimlgnlab._domainkey.lgnlab.com
Type = TXT
Value = "v=DKIM1; k=rsa; p=<clé publique>;"
```

Puis nous allons ajouter la ligne suivante dans le notes.ini du serveur Domino :

```
DKIM_KEY_<domain>=<selector>
```

Dans notre cas

```
DKIM_KEY_lgnlab.com=dkimlgnlab
```

Activation de la signature DKIM (via notes.ini) sur le serveur.

RouterDKIMSigning=1

Redémarrez Domino.