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

- DMARC est une règle de sécurité pour les e-mails.
- Elle permet aux propriétaires de domaines (comme "exemple.com") de dire comment gérer les e-mails suspects (par exemple, les rejeter ou les marquer comme spam).
- Cela aide à empêcher les usurpations d'identité (phishing) et donne des rapports sur les problèmes d'e-mails.

2. SPF (Sender Policy Framework)

- SPF est une liste qui dit quels serveurs sont autorisés à envoyer des e-mails pour un domaine.
- Si un e-mail est envoyé par un serveur non autorisé, il peut être marqué comme suspect.
- Cela protège contre les faux e-mails envoyés en utilisant votre domaine.

3. DKIM (DomainKeys Identified Mail)

- DKIM ajoute une signature numérique dans les e-mails pour prouver qu'ils n'ont pas été modifiés pendant leur envoi.
- Cela montre que l'e-mail vient bien de l'expéditeur déclaré et qu'il est fiable.
- C'est comme un sceau de confiance pour les e-mails.

Ces trois outils travaillent ensemble pour rendre vos e-mails plus sûrs et empêcher les attaques de phishing ou de spam. 😊

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

DMARC est une norme qui agit comme une "surcouche" à SPF et DKIM pour améliorer la sécurité des e-mails. Voici les points essentiels :

Rôle principal :

- DMARC permet au propriétaire d'un domaine de spécifier une politique pour les e-mails qui échouent aux vérifications SPF ou DKIM.
- Exemple : Vous pouvez décider de rejeter, mettre en quarantaine ou accepter les e-mails non vérifiés.

Fonctionnement :

1. Lorsqu'un e-mail est envoyé à un destinataire, le serveur de réception vérifie :
    - Si l'expéditeur est autorisé par **SPF**.
    - Si l'e-mail a une signature numérique valide avec **DKIM**.
2. Si ces vérifications échouent, DMARC indique au serveur comment traiter l'e-mail (rejeter, marquer comme spam, etc.).

Avantage supplémentaire :

- DMARC envoie des **rapports** (quotidiens ou périodiques) au propriétaire du domaine. Ces rapports montrent qui envoie des e-mails depuis votre domaine, ce qui aide à détecter les abus ou les piratages.

Pourquoi c'est important ?

- DMARC est essentiel pour éviter que des pirates utilisent votre domaine pour envoyer des e-mails de phishing ou de spam (usurpation d'identité).
- Il protège la réputation de votre domaine auprès des destinataires et des fournisseurs d'e-mails.

2. SPF (Sender Policy Framework)

SPF est un protocole de sécurité qui aide à protéger les e-mails en spécifiant quels serveurs sont autorisés à envoyer des messages pour un domaine donné. Voici une vue détaillée :

Rôle principal :

SPF empêche les expéditeurs non autorisés (comme les usurpateurs ou les spammeurs) d'envoyer des e-mails en utilisant votre domaine. Il protège ainsi contre les attaques de **phishing** et d'**usurpation d'identité**.

Fonctionnement :

1. Le propriétaire du domaine configure un **enregistrement TXT SPF** dans le DNS.
    - Cet enregistrement liste les serveurs ou adresses IP autorisés à envoyer des e-mails au nom du domaine.
    - Exemple : Un domaine "exemple.com" peut indiquer que seuls les serveurs "mail.exemple.com" ou "192.168.0.1" sont autorisés.

      v=spf1 ip4:192.0.2.1 include:mail.example.com -all

        - **ip4:192.0.2.1** : autorise cette adresse IP.
        - **include:mail.example.com** : autorise les serveurs listés dans le SPF de `mail.example.com`.
        - **-all** : rejette les messages provenant de serveurs non autorisés.
2. Lorsqu'un e-mail arrive sur un serveur de réception :
    - Le serveur vérifie l'adresse IP de l'expéditeur.
    - Il compare cette IP avec les règles de l'enregistrement SPF du domaine expéditeur.
    - Si l'IP est autorisée, l'e-mail passe la vérification SPF. Sinon, il est marqué comme suspect ou rejeté.

Avantage supplémentaire :

- **Préservation de la réputation du domaine :**
  En empêchant les usurpateurs d'envoyer des e-mails frauduleux avec votre domaine, SPF protège votre image et réduit les risques de voir vos e-mails légitimes classés comme spam.

Pourquoi c'est important ?

1. **Sécurité accrue :**
    - SPF empêche les usurpateurs d'envoyer des e-mails de phishing au nom de votre domaine, protégeant vos clients et partenaires.
2. **Confiance des destinataires :**
    - Les serveurs de réception considèrent que les e-mails conformes au SPF sont plus fiables. Cela améliore vos taux de délivrabilité.
3. **Complément avec DKIM et DMARC :**
    - Bien que SPF soit puissant, il ne protège pas contre les modifications du contenu des e-mails. Lorsqu'il est utilisé avec DKIM et DMARC, il constitue une défense complète contre les abus.

En résumé, SPF est une couche de sécurité essentielle pour protéger votre domaine et assurer que vos e-mails atteignent leur destination sans être rejetés ou marqués comme spam.

3. DKIM (DomainKeys Identified Mail)

DKIM est un système qui permet d'ajouter une **signature numérique** unique à chaque e-mail, garantissant qu'il est authentique et n'a pas été modifié.

Rôle principal :

- DKIM vérifie que le contenu d'un e-mail n'a pas été altéré après son envoi.
- Il prouve que l'e-mail provient bien du domaine déclaré.

Fonctionnement :

1. Lorsqu'un e-mail est envoyé :
    - Le serveur d'envoi ajoute une **signature numérique** (basée sur une clé privée) dans les en-têtes de l'e-mail.
    - Cette clé privée correspond à une clé publique stockée dans les **DNS** du domaine.
2. Le serveur récepteur :
    - Récupère la clé publique dans le DNS pour vérifier la signature.
    - Compare la signature avec le contenu du message et son expéditeur.
    - Si tout correspond, l'e-mail est validé comme authentique.

Pourquoi c'est important ?

- Cela empêche les pirates de modifier un e-mail en transit pour ajouter du contenu malveillant (comme des liens frauduleux).
- En renforçant la confiance, DKIM améliore les chances que vos e-mails arrivent dans la boîte de réception plutôt que d'être classés comme spam.

Résumé DMARC et DKIM :

- **DMARC** établit des règles pour gérer les e-mails suspects et fournit des rapports pour détecter les abus.
- **DKIM** garantit que l'e-mail est authentique et qu'il n'a pas été modifié, en utilisant une signature numérique fiable.

Ces deux systèmes, combinés avec **SPF**, forment une puissante défense contre le phishing et le spam.

https://dns.google/resolve?name=fredon-corse.com&type=txt

https://dns.google/resolve?name= fredon-corse.com &type=A

Récupérer la **clé publique DKIM** qui est utilisée pour vérifier les signatures DKIM des e-mails envoyés depuis **fredon-corse.com**.
https://dns.google/resolve?name=default._domainkey.fredon-corse.com&type=txt

Voici une explication simple de ce que font ces commandes :

---

1. https://dns.google/resolve?name=fredon-corse.com&type=txt

- Cette commande demande à Google DNS de récupérer les **enregistrements TXT** du domaine **fredon-corse.com**.
- Les enregistrements TXT sont des informations supplémentaires ajoutées au DNS d'un domaine.
- **À quoi servent-ils ?**
    - Ils sont souvent utilisés pour des configurations comme **SPF**, **DKIM**, ou **DMARC**.
    - Exemple : Un enregistrement TXT pourrait ressembler à ceci :

"v=spf1 include:spf.jabatus.fr -all"

    - Cela indique les règles SPF (qui peut envoyer des e-mails au nom de ce domaine).

Résumé :

Cette commande récupère les données TXT associées à **fredon-corse.com**, qui sont souvent utilisées pour la sécurité des e-mails ou d'autres configurations techniques.

---

2. https://dns.google/resolve?name=fredon-corse.com&type=A

- Cette commande demande à Google DNS de récupérer les **enregistrements A** du domaine **fredon-corse.com**.
- Les enregistrements A indiquent l'**adresse IP** associée à un domaine.
- **À quoi sert un enregistrement A ?**
    - Il connecte un nom de domaine (comme **fredon-corse.com**) à une adresse IP (par exemple, **109.234.161.215**).
    - C'est ce qui permet à un navigateur de trouver le serveur où se trouve le site web associé à ce domaine.

Résumé :

Cette commande récupère l'adresse IP correspondant au domaine **fredon-corse.com** pour que les navigateurs ou services puissent s'y connecter.

En résumé :

- La commande avec `type=TXT` interroge les informations techniques du domaine (souvent liées à la sécurité ou à des configurations).

- La commande avec `type=A` interroge l'adresse IP associée au domaine pour permettre l'accès à son site web ou serveur.

Note brouillon :

Vérifier une signature DKIM manuellement est possible, mais cela demande un peu de technicité. Voici une vue d'ensemble des étapes et des outils nécessaires :

Étapes pour vérifier une signature DKIM :

1. **Récupérer les en-têtes de l'e-mail :**
   - Chaque e-mail a des en-têtes cachés qui incluent les détails de la signature DKIM (champ `DKIM-Signature`).
   - Pour accéder aux en-têtes :
     - **Gmail :** Ouvrez l'e-mail, cliquez sur les "..." (options) > "Afficher l'original".
     - **Outlook :** Faites un clic droit sur l'e-mail > "Afficher les sources du message".
     - **Thunderbird :** Menu > "Afficher l'en-tête source complet".
2. **Analyser la signature DKIM :**
   - L'en-tête DKIM contient plusieurs champs importants comme :
     - `d=` (le domaine qui a signé le message).
     - `s=` (le sélecteur DKIM utilisé).
     - La signature proprement dite (`b=`).
3. **Récupérer la clé publique DKIM dans le DNS :**
   - Utilisez les valeurs `d=` (domaine) et `s=` (sélecteur) pour rechercher l'enregistrement DNS TXT associé.
   - Exemple : si `d=example.com` et `s=selector1`, cherchez `selector1._domainkey.example.com` dans le DNS.
4. **Vérifier la signature :**
   - Comparez la signature DKIM (`b=`) avec la clé publique récupérée dans le DNS en recalculant le hachage. Cela nécessite un outil ou un script spécialisé (voir ci-dessous).

Outils pour vérifier une signature DKIM :

1. **Outils en ligne :**
   - DKIM Core Validator : Saisissez le domaine et le sélecteur pour vérifier l'enregistrement DNS et la clé publique.
   - MXToolbox DKIM Lookup : Vérifie et analyse les enregistrements DKIM et DNS.
2. **Clients de messagerie avancés :**
   - Thunderbird peut être configuré avec des extensions comme **"Vérificateur DKIM"** pour valider automatiquement les signatures.
3. **Outils en ligne de commande :**
   - **OpenDKIM:** Un outil open-source qui peut vérifier les signatures DKIM localement.
     - Installez OpenDKIM sur un serveur ou un PC.
     - Utilisez la commande pour analyser l'e-mail brut avec la clé publique.
   - **Python scripts :** Il existe des bibliothèques comme `dmarc` ou `dkimpy` pour écrire des scripts de vérification.

- **Facile :** Utiliser des outils en ligne ou des extensions de client mail pour valider rapidement une signature.
- **Complexe :** Vérification manuelle en récupérant et comparant les clés dans le DNS, car cela implique de manipuler les en-têtes et de recalculer des signatures.