Messagerie souveraine : la checklist avant mise en service

Utilisez cette liste pour cadrer une messagerie électronique souveraine, depuis les choix de gouvernance jusqu'aux tests de restauration. Cochez uniquement les points réellement vérifiés et documentés.

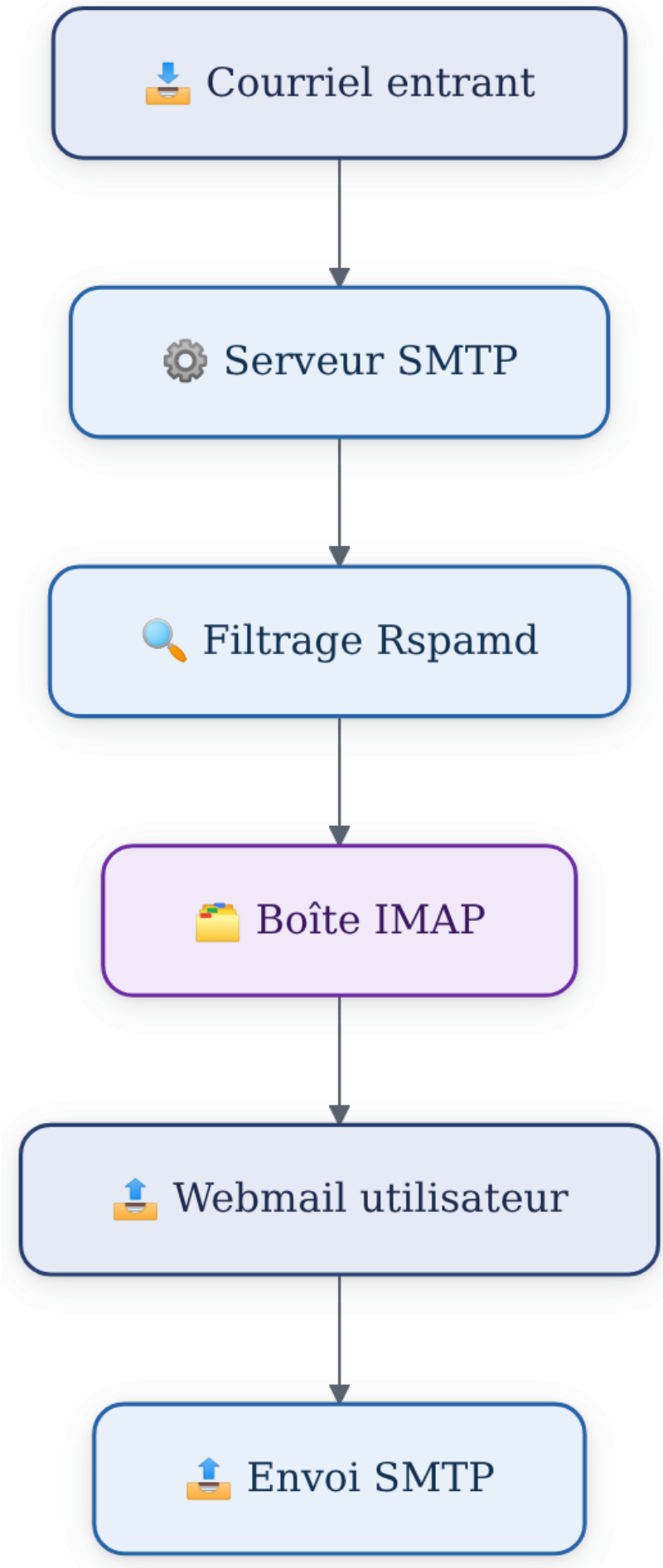
Au sommaire

Le repère essentiel

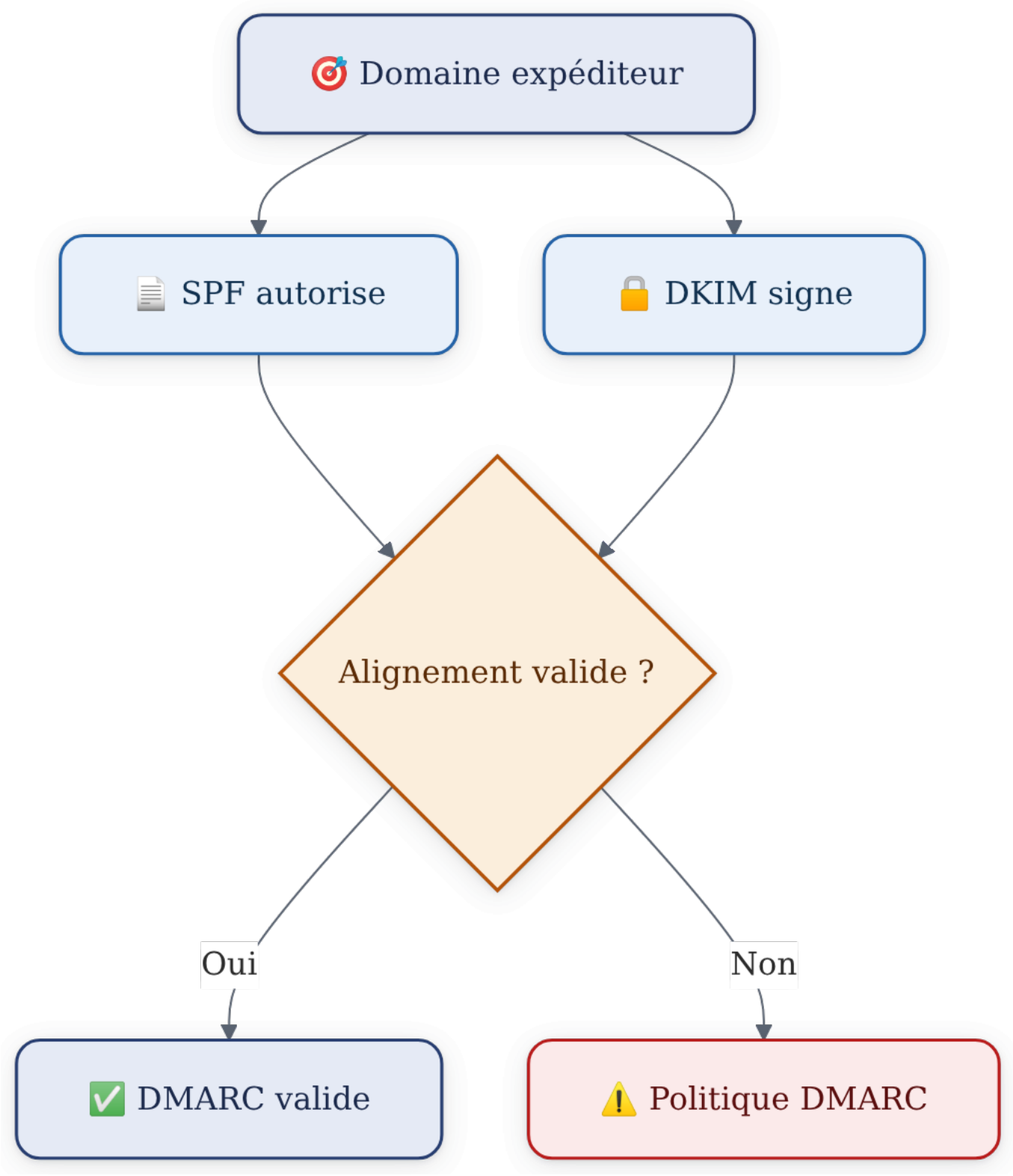
La souveraineté ne dépend pas uniquement du logiciel libre : elle implique aussi la maîtrise de l'hébergement, des données, des accès administrateurs, des sauvegardes et des conditions d'exploitation.

Le chiffrement TLS protège les échanges en transit ; il ne remplace ni la protection des comptes d'administration ni celle des sauvegardes.

Une messagerie opérationnelle doit être maintenue, surveillée et restaurable dans la durée.


Courriel entrant
Serveur SMTP
Filtrage Rspamd
Boîte IMAP
Webmail utilisateur
Envoi SMTP

INFOGRAPHIE *Schéma d'architecture de messagerie libre avec SMTP, filtrage antispam, IMAP et webmail*



INFOGRAPHIE *Infographie SPF DKIM DMARC pour sécuriser la délivrabilité des courriels*

1. Définir le périmètre de maîtrise

- [ ] **Identifier les données hébergées et leur lieu de stockage**
  Inclure les boîtes, journaux, sauvegardes et copies éventuelles.

Lister les opérateurs disposant d'un accès d'administration
Prévoir les accès d'urgence et leur traçabilité.

Vérifier les sous-traitants, la juridiction applicable et les conditions d'exploitation

Définir une procédure de réversibilité
Prévoir l'export et la migration des boîtes, données et configurations.

Faire valider les exigences juridiques ou sectorielles par les responsables compétents
Particulièrement pour les données sensibles.

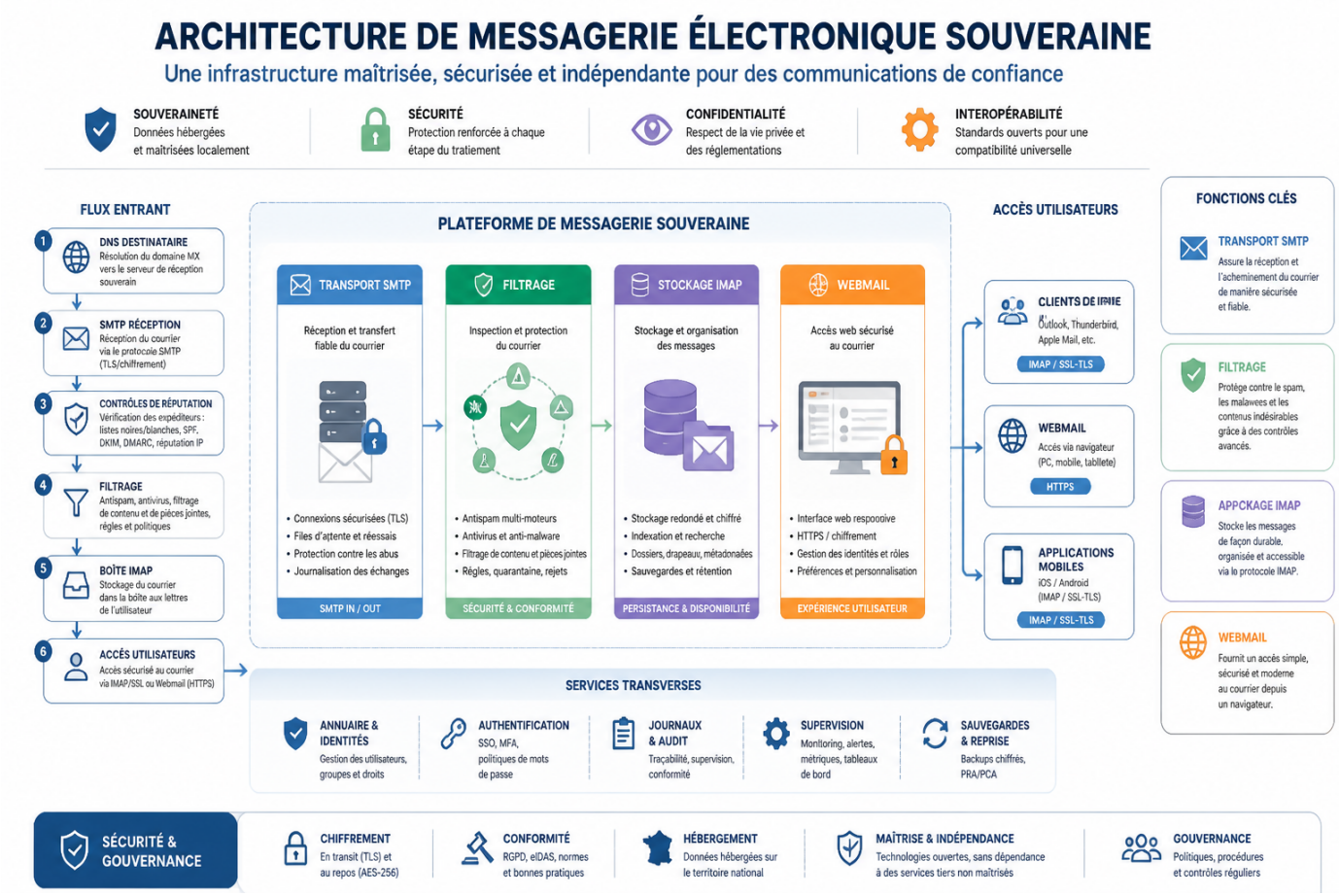


SCHÉMA *Vue d'ensemble : du DNS à l'accès IMAP dans une architecture de messagerie souveraine.*

2. Assembler les briques et leurs responsabilités

Prévoir un service SMTP pour la réception, le routage et l'envoi
Postfix est une brique libre courante.

Prévoir un accès aux boîtes via IMAP et une authentification adaptée
Dovecot est couramment utilisé pour ce rôle.

Mettre en place un filtrage antispam
Rspamd peut appliquer des contrôles, règles et politiques de filtrage.

Choisir un webmail maintenu si un accès navigateur est nécessaire
Roundcube convient à un webmail classique ; SOGo peut couvrir des usages collaboratifs.

Séparer les fonctions de transport, filtrage, stockage et accès utilisateur
Cette séparation facilite le diagnostic des incidents.

Contrôles à ne pas confondre

Sujet	À vérifier concrètement
Logiciel libre	Code auditable, possibilité d'adapter la solution et de changer de prestataire selon les licences applicables.
Hébergement maîtrisé	Localisation connue, opérateurs identifiés, sauvegardes et sous-traitants documentés.
TLS	Certificats valides, renouvellement prévu et chiffrement des accès aux services publiés.
Authentification	Comptes protégés, accès administrateurs maîtrisés et authentification forte mise en place.
Stockage et sauvegardes	Quotas, droits, chiffrement au repos si retenu, cohérence des boîtes et capacité de restauration.
Délivrabilité	DNS cohérent, identité technique des envois, réputation de l'adresse IP et traitement des refus.

3. Sécuriser l'envoi, la réception et les accès

- [ ] **Configurer correctement le DNS du domaine de messagerie**
- [ ] **Activer et contrôler SPF, DKIM et DMARC**
  Ces mécanismes contribuent à sécuriser et à rendre cohérente l'identité des envois.
- [ ] **Installer des certificats TLS et surveiller leur renouvellement**
- [ ] **Empêcher tout relais SMTP ouvert**
  Un relais trop permissif peut entraîner des abus et nuire à la réputation de l'adresse IP.
- [ ] **Protéger les comptes utilisateurs et administrateurs par une authentification forte**
- [ ] **Prévoir la journalisation nécessaire au diagnostic et au suivi des incidents**

4. Valider l'exploitation avant ouverture

- [ ] **Documenter les procédures de mise à jour de chaque composant**
- [ ] **Mettre en place une supervision des services, des journaux et des alertes**
- [ ] **Tester les sauvegardes et une restauration complète**
  Vérifier aussi la cohérence des messages et des index après restauration.
- [ ] **Tester les flux entrants, sortants, IMAP et webmail**
- [ ] **Prévoir le traitement d'un message légitime refusé ou placé en filtrage**
- [ ] **Prévoir la réponse à un compte compromis**
- [ ] **Évaluer la capacité réelle de l'équipe à assurer l'astreinte et les interventions**
  Si elle est insuffisante, un prestataire maîtrisé peut conserver une part de souveraineté sans internaliser toute l'exploitation.

> ! **Point de vigilance : la délivrabilité**
> Un serveur qui fonctionne techniquement ne garantit pas que ses messages seront acceptés partout. La réputation de l'adresse IP, la configuration DNS et la cohérence de l'identité d'envoi doivent être suivies dans le temps.

Cette checklist aide à structurer un projet de messagerie électronique souveraine ; les exigences juridiques, sectorielles et de sécurité doivent être validées selon votre contexte.