8. MOTS DE PASSE : GENERATION ET ROBUSTESSE

- GESTION DES MOTS DE PASSE SMTP2GO

GESTION DES MOTS DE PASSE SMTP2GO

Générateur de mot de passe :

Un bouton (icône de rafraîchissement, à droite du champ mot de passe) « Générer » permet de générer automatiquement, côté navigateur, un mot de passe aléatoire de 20 caractères respectant les 4 classes de caractères (minuscules, majuscules, chiffres, symboles). Le mot de passe généré est affiché en clair pour permettre de le noter ou de le copier.

Une jauge de robustesse (affichée en temps réel sous le champ, dès qu'une valeur y est saisie) :

- Une barre de couleur (rouge -> jaune -> vert) et un score en bits d'entropie estimée évoluent au fur et à mesure de la saisie.
- Un message indique, si le mot de passe est encore trop faible, les catégories de caractères manquantes (minuscules, majuscules, chiffres, caractères spéciaux) et une estimation du nombre de caractères supplémentaires nécessaires.
- Lorsque le mot de passe atteint le seuil requis, le message « mot de passe suffisamment robuste » s'affiche en vert.
- **Si le mot de passe est suffisamment robuste :** « <N> / <minimum> bits estimés - mot de passe suffisamment robuste ».
- **Si le mot de passe est trop faible :** « <N> / <minimum> bits estimés - trop faible, ajoutez : <types de caractères manquants>, et environ <N> caractère(s) de plus ».

> Le formulaire refuse la validation tant que le mot de passe saisi n'atteint pas le seuil minimum requis.

Règles à respecter pour un mot de passe :

- **À la création :** Le mot de passe est obligatoire (SMTP2GO ne renvoie jamais de mot de passe auto-généré, il ne pourrait donc pas être enregistré localement).
- **À l'édition :**
    - Le champ mot de passe est pré-rempli automatiquement (le mot de passe déjà connu localement est déchiffré et récupéré en tâche de fond au clic sur le crayon « Modifier »).
    - Laisser le champ tel quel, ou le vider complètement, conserve le mot de passe actuellement enregistré côté SMTP2GO.

    - Si un nouveau mot de passe est saisi, il doit lui aussi respecter les critères de robustesse ci-dessus.

Dans tous les cas où un mot de passe est saisi : au moins un nombre minimum de classes de caractères différentes (minuscules, majuscules, chiffres, symboles) et une entropie estimée minimale (exprimée en bits) doivent être atteints. Plus le mot de passe est long, plus il est considéré comme robuste.