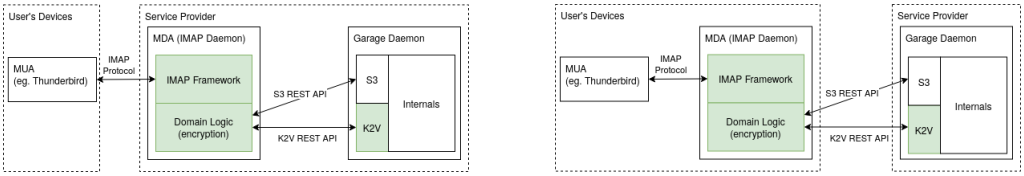

(a) Mode « transparent »

(b) Mode « chiffré de bout-en-bout »

FIGURE 1 – Comparaison entre les 2 modèles de sécurité

Définition et évaluation de deux modèles de sécurité IMAP est un protocole qui n'a pas été conçu pour être chiffré de bout en bout : le serveur exposant un service derrière ce protocole doit avoir accès au contenu des e-mails pour pouvoir répondre aux requêtes du client. Afin de contourner ce problème, nous explorons deux modèles de sécurité différents : l'un qui favorise la compatibilité au détriment de la sécurité (Figure 1a), l'autre qui favorise la sécurité au détriment de la compatibilité (Figure 1b).

Le modèle « transparent » ne nécessite aucun changement de la part de l'utilisateur dans ses pratiques : le travail de déchiffrement est réalisé par le serveur. C'est un modèle de sécurité similaire à celui de TREES [19] qui ne protège pas contre un acteur malveillant ayant accès à la RAM du serveur, mais qui protège les données quand elles sont stockées sur le disque dur et quand l'utilisateur est déconnecté.

Le second modèle, chiffré de « bout en bout », propose à l'utilisateur d'exécuter lui-même la logique du serveur IMAP sur sa machine, tel un proxy. Les données sont quant à elles toujours stockées à distance, sur le système de stockage de données distribué Garage. Le modèle de sécurité est similaire à celui de ProtonMail [1] ou Tutanota [2] avec le bénéfice supplémentaire que l'utilisateur peut continuer à utiliser son client e-mail habituel (MUA). Ces deux modèles de sécurité ont été définis en amont, sont validés en continu lors de l'avancement sur les autres étapes, et un même déploiement peut être utilisé par certains utilisateurs en « mode transparent » et par d'autres en monde « de bout en bout ».

Références

[1] Nadim KOBEISSI. *An Analysis of the ProtonMail Cryptographic Architecture*. Published : Cryptology ePrint Archive, Paper 2018/1121. 2018. URL : `https://eprint.iacr.org/2018/1121`.

[2] Scott RUOTI et Kent SEAMONS. « Johnny's Journey Toward Usable Secure Email ». In : *IEEE Security & Privacy* 17.6 (nov. 2019), p. 72-76. ISSN : 1540-7993, 1558-4046. DOI : `10.1109/MSEC.2019.2933683`. URL : `https://ieeexplore.ieee.org/document/8886906/` (visité le 14/08/2023).