Je comprends que votre objectif est d'améliorer l'efficacité de votre automatisation tout en maintenant une posture de sécurité robuste. Vous trouverez ci-dessous un aperçu détaillé du flux d'authentification recommandé.

L'utilisation d'une authentification “application seule” (app-only) basée sur des certificats est la méthodologie la plus sécurisée pour permettre à une application Microsoft Entra ID de gérer les enregistrements de sites SharePoint. Pour faciliter la capacité d'une application à modifier du contenu sur un site SharePoint connecté à Teams, Microsoft préconise une approche moderne “app-only” basée sur des certificats. Cela garantit que votre service fonctionne indépendamment d'une identité utilisateur spécifique tout en respectant des limites de sécurité strictes.

Les étapes suivantes décrivent le cadre complet requis pour mettre en œuvre efficacement ce modèle d'authentification :

Enregistrement de l'application : Le processus commence par l'établissement d'un enregistrement d'application au sein de Microsoft Entra ID pour servir de principal de service. Exigences d'authentification : Il est essentiel de noter que SharePoint Online impose l'utilisation de certificats X.509 pour l'authentification “app-only” ; les secrets clients standard ne sont pas pris en charge pour cette configuration spécifique. Stratégie d'autorisation : En ce qui concerne les autorisations, le modèle Sites.Selected est la norme privilégiée pour respecter le principe du moindre privilège. Cette configuration garantit que l'application ne possède pas d'accès non autorisé sur l'ensemble du tenant. Provisionnement au niveau du site : Une fois les autorisations consenties dans Entra ID, un administrateur doit explicitement accorder à l'application l'accès au site SharePoint cible via l'API REST ou PowerShell. Exécution opérationnelle : Suite à cette configuration, l'application peut s'authentifier via un flux d'informations d'identification client (client credentials flow) pour gérer le contenu du site via Microsoft Graph ou le modèle d'objet côté client (CSOM). Certaines considérations de sécurité critiques doivent être prises en compte pour garantir l'intégrité et la sécurité de votre mise en œuvre :

Étendue des autorisations : Veuillez noter que les autorisations sont appliquées strictement au niveau du site SharePoint et sont indépendantes de l'appartenance à Microsoft Teams. Gestion des informations d'identification : Le maintien de la sécurité de la clé privée du certificat est primordial. L'utilisation d'une solution dédiée, telle qu'Azure Key Vault, pour le stockage et la rotation est fortement recommandée. J'ai inclus les ressources suivantes pour votre référence technique :

Accorder l'accès via Entra ID app-only (SharePoint Online) En tant que modérateur, je peux fournir la carte architecturale et les meilleures pratiques pour votre conception. Cependant, je n'ai pas de visibilité sur votre environnement spécifique, tel que les configurations de votre tenant, les politiques d'accès conditionnel ou les conflits de permissions internes.