ZONEPOINT

FOR MS SHAREPOINT™ LIBRARIES

CONFIDENTIALITÉ ET CLOISONNEMENT DANS MS SHAREPOINT™

ZONEPOINT garantit la confidentialité des documents déposés dans les bibliothèques MS SharePoint™. Le chiffrement apporte cette protection à la source, depuis le terminal de l'utilisateur. Il applique le droit d'en connaître en cloisonnant l'accès aux documents de manière transparente pour l'utilisateur. Les informations sensibles publiées, partagées, ne sont accessibles qu'aux ayants droit et sont ainsi protégées contre le vol, l'espionnage et la divulgation.

Protection des partages internes des documents

Les documents sont déposés, publiés, partagés, en nombre, tous les jours, sur des sites internes MS SharePoint™ par les collaborateurs, souvent sans véritable maîtrise de qui y aura véritablement accès. En appliquant automatiquement la politique de chiffrement en fonction des dossiers, **ZONEPOINT** permet d'assurer de façon transparente le cloisonnement cryptographique entre dossiers et entre groupes de travail et garantit ainsi la confidentialité des données publiées au sein de chaque équipe. Cette gestion du droit d'en connaître peut être synchronisée avec les droits MS SharePoint™ ou Active Directory.

Protection des publications et des partages entre partenaires

Les collaborations inter-entreprises (publications scientifiques, plans pour les sous-traitants, data rooms financières,...) nécessitent une plateforme IT structurée et maîtrisée souvent par le chef de file qui permet un niveau de service suffisant pour gérer de gros volumes généralement sur le long terme. Les solutions populaires de dépôt sur internet peinent à répondre à ces besoins. MS SharePoint™ est une solution souvent retenue mais dans ce cas d'usage, son ouverture sur internet et à des partenaires tiers augmente le risque d'accès non maîtrisé aux données. En apportant une couche de chiffrement, **ZONEPOINT** permet de garantir la confidentialité des données, rendue indispensable par l'accessibilité des bibliothèques via Internet.

Confidentialité vis-à-vis de l'exploitant IT et de l'hébergeur

Le serveur MS SharePoint™ ne fait pas partie de la zone de confiance : les documents stockés sont chiffrés en permanence. À aucun moment, il n'y a passage des données en clair sur les serveurs. Les documents sont chiffrés/déchiffrés localement sur les postes de travail avec la clé de l'utilisateur. Avec **ZONEPOINT**, exploiter un serveur MS SharePoint™ externalisé est possible sans risque de perte de confidentialité.
Les données restent toujours chiffrées sur les serveurs et lors de leur transport. Cela garantit leur confidentialité vis-à-vis des exploitants. L'entreprise reste libre de la localisation de ses serveurs : interne ou externalisée chez un tiers.

Gouvernance du chiffrement par l'entreprise

Tout document déposé dans une bibliothèque est automatiquement chiffré conformément à la politique de sécurité définie par le 'propriétaire' (au sens MS SharePoint™).
ZONEPOINT permet aux responsables d'applications métier ou de la sécurité de piloter, depuis leurs postes, la mise en œuvre de la stratégie de chiffrement. Ils peuvent déléguer tout ou partie de ces opérations à certains utilisateurs habilités.

PRIMX
MAKE ENCRYPTION HAPPEN

business@primx.eu - Tél. : +33 (0)1 40 95 24 80
Siège social : 18 Rue du Général Mouton-Duvernet, 69003 Lyon / Direction commerciale : 21 Rue Camille Desmoulins, 92130 Issy-les-Moulineaux
www.primx.eu

CHIFFREMENT

- Chiffrement des bibliothèques Microsoft SharePoint™
- Accès aux documents chiffrés par le navigateur ou par l'explorateur de fichiers *(webDAV)*
- Chiffrement transparent pour l'utilisateur
- Chiffrement des données internes ou partagées avec l'extérieur

AUTHENTIFICATION

- Authentification par certificat *(PKI)* et/ou mot de passe
- Compatible avec les cartes et tokens des principaux fabricants *(poste de travail)*
- Compatible Microsoft CSP/CNG

ADMINISTRATION - IT

- Solution standard MS SharePoint™ déployable côté serveur
- Agent logiciel poste de travail pour toutes les opérations cryptographiques
- Déploiement via les infrastructures IT courantes *(SCCM, AD, etc.)*
- Pas de changement, pas d'impact dans la gestion des ressources IT

ADMINISTRATION - SÉCURITÉ

- Politiques de Sécurité définies par les responsables de la sécurité
- Plan de chiffrement administré
- Supervision de l'application des Politiques de Sécurité
- Mécanisme de recouvrement des données configurable
- Secours utilisateurs (perte de clé ou de mot de passe)

CARACTÉRISTIQUES TECHNIQUES

+ Compatible avec les serveurs **MS SharePoint™ 2019, 2016 et 2013, SharePoint™ Subscription Edition**
+ Navigateurs supportés : **Chrome, Firefox, Edge**
+ Chiffrement **AES 256**
+ Accès par **certificats/clés RSA** *(jusqu'à 4096 bits)* **et/ou mots de passe** *(de force configurable)*
+ Compatible avec les principaux **badges à crypto-processeurs** PKCS#11 *(format carte ou USB)*
+ Compatible avec la plupart des **PKI** *(IGC)* du marché
+ Application mobile : **ZONEMOBILE** sur **iOS** et **Android**

CERTIFICATIONS

EU UE RESTRICTED

Certification critères communs EAL3+

EU UE RESTRICTED

NATO OTAN RESTRICTED

Protection des données marquées : diffusion restreinte OTAN et UE

PRIMX
MAKE ENCRYPTION HAPPEN

business@primx.eu - Tél. : +33 (0)1 40 95 24 80
Siège social : 18 Rue du Général Mouton-Duvernet, 69003 Lyon / Direction commerciale : 21 Rue Camille Desmoulins, 92130 Issy-les-Moulineaux
www.primx.eu