# ZONEPOINT

## FOR MS SHAREPOINT™ LIBRARIES

CONFIDENTIALITY AND PARTITIONING IN MS SHAREPOINT™

**ZONEPOINT guarantees the confidentiality of documents deposited in MS SharePoint™ libraries. Encryption provides this protection at the source, from the user's terminal. It applies the right-to-know by partitioning access to documents in a way that is transparent to the user. Sensitive information that is published and shared is only accessible to the rightful owners and is therefore protected against theft, espionage and disclosure.**

## Protection of internal document sharing

Documents are filed, published, shared, in large numbers, every day, on internal MS SharePoint™ sites by employees, often without any real control over who actually has access to them.
By automatically applying the encryption policy on a folder-by-folder basis, **ZONEPOINT** makes it possible to transparently ensure cryptographic partitioning between folders and between work groups, thus guaranteeing the confidentiality of the data published within each team. This right-to-know management can be synchronised with MS SharePoint™ or Active Directory rights.

## Protection of publications and shares between partners

Inter-company collaborations (scientific publications, plans for subcontractors, financial data rooms, etc.) require a structured IT platform, often controlled by the lead partner, enabling a sufficient level of service for managing large volumes, generally over the long term. Popular document filing solutions on the web struggle to meet these needs.

MS SharePoint™ is a solution that is often chosen but, in this use case, its exposure on the web and to third-party partners increases the risk of uncontrolled access to the data. By providing an encryption layer, **ZONEPOINT** guarantees data confidentiality, made indispensable by the accessibility of libraries via the Internet.

## Confidentiality in relation to the IT operator and the hosting provider

The MS SharePoint™ server is not part of the trusted zone: stored documents remain permanently encrypted. At no time does the data switch to unencrypted status on the servers. The documents are encrypted and decrypted locally on the workstations with the user key.

With **ZONEPOINT,** an outsourced MS SharePoint™ server can be used with no risk of compromised confidentiality.

The data always remains encrypted on the servers and during transit thereby guaranteeing their confidentiality vis-à-vis the operators. Companies are free to choose where to host their servers: in-house or outsourced to a third party.

## Corporate governance of encryption

Any document filed in a library is automatically encrypted in accordance with the security policy set by the "owner" (in the MS SharePoint™ sense of the term).

**ZONEPOINT** allows business line application or security officers to coordinate from their workstations the application of their encryption strategy.

They can delegate some or all of these operations to certain authorised users.

PRIMX
MAKE ENCRYPTION HAPPEN

**business@primx.eu - Tel: +33 (0)1 40 95 24 80**
Head Office : 18 Rue du Général Mouton-Duvernet, 69003 Lyon / Sales Department : 21 Rue Camille Desmoulins, 92130 Issy-les-Moulineaux
**www.primx.eu**

## ENCRYPTION

- Encryption of Microsoft SharePoint™ libraries
- Access to encrypted documents via browser or file explorer *(webDAV)*
- Transparent encryption for users
- Encryption of internal or externally-shared data

## AUTHENTIFICATION

- Authentication by certificate *(PKI)* and/or password
- Compatible with cards and tokens from major manufacturers *(workstations)*
- Compatible with Microsoft CSP/CNG

## ADMINISTRATION - IT

- Standard MS SharePointTM solution that can be deployed server-side
- Workstation software agent for all cryptographic operations
- Deployment via standard IT infrastructures *(SCCM, AD, etc.)*
- No change, no impact in the management of IT resources

## ADMINISTRATION - SECURITY

- Security policies defined by security officers
- Administered encryption plan
- Supervised application of security policies
- Configurable data recovery mechanism
- User support *(loss of key or password)*

## TECHNICAL SPECIFICATIONS

+ Compatible with **MS SharePointTM 2019, 2016 et 2013, SharePointTM Subscription Edition** servers
+ Supported browsers: **Chrome, Firefox, Edge**
+ **AES 256** encryption
+ Access via **certificates/RAS keys** *(up to 4096 bits)* and/or passwords *(configurable strength)*
+ Compatible with all major PKCS#11 **cryptoprocessor passes** *(smartcard or USB format)*
+ Compatible with most **PKI** on the market
+ Mobile app: **ZONEMOBILE** on **iOS** and **Android**

## CERTIFICATIONS

EU UE RESTRICTED

NATO OTAN RESTRICTED

Endorsed for protecting EU and NATO information

CERTIFIED CC EAL3+

Common criteria certification at the level EAL3+

PRIMX
MAKE ENCRYPTION HAPPEN

**business@primx.eu - Tel: +33 (0)1 40 95 24 80**
Head Office : 18 Rue du Général Mouton-Duvernet, 69003 Lyon / Sales Department : 21 Rue Camille Desmoulins, 92130 Issy-les-Moulineaux
**www.primx.eu**