ORIZON

FOR CLOUD STORAGES

CONFIDENTIALITY OF DOCUMENTS IN THE CLOUD

ORIZON guarantees the confidentiality of files uploaded to the Cloud. Encryption provides this protection at the source, from the user's terminal. It establishes the right-to-know with data being protected from unwanted access by the Cloud storage provider, employees or external contacts.

Company sovereignty over its data

File synchronization services in the **Cloud** or in an internal enterprise file sync & share ***(EFSS)*** type system for storage, sharing, and backup expose data to the risk of theft, disclosure, and espionage during transport and storage. The company no longer has full control over who can access this data and does not know the degree of porosity or level of risk exposure (interference, hacking and security breaches, Cloud provider personnel). The right-to-know afforded by encryption provides a strong and mathematical answer that guarantees that the information is only intelligible to authorised persons, while maintaining the flexibility and elasticity of the Cloud.

Protected synchronised data

ORIZON automatically protects documents stored by users in the Cloud since the files are encrypted, as soon as they are created and in real time, at the source location. They continue to remain encrypted when they are synchronised and then stored with the host (including during file transport). They can only be decrypted by the authorised user(s) (in possession of the appropriate keys) on the terminal of their choice. In this way, only these users *are able to understand* the content of the documents.

Sharing confidential documents

ORIZON automatically encrypts all synchronised documents. If a file share is in place, the corresponding cryptographic rights are applied automatically, specifically and solely for the rights holders. The right-to-know is also assured on Cloud shares, and **ORIZON** guarantees partitioning of this information between users, services and service providers, but above all with the Cloud provider. What is more, even external partners can work on encrypted documents that are shared with them thanks to a free, multi-platform version of **ORIZON**.

No impact on the user experience

Designed to be transparent, **ORIZON** remains highly discreet and imposes no changes on user working habits. Collaboration and ubiquity of access to data (in the office, at home, on a telephone, on a tablet) are preserved. Any type of file can be encrypted without any user interaction.

Security governance

ORIZON applies the encryption policy defined by the company: shared / unshared, all synchronised folders, or just one "strongbox" folder. Different types of access keys are possible (smartcards, certificates, passwords, etc.) and recovery (SOS) accesses can be imposed.

Light and non-structural solution

ORIZON imposes no changes whatsoever. Present only on workstations or mobile devices, it is deployed like any other component of the office software platform, and is simply downloaded from the Company's app stores or from official mobile terminal app stores.

CONNECTORS

OneDrive

Dropbox

ENCRYPTION

- Zone encryption of synchronised folders
- Encryption on-the-fly, transparent for users
- Encryption of internally 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

- Workstation software agent, no server component
- Deployment via standard IT infrastructures (SCCM, AD, etc.), available on app stores
- 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 most EFSS solutions on the market (OneDrive™, Google Drive, Box, Dropbox™, etc.)
- **Windows** 7 to 10+
- **AES 256** encryption
- Access via **RSA certificates/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

PRIMX
MAKE ENCRYPTION HAPPEN

business@primx.eu – **Tel.: 01 77 72 64 80**
Head Office: 18 Rue du Général Mouton-Duvernet, 69003 Lyon / Sales Department: 21 Rue Camille Desmoulins, 92130 Issy-les-Moulineaux
www.primx.eu