CYBER SECURITY

C2TECH

KRYPTOS

CUSTOS™ SOLUTIONS

HIGHEST SECURITY
FOR YOUR FILES,
FROM ANYWHERE,
MADE SIMPLE

www.kryptos.com.tr

TURKISH AEROSPACE SUBSIDIARY

OUTLOOK ADD-IN

Outlook users can send and receive secure emails using KRYPTOS without any knowledge of information security or encryption. KRYPTOS does not change the day-to-day user experience of Outlook. It just adds an ”Encrypt” option to the Outlook ribbon and everything else is handled in the background by KRYPTOS.

ZERO KNOWLEDGE

On our servers, we only store data that identifies you as a KRYPTOS user and validates your license. All other data is encrypted on your device before it is transferred to our servers.

ENTERPRISES

Many more features for enterprises; corporate backups using a Golden Token, central user management, policy customizations, auditing, on-premise installations for critical or regulated environments.

PLANS

	Basic Plan	Premium Plan	Enterprise Plan
Hybrid Encryption AES/RSA	●	●	●
Operating System (Windows, MacOSX, Android, iOS)	●	●	●
Transparent End-to-End Encryption	●	●	●
Virtual Disk	●	●	●
FIPS 140-2 Level 3 Certified PKCS11 Hardware Token	●	●	●
Zero Knowledge	●	●	●
Cloud Service	●	●	●
E-mail Encryption		●	●
Collaboration		●	●
Key Management			●
User Management			●
Policy Management			●
On Premise			●

WHEN YOU NEED DATA ENCRYPTION?

With cloud storage services becoming a standard for business, data security is an increasing concern for enterprises. It's clear that cloud storages either public or private aren't exactly as secure as they were made out to be.

By encrypting your data, you can add a layer of protection before they synchronize to the cloud. But who will hold the keys? No matter what security measure you have, you can't be sure where your data will end up when someone else handles the keys. KRYPTOS decouples the data, that is stored either on Dropbox, Google Drive, etc. or on your private cloud, and the encryption keys required to access it.

EU-GDPR COMPLIANCE

"In order to maintain security and to prevent processing in infringement of this regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption." (EU-GDPR)

KRYPTOS makes use of the most secure encryption algorithm, to date. Therefore, KRYPTOS is considered to be an "appropriate technical and organizational encryption measure" to protect personal data according to EU-GDPR.

Process-oriented Measures EU-GDPR Implementation

With KRYPTOS, you do not need to change much in existing processes. All the data is encrypted conveniently in the background.

Employees and Data Protection

KRYPTOS does not require any IT expertise. There is no disruption to existing processes and employees are able to continue working efficiently, right from day one using KRYPTOS. Hence, you do not need to train your employees in order to use KRYPTOS.

EASY FOR EVERYONE

There is no disruption to existing processes and employees are able to continue working effciently, right from day one using KRYPTOS. Hence, you do not need to train your employees in order to use KRYPTOS.

- KRYPTOS does not require any IT expertise
- There is no disruption to existing processes and employees are able to continue working effciently, right from day one using KRYPTOS
- Hence, you do not need to train your employees in order to use KRYPTOS

TRANSPARENT END-TO-END ENCRYPTION

KRYPTOS creates a virtual hard drive that you can work on it as if it were a USB thumb drive that automatically encrypts its contents. This virtual hard drive becomes a proxy for your encrypted data living in the cloud or in a network share and provides a seamless user experience.

KRYPTOS encrypts every file you put onto this virtual drive using a unique per-file key, on your device, before it's synchronized to its final location. Per-file keys are encrypted using your personal key that is stored securely in a PKCS11 Hardware Token.

This double encryption scheme utilizing AES and RSA provides the highest level of security for your files.

COLLABORATION

You can allow a colleague to access your protected files/folders securely, send/receive secure emails and you can even create groups to manage file sharing in larger environments.

MULTI CLOUD

KRYPTOS works via the local folder, managed by the synchronization client of your cloud storage provider. Therefore, it is Cloud-Neutral and seamlessly integrates with any cloud provider.