

TAKAKRYPT Data Security Protection

Enterprise-Grade data protection made simple

Overview

TAKAKRYPT offers innovative and adaptive solutions for data security. Our products and services are specifically designed to meet the needs of various business sectors. Our mission is to protect sensitive data from theft and misuse while ensuring the smooth continuity of your business operations.

Secure your data with cutting-edge encryption

Data Encryption

We use industry standard RSA and AES algorithms to convert sensitive data into secure, unreadable text that can only be accessed through authorized decryption.

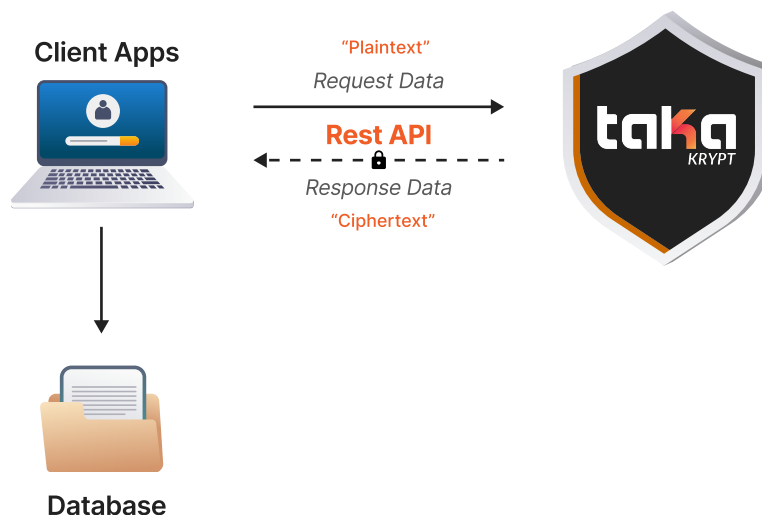
Tokenization

Using format-preserving encryption (FPE), we replace sensitive data with tokens that keep the original format, enabling secure use across systems without exposing real values.

Data Masking

Data masking hidden original information to prevent exposure and ensure it can't be misused.

How TAKAKRYPT Secures Data





Capabilities

a. Data protection techniques

- Transparent encryption for files & databases
- Format-Preserving Encryption (FPE)
- Tokenization with dynamic data masking
- Static data masking

b. Monitoring and reporting

c. Audit Log

- Track every user activity, including access, changes, or other actions performed on data.
- Provide historical data that can be used to investigate security incidents and identify unauthorized access or misuse of access rights.
- Integrated with other system log.

d. Integrated with REST API

e. External KMS Integration (Support with KMIP)

TAKAKRYPT Product Benefits



Secure Access

TAKAKRYPT protects sensitive data in your business from unauthorized access while reducing the risk of data breaches and redirects.



Transparent Auditability

TAKAKRYPT provides audit log and reporting features to monitor data access and use transparently, making investigations and audits easier.



Threat Isolation

With TAKAKRYPT data protection, the system can operate smoothly without interference from both external and internal threats.



Flexible Deployment

TAKAKRYPT enables flexible data protection both in the cloud and on-premises, providing greater control without compromising



Regulatory Compliance

TAKAKRYPT help companies meet data protection standards by Law UU PDP No. 27 of 2022.



Risk Mitigation

TAKAKRYPT helps businesses mitigate sensitive data risks by identifying threats and protecting against potential financial and reputational

Specification	Data Encryption	Tokenization	Data Masking
Algorithm Method (AES, RSA, dan FPE)	 AES (128/256) RSA (1024/2048/4096)	 FPE (FF1 & FF3-1)	
Identity Data Types (ID number, passport, driver's license, tax identification number, and credit card)			
General Data Types (Email, IMEI, IP Address and Date)			
Method Parameters (Alphabet, Numeric, Alphanumeric, and Special Characters)			
Interfaces Method (REST API, and Command Line)			



Environments

Clouds & On-Premise

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure

Supported OS

- Linux
- Windows

