

TAKAKRYPT Batch Transformation

Enterprise-Grade data protection made simple

Overview

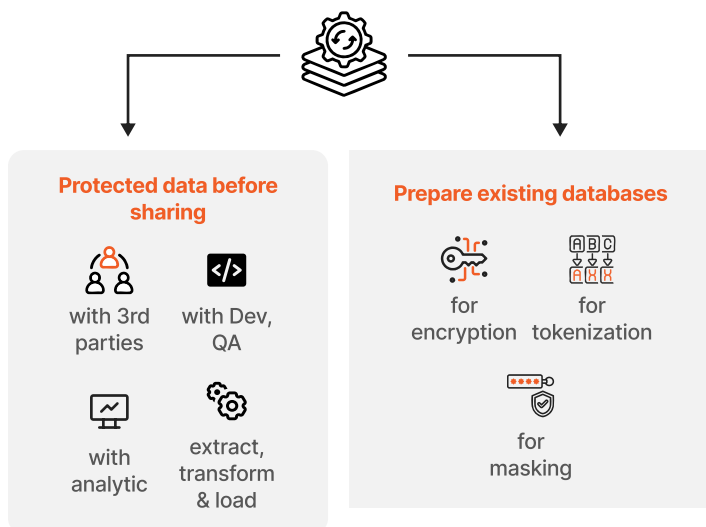
TAKAKRYPT Batch Transformation (TBT) provides high-performance data encryption with centralized key management, using TBT to support encryption, tokenization, and masking for fast protection of large volumes of data.

Static Data Masking has many use cases, such as:

1. Prior to sharing data with third parties.
2. In databases shared with development, QA, R&D or analytics.
3. Before adding a data set to a big data environment.
4. In advance of extract, transform and load (ETL) operations.

Other Use Cases Include

- Preparing a database for a tokenization or encryption deployment.
- Rekeying an encrypted column of data.



Key Benefits

Data transformation options:

- Enable database sharing with reduced risk
- Accelerates protection of existing data
- Static data masking where you need it. Deploy on premises, in the cloud, or as a hybrid deployment.

Technical Specifications

Data Transformation Options:

- Tokenization, Data Encryption, Masking
- Formatting, preserving alpha/numeric.

Policy Options:

- Specific action for each individual column transformation Encrypt, decrypt, tokenize, de-tokenize and key rotation
- Easy to apply encryption without the need for application changes
- Key management is handled through TAKAKRYPT.

Data Security Platform Requirements

- Key sources: TAKAKRYPT Data Protection.

Supported Database

- MariaDB (12.1.2, 11.8.5, 11.4.9)
- PostgreSQL (18.1, 17.7, 16.11)
- MS SQL (2025, 2022, 2019)
- Oracle (23c (beta), 19c, 21c*)
- MySQL (8.4.3, 9.1.0, 9.0.1)

Hardware and Operating System Requirements:

- Processor with 4 cores, 16GB RAM (minimum)
- Windows
- Linux – CentOS & Ubuntu.

Technical Specifications	
Data Transformation Option	• Tokenization • AES-256 Data Encryption • Static Data Masking • Format-preserving alpha/numeric transformations
Policy Options	• Per-column granular control • Encrypt / decrypt / tokenize / detokenize / mask • Key rotation without application changes • Fully integrated with TAKAKRYPT Key Manager
Platform Requirements	• TAKAKRYPT Data Protection (key sources) • On-premises, private cloud, or public cloud support
Hardware & OS Requirements	
CPU	4 cores (recommended)
RAM	16 GB (recommended)
Operating System	• Windows • Linux - Debian, CentOS & Ubuntu