Get started with Encryption

Privacera Encryption enhances the data security provided by Privacera Access Management and Privacera Discovery.

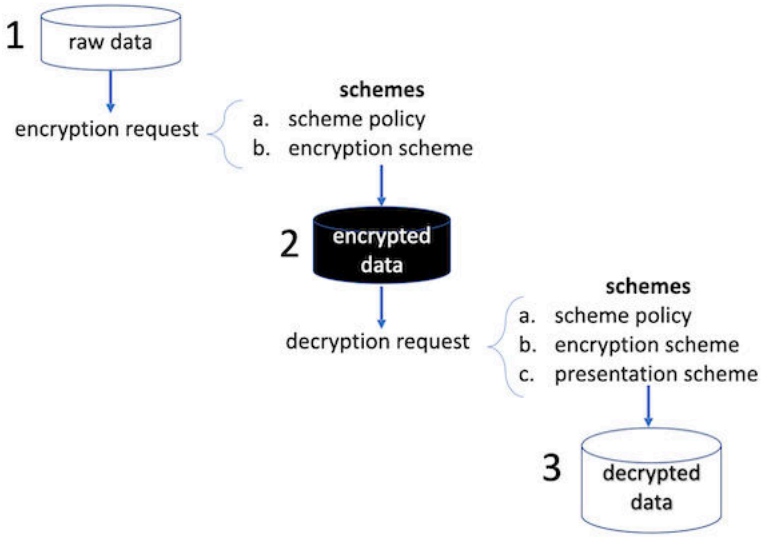
You can encrypt tables, columns, rows, fields, or other data in connected systems. Even if the data are accessible by policies created in Privacera Access Management, the encrypted data cannot be seen.

Encryption can be two-way: you can encrypt the data in place and decrypt it later. Or it can be one-way: with hashing or overwriting with string literals. You can replace the original data to make it invisible and unrecoverable.

You can also completely mask data with a one-way transform.

The encryption process

The following graphic shows the general process of Privacera Encryption.



The Privacera encryption process is:

1. An endpoint is called to encrypt raw data.
   a. The scheme policy protecting access to encryption functions is checked.
   b. The encryption scheme encrypts the data according to its associated format, algorithm, and scope [32].
2. The data is encrypted.
3. An endpoint is called to decrypt the encrypted data.
   a. The scheme policy protecting access to encryption functions is checked.
   b. The same encryption scheme that encrypted the data is used to decrypt according to the encryption scheme's format, algorithm, and scope [32].
   c. The presentation scheme obfuscates the decrypted data for presentation to the user.

Encryption architecture and UDF flow

The following diagram shows the PEG architecture for viewing a record. For a description of the keys in this architecture, see Encryption keys [18].