PRISMA/DB Overview

Prisma/DB is a secure data management and processing platform with a primary focus on data confidentiality. Exposing rich querying capabilities and high performance, it guarantees confidentiality of stored and processed data even if the storage infrastructure is compromised. Even in case of an attacker gaining full control over the database server (e.g., an intruder or a compromised employee), the data is protected by strong cryptography, and the system architecture ensures that the encryption keys never leave trusted perimeter.

Prisma/DB can use one of the well-established database management systems as a storage backend. Prisma/DB provides per-column encryption granularity and enables operations over encrypted columns without *ever* sharing private keys with the untrusted components. Prisma/DB was created as a result of years of meticulous research done within Cyber Security Lab, Nanyang Technological University, Singapore. Prisma/DB puts together many well-established cryptosystems and secure data processing techniques and makes them work together in a seamless way.

There is a multitude of database security solutions on the market. An absolute majority of database encryption products available today provide a so-called Transparent Data Encryption (TDE): the database server encrypts and decrypts the data when it is written to and read from disk. While efficient and simple, TDE has major drawbacks: it only protects data-at-rest, leaving out data-in-use and data-in-motion; it requires that the private key is stored within the database server—a blocking issue for over 60% of polled institutions, according to 2015 Cloud Security Alliance report. Another solution that is available on the market today is "Always Encrypted", a feature of MS SQL Server 2016 and newer. However, while "Always Encrypted" is built on similar principles as Prisma/DB, it provides much narrower capabilities while requiring higher integration costs.

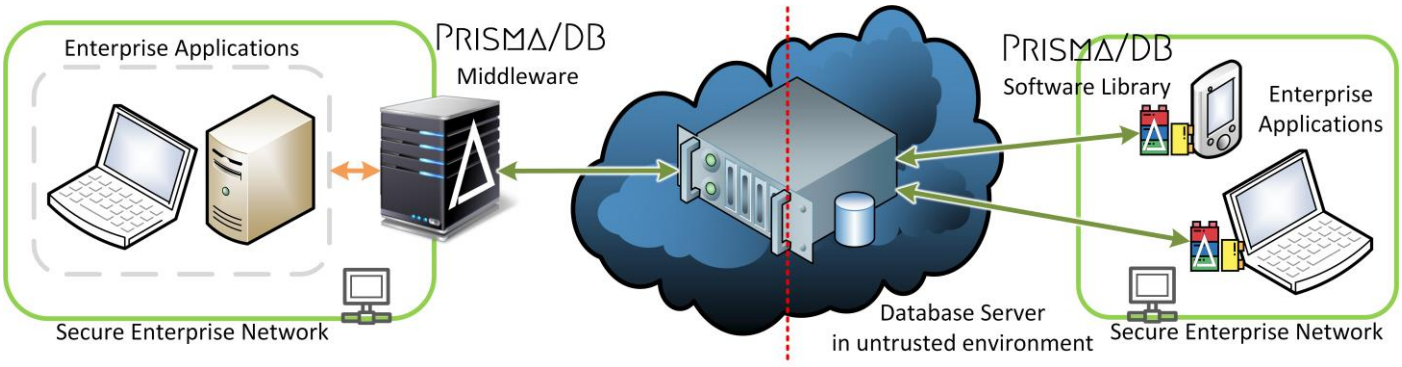

Figure 1. Two modes of operation. As a middleware (or a proxy, left) or as a software library (right). Private keys never leave secure perimeter.

Prisma/DB comes in two "flavors": as a stand-alone transparent middleware, and as a software library. The proxy holds the private and public keys, intercepts queries from applications to the database, transforms and encrypts them and sends to the database server. When the database server sends an encrypted result of the query, the proxy intercepts it, decrypts, and hands back to the application. By fully implementing the database network protocol, the proxy generally does not require any changes to the application code. The software library "flavor" can provide a tighter coupling and alleviate unnecessary overhead but requires minor changes to the applications to use the library instead of the regular database client driver libraries.

Prisma/DB supports Microsoft SQL Server, MySQL and MariaDB, CockroachDB and PostgreSQL. Prisma/DB Software Library can be used with any .NET and compatible language. Prisma/DB currently uses a synergy of AES, ElGamal and Paillier cryptosystems, HMAC-based and other types of hashes, and could be easily extended to use any other cryptosystem due to its modular design.