Inpher _*ultra* SDK Description and Pricing

August 10, 2016

for more information contact info@inpher.io

Inpher _*ultra* SDK: Modules and Functional Description

The following describes the functionality and basic components of each module. For a full technical description, dependencies, and sample applications please reference our online documentation at https://dev.inpher.io

Encrypt.

The **Encryption Module** enables trusted and easy implementation of data/file encryption. Components include:

Authenticated Randomized Encryption

The Inpher recommended method. Plaintext is transformed to randomized ciphertext on each encryption, and adds authentication tags which are verified on decryption. Useful when specific, sensitive plaintext needs to be consistently protected and authenticated.

Order Revealing Encryption (ORE)

Useful when it is required to perform order comparison on the ciphertexts. When encrypting data which can be ordered such as dates, ORE allows comparison of the order between two ciphertexts. This method will reveal the plaintext order to an attacker and is recommended only when the order in the data is not sensitive.

Deterministic Encryption

The same plaintext will always generate the same ciphertext. This method should only be used when explicitly required.

Collaborate.

The **Secure Data Collaboration Module** (which includes the Encryption Module) allows you to build applications with multi-user support, secure data sharing and synchronization of shared data across users, with standard storage infrastructure.

Key Management

Data session keys are encrypted with a password-derived key, providing maximum flexibility across endpoints. Standard features such as key recovery and rotation are included. There is also an option to use third-party systems to generate and manage persistent keys.

Secure Data Sharing

Secure data sharing utilizes both private and public key cryptography. Data sharing is achieved with a single key exchange so even massive data sets are immediately available for collaboration.

Encrypted Data Storage

Provides the application an abstract interface to a fully encrypted backend file system or DB such as HDFS, Hadoop, MongoDB, AWS S3 etc.

Query.

Sensitive data can be encrypted, indexed and searched using the **Encrypted Query Module**. Compatible with standard search engines Solr and Elasticsearch, it can be quickly deployed on existing infrastructure. The index, keyword searches and results are all encrypted so the hosting provider has no visibility. Additionally, Inpher uses proprietary obfuscation techniques to protect against static attacks on the index. Components include:

Parsing, Indexing and Encryption

Data is parsed, indexed and encrypted on the trusted endpoint application or device. Custom parsers can be used.

Search

Available search functionalities include ranking, stemming, disjunctive queries, boolean queries, and global queries across sharing groups when using the **Secure Data Collaboration Module.**