DATASHEET

Data Security SDK

Easy-to-use developer kit to secure digital assets everywhere.

BENEFITS

- Easily integrate security into your applications and products
- Single solution to protect both data in-transit and at-rest
- Extremely low system overhead – works even on a gen1 Raspberry Pi
- Supports live streaming content with no latency
- Hardened encryption and delivers "always-on" compliance
- Transmission-agnostic, operating over Internet Protocol (IP), radio, cellular, microwave, or satellite
- Perfect for any application including IoT environments

TECHNICAL SPECIFICATIONS

What's included in the SDK:

Executables:

- CLI program- Command line-based program that can be used to protect data on a drive or used as a receiver/transmitter to quickly stream encrypted data across a network.
- API header files- Source files you'll need to incorporate into your project.

Libraries:

- DLL files- Libraries needed for Windows platforms
- Static Object .so files- Libraries needed for Linux-based platforms

Documentation:

- API documentation and instructions- Description of functions your program will call to interact with the Ubiq libraries.
- CLI documentation- ReadMe describing how to use the CLI program to encrypt/decrypt and stream data.
- Sample scripts and programs

Supported Platforms:

Software Development Environments:

- Linux-based platforms (Ubuntu, Red Hat, CentOS)
- Windows (7,8,10 and Server)

Generate Executables that Run On:

- Ubuntu 16.04 and up
- CentOS/RedHat 6.9 and up
- Windows 7,8,10 and Server
- Android 6 and up

Contact us to learn more!
www.ubiqsecurity.com

DATA, DATA, EVERYWHERE

The network perimeter has disappeared due to collaboration, mobile and cloud, and the convergence of IT and operational technology (OT) enterprise networks. This is effectively creating a far more complex environment.

Organizations are gathering and storing vast amounts of sensitive data across multiple domains, systems and devices. It is imperative to provide continuous data protection to safeguard against insider threats and hostile intruders without impacting standard business operations, system performance, and efficiency.

HERE'S HOW UBIQ HELPS

Ubiq has developed a patented, 100% data security software solution to support the unstoppable data growth fueled by cutting-edge technologies such as virtualization, image recognition, video analytics, IoT and edge computing, AI, machine learning and big data analytics.

Ubiq developed and patented an **asynchronous multithreading** technique, which allows us to exploit available compute on a system, without impacting system performance. We then leverage this technique with our data security model, which involves a 4-step-process to secure any data type:

1. Fragmentation
2. Disassociation
3. Encryption
4. Dispersion

Each fragment (and you can make as many as you like) is encrypted with its own unique encryption key (AES 256 out-of-box) and can be stored separate from the other fragments. If an encrypted fragment is intercepted in-transit or accessed at-rest, it is nearly impossible for the bad guys to make any use of it. They don't know what data type it is or if it represents all or just a small portion of the data. This renders the stolen data useless.

UBIQ DATA SECURITY SDK

The Ubiq SDK allows you to leverage our core technology to efficiently secure digital data of any type.

With the Ubiq SDK, you can engineer solutions that:

a) Encrypt data and store it anywhere the device can access - local disk or cloud storage
b) Retrieve and decrypt Ubiq protected data
c) Stream data securely from A to B in real-time (including live video)
d) Create a secure remote access function
e) Restrict access to Ubiq protected data
f) Securely encrypt and decrypt files within a local or remote filesystem

UBIQ

STREAM ENCRYPTED DATA BETWEEN DEVICES

The Ubiq technology has been architected to allow data to be streamed between any endpoints and allows you to customize the network topology or protocol as required by your application. Ubiq encrypts the data on the sender prior to transmission, and after transmission over your network. Ubiq then decrypts the data within the consuming application (eg. video player) or it an be saved as a file for later use.

Ubiq can also simultaneously send the encrypted data over multiple pathways to a sender (e.g. WiFi, LTE, satellite), greatly enhancing performance and security.

An example of this technology in use is an Android-based camera App, where video data is captured on the device and transmitted securely to a remote receiver.

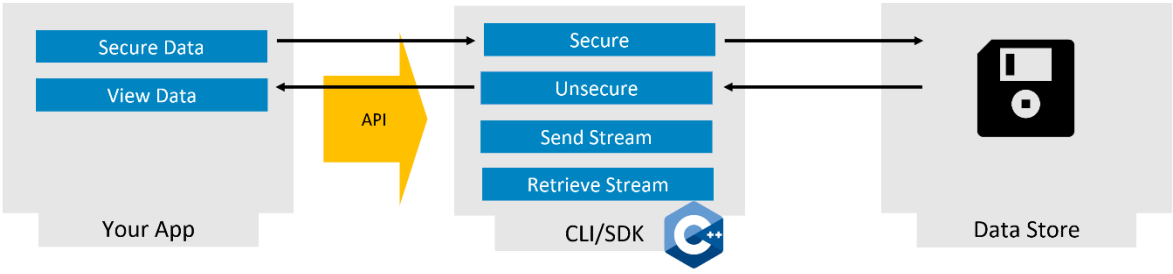
- Transfer confidential, live video files between computers anywhere on the internet
- Transmit real-time command codes to factory controls
- Live stream any data while fully encrypted in real-time with no loss, no compression, and nearly no latency

SECURITY BUILT INTO IOT DEVICES

Security is key for IoT to succeed in the future and to fulfill its full potential. However, it is often forsaken due to business needs – time to market and costs. Rather than focus on an infinite number of potential attacks, Ubiq helps secure IoT's data. Manufacturers don't need to invest into more expensive engineering resources or components and can instead implement Ubiq quickly with our SDK.

The Ubiq SDK allows encryption technology to be embedded at the manufacturing level, ensuring that security is built-in from conception. Manufacturers can leverage the SDK to securely:

- Transmit sensor data to fog computing infrastructure or the cloud
- Send remote commands or sensor data securely with <1ms latency
- Store data locally on disk without fear of physical theft
- Create a trusted command and control channel
- Authenticate devices to the network



Add security to any applications.

Robust set of APIs to protect files

Flexibility to use any data store: locally or in the cloud

HOW OUR ENCRYPTION FEATURE WORKS

The primary feature set the Ubiq SDK provides is a set of functions for performing data encryption (AES-256 out-of-box) at multiple layers of abstraction.

The Ubiq SDK enable users to perform direct encryption (resulting in raw binary bytes) or select from a suite of "Ubiq Ciphers" which perform encryption and encode the resulting ciphertext in specific formats.

Using Ubiq, your data is "uploaded" to a storage location and stored in an encrypted state.

You may "download" the data using Ubiq to decrypt the data.

- Keep data secured within a protected filesystem
- Backup your data to a secure drive on-premise or in the cloud
- Protect vulnerable portable drives and USB storage devices
- Very fast process protects data with minimal CPU usage
- Minimize data loss if device is lost/stolen

To find out more about our Data Security SDK, contact us for a demo or free trial.
www.ubiqsecurity.com

UBIQ