absio Dev Tools

Your Data, Your Rules: Easy Data Security Toolkit for Developers

THE CYCLE OF RISKY DATA

Today's applications generate, store and share a breathtaking amount of data. All that data is at risk from the moment it is created, because applications produce files that are inherently unsecure and uncontrollable. This data is perpetually vulnerable to insider threat, malware, and accidental misuse. As organizations continually invest in new applications, they create more and more data at risk. There will never be enough dollars or manpower to find and secure all the sensitive data that is continually generated by new and existing applications. In order to fix the problem, organizations must make data security part of the initial application investment to prevent the creation of data that puts them at risk.

BREAK THE CYCLE WITH ABSIO TECHNOLOGY

Absio offers a suite of software development kits (SDKs) that application developers can use to easily and automatically encrypt data objects in transit and at rest everywhere, without hindering application performance or restricting existing application logic. Optionally, developers can use Absio SDKs to cryptographically bind control information to each data object determining the time, manner and extent of any use of the data once decrypted. Absio technology integrates with both legacy and new applications to secure existing data and ensure that all new data generated is inherently secure. This enables organizations to break the endless cycle of finding and securing data post-creation, and instead make data security a process with a clear, measurable result.

ABSIO SOLUTION BENEFITS

Absio technology is designed to offer application developers the most complete data security and control solution available today that is easy to implement across a wide range of applications without needing to become security experts. This enables valuable developer assets to focus on building feature-rich applications with great user experiences without sacrificing data security.

Easy data security and control

- Data object-level encryption
- Data object-level control
- Automatic key generation, management and exchange
- Automatic secure data storage and routing
- No domain or network restrictions
- No need to rely on a third-party service provider

Simple implementation

- Only requires a few simple method calls to implement
- Highly portable; can be used for a wide array of applications across multiple platforms
- Can leverage existing IT infrastructure, access management and policy engines
- Requires minimal changes to existing applications

Highly-flexible economic model

- Offered via a variety of pricing models, including license-based, SaaS, partnerships and more

Powered by Britecloud™

+44 (0) 203 876 5221 | absio.britecloud.com

absio Dev Tools

Your Data, Your Rules: Easy Data Security Toolkit for Developers

ABSIO DEVELOPER TOOLS

Absio SDKs are available in C#, JavaScript and Node.js, and can be delivered as a library, command line utility or service depending on the specific requirements of the application. The SDKs use a server application for authentication, as well as data and key routing. This server application can be hosted by the organization on-premise or in the cloud, or is available as a SaaS offering. Using a few simple method calls, software developers can add the following capabilities to new or existing applications:

Object-level encryption of data at rest and in transit

The Absio SDK enables applications to output encrypted data by default. The SDK generates a distinct encryption key for each digital object created or shared by an application. Data is only decrypted in memory when in use by an authenticated, SDK-enabled application. Encrypted data objects can be nonsensically named and stored in a randomized folder structure to make sensitive data even harder to target for brute force decryption. All data is encrypted on the device running the SDK-enabled application and is only transmitted in encrypted form via an encrypted TLS connection. Content encryption keys can be stored in an encrypted database on the device running the SDK-enabled application or in another database location, so that applications do not have to call a central server to decrypt content stored on the device. This enables object-level encryption to be used without introducing significant latency to application processes, and enables content to be available in an offline environment.

Automatic key management and exchange

If encrypted data needs to be shared, the Absio SDK handles all key generation, management and exchange for an application. Using an automatic, public key infrastructure process, the Absio SDK generates a private and public key pair for each application user to be used for authentication and derivation of shared keys. The SDK sends the public results of the cryptographic processes to the Absio Server application, enabling data to be shared both inside and outside the organization regardless of domain or network. Shared encrypted files can either be stored by the Absio Server application or in another file repository for access by shared users. Only encrypted objects and public shared keys are stored by the Absio Server application. If Absio hosts the Server application, it never has access to the content encryption keys needed to decrypt user content. Using Absio SDK methods, access to shared information can be revoked at any time.

Object-level control of data in use

The Absio SDK can apply control metadata generated by an application to each data object that dictates what happens to the information payload once accessed by an authenticated user. The control metadata is cryptographically bound to the data objects, so that the controls persist with the data everywhere it resides. Absio technology is designed to support a wide range of access, action, location and time-based controls depending on the type of data and application being used.