appdome

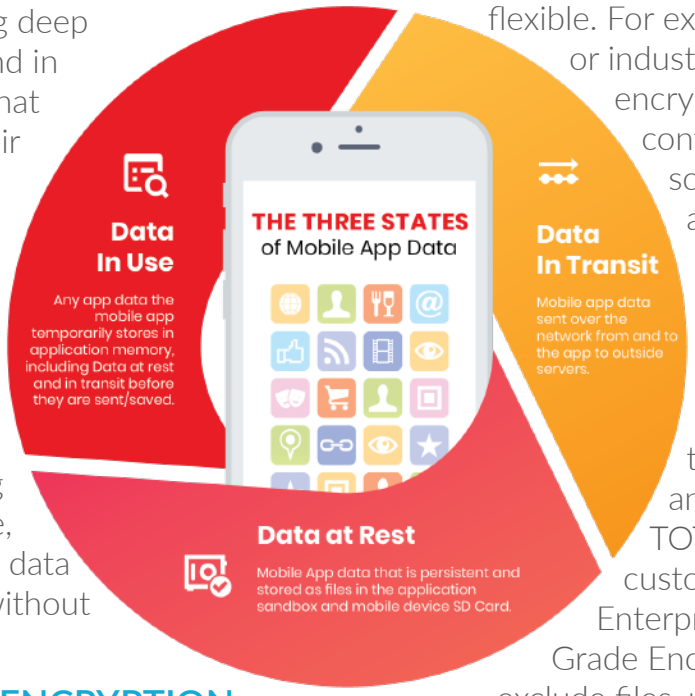
TOTALData™ ENCRYPTION

Comprehensive Mobile Data Encryption in Minutes - No Code or Coding Required

MOBILE DATA ENCRYPTION CHALLENGE

Every mobile app uses three states of digital data: data at rest, data in transit and data in use. The challenge is that encrypting mobile data is not easy. Mobile apps generate and take advantage of multi-dimensional pockets of data everywhere, including deep within the logic of the app and in external services and SDKs that write and retrieve data in their own way.

With so many different ways that apps generate data, there is no one-size-fits-all approach to secure data. This is why manually adding Android and iOS data encryption are such daunting undertakings. With Appdome, all three states of mobile app data can be encrypted instantly, without code or coding.



APPDOME TOTALDATA ENCRYPTION

Appdome's TOTALData Encryption allows encryption of mobile app data quickly and easily. TOTALData Encryption eliminates the need for a developer to design, build and maintain encryption inside mobile apps. TOTALData Encryption automatically encrypts all or selected mobile app data, regardless of how that data is generated or where it's stored and used by the app; at rest, in transit or in use. No code or coding is required. Users have complete control over the encryption methods applied to each app.

TOTALData Encryption is comprehensive and flexible. For example, some organizations or industry verticals may require encryption methods and more control over the encryption scope or encryption keys. To address this, TOTALData Encryption delivers a customer defined encryption model, enabling users to tailor encryption according to their specific app needs and risk profiles. Within TOTALData Encryption, customers can choose Enterprise Grade or Military Grade Encryption levels, include or exclude files, use advanced encryption management and more.

With Appdome's TOTALData Encryption, developers don't have to learn any encryption methods, can save months of work and avoid the trial and error involved when implementing mobile data encryption manually.

ENCRYPTING MOBILE APP DATA	
DATA AT REST ENCRYPTION	Protects mobile app data with dynamic AES 256-CTR (industry standard cryptographic protocols), without any dependencies on data structure, databases or file structures. Discrete blocks of data are encrypted and placed in a self-contained and segregated environment to isolate mobile app data from other resources. This makes it impossible for non-secure apps on the same device or different devices to decrypt and open this encrypted data.
DATA IN TRANSIT ENCRYPTION	Protects mobile app data as it is sent sent from the app to outside servers or other app users, by SSL certificate validation, pinning trusted CA's and enforcing TLS versions, strong RSA and ECC version and SHA256 digest.
DATA IN USE ENCRYPTION	Protects mobile app data stored in memory. Encrypting data in use is equally critical to protecting data at rest and data in transit. This because any app data first exists in memory before it is encrypted at rest.
FIPS 140-2 CRYPTOGRAPHIC MODULES	Adds FIPS 140-2 certified versions of the commercially available encryption libraries to be implemented to apps. With this option enabled, Appdome upgrades industry standard AES 256 Encryption to FIPS 140-2 Cryptography to protect mobile app data and network connections.
AMI SECURE ENCLAVES™	Mobile devices are now powered by chipsets designed from the ground up with segmented areas for encrypted data. For iOS devices, this is known as 'Secure Enclaves' and for Android devices it's called 'TrustZone". With AMI Secure Enclaves enabled, Appdome's AI system determines if the app is installed on a device equipped with this more secure chipset design, and immediately switches to the more secure data storage in the app.
SECURE DOWNLOAD	Enforces Appdome security that the app was built with when device downloads are opened in the app. By enabling secure downloads, all the app downloads will be executed within the context of the application, so that any protection (DAR, Secure Communication, or others) will be validated to the downloads when they are opened.
ENCRYPTING IN-APP CODE	
ENCRYPT IN-APP SECRETS, USER PREFERENCES, STRINGS AND RESOURCES	Encrypts application specific sensitive data such as keys, shared secrets, and tokens. It also encrypts all user preferences, such as username, email, contact information and other PII data. This data is otherwise stored in the clear inside the app, encrypting it ensures user and resource privacy. And finally, Appdome encypts the apps' constants, strings and runtime information, removing critical loopholes hackers use to infiltrate apps.
APPCODE PACKER	Appdome's no-code Android App Packer hides and encrypts all Java code of an Android app. This eliminates the component hijacking vulnerability in Android apps and optimizes the performance of the app.
ENCRYPT SHARED LIBRARIES	Encrypts dynamic shared libraries, which contain native code stored inside an app package. For instance, if an attacker loads an Android app into a reversing tool, such as IDA or Hopper, Appdome ensures the attacker can't access dynamic libraries even if they are extracted directly from app binary or device.
CHECKSUM VALIDATION	Performs checksum validation to calculate a unique hash or fingerprint of binary data and assets and validates them at runtime. This prevents changes to the app, its resources, code, and configuration.
ENCRYPTION CONTROL	
ENCRYPT USING IN-APP SEED	Enables app developers to use Appdome-DEV™ to seed the encryption keys used by Appdome from any key management system.
IN-APP ENCRYPTION KEYS	Uses industry standard AES 256 Encryption Mechanisms and in-app keys to protect mobile app data.
SMARTAPP™ OFFLINE ACCESS	Grants users offline access to encrypted files and data stored in the app. Access is enabled using shared or derived keys inside DEV-Events. SMARTApp allows the user to maintain their state within the app, accessing files and other protected data for a period of time or so long as relevant conditions are met, all pre-defined by the Appdome admin in DEV-Events.
STORE AND ENCRYPT SECRETS IN PROTECTED MEMORY	With In-App Generated Seed and Smart Offline Handoff for Data at Rest Encryption, developers or other mobility, security or IT professionals can protect the data stored within a mobile app and seed it with an external secret, derived from a backend server or from user input. Appdome's Storing in Protected Memory enable Appdome admins to protect those secrets by storing them in the mobile app encrypted memory.

Learn more about Appdome TOTALData Encryption at **www.appdome.com** or open a free Appdome account at **fusion.appdome.com** and start fusing!

ABOUT APPDOME

Appdome is the industry's first no-code mobile integration and solutions platform. Appdome's patented, Fusion technology and its AI-Digital Developer™, known as AMI, powers a self-service platform that allows anyone to easily build mobile features, standards, and vendor SDKs and APIs in security, authentication, access, mobility, mobile threat, analytics and more into any mobile app instantly. Leading financial, healthcare, government and e-commerce providers use Appdome to deliver rich mobile experiences, eliminating development complexity and accelerating mobile app lifecycles.

*Yehuda et al. Method and a system for merging several binary executables. U.S. Patent 9,934,017 B2 filed November 15, 2015, and issued April 3, 2018.