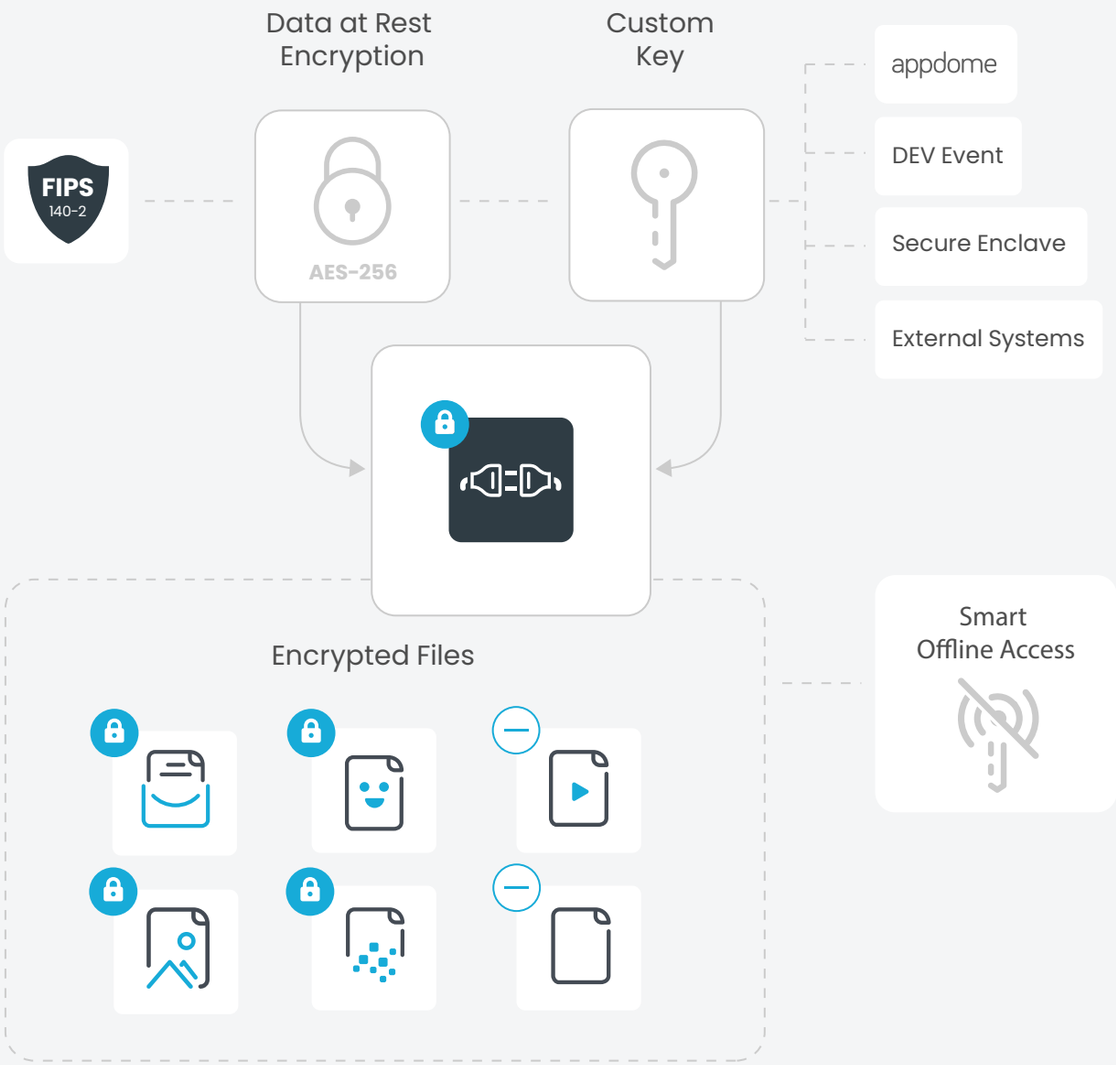
appdome TOTALData™ ENCRYPTION



DATA-AT-REST ENCRYPTION

- All stored data generated by the app is encrypted at runtime using industry standard AES-256 cryptographic protocols.
- Customers looking for military grade encryption can enable FIPS 140-2 cryptographic modules.

ENCRYPTION KEYS

- Appdome generates Encryption Keys by using industry standard AES mechanisms. Keys are never stored on the device and are derived at run-time.
- Custom Encryption Key generation options available to the mobile app developer are:
    - Seeding the Encryption Keys via Appdome-DEV Events
    - Use the device Secure Enclave chipset to generate the Encryption Keys
    - Seeding the Encryption Keys via external, customer controlled, systems

ENCRYPTED FILES

- By default, all stored data generated by the app is encrypted
- Identify certain files, file types or media types that do not need to be encrypted.
- Protect all application secrets and other sensitive data by Encrypting In-App Preferences.
- Protect all the app's content, such as PII and server information (server URL, user names, passwords, tokens, etc...) by Encrypting Strings and Resources
- Smart Media Sharing replaces an encrypted media file in the application with a temporary one-time file path so that Android MediaPlayer can read the media file.
- Appdome Smart Offline Access allows a mobile app to specify folders for offline file access, and specify access restriction with a time expiration or local authentication like pincode / biometric authentication.