TRIVALENT

Trivalent Protect™ Cryptographic Development Kit

Integrate Trivalent's encryption and shredding technology into your own applications for next generation data protection.

Sensitive app data secured

Full data-at-rest protection of data generated by your own apps integrated with Trivalent's cryptography

Intelligence-grade security

Security that stays with the data when the device is powered off, on, and at runtime.

Possession does not equal Access

Encryption and shredding for secure storage prevents unauthorized users from accessing protected data, even if they have access to the device.

Transparency

Protect your data without impact to productivity or device performance.

Secure Your App Data with the Trivalent Protect CDK

The Trivalent Protect Cryptographic Development Kit (CDK) provides a complete and easy to integrate solution for protecting all data generated by your Android app. The CDK includes a series of cryptographic libraries that integrate into Android applications to secure individual files and mobile database records, adding an additional layer of security for data stored on mobile devices. Any data generated by a CDK-integrated app will automatically be protected by Trivalent's NSA-approved encryption, shredding, secure dispersal, and recombination approach.

CDK Secure Elements

- AES-256 Encryption Library
- Information Dispersal Algorithm Engine
- File Encryption API
- Mobile Database API
- Trivalent Management Service App

Cryptographic Libraries

Android application developers that wish to use Trivalent Protect CDK can integrate the library components, which contain the data protection APIs. The libraries are responsible for encryption/decryption, shredding, and communicating with the Management Service. The CDK mobile database allows Android application developers to encrypt and shred database records. The CDK supports two different languages, C API and Java API.

Trivalent Management Service

The Trivalent Management Service is an Android app that handles all Trivalent administrative functions:

- Configuration
- Authentication
- Key generation and management
- Valid integrated app registration and Anti-Tampering checks
- Licensing

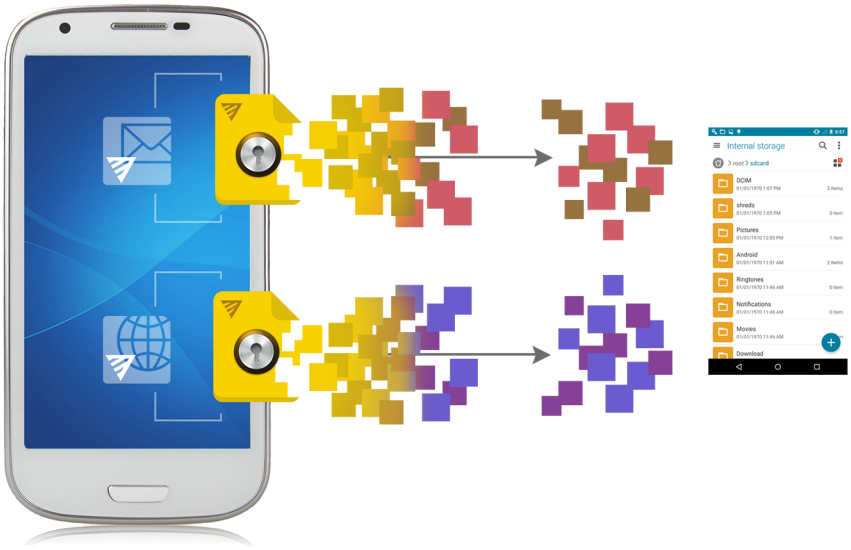
TRIVALENT

1 **Encrypts** files as they are saved to disc

2 **Shreds** the encrypted files for storage

3 **Stores** the shreds across the device file directory

4 **Recombines** the shreds and decrypts for authorized user



Empowering Developers

Trivalent provides turnkey tools for easy integration of next generation cryptographic libraries. Trivalent Protect Cryptographic Development Kit enables developers to build intelligence-grade data security for their apps. No expertise in security is required for integration.

Benefits

- NIAP certified and NSA CSfC approved to Top Secret
- Minimal integration effort required
- Transparent to the end user with no discernible performance impact
- Data integrity ensured with file level fault tolerance
- Keeps PII and PHI data compliant, meets HIPAA, GDPR, PCI DSS, NIST 800-171 data protection requirements

Features

- FIPS 140-2 certified encryption module
- Protects data using AES-256 bit encryption in combination with a randomized Information Dispersal Algorithm to shred data in a non-deterministic manner
- Separate layer of user authentication abstracted from native device log-on
- Obfuscation for tamper-resistant code
- Intelligence-grade security to keep data safe even if the device is compromised

Supported Platforms:

Android 4.4, 5, 6, 7

About Trivalent

Founded in 2010, Trivalent's next generation data protection stays with data to keep information safe and industries thriving. Trivalent supports the classified or sensitive data protection needs of Government agencies (DoD and Intelligence communities) and companies in regulated markets, such as Healthcare and Financial Services.

www.trivalent.co 443-472-6712 sales@trivalent.us.com