BEEKEEPER

ENCRYPTION DOCUMENTATION FOR BEEKEEPER PRODUCT AND SERVICES

Encryption at Rest Swiss Data Center VPC:
Data Center Hosting Partner: Interoute
Encryption Support Partner: VSHN AG
Component Encrypted: DB
Encryption Layer: Full Disk Partition
Encryption Product: Linux Unified Key Setup (LUKS)
Cipher Specification: AES 256 Bit
Cipher mode: xts-plain64
Hash Specification: SHA 1 (Hash algorithm used for key derivation)

Encryption in Transit to Backup Systems Swiss Data Center VPC:
Data Center Hosting Partner: Interoute
Encryption Support Partner: VSHN
Component Encrypted: Data Transfer to Backup Systems
Encryption Layer: Transit Layer
Encryption Product: Transport Layer Security (TLS) 1.2
Cipher Specification: TLS 1.2
Hash Specification: SHA 384 Bits (Hash algorithm used for key derivation)
RSA Key Length: 2048 Bit
In addition a client side encryption occurs as well based on a symmetric key using BF-CBC (Blowfish-Cipher Block Chaining).

Encryption at Rest Swiss Data Center VPC:
Data Center Hosting Partner: Interoute
Encryption Support Partner: Interoute
Component Encrypted: Object Storage
Encryption Layer: Encryption at Rest & Encryption in Transfer
Encryption Product: Transport Layer Security (TLS 1.2) and AES as provided by Interoute.
Cipher Specification: AES 256 Bit for Data at Rest and SSL 1.2 for Data in Transfer
Cipher mode: Unspecified
Hash Specification: MD5 Digest
Key Length: 128-bit

Encryption at Rest Frankfurt Data Center VPC:
Data Center Hosting Partner: AWS
Encryption Support Partner: AWS
Component Encrypted: DB
Encryption Layer: Data that is encrypted at rest includes the underlying storage for a DB instance, its automated backups, Read Replicas, and snapshots.
Encryption Product: AES as provided by Amazon Web Services
Cipher Specification: AES 256 Bit
Cipher mode: AES-GCM
Hash Specification: RIPEMD-160
Key Length: 256 Bit
See: https://aws.amazon.com/kms/faqs/

Encryption at Rest Dublin Data Center VPC:
Data Center Hosting Partner: AWS
Encryption Support Partner: AWS
Component Encrypted: DB
Encryption Layer: Data that is encrypted at rest includes the underlying storage for a DB instance, its automated backups, Read Replicas, and snapshots
Encryption Product: AES as provided by Amazon Web Services
Cipher Specification: AES 256 Bit
Cipher mode: AES-GCM
Hash Specification: RIPEMD-160
Key Length: 256 Bit

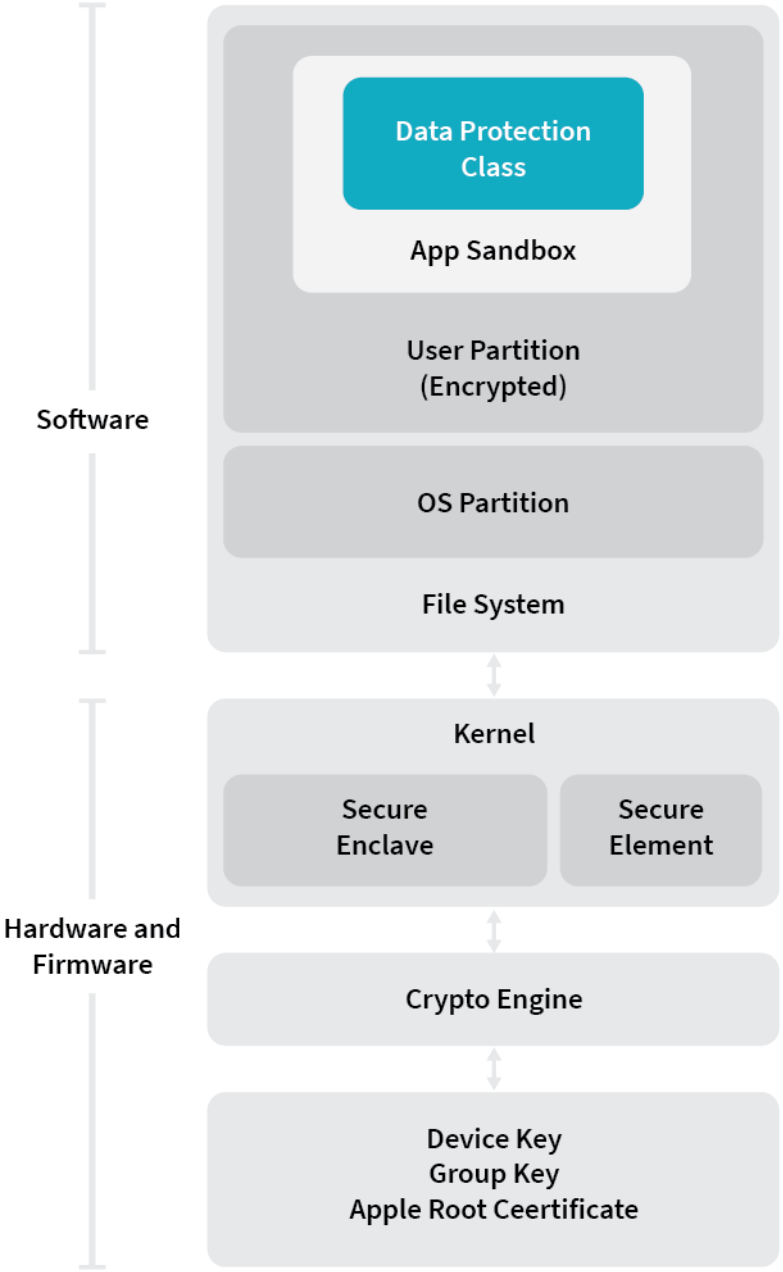
Encryption at Rest Oregon Data Center VPC:
Data Center Hosting Partner: AWS
Encryption Support Partner: AWS
Component Encrypted: DB
Encryption Layer: Data that is encrypted at rest includes the underlying storage for a DB instance, its automated backups, Read Replicas, and snapshots
Encryption Product: AES as provided by Amazon Web Services
Cipher Specification: AES 256 Bit
Cipher mode: AES-GCM
Hash Specification: RIPEMD-160
Key Length: 256 Bit

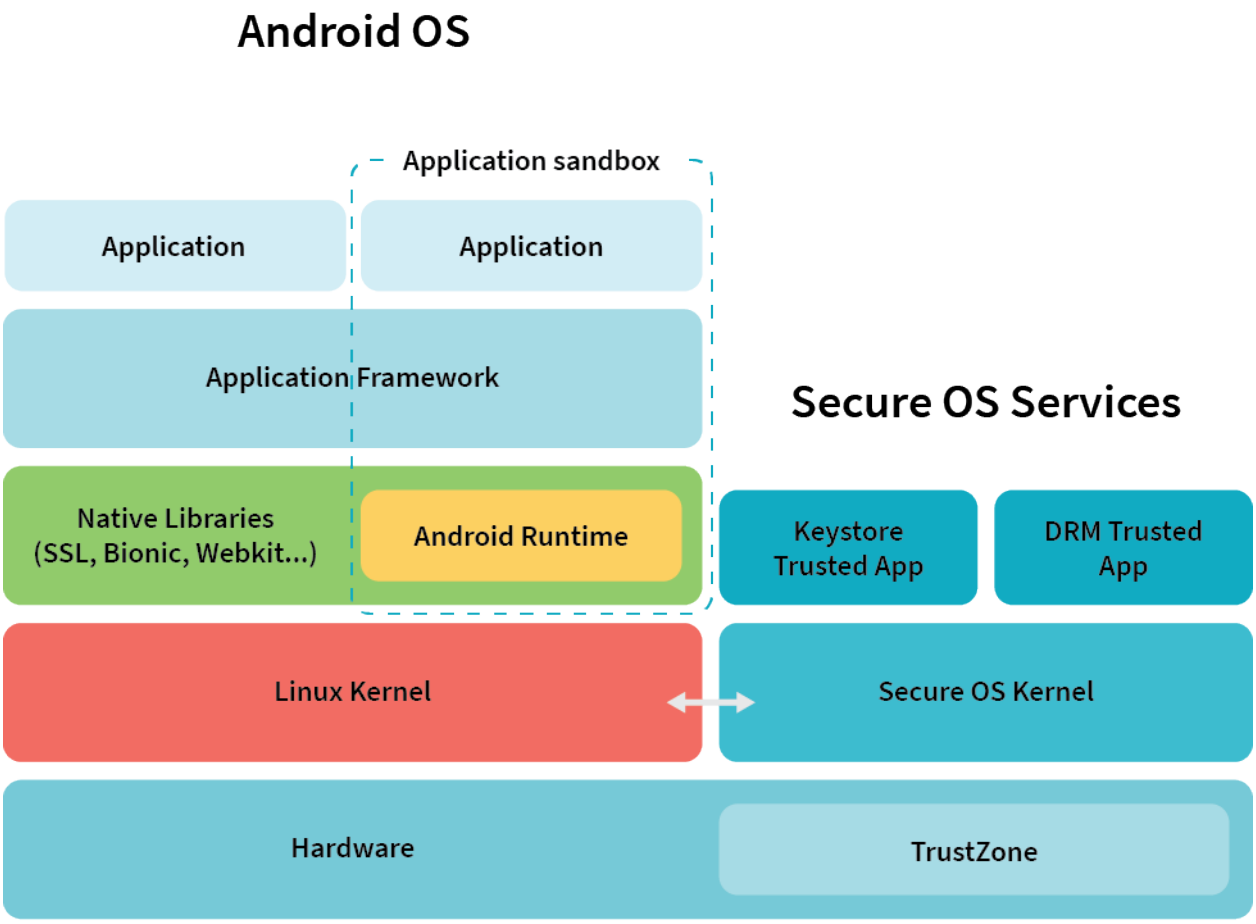
Encryption at Rest on iOS Devices:
Operating System: iOS Release 8
Product: Realm Mobile Platform
Component Encrypted: DB
Encryption Layer: Data at rest
Encryption Product: Realm
Cipher Specification: AES 256
Cipher mode: Cipher Block Chaining (CBC)
Hash Specification: SHA-2 HMAC
Key Length: User Supplied 64 Byte encryption key when DB is created. (Stored in the Secure Key Chain or the Key Store of the Device)

Encryption at Rest on Android Devices:
Operating System: Android 4.3
Product: Realm Mobile Platform
Component Encrypted: DB
Encryption Layer: Data at rest
Encryption Product: Realm
Cipher Specification: AES 256
Cipher mode: Cipher Block Chaining (CBC)
Hash Specification: SHA-2 HMAC
Key Length: User Supplied 64 Byte encryption key when DB is created. (Stored in the Secure Key Chain or the Key Store of the Device)

Encryption in Transit between Web / iOS / Android Devices and Beekeeper:
Data Center Hosting Partner: Interoute or AWS
Component Encrypted: Data Transfer to/from Beekeeper VPC
Encryption Layer: Transit Layer
Encryption Product: Transport Layer Security (TLS) 1.2
Cipher Specification: AES 256 Bit
Hash Specification: SHA 384 Bits (Hash algorithm used for key derivation)
RSA Key Length: 2048 Bit

Realm Mobile Platform DB encryption is in addition to any operating system security measures that may be in place as depicted below for iOS[1] and Android OS[2].


Data Protection Class
App Sandbox
User Partition (Encrypted)
OS Partition
File System
Software
Kernel
Secure Enclave
Secure Element
Hardware and Firmware
Crypto Engine
Device Key
Group Key
Apple Root Ceertificate

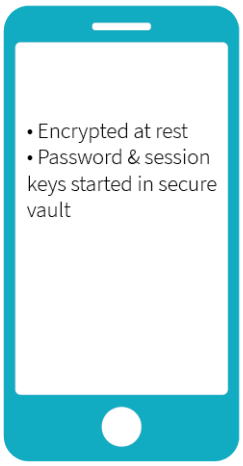


Android security architecture on ARM with TrustZone support

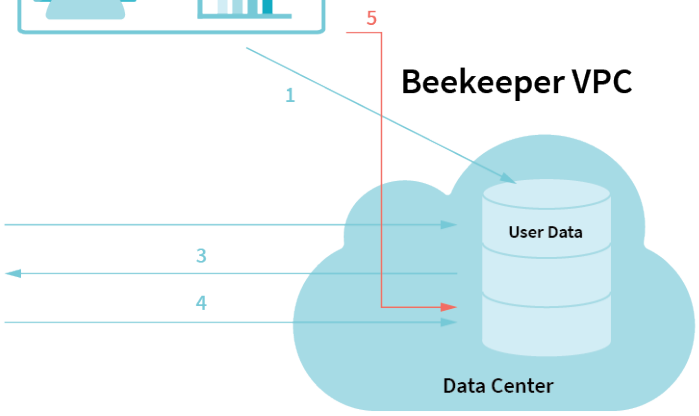
- Data sent over HTTPs
- Only Global Admins can add and suspend users

Admin Dashboard

Mobile Device



- Encrypted at rest
- Password & session keys started in secure vault



- Encrypted at rest
- Any data leaving the VPC leaves via secure channels (over HTTPS)
- Password and secrets are stored as bcrypt

1. When a Global Admin adds a new user manually via file import or through a user generation app from the Beekeeper Marketplace, a new user entry is created in Beekeeper's database.
2. The user logs in with a username & password
3. Beekeeper generates a session key, which is stored on the mobile device
4. The user cannot access the Beekeeper platform using the session key as authentication
5. If the user's account is deleted in the Dashboard by a Global Admin, the user record is deleted from the database. The session key is invalidated

Owner	Risk & Compliance
Current Release Date	September 12th, 2017
Previous Release Date	Not Applicable

List of Reference Documents:

1. "iOS Security. iOS 10. March 2017." Available from Apple.com website.
2. "Android Security White Paper. Last Updated April 2016." Available from Google.com website.
3. "Realm Security Recommendations for the Realm Mobile Platform." Available from Realm.io Website.
4. "Interoute Object Storage Data Sheet. Published date: 23.03.2017." Available from Interoute.com.
5."http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html" 18.09.2017. Available from Amazon Web Services on Encrypting Amazon RDS Resources.
6. VSHN AG Standard DB Services Configuration Parameter Document. (Confidential. Restricted distribution.)