QikID PTY LTD ABN 14 154 042 761
PO Box A2626, SYDNEY SOUTH NSW 1235
PHONE 1300 553 256
WEB https://qikid.com EMAIL service@qikid.com
MASTER SECURITY LICENCE (NSW) 000100799

QikID SYSTEMS SECURITY STATEMENT

1 MOBILE CLIENT

No information is stored on the mobile client other than a unique identifier that we use to determine which device is accessing the QikID service layer. The unique identifier stored is not specific to any of the hardware features of the device or the user, if you uninstall the application then reinstall the application a new unique identifier is created - the old one being irrevocably lost. All information transported between the mobile client and the service layer is secured by 256bit SSL - QikID ensures that the digital certificates used to encrypt the channel are not only valid but authentic by using trusted root certificates much like most secure websites and browsers do.

2 SERVICE LAYER AND API

The service layer presents a REST/JSON endpoint that mobile clients and other API consumer connect to. The connection between the mobile client / API consumer and the service layer is secured by 256bit SSL - QikID ensures that the digital certificates used to encrypt the channel are not only valid but authentic by using trusted root certificates much like most secure websites and browsers do. No data is stored within the service layer, all data is stored either on disk or in our database as below.

3 DISK STORAGE

All disk storage is encrypted at a minimum of 256bit.

4 DATABASE STORAGE

All data secured in the database is encrypted both at rest and inflight by 256bit encryption.

5 BACKUPS

Backups are held off site from the data centre hosting the QikID service layer. All backups are encrypted at rest and in flight with 256bit encryption, keys are not stored with the backups.