QShield

DATA PROTECTION

Securely store secrets and data

QShield Data Protection enables developers to securely store secrets and data for embedded and mobile applications, without the need for a pre-existing Secure Element.
With this module, be just one OTA update from re-securing your existing device fleet or mobile application.

The best cost/security ratio to (re) secure firmware and mobile apps

QShield Data Protection doesn't require any specific security skills thanks to its simple C API, and can be seamlessly integrated into any software and CI/CD. Thanks to this developer-friendly design, QShield Data Protection significantly drives down the cost of securing a fleet of devices or apps by protecting secrets such as PII, connection tokens, x.509 certificates, etc. that otherwise might just be easily accessible to an attacker.

Partners

Authorized Partner
life.augmented

MENDER

Key features

- Key-value interface to protect files, docs and data at rest
- Store up to 1024 entries per vault with up to 10MB per entry
- Provisioning of secrets at build time
- Anti-lifting protection with strong automatic device binding
- Simple C API
- Linux, Android on ARM, x86 and x64 architectures
- Ability to automatically leverage the Android KeyStore

Key benefits

- Prevent theft of JWT, connection strings, x509 certificates and key, PII, etc.
- Decrypt confidential data only when needed
- Easy to integrate with low impact, no specific security skills required
- Protect against reverse-engineering and data theft attacks
- Seamless integration of all C/C++ firmware or software