QShield

KEYS PROTECTION

Software whitebox to protect cryptographic keys

White-box cryptography combines **methods of encryption and obfuscation to embed secret keys within an application code**. The code and keys are combined to make the two indistinguishable to an attacker.
QShield offers whitebox implementations of the most common cryptographic algorithms, especially fitting specific use cases in the entertainment and mobile payment market.

- **Each whitebox implementation is unique, no sharing among customers**
- **Easily protect against software & hardware attacks without the need for a dedicated hardware component**
- **Resistant against known side-channel attacks (DCA,DFA)**

On the field and lab tested proven security

QShield Keys Protection has been successfully certified under the stringent evaluation process for EMVCo's Software-Based Mobile Payment Solution, by an independent third-party lab.
QShield is also the first product worldwide to have a white-box cryptography component certified under this evaluation process.

This certification guarantees **a high level of security assurance** as technologies evaluated under this process must showcase **a high level of robustness against software and hardware attacks**.

QShield's whitebox cryptography has **successfully cleared the NIST algorithm certification process**, allowing our customers to **accelerate FIPS certification** for their products.

EMVCo EVALUATED

The art of hiding secret keys in the plain visible sight of a software binary