Quintessence Labs

qProtect™

Powerful Data Protection for the most Sensitive and Critical Assets

Virtual zeroization option automatically destroys encryption keys while the data is encrypted

Virtual zeroization option uses one-time pad encryption against the strongest attacks

Data protection option incorporates a secure key store with AES encryption

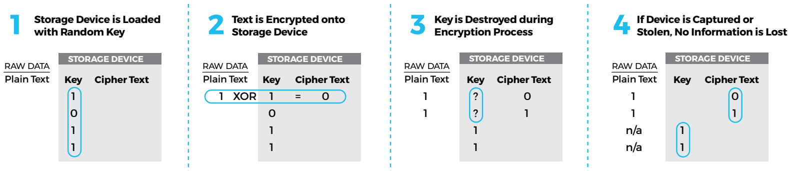
OVERVIEW

The most critical information needs the strongest protection, particularly when it is stored in unsafe environments. Financial details, personal files, or other records often need to be protected not just today, but into the future. QuintessenceLabs' qProtect™ secure storage solutions offer a solution to these challenges.

PROTECTION THROUGH VIRTUAL ZEROIZATION

Systems protecting sensitive data on storage devices need to be able to automatically remove, or zeroize, sensitive information. The qProtect 100 secure storage solution integrates a powerful alternative to manual physical zeroization, with automatic "virtual" zeroization. Virtual zeroization automatically erases one-time key material as it records and encrypts data using the one-time pad (OTP), the strongest encryption technique.

The virtual zeroization process is illustrated below:



The qProtect 100 secure storage solution allows encrypted data to be transmitted across networks without risk, where it can be accessed by authorized users for decryption and use in a secure location. The process also provides tamper-resistance revealing, on decryption, any attempts to modify the data.

FLEXIBLE DATA PROTECTION FOR STORAGE DEVICES

The qProtect™ 200 secure storage solution is a flexible encryption capability integrating a SD/microSD card with a secure element that protects data with AES-XTS full flash encryption. Encryption keys are stored in and protected by the secure element. The qProtect 200 secure storage solution is a flexible, plug and play solution that can be used by any device that can accept SD or microSD cards. It supports read and write operations by default. The secure element has tamper detection and traditional zeroization capability.

QPROTECT CAPABILITIES

The qProtect secure storage solution offers data protection choices for storage devices to meet the needs of your organization.

Through virtual zeroization, the qProtect 100 secure storage solution offers the ultimate in data protection, ensuring that the data and its encryption key are never co-located on the same device, while removing the steps needed in traditional physical zeroization. The qProtect 100 secure storage solution offers flexible deployment capabilities protected by a common criteria or FIPS 140-3 level 3 validated secure element with AES-XTS full flash encryption.

QPROTECT DEPLOYMENT

The high security of the qProtect 100 and qProtect 200 secure storage solutions have practical applications in the military, law enforcement, and aeronautical industries. Securely transporting data is also paramount in media, financial institutions, and multiple commercial applications.

The QuintessenceLabs team can partner with you to define the best qProtect product and implementation strategy for your organization.

SPECIFICATIONS

qProtect™

Unbeatable security for data in uncontrolled environments

<table>
<tr><th></th><th>qProtect 100</th><th>qProtect 200</th></tr>
<tr><td rowspan="2"><b>Configuration</b></td><td>• Standard form factor: 16GByte microSD
Other device types available on request
• Storage densities from 8 to 32GByte
Higher densities available on request</td><td>• 8 - 16GByte microSD card
– Flash controller and flash storage
– Secure element (security controller chip)
• Two operational modes
– Standard flash storage mode
– Full flash encryption mode (AES256-XTS)</td></tr>
<tr><td colspan="2">• MLC NAND flash
• UHS-1 Speed class 10
• Temperature -25C to 85C</td></tr>
<tr><td><b>Security</b></td><td>• The one-time pad key on the device is automatically destroyed during encryption
• Removes need for manual data destruction or additional zeroization steps
• Data accessible to authorized users for decryption in a secure location</td><td>• Secure element used to manage and secure flash encryption keys
• Infineon SLE smart card chip, Java card 3.0.4, Global Platform 2.2.1
• CC EAL 5+/6+ HW and OS, optional FIPS 140-3 level 3 conformant version
• RSA up to 2048 bit, optional EEC up to 512/521 bit
• AES up to 256 bit, SHA2 up to 512 bit</td></tr>
<tr><td rowspan="2"><b>Key &amp; Policy Management</b></td><td>• Administered via the Trusted Security Foundation® (TSF®) key and policy manager solution
• True random one time pad generated by Quantum Random Number Generator embedded in the TSF key and policy manager</td><td>• QuintessenceLabs key management applet available for secure element:
– Pin access control
– AES256-XTS key generation, import, export
• Customers can develop and use own key management applets
• AES256-XTS keys can be generated and imported from the TSF key and policy manager product suite</td></tr>
<tr><td colspan="2"><i>See the TSF key and policy manager product sheet for more details.</i></td></tr>
<tr><td rowspan="2"><b>Implementation</b></td><td colspan="2">• Delivered with qClient™ 100, a software development kit adhering to the OASIS Key Management Interoperability Protocol (KMIP). See qClient 100 product sheet for more details.
• SDIO interface and optional direct I/O interface
• Linux PC/SC drivers available</td></tr>
<tr><td></td><td>• Secure element fully configurable by customer</td></tr>
</table>

Quintessence Labs

AUSTRALIA
Unit 11, 18 Brindabella Circuit
Brindabella Business Park
Canberra Airport ACT 2609
+61 2 6260 4922

UNITED STATES
175 Bernal Road
Suite 220
San Jose CA 95119
+1 650 870 9920

www.quintessencelabs.com

Document ID: 6515-00