**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. qProtect from QuintessenceLabs offers 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. qProtect-VZ 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:

qProtect-VZ 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**

qProtect-DP 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. qProtect-DP is a flexible, plug and play solution that can be used by any device that can accept SD or micro SD cards. It supports read and write operations by default. The secure element has tamper detection and traditional zeroization capability.

**qProtect Capabilities**

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

Through virtual zeroization, qProtect-VZ 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. qProtect-DP offers flexible deployment capabilities protected by a common criteria or FIPS 140-2 level 3 validated secure element with AES-XTS full flash encryption.

**qProtect Deployment**

The high security of qProtect-VZ and qProtect-DP has 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>
<thead>
<tr>
<th>Configuration</th>
<th>qProtect VZ</th>
<th>qProtect DP</th>
</tr>
</thead>
</table>
|               | Standard form factor: 16GByte microSD  
Other device types available on request  
Storage densities from 8 to 32GByte  
Higher densities available on request | 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) |
| Security       | 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 | Secure element used to manage and secure flash encryption keys  
Infineon SLE smart card chip, Java card 3.04, Global Platform 2.2.1  
CC EAL 5+/6+ HW and OS, optional FIPS 140-2 level 3 conformant version  
RSA up to 2048 bit, optional ECC up to 512/521 bit  
AES up to 256 bit, SHA2 up to 512 bit |
| Key & Policy Management | Administered via qCrypt products  
True random one time pad generated by Quantum Random Number Generator embedded in qCrypt  
See qCrypt data sheets for more details | 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 qCrypt product suite.  
See qCrypt data sheets for more details |
| Implementation | Delivered with qClient SDK, a software development kit adhering to the OASIS Key Management Interoperability Protocol (KMIP). See qClient data sheet for more details.  
SDIO interface and optional direct I/O interface  
Linux PC/SC drivers available | Secure element fully configurable by customer |