DOQEX® CRYPTOGRAPHY

SECURITY STANDARDS CONFORMITY

OVERVIEW

DOQEX Limited is ISO27001 compliant.

They are a dedicated security services vendor that also delivers Pen Testing, ISO27k, PCI-DSS, IG and Data Protection consultancy.

Their email gateway and secure data exchange platform is DOQEX® which is deployed as discrete private data exchanges as well as integrated into software products across local government and the healthcare and education sectors.

DOQEX® Enterprise is available on the UK Government Digital Marketplace on the G-Cloud 11 framework.

- DOQEX uses FIPS 140-2 approved encryption algorithms
- DOQEX complies with FIPS 180-4 for the Secure Hash Standard
- DOQEX complies with FIPS 186-4 for the Digital Signature Standard
- DOQEX complies with FIPS 197 for use of the Advanced Encryption Standard
- DOQEX exceeds FIPS 140-2 standards for IV generation
- DOQEX is a PCI-DSSv3 compliant solution component
- DOQEX is compliant with PSN and N3 code of connection requirements
- DOQEX is compliant with NHS IG (v14) controls
- TLSv1.2 with Extended Validation (EV) Security Certificates
- DOQEX hosted services are delivered from TIA-942 Tier 3 data centres.

DOQEX® is NOT FIPS **certified** – indeed in the context of appropriate use, FIPS 140-2 certification of **any** FIPS certified **security module** is completely dependent upon the implementation.

TECHNICAL SUMMARY

DOQEX® has two encryption regimes: 1. **File data** is encrypted using AES-256 with a 256-bit key in Galois/Counter mode (GCM). 2. **SecureMail email text data** and **sensitive configuration data** is encrypted using XSalsa20 with Poly1305 MAC; the option exists to enable “legacy encryption” which reverts to AES-256 in Cypher Block Chain mode (CBC).

The Initialisation Vectors (IV) for use in all encryption modes are generated using a cryptographically secure random number generator which selects a 256-bit value unique to each file.

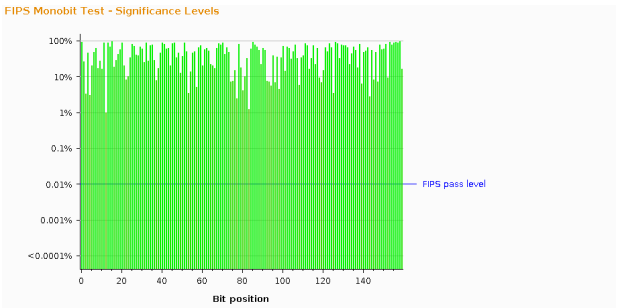
Each file (or SecureMail or configuration data) is encrypted using a unique key for that file. These unique keys are themselves encrypted with AES using a master key which is never stored on disk. The individual encrypted file encryption key is stored in plain text along with the file's individual IV.

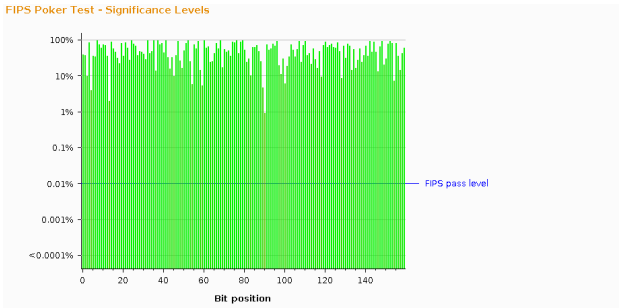
All data is encrypted in-memory on receipt. Encrypted data is stored within the encrypted FileVault, which is a separate volume on the DOQEX® Node. The FileVault is encrypted using AES-256 in GCM/CBC mode, and is mounted by an administrator at node boot time. The encryption key for the FileVault is never stored on disk on the node.

FIPS 140-2

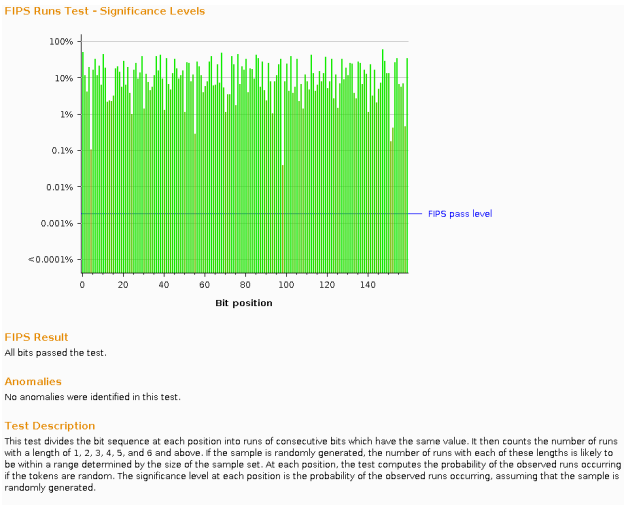
DOQEX® uses an FIPS 140-2 approved encryption algorithm – Advanced Encryption Standard (AES). This is implemented in Galois Counter Mode (GCM) mode, which requires the use of an Initialisation Vector (IV) which is generated using a cryptographically secure method (see section 4.7.1 of FIPS 140-2). Taking a significant sample-size from DOQEX's IV generation mechanism (note that a test generation suite using real data is available as part of the DOQEX® tools which are included with every node) produces the following FIPS-compliant results;

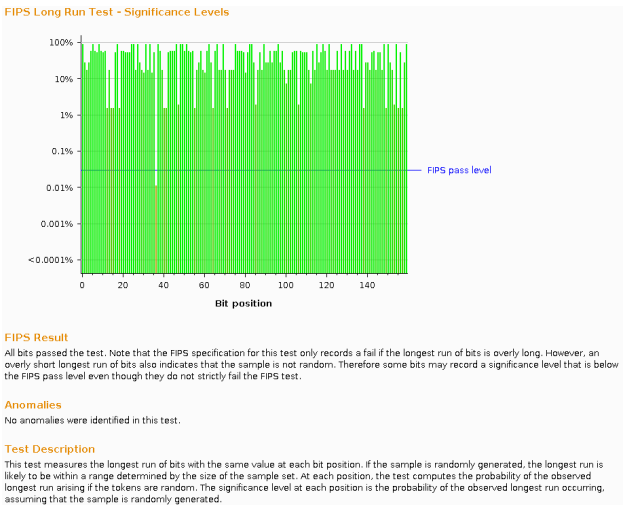
FIPS Monobit & Poker Tests;





FIPS Runs & Long Runs Tests;





DOQEX® makes use of PyCrypto (https://www.dlitz.net/software/pycrypto) to perform all cryptographic operations. Under the definitions of FIPS 140-2, this means the “cryptographic module” in use is PyCrypto.

ISO 27001:2013, ISO 27002:2013

In accordance with the requirements of Section 10.1.1 (Policy on the use of cryptographic controls) of ISO 27002:2013, DOQEX® segregates secure data storage from operating system and application storage within the FileVault using AES encryption with a key unique to each node that is not held on disk on that node. Each file or SecureMail object has a unique encryption key.

Encryption keys for files are not re-used and are not available for re-use once the file or SecureMail object has been deleted.

Data destruction; all file data (although already encrypted and stored on an encrypted volume) is overwritten three times using random data before being discarded.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI-DSS) V3.2

Although DOQEX® is not a payment processing or CHD storage or processing system, DOQEX® may be used as part of an organisation's PCI-compliant solution.

Key relevant PCI DSS controls (from version 3.2) are;

- **3.1 “Keep cardholder data storage to a minimum....”**: DOQEX's default policy means that uploaded files are only kept for a short period of time. After this time, the file and the associated encryption keys are securely removed.
- **3.4.1 “If disk encryption is used....”**: DOQEX® encrypts each file or SecureMail with its own encryption key which is independent of the operating system. Further, each encrypted file is stored on an encrypted volume which is not auto-mounted by the operating system and has its own unique key.
- **3.5 “Document and implement procedures to protect keys...”**: DOQEX's individual encryption keys are encrypted using a key-encrypting key (KEK). The KEK is not stored locally on the node. Where relevant, DOQEX Ltd will advise customers on including the management of KEK material into their site security policy.
- **3.5.1 “Maintain a documented description...”** Where relevant and upon request, DOQEX Ltd will supply a more detailed version of the summary section of this document should additional information be required.
- **3.5.3 “Store secret and private keys...”**: See 3.5.
- **3.6 “Fully document and implement all key-management....”**: See 3.5 and 3.5.1.

For information on DOQEX® and DOQEX Ltd's conformity with additional PCI DSS control applicability such as section 4 or 5, (or interpretation for use with PCI DSS controls), please contact DOQEX Ltd.

NHS INFORMATION GOVERNANCE TOOLKIT (IG) V14 (2016/17)

Although DOQEX® is not a clinical system, it may be used as part of an organisation's clinical management system for the secure transfer of data. DOQEX® is also available on the UK NHS National Network (N3) for additional security.

Key relevant Information Governance Toolkit controls (from version 14) are;

- **14-201 "…arrangements are in place to support and promote information sharing…"**: DOQEX's in-memory encryption technology ensures sensitive data is not written to disk and each file or SecureMail is individually encrypted.
- **14-206 "staff access to confidential […] monitored and audited…"**: See 14-302 below.
- **14-302 (…documented […] event reporting…)**: DOQEX creates an audit record for every action that modifies (creates, updates or deletes) data and for every access of sensitive data (e.g. shared file access). This audit record contains detailed fingerprint information showing the client computer, login account (where relevant) and browser data.
- **14-308 "All transfers […] technical and organisational measures adequately secure…"**: DOQEX's encryption and access management technology prevent users from accessing data they have not been given explicit access to.