Enigma Bridge – Data Security for the Cloud
Cryptographic Specification

Enigma Bridge brings data security to the cloud using the most advanced hardware and state-of-the-art cryptographic algorithms and protocols.

Cryptographic Validity & Algorithms

At the core of the Enigma Bridge solution is our hardware security unit with secure processors that are NIST FIPS140-2 Level 3 validated and satisfy Common Criteria EAL5+.

The cryptographic algorithms that can be executed on the Enigma Bridge platform are either composite operations or certified cryptographic libraries. The list of FIPS140-2 certified operations includes:

- AES – 128, 192, 256 bits – ECB and CBC modes of encryption;
- 3DES – three key – ECB and CBC modes of encryption;
- RSA – up to 2,048 bits;
- EC FP – 128 to 256 bits;
- SHA-1, SHA-256, SHA-384, SHA-512; and
- PRNG – secure hardware generator of random numbers.

Composite cryptographic algorithms (e.g., HMAC-SHA2, OATH HOTP) are available as atomic operations, i.e., executable by Enigma Bridge hardware security units via a single API call.

Enigma Bridge Lifecycle

Enigma Bridge is initialised in a controlled environment. Once the initialisation is complete the secure processors protect all operational keys, such that the keys are only accessible within the physically secure and trusted environment.

Any sensitive data and results of computations sent between Enigma Bridge and application servers are encrypted. The encryption algorithms typically used are AES256 and HMAC-SHA256. This provides end-to-end protection between the customer's application servers and the Enigma Bridge secure processors.

Scalability

Enigma Bridge platform subscriptions are scalable depending on the application requirements – from occasional use through to massively parallelised or distributed applications processing bulk amounts of data.

A single Enigma Bridge hardware security unit currently provides the following resources:

- 500 RSA signatures (1,024b) / second;
- 120 RSA signatures (2,048b) / second; and
- 8 Mbps for symmetric encryption.

Please contact sales@enigmabridge.com or +44 1223 321 999 for more information.