Enigma Bridge – Data Security for the Cloud
User Case Applications

Enigma Bridge provides secure data solutions for enterprise and large corporate customers. At the heart of the Enigma Bridge technology is the hardware security unit that enables delivery of a range of off-the-shelf and customised security solutions. Deployment models include web-based services for cloud applications as well as dedicated onsite systems for large corporates.

Enigma Bridge Solution Overview

Enigma Bridge protects sensitive data through the use of security keys such as data encryption keys or passphrases, which are stored using the most secure data storage technology available on the market today. The technology is FIPS140-2 Level 3 validated, which is the banking industry standard. As a result, access to sensitive data is always out of reach of security threats even if the security of the application or web server is compromised.

The high level functional operations performed by the Enigma Bridge solution include:

- Secure software key management.
- Data encryption/decryption.
- Secure data processing.
- Data transaction management.
- Application usage metering.

Business oriented API allows easy integration with client business applications to meet individual customer business needs and technical requirements. Some examples of the standard user case applications are as provided below.

Licence Key, Password Protection and Authentication User Case

Sensitive data such as licence keys, passwords, OTP secrets that are secured by Enigma Bridge are protected even if/when your application server is hacked or compromised. User data in Enigma Bridge systems is physically separated and protected with the most secure technology available.

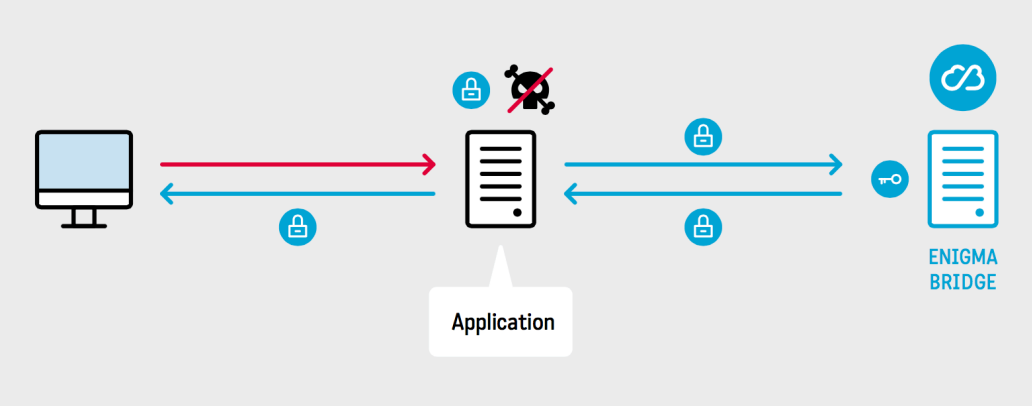

Figure 1: Enigma Bridge encrypts password, authentication data and license keys and securely compares user/application access requests with the stored data.

Secure Data Storage and Handling User Case

Enigma Bridge can be used to protect large amounts of data. This can be done in several ways depending on the type of the data and business requirements. Sensitive data files can be encrypted/decrypted using the Enigma Bridge master key solution to support secure data storage, sharing and processing on application servers. Enigma Bridge can also encrypt/decrypt data or perform customised business operations directly on the Enigma Bridge hardware.

Access Management and Metering User Case

Enigma Bridge can be used as an independent metering and management solution for chargeable software services delivered as cloud applications. One of the advantages with using Enigma Bridge for monitoring application usage in the cloud is that it works as an independent and verifiable black box meter. As a result, the integrity of the usage data is guaranteed and accessible to all parties - the software supplier, cloud service provider and end user.

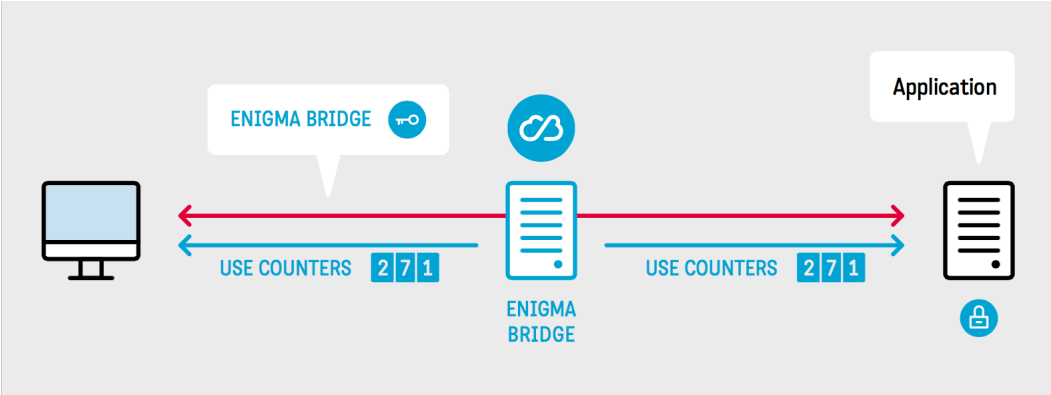

Figure 2: Enigma Bridge measures the usage of application/cloud resources and provides independently verifiable meter readings.

SSL Certificate Key Management User Case

Enigma Bridge can be used to actively manage, generate, use and track SSL certificates resulting in more efficient certificate usage and reduced cost. Use of Enigma Bridge ensures that private keys are never compromised or copied to unknown or insecure locations.

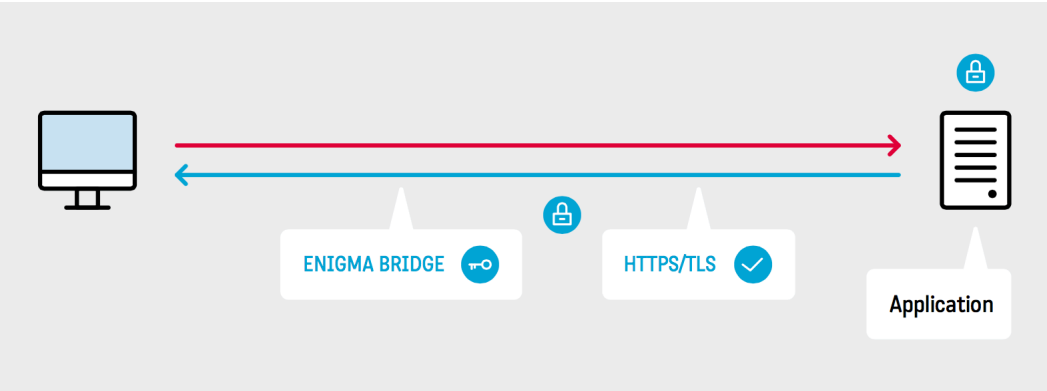

Figure 3: Enigma Bridge provides a secure environment for use and effective management of HTTPS/TLS private keys.

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