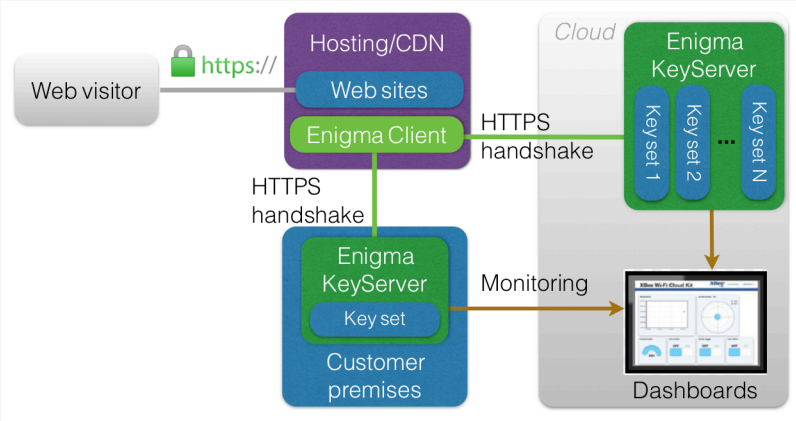
ENIGMA BRIDGE

HTTPS Key Service

Keyless HTTPS with Secure Hardware

HTTPS Key Service is an end-to-end solution for managing secure data connections to web servers using the revolutionary Enigma Bridge platform. HTTPS Key Service protects, manages and monitors usage of private encryption keys. It enables hosting and CDN companies to easily set up and manage secure data connections, and provide superior data security for protection against cyber-attacks such as phishing and DDoS.

Enigma Bridge System



HTTPS Key Service is based around the revolutionary Enigma Bridge KeyServer which has been purpose built to provide high speed access to encryption keys stored on physically partitioned tamper-proof processing units (Common Criteria EAL5 / FIPS140-2 Level 3).

Enigma Bridge services can be deployed as a shared cloud instance or as a dedicated internal system.

Security

Secure hardware ensures that the physical location of private keys is always known. This significantly improves security controls, cloud SLAs, and liability management. The Enigma Bridge KeyServer appliance can be located in the cloud service provider's data centre or at the customer's premises if the customer would like to physically hold their keys.

Scalability

The Enigma Bridge architecture allows for scalability (for big data application) as well as secure partitioned sharing of the hardware resources between multiple customers. In addition, HTTPS Key Service elastically adjusts to customers' changing computational requirements.

Deployment

HTTPS Key Service is a fully managed service for public and private cloud. Deployment includes pre-packaged web servers or Keyless SSL Client software running on hosting / CDN platforms which talks to Enigma Bridge KeyServer.

Benefits Summary

The key benefits of HTTPS Key Service are hassle free, large scale and low cost deployment of HTTPS security as well as superior data security by design. Other benefits include:

- Improved liability and security policy management.
- "Elastic" computational resources to manage varying customer requirements.
- Secure sharing of partitioned hardware resources between multiple customers.
- Highest level of protection for private keys stored in tamper-proof hardware.
- Real time monitoring and control of keys for better analytics and defence against cyberattacks.
- More efficient networks and load balancing.

Enigma Bridge Ltd | 20 Bridge Street, CB2 1UF, Cambridge | www.enigmabridge.com
email: sales@enigmabridge.com |phone: +44 1223 321 999 | registered in England as Enigma Bridge Ltd – 09601316.

Key Features	Benefits
Security	
Supports Multiple Keys	Supports multiple SSL certificates per key server
Mutually authenticated connections	AES256 communication key protecting connections with secure hardware end-to-end.
	Optional HTTPS security – mandatory with CloudFlare keyless SSL
Key generation	Keys can be generated directly in secure hardware or on client computers and pushed to Hardware HTTPS Key Service.
Standards	
Compatible with standard SSL protocol	Doesn't require any modifications to existing web browsers or web servers.
Enterprise key management	Private keys are managed in accordance with majority of enterprise key management systems using secure hardware with EAL5 and/or FIPS140-2 Level 3 validations.
Supports multiple cryptographic algorithm	Supports a number of SSL/TLS cryptographic algorithms for wide compatibility.
Flexibility	
Universal availability	No requirements on client systems.
Multiple operating systems	Linux and Windows operating systems are supported with our PKCS11 library.
Pre-packaged (for on-premise use)	Key server packaged as a docker image.
Source available	Key server source code available for review.
Software-only or service solution	Runs entirely on standard servers, no new hardware required.
Performance	
Server handshake in line with secure hardware products (HSMs)	RSA 2,048bit handshake completed within 150-200ms. Elliptic curve handshake in 50-100 ms.
Session Tickets	Not impacted.
Session ID	Not impacted.
Persistent connections	Not impacted.
Availability	
Load balancing	Multiple Hardware HTTPS Key Servers available to distribute load.
Automatic failover	Hardware HTTPS Key Service is stateless and can be configured for automatic failover.
Cloud-based monitoring	Access to keys monitored within Enigma Bridge service. Keyless SSL usage monitored by cloud provider.
Web-based configuration	Services managed through web-based portal.

For more information please contact sales@enigmabridge.com.