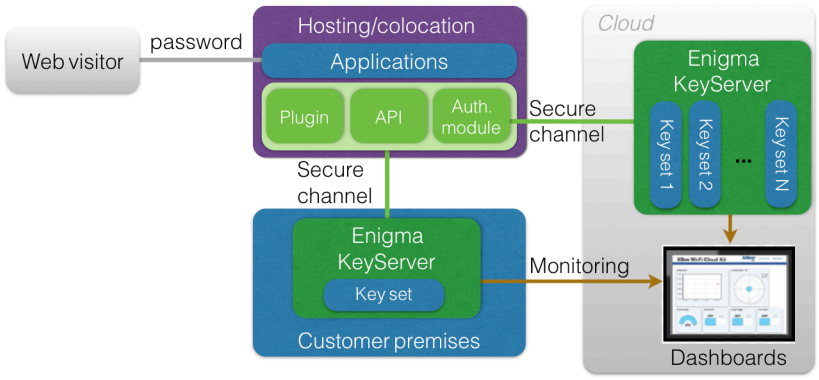
ENIGMA BRIDGE

Password Protect Service

Login Authentication with Secure Hardware

Password Protect Service provides secure login to applications and website services for advanced protection against theft of data and unauthorised use of online services using the revolutionary Enigma Bridge platform. The Service allows online businesses to manage, monitor and control user logins using encryption keys securely stored on tamper proof hardware. The secure login process requires access to the securely stored encryption key such that stolen password databases cannot be used without access to the key. Enigma Bridge Password Protect Service greatly reduces the risk of cyber-attacks and the associated damage to online business.



Password Protect 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 greatly improves cyber security controls, cloud SLAs, and liability management. For example, if a website database is stolen, unauthorised access to sensitive customer data and services as well as offline password attacks are prevented without access to the securely stored encryption key. The KeyServer appliance can be located in the cloud service provider's data centre or at the customer's premises if they want to physically hold their own keys.

Scalability

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

Deployment

Password Protect Service is a fully managed service for public and private cloud. Deployment facilities for developers include plugins for various web platforms (including WordPress, Salesforce, etc.), an API for web applications that have been developed from the ground up, as well as, authentication modules for Windows and Linux operating systems.

Benefits Summary

The key benefits of the Password Protect Service are greatly reduced the risk of data theft and user passwords being compromised. Other benefits include:

- Superior data security by design.
- 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.

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 Applications, Users	Partitioned processing units (FIPS140-2 Level 3) support large-scale secure resource sharing between customers & applications.
Mutually authenticated connections	AES256 communication key protecting connections with secure hardware end-to-end.
	Optional HTTPS security.
Key generation	Keys can be generated directly in KeyServer secure hardware or on client computers and pushed to the KeyServer.
Standards	
Compatible with standard authentication systems	Authentication is implemented via a single-call web service API.
Enterprise key management	Managed in accordance with the majority of enterprise key management systems, with EAL5 and/or FIPS140-2 Level 3 validations.
Supports multiple authentication methods	OATH HOTP and OATH TOTP authentication supported.
Flexibility	
Multiple operating systems	Supported on any operating system/environment that provides access to web services. Experimental PAM modules are available.
Universal availability	No requirements on client systems if used with a cloud provider.
Service solution	Operates on any standard server setup.
Network impact	Each transaction is a single TCP request and response.
Performance	
Password verification	Typical transaction time per processing unit is less than 50ms. Higher transaction rates available using multiple processing units.
Transaction rate	According to SLA requirements – “Elastic” computational resource management.
Availability	
Load balancing	Load balancing supported.
Automatic failover	Internal automatic failover supported.
Cloud-based monitoring	Dashboard monitor and controls supported.
Web-based configuration	Managed through web-based portal.

For more information please contact sales@enigmabridge.com.