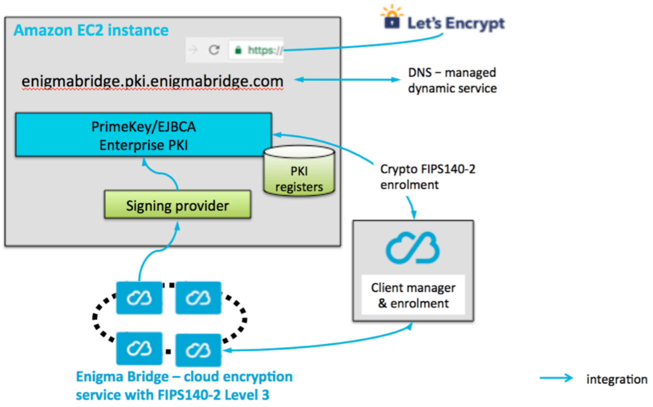
ENIGMA BRIDGE

Enigma Bridge PKI

Cloud Professional PKI with remote FIPS140-2

Enigma Bridge PKI is a professional cloud certificate management system with an ultimate secure hardware protection for small users as well as enterprises. Enigma Bridge PKI can be used for internal as well as external certificate management. You can start issuing your own certificates in 19 minutes.

You can use Enigma Bridge PKI directly with its own custom root certificate (trust anchor). The root public key can be signed by a recognized PKI system so that issued certificates are trusted by operating systems.


Amazon EC2 instance
https://
enigmabridge.pki.enigmabridge.com
Let's Encrypt
DNS – managed dynamic service
PrimeKey/EJBCA Enterprise PKI
PKI registers
Crypto FIPS140-2 enrolment
Signing provider
Client manager & enrolment
Enigma Bridge – cloud encryption service with FIPS140-2 Level 3
integration

Enigma Bridge PKI integrates several technologies to give customers an enterprise key management system initialized and ready in less than 19 minutes.

A new instance of the PKI can be automatically launched with a single command.

Certificates are signed by secure hardware to ensure the ultimate level of security while you get all the benefits of a cloud service.

Security

Signing keys used by the Enigma Bridge PKI instances exist only inside a secure, tamper-resistant hardware. The keys never leave it or get stored on disk or in memory anywhere outside the FIPS140-2 Level 3 secure processors.

Access Security

The default authentication of administrators is with a client-side HTTPS authentication. Your PKI instance will create an initial administrator authentication key and store it in a PKCS12 / PFX file.

Your PKI instance can also be placed within a virtual private network (VPN). Authentication is then implemented on the VPN level. Administrators can access the functionality of the PKI with a single sign-on (SSO) authentication once they log into the VPN. The VPN uses a dynamic authentication method with RSA / public keys.

Operation Audit

The PKI system provides internal logs of all activities performed by its administrators and operators. The Enigma Bridge signing platform also provides independent logs of each operation with PKI private keys. This logging covers all keys, whether they sign certificates, revocation lists (CRL), or real-time status responses (OCSP).

Operational Capabilities

The key management system is powered by Enigma Bridge hardware encryption platform and the EJBCA PKI application from PrimeKey Solutions AB. The main features include:

- **Certificate Authority** – an X.509 certificate authority supporting a wide range of protocols including X.509, PKIX (RFC5280), SCEP, or CMP (RFC4210 and RFC4211).
- **Registration Authority** – a front-end for manual approvals of certificate requests.
- **OCSP Responder** – on-line certificate validation according to RFC2560, RFC6960 and RFC5019.
- **Physical security of PKI keys** – keys for issuing certificates are protected with secure hardware with FIPS140-2 Level 3 and Common Criteria EAL4+ or EAL5 certifications.
- **Domain Name with HTTPS** – out-of-the-box HTTPS to your new PKI system with DNS records instantly and securely updated each time you restart the EC2 instance.

Key Features	Benefits
Security	
Secure user authentication	Any or a combination of: • Client-side HTTPS certificates • Certificate-based VPN
Private key security	Generated, stored, and used in FIPS140-2 Level 3 hardware processors.
Functions	
PKI (selection)	Multiple CAs and levels of CAs
	X.509 v3 implementation
	PKIX standards - RFC5280
	Certificate export in multiple formats
	Online certificate repository
	SCEP interface
	OCSP – online certificate status protocol
Cryptography	RSA 1024b, RSA 2048b SHA-2
User / administration Interface	
Web management interface	With a valid https certificate (green bar) out of the box.
Operator / administrator management	All available via its web interface.
VPN access management	Unified with the main PKI web management interface.
Deployment options	
Public cloud	PKI instances run on a public cloud platform. Secure hardware is available from a public cloud instance of the Enigma Bridge service.
Private / mixed cloud	Clients can host own instance of the secure hardware encryption service. PKI instances can be then launched in public cloud or in private cloud.

For more information please contact sales@enigmabridge.com. Indicative pricing, subject to change, is available at: https://enigmabridge.com/pki.html