Enigma Bridge – KeyTwist

Secure interchange of keys between systems

Enigma Bridge KeyTwist is a solution for secure handling of keys between independent information systems and for back-up and recovery of keys kept in printed form. All parts of KeyTwist used for entry, storage, or handling of sensitive keys, are small enough to be stored in a safe. The KeyTwist itself is a self-contained system. You can use it in secure shielded rooms, which is isolated from any electronic or computer systems, when used with a portable power bank.

Establishing the identity of the owner of an encryption key is the most difficult part of the encryption. Once you know it, the rest can be automated.

Enigma Bridge KeyTwist enables and simplifies physical delivery of keys. A recognized approach is to split each key into several components. Once delivered, the components have to be securely combined into the original key. KeyTwist provides a secure environment for that.

KeyTwist also helps when keys, split into components are the preferred form of low-tech backup of long-term keys.

Selected Use Cases

Many FinTech and payment companies need secure connections into banking networks / schemes. Depending on the operating processes, they may need to import keys from an acquirer (a bank or a payment processor). KeyTwist is an ideal solution for that, as it enables secure remote loading of keys into a target system, whether it is an HSM or a software system.

Link encryption is a secure mechanism for protection of data in-transit. While these encrypted communication links can be established using asymmetric algorithms (i.e., RSA), the strength of symmetric-only design is in its simplicity. Again, KeyTwist provides a versatile tool for secure transport of such keys.

Reliable, non-electronic back up is another example of the KeyTwist usage. It is hard to build information systems, which last more than a few years. The same is true about encryption. Storing important, long-term keys in a printed form, is a low-tech solution, which may be the simplest and most flexible.

Design of KeyTwist

KeyTwist is a self-contained product. It uses smart cards to store sensitive keys and key components to lower the burden of secure storage in safes and strongboxes. The interface component is implemented with a small computer for easy storage. The cost of these semi-trusted computers allows each authorized personnel to have its own unit if a complete physical separation of all parts of KeyTwist is required.

Portable power banks can power operation of the whole system. It gives users high-level of flexibility in terms of where they import/export sensitive keys.

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.

Purpose

There are two main functions of KeyTwist. The first is import of external / third-party keys into an Enigma Bridge encryption platform. This import function results in an encrypted object for remote loading. These objects contain the key, as well as a definition of its use and a service-layer agreement (SLA) definition.

The second function is handling of symmetric keys for hardware security modules (HSMs) and software encryption systems. Whether it is secure injection of third-party keys, supporting backup of the keys in components, or transport of internal keys into external encryption systems.

Functions

Functions of KeyTwist include:

- definition of multiple-user control, i.e., how many persons must approve import or export of keys (for each key encryption key);
- import or export of key encryption keys;
- export of encrypted keys in different formats: new keys, rollover keys, RSA encrypted keys;
- audit log of all operations;
- supported key algorithms: 2DES, 3DES, AES128, AES256, and RSA2048 for asymmetric key encryption keys.

Security

KeyTwist uses high-security smart cards to protect keys, key components, and the integrity of audit logs.

Physical Security

Smart cards provide physical security validated at FIPS140-2 Level 4, i.e., removal, penetration, or dissolving of the enclosure will damage the module with high probability.

Protection of Secrets

KeyTwist smart cards are validated to detect and respond to attempts at physical access, they also provide authentication methods, and a trusted path for sensitive data.

Audit Logs

A firmware in smart cards ensures that operations performed with keys and key components, including initial configurations, are logged and available for audits.

Dual Control / Four Eyes Principle

Users can define properties of dual control with the “m of N” model. This approach defines the total number of operators (N) and a minimum number of operators (m), required for successful completion of sensitive functions. Each operator will then get her/his own authorization smart card, which has to be connected to the system throughout sensitive operations.

For more information please contact sales@enigmabridge.com. You can also visit our website at: https://enigmabridge.com/ or follow us on Twitter @enigmabridge.