ENCRYPTION CONSULTING

Top 5 Best Practices of Cryptographic Key Management

Cryptographic keys form the backbone of all organizations encryption practices. Keeping these secure is extremely important, the compromise of a key leads to the compromise of whatever data that key secures. Whether you manage your own cryptographic keys, or you allow your Cloud Service Provider (CSP) to manage the keys, key management best practices should be followed.

Below are 5 best practices for cryptographic key management.

ENCRYPTION CONSULTING

CENTRALIZATION

Many organizations have thousands of certificates that are all encrypted by different keys, which can be complicated to keep track of. Keeping the keys centralized to one location can help with accessing the keys necessary, as well as keeping the keys secure. Centralizing the keys exposes less places for an attacker to attempt infiltration. Third-party key management services help centralize and protect keys away from the data they encrypt, so that even if the data is stolen, the keys to decrypt the data are still safe.

+1- 469-815-4136 info@ecncryptionconsulting.com www.ecncryptionconsulting.com

ENCRYPTION CONSULTING

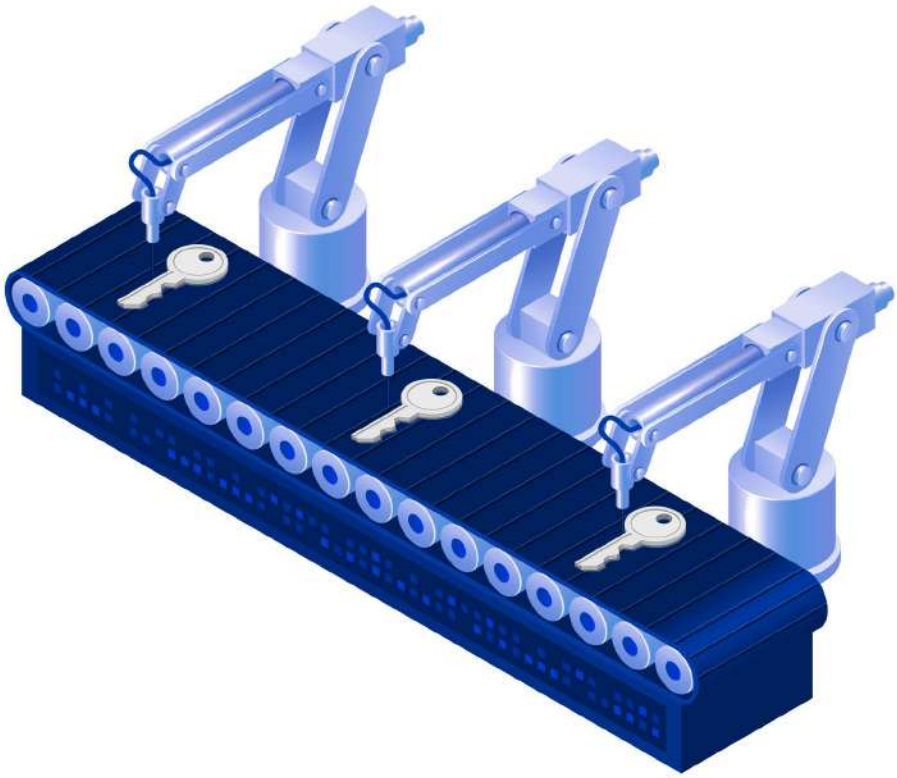
PRINCIPLE OF LEAST PRIVILEGE

The principle of least privilege is the idea that users should have the least amount of privileges necessary to complete their task. This ensures a user who only needs the key necessary to decrypt the date of birth of a client cannot also use the key for decrypting a client's credit card number. IAM policies can help with centralizing these user permissions, along with helping with authentication of user's.

+1- 469-815-4136 info@ecncryptionconsulting.com www.ecncryptionconsulting.com

ENCRYPTION CONSULTING

AUTOMATION



Automation of key management services makes an organization's job easier while also ensuring important key management tasks are undertaken. Certain jobs, like renewing keys, rotating keys, and generating key pairs, can be automated so that an organization does not forget to do these tasks. This allows the security team of an organization to focus on other parts of the keys' security.

+1- 469-815-4136 info@ecncryptionconsulting.com www.ecncryptionconsulting.com

ENCRYPTION CONSULTING

DIGITAL KEY SIGNING

Digital signatures verify the authenticity and integrity of keys, while ensuring keys cannot be repudiated. Authentication is one of the most important steps in data security, which is why digital signatures are built into most organizations' key generation policies.

+1- 469-815-4136 info@ecncryptionconsulting.com www.ecncryptionconsulting.com

ENCRYPTION CONSULTING

HARDWARE SECURITY MODULES (HSMs)

HSMs are an extremely secure hardware device that can generate keys, store keys, encrypt or decrypt data, authenticate a user, and much more. HSMs can integrate with most CSPs, and are FIPS 140-2 Level 3 compliant.

+1- 469-815-4136 info@ecncryptionconsulting.com www.ecncryptionconsulting.com

ENCRYPTION CONSULTING

"Encryption Consulting is a customer-focused cybersecurity consulting firm providing an array of services in all aspects of data protection."

Our areas of expertise include Public Key Infrastructure, enterprise key management, cloud key management, code-signing, hardware security modules, transparent data encryption, element level format preserving encryption, homomorphic encryption, and tokenization.

Contact Information

130 N Preston Rd,
Prosper, TX 75078, USA
+1- 469-815-4136
info@encryptionconsulting.com
www.encryptionconsulting.com

\encryptionconsulting\
@encryptioncons
\encryptionconsulting\