Key and Certificate Management Reference Architecture

Todd M. Hammond

Pace University

Introduction to Cybersecurity Fall 2024 72308 - CYB 611- 72308 - 202470

Jeytha Sahana Venkatesh Babu

October 27, 2024

Key generation

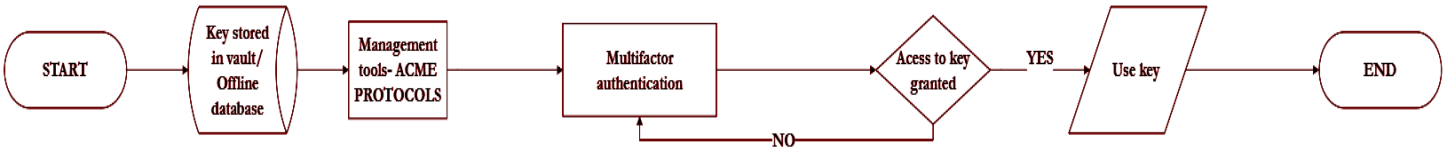
A key can be created by utilising the key management by a hardware security model or even by a third party. The process merely includes the generation of a key using the output of a cryptographically secure random bit generator (RBG) or it can also be generated by the derivation of a key from another key, the derivation of a key from a password, and key agreement performed by two entities using an approved key agreement scheme(Barker et al., 2020). According to the federal government, two admissible cryptographic keys have been identified, i.e., symmetric and asymmetric keys (Barker & Roginsky, 2018). The elliptic curve cryptography (ECC) is normally used for smaller key sizes and better performance.

Provisioning

Once a key has been created the database will store the key and its attributes. Attributes of the key may include name, date, activation size etc. Each key would have its strength usually measured in bits and is capable enough to protect throughout its lifetime. With the help of the generated key a CSR - Certificate Signing Request is generated as well - it is passed on to a Certificate Authority(CA), who then validates the resource for which the certificate was requested belongs to the owner, the CA finally provides a certificate, signed by them, which identifies the public key, and the resource it is authenticated for.

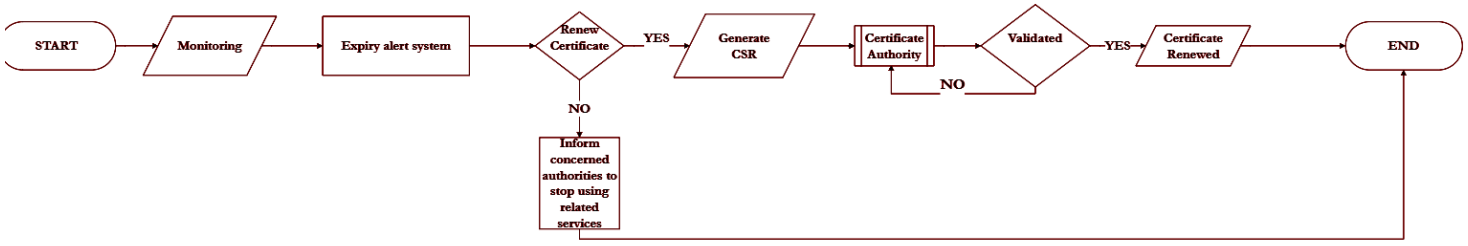
Monitoring

Once the key is generated and the certificate has been issued it is very crucial to ensure the safety of keys from unauthorised access, typically this process is considered key management (Furtak, 2020), in this regard we can adopt the hardware security module which is a device that protects keys in a tamper-resistant vault, separate from the network or Encrypt keys using Key Encryption Keys (KEKs) before storing them in offline devices or databases as well as utilising secure storage API'S. It can also be secured by ensuring that only authenticated and authorised users or machines can use keys to encrypt or decrypt data. Certificate management tools may also be used to automate this task and further, it can also be evaluated if the certificates are used ethically through monitoring activity. Key management would include multi-factor authentication (MFA) for key and certificate access to improve security and ensure a proper balance between key lifetime and strength. According to NIST SP 800-57 Part 1, the hash function may be used to provide security services. Robust hash functions like SHA-256 or SHA-3NIST protect to prevent loss of integrity of data. (Special Publications (SP) 800-56A, 800-56B, 800-56C and 800-108).



Management

Management of a key makes it imperative to constantly monitor the expiration of the issued certificates that have been deployed for the keys to ensure downtime is avoided. To ensure that certificates have not expired, administrators can enable alerts that notify them when a certificate is nearing expiry to ensure there are no disruptions in systems and services. Through the ACME protocol, users can also automate certificate lifecycle management communications between the CA and the organisation's servers. Before a certificate expires, a renewal process may be initiated. The CA will issue a new certificate with the same public key. This process may be done by generating a new CSR that needs to be sent over to the CA for authenticating the ownership as done in the first round and once it is validated a new certificate is issued, mostly using the same public key unless it's a case where key renewal is also necessary. Important to bear in mind that failure to renew would result in authentication failures or loss of efforts to establish secure connections

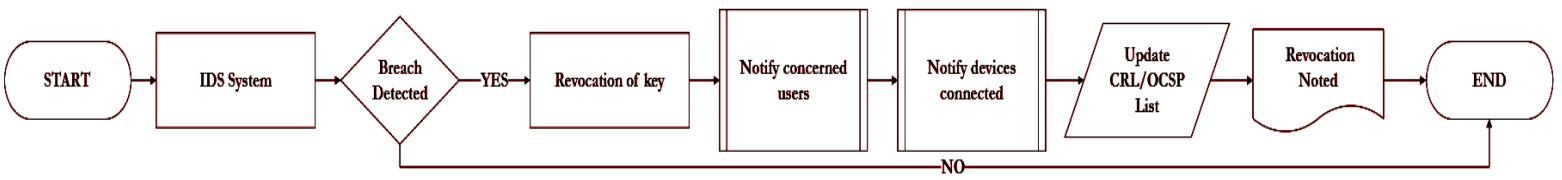


Revocation

When a key is compromised, or lost, this can be identified with the help of an intrusion detection system. When a key is revoked, it is made known to the users and they are informed to no longer use it, that is, they can't use the key to encrypt or decrypt messages or even verify digital signatures. There is also a notification sent to any devices or applications that may be linked to the certificate to ensure they immediately end their association with the certificate. The Certificate Authority (CA) must update the Certificate Revocation List (CRL), it ensures that the compromised certificate is added to the list. The list ensures it is known that a site's digital certificate is not trustworthy. The Online Certificate Status Protocol (OCSP) is also an alternative to the certificate revocation list (CRL) and is used to check whether a digital certificate is valid or if it has been revoked and this whole process is understandably called blacklist management.

Decommissioning

After a certificate has expired and is no longer needed for use or when a breach has occurred and the certificate was revoked, the key that was issued by the certificate authority needs to mandatorily be destroyed to mitigate any threats or risks this process is called decommissioning. After destroying the keys it is necessary to document the proof of deletion to comply with standards for compliance and auditing and important for meeting regulations set by PCI DSS and GDPR.



Alignment with Industry Best Practices

The above-mentioned cryptographic key lifecycle has been chalked out to ensure that it aligns and complies in terms of security and operational efficiency according to the NIST SP 800-57 (Guiding how organizations should manage cryptographic keys) and NIST SP 800-130 (Providing a Framework for Designing Cryptographic Key Management). It focuses on the safety and integrity of the key that is maintained by using hash functions as well as incorporating continuous monitoring of secure key storage and revocation procedures to ensure a physically secure environment for storing private keys and protecting them from unauthorized access and tampering. This lifecycle is also drafted keeping in mind that it can be utilised globally in compliance with the regulations laid down by the General Data Protection Regulation law.

References

Barker, E. (2020, May 4). *Recommendation for Key Management: Part 1 – General*. Csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final

Barker, E., & Roginsky, A. (2018). *Withdrawn NIST Technical Series Publication Warning Notice Withdrawn Publication Series/Number NIST Special Publication 800-133 Title Recommendation for Cryptographic Key Generation Publication Date(s) December 2012 Withdrawal Date Superseding Publication(s) (if applicable) Title Recommendation for Cryptographic Key Generation Author(s) Additional Information (if applicable)*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133.pdf

Barker, E., Roginsky, A., & Davis, R. (2020). *Recommendation for cryptographic key generation*. https://doi.org/10.6028/nist.sp.800-133r2

Cooper, D. (n.d.). *A Closer Look at Revocation and Key Compromise in Public Key Infrastructures*. https://csrc.nist.rip/nissc/1998/proceedings/paperG2.pdf

Furtak, J. (2020). Cryptographic Keys Generating and Renewing System for IoT Network Nodes—A Concept. *Sensors*, *20*(17), 5012. https://doi.org/10.3390/s20175012

Göppert, J., Walz, A., & Sikora, A. (2024). A Survey on Life-Cycle-Oriented Certificate Management in Industrial Networking Environments. *Journal of Sensor and Actuator Networks*, *13*(2), 26–26. https://doi.org/10.3390/jsan13020026

Key Management - OWASP Cheat Sheet Series. (n.d.). Cheatsheetseries.owasp.org. https://cheatsheetseries.owasp.org/cheatsheets/Key_Management_Cheat_Sheet.html

Key Revocation - CSF Tools. (2023, December 23). CSF Tools - the Cybersecurity Framework for Humans. https://csf.tools/reference/cloud-controls-matrix/v4-0/cek/cek-13/

Rana, S., Parast, F. K., Kelly, B., Wang, Y., & Kent, K. B. (2023). A comprehensive survey of cryptography key management systems. *Journal of Information Security and Applications*, *78*, 103607. https://doi.org/10.1016/j.jisa.2023.103607

What is Encryption Key Management? | Entrust. (2024). Entrust.com. https://www.entrust.com/resources/learn/what-is-encryption-key-management