Key management

Questions and answers

1. Name major stages of the key lifecycle
    - generation
    - distribution
    - destruction
2. Name places where keys could be present/stored. Sort them best to worst location
    1. Hardware security module
    2. Isolated cryptographic service
        - e.g. Isolated storage on windows
        - Trust stores (e.g. certificates)
    3. Write them down a paper and store it in a safe (probably pretty safe but not scalable and errorprone)
    4. Plaintext in a file (bad)
3. Name techniques to protect stored keys?
    - Hardware security module
    - encryption of keys with Key encryption keys (basically store them encrypted)
    - Maybe use OS services for encryption?
4. What is important when generating keys?
    - key lenght has match requirements: how long is the data to be stored and may not be decrypted?)
    - keys have to be random (ideally hardware randomness)
    - The same key should only be used for one purpose (as ciphery may be weakened, potenatial damage is minimised)
5. How long should a key be valid?
    - depends on the requirements. The more sensitive the data, the shorter the validity of a key should be. Or to put differently: the shorter the the safer
6. What needs to be considered when keys are distributed?
    - this should only be done via secure channels
7. Assuming you need a backup of your keys. Where would you place it and how would you protect the keys from illegitimate access. Who guards the guards?
    - encrypted database.. (Key Encryption Keys: KEKs)
    - keys for encryption for the keys might be escrowed (given to a third party)
        - never escrow key for signature
        - better just escrow the keys that are used to encrypt the keys (I believe)
    - As the guards (of the KEKs) don't have access to the encrypted keys they cannot do anything with them (except guard them) or there is a double encryption of the backup (with 2 keys).. see next questions.
8. Name concepts on how you could prevent a single person to access a system or key?
    - 4 eye principle (kind of): a person alone may not access a key.
        - Storage not directly accessible to the person with the key
            - separation of duties

        - Split key or double encryption so we need 2 keys (or to parts to form the key) to decrypt and these 2 keys are "owned" by different people.
            - could also be called split knowledge
9. Name concepts to reveal keys in an emergency but only with approval of multiple persons?
    - Not sure I understand, question seems similar to the previous ones
    - see previous questions: split knowledge, separation of duties (see previous)
    - Auditing (ensure we can track who accessed aka "revealed" keys)
10. Assuming we lost a key. What needs to be considered? Provide a bullet-list.
    - gather information about impact
        - Who was using this key?
        - What was protected (encrypted, signed etc.) with this key?
        - verify that other keys and data is not affected
    - check if key can be recovered (since we should have a backup)
        - if yes recover key but I generally assume this is not possible
    - inform affected people
    - perform revocation actions (example revokation of certificates)
        - provided safe recovery is not possible
    - reissue keys (if necessary)
    - try prevent such an incident in the future
        - review processes, software, equipment
        - educate personel
    - leftovers
        - handle potential legal issues (liability) -> i believe this is normally solved beforehand (no liability etc.)
        - minimize damage to reputation..

Notes

https://en.wikipedia.org/wiki/Key_management
https://cheatsheetseries.owasp.org/cheatsheets/Key_Management_Cheat_Sheet.html
https://info.townsendsecurity.com/definitive-guide-to-encryption-key-management-fundamentals
https://en.wikipedia.org/wiki/Hardware_security_module -> HSM Hardware security module

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p1r3.pdf