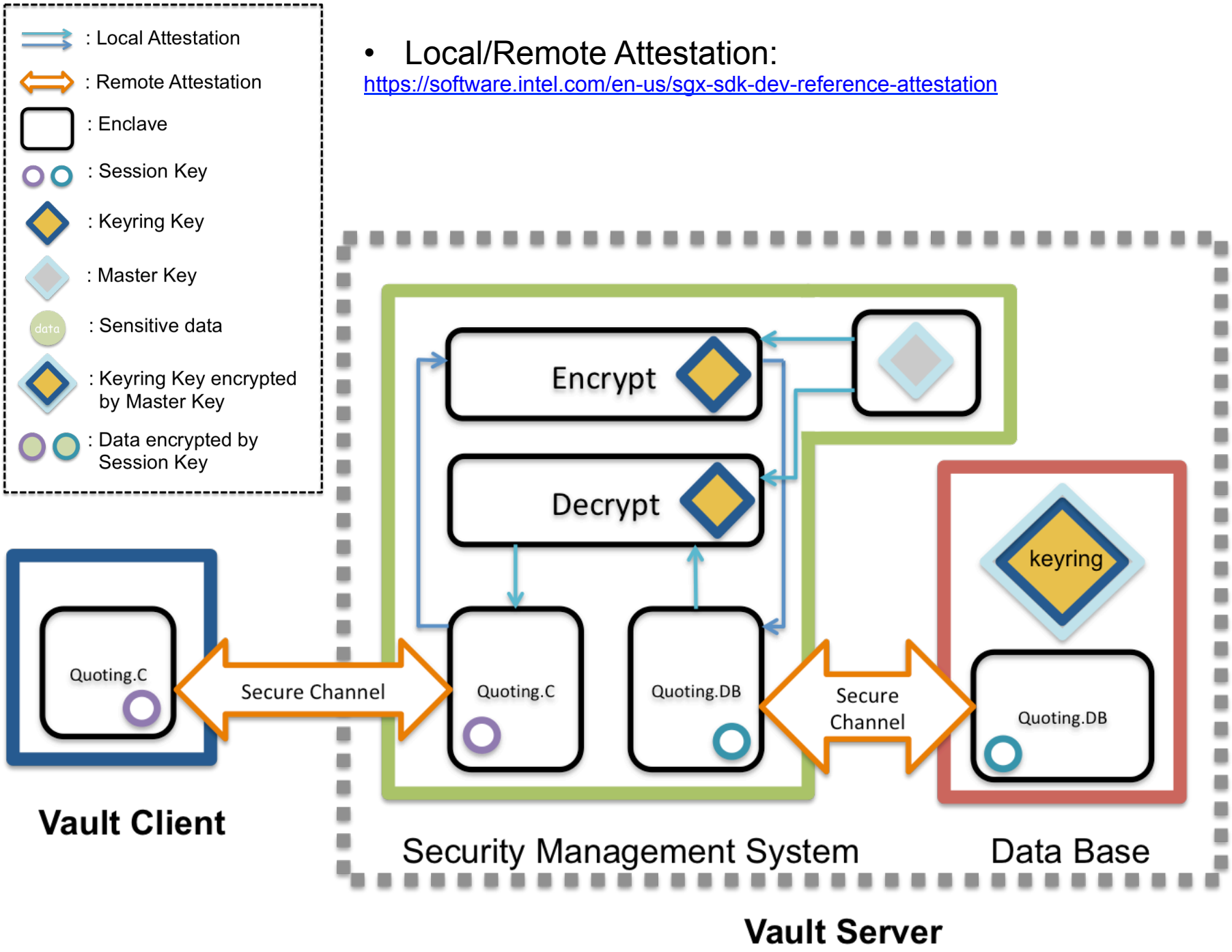
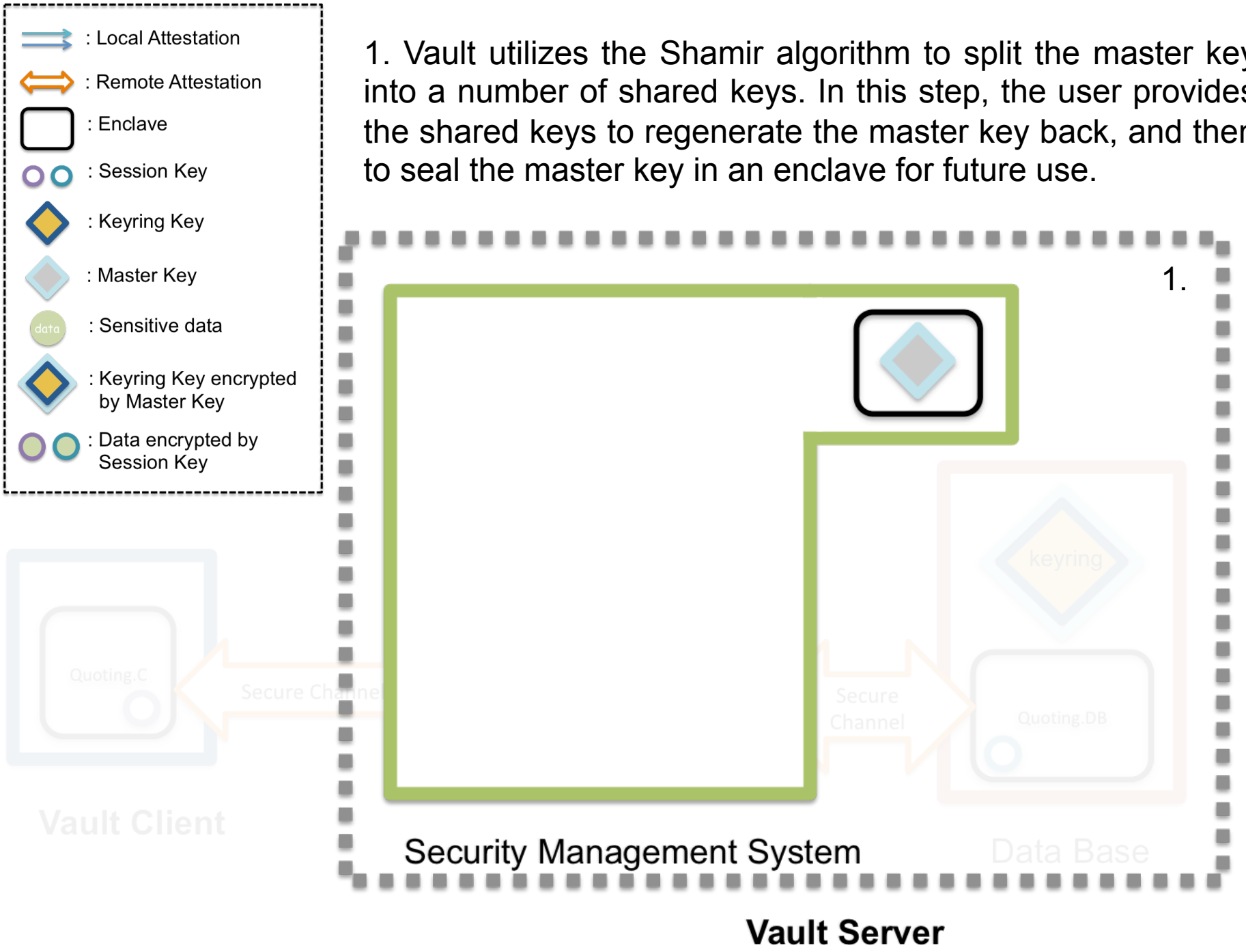
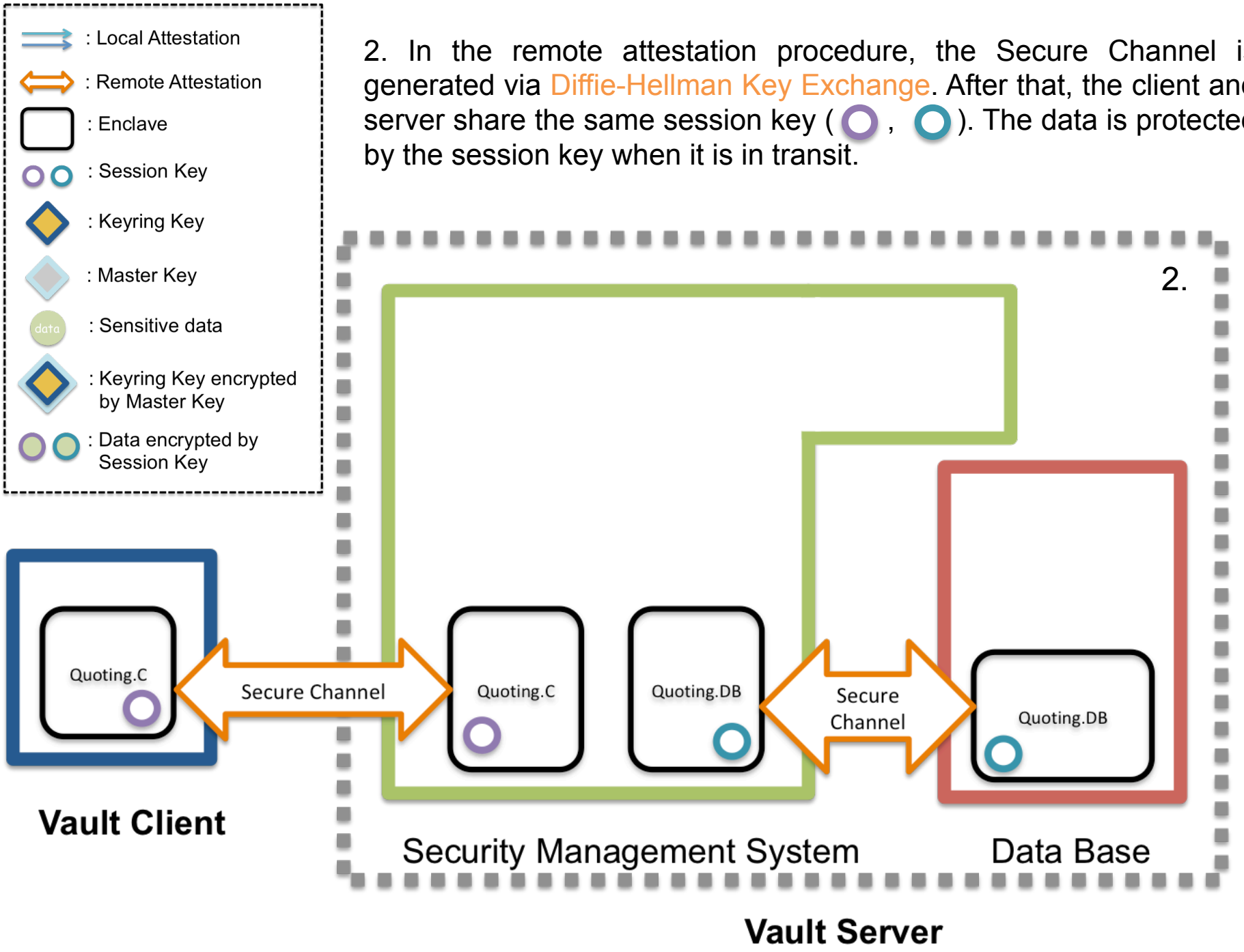
Prototype: Vault with Intel SGX

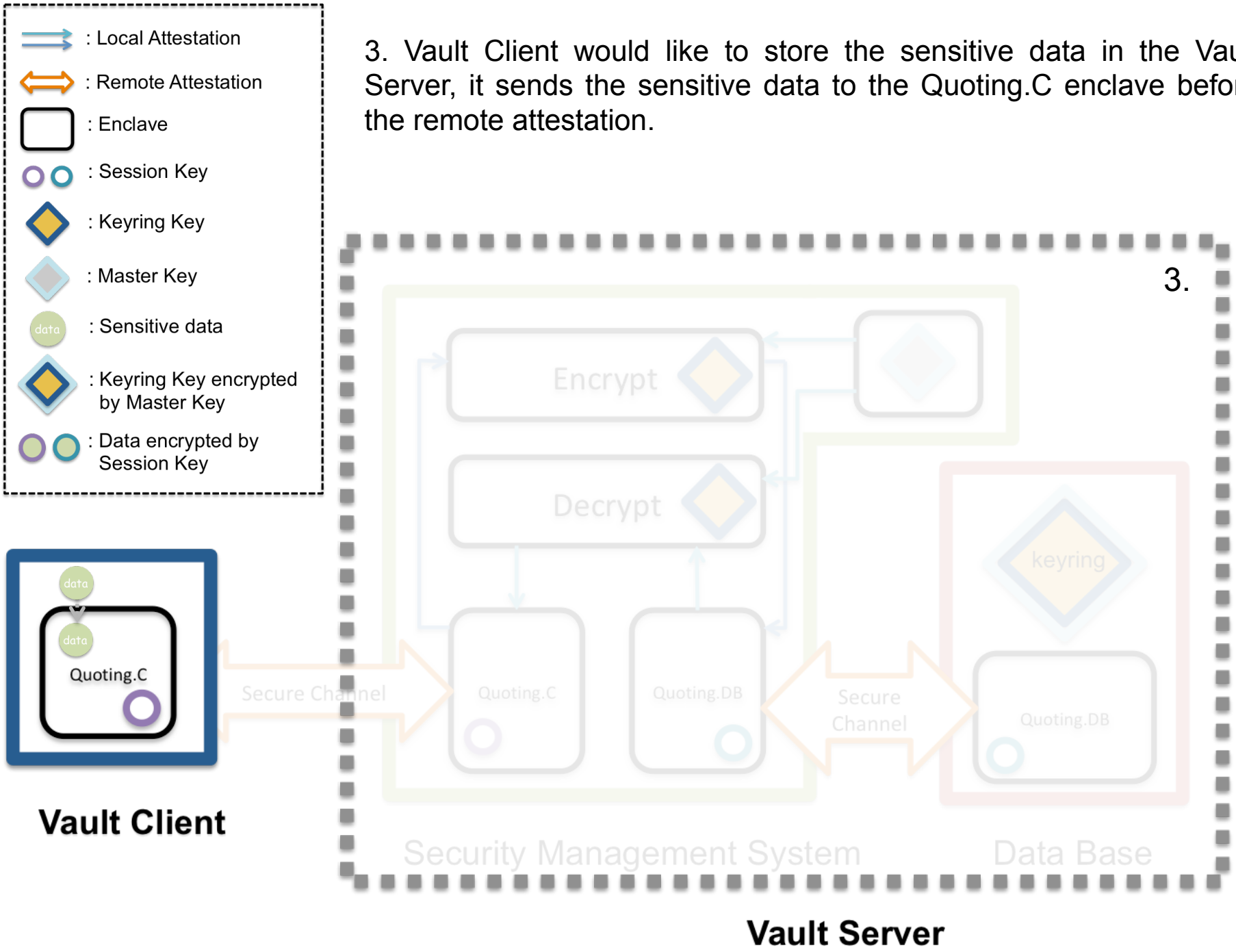
-Shan Kuan

- Local/Remote Attestation:
https://software.intel.com/en-us/sgx-sdk-dev-reference-attestation




: Local Attestation
: Remote Attestation
: Enclave
: Session Key
: Keyring Key
: Master Key
data
: Sensitive data
: Keyring Key encrypted by Master Key
: Data encrypted by Session Key
1. Vault utilizes the Shamir algorithm to split the master key into a number of shared keys. In this step, the user provides the shared keys to regenerate the master key back, and then to seal the master key in an enclave for future use.
1.
keyring
Quoting.C
Secure Channel
Secure Channel
Quoting.DB
Vault Client
Security Management System
Data Base
Vault Server


: Local Attestation
: Remote Attestation
: Enclave
: Session Key
: Keyring Key
: Master Key
data
: Sensitive data
: Keyring Key encrypted by Master Key
: Data encrypted by Session Key
2. In the remote attestation procedure, the Secure Channel is generated via Diffie-Hellman Key Exchange. After that, the client and server share the same session key (,). The data is protected by the session key when it is in transit.
2.
Quoting.C
Secure Channel
Quoting.C
Quoting.DB
Secure Channel
Quoting.DB
Vault Client
Security Management System
Data Base
Vault Server


: Local Attestation
: Remote Attestation
: Enclave
: Session Key
: Keyring Key
: Master Key
data
: Sensitive data
: Keyring Key encrypted by Master Key
: Data encrypted by Session Key
3. Vault Client would like to store the sensitive data in the Vault Server, it sends the sensitive data to the Quoting.C enclave before the remote attestation.
3.
Encrypt
Decrypt
keyring
data
data
Quoting.C
Secure Channel
Quoting.C
Quoting.DB
Secure Channel
Quoting.DB
Security Management System
Data Base
Vault Client
Vault Server

: Local Attestation

: Remote Attestation

: Enclave

: Session Key

: Keyring Key

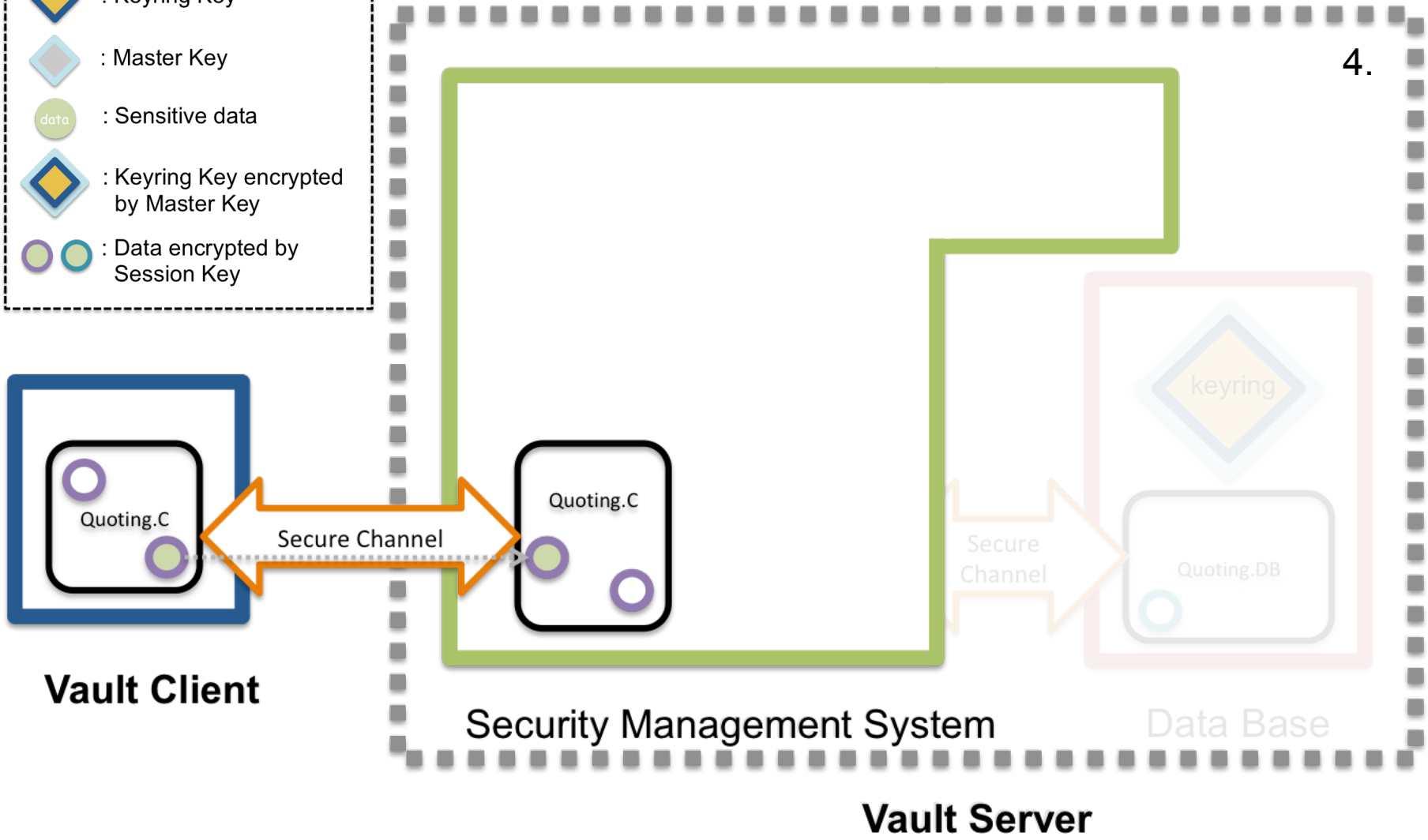
: Master Key

: Sensitive data

: Keyring Key encrypted by Master Key

: Data encrypted by Session Key

4. The sensitive data (data) is encrypted by the session key ( ) in the Quoting.C enclave. After that, the encrypted data ( ) is sent to another Quoting.C enclave, which runs in the Security Management System via Secure Channel.



: Local Attestation

: Remote Attestation

: Enclave

: Session Key

: Keyring Key

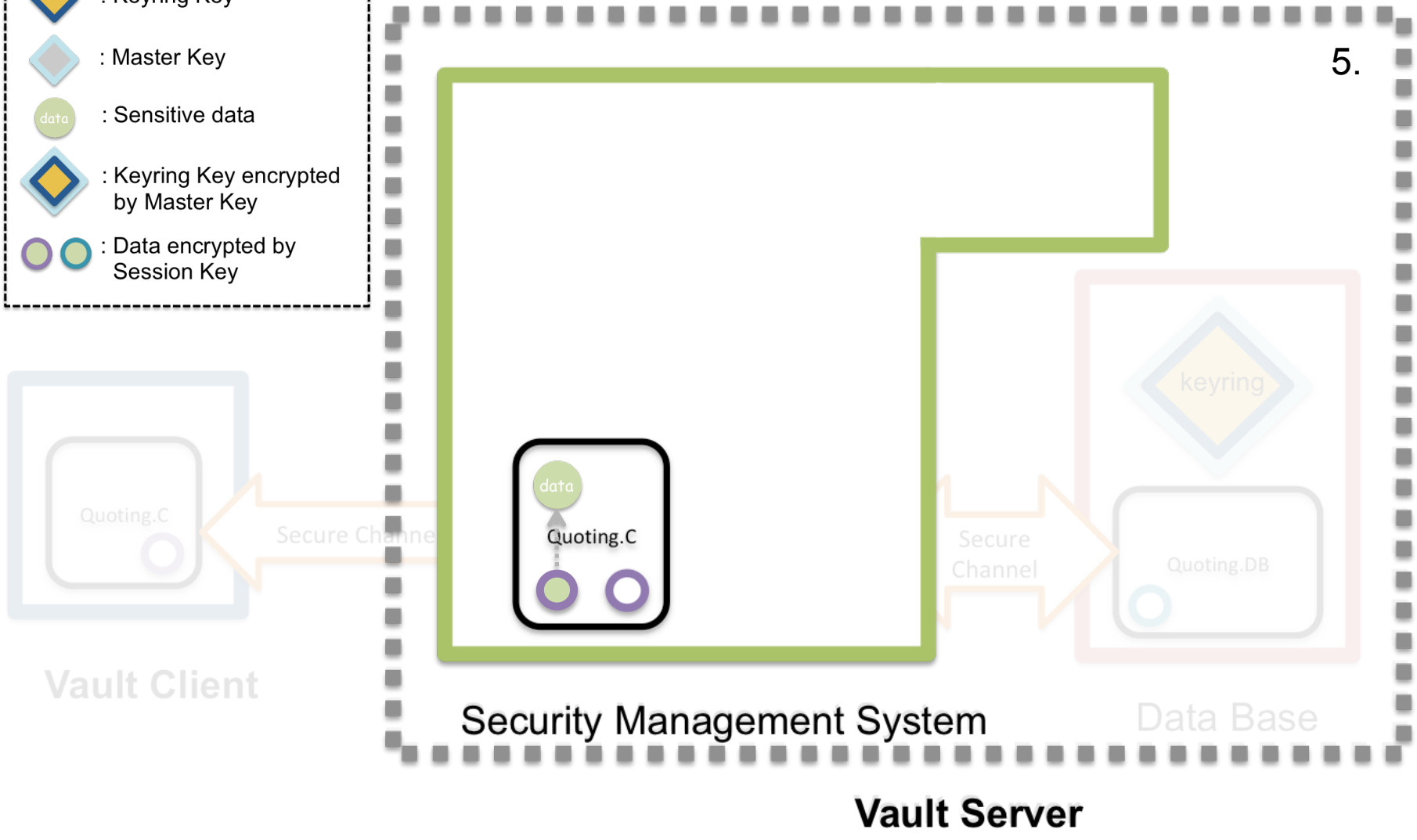
: Master Key

: Sensitive data

: Keyring Key encrypted by Master Key

: Data encrypted by Session Key

5. The encrypted data ( ) is decrypted by the session key ( ) in the Quoting.C enclave. The sensitive data ( ) is retrieved back in this step.



: Local Attestation

: Remote Attestation

: Enclave

: Session Key

: Keyring Key

: Master Key

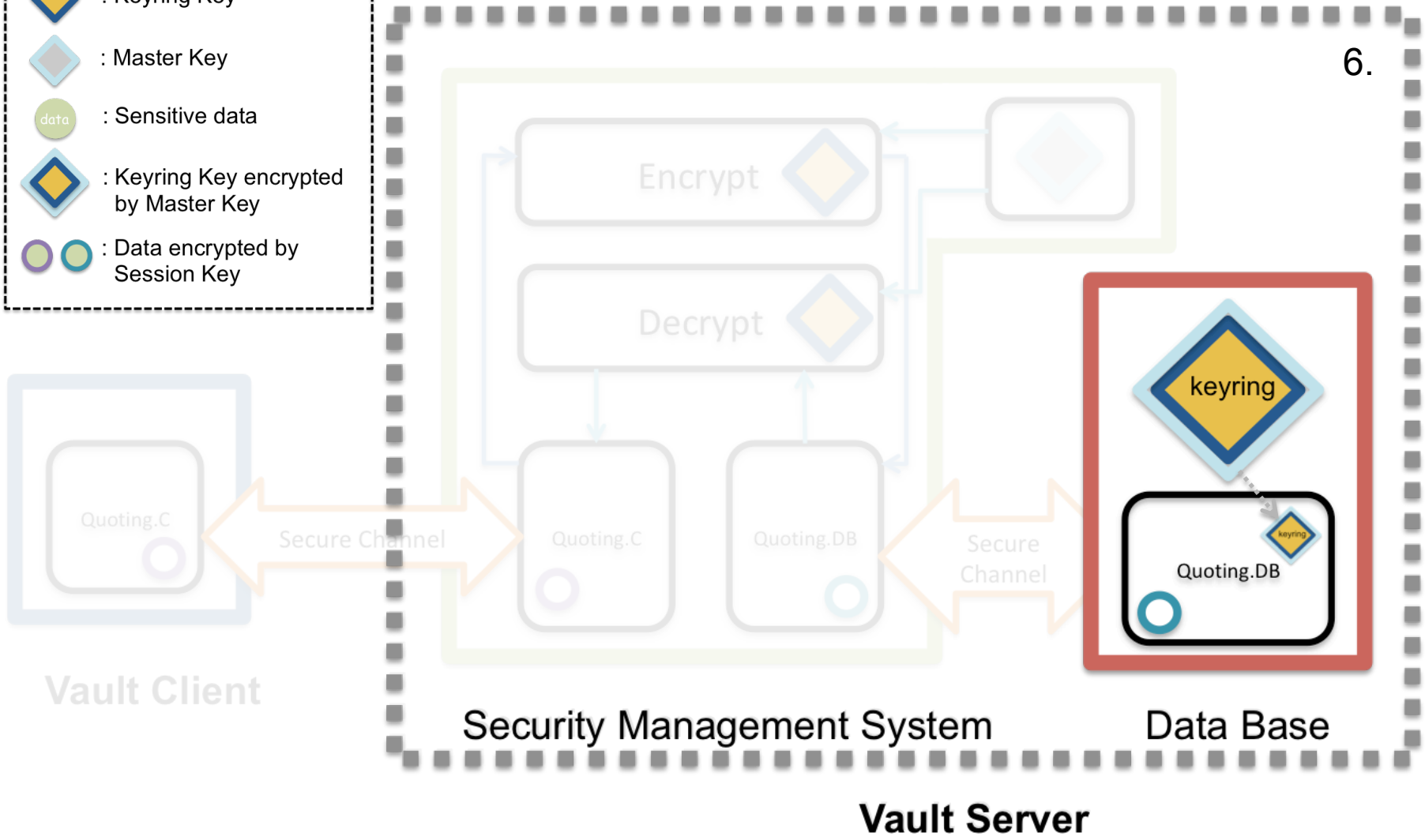
: Sensitive data

: Keyring Key encrypted by Master Key

: Data encrypted by Session Key

6-9. In the step from 6 to 9 is the procedure, which retrieve the keyring key back from the database , keyring key is the key use to encrypt the data before store in the database.

6. Send the encrypted keyring key (keyring) to the Quoting.DB enclave before the remote attestation.



: Local Attestation

: Remote Attestation

: Enclave

: Session Key

: Keyring Key

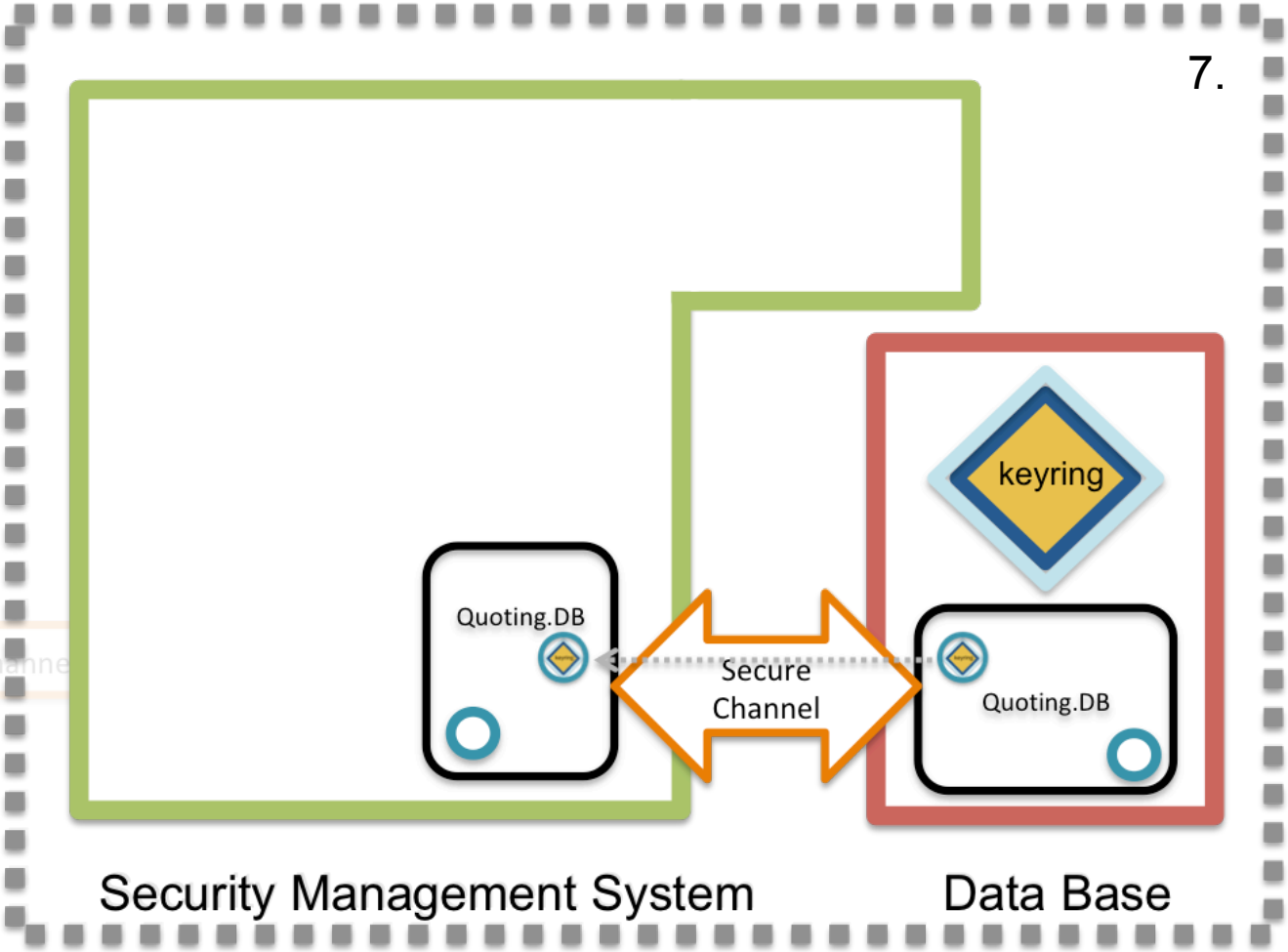
: Master Key

: Sensitive data

: Keyring Key encrypted by Master Key

: Data encrypted by Session Key

7. The encrypted keyring key ( ) is encrypted by the session key ( ). After that, the double layer encrypted keyring key ( ) is sent to another Quoting.DB enclave, which runs in the Security Management System via Secure Channel.



: Local Attestation

: Remote Attestation

: Enclave

: Session Key

: Keyring Key

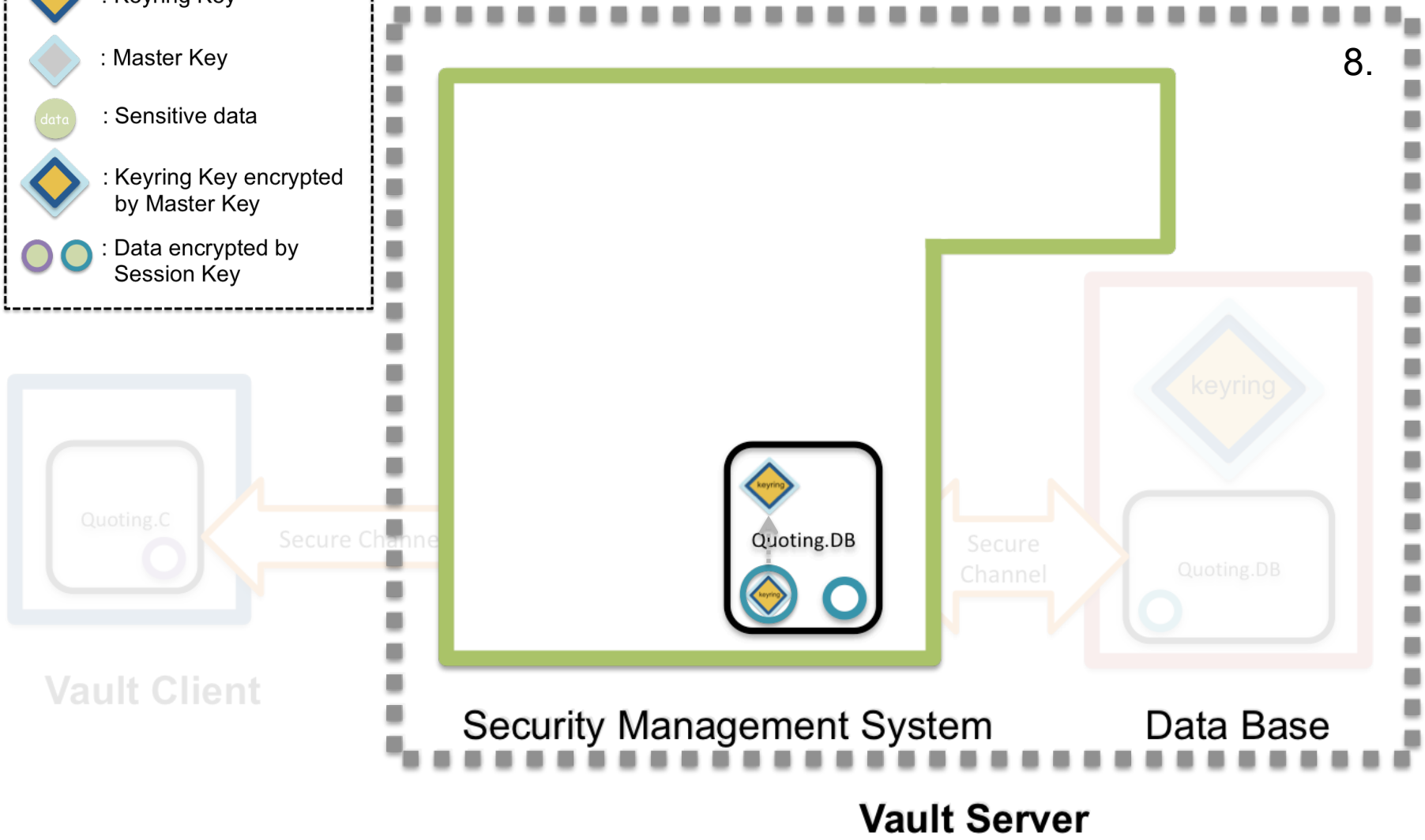
: Master Key

: Sensitive data

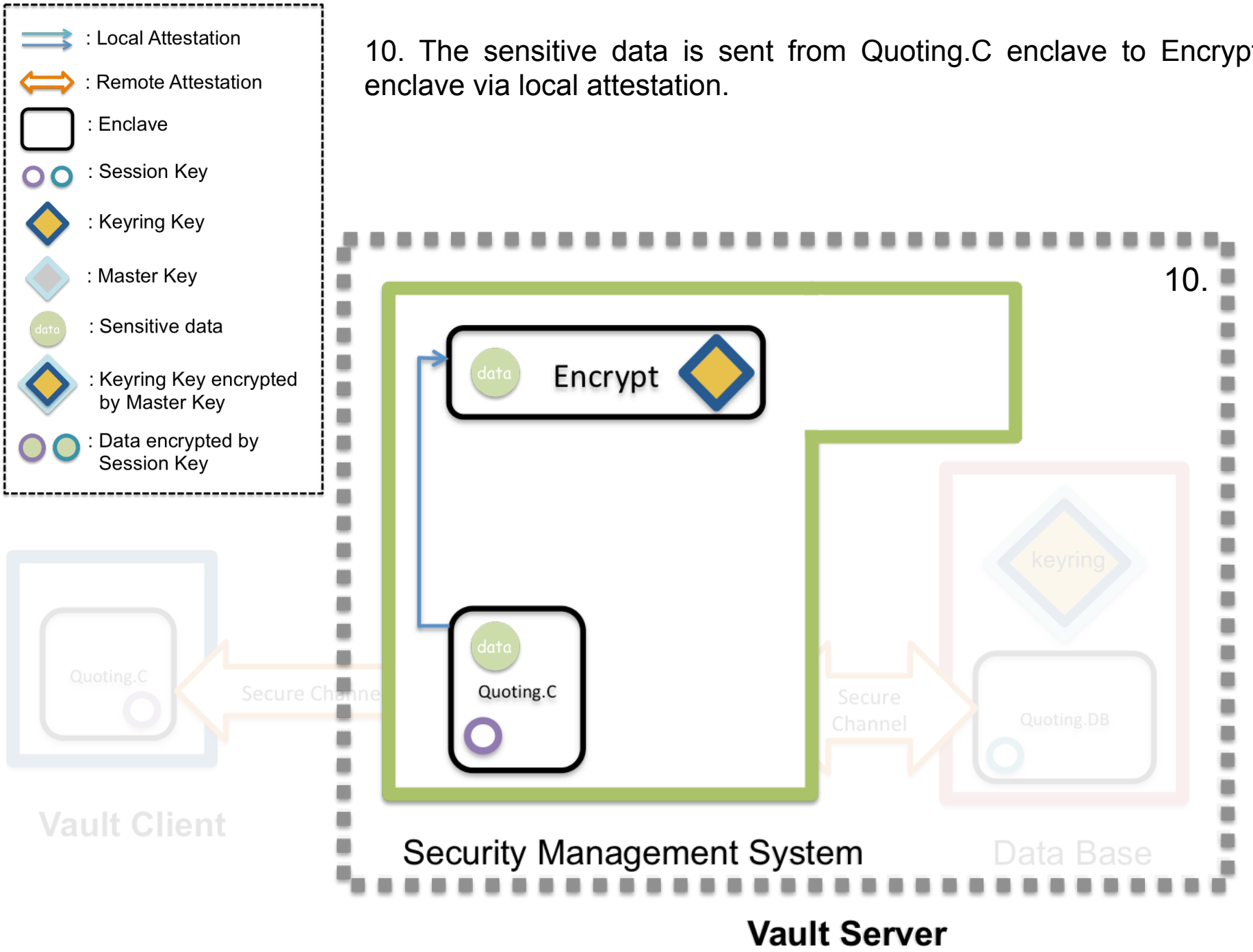
: Keyring Key encrypted by Master Key

: Data encrypted by Session Key

8. The double layer encrypted keyring key ( ) is decrypted by the session key ( ) in the Quoting.DB enclave. The one layer encrypted keyring key ( ) is retrieved back in this step.



10. The sensitive data is sent from Quoting.C enclave to Encrypt enclave via local attestation.



: Local Attestation

: Remote Attestation

: Enclave

: Session Key

: Keyring Key

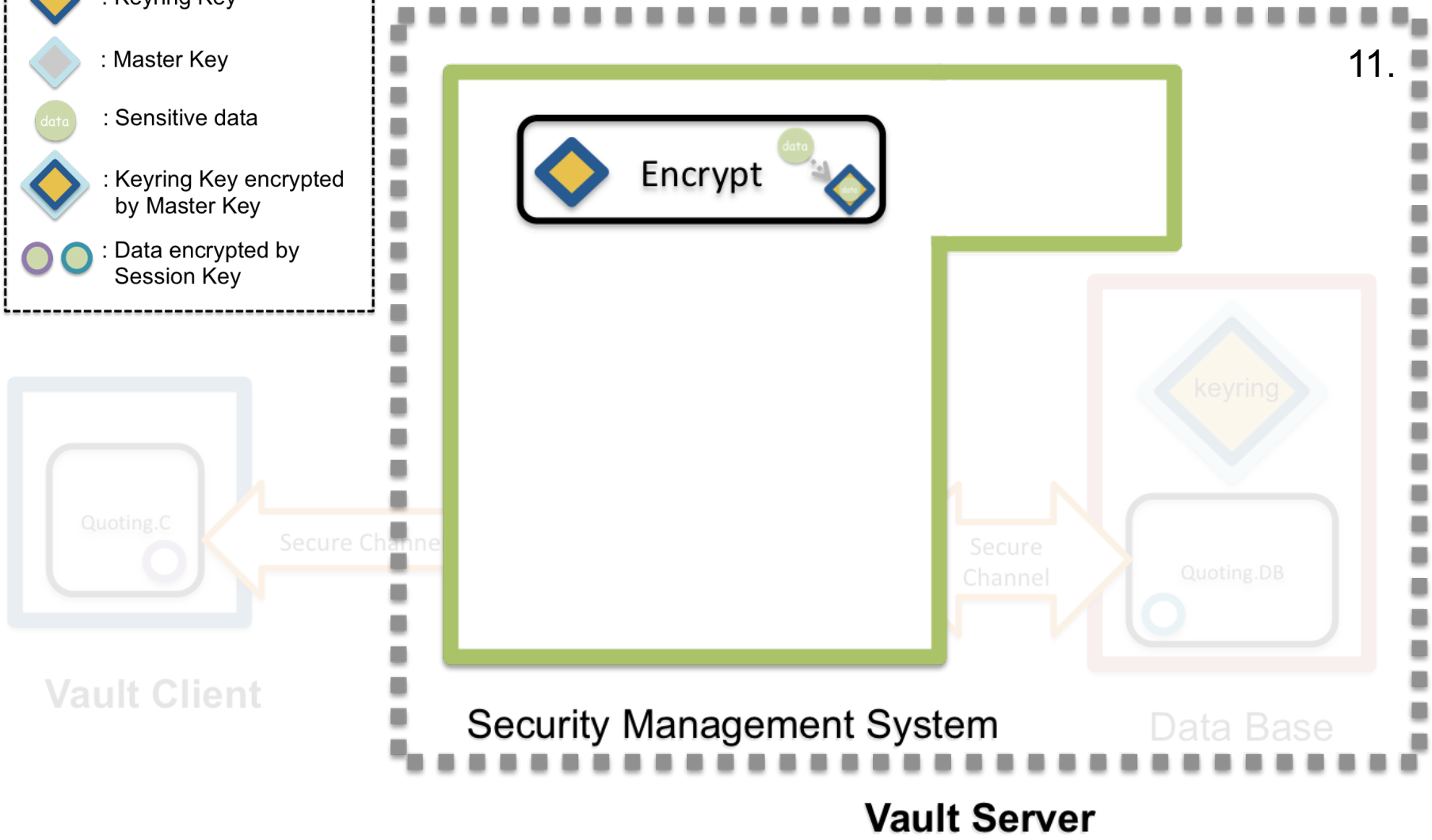
: Master Key

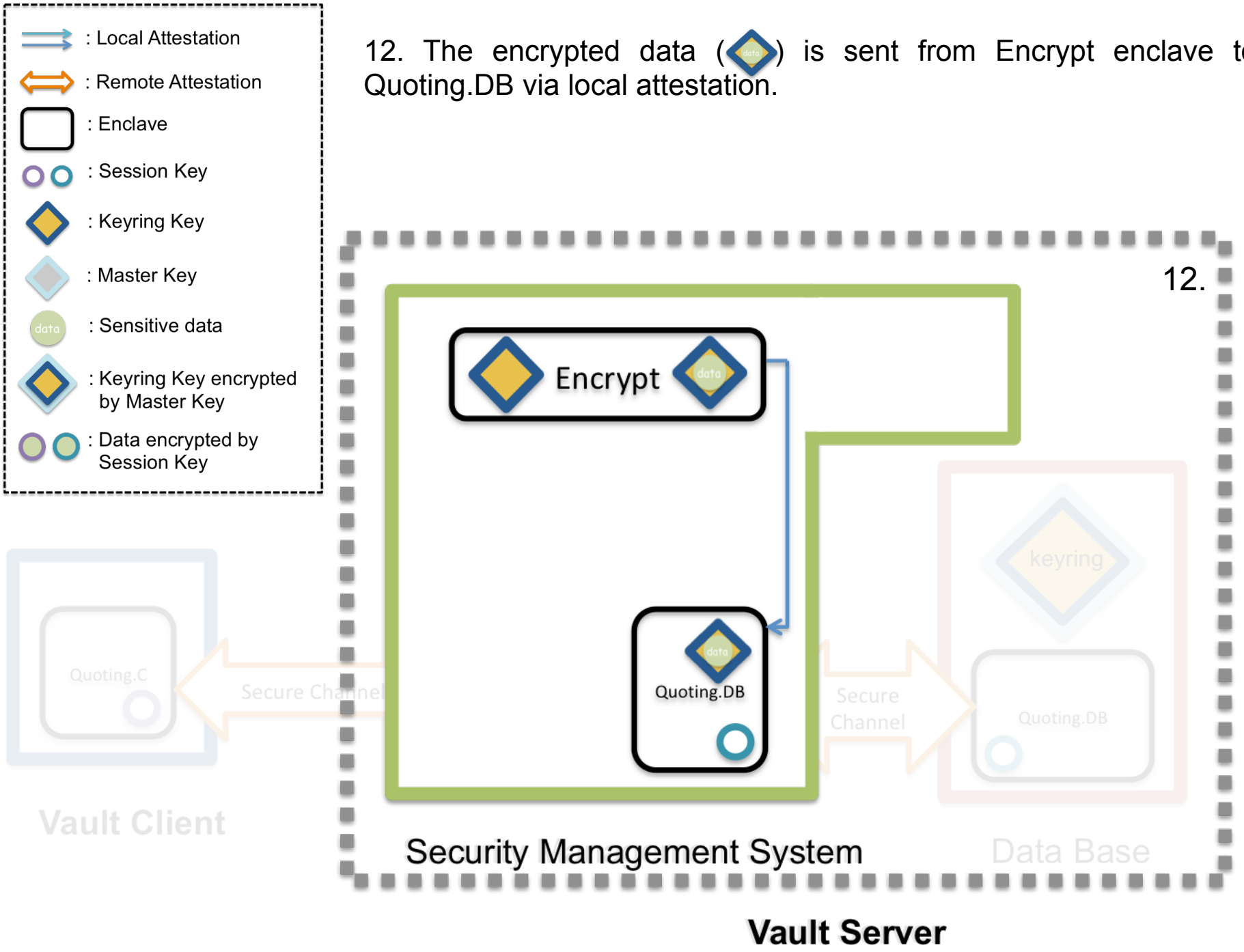
: Sensitive data

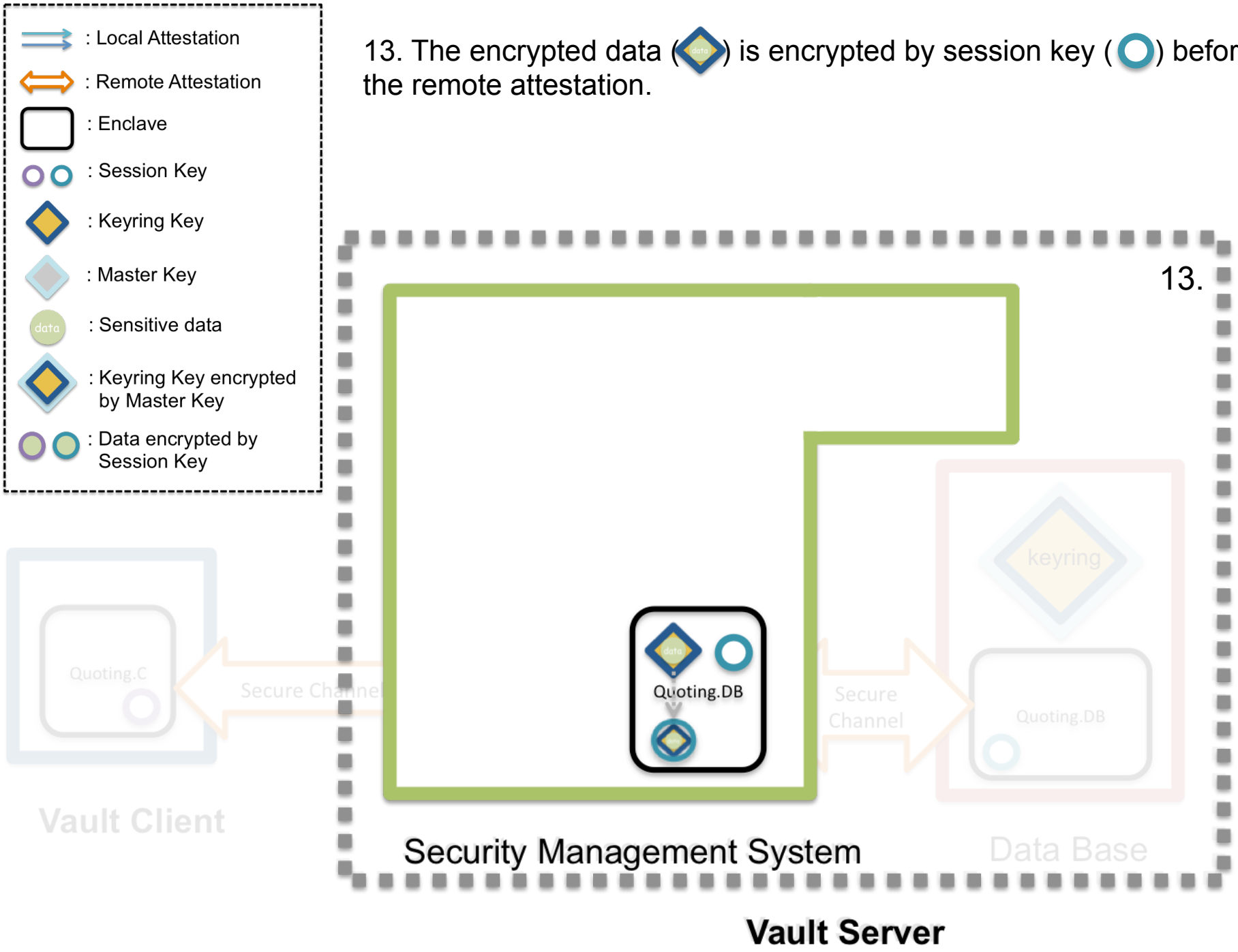
: Keyring Key encrypted by Master Key

: Data encrypted by Session Key

11. The sensitive data (data) is encrypted by keyring key ( ) in the Encrypt enclave. After that, to obtain the encrypted data ( ).




: Local Attestation
: Remote Attestation
: Enclave
: Session Key
: Keyring Key
: Master Key
data
: Sensitive data
: Keyring Key encrypted by Master Key
: Data encrypted by Session Key
12. The encrypted data (data) is sent from Encrypt enclave to Quoting.DB via local attestation.
12.
Encrypt
data
Quoting.DB
Quoting.C
Secure Channel
Secure Channel
keyring
Quoting.DB
Vault Client
Security Management System
Data Base
Vault Server


: Local Attestation
: Remote Attestation
: Enclave
: Session Key
: Keyring Key
: Master Key
: Sensitive data
: Keyring Key encrypted by Master Key
: Data encrypted by Session Key
13. The encrypted data ( ) is encrypted by session key ( ) before the remote attestation.
13.
Quoting.C
Secure Channel
Quoting.DB
Secure Channel
keyring
Quoting.DB
Vault Client
Security Management System
Data Base
Vault Server

: Local Attestation

: Remote Attestation

: Enclave

: Session Key

: Keyring Key

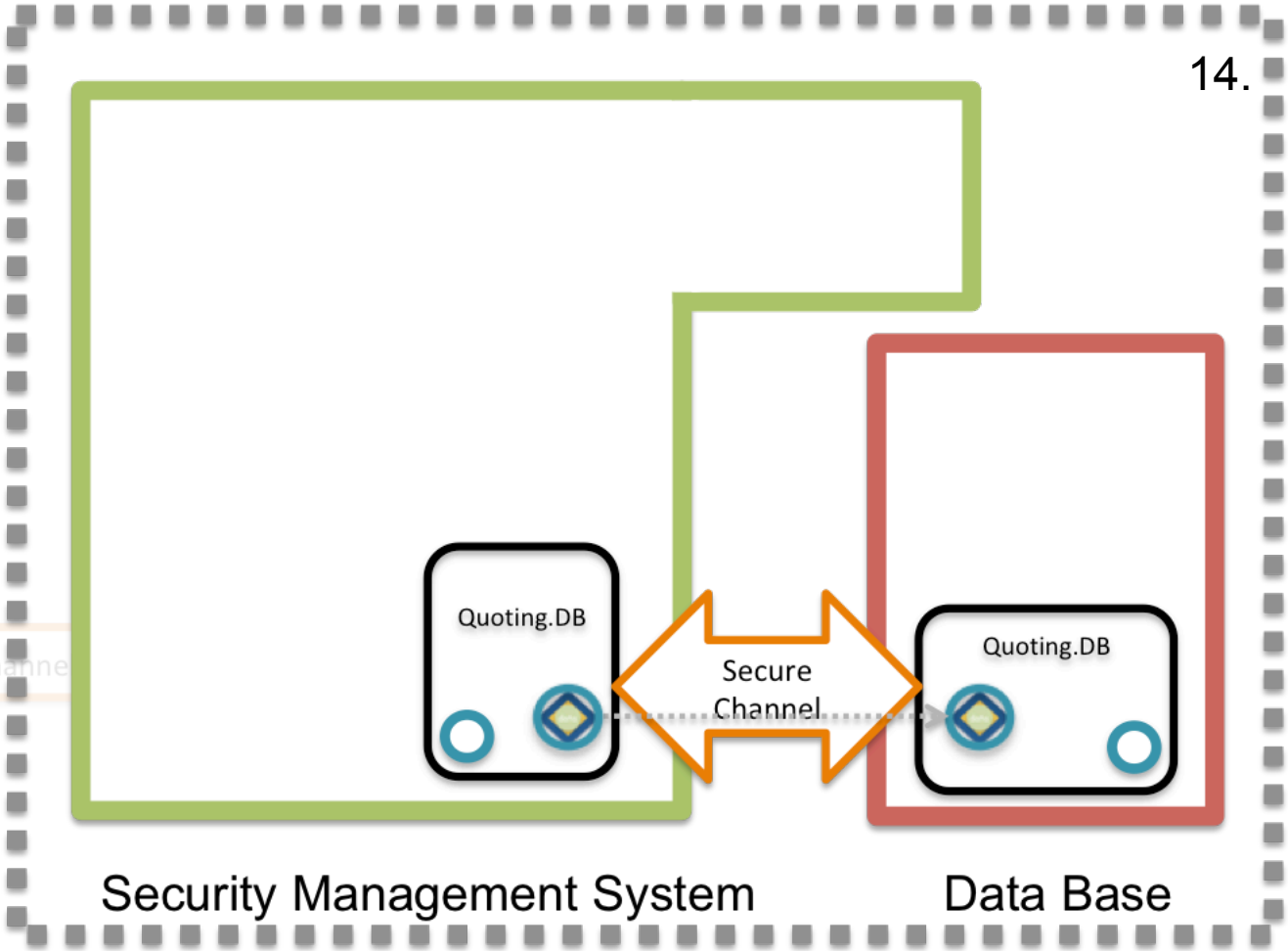
: Master Key

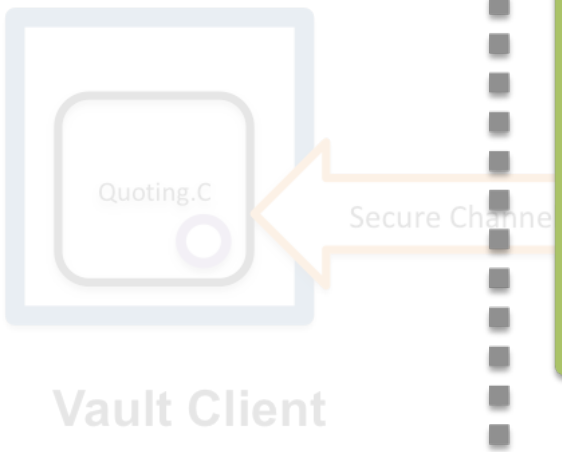
: Sensitive data

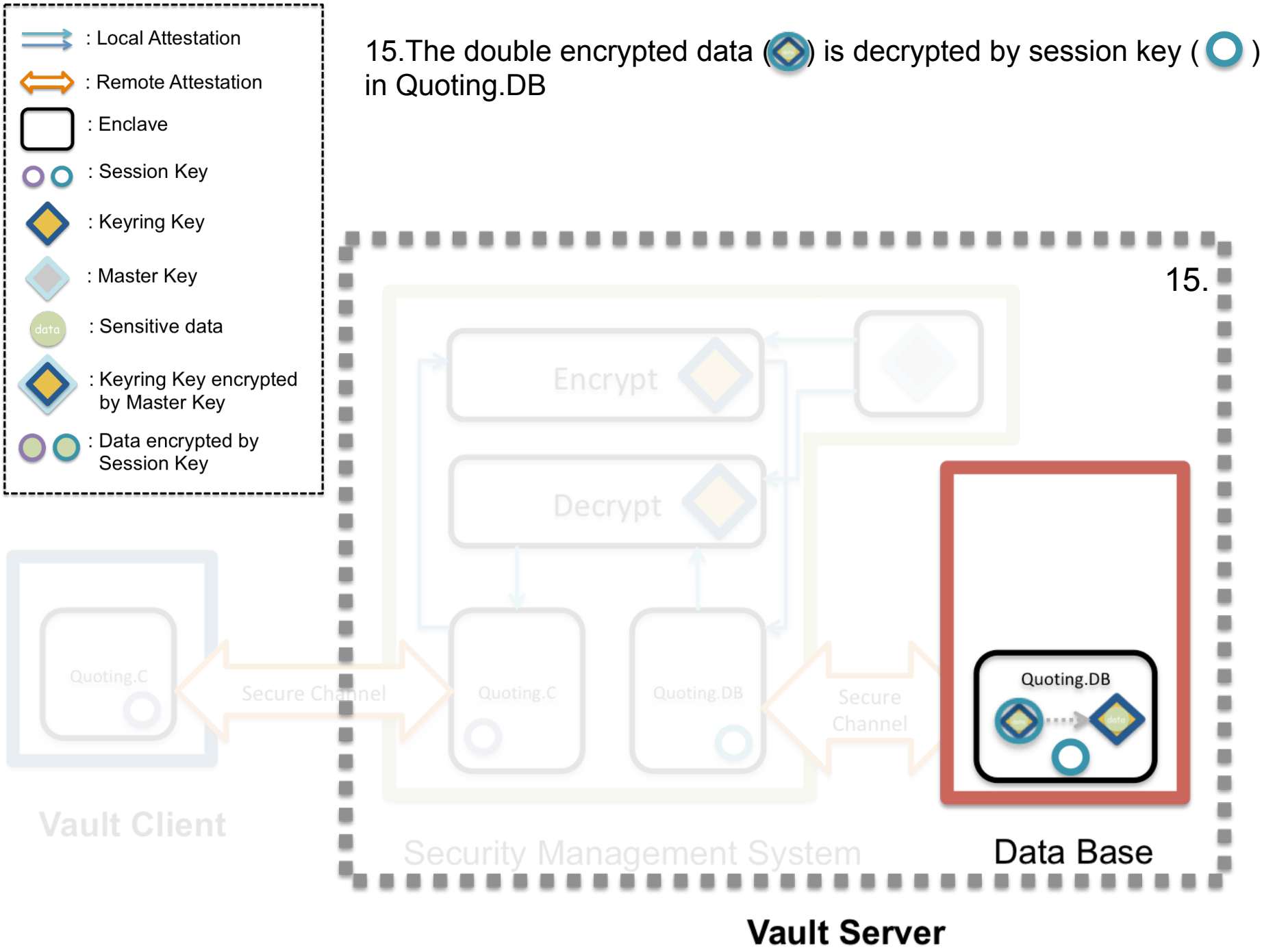
: Keyring Key encrypted by Master Key

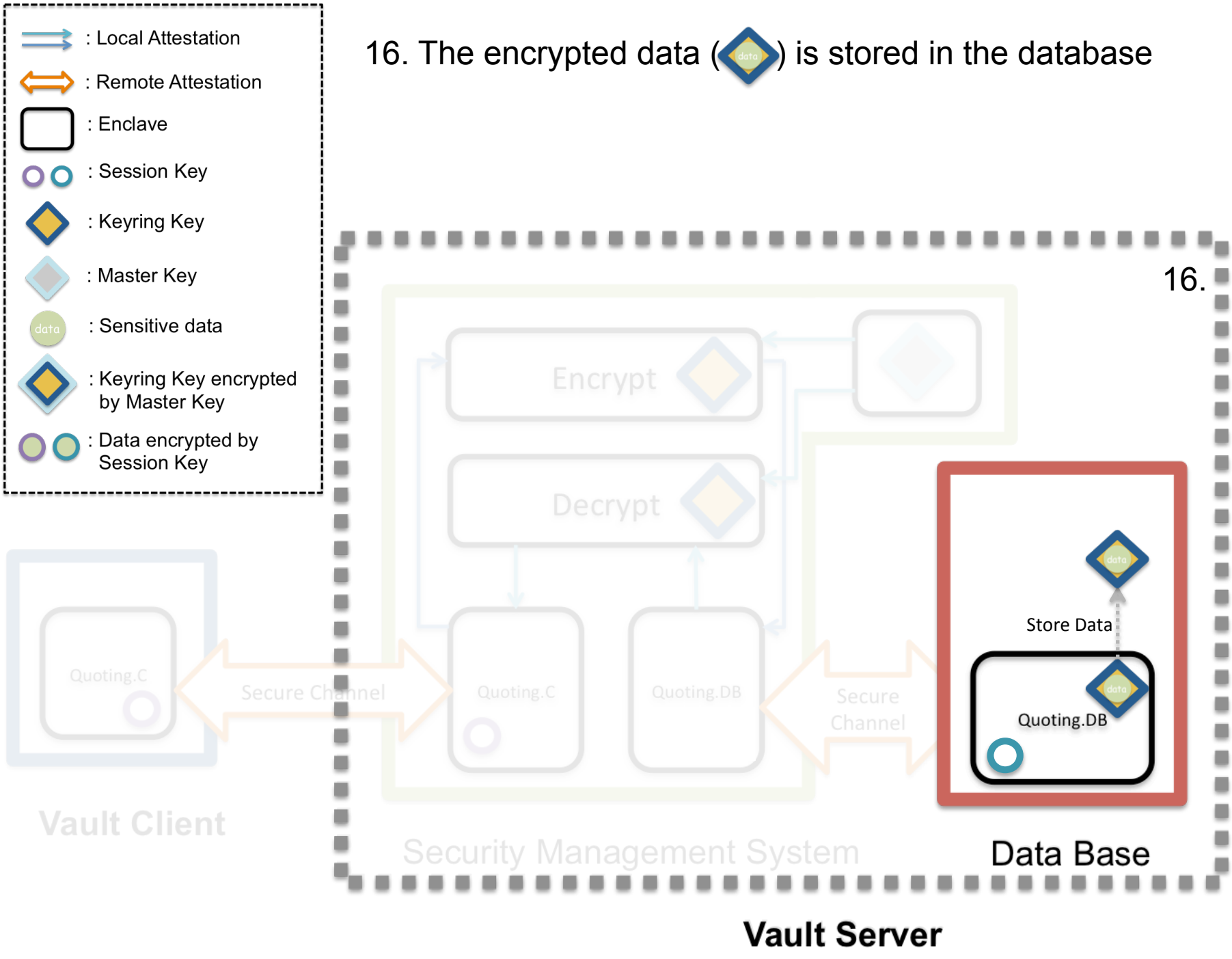
: Data encrypted by Session Key

14. The double encrypted data ( ) is sent to another Quoting.DB, which run on the database via Secure Channel

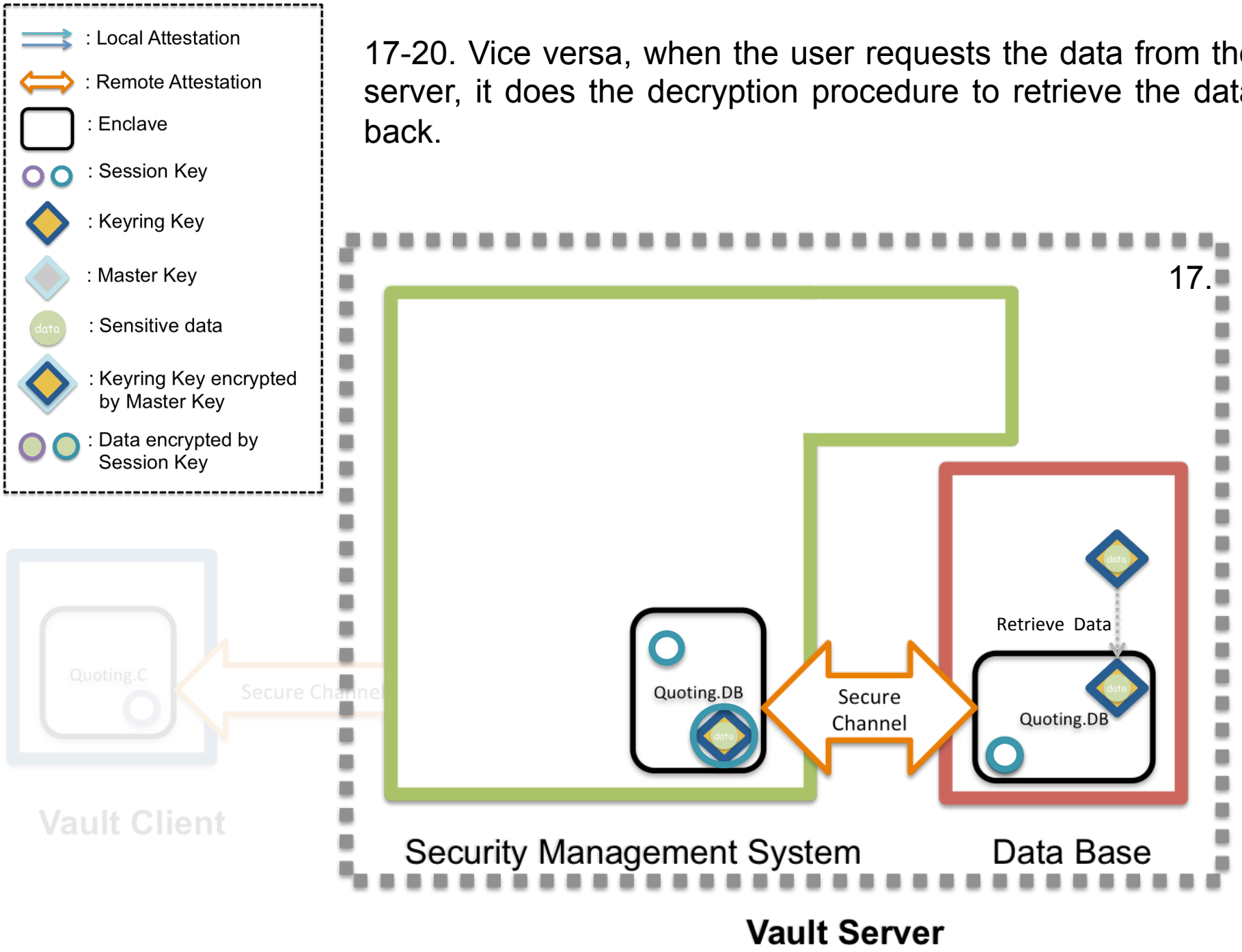


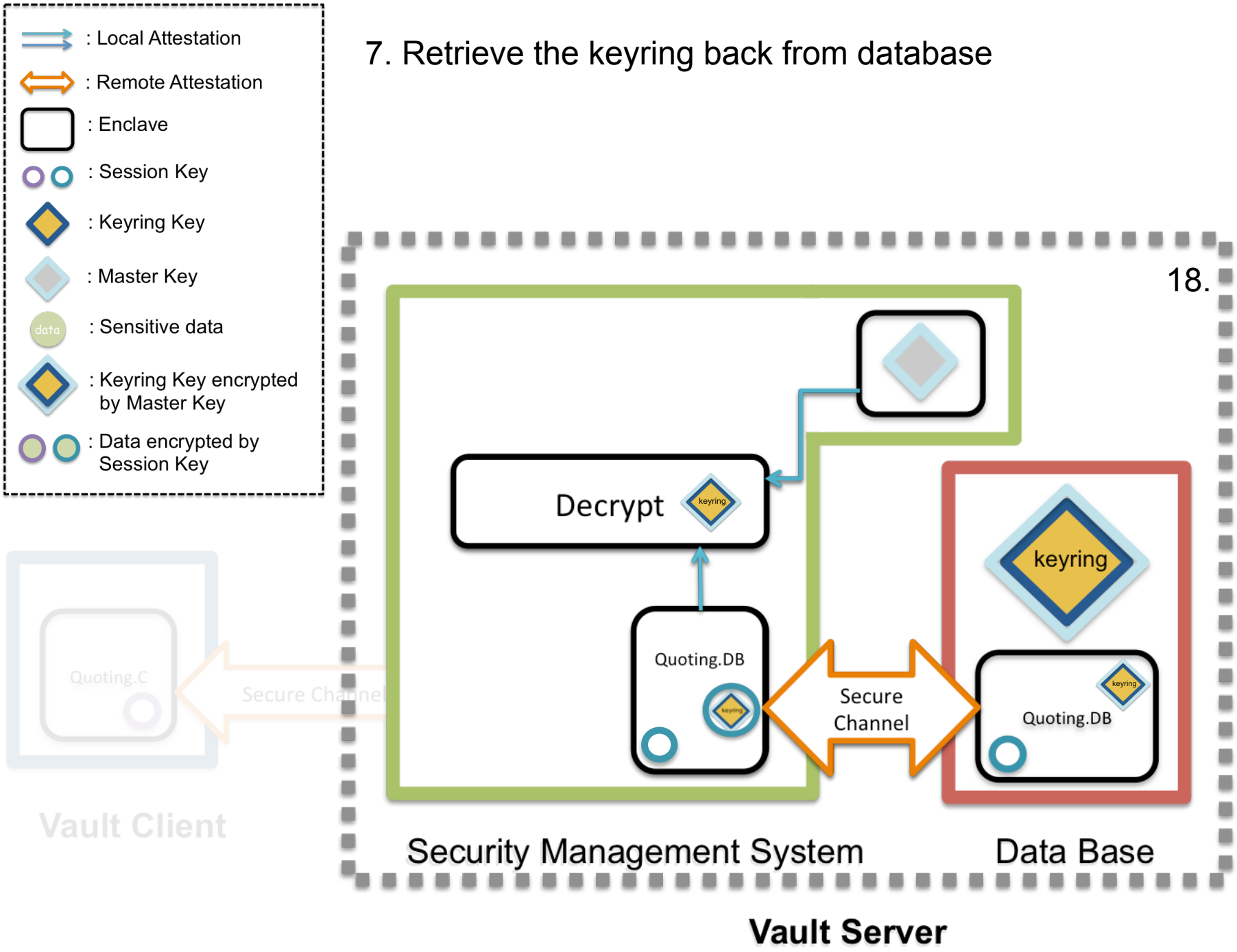


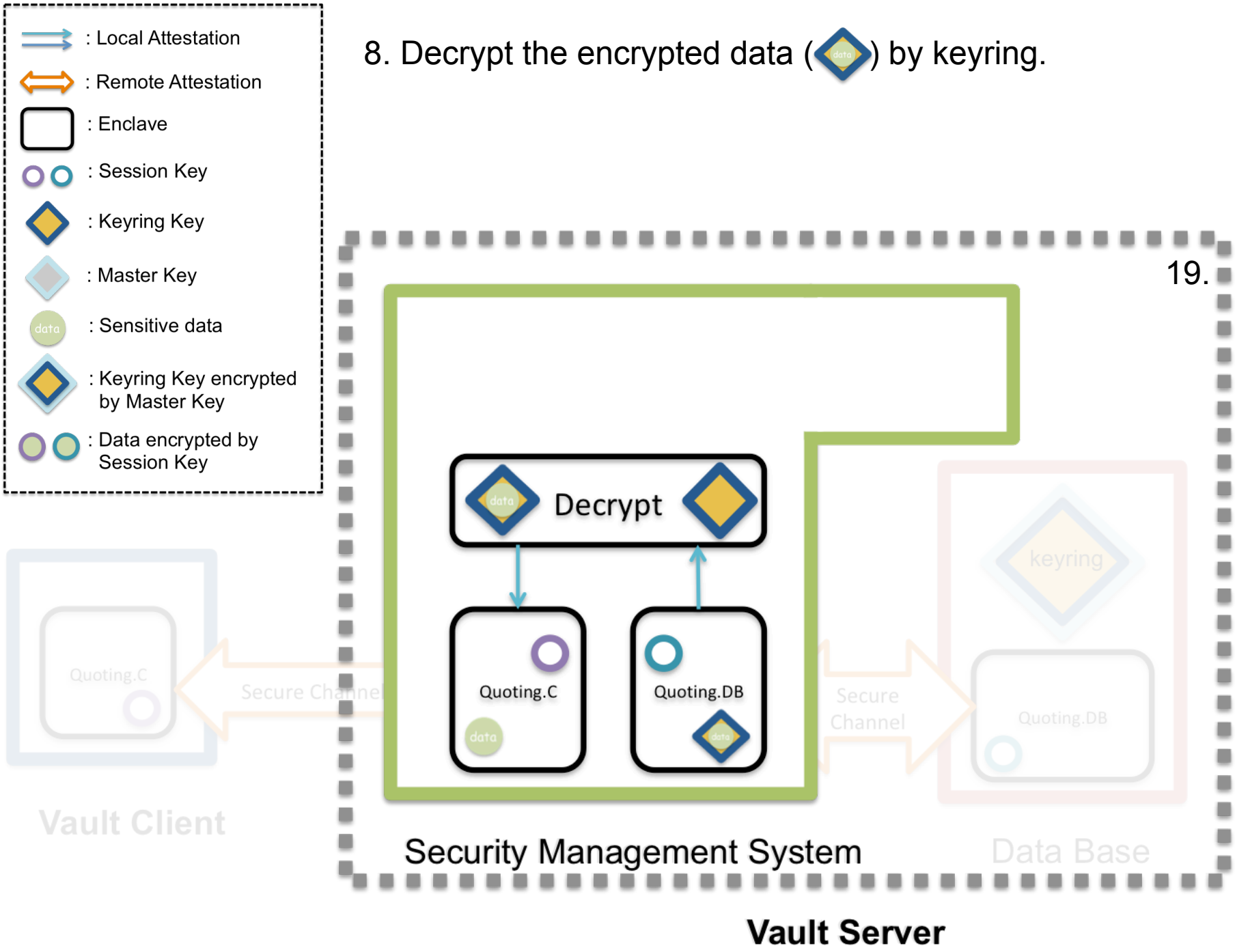

: Local Attestation
: Remote Attestation
: Enclave
: Session Key
: Keyring Key
: Master Key
: Sensitive data
: Keyring Key encrypted by Master Key
: Data encrypted by Session Key
15.The double encrypted data ( ) is decrypted by session key ( ) in Quoting.DB
15.
Encrypt
Decrypt
Quoting.C
Secure Channel
Quoting.C
Quoting.DB
Secure Channel
Quoting.DB
data
Vault Client
Security Management System
Data Base
Vault Server


: Local Attestation
: Remote Attestation
: Enclave
: Session Key
: Keyring Key
: Master Key
data
: Sensitive data
: Keyring Key encrypted by Master Key
: Data encrypted by Session Key
16. The encrypted data (data) is stored in the database
16.
Encrypt
Decrypt
Quoting.C
Secure Channel
Quoting.C
Quoting.DB
Secure Channel
data
Store Data
data
Quoting.DB
Vault Client
Security Management System
Data Base
Vault Server

17-20. Vice versa, when the user requests the data from the server, it does the decryption procedure to retrieve the data back.




: Local Attestation
: Remote Attestation
: Enclave
: Session Key
: Keyring Key
: Master Key
data
: Sensitive data
: Keyring Key encrypted by Master Key
: Data encrypted by Session Key
7. Retrieve the keyring back from database
18.
Decrypt
keyring
Quoting.DB
keyring
Secure Channel
keyring
Quoting.DB
keyring
Quoting.C
Secure Channel
Vault Client
Security Management System
Data Base
Vault Server


: Local Attestation
: Remote Attestation
: Enclave
: Session Key
: Keyring Key
: Master Key
: Sensitive data
: Keyring Key encrypted by Master Key
: Data encrypted by Session Key
8. Decrypt the encrypted data ( ) by keyring.
19.
Decrypt
Quoting.C
Quoting.DB
Secure Channel
Secure Channel
keyring
Quoting.DB
Quoting.C
Vault Client
Security Management System
Data Base
Vault Server

9. Send the raw data to the client via Secure Channel (remote attestation).