

A B S T R A C T

A server apparatus according to an embodiment generates a random number on receiving from a user apparatus a notification showing that a re-encryption key should be updated, and calculates re-encryption key data on the basis of the re-encryption key stored and the random number generated. The server apparatus transmits the re-encryption key to the user apparatus and receives, from the user apparatus, the user private key not updated yet and re-encryption key updating data calculated from the re-encryption key data on the basis of the user private key updated. The server apparatus calculates the re-encryption key updated, on the basis of the re-encryption key updating data and the random number, and replaces the re-encryption key stored in the storage device with the updated re-encryption key.