

MANAGING CRYPTOGRAPHIC KEYS BASED ON IDENTITY INFORMATION

ABSTRACT

Disclosed herein are methods, systems, and apparatus, including computer programs encoded on computer storage media, for managing cryptographic keys based on user identity information. One of the methods includes receiving biometric information associated with a user and a request to store a user key pair to a memory on an identity cryptographic chip (ICC); comparing the biometric information associated with the user with biometric information pre-stored in the memory as pre-stored biometric information; in response to determining that the biometric information associated with the user matches the pre-stored biometric information, encrypting the user key pair to provide an encrypted user key pair; and storing the encrypted user key pair to the memory.

FIG. 2