

KEY TRANSFER METHOD AND SYSTEM BASED ON SHARED SECURITY APPLICATION, STORAGE MEDIUM, AND DEVICE THEREOF

5

TECHNICAL FIELD

[0001] One or a plurality of embodiments of the present specification relate to the field of key communication of a mobile terminal, and in particular, to a key transfer method and system based on a shared security application, a storage
10 medium, and a device thereof.

BACKGROUND

[0002] As mobile intelligent terminals become more and more powerful and have increasingly improved processing performance, secure elements have
15 been more and more integrated in mobile intelligent terminals and applied to more and more service scenarios having high security requirements. In conventional mobile applications using a secure element for secure computing, for each mobile application, a corresponding independent security application needs to be installed in the secure element, and the independent security application is responsible for
20 accomplishing secure computing requirements of the mobile application.

[0003] For some mobile applications, especially for those having unified requirements for secure computing, for example, when corresponding service keys are mainly used to perform encryption and decryption operations or a signing operation, if the conventional approach of separately installing
25 corresponding secure applications is used, high development costs and promotion costs will be caused. A faster or more reliable solution needs to be provided to implement key transfer based on a shared security application.

application A and the management server of mobile application B; the management server of mobile application A generates an application key of mobile application A, the management server of mobile application B generates an application key of mobile application B, and the application keys include communication security protection keys and service keys; the management server of mobile application A and the management server of mobile application B respectively encrypt application keys to be written to the shared security application using a public key of the management server of the shared security application, and deliver the application keys to the corresponding mobile applications (for example, mobile application A and mobile application B) in the trusted execution environment of the mobile terminal; the mobile applications (for example, mobile application A and mobile application B) in the trusted execution environment store respective communication security protection keys; the mobile applications (for example, mobile application A and mobile application B) in the trusted execution environment invoke corresponding interfaces provided by a shared security application proxy in the rich execution environment to import respective application keys encrypted and protected using the management server of the shared security application; the shared security application proxy in the rich execution environment sends the imported encrypted application keys (for example, the application key of mobile application A and the application key of mobile application B) to the management server of the shared security application; the management server of the shared security application performs decryption using a private key thereof to obtain the application keys of the mobile applications (for example, the application key of mobile application A and the application key of mobile application B) to be written to the shared security application; the management server of the shared security application delivers the application keys of the mobile applications (for example, the application key of mobile application A and the application key of mobile application B) to the shared security application in the secure element of the mobile terminal; the shared security application securely stores the application keys of the mobile