ABSTRACT

METHOD OF SECURE COMMUNICATION AMONG PROTECTED CONTAINERS AND SYSTEM THEREOF

There is provided a method of communication among at least two processes running on the 5 same computer. The method comprises: generating, by at least one process of the at least two processes, a group key usable for encrypting/decrypting a data unit retrieved from/stored to shared access memory, where in the generating utilizes, at least, a nonce provided by each of the at least two processed, and wherein the nonces are provided as encrypted integrity-protected data according to, at least, a platform-provided hiding function, wherein each process executes in a protected container, the 10 processes are signed by a single signing authority, and the protected container infrastructure enables use of encrypted, integrity-protected data according to a platform-provided hiding function and a platform-provided revealing function; and verifying, by at least one process of the at least two processes, that a data unit read from shared access memory is successfully decrypted using the group key.

[Fig. 1]