

TITLE OF INVENTION: [A METHOD AND SYSTEM FOR MANAGING A GROUP-SHARED PRIVATE KEY FOR MULTI-PARTICIPANT]

ABSTRACT

The invention relates to a method and system for managing a Group-shared Private Key (GPK). The method involves transmitting a GPK generation request by an initiating Key Shard Holder (KSH) to a Communication Coordination Application (CCA), creating a key creation session by the CCA, accepting participating KSHs, and forwarding the GPK generation request to a Trusted Execution Environment (TEE). The TEE program generates a GPK and multiple GPK shards based on the GPK, encrypts the GPK shards with public keys, and transmits the encrypted GPK shards to the CCA. The CCA then creates a key distribution session to distribute the encrypted GPK shards to its corresponding KSH. The system comprises a plurality of KSHs, a CCA, a TEE, and a GPK generation application operating in the TEE.

Fig. 1a