

A KEY GENERATION AND DISTRIBUTION METHOD BASED ON IDENTITY-BASED CRYPTOGRAPHY

Abstract

This invention relates to a key generation and distribution method for an authentication framework for an operator provider network and a service provider network. The method comprises receiving a first request from a first requestor, the first requestor comprising an identity of the first requestor; generating a new identity (ID) based on the identity of the first requestor; generating a secret key based on an Identity Based Cryptography (IBC) key generation algorithm for the new ID with a predetermined pair of global keys, namely Global Secret Key (GSK), Global Public Key (GPK); transmitting the new ID, secret key and the GPK to the first requestor; receiving a request from a second requestor, the request comprising a plurality of identities; generating a new ID for each of the plurality of identities; generating a secret key based on the IBC key generation algorithm for each of the plurality of new IDs; and transmitting the plurality of new IDs, secret keys corresponding to each of the plurality of IDs and the GPK to the second requestor.

Figure 9 to accompany the abstract