162162

G00002

Abstract

For transmitting confidential data, two devices (D1, D2) are linked through a transmission channel which is secured by symmetric encryption with a shared secret session key. Both devices (D1, D2) possess the same secret session key (K) which is developed from two random keys (K1, K2) each of which is generated in a different one of the devices. Both random keys are exchanged between the devices (D1, D2) using asymmetric encryption.

Single Figure