

IMPLICIT CERTIFICATE VERIFICATION

Abstract

A method of computing a cryptographic key to be shared between a pair of correspondents communicating with one another through a cryptographic system is provided, where one of the correspondents receives a certificate of the other correspondents public key information to be combined with private key information of the one correspondent to generate the key. The method comprises the steps of computing the key by combining the public key information and the private key information and including in the computation a component corresponding to verification of the certificate, such that failure of the certificate to verify results in a key at the one correspondent that is different to the key computed at the other correspondent.

Figure 1