Abstract

In a server-client computer network system, for carrying out cryptographic operations via a network between a client computer workstation and a cryptography server computer system, in the client computer workstation and in the cryptography server computer system, computer software programs which are set up to communicate with each other are installed. These computer software programs are executed so that when the client computer workstation directs a request to carry out a cryptographic operation to the cryptography server computer system, the cryptography server computer system responds to it. For this purpose, the cryptography server computer system requests strong authentication from the requesting client computer workstation. As a reaction to this, the client computer workstation accesses a key of its user, under strong authentication. In the case of successful authentication, the client computer workstation receives a release to initiate just one or a few cryptographic operations using the private key. According to the invention, the private key is held on the cryptography server computer system, and the cryptographic operation(s) is/are permitted only within a defined, short period after successful authentication, to carry out the cryptographic operation(s) which application program software running on the client computer workstation has requested. The client computer workstation makes the result of the cryptographic operation(s) available to the application program software.

(Fig. 1)