

TRUSTED COMPUTING METHOD, AND SERVER

ABSTRACT

Disclosed in an embodiment of the present disclosure is a trusted computing method applicable in a server. The server is provided with a first and second trusted computing chips. The method comprises: during a startup process of the server, the first trusted computing chip performing a static measurement on the server to obtain a static measurement result, and sending the same to a verification center; and during operations of process after startup of the server, the second trusted computing chip performing a dynamic measurement on the server to obtain a dynamic measurement result, and sending the same along with association evidence to the verification center, wherein the association evidence indicates that the first trusted computing chip and the second trusted computing chip are provided within the same server, such that the verification center associates the two measurement results and then verifies the integrity of a software system of the server. In this way, the invention conducts both a static measurement and a dynamic measurement, and improves reliability of trusted computing, thereby achieving a technical effect of meeting requirements of high-security scenarios. Further disclosed is a server.

Figure 1