

the association evidence, and to verify integrity of a software system of the server based on associated results.

[00111] In an optional embodiment, the first trusted computing chip 201 is inserted into an SPI interface or an LPC interface on the server, and the second trusted computing chip 202 is inserted into a PCIE interface, a SATA interface, or a USB interface on the server.

[00112] In an optional embodiment, the first trusted computing chip 201 is further configured to:
[00113] perform an initialization, and receive a first device certificate issued by a CA.

[00114] In an optional embodiment, the first trusted computing chip 201 is further configured to:
[00115] further send the first device certificate to the verification center when sending the static measurement result to the verification center, for the verification center to verify the first device certificate.

[00116] In an optional embodiment, the second trusted computing chip 202 is further configured to:

[00117] perform an initialization, and receive a second device certificate issued by the CA.

[00118] In an optional embodiment, the second trusted computing chip 202 is further configured to:

[00119] further send the second device certificate to the verification center when sending the dynamic measurement result to the verification center, for the verification center to verify the second device certificate.

[00120] In an optional embodiment, the second trusted computing chip 202 is further configured to:

[00121] receive the association evidence signed by the CA before the first trusted computing chip 201 performs the static measurement on the server, where the association evidence is used for representing that the first trusted computing chip 201 and the second trusted computing chip 202 are disposed in the same server.

[00122] In an optional embodiment, the association evidence includes:

[00123] identification information of the first trusted computing chip 201;

[00124] identification information of the second trusted computing chip 202; and

[00125] a signature of the CA.

[00126] In an optional embodiment, the first trusted computing chip 201 is configured to: