CLAIMS

1. A method for verifying security of a smart card application, the method comprising:

receiving a prompt of a current service performed by the smart card application (Step 303);

obtaining related data of the current service (101);

determining the related data of the current service and a security parameter (102);

verifying if the related data of the current service complies with the security parameter to generate a verification result (103); and

sending a service instruction to the smart card application based on the verification result (Step 305).

2. The method according to claim 1, further comprising: enabling performance of the current service if the related data of the current service complies with the security parameter.

3. The method according to claim 1, further comprising: terminating the current service if the related data of the current service does not comply with the security parameter.

4. The method according to any one of claims 1 to 3, wherein the related data of the current service comprises at least one or a combination of a current location information, a current time information, or a transaction information.

5. The method according to claim 4, wherein the related data of the current service comprises the current location information and verifying if the related data of the current service complies to with the security parameter comprises comparing the current location information to a location range.

6. The method according to any one of claims 1 to 5, wherein obtaining related data of a current service when the smart card application performs service processing with the outside further comprises: when a smart card application built in an embedded security chip communicates with a near field communication (NFC) controller, monitoring communications between the two parties, and obtaining the related data of the current service.

7. The method according to any one of claims 1 to 6, wherein obtaining related data of a current service when the smart card application performs service processing with the outside further comprises: when a virtual smart card application communicates with an NFC controller, monitoring communications between the two parties in the virtual smart card application, and obtaining the related data of the current service.

8. The method according to any one of claims 1 to 7, wherein before determining the related data of the current service and a security parameter, the method further comprises: receiving and storing the security parameter entered by a user; or

receiving and storing a security parameter obtained by a server through analysis based on related data of a user.

9. The method according to any one of claims 1 to 8, wherein the security parameter is based on an analysis of historical behavior of a user.

10. The method according to claim9, wherein the security parameter is based on a statistical analysis of the historical behavior of the user relative to an area.

11. A device for verifying security of a smart card application, the device comprising a plurality of modules configured to perform the method of any one of claims 1 to 10.