CLAIMS

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

monitoring, by a security verification application of an intelligent terminal, communications between a smart card application and a near field communication controller of the intelligent terminal, wherein the security verification application is distinct from the smart card application and the near field communication controller, and wherein the smart card application is installed in an embedded security element of the intelligent terminal or in a host card emulation environment of the intelligent terminal;

obtaining, by the security verification application, from the monitored communications between the smart card application and the near field communication controller, related data of a current service (101);

determining, by the security verification application, whether the related data of the current service complies with a security parameter of a user (102); and

terminating the current service if the related data of the current service does not comply with the security perimeter (Step 306).

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 any one of claims 1 to 2, 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.

4. The method according to claim 3, wherein the related data of the current service comprises the current location information and determining whether the related data of the current service complies with the security perimeter comprises comparing the current location information to a location range.

5. The method according to claim 4, wherein the location range is derived from a statistical analysis of historical location data of the user.

6. The method according to any one of claims 1 to 5, wherein the method further comprises: receiving and storing the security parameter entered by the user; or receiving and storing a security parameter obtained by a server through analysis based on related data of the user.

7. The method according to any one of claims 1 to 6, wherein the security parameter is based on an analysis of historical data of the user, the historical data comprising payment transaction habits, daily payment transaction amounts, locations, times, and commodity categories of the user.

8. The method according to claim 7, wherein the security parameter is based on a statistical analysis of the historical data of the user relative to an area.

9. The method according to any one of claims 1 to 8, in which the security parameter comprises one or a combination of: location limitations, range limitations, time parameters, or a transaction amount threshold.

10. 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 9.