What is Claimed:

1. A smart card terminal infrastructure (300) for a smart card terminal (200), the terminal infrastructure (300) comprising:

a data and management framework (310), wherein the framework (310) comprises:

an interface component (410) for obtaining information related to a smart card application (230) on a smart card (220);

an error condition management component (420) for detecting an error of the smart card (220);

a usage management component (430) for enforcing a usage policy related to the smart card (220); and

a communication component (440) for communicating between the smart card (220) and the smart card terminal (200).

2.The smart card terminal infrastructure (300) of claim 1, wherein the data and management framework (310) is an application program interface (API).

3.The smart card terminal infrastructure (300) of claim 1, wherein the information related to the smart card application (230) on the smart card (220) is at least one of (i) an interface of the smart card application (230); (ii) a protocol used by the smart card application (230); and (iii) a security model of the smart card (220).

4. The smart card terminal infrastructure (300) of claim 1, further comprising:

a card module (340) for providing the information related to the smart card application (230) on the smart card (220) to the data and management framework (310).

5.The smart card terminal infrastructure (300) of claim 4, further comprising

a terminal application (305) corresponding to the smart card application (230) and created from the information related to the smart card application (230) on the smart card (220).

6.The smart card terminal infrastructure (300) of claim 1, wherein the error condition management component (420) further operates to relay an error message to the communication component (440) upon detection of the error.

7.The smart card terminal infrastructure (300) of claim 6, wherein the communication component (440) relays the error message of the smart card terminal (200) by at least one of (i) displaying the error message on a display device (191); (ii) creating a log

~~entry corresponding to the error message; and (iii) sending the error message to an application.~~

~~8.The smart card terminal infrastructure (300) of claim 1, wherein the usage management component (430) further operates to relay usage information to the communication component (440) upon detection of a violation of the usage policy related to the smart card (220).~~

~~9. The smart card terminal infrastructure (300) of claim 8, wherein the communication component (440) relays an indication of the violation of the usage policy related to the smart card (220) by at least one of (i) displaying the indication of the violation on a display device (191); (ii) creating a log entry corresponding to the violation; and (iii) sending the indication of the violation to an application.~~

~~10. The smart card terminal infrastructure (300) of claim 1, wherein the data and management framework (310) further comprises:~~

~~a connection component (450) for creating a channel between the smart card application (230) and a corresponding terminal application (305) if no error is detected or the usage policy is enforced.~~

~~11. The smart card terminal infrastructure (300) of claim 1, wherein the data and management framework (310) further comprises:~~

~~a terminal policy component (460) for incorporating terminal policies or restrictions related to the processing of the smart card application (230).~~

~~12.~~1. An interoperability method between a smart card terminal application ~~(305)~~ and a smart card application ~~(230)~~ on a smart card ~~(220)~~, the method comprising:

obtaining an application program interface ~~(API)~~ written to a framework of a smart card terminal ~~(505)~~;

obtaining by one or more computer processors information related to the smart card application from the application program interface ~~API (510)~~; ~~and~~

providing by the one or more computer processors the information obtained from the application program interface for developing the smart card terminal application in accordance with the smart card application; and

using the one or more computer processors to generate the smart card terminal application by incorporating the information obtained from the application program

interface ~~related to the smart card application~~ into the smart card terminal application ~~(515)~~.

~~13.~~2. The interoperability method of claim 1~~12~~, wherein obtaining information related to the smart card application from the application program interface~~API (510)~~ comprises obtaining at least one of (i) an interface of the smart card application; (ii) a protocol used by the smart card application; and (iii) a security model of the smart card.

~~14.~~3. The interoperability method of claim 1~~12~~, wherein the framework comprises a usage management component for ~~further comprising:~~enforcing a ~~the~~ security model of the smart card at the smart card terminal ~~(520)~~.

4. The interoperability method of claim 1, wherein the framework comprises an error condition management component for detecting an error of the smart card.

~~15.The interoperability method of claim 14 , wherein enforcing the security model of the smart card (520) comprises:~~

~~monitoring usage of the smart card (525); and~~

~~upon a determination that the monitored usage violates the security model (530), indicating a violation message (535).~~

~~16.~~5. The interoperability method of claim 1~~12~~, wherein the framework comprises a usage management component for ~~further comprising:~~creating a secure communication channel between the smart card and the smart card terminal ~~(540)~~.

~~17.~~6. The interoperability method of claim 1~~12~~, further comprising

configuring the smart card terminal application to further define a terminal policy or a restriction ~~(545)~~.

~~18.~~7. A method of enforcing a security model of a smart card on a smart card terminal, the method comprising:

obtaining by one or more computer processors the security model of the smart card from a data and management framework of the smart card terminal ~~(610)~~; ~~and~~

providing by the one or more computer processors ~~incorporating~~ the security model obtained from the data and management framework for developing ~~into~~ a smart card terminal application in accordance with ~~corresponding to~~ the smart card; and~~(615).~~

using the one or more computer processors to generate the smart card terminal application by incorporating the security model obtained from the data and management framework into the smart card terminal application.

~~19.~~8. The method of claim 7~~18~~, wherein obtaining the security model of the smart card from a data and management framework of the smart card terminal comprises reading an application program interface ~~(API)~~ applied to the data and management framework.

~~20.~~9. The method of claim 7~~18~~, wherein the framework ~~further~~ comprising an error condition management component for:

detecting an error condition defined by the security model ~~(620)~~; and

transmitting an error message corresponding to the error condition upon detection of the error condition ~~(625)~~.

10. A smart card terminal infrastructure for a smart card terminal, the smart card terminal infrastructure comprising:

a data and management framework;

an interface component within the data and management framework for obtaining information related to a smart card application on a smart card, wherein the information allows for developing a terminal application in accordance with the smart card application, the interface component incorporating the obtained information into the terminal application; and

a communication component within the data and management framework in operative communication with the smart card and the smart card terminal.

11. The smart card terminal infrastructure of claim 10, wherein the information related to the smart card application on the smart card is at least one of (i) an interface of the smart card application; (ii) a protocol used by the smart card application; and (iii) a security model of the smart card.

12. The smart card terminal infrastructure of claim 11, wherein the error condition management component further operates to relay an error message to the communication component upon detection of the error.

13. The smart card terminal infrastructure of claim 12, wherein the communication component relays the error message of the smart card terminal by at least one of (i) displaying the error message on a display device; (ii) creating a log entry

corresponding to the error message; and (iii) sending the error message to an application.

14. The smart card terminal infrastructure of claim 10, further comprising:

an error condition management component for detecting an error of the smart card.

15. An interoperability method between a smart card terminal and a smart card application on a smart card, the method comprising:

exposing a data and management framework at a smart card terminal;

receiving, at the data and management framework, an application program interface corresponding to the smart card application;

obtaining by one or more computer processors information related to the smart card application from the application program interface;

providing by the one or more computer processors information obtained from the application program interface for developing a terminal application accordance with the smart card application; and

generating the terminal application by incorporating the obtained information into the terminal application.

16. The interoperability method of claim 15, further comprising:

receiving a communication from the terminal application to the smart card application, wherein said smart card terminal application is developed based on the information obtained from the application program interface;

relaying the communication to the smart card application via a uniform interface to the smart card.

17. The interoperability method of claim 15, wherein obtaining information related to the smart card application from the application program interface comprises obtaining at least one of (i) an interface of the smart card application; (ii) a protocol used by the smart card application; and (iii) a security model of the smart card.

18. A method of enforcing a security model of a smart card on a smart card terminal, the method comprising:

exposing a data and management framework at a smart card terminal;

receiving, at the data and management framework, an application program interface corresponding to the smart card application;

obtaining by one or more computer processors information related to the smart card application from the application program interface, said information comprises the security model of the smart card application;

providing by the one or more computer processors said security model for developing a terminal application in accordance with the smart card application; and

generating the terminal application by incorporating the obtained information into the terminal application.

19. The method of claim 18, further comprising:

detecting an error condition defined by the security model; and

transmitting an error message corresponding to the error condition upon detection of the error condition.

20. The method of claim 18, wherein obtaining the security model of the smart card from the data and management framework of the smart card terminal comprises reading an application program interface applied to the data and management framework.