

WHAT IS CLAIMED IS CLAIMS:

~~1.—A method, comprising:~~

~~storing on a smartcard an applet configured to generate a digital tag;~~

~~receiving a request at the smartcard for requested information after entry into a communication field generated by a smartphone;~~

~~configuring the digital tag to be associated with at least one of (i) an application or (ii) an input on the smartphone, such that receipt of the digital tag by the smartphone causes the application to launch on the smartphone upon a successful completion of a security review; and~~

~~emitting from the smartcard the digital tag, wherein the digital tag is configured to restrict the requested information to be accessible only by the application to prevent unauthorized access to the requested information;~~

~~prompting, by the digital tag, the security review of the application prior to the launch;~~

~~and~~

~~precluding the launch of the application upon an unsuccessful completion of the security review.~~

~~2.—The method of claim 1, wherein the application is configured to prevent other applications on the smartphone from accessing the requested information.~~

~~3.—The method of claim 1, wherein the smartcard is a contactless credit card.~~

~~4.—The method of claim 1, wherein the smartcard emits a Near-Field-Communication field.~~

~~5.—The method of claim 1, wherein the smartphone contains an Android-based operating system.~~

~~6.—The method of claim 5, wherein the applet is configured to generate at least one digital tag in accordance with the NFC Data Exchange Format (NDEF) specification.~~

~~7. The method of claim 6, further wherein the at least one digital tag in accordance with the NDEF specification is further configured to be an Android Application Record (AAR) launch tag.~~

~~8. A system, comprising:~~

~~a contactless smartcard; and~~

~~a user device application configured to:~~

~~automatically request from the contactless smartcard requested information after entry by the contactless smartcard into a communication field generated by a user device;~~

~~receive from the contactless smartcard a digital tag, wherein:~~

~~the digital tag is configured to launch an application associated with the digital tag upon successful completion of a security review; and~~

~~the digital tag is configured to restrict the requested information to be accessible only by the application to prevent unauthorized access to the requested information; perform the security review of the application prior to the launch of the application associated with the digital tag; and~~

~~preclude the application associated with the digital tag from launching upon an unsuccessful completion of the security review. —~~

~~9. The system of claim 8, wherein the digital tag is configured to launch the application associated with the digital tag when the user device is inactive.~~

~~10. The system of claim 8, wherein the digital tag is configured to launch the application associated with the digital tag when the display of the user device is inactive.~~

~~11. The system of claim 10, wherein the application associated with the digital tag is further configured to launch when the user device has not received user input for a pre-determined period of time.~~

~~12. The system of claim 10, wherein the user device is configured to contain an Android-based operation system.~~

~~13. The system of claim 11, wherein the user device is configured to launch, responsive to an NFC Data Exchange Format (NDEF) tag or an Android Application Record (AAR) launch tag, the application associated with the digital tag.~~

~~14. The system of claim 13, wherein the user device is further configured to launch an application manager responsive to the NDEF tag when the application associated with the digital tag is not present on the system.~~

~~15. The system of claim 14, wherein the application manager is the Google Play Store.~~

~~16. The system of claim 14, wherein the user device is further configured to download and install the application associated with the digital tag from the Google Play Store.~~

~~17. A contactless card comprising a processor, a communication interface, and a non-transitory computer-accessible medium having stored thereon computer-executable instructions, wherein when the instructions are executed by the processor the contactless card is configured to perform procedures comprising:~~

~~receiving a request for information via the communication interface after entry into a Near Field Communication (NFC) communication field generated by a smartphone; and~~

~~emitting an NFC Data Exchange Format (NDEF) tag, wherein:~~

~~the NDEF tag is configured to be an Android Application Record (AAR) tag,~~

~~the NDEF tag is associated with an applet stored on the contactless card, the~~

~~NDEF tag is configured to be associated with an application on the smartphone,~~

~~the NDEF tag is configured to launch the application associated with the NDEF tag upon receipt by the smartphone and successful completion of a security review.~~

~~18. The method of claim 1, wherein the unsuccessful completion of the security review comprises a detection of a software virus.~~

~~19. The system of claim 8, wherein the unsuccessful completion of the security review comprises a detection of functionality that exceeds a security rule.~~

~~20. The contactless card of claim 17, wherein the successful completion of the security review comprises the absence of a detection of a software virus and the absence of a detection of functionality that exceeds a security rule.~~

1. A contactless card, comprising:

a processor;

a memory storing a Near Field Communication (NFC) Data Exchange Format (NDEF) tag;

and

a communication interface,

wherein, upon receipt of a request for information, the contactless card is configured to transmit the NDEF tag to a user device, and

wherein the NDEF tag is configured to:

prompt a launch of an application on the user device, and

restrict access to the requested information to only the application.

2. The contactless card of claim 1, wherein the NDEF tag is further configured to prompt the launch of the application when the user device is inactive.

3. The contactless card of claim 1, wherein the NDEF tag is further configured to prompt the launch of the application when no other application on the user device is active.

4. The contactless card of claim 1, wherein the NDEF tag is further configured to preclude a second application from opening or becoming active.

5. The contactless card of claim 1, wherein:

the NDEF tag is configured to prompt the launch of a plurality of additional applications,
and

the NDEF tag includes an associational parameter identifying a sequence for launching the plurality of additional applications.

6. The contactless card of claim 5, wherein the sequence comprises completion-triggered launching.

7. The contactless card of claim 5, wherein the NDEF tag includes a temporal parameter selected from the group of a designated time to launch the application, a time interval between launching the application and one of the plurality of additional applications and a time delay precluding the launch of one of the plurality of additional applications following the launch of the application.

8. The contactless card of claim 5, wherein the NDEF tag is configured to launch the application after the user device has gone without receiving user input for a specified period of time.

9. The contactless card of claim 5, wherein the NDEF tag is configured to launch the application after the user device has received a specified input.

10. A method for application control performed by a contactless card comprising a processor, a memory storing a Near Field Communication (NFC) Data Exchange Format (NDEF) tag, and a communication interface, the method comprising:

transmitting, to a user device, the NDEF tag, wherein the NDEF tag is configured to:
prompt a launch of an application on the user device, and
restrict access to the requested information to only the application.

11. The method of claim 10, wherein the NDEF tag includes an interference parameter specifying an effect comprising pausing the execution of a second application once the application has launched for at least one selected from the group of a predetermined time period and until a certain action is performed by the application.

12. The method of claim 11, wherein the NDEF tag includes an interference parameter specifying an effect comprising pausing the execution of a second application once the application has launched for at least one selected from the group of until the application signals other applications can resume and until the application closes.

13. The method of claim 11, wherein the NDEF tag includes an interference parameter configured to close a second application.

14. An application control system, comprising:
a contactless card comprising a processor, a memory storing a Near Field Communication (NFC) Data Exchange Format (NDEF) tag, and a communication interface,
wherein, upon receipt of a request for information, the contactless card is configured to transmit the NDEF tag to a user device, and
wherein the NDEF tag is configured to:
prompt a launch of an application on the user device, and
restrict access to the requested information to only the application.
15. The application control system of claim 14, wherein:
the system further comprises a server, and
the NDEF tag is further configured to prompt a security review performed by the server.
16. The application control system of claim 15, wherein the security review is performed on all applications associated with the NDEF tag.
17. The application control system of claim 15, wherein the security review comprises at least one selected from the group of scanning for malicious element and scanning for functionality that exceeds a rule.
18. The application control system of claim 15, wherein, upon a successful completion of the security review, the application is launched.

19. The application control system of claim 15, wherein, upon an unsuccessful completion of the security review, the application is precluded from launching.

20. The application control system of claim 15, wherein, upon an unsuccessful completion of the security review, the application held in abeyance until a security issue is resolved.