

CLAIMS:

1. A method for managing an installation of an Android application package (APK) in a device, the method comprises:
 - receiving, by the device, an installation request for the APK;
 - retrieving, by the device, a permission certificate for the APK when the installation request contains a request for a high-risk permission, wherein the permission certificate for the APK includes a cryptographic signature
 - determining, by the device, a validity of the permission certificate by verifying the cryptographic signature included in the permission certificate using a permission certification public key of the manufacturer of the device, wherein the permission certification public key is stored in the device; and
 - allowing the installation of the APK in the device when the permission certificate is determined to be valid.
2. The method according to claim 1, wherein preceding the step of allowing the installation of the APK in the device if the permission certificate is determined to be valid, the method further comprises the step of:
 - determining whether the high-risk permission request contained in the installation request corresponds to a permission granted in the permission certificate for the APK;
 - and
 - validating the permission certificate when it is determined that the high-risk permission request contained in the installation request corresponds to the permission granted in the permission certificate.
3. The method according to any one of claims 1 or 2, wherein the verifying the cryptographic signature included in the permission certificate comprises:
 - computing a cryptographic hash of the APK using a cryptographic hash function; and
 - comparing the computed cryptographic hash of the APK with a cryptographic hash of the APK stored in the permission certificate.
4. The method according to any one of claims 1 to 3, wherein the cryptographic signature included in the permission certificate is generated at a server associated with the manufacturer of the device, the server being configured to generate the cryptographic signature by:

cryptographically signing a request for the permission certificate for the APK using a permission certification private key of the manufacturer of the device as stored in the server, wherein the request for the permission certificate for the APK comprises a development public key of the APK, a name of the APK, a high-risk permission granted to the APK and a validity period of the permission certificate.

5. The method according to claim 4 wherein the permission certificate for the APK comprises the development public key of the APK, the name of the APK; the high-risk permission granted to the APK, the validity period of the permission certificate and the cryptographic signature.
6. The method according to any one of claims 4 or 5,
 - wherein the permission certificate for the APK is cryptographically signed after the server receives a pre-release APK that contains a development permission certificate that has been cryptographically signed using the permission certification private key of the manufacturer of the device, and
 - wherein the development permission certificate allows the pre-release APK to be installed in a predetermined development device.
7. The method according to any one of claims 1 to 6, wherein the retrieving the permission certificate for the APK comprises de-embedding the permission certificate from the APK.
8. The method according to any one of claims 1 to 6, wherein the retrieving the permission certificate for the APK comprises downloading the permission certificate from a remote server to the device.
9. A system for managing an installation of an Android application package (APK) in a device, the system comprising:
 - a processing unit; and
 - a non-transitory media readable by the processing unit, the media storing instructions that when executed by the processing unit cause the processing unit to:
 - receive an installation request for the APK;
 - retrieve a permission certificate for the APK when the installation request contains a request for a high-risk permission, wherein the permission certificate for the APK includes a cryptographic signature;

determine a validity of the permission certificate by verifying the cryptographic signature included in the permission certificate using a permission certification public key of the manufacturer of the device, wherein the permission certification public key is stored in the device; and

allow the installation of the APK in the device if the permission certificate is determined to be valid.

10. The system according to claim 9, wherein preceding the instructions to allow the installation of the APK in the device if the permission certificate is determined to be valid, the instructions further comprises:

instructions for directing the processing unit to:

determine if the high-risk permission request of the APK corresponds to a permission granted in the permission certificate for the APK; and

validate the permission certificate if the high-risk permission request of the APK corresponds to the permission granted in the permission certificate.

11. The system according to any one of claims 9 or 10, wherein the instructions to verify the cryptographic signature included in the permission certificate comprises:

instructions for directing the processing unit to:

compute a cryptographic hash of the APK using a cryptographic hash function; and

compare the computed cryptographic hash of the APK with a cryptographic hash of the APK stored in the permission certificate.

12. The system according to any one of claims 9 to 11, wherein the cryptographic signature included in the permission certificate is generated at a server associated with the manufacturer of the device the server being configured to generate the cryptographic signature by:

cryptographically signing a request for the permission certificate for the APK using a permission certification private key of the manufacturer of the device as stored in the server, wherein the request for the permission certificate for the APK comprises a development public key of the APK, a name of the APK, a high-risk permission granted to the APK and a validity period of the permission certificate.

13. The system according to claim 12 wherein the permission certificate for the APK comprises the development public key of the APK, the name of the APK; the high-risk

permission granted to the APK, the validity period of the permission certificate and the cryptographic signature.

14. The system according to any one of claims 12 or 13, wherein the permission certificate for the APK is cryptographically signed after the server receives a pre-release APK that contains a development permission certificate that has been cryptographically signed using the permission certification private key of the manufacturer of the device, and wherein the development permission certificate allows the pre-release APK to be installed in a predetermined development device.
15. The system according to any one of claims 9 to 14, wherein the instructions to retrieve the permission certificate for the APK comprises instructions to de-embed the permission certificate from the APK.
16. The system according to any one of claims 9 to 14, wherein the instructions to retrieve the permission certificate for the APK comprises instructions to download the permission certificate from a remote server to the device.