CLAIMS:

1. A secure module for attesting an authenticity of an application that is provided within a standard operating system of a computing device, the module comprising:

an identification module communicatively connected to the application, the identification module being configured to:

establish a first cryptographic bond between the application and the secure module when communication is established between the application and the secure module, whereby the first cryptographic bond is generated based on information associated with the application as preloaded in the secure module and on information obtained from the application;

authenticate an integrity of the application based on the first cryptographic bond; and

process an action for the authenticated application when the integrity of the application has been authenticated,

wherein the secure module further comprises:

a non-transitory media readable by a processing unit to store instructions for directing the processing unit to:

provide a cryptographic sandbox that includes a virtual cryptographic machine that performs cryptographic operations including decrypting virtual machine codes, and a tamper-proof virtual layer within the cryptographic sandbox to protect cryptographic operations from unauthorized observers.

2. The module according to claim 1, wherein the identification module is further configured to dynamically re-authenticate the integrity of the authenticated application based on a second cryptographic bond, wherein the second cryptographic bond is generated based on the information associated with the application as preloaded in the secure module and on information newly obtained from the application, and process further actions for the application when the integrity of the application has been re-authenticated.

3. The module according to claim 1 or 2, wherein the establishing of the first cryptographic bond between the application and the secure module by the identification module comprises:

the identification module being configured to:

receive an app-checksum from the application, wherein the app-checksum is derived from the application based on the application's source code, the application's binary and/or the application's programming flow;

retrieve a trusted-checksum associated with the application from a trusted-storage module provided in the secure module; and

generate the first cryptographic bond based on the app-checksum received from the application and the retrieved trusted-checksum.

4. The module according to claim 4, wherein the generation of the app-checksum by the application comprises the application being configured to utilize a SHA-256 hash function to hash the source code of the application to generate the app-checksum.

5. The module according to claim 1 or 2, wherein the establishing of the first cryptographic bond between the application and the secure module by the identification module comprises:

the identification module being configured to:

receive from the application a digital signature associated with the application, wherein the digital signature is generated when the application's source code is signed using a private key unique to the application each time the application's source code is compiled;

retrieve a trusted-public key associated with the application from a trusted-storage module provided in the secure module; and

generate the first cryptographic bond based on the digital signature received from the application and the retrieved trusted-public key associated with the application.

6. The module according to claim 5, wherein the identification module is further configured to:

receive an app-checksum from the application, wherein the app-checksum is derived from the application based on the application's source code;

retrieve a trusted-checksum associated with the application from a trusted-storage module provided in the secure module; and

re-generate the first cryptographic bond based on the app-checksum received from the application, the retrieved trusted-checksum, the received digital signature and the retrieved trusted-public key.

7. The module according to any one of claims 3 to 5, wherein the authentication of the integrity of the application based on the first cryptographic bond by the identification node

comprises the identification node being configured to authenticate the integrity of the application when it is determined from the cryptographic bond that information obtained from the application matches with the information associated with the application as preloaded in the secure module.

8. The module according to claim 5, wherein the processing of the action for the authenticated application by the identification module comprises:

the identification module being configured to:

sign, using a cryptographic key-signing algorithm, the action using a private key unique to the application; and

communicate the signed action and a retrieved certificate chain to another application, whereby upon receiving the signed action and the certificate chain, the another application is configured to verify the signed action based on the received certificate chain.

9. The module according to claim 5, wherein the action comprises a request signed by another application and a certificate chain, whereby the processing of the action for the authenticated application by the identification module comprises:

the identification module being configured to:

verify the signed request based on the certificate chain;

execute instructions contained within the request when it is determined that the signed request has been verified;

construct a response based on an outcome of the executed instructions;

sign the response using a private key unique to the application;

encrypt the signed response and communicate the encrypted signed response to the another application.

10. The module according to claim 1, wherein the processing of the action for the authenticated application by the identification module comprises:

the identification module being configured to:

retrieve a trust attribute from a trusted-storage module provided within the secure module based on requirements of the action, and where the trust attribute is signed by a trusted third party that has certified that the application is qualified to be given the attribute;

generate a response based on the retrieved trust attribute; and

send the generated response to another application, wherein upon receiving the generated response, the another application is configured to use the trust attribute contained within the response to perform a secure transaction.

11. A system for establishing, using the secure module according to claim 1 or 2, mutual trust between a first computing-application and a second computing-application that are provided within a standard operating system of a user's computing device, wherein the application comprises the first computing-application, and whereby the secure module is communicatively connected to the first computing-application, the system comprising:

the second computing-application being configured to send an authentication request to the first computing-application;

the first computing-application being configured to:

authenticate, using the secure module, the first computing-application when the authentication request from the second computing-application is received by the first computing-application;

generate a verification response when the first computing-application has been authenticated by the secure module; and

send the verification response to the second computing-application, wherein the second computing-application is configured to use the verification response to establish the mutual trust between the first and second computing-applications.

12. The system according to claim 11 wherein, the second computing-application is configured to:

share secure data with the first computing-application when the second computing-application determines from the received verification response that the first computing-application has been authenticated.

13. A system for establishing, using the secure module according to claim 1 or 2, mutual trust between a third computing-application and a trust element bound to a user's computing device, the third computing-application being provided within a standard operating system of the user's computing device, wherein the application comprises the third computing-application, and whereby the secure module is communicatively connected to the third computing-application, the system comprising:

the trust element being configured to send an authentication request to the third computing-application;

the third computing-application being configured to:

authenticate, using the secure module, the third computing-application when the authentication request from the trust element is received by the third computing-application;

generate a verification response when the third computing-application has been authenticated by the secure module; and

send the verification response to the trust element, wherein the trust element is configured to use the verification response to establish the mutual trust between the third computing-application and the trust element.

14. A system for establishing, using the secure module according to claim 1 or 2, mutual trust between a fourth computing-application and a fifth computing-application, the fourth computing-application being provided within a standard operating system of the user's computing device, wherein the application comprises the fourth computing-application, and whereby the secure module is communicatively connected to the fourth computing-application, the system comprising:

the fifth computing-application being configured to send an authentication request to the fourth computing-application;

the fourth computing-application being configured to:

authenticate, using the secure module, the fourth computing-application when the authentication request from the fifth computing-application is received by the fourth computing-application;

generate a verification response when the fourth computing-application has been authenticated by the secure module; and

send the verification response to the fifth computing-application, wherein the fifth computing-application is configured to use the verification response to establish the mutual trust between the fourth computing-application and the fifth computing-application.

15. A method for attesting an authenticity of an application provided within a standard operating system of a computing device, the method comprising the steps of:

establishing, using a secure module, a first cryptographic bond between the application and the secure module when communication is established between the application and the secure module, whereby the first cryptographic bond is generated based on information associated with the application as preloaded in the secure module and on information obtained from the application;

authenticating, using the secure module, an integrity of the application based on the first cryptographic bond; and

processing, using the secure module, an action for the authenticated application when the integrity of the application has been authenticated,

wherein the secure module further comprises:

a non-transitory media readable by a processing unit to store instructions for directing the processing unit to:

provide a cryptographic sandbox that includes a virtual cryptographic machine that performs cryptographic operations including decrypting virtual machine codes, and a tamper-proof virtual layer within the cryptographic sandbox to protect cryptographic operations from unauthorized observers.

16. The method according to claim 16, wherein the method further comprises the step of: dynamically re-authenticating, using the secure module, the integrity of the authenticated application based on a second cryptographic bond, wherein the second cryptographic bond is generated based on the information associated with the application as preloaded in the secure module and on information newly obtained from the application, and process further actions for the application when the integrity of the application has been re-authenticated.

17. The method according to claim 15 or 16, wherein the step of establishing the first cryptographic bond between the application and the secure module comprises the steps of:

receiving, using the secure module, an app-checksum from the application, wherein the app-checksum is derived from the application based on the application's source code, the application's binary and/or the application's programming flow;

retrieving, using the secure module, a trusted-checksum associated with the application from a trusted-storage module provided in the secure module; and

generating, using the secure module, the first cryptographic bond based on the app-checksum received from the application and the retrieved trusted-checksum.

18. The method according to claim 17, wherein the generation of the app-checksum by the application comprises the application being configured to utilize a SHA-256 hash function to hash the source code of the application to generate the app-checksum.