LEONARDO

PATENT BROCHURE

MULTI-LEVEL TOKEN POLYMORPHIC SW LICENSE (MUTOPS-L)

Main Technological Area ⟶ Data Processing

Keywords⟶ token | cryptography |memory | random generation | polimorphic engine

System and method for protecting information data and, in particular, for checking and granting authorization to access information data.

TECHNICAL SPECIFICATIONS

A HW device, in addition to SW components, which:

- Authorize access in versatile and modular way to protected information
- Allow the execution of computer programs (software) subject to obtaining a license to use them

The HW can be any PKCS11-compliant token (as for example of Figure 1), including a microprocessor and capable of data storage using two different memory segments: one having free access, another one protected using an access control system. Inside this area lies the proprietary algorithm that will generate the authentication code.
The software to be protected requires the user to enter the token and a PIN and, if the PIN is correct, the communication with the token is opened.

Figure 1 - Example of USB token

Usually, these kind of tokens are tamper proof; information saved therein becomes destroyed if somebody attempts to physically extract it.
The SW includes two components:

- An "Initializer" to initialize the SW license at first access
- An "Enforcer" to be included in the SW to protect (in the form of a DLL), which manage the usage limitations.

The innovative method mainly comprises three phases:

- Initialization phase - during this phase a "seal" is generated that includes data that constitute the text to be deciphered.
- Encryption phase - during this phase, known encryption techniques are used for encrypt the seal generated in the initialization phase.
- Decryption phase - during this phase the seal that allows authorization and execution of a specific program is decrypted.

The data set that constitute the "seal", is a combination of data including content which does not vary with time (e.g. SW identifier, manufacturer, license number, initialization date, and other optional fixed data) with a variable data set which are dependent on usage conditions.

A Polymorphic Engine assure that the above data set (payload) is encrypted and stored in different memory areas each time, adequately filling the remaining memory gaps with randomly generated data; the memory storage schema is also encrypted and the combination of payload key with the encrypted storage schema is stored in the memory area protected with access control.

The operating phase of SW protection is started when the user starts the application; the included enforcer access the private area, and if successful, perform the decryption of information stored in it subsequently accessing the payload. After the verification of information stored in the payload (and therefore the license information), the encryption

phase is reactivated at every defined interval of time or based on user action and a new seal is created and stored in background while the application is active.

With the metodology described in this patent, the following protection levels are assured:

a) Phyisical protection, since physical access to the token is mandatory; if the token is missing or is removed the access to the SW to protect is forbidden.
b) The “seal" is not directly accessible by the user
c) Cryptographic mechanisms are stored and executed in the token, and cannot be tampered.
d) Even if a malicious user can access the private area, every time is needed he has to know the key to decrypt the seal, correlate the stored information and to replicate somehow the Polymorphic Engine to continue to use the protected SW.

INNOVATION/ADVANTAGES

The solution and the novelty claimed in the patent allow:

- A customized SW license control; licenses can be customized on the customer basis and limitations can be added or removed for each single component of an application using the token.
- Extensibility to other contexts; the system is able to implement protection mechanisms for every kind of data, not only SW.
- A convenient alternative to authentication mechanisms requiring access to a server and information exchange on a network (e.g. two factor authentication).

FIELDS OF APPLICATION

Information Technology	SW license management, data access protection, authentication mechanisms in restricted network areas

PATENT INFORMATION

Priority Date – 28/05/2012
Priority Code – IT TO2012A000462
IPC Codes - H04L9/08 - H04L9/32 - G06F21/10 - G06F21/62 - G09C1/00

Active worldwide applications

EPO – EP2670080B1; filing date 28/05/2013; grant date 31/01/2018
National Extensions: Italy - Germany – France – United Kingdom – Spain

USA - US9246684; filing date 24/05/2013; grant date 26/01/2016
Japan - JP06184751; filing date 28/05/2013; grant date 4/08/2017
China - CN103559454; filing date 28/05/2013; grant date 17/04/2018

Leonardo internal code

LDO-0490