Use of Hardware Algorithms

Symmetric Data Conversion: GrdCryptEx function

GrdCrypt function can use GSII64 and AES algorithms. Conversion using this function features the following:

- Reversibility
- Tamperproofness against cryptanalysis
- Dongle-based conversion

Such conversion is used for encrypting and decrypting data used by the application inside the dongle. The volume of converted data should be relatively small.

Unidirectional Data Conversion: GrdHashEx function

Normally, the conversion using **GrdHash** operation is implemented for the legitimacy analysis of an application. The main purpose of this method is to complicate the logic of the dongle operation and therefore prevent its emulation. This conversion can be used for integrity and validity verification of data.

The main features of conversion are as follows:

- Unidirectionality, i.e. for function F(X) there is no function F1(), so that X=F1(F(X)).
- Tamperproofness against cryptanalysis
- Conversion done by the dongle

Based on these features, we can outline the tasks that we are able to resolve using such conversion. It can be used in the following cases:

- If the volume of information being converted is relatively small (tens or hundreds of bytes)
- For encrypting data that does not require decrypting back to the original form. For example, in a simple case an application can convert some random sequence of data, calculate hash function of the output sequence and compare it with the pre-calculated hash value received on the stage of installing the protection. If the two values match, the copy of the protected application is recognized legitimate
- In combination with software-based symmetric algorithms. For example, for generating of AES algorithm key.

You should not use this method to encrypt data used by the application, since the conversion is unidirectional.

Loadable code execution: GrdCodeRun function (Guardant Code/Code Time only)

The loadable code calls are performed using the **GrdCodeRun()** function. If the loadable code is developed in accordance with the recommendations and meets the requirements listed in the beginning of the chapter, it implements the algorithm the results of execution of which may be used in the application directly.

Thus, the missing dongle rids the application of its functionality without which the operation becomes impossible.