

Typical Protection Strategy for Business Layer API's

Program Start

1. If your protected application is running in Network Mode, do a **SFNTSetContactServer** with a setting of the Sentinel Keys Server Computer_Name or IP_Address.
2. Do a **SFNTGetLicense** to obtaining the License from the key.
3. If your application is running in Network Mode, do a **SFNTSetHeartbeat** with a setting of 10 minutes (600 seconds) or so.
4. Verify that the key is correct by running the following API's:
SFNTQueryFeature
SFNTEncrypt and then **SFNTDecrypt**
SFNTSign and then **SFNTVerify**
5. Do a **SFNTGetFeatureInfo** to determine if the license is a Trial License.
If "bEnableCounter" is set to 1, then execution counter is used.
 Display "featureInfo.leftExecutionNumber" the number of application execution remaining.
If "bEnableStopTime" is set to 1, then expiration date is used.
 Display the Trial License expiration date and time:
 Date is featureInfo.timeControl.stopTime.month
 Month is featureInfo.timeControl.stopTime.dayOfMonth
 Year is featureInfo.timeControl.stopTime.year
 Hour is featureInfo.timeControl.stopTime.hour
 Minutes is featureInfo.timeControl.stopTime.minute
 Seconds is featureInfo.timeControl.stopTime.second
6. Read in application option(s) configuration data stored in the key.
 Do a **SFNTReadInteger** to read the value of an Integer or Boolean stored in the key
 Do a **SFNTReadString** to read the value of a string stored in the key
 Do a **SFNTReadRawData** to read the value of a Raw Data string stored in the key
7. Every 3 to 9 minutes do one of the following API's to verify the presents of the key:
SFNTQueryFeature
SFNTEncrypt and then **SFNTDecrypt**
SFNTSign and then **SFNTVerify**
8. Every once in a while do one of the following API's, just to confuse a hacker.
 Do a **SFNTGetDeviceInfo**
 Do a **SFNTGetLicenseInfo**
9. Do a **SFNTReleaseLicense** to release the license before exiting the application.

Exit program