SMH Technologies®

AN00180
DC11618
April 2024
R. Ertolupi

Applying Cyber Security in the In-System Programming



1. Introduction

This Application Note aims to explain how Cyber Security is becoming such an important topic also for In-System Programming and how FlashRunner is capable of meeting the higher requirements that are coming from the market.

We often hear about this topic, also in our daily life, but what is “Cyber Security”? It is a practice of defending electronic systems and data from malicious attacks. This is extremely important nowadays in many aspects of our life and we have to take care of that in both business and private life. Obviously, Cyber Security is involving also the In-System Programming market, customers’ requests are constantly increasing, especially for automotive applications, and we keep investing in that.

We have to make a distinction between those Cyber Security features applied on the **target side** and those applied on the **FlashRunner side**. Both sides are interesting and, in this document, we are going to explore both of them, with a special focus on the FlashRunner side and the three concepts that are applied: **antipiracy**, **traceability** and **integrity**.

HQ and Registered Office
Via Giovanni Agnelli 1
33083 Villotta di Chions (PN) Italy
Società Unipersonale

Capitale sociale €102.040
P.I. 01697470936
C.F. 01697470936
REA PN-97255

D-U-N-S® 51-724-9350
T + 39 0434 421 111
F + 39 0434 639 021

→smh-tech.com

info@smh-tech.com

2. Contents

1. Introduction 1
2. Contents 2
3. Target side 3
4. FlashRunner side 4
5. Data encryption 5
6. Permission management 6
7. Data integrity check 7
8. Firmware authenticity check 8
9. Flashing cycles control 9

HQ and Registered Office
Via Giovanni Agnelli 1
33083 Villotta di Chions (PN) Italy
Società Unipersonale

Capitale sociale €102.040
P.I. 01697470936
C.F. 01697470936
REA PN-97255

D-U-N-S® 51-724-9350
T + 39 0434 421 111
F + 39 0434 639 021

→smh-tech.com

info@smh-tech.com

3. Target side

When talking about cyber security on the target side, we mean all the features that protect the devices from cyber attacks when they are applied in the actual customers' applications. Especially for automotive projects, these cyber security features on the microcontrollers are extremely important since we are moving towards a future with autonomous driving cars. Just think about how dangerous could be if an autonomous car was hacked.



In the market there are several different architectures of microcontrollers and microprocessors, produced by different silicon producers, they all are implementing some features to protect themselves. Anyway, there are no common standards, so each architecture has its own peculiarities and they can be extremely complex. This is not a big problem for FlashRunner because it is a Universal programmer and it is supporting all the features that are required for production (flashing and re-flashing), such as:



- OTP fuses
- Permanently lock debug port
- Lock and unlock using passwords
- HSM programming
- Memory protections
- Etc.

It is possible to find detailed info about the specific features of each architecture in the Wiki section of SMH Technologies' website: https://smh-tech.com/wiki-list/

HQ and Registered Office
Via Giovanni Agnelli 1
33083 Villotta di Chions (PN) Italy
Società Unipersonale

Capitale sociale €102.040
P.I. 01697470936
C.F. 01697470936
REA PN-97255

D-U-N-S® 51-724-9350
T + 39 0434 421 111
F + 39 0434 639 021

→smh-tech.com
info@smh-tech.com

4. FlashRunner side

On the other side, FlashRunner includes several methods to protect itself and the customers' data that it manages. In fact, as anticipated in the introduction, three concepts are implemented:

- **Antipiracy**
  FlashRunner has to prevent any undesired access to its data and to its features, but at the same time, it must preserve its characteristic of flexibility. That's why all the cyber security features that can impact the user experience, have to be enabled by the user who has full control of FlashRunner features.
  For example, the user can choose to use **encrypted data**, both static data and dynamic data, to protect his intellectual property (see chapter 5).
  Moreover, FlashRunner allows the user to create two different levels of permissions: **Admin** and **Guest**. So, the Admin user has full access to the FlashRunner and he can choose what commands and features are available for the Guest user and he can also choose to disable some features for both users if needed (see chapter 6).
  In addition to these standard features, SMH Technologies can also develop custom solutions to encrypt data that are decrypted directly on the target device. This can be used to implement an "encrypted cable" so, even if someone sniffs the ISP signals, he cannot get any sensitive data.

- **Integrity**
  FlashRunner must be able to guarantee that the data used are exactly the ones expected by the customers. So it must **detect** any kind of data **alteration** or corruption and this can be done using several methods explained in chapter 7. After that, FlashRunner must program those data and, in conclusion, it must **verify** that the data programmed are the ones defined by the customer. This verification step is typically done internally by FlashRunner but, if the user wants, it is also possible to dump the memory content of the target device and store all data into a binary file that can be parsed by the local computer.

- **Traceability**
  FlashRunner can be integrated into the production line to improve traceability, in fact, it is providing a detailed log of what operations were executed and when. The **log** can also be configured to be more or less verbose according to the customer's needs (some customers do want not to track anything on the log). Moreover, when the target device allows it, FlashRunner can read the **unique id** and return that value to the user which can be very important to trace the full story of that product starting from the silicon producer factory.
  One more interesting feature that allows customers to trace their production line is the possibility to set a limitation to the number of boards programmed, in this way he can be sure that no additional boards are produced (see chapter 8).

HQ and Registered Office
Via Giovanni Agnelli 1
33083 Villotta di Chions (PN) Italy
Società Unipersonale

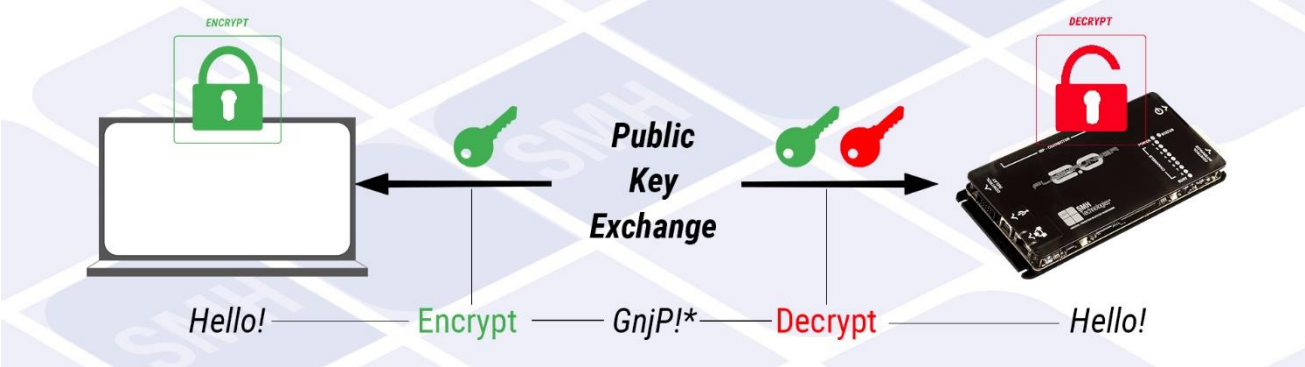
Capitale sociale €102.040
P.I. 01697470936
C.F. 01697470936
REA PN-97255

D-U-N-S® 51-724-9350
T + 39 0434 421 111
F + 39 0434 639 021

→smh-tech.com
info@smh-tech.com

5. Data encryption

FlashRunner uses a very secure way to encrypt data, in fact, it implements the public and private key method. Keys are randomly generated by FlashRunner, the private key is securely stored inside FlashRunner, while the public key can be shared with the computer. So, data are encrypted by the computer (from Workbench, DLL or command-line tools) using the public key and then data are decrypted by FlashRunner using the private key.



Since the pair of keys are randomly generated, each FlashRunner has its own unique keys and data encrypted for a specific FlashRunner **can only be decrypted by that FlashRunner**. Moreover, each FlashRunner model can only have a single pair of keys and the user can choose to regenerate the keys anytime that he wants. It must be noticed that when regenerating the keys, all the data encrypted with the previous keys cannot be decrypted anymore (even SMH cannot decrypt those data). This may result useful in case the user wants to actually invalidate those data.



This encryption method can be applied to both **static data**, such as the microcontroller firmware, and **dynamic data**, such as passwords, serial numbers, or other keys that are different for each board programmed by FlashRunner.

HQ and Registered Office
Via Giovanni Agnelli 1
33083 Villotta di Chions (PN) Italy
Società Unipersonale

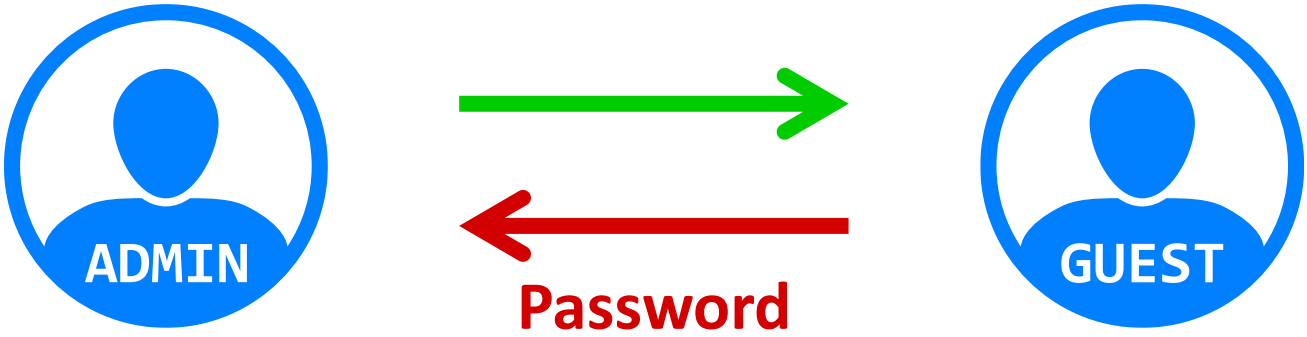
Capitale sociale €102.040
P.I. 01697470936
C.F. 01697470936
REA PN-97255

D-U-N-S® 51-724-9350
T + 39 0434 421 111
F + 39 0434 639 021

→smh-tech.com
info@smh-tech.com

6. Permission management

As anticipated earlier in this document, FlashRunner offers an advanced method to fully control access to its functionalities. Customers can enable the two user levels: the **admin** user and the **guest** user. To log in as admin a **password** is needed and that password can be freely defined and changed by the customer when using FlashRunner as admin.



FlashRunner is very flexible, in fact, the admin user can configure the system to choose specifically which commands are allowed to be used by the guest user. For example, the admin user can choose to disable the commands to send files to FlashRunner, so the guest user will not be able to change the files in the FlashRunner memory. The admin user can also choose to disable the commands to receive files from FlashRunner, so there will be no way for the guest user to obtain the data stored in FlashRunner. In general, the admin user can disable any command that is not needed by the guest user and that could change something relevant in the FlashRunner.
Moreover, the admin can choose to disable some system features also for himself in case he wants to have a higher level of protection regarding some specific aspects. To re-enable those features, the admin user will be asked to login again using the password to confirm that he is really sure about that choice.

In conclusion, this feature has a big potential due to its versatility and can be useful in several conditions, such as protecting FlashRunner data and configurations from undesired accesses. Anyway, these undesired accesses could be from an operator that does not fully know FlashRunner systems and may cause some damage. In the previous chapter, we explained what happens when a user regenerates the public and private keys, think about a non-expert operator accidentally regenerating the keys and invalidating all the encrypted firmware files, it could cause a big problem to the production line because those files will not be usable anymore. So we suggest combining this feature with encryption.

HQ and Registered Office
Via Giovanni Agnelli 1
33083 Villotta di Chions (PN) Italy
Società Unipersonale

Capitale sociale €102.040
P.I. 01697470936
C.F. 01697470936
REA PN-97255

D-U-N-S® 51-724-9350
T + 39 0434 421 111
F + 39 0434 639 021

→smh-tech.com
info@smh-tech.com

7. Data integrity check



FlashRunner offers several ways to protect the data that it manages, but it offers also several ways to be sure that the data are the ones expected by the customers and they have not been altered or corrupted. In fact, this can be useful as a double-check when using the cyber security features already described in this document and it is even more useful when not applying any protection to the FlashRunner. This is a list of features that allow the customer to perform the data integrity check:

- **CRC32 check on FRB file**
  The FRB format file is an SMH Technologies' proprietary format, designed to contain the customers' firmware files by guaranteeing both performance and security. Each FRB file contains a header with a CRC32 value calculated based on the content of the file. Anytime that FlashRunner uses that file for the first time, it calculates a CRC32 based on the data read from the file and it checks that this calculated CRC32 matches with the one stored in the header of the file. If this check is not successful, then all the operations are stopped. The user can also choose to force the execution of this check for each board produced.

- **CRC32 check on PRJ file**
  Even the PRJ format is an SMH Technologies' proprietary format, designed to contain information, parameters and commands about the target device to program and what operations to execute on that. The first part of the project (PRJ) file contains some fixed information about the device and that part should never be altered, that is why those data are validated by a CRC32. So, anytime that a project is executed, there is a check that the expected CRC32 value matches the CRC32 calculated based on the actual data.

- **CRC32 or SHA256 for any file**
  FlashRunner's users can obtain the CRC32 value or the SHA256 value of any file that is stored inside the FlashRunner memory. These values are calculated based on the file content and they can be useful instruments to validate that the files that FlashRunner is using are actually the ones that the customer needs to use. By checking these values it is possible to detect any alteration to the file.

- **CRC/CheckSum for the actual memory content of the target device**
  According to the target device specifications, FlashRunner can offer the possibility to get a CRC/CheckSum value that is calculated based on the actual data contained in the target device memory. So this can be useful as the very last step of the flashing sequence to be sure about the data integrity until the end of all operations.

HQ and Registered Office
Via Giovanni Agnelli 1
33083 Villotta di Chions (PN) Italy
Società Unipersonale

Capitale sociale €102.040
P.I. 01697470936
C.F. 01697470936
REA PN-97255

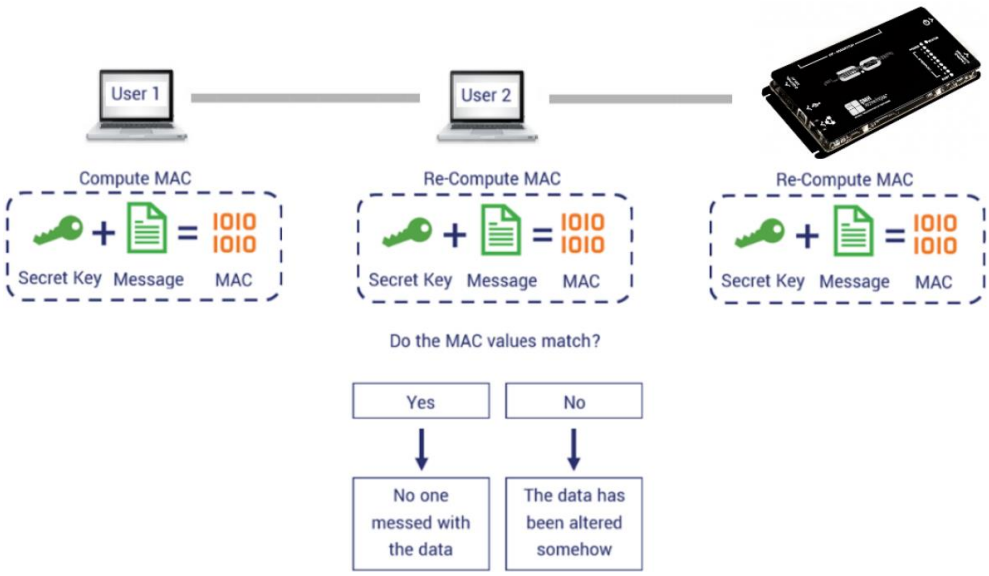
D-U-N-S® 51-724-9350
T + 39 0434 421 111
F + 39 0434 639 021

→smh-tech.com

info@smh-tech.com

8. Firmware authenticity check

FlashRunner goes beyond basic error detection methods like CRC and CheckSum to ensure the authenticity of your firmware files. While CRC and CheckSum can identify accidental data corruption, they are vulnerable to intentional modifications.
FlashRunner addresses this by allowing you to sign encrypted FRB files using a secret key with a method called CMAC (Cipher-based Message Authentication Code). CMAC is specifically designed to provide robust security and guarantee file authenticity throughout its lifecycle.
You can choose a secret key length of 128, 192, or 256 bits. This key is used to calculate a CMAC value for the data. Both the secret key and the CMAC value are then stored within the encrypted FRB file. When FlashRunner uses the file, it recalculates the CMAC using the embedded secret key and compares it to the stored value. Only if the values match is the file considered authentic, ensuring the integrity of your firmware.



HQ and Registered Office
Via Giovanni Agnelli 1
33083 Villotta di Chions (PN) Italy
Società Unipersonale
Capitale sociale €102.040
P.I. 01697470936
C.F. 01697470936
REA PN-97255
D-U-N-S® 51-724-9350
T + 39 0434 421 111
F + 39 0434 639 021
→smh-tech.com
info@smh-tech.com

9. Flashing cycles control



FlashRunner offers a very special feature that allows customers to have full control of the number of flashing cycles executed by the programmer. This can be useful especially if there is a third-party company involved in the production, in this way it is possible to track the exact number of boards produced.

This feature must be combined with the “permission management” explained in chapter 6. In fact, it is only the admin user who can set the limit and reset the counter. The counter is counting only the flashing cycles executed by the guest user. When the guest user reaches the limit, he cannot execute any additional project on that FlashRunner until the admin user resets the counter or changes the limit.

HQ and Registered Office
Via Giovanni Agnelli 1
33083 Villotta di Chions (PN) Italy
Società Unipersonale

Capitale sociale €102.040
P.I. 01697470936
C.F. 01697470936
REA PN-97255

D-U-N-S® 51-724-9350
T + 39 0434 421 111
F + 39 0434 639 021

→smh-tech.com
info@smh-tech.com