

12.15 – 12.40

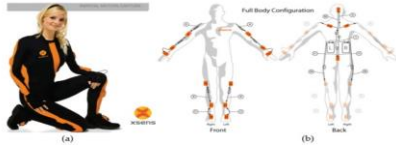
Bescherming van (software) IP bij uitbesteding van productie

Gerard Fianen
INDES-IDS BV

The choice of professionals

Wie zijn wij ?

Tools, software components and services for the development, testing and production of Real-Time Embedded Software



INDES -
Integrated Development Solutions BV

Wie zijn wij ?

Tools, software components and services for the development, testing and production of Real-Time Embedded Software



INDES -
Integrated Development Solutions BV

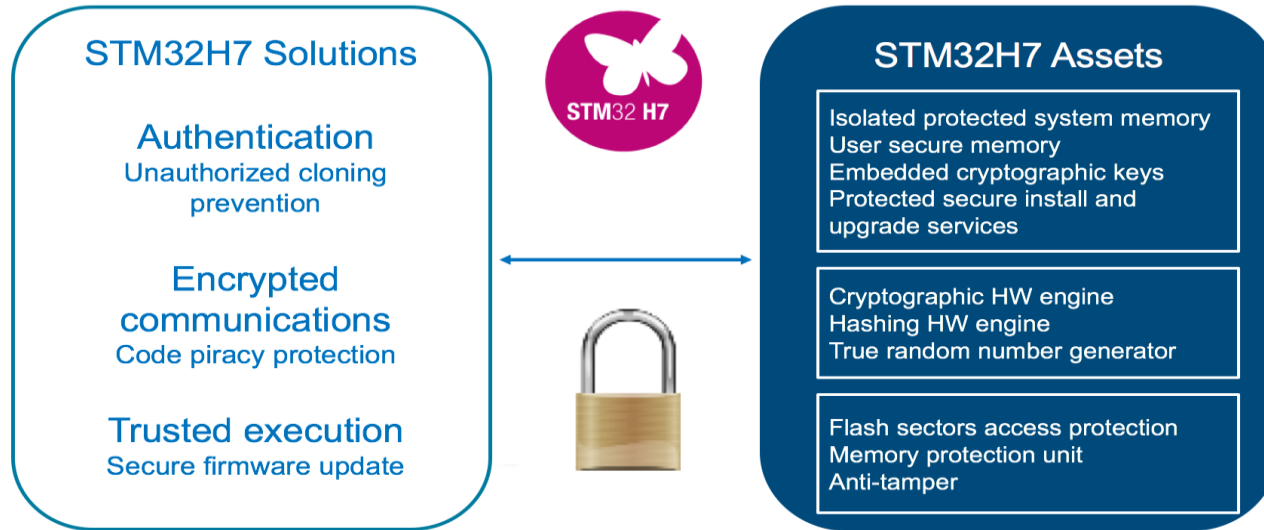
Even een paar open deuren

- Productie van geavanceerde hardware is goedkoop..
Mits je die uitbesteed
- Uw kennis zit grotendeels in de Software
Die je hoogstens alleen met mate moet uitbesteden



Er zijn tegenwoordig secure MCU's

Advanced Security on STM32H7 1



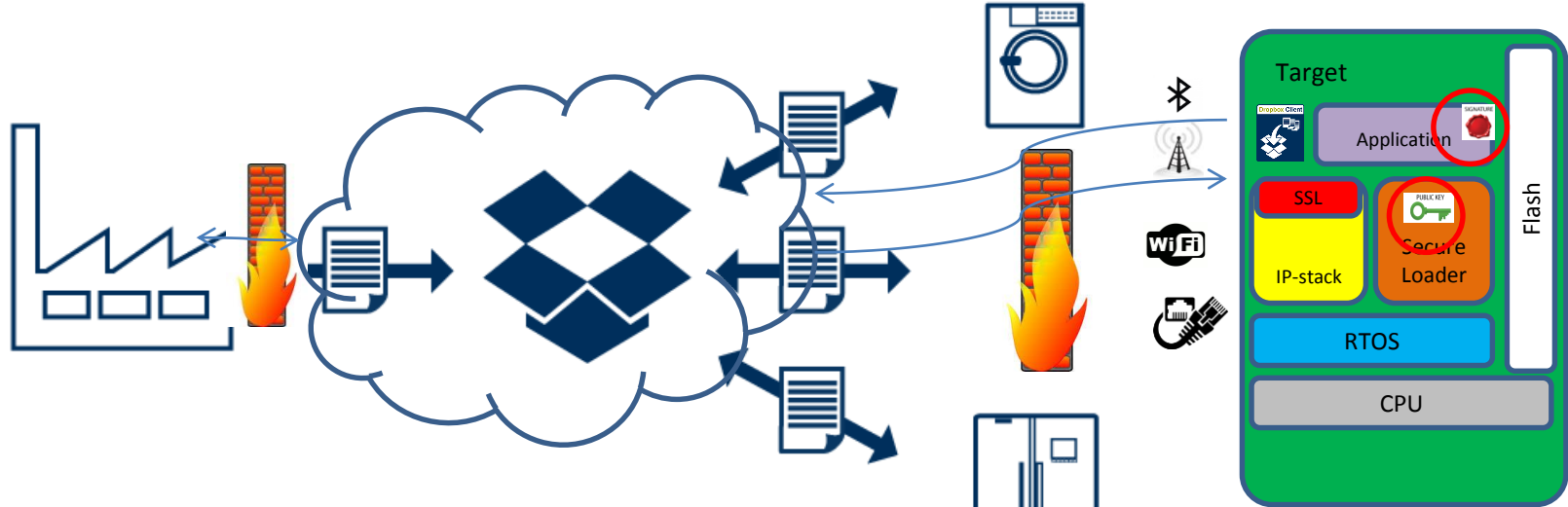
Er zijn tegenwoordig secure MCU's

De uitdaging:

Hoe krijg ik mijn code daar op een veilige manier in ?



Remote update ..



30/31 MEI & 1 JUNI 2017
JAARBEURS UTRECHT

ELECTRONICS
& APPLICATIONS
WWW.EABEURS.NL

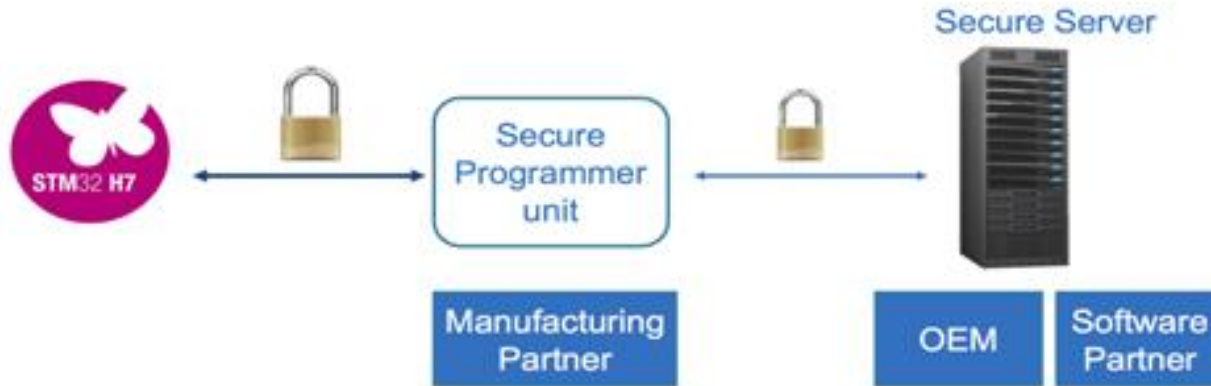
Aandachtspunten :

- Bewaking productievolume bij Contract Manufacturer(s)
- Voorkomen van namaak
- Alleen authentieke software mag opstarten
- Kleine overhead in codesize, productietijd en kosten
- Moet eenvoudig in te passen zijn in het process

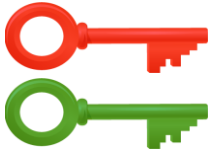


Encryptie en Authenticatie :

- Digital signatures, aangemaakt door een trusted server
- Signatures worden gebruikt voor authenticatie hardware en firmware
- Alle communicatie is versleuteld



Componenten :



1. **Key Set**
 - a) Private key
 - b) Public key

2. **Verificatie Library (Target)**
 - a) RSA based signatures
 - b) ECDSA based signatures

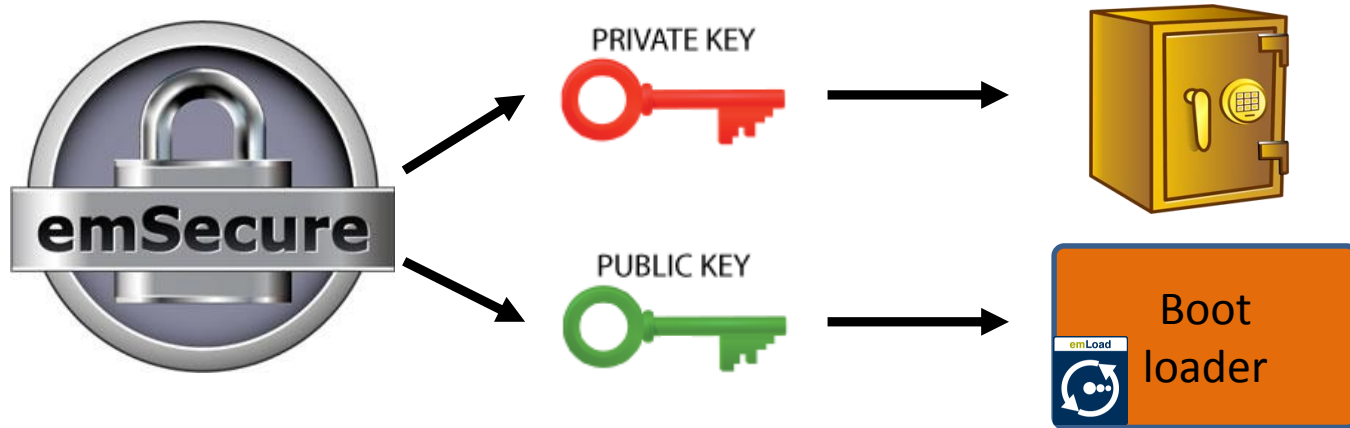
3. **Secure Server**
 - a) Trusted Company (e.g. Segger)
 - b) IP owner itself

4. **Secure Programmer**
 - a) Flasher Secure
 - b) Secure Flash Programming utility



Voorbeeld secure bootlader :

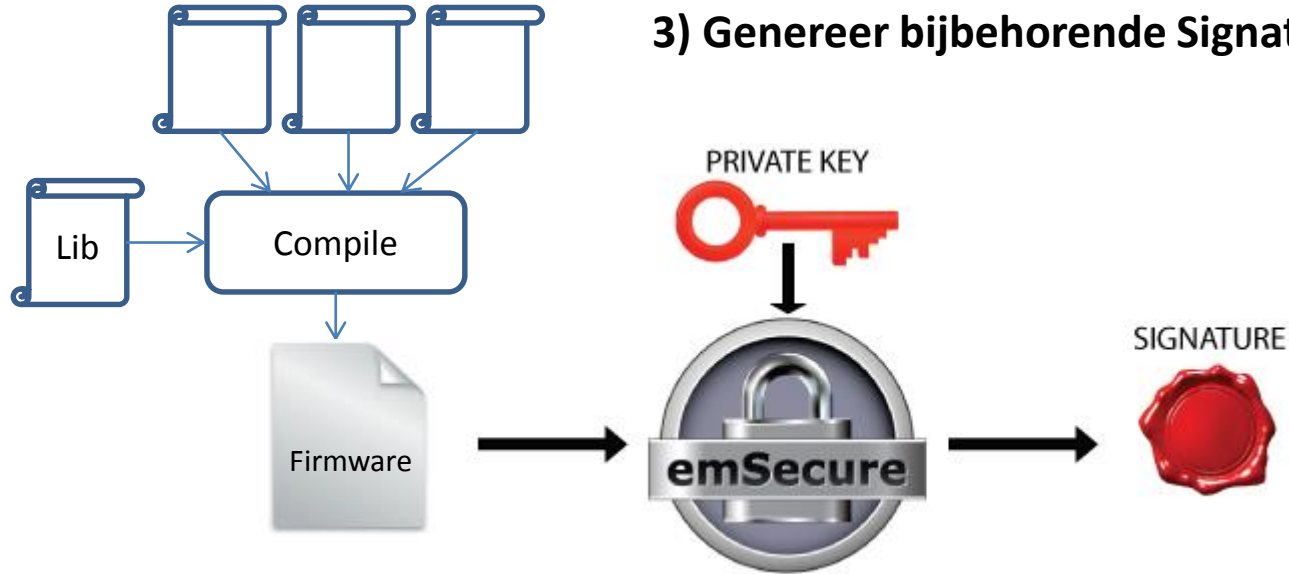
1) Genereer een Key set



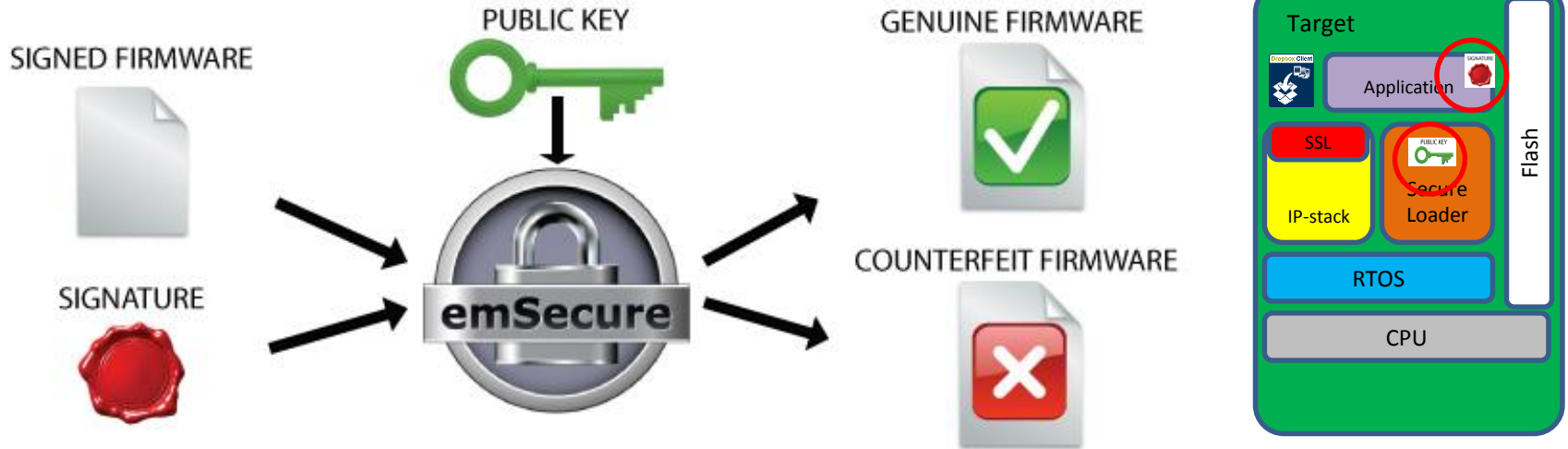
Genereer een signature

2) Genereer applicatie code

3) Genereer bijbehorende Signature

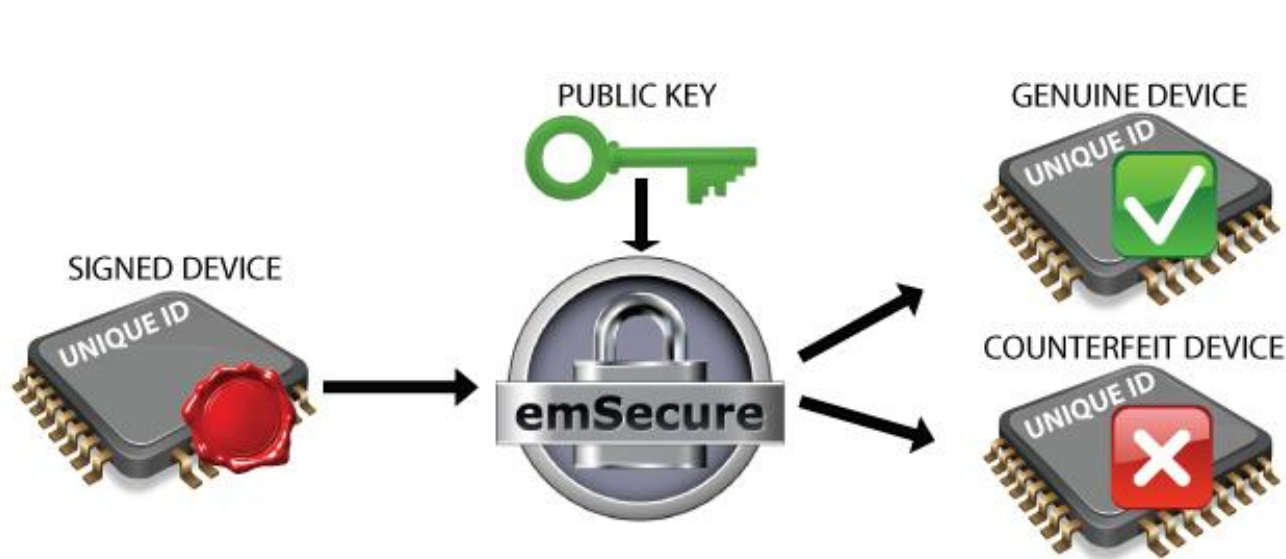


Secure bootloader



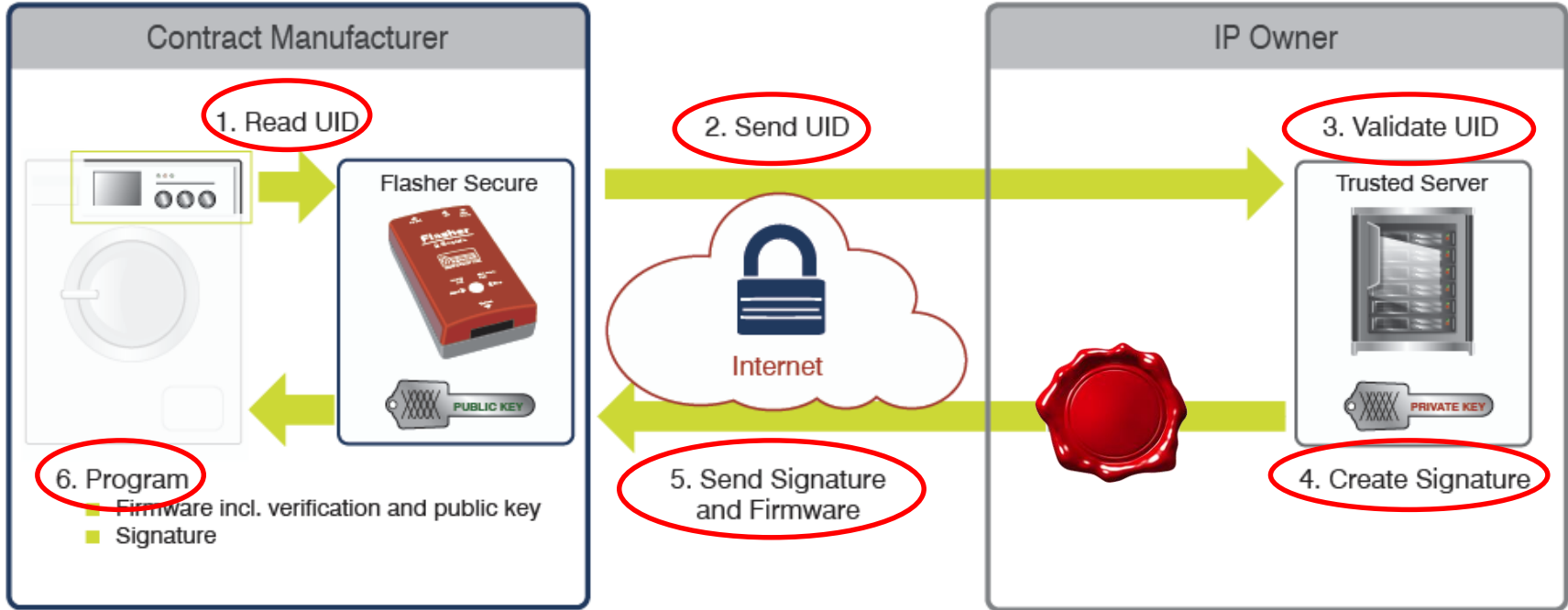
On a firmware update and when starting the product, the bootloader will verify the firmware by its signature. If they match, the firmware is started, otherwise the application will stay in the bootloader or even erase the firmware.

Maar wat als we in plaats daarvan een MCU signen ?

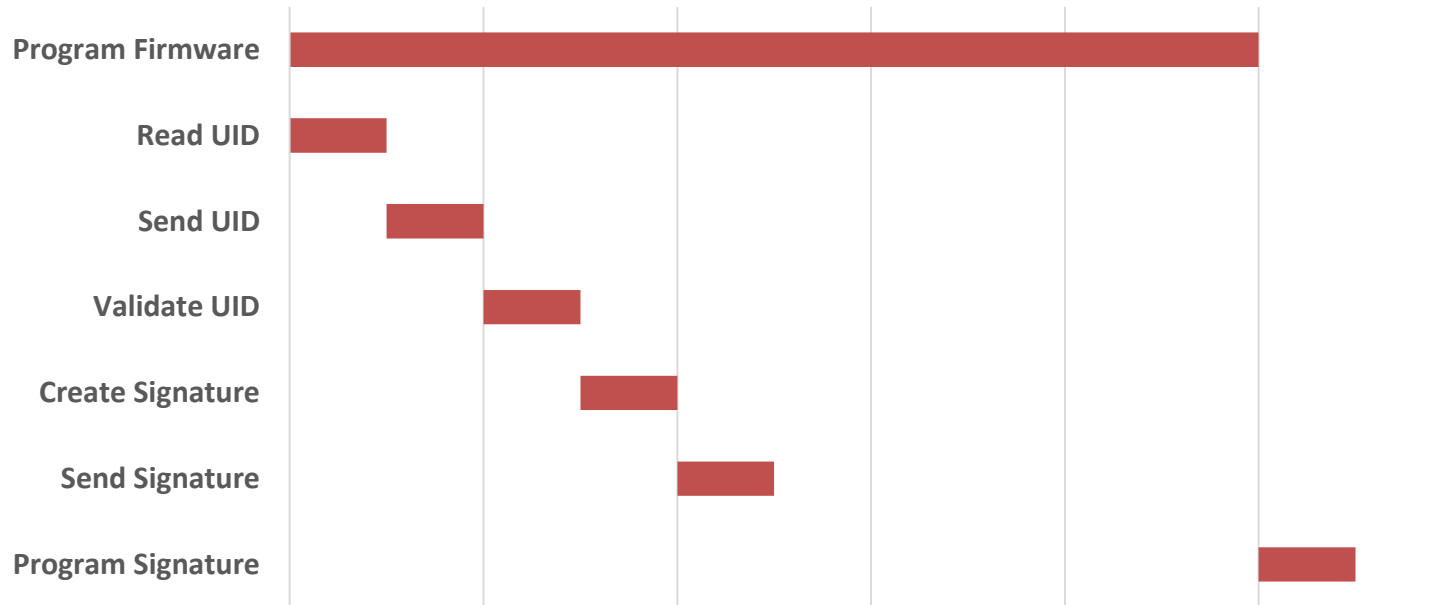


The public key will be included in the firmware, which will run on the product. When the firmware is running, it will read the unique data from the unit and verify it with the signature. When the signature does not match, the firmware will refuse to run

Secure productie proces :



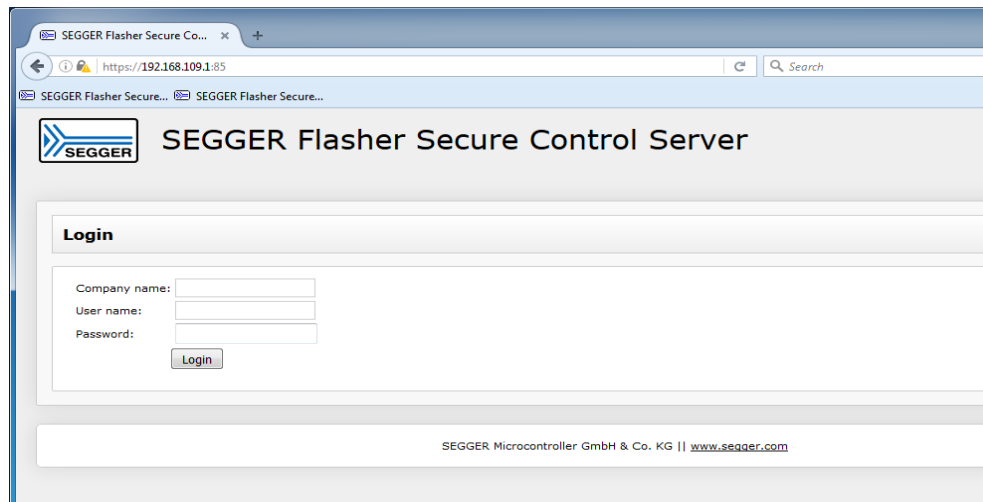
Overhead in productietijd ?



Finalizing the authentication process needs to wait for programming to finish. No additional process time, as signature handling is performed in parallel.

Account management :

- Account management
 - Administration
 - User
 - Contract manufacturers
- Firmware management
 - Firmware binary
 - Signature key management
- Project management
 - Manufactured volume
 - Contract manufacturer
- Production recording
 - Logging of programming records
 - Report of failed programming tries



100% transparant & veilig

Firmware management :

- Account management
 - Administration
 - User
 - Contract manufacturers
- Firmware management
 - Firmware binary
 - Signature key management
- Project management
 - Manufactured volume
 - Contract manufacturer
- Production recording
 - Logging of programming records
 - Report of failed programming tries

Devices

Current project: Drill

Programmed devices:

No.	Serial no.	Unique device ID	Cycles	Last result
1	10000	00460019 34345109 35353835 00000000	3	OK (1)

No.	IP	Programmed	Flasher S/N	Result
1	192.168.109.1	2016-10-07 14:13:34	3735928559	OK (1)
2	192.168.109.1	2016-10-07 14:14:01	3735928559	Abandoned (0)
3	192.168.109.1	2016-10-07 14:14:21	3735928559	OK (1)

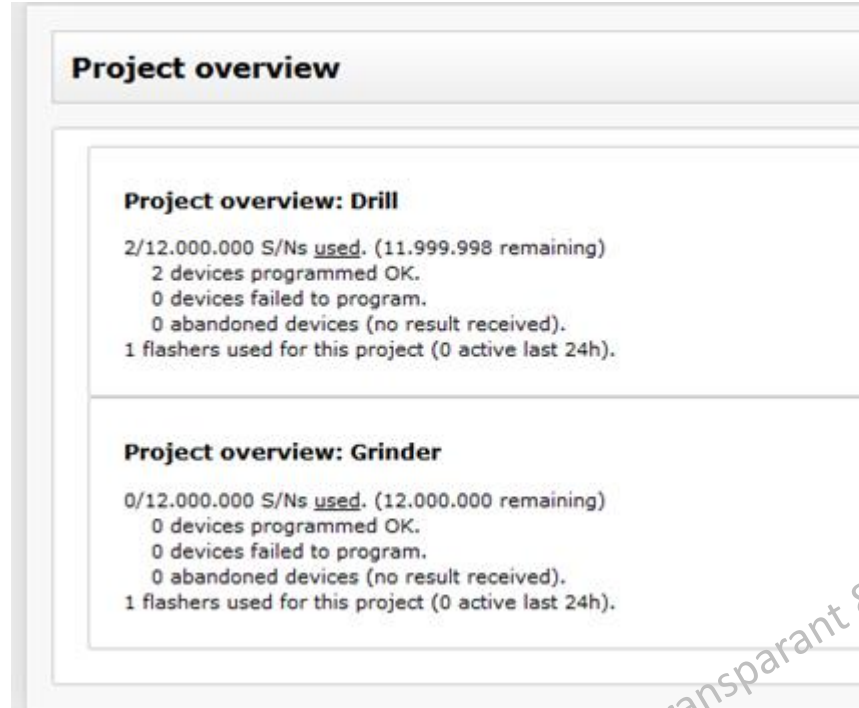
2	10001	001E0033 34345109 35353835 00000000	3	OK (1)
---	-------	-------------------------------------	---	--------

No.	IP	Programmed	Flasher S/N	Result
4	192.168.109.1	2016-10-07 14:16:03	3735928559	OK (1)
5	192.168.109.1	2016-10-07 14:16:20	3735928559	Abandoned (0)
6	192.168.109.1	2016-10-07 14:16:48	3735928559	OK (1)

<< < Page 1/1 > >>

Project management & recording:

- Account management
 - Administration
 - User
 - Contract manufacturers
- Firmware management
 - Firmware binary
 - Signature key management
- Project management
 - Manufactured volume
 - Contract manufacturer
- Production recording
 - Logging of programming records
 - Report of failed programming tries



Project overview

Project overview: Drill

2/12.000.000 S/Ns used. (11.999.998 remaining)
2 devices programmed OK.
0 devices failed to program.
0 abandoned devices (no result received).
1 flashers used for this project (0 active last 24h).

Project overview: Grinder

0/12.000.000 S/Ns used. (12.000.000 remaining)
0 devices programmed OK.
0 devices failed to program.
0 abandoned devices (no result received).
1 flashers used for this project (0 active last 24h).

100% transparant & veilig

Stand 22



- BLE RF Tester
- ATE platform for wireless



Bedankt voor uw tijd !

