12.15 – 12.40

Bescherming van (software) IP bij uitbesteding van productie

Gerard Fianen
INDES-IDS BV
The choice of professionals

Wie zijn wij ?

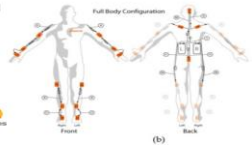
indes
The choice of professionals

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

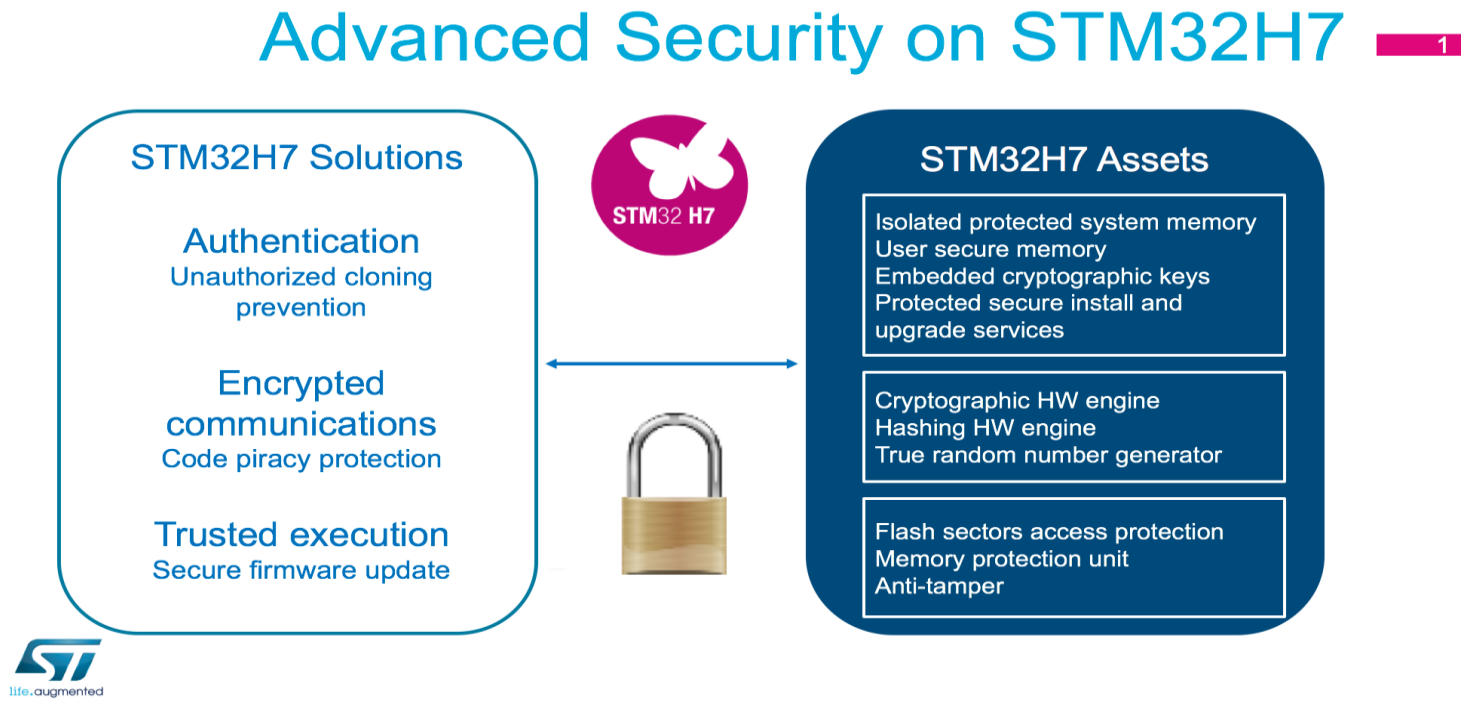
INDES -

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

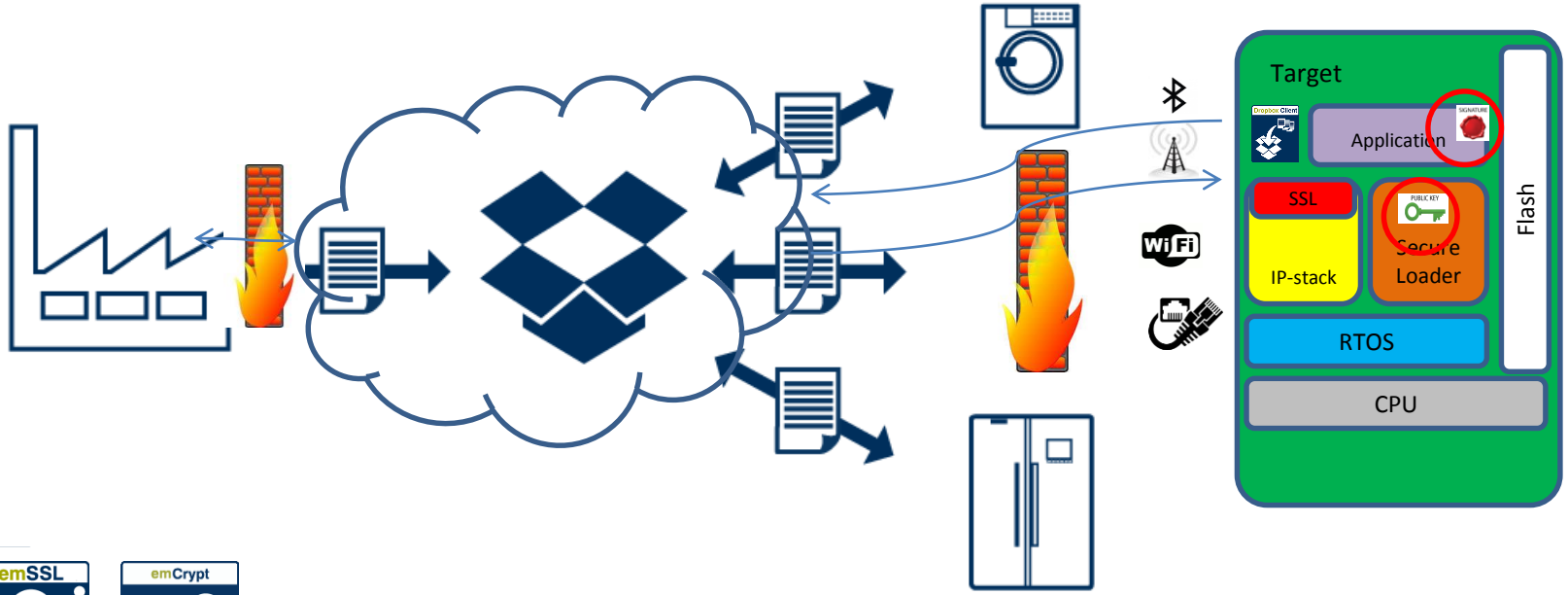


Er zijn tegenwoordig secure MCU's

De uitdaging:

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

Remote update ..



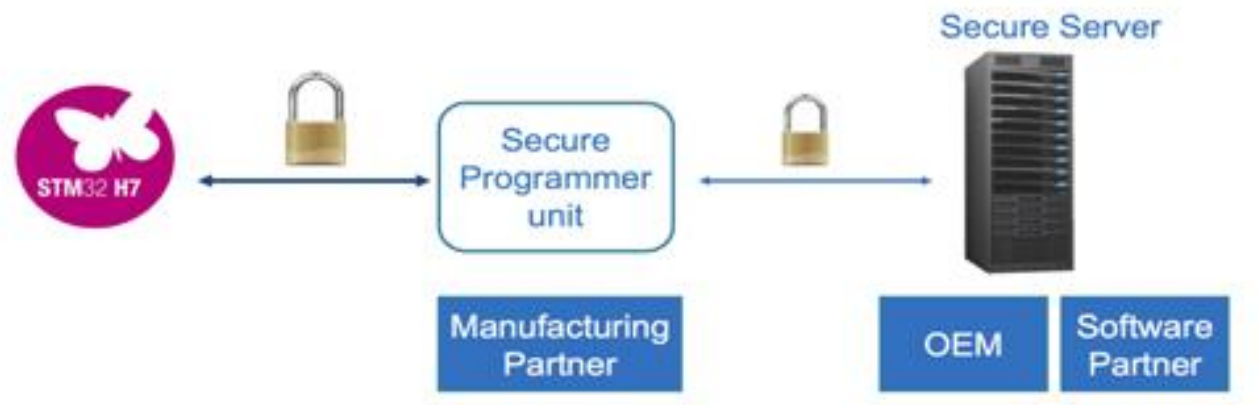
emLoad emSSL emCrypt

Aandachtspunten :

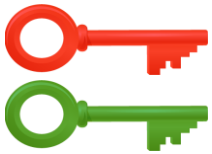
- Bewaking productievolume bij Contract Manufacturer(s)
- Voorkomen van namaak
- Alleen authentieke software mag opstarten
- Kleine overhead in codesize, productietijd en kosten
- Moet eenvoudig in te passen zijn in het process

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

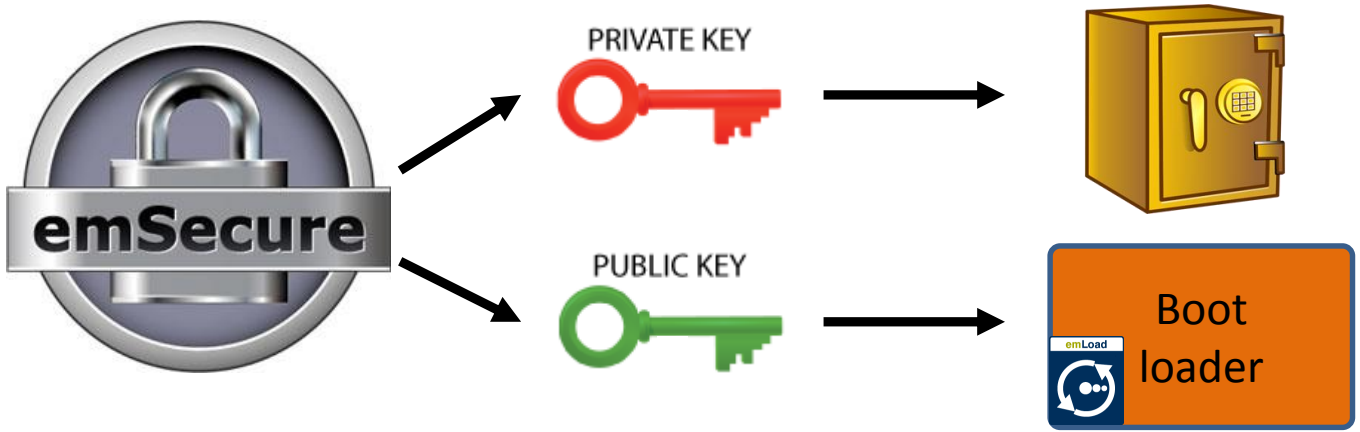
2. **Verificatie Library (Target)**
   a) RSA based signatures
   b) ECDSA based signatures

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 bootloader :

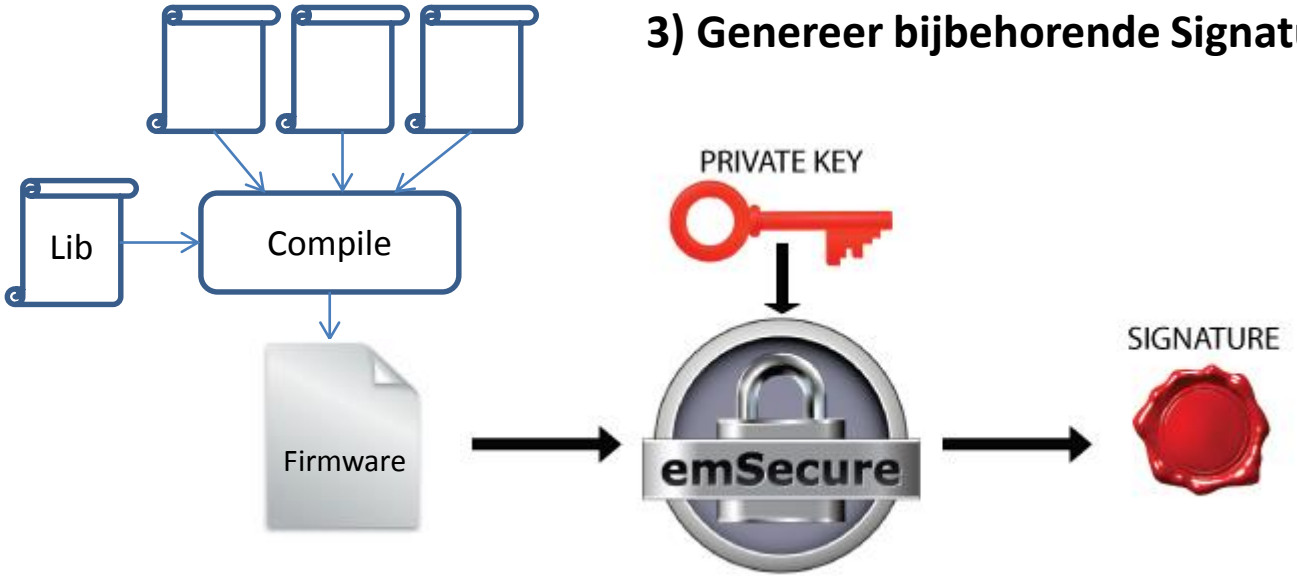
1) Genereer een Key set



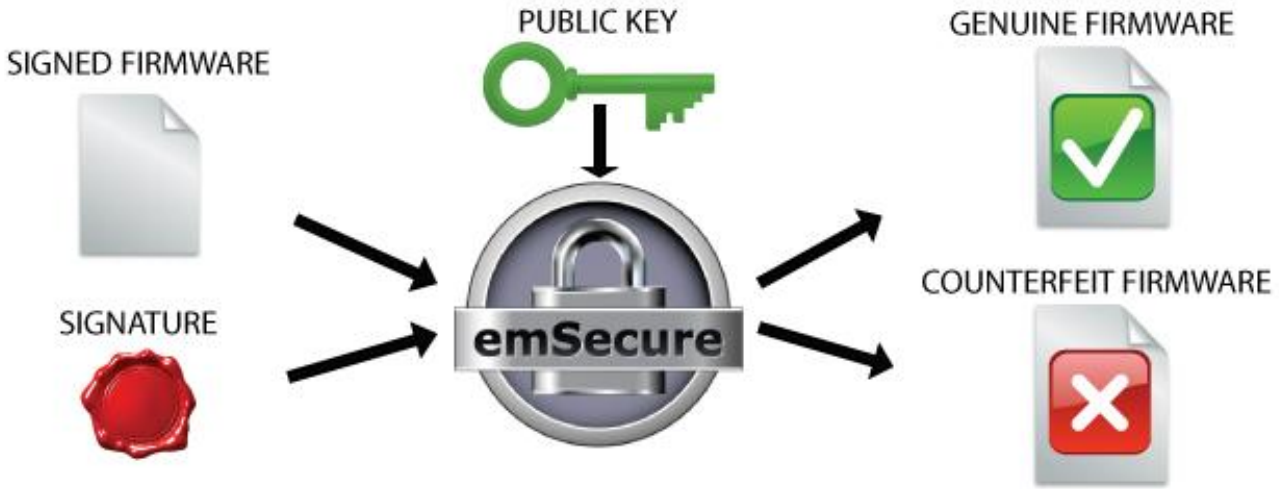
Genereer een signature

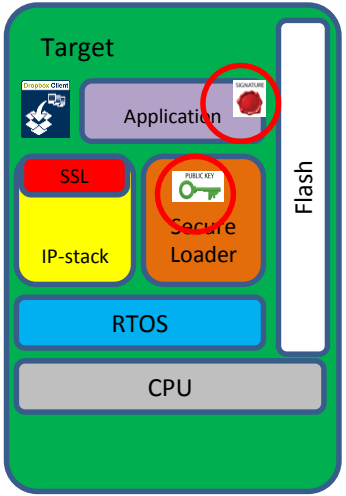
2) Genereer applicatie code

3) Genereer bijbehorende Signature



Secure bootloader



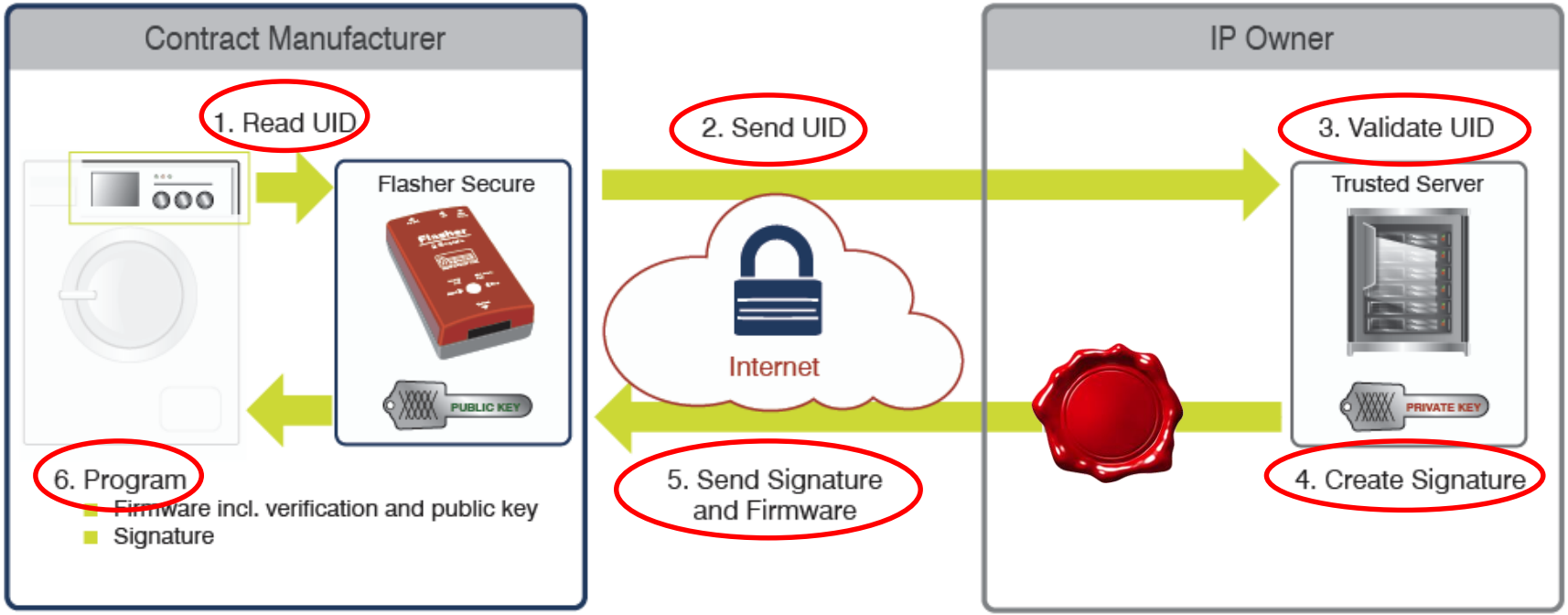


On a firmware update and when starting the product, the bootloader will verify the firmware by its signature. If they match, the firmware is started, otherwise the application will stay in the bootloader or even erase the firmware.

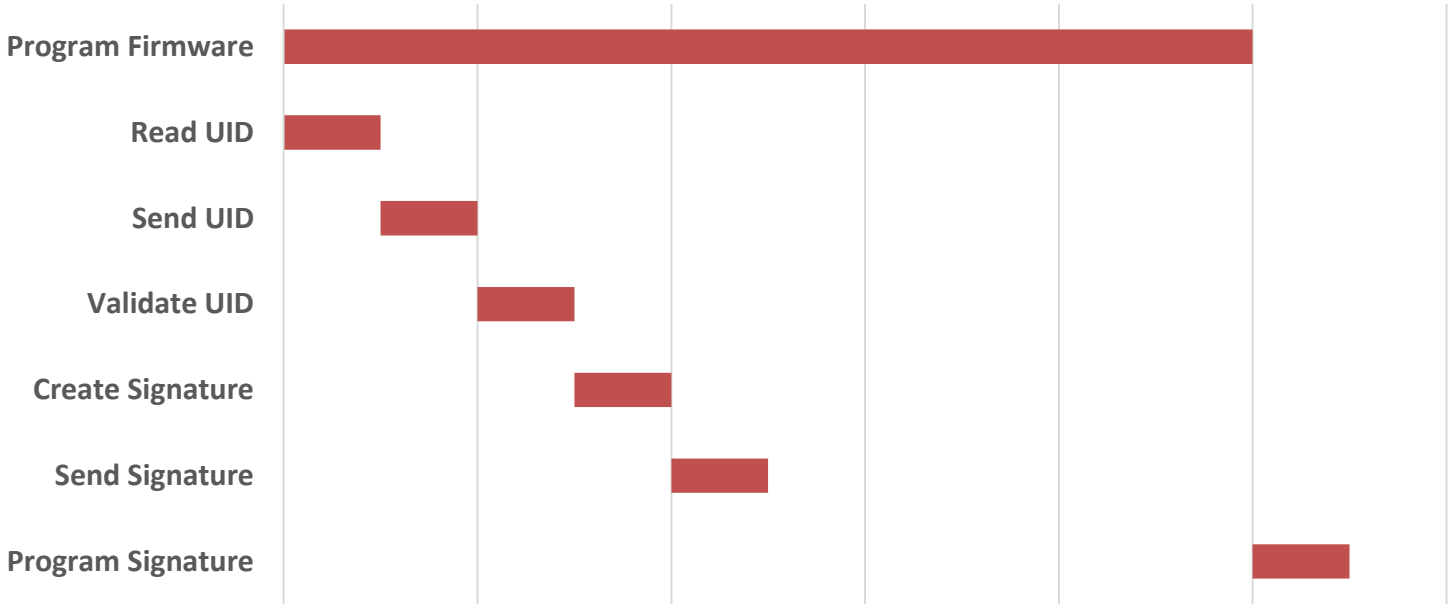
Maar wat als we in plaats daarvan een MCU signen ?

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 :



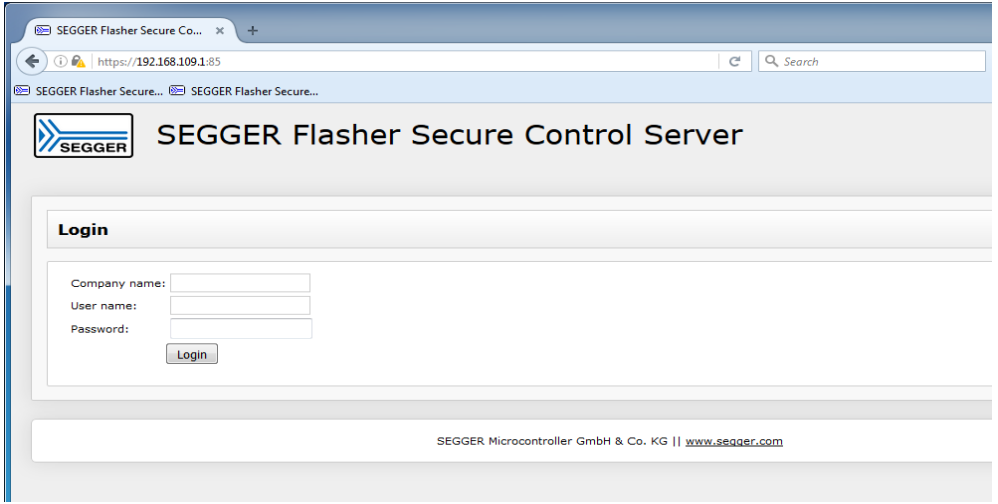
Overhead in productietijd ?



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

Account management :

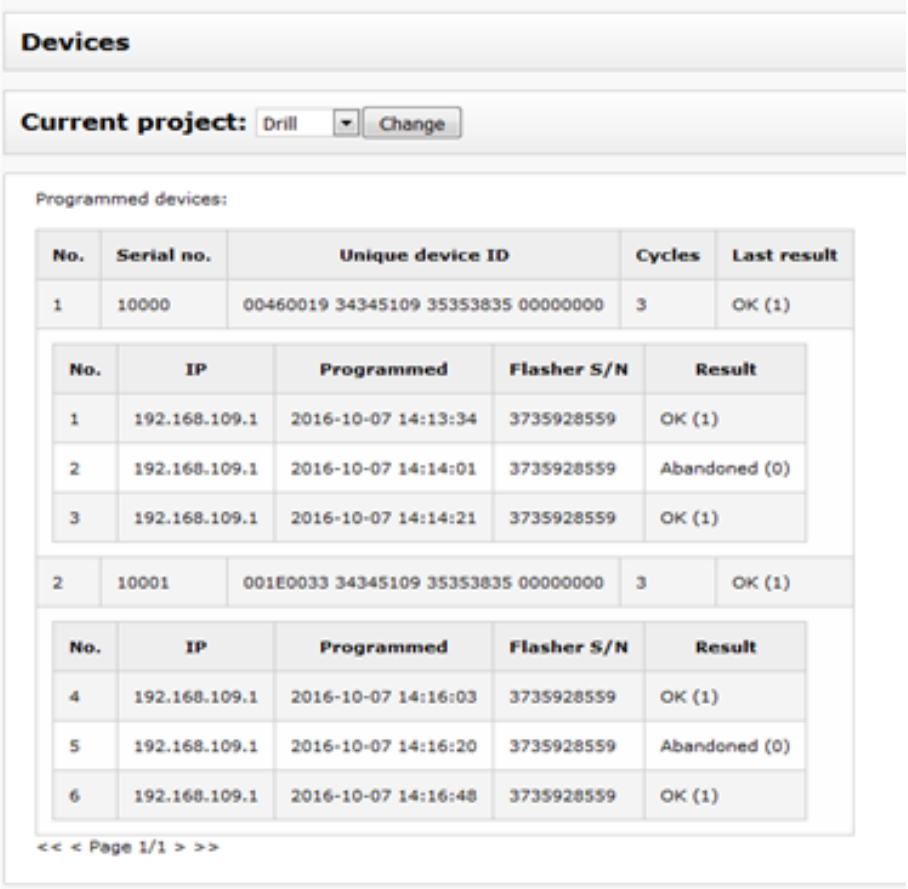
- Account management
  - Administration
  - User
  - Contract manufacturers
- Firmware management
  - Firmware binary
  - Signature key management
- Project management
  - Manufactured volume
  - Contract manufacturer
- Production recording
  - Logging of programming records
  - Report of failed programming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



100% transparant & veilig

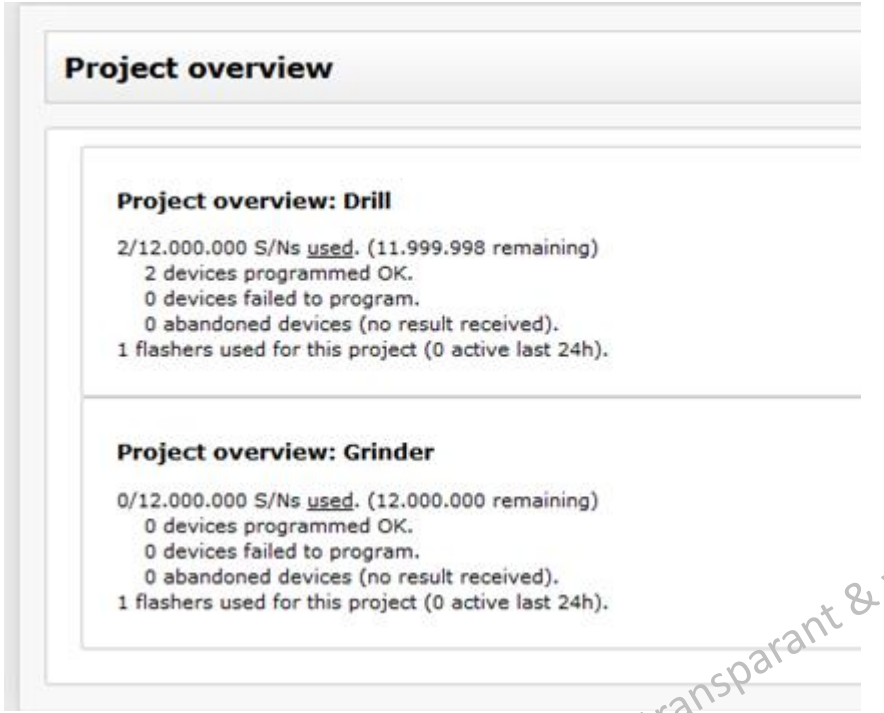
Firmware management :

- 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



Project management & recording:

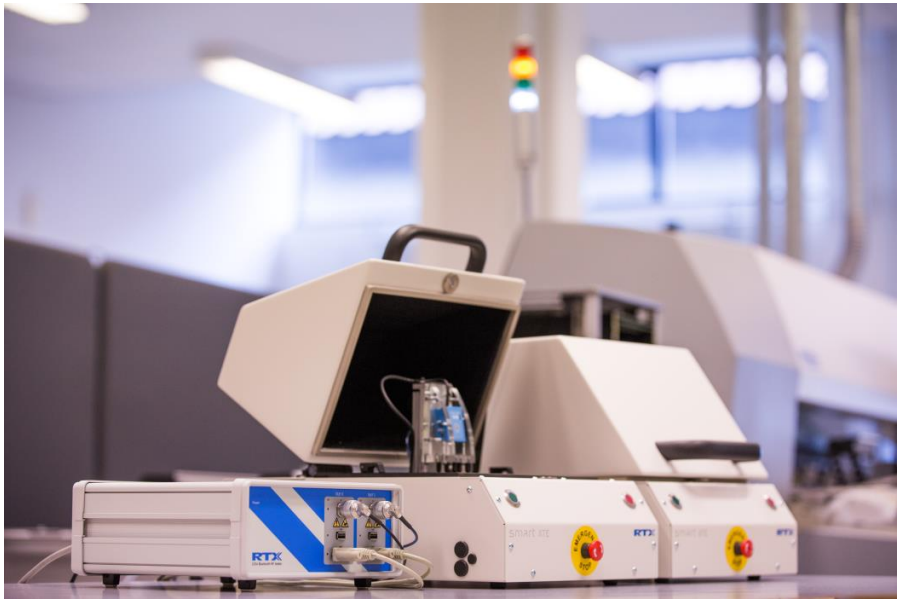
- Account management
  - Administration
  - User
  - Contract manufacturers
- Firmware management
  - Firmware binary
  - Signature key management
- Project management
  - Manufactured volume
  - Contract manufacturer
- Production recording
  - Logging of programming records
  - Report of failed programming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



100% transparant & veilig

Stand 22

- BLE RF Tester
- ATE platform for wireless



Bedankt voor uw tijd !

sales@indes.com www.indes.com/embedded Tel : 0345 – 545.535