

hello, whitepaper

# Cyber security in the elecontronics manufacturing: the holistic concept



Everything about cyber security solutions, ProMik's detailed performance spectrum, exciting use cases and much more!

# Content

**3**

Relevance

**4**

Application areas of cyber security in the electronics manufacturing

**5**

Cyber security infrastructure

**5**

On chip cyber security

**7**

Encryption methods

**9**

Keys for cyber security

**10**

ProMik: expert for cyber security in the electronics production

**11**

Use case: cyber security implementation of an ADAS-application

**12**

Get to know more about cyber security in the electronics production





## Relevance

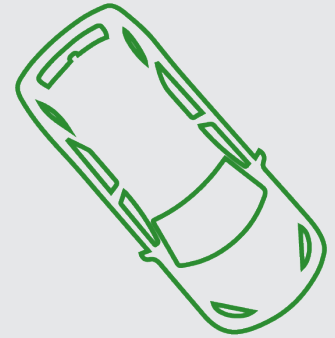
Imagine - you are on your way to work in your car. Music is playing while you accelerate. Suddenly a wind blows towards you. The air conditioning has set itself to a frosty 16 degrees. Before you can remedy this, your windscreen wiper switches on and the volume of the music suddenly increases. You want to brake, but contrary to your wishes, the car accelerates. Before you realise what is happening, you run off the road.

Such an incident occurred in 2015, when hackers manipulated the accelerator, brake, air conditioning, windscreen wipers and radio of a vehicle. At the time, the hackers wanted to draw attention to the security vulnerabilities of modern cars - with success.

This demonstrates the relevance of cyber security in electronics manufacturing. Because such interventions can be prevented by investing in security mechanisms already during production. ProMik has recognised the increased requirements and expanded the existing toolchain to meet them.

# Application areas of cyber security in the electronics manufacturing

In the automotive sector, cyber security is already considered an important standard in production. By securing electrical components as early as possible, vehicle drivers and other road users can be protected. Examples of automotive applications are infotainment and battery management systems, ADAS-applications and many more.

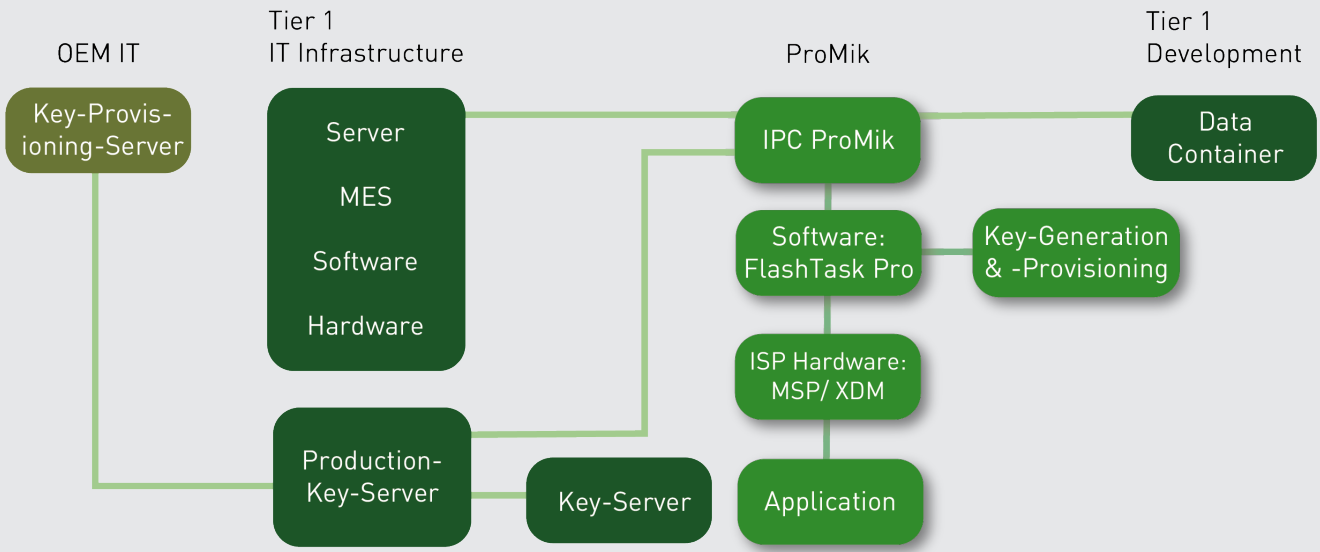


[→ READ MORE](#)

However, cyber security in electronics manufacturing is also becoming increasingly important in other areas. Due to the growing proportion of technology, which is also becoming more complex, the attack surface for hackers is becoming larger as well. Sectors which for this reason also belong to ProMik's areas of expertise include the IOT, industrial and consumer goods.



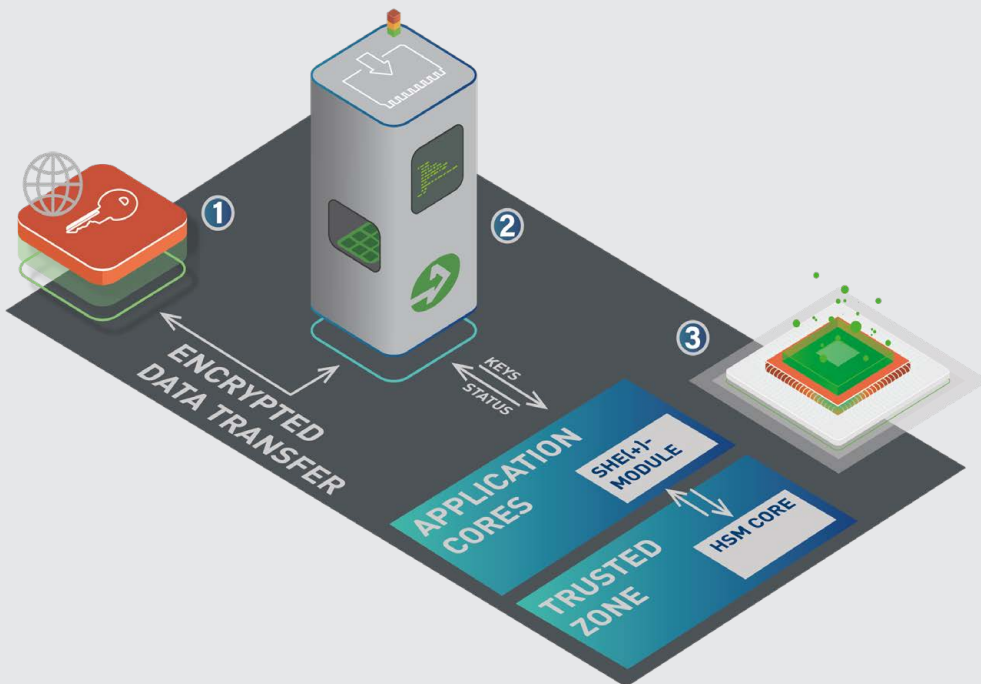
# Cyber security infrastructure



The cyber security infrastructure of ProMik, Tier 1 and OEM

[→ READ MORE](#)

# On chip cyber security



1. Key management server
2. Secure programming
3. On chip cyber security

Integration of on chip cyber security into the production process.

[→ READ MORE](#)

# Process

First, the ProMik Bootloader is developed. It executes the flash programming of the firmware on the hardware security module (HSM), which initialises and starts it.

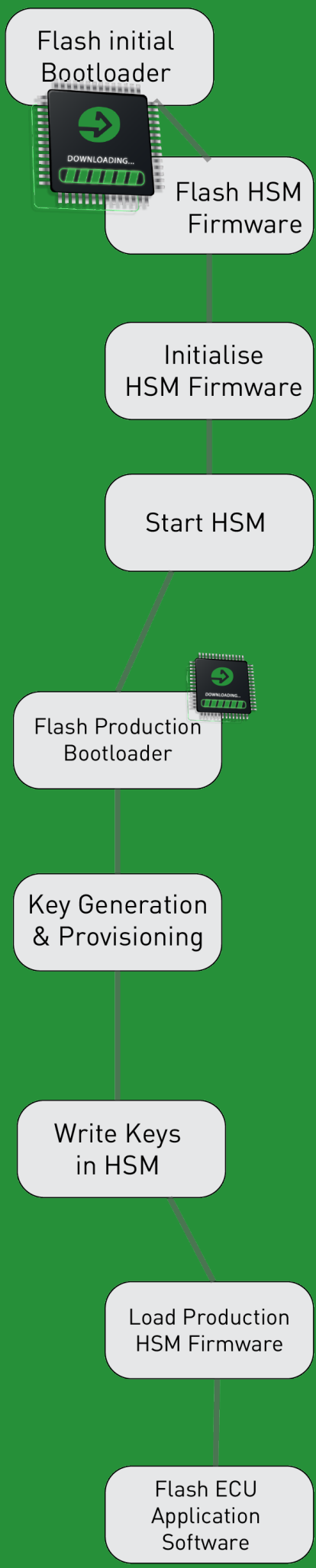
An important step in on chip security is key generation and key provisioning. The key generation can be done either by ProMik or by the OEM.

Subsequently, the keys are transferred to the HSM via the ProMik Bootloader and stored there. The Bootloader interacts with the secure hardware extension (SHE+) module.

During the entire programming process, data is exchanged with the manufacturing execution system (MES). The latter is also responsible for transmitting the data to the OEM's electronic control unit (ECU) database.

After the programming is done, the chain of trust for the secure boot is configured. The ECU is now ready to be programmed with the application software.

With ProMik's product portfolio, all tasks of on chip security can be covered without any problems. This includes an integrated power supply with which the application can be easily controlled.



The steps of cyber security on chip.

# Encryption methods

Encryption methods are procedures of translating plain text into a string of characters with the help of cryptographic keys. A general distinction is made between public and private keys. The former are keys to which several parties have access. private keys are secret and only accessible to one communication partner.

[→ READ MORE](#)

Encryption methods are divided into symmetric and asymmetric methods.

symmetric methods are characterised by the fact that only one private Key is used for the encryption and decryption of the data.

With asymmetric methods, on the other hand, each communication partner generates its own key pair consisting of a public and private Key.

## Symmetric encryption

**AES**

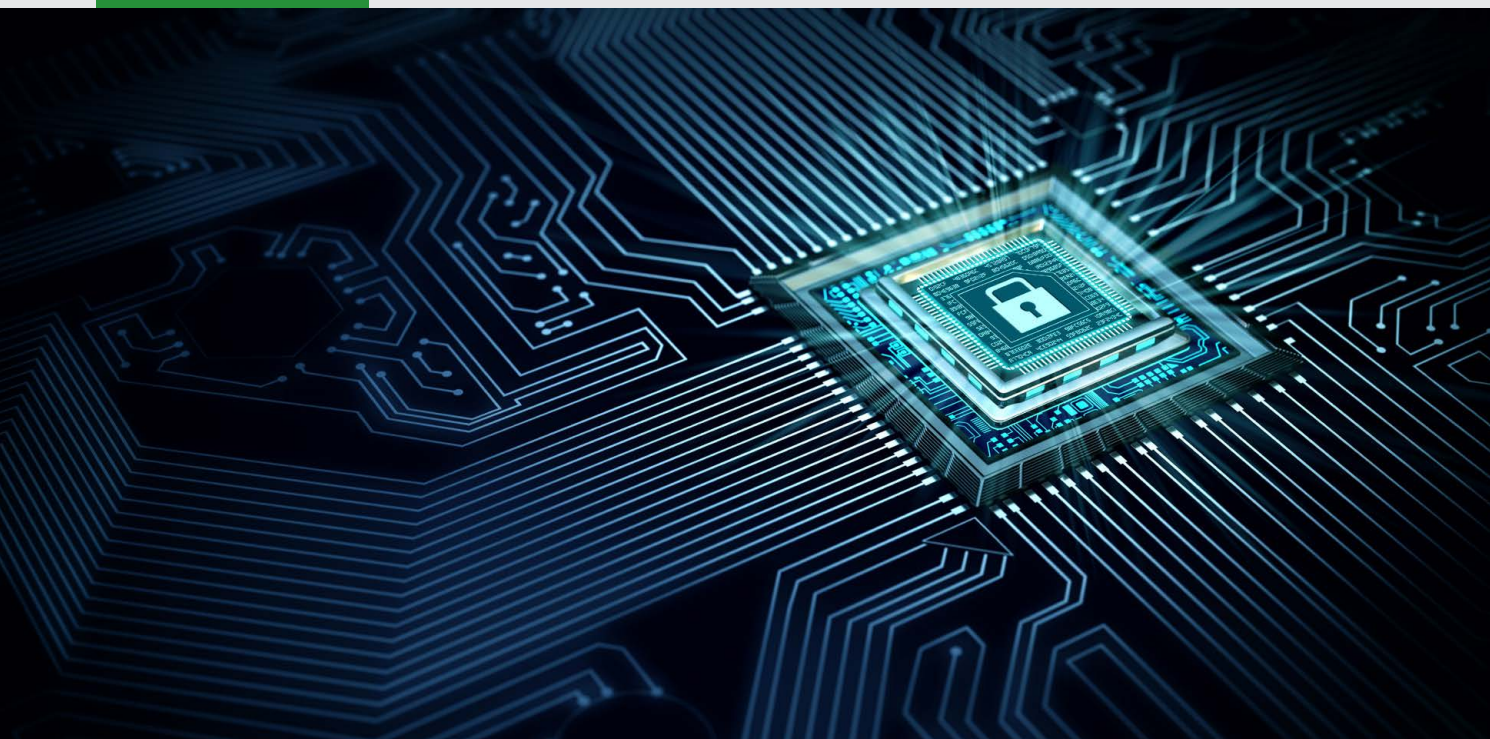
Advanced encryption standard (AES) is the successor of the likewise symmetrical encryption method Data encryption standard (DES). It is often used for encrypted data transfer as well as for internet protocol security (IPsec) and secure shell (SSH).



# Asymmetric encryption

## ECC

Elliptic curve cryptography (ECC) uses operations on elliptic curves over finite bodies. Since ECC is considered one of the most efficient methods, it is mostly preferred to other asymmetric methods.



## RSA

RSA is named after its inventor Rivest Shamir Adleman. After the keys have been generated, the public key is sent, which the recipient can use to encrypt the data. The public key is solely responsible for encryption, so it is useless on its own. The data can only be decrypted with the matching private key of the recipient.



# Keys for cyber security

Key lifecycle management (KLM) describes the creation, maintenance, protection and deletion of cryptographic keys. The process is divided into individual tasks.



The key lifecycle management

The relevance of the KLM is shown by the fact that keys lose their security over time. This is because more and more people have access to the keys, but also because they can become outdated or compromised. For this reason, the keys must be replaced regularly.

[→ READ MORE](#)

During key generation, the cryptographic keys are generated and then transferred to the production environment (key provisioning). There, the keys are stored, for example, in the HSM or SHE(+) (key storage) and used differently depending on the encryption method (key usage). The generation of new keys and replacement of invalid ones is called key rotation. Invalid keys are first revoked during key revocation and finally deleted (key destruction).

# ProMik: expert for cyber security in the electronics production

ProMik has been expert for flashing and testing in microelectronics for more than 25 years. Thanks to in-depth know-how and the homogeneous product portfolio, customers can implement state-of-the-art security mechanisms in their production.

↓ DATASHEET

Securing ECUs in production brings with it a number of challenges. Here, ProMik supports its customers and implements individual requirements taking into account current cyber security standards such as ISO21434. ProMik convinces with a holistic concept: from the determination of the security concept to the creation of the protection concept in the application.

As a result, ProMik has comprehensive technological knowledge about secure boot, security modules, key management and many other cyber security topics. With the plug & play solutions, it is also very easy to implement ProMik's solutions in the customer's production.

→ CONTACT



```
mirror_mod = modifier_ob.modi

# set mirror object to mirror_ob
mirror_mod.mirror_object = mi


if operation == "MIRROR X":
    mirror_mod.use_x = True
    mirror_mod.use_y = False
    mirror_mod.use_z = False
elif operation == "MIRROR Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif operation == "MIRROR Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end -add ba
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active =
print("Selected" + str(modifier_ob
#mirror_ob.select = 0
#one = bpy.context.selected_obj[0]
#bpy.data.objects[one.name].select
except:
    print("please select exactly

----- OPERATOR CLASSES
ror Tool
modifier_ob.se
bpy.context.se
print("Selecte

MirrorX(bpy.types.Operator):
"""This adds an X mirror to the selected
l_idname = "object.mirror_mirror_x", con
l_label = "Mirror X"
#bpy.data.obje

classmethod except:
ef poll(cls, context):
return context.active object
```



## Use case: cyber security implementation of an ADAS-application

In an innovative project, ProMik supported the realisation of a high-tech camera. The flashing, testing and cyber security implementation of the application were carried out. In the area of cyber security, ProMik convinced with its comprehensive service portfolio. This included the development of a special Bootloader, the programming of the HSM and much more.

### The difference in production

- Flashing, testing and cyber security out of one hand
- Encryption methods like e.g. RSA and ECC
- High-performance ProMik Bootloader

[→ READ MORE](#)

# Get to know more about cyber security in the electronics production

