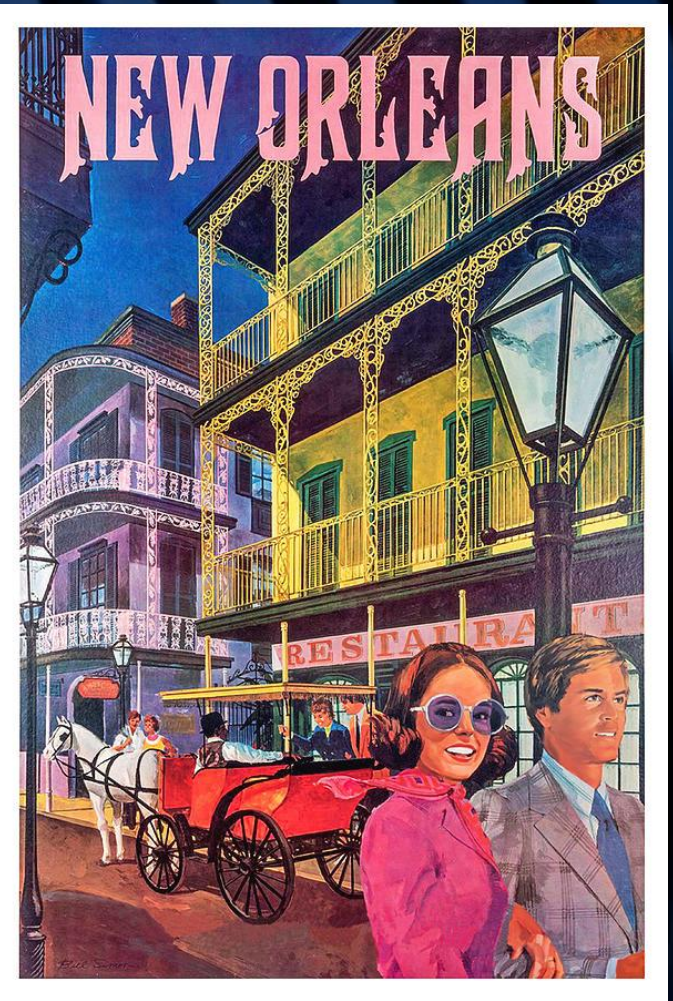
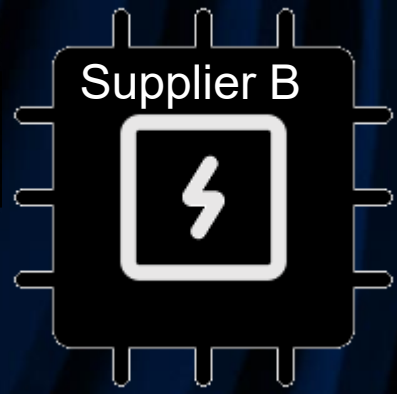
helicopter view of Key Management

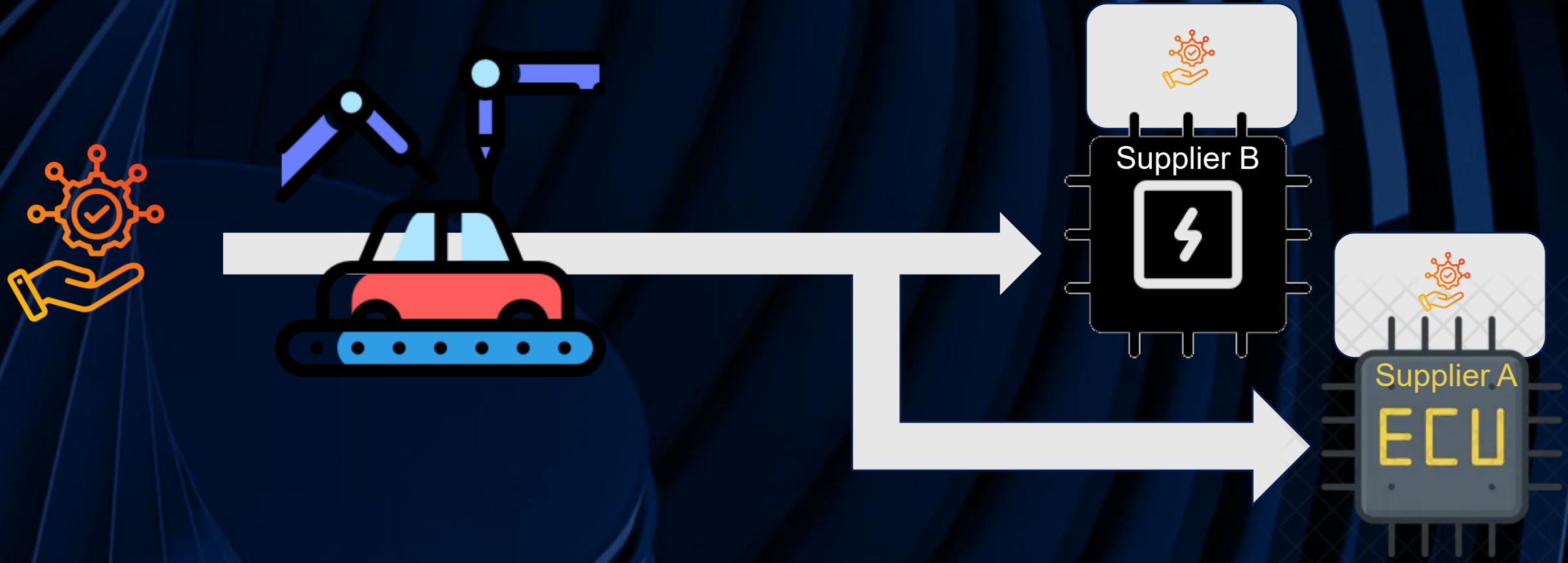


Main problem to solve (1/2)

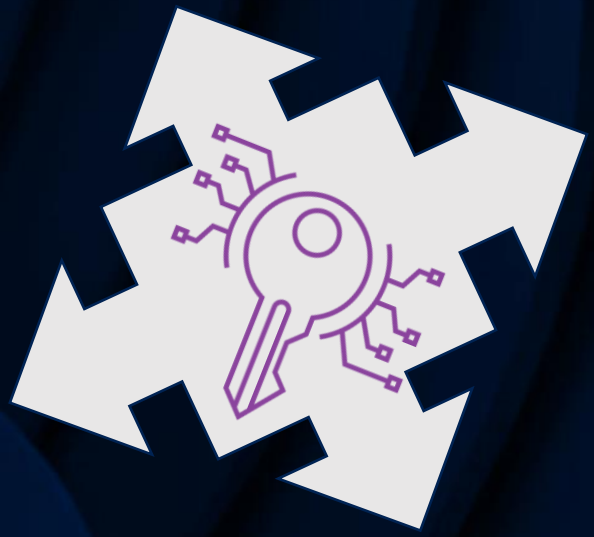


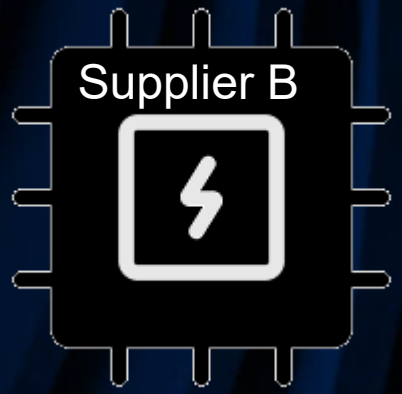
Main problem to solve (2/2)

May be even more complex



Key Management is needed across the supply chain





From the initial Keys To applicative Keys

Some basics

Some good practices

- One Key one purpose.
- Document and enforce key management policies.
- Don’t hard code keys

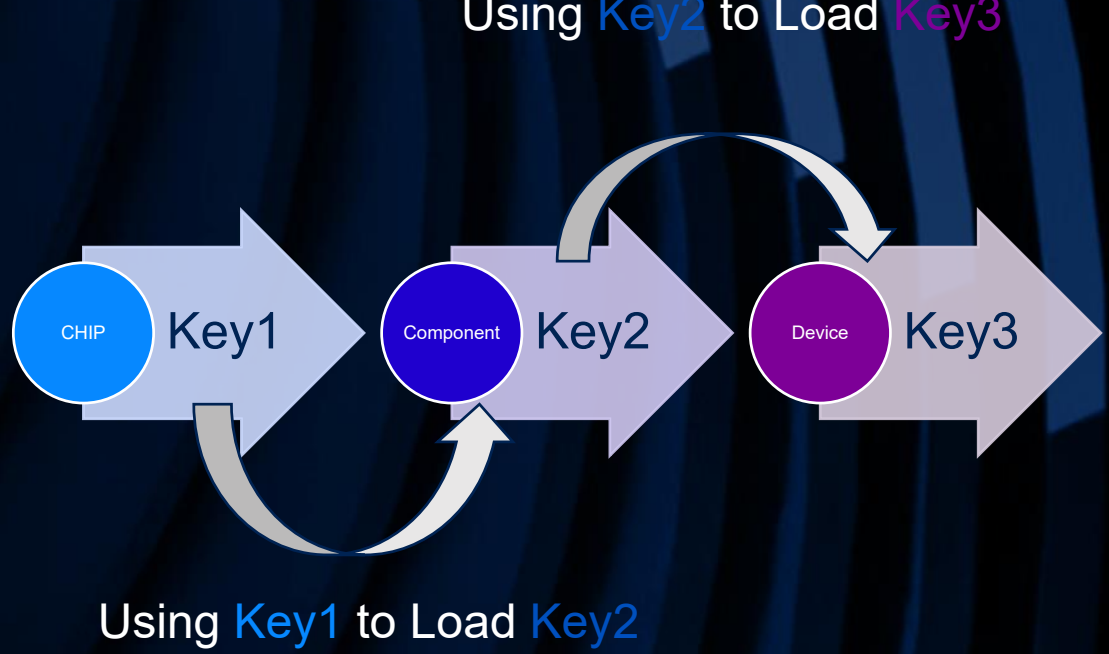
  Key should be updated , changed
- Use hardware security modules (HSMs) for key storage.
- Use key management systems (KMSs) to automate tasks.
- Include in your 21434 procedure
  - –Conduct regular audits
  - –Create a disaster recovery strategy
  - –Inventory your keys and document usage.

Key Rotation a tool to manage supply chain control

Key rotation is the process of replacing old cryptographic keys with new ones.

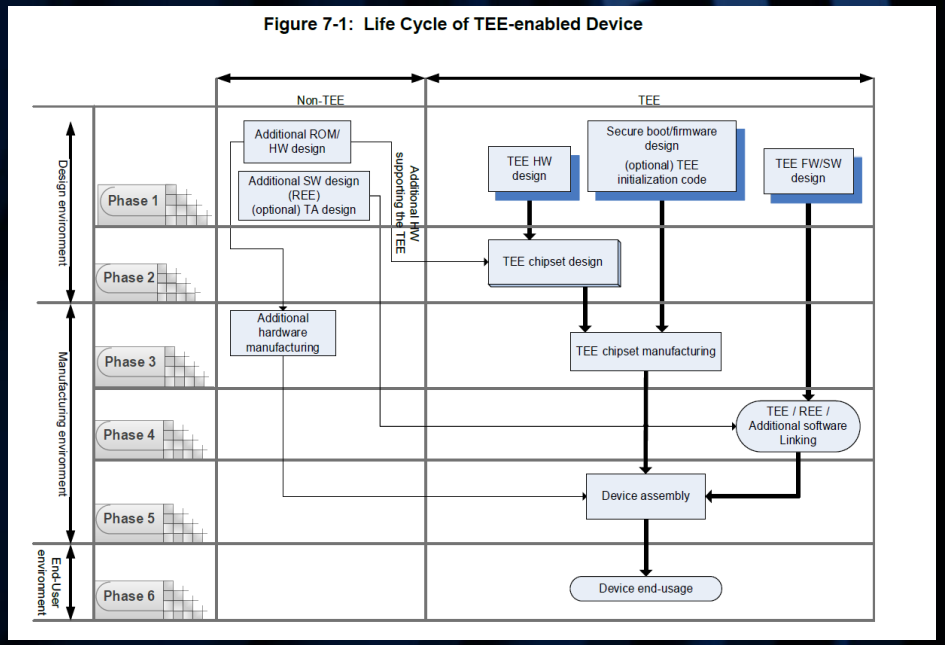
Key Rotation is used to transfer ownership across the supply chain

This is also done on a regular schedule or in response to specific events, such as a suspected security breach



ROT Keys <> Applicative Keys

GlobalPlatform ROT Definitions and requirements defines the ROT implementations



If you have ROT Services , it's possible to load securely applicative Keys

Different solutions for ROTs Keys

Hardware Trouud

Sallicipuce Trouls

Hardvare Troips

Discoloucke wily Atttaks

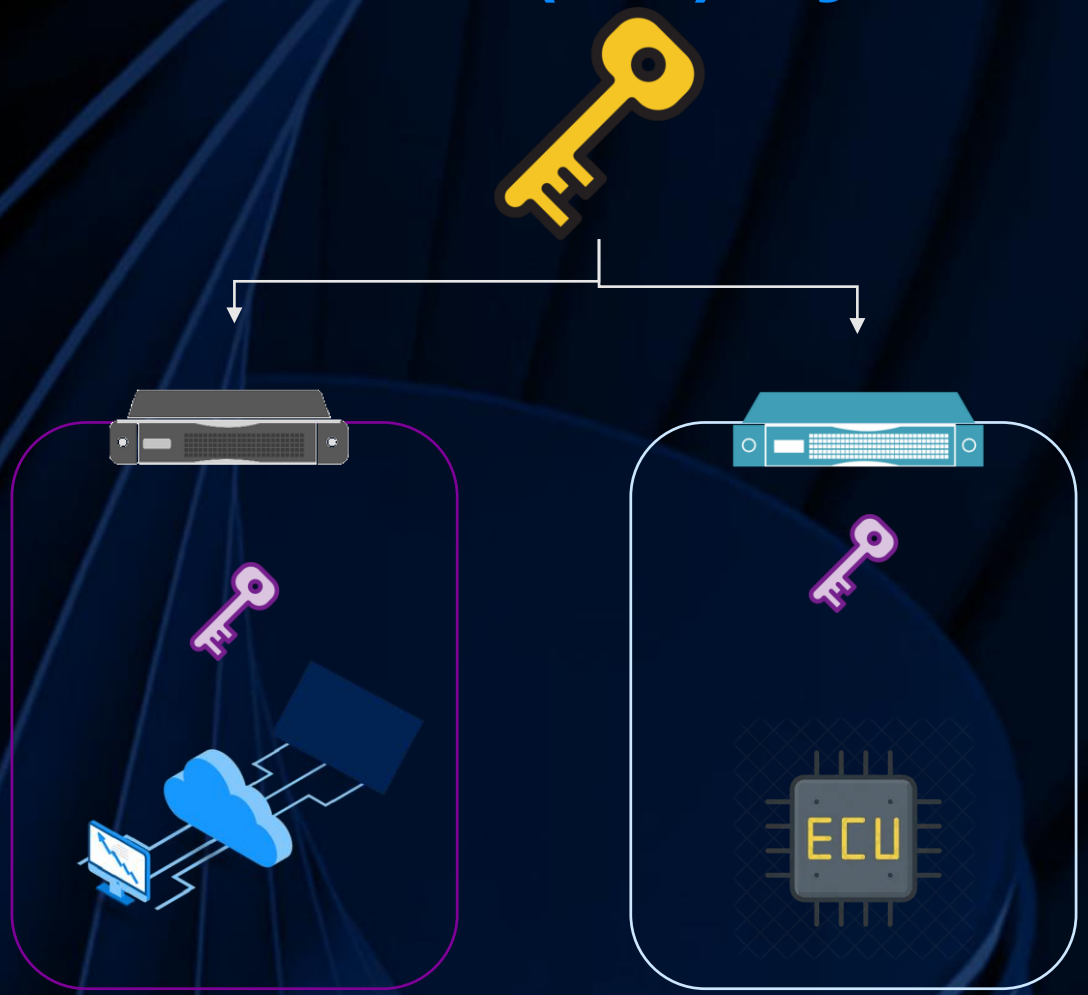
Crptoaphic strond

Sondvrnoe vehlle and

Key Initmephiic Attack

Global Platform™

Solutions (1/3) Symmetric Keys



Use a Symmetric Master Key

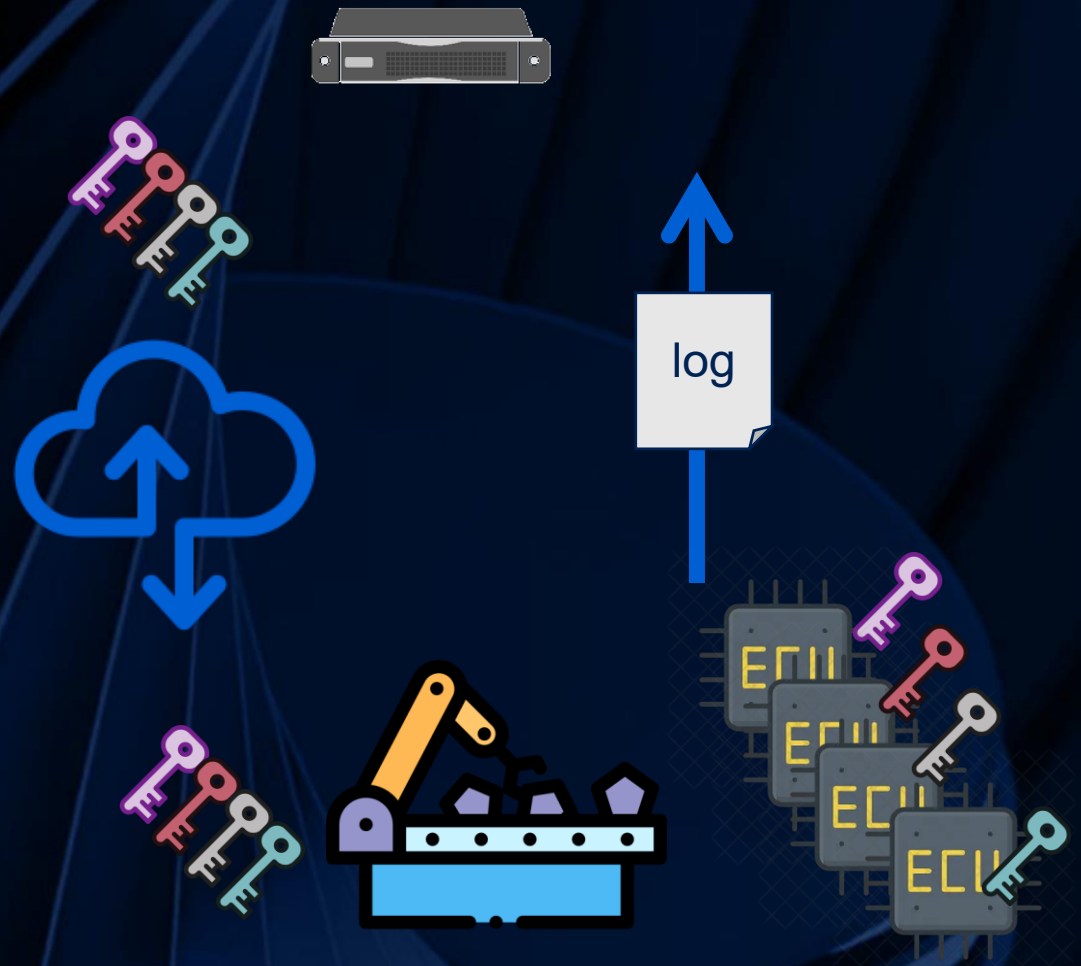
This master Key is store in a HSM

Derived Keya are generated based on algorithm that uses information of the specific ECU and the master Keys

ECU providers are loading the derived Key in the specific ECU

Car OEM are able to open a secure connection with the ECU using another HSM (with the same master Key and the same derivative algorithm)

Solutions (2/3) Load Keys/certificate



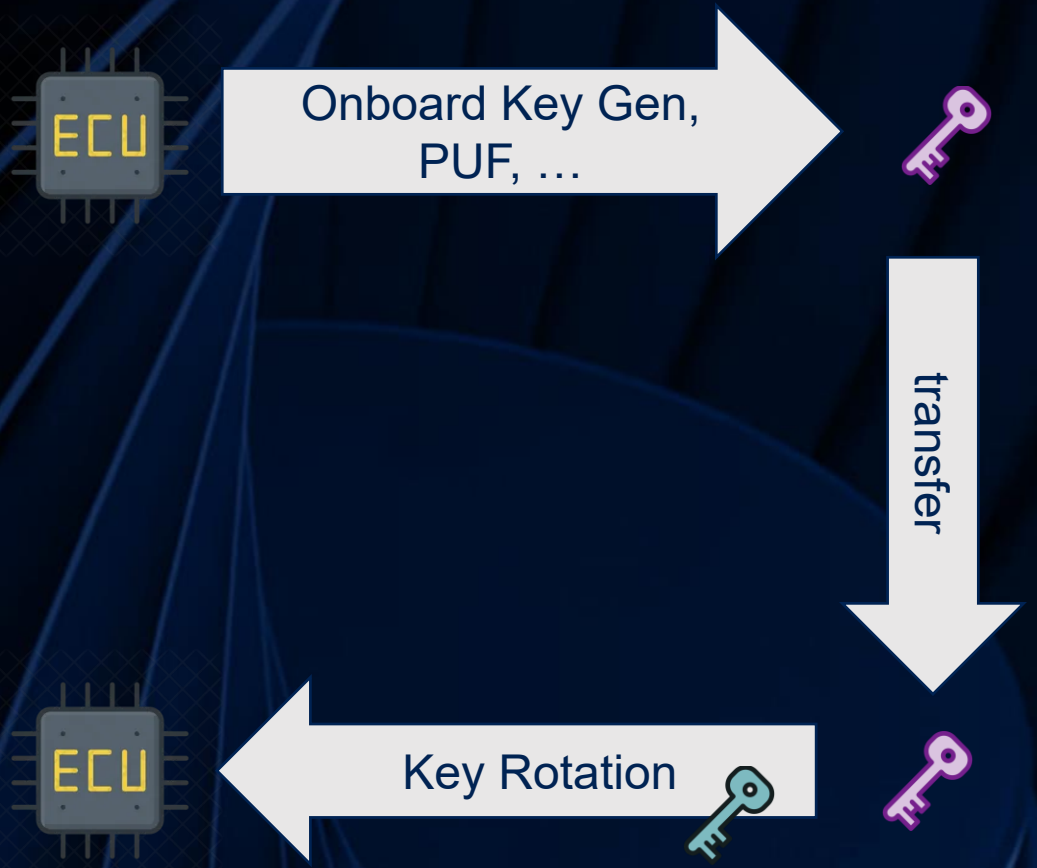
Generation of batch of Certificate or Key

Send to all Keys in a protected manner to the production center

During the production flow, load one Key in one specific Device

Give a log with the Key information and the specific device ID for management

Solutions (3/3) on board generation



You can use internal chip capability to generate primary keys

But you'll need to transfer the Key or the information about the Key to enroll this component

Then you can use

- key rotation mechanism to change theses primary Keys
- or load new keys

Next ?

In the context of the

- SDV ,
- with regular update
- Across multiple actors
- with the PQC migration soon to arrive

- A guideline for Key management in the automotive market may be a good tool to help this industry to face all problem and help standardizing this complex environment

Global Platform™

Membership
membership@globalplatform.org

PR Contact
pressoffice@globalplatform.org
+44 (0) 113 350 1922

Questions
secretariat@globalplatform.org

→ globalplatform.org