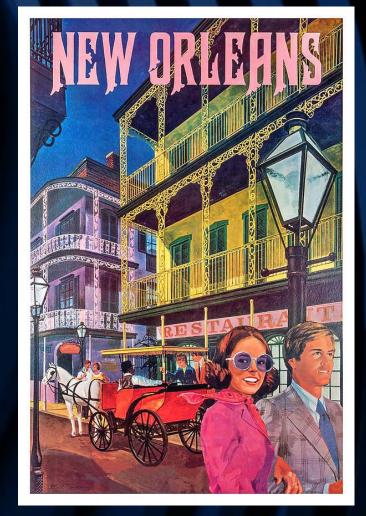


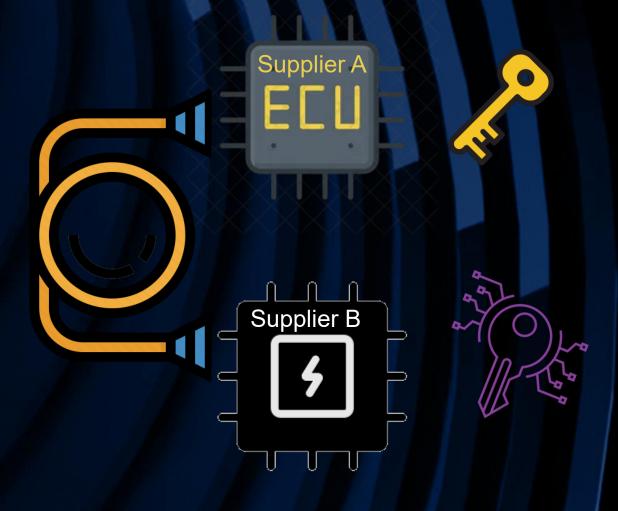
helicopter view of Key Management





Main problem to solve (1/2)





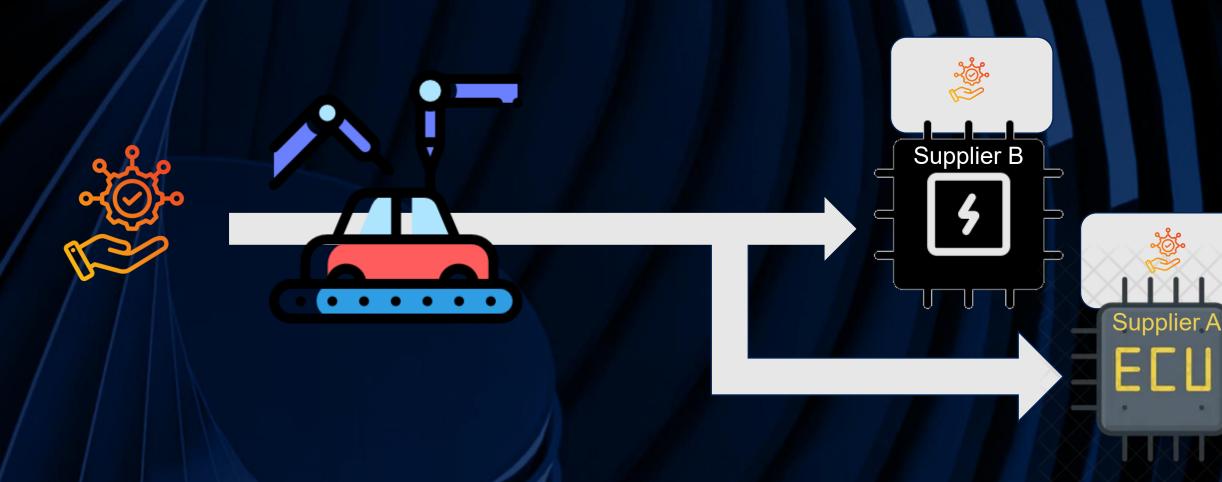


Main problem to solve (2/2)





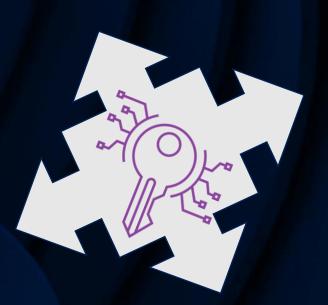
May be even more complex





Key Management is needed across the supply chain

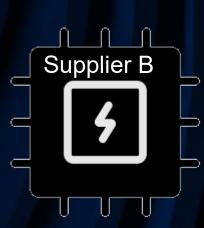






From the initial Keys
To applicative Keys









Some 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

Using Key to Load Key1 Key3 Key2 Component Device

Using Key1 to Load Key2



ROT Keys <> Applicative Keys



GlobalPlatform Technology

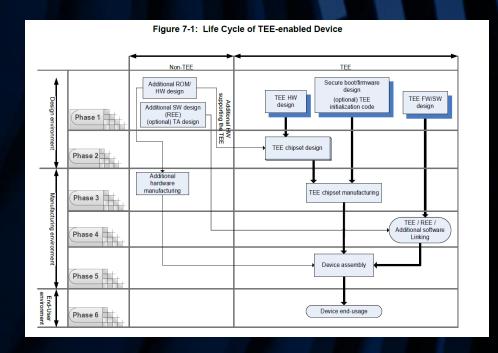
Root of Trust Definitions and Requirements

Version 1.1.1

Public Release June 2022

Document Reference: GP_REQ_025

GlobalPlatform ROT Definitions and requirements defines the ROT implementations



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

Copyright & 2014-2022 GlobelPfatform, Inc. All Rights Reserved.
Reciplents of this document are invited to submit, with their comments, notification of any relevant palents

Recipient of this document are involved to submit, with their comments, notification of any relevant patients or other intelligents properly digits (operating). They give the property of which they may be assess which might be necessarily intelligent by the implementation of the specification or other work product set forth in this document, and to provide supporting documentation. The storthough provided or described herein is subject to updates, revisions, and extensions by Global-Platform. Use of this Instrumation is governed by the Global-Platform locance agreement and any use locansistent with that greeners it is strictly prohibited.

Different solutions for ROTs Keys





Sallicipuœ Trouls



Hardvare Troups



Crpptoaphic strond

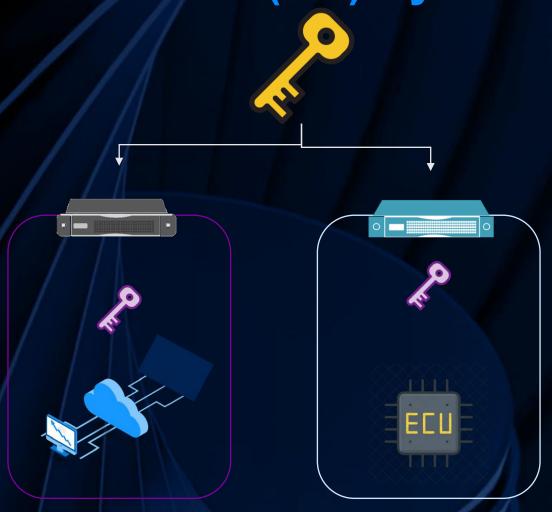


Sondvinge vehill and





Solutions (1/3) Symmetric Keys



Use a Symmetric Master Key

This master Key is store in a HSM

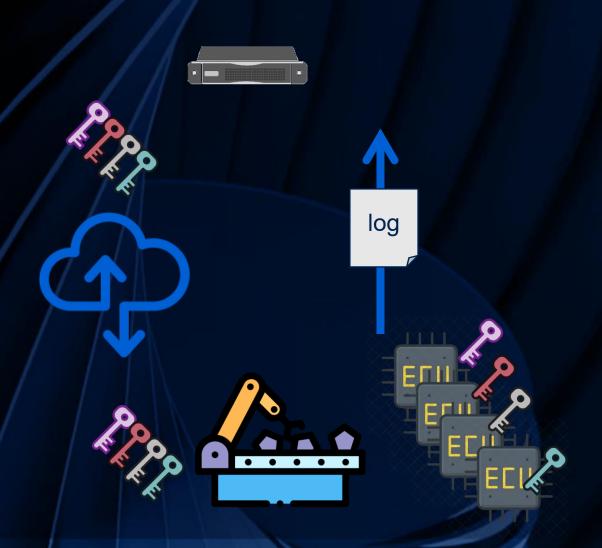
Derived Keya are generated based on algorithm that uses information of the specific ECU and the master Keys

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

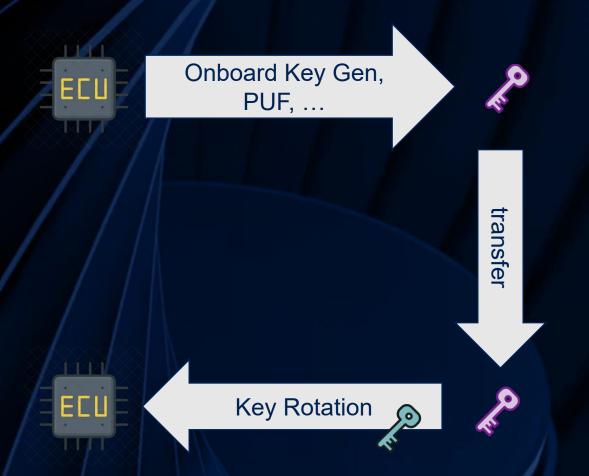
Send to all Keys in a protected manner to the production center

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





Membership membership@globalplatform.org

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

Questions secretariat@globalplatform.org

→ globalplatform.org









