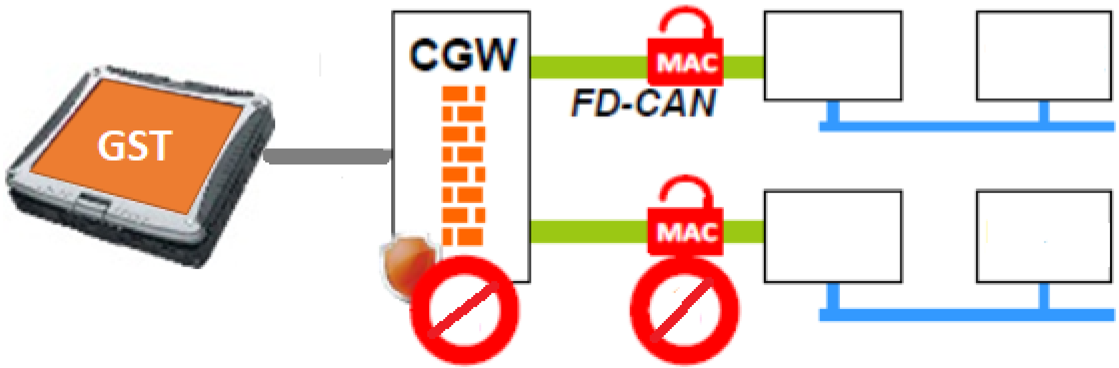
How to replace MAC ECUs

Nissan Motor Co., Ltd.

What is MAC ?

- MAC = Message Authentication Code
- Objectives:
  - Secure communication sending through CGW (gateway)
    - **Diagnostic communication not applied, only in-vehicle communications**

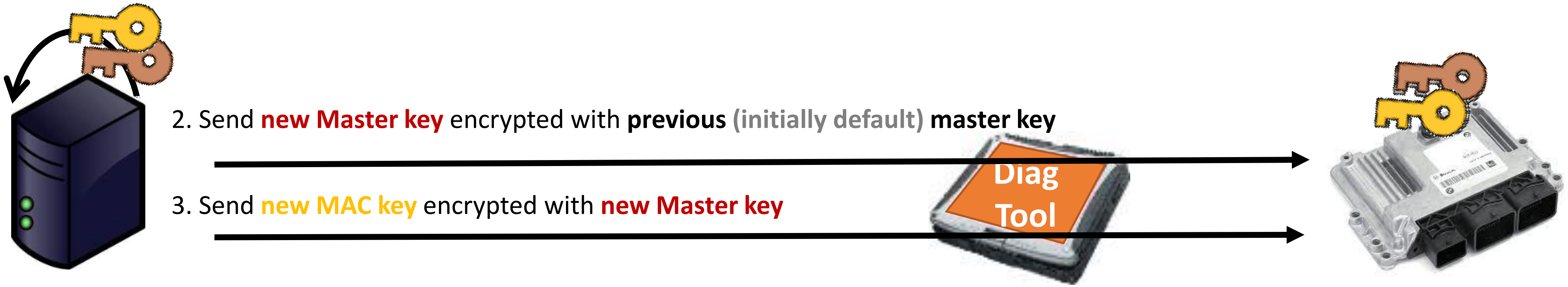
➔Sign the messages with a **key** shared between the ECUs* connected to CGW



What about the keys?

- 2 keys per MAC ECU
  - 1 for **MAC computation**, unique for each vehicle (linked to VIN) → **MAC Key**
  - 1 for **key provisioning**, unique for each ECU (linked to VIN+ECU type)→ **Master Key**
  - All ECUs are shipped with **default** MAC and Master keys

1. Compute **MAC key** & **Master key**



2. Send **new Master key** encrypted with **previous (initially default) master key**

3. Send **new MAC key** encrypted with **new Master key**

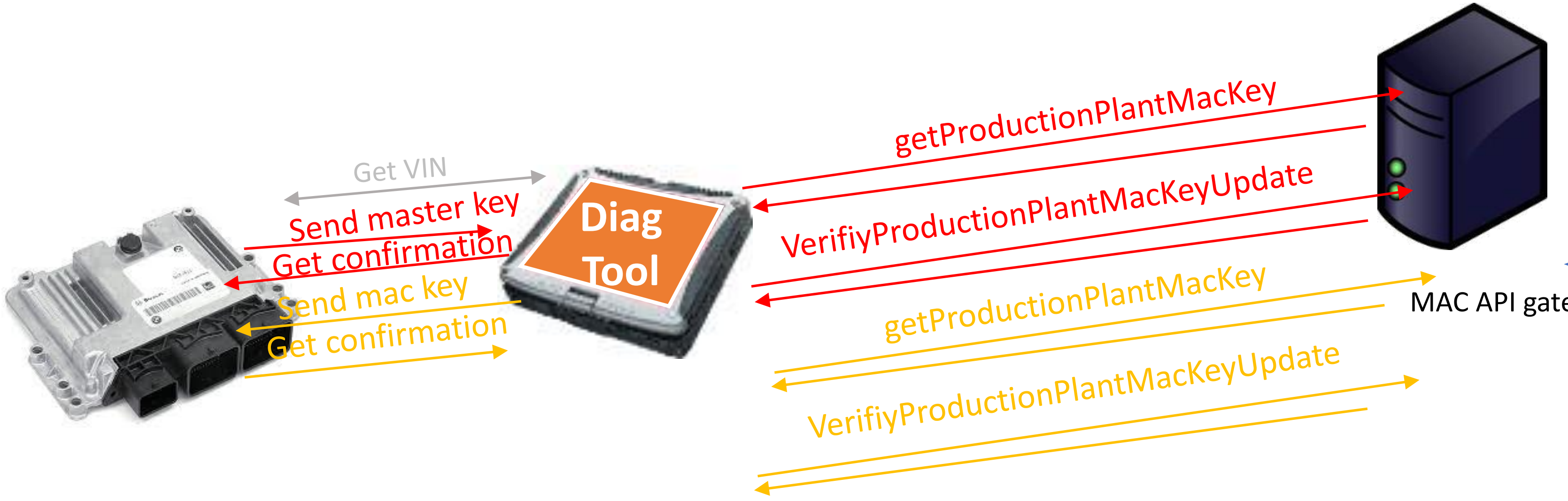
MAC API Gateway

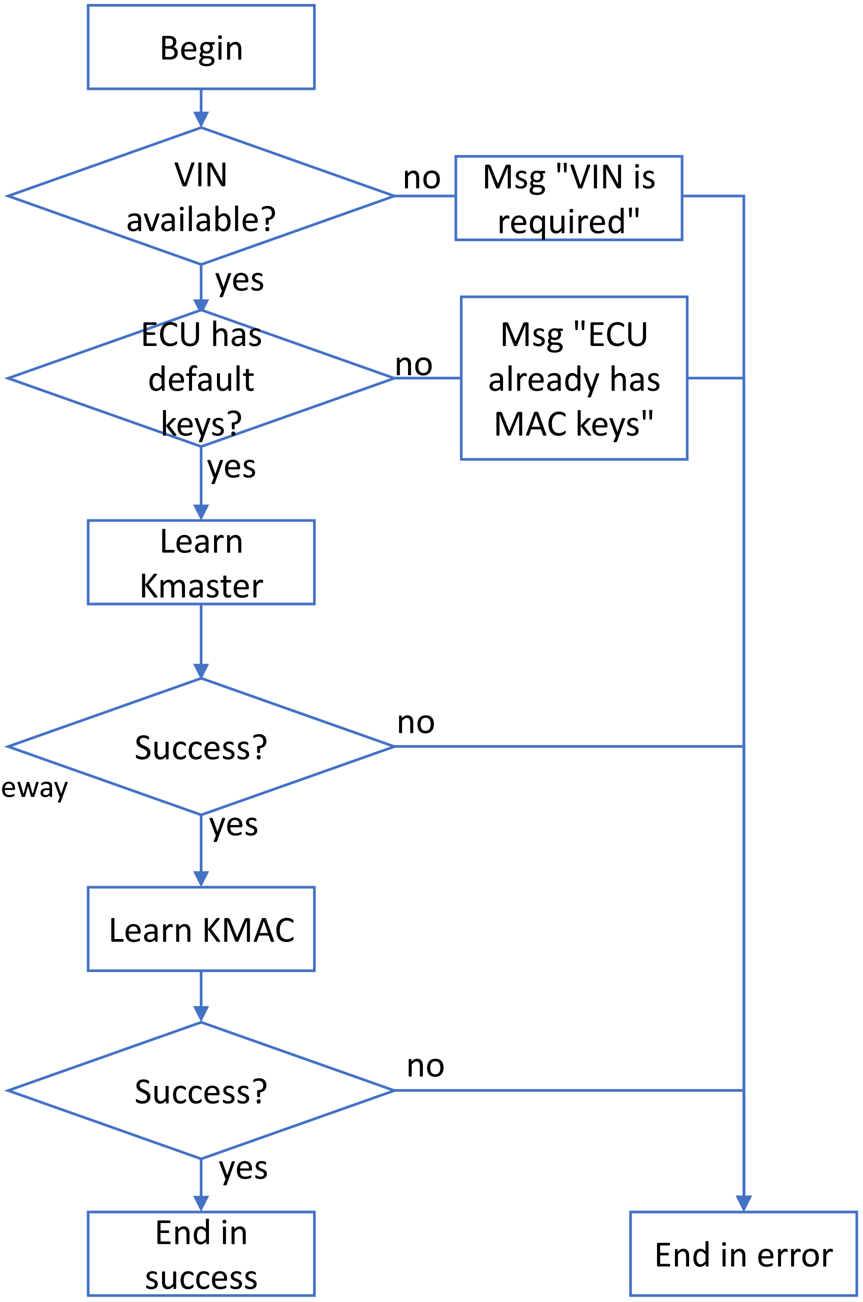
ECU

How to replace a MAC ECU?

MAC ECU needs to update keys to authenticatiton in-vehicle communication with other MAC ECUs.

Communication sequences with relavant command & parameter to be disclosed along with Diagnostic communicatin disclosure to ETI





0: Replace ECU&Get Vehicle VIN

1: Download master key into ECU & check if download successful

2: Download MAC key into ECU & check if download successful