ISO TC22/SC31/WG2

Authentication, Authorization, and Secure Diagnostic Communication

Jean-Baptiste Mangé

DRIVE THE CHANGE

RENAULT

Secure diagnostic objectives

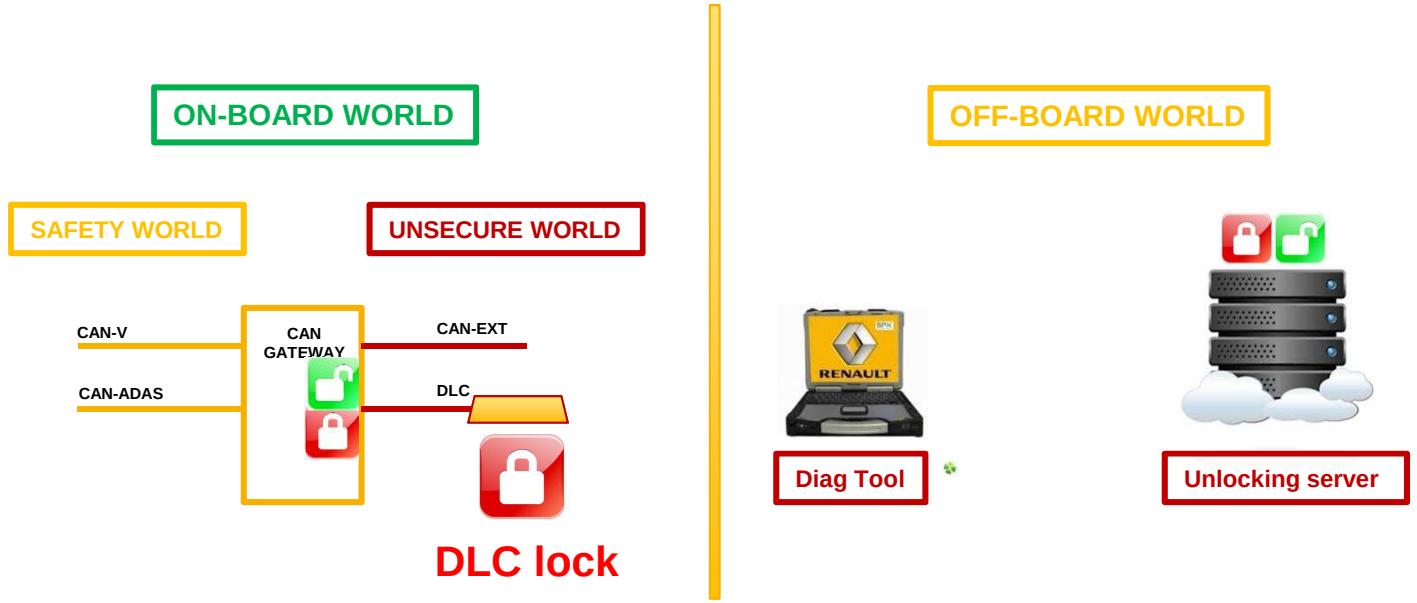
- **Restrict access to legitimate privileged functions**
  - Malicious usage of diagnosis functions directly leads to code execution, denial of services, or any tampering
  - Restricting their usages through any vectors is a strong priority

- **Authenticate legitimate devices and users**
  - Need to define what are the legitimate devices and users
  - And also roles and related rights
  - Defining a security policy for diagnosis devices and related users is a key aspect to avoid any intrusive solution on vehicle design or development planning

- **Accounting**
  - Proofs for inforensics and live-monitoring (Security Operation Center)

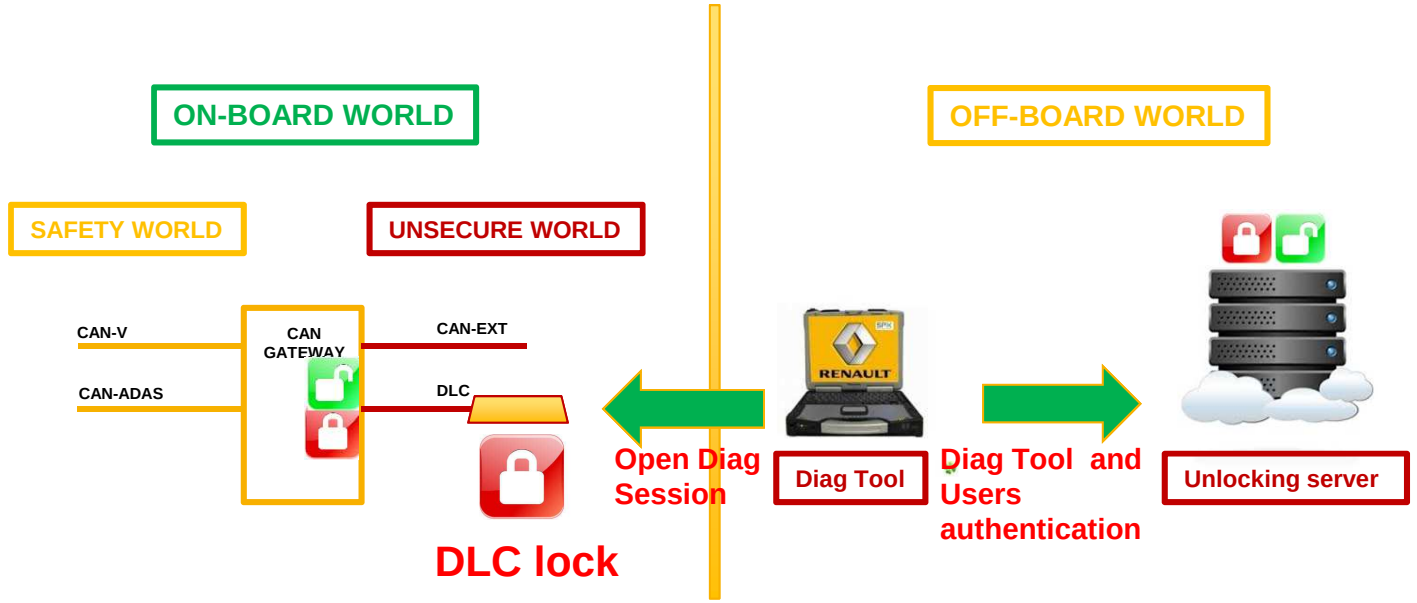
Secure diagnostic – Actual workflow

- **CAN Gateway isolates DLC port**
- **In normal conditions the DLC port is closed**
  - Only few UDS services are available (read DTC, read parameters, …)
  - All other services are filtered-out by the CAN Gateway (Deep Packet Inspection)



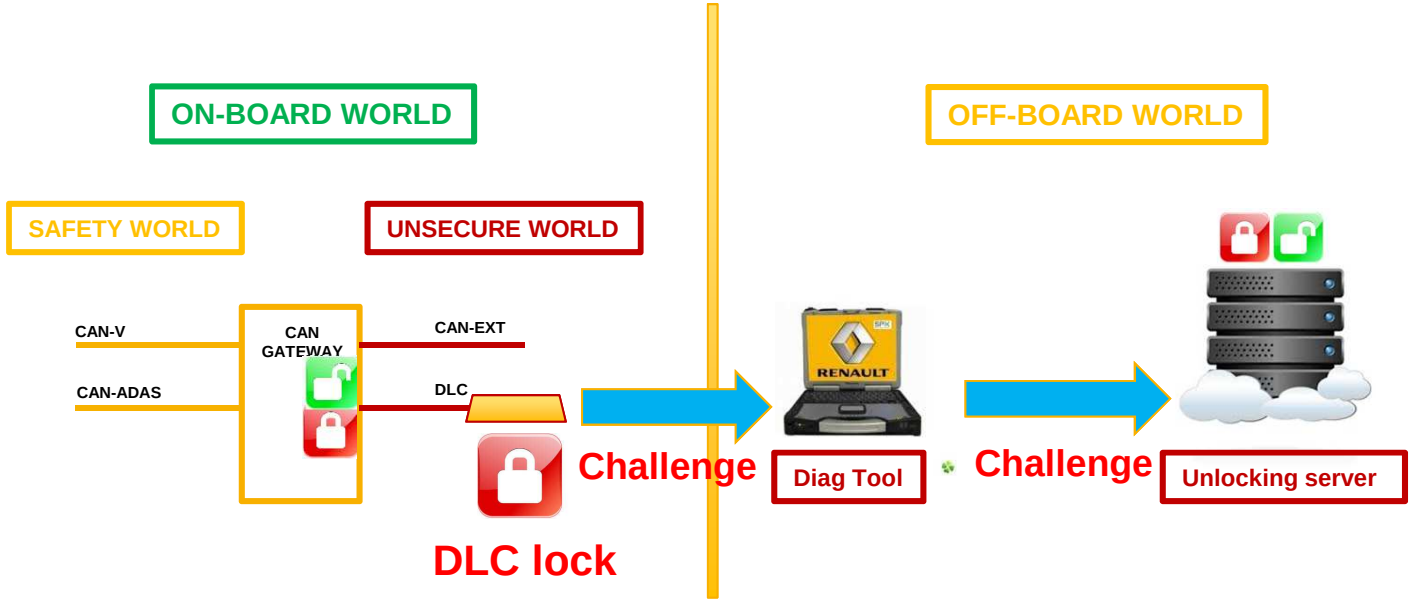
Secure diagnostic – Actual workflow

- **To perform advanced diagnosis operation the Diag Tool must connect to the Gateway to retrieve a challenge**
- **And must connect and authenticate itself on the Unlocking Server**



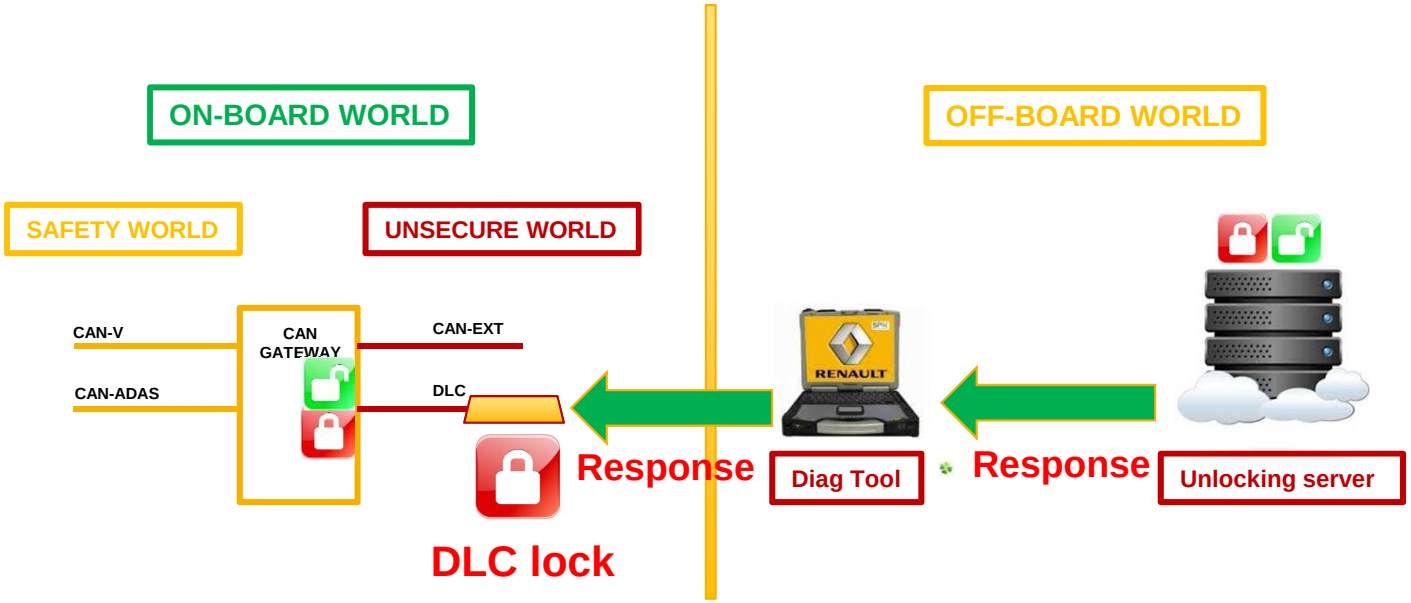
Secure diagnostic – Current workflow

- **The GTW challenge is send to the Unlocking Server (OEM property)**
- **This Unlocking server:**
  - Authenticates the Diag Tool and the repairer
  - Generates the challenge signature
  - Logs the activity (information on Diag Tool, the repairer, and the Gateway)



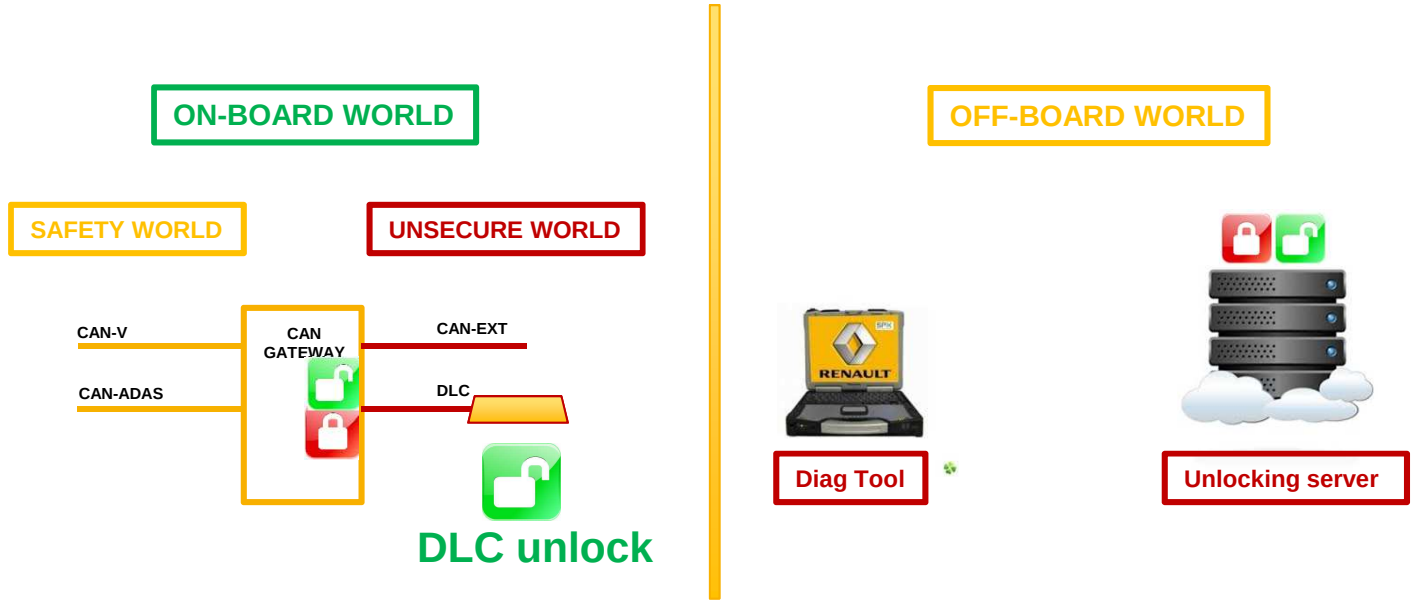
Secure diagnostic – Current workflow

- **The Diag Tool forward the Response (Challenge + Signature) to the Gateway**
- **The Gateway validates the signature**



Secure diagnostic – Current workflow

- **If the signature is validated the Gateway switch in the Diag mode**
- **In this mode:**
  - All UDS operations are granted
  - Other ECU could be reached and unlocked if necessary



Standard Secure diagnostic objectives

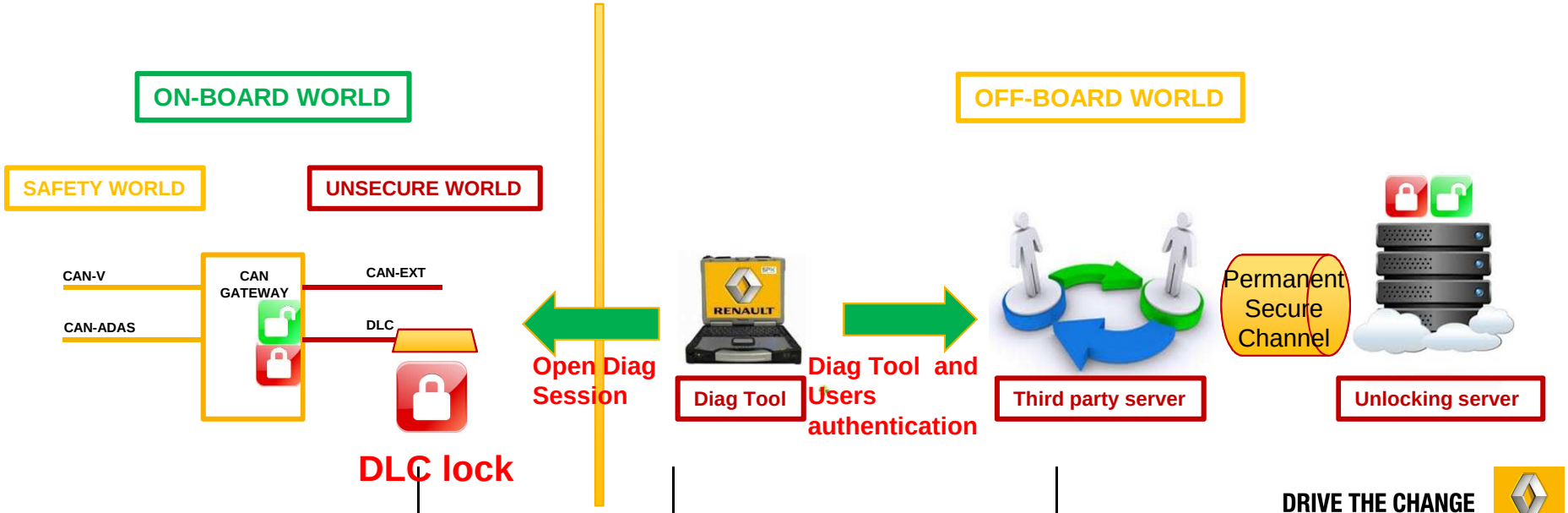
- **Secure diagnostic objectives**

+

- **Hook for legislator**
- **Hooking on this kind of process has two main advantages:**
  - It enables third party to take control of users and devices authentication easily
  - It avoid to mix OEM ‘s legacy solutions with new legal constraints

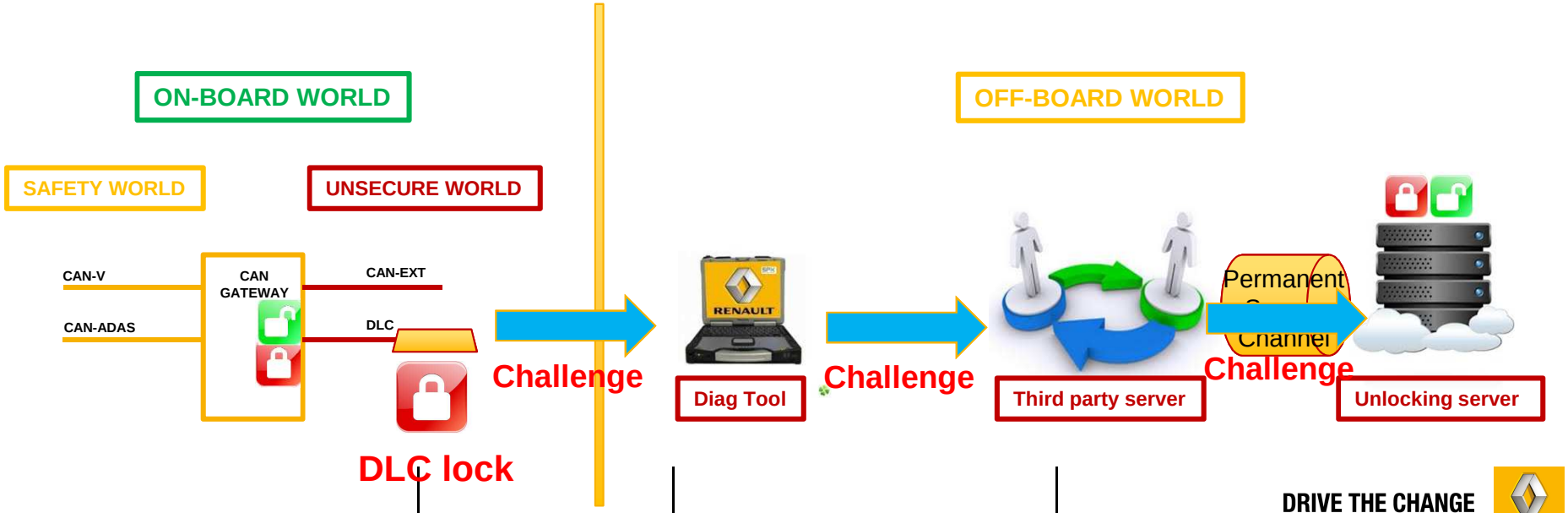
Standard Secure diagnostic – Expected workflow

- **Third Party Server takes place in the solution**
- **The Third Party Server :**
  - Has a permanent secure channel established with the Unlocking Server of each OEMs
  - Could submit challenge to these Unlocking servers
  - Is responsible of the authentication of all legitimate tools and repairers



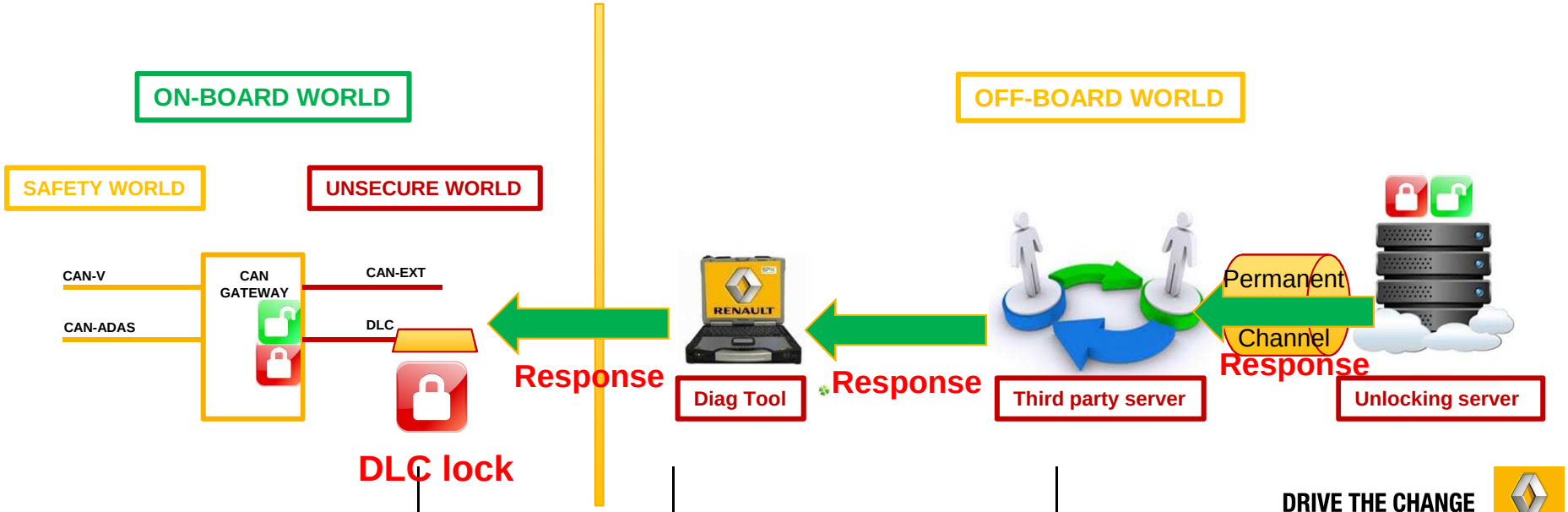
Standard Secure diagnostic – Expected workflow

- **The GTW challenge is send to the Unlocking Server (OEM property) through Third Party**
- **No modification on Unlocking server to manage the signature**



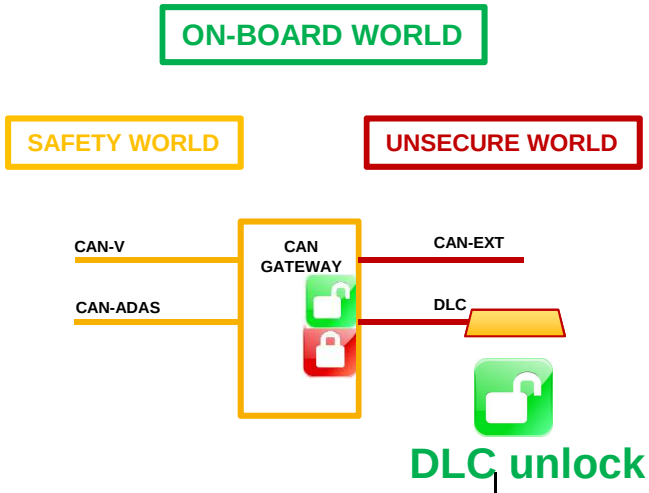
Standard Secure diagnostic – Expected workflow

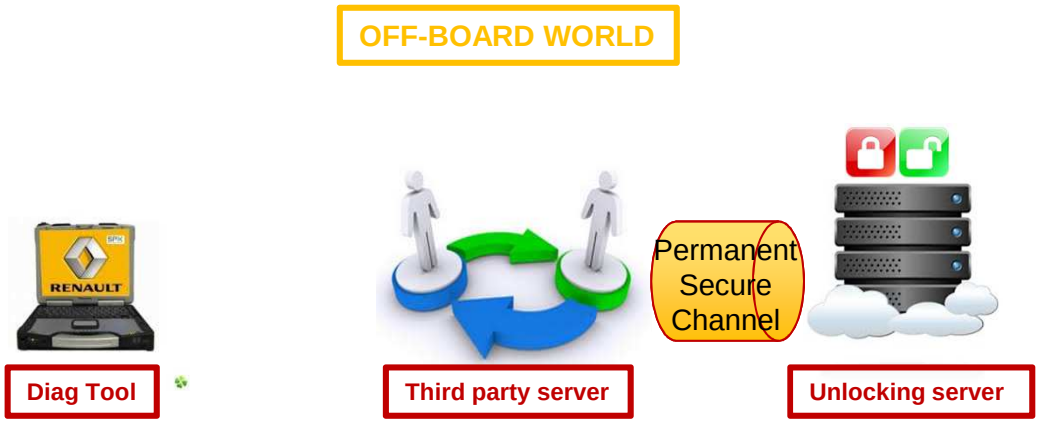
- **The Diag Tool forward the Response (Challenge + Signature) to the Gateway**
- **The Gateway validates the signature**



Standard Secure diagnostic – Expected workflow

- **If the signature is validated the Gateway switch in the Diag mode**
- **In this mode:**
  - All UDS operations are granted
  - Other ECU could be reached and unlocked if necessary





Keys elements for success

- **Unanimity on general objectives**

- **Inventory of all constraints and specific needs**

- **Road-map**
  - Example of high level road-map from minimal solution to the full-complete scenario
    - Step 1 : Implement third party to authenticate Diag Tool and Repairer
    - Step 2 : Introduce role and privileges on GTW
      - Challenge signature for Repairer grant a specific access level
        - » E.g. Could have access to reflashing
      - Challenge signature for Technical Control grant an another level
        - » E.g. Could use IO Controls but not performing reflashing
    - Step 3 : Management of proofs
      - Audit logs for third party inforensics

FIN