|  |  |
| --- | --- |
| **Title：** | **Peripheral Provision (Ford cloud)MRD** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Document Owner** | **Changes** |
| <0.1> | 2020-02-24 | 刘晨曦 | 初稿 |
| <1.0> | 2020-02-27 | 刘晨曦 | 修改完善部分描述  内部评审完成后, 升级版本号至1.0,发送福特客户确认签署 |
| <1.1> | 2020-02-28 | 刘晨曦 | 按照福特客户评审意见, 修改部分描述:  - 删除认证状态中自检未完成的描述  - 完善中控主机发送设备元数据的条件描述 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目录

1 需求介绍 3

2 需求内容 4

2.1 车型配置及差异 4

2.2 需求概述 4

2.3 需求详述 6

2.3.1 交互架构 7

2.3.2 认证状态 7

2.3.3 认证过程 9

2.3.3.1 中控主机发送设备元数据 9

2.3.3.2 ECG设置中控主机认证状态 10

2.3.3.3 ECG广播认证状态 12

2.3.4 交互数据 12

2.3.5 电源管理相关 14

2.3.6 网络通道功能 14

# 需求介绍

本文档用于整理中控主机通过福特后台进行设备认证的相关需求，参考福特提供如下文档:

* Peripheral Module Provisioning SPSS v1.4.pdf
* Peripheral Module Provisioning APIM Imp Guide v1.4 July 30, 2019.xlsx

以及前期调研过程中, 福特同事和DSV就需求相关问题的沟通记录文件

* Ford Project Q&A list.XLSX

# 需求内容

## 车型配置及差异

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | CD542 | | CX727 | U725 | P702 | U554 | U625ICA |
| 功能 | Ambient/Trend | Titanium/ST Line | Mid/High | Ford Bronco SUV | Ford Raptor F-150  Pickup truck | Lincoln Navigator  Large SUV (3 row seat) | Explorer |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

所有车型均包含此功能，可视为无功能差异

## 需求概述

Provision功能, 中文表达可称之为设备设备认证, 其主要目的是为了对每台设备通过其特有的属性进行标记, 以识别该设备, 作为车辆中装配件关联管理, 基于设备的服务鉴权以及后续个性化服务的基础.

在福特相关需求文档描述中, 中控主机的设备认证涵盖多个逻辑部件, 每个部件在认证过程中承担不同的职责, 包括:

|  |  |  |
| --- | --- | --- |
| **Logical Class** | **Physical Module (ECU)** | **Responsibility** |
| ProvServer | ECG | 车辆内部负责设备认证的主控设备, 和中控主机进行交互 |
| ProvOnBoardClient2 | SYNC | 中控主机的逻辑职能之一, 负责提供WiFi通道, 以便ECG和后台进行交互 |
| ProvOnBoardClient3 | Peripheral ECU (SYNC/OBCC/DSRC) | 中控主机的在本文档范围内主要逻辑职能, 负责和ECG通过以太网就设备认证功能的相关交互 |
| ProvOffBoardClient1 | UPG Cloud | 福特后台, 和中控主机无直接关联 |
| ProvOffBoardClient2 | Regional/Home Cloud Instance | 福特后台, 和中控主机无直接关联 |

一般情况下, ECG使用TCU的蜂窝数据网络或者WiFi连接后台.



当作为广域网网络通道的TCU不可用时, ECG也可以通过SYNC的WiFi通道连接后台.



需要特别说明的是, 这里的ProvOnBoardClient2和ProvOnBoardClient3在上图中虽然是两个逻辑部件, 但物理上是同一实体, 即中控主机(SYNC).在这此框架中, 作为网络通道部件的ProvOnBoardClient2仅提供数据的透明传输, 对数据内容不做逻辑判断和处理.

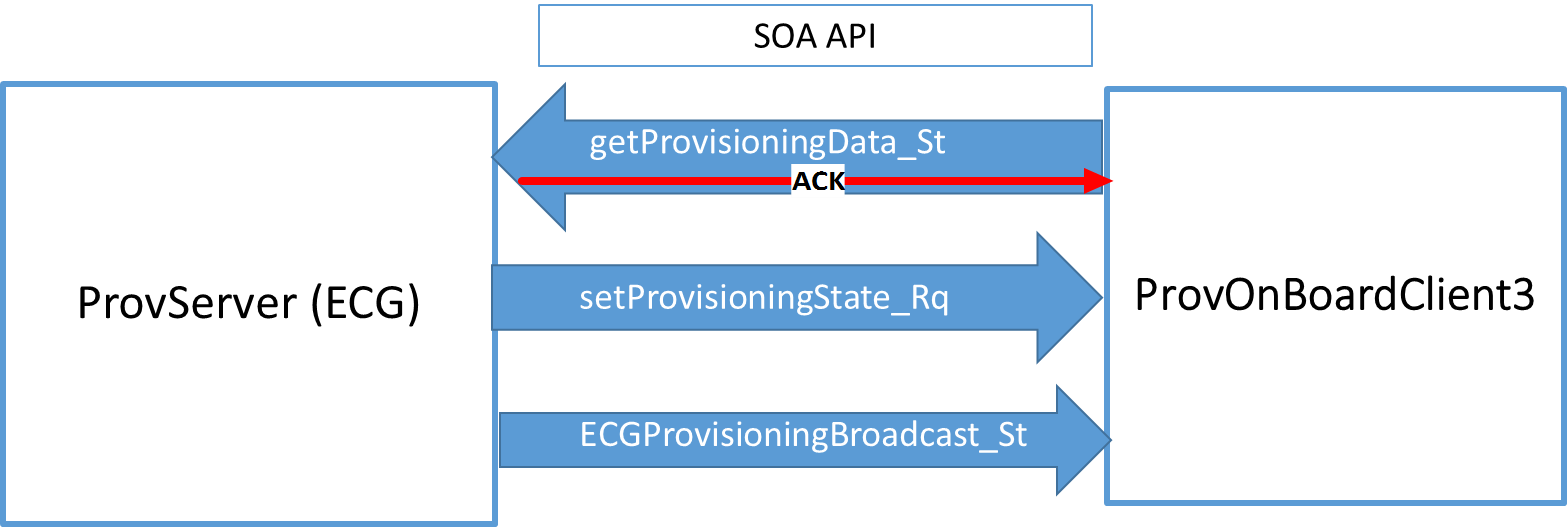
基于以上系统边界分析, 本文档将中控主机和关联部件(ECG)的交互过程进行整理, 以作为后续功能开发的依据和基础.



## 需求详述

### 交互架构

福特CVPP平台架构中, 中控主机和ECG使用以太网进行交互. 认证功能交互过程如下



包括三个步骤:

1. 中控主机发送设备元数据
2. ECG设置中控主机认证状态
3. ECG广播认证状态

据后续章节将对每一步骤进行详细描述

### 认证状态

中控主机的设备认证过程中, 需要记录认证状态. 共包括四种可能的取值:

|  |  |  |
| --- | --- | --- |
| **State** | **Value** | **Description** |
| FactoryMode | 0x38 | ECU is not Configured |
| Unprovisioned | 0x39 | ECU Configured |
| ECUProvAlertACK | 0x3A | ECU is waiting for Provisioning Alert Ack from ECG |
| ECUProvisioned | 0x3B | ECU Provisioned |

状态迁移条件如下图所示:

认证状态迁移如下图所示



中控主机需要持久化存储本机的认证状态, 且不因软件空中升级而发生变化.

### 认证过程

#### 中控主机发送设备元数据

在满足如下任意一种条件情况下, 中控主机需要以5S为周期, 通过“getProvisioningData”消息向ECG发出设备认证状态以及认证元数据.

* 上电
* 引擎启动
* 认证状态变更

发送需持续进行, 直到收到ECG发来的ACK

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |
| **Method Type** | | Periodic | | | | |
| **QoS Level** | | Default | | | | |
| **Retained** | | Yes | | | | |
|  | | | | | | |
| **R/O** | **Name** | | **Type** | **Literals** | **Value** | **Description** |
| **Request** | | | | | | |
| - | - | | - | - | - | N/A |
| **Response** | | | | | | |
| R | ECU\_ProvDID | | Enum | - | - | To indicate the provisioning state of the Peripheral ECU |
|  |  | |  | Factory Mode | 0x38 | Peripheral ECU is not Configured |
|  |  | |  | Unprovisioned | 0x39 | Peripheral ECU Configured, Self-Test not complete |
|  |  | |  | ECU Provisioning Ack | 0x3A | Peripheral ECU Configured, Waiting for ACK |
|  |  | |  | Provisioned | 0x3B | Peripheral ECU Provisioned Mode |
| R | ECUFESN | | String | - | 8 chars. | ECU Ford Serial Number |
| R | ECUProvisioningData  Secure | | Bytes | - | The max allowed by GPB | Specifies GPB encoded ECU Provisioning data signed with ECU SyncP key.  Refer to Rqmt PMPR-Req-348833 and **PMPR-REQ-354876/A** for details of the attributes that shall be included in the payload, |
| R | PayloadType | | Enum | - | - | Specifies payload type as defined in FTCP proto file – Refer to requirement **PMPR-REQ-354875/A- and PMPR-REQ-354876/A** |
|  |  | |  | Encrypted | 0x0 |  |
|  |  | |  | Signed | 0x1 |  |
| R | ECUID\_CAN | | Int32 | - | 0-4095 | Refer to Netcom ECUID table |
| O | ErrorCode | | Enum | - | - | To indicate a feature specific error code (see IVI-SOA-FUR-REQ-277456 for full list of errors) |
|  |  | |  | No Error | 0x000 |  |
|  |  | |  | Response  Time Error | 0x001 |  |
|  |  | |  | Cancel  Time Error | 0x002 |  |
|  |  | |  | … | … |  |
|  |  | |  |  | 0xFFF |  |

#### ECG设置中控主机认证状态

ECG将从中控主机获取的设备元数据发送给福特认证后台通过后, 通过setProvisioningState 接口向中控主机发送命令, 要求切换认证状态.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |
| **Method Type** | | One-Shot(Message is sent continuously until the ProvServer receives Ack) | | | | |
| **QoS Level** | | Default | | | | |
| **Retained** | | No | | | | |
|  | | | | | | |
| **R/O** | **Name** | | **Type** | **Literals** | **Value** | **Description** |
| **Request (\_Rq)** | | | | | | |
| R | ProvisioningStateRequest | | Enum | - | - | To request the ProvOnBoardClient3 and/or ProvOnBoardClient5 to enter one of the supported provisioning states. |
|  |  | |  | Factory Mode | 0x38 |  |
|  |  | |  | Unprovisioned | 0x39 | ProvServer is the only one that can request the ProvOnBoardClient3 and/or ProvOnBoardClient5 to enter Unprovisioned Mode (0x39) |
|  |  | |  | ECU Provisioning Ack | 0x3A |  |
|  |  | |  | Provisioned | 0x3B | ProvServer is the only one that can request the ProvOnBoardClient3 and/or ProvOnBoardClient5 to enter Provisioned (0x3B) |
| **Response (\_Rsp)** | | | | | | |
| R | ProvisioningStateResponse | | Enum | - | - | ProvOnBoardClient3 and/or ProvOnBoardClient5 response to a provisioning state change request. |
|  |  | |  | Success | 0x00 |  |
|  |  | |  | Wait | 0x01 |  |
|  |  | |  | Fail-Param Does Not Exist | 0x02 |  |
|  |  | |  | Fail-Param Read Only | 0x03 |  |
|  |  | |  | Fail-Param Out Of Range | 0x04 |  |
|  |  | |  | Fail-Param Size Incorrect | 0x05 |  |
|  |  | |  | Fail-Unknown Command Type | 0x06 |  |
|  |  | |  | Fail- SYNC Internal Error | 0x07 |  |
|  |  | |  | Fail-Command Already In Progress | 0x08 |  |
|  |  | |  | Fail-Comman Not Permitted | 0x09 |  |
|  |  | |  | Fail-Internal Memory Error | 0x0A |  |
|  |  | |  | Fail-Invalid Config Data | 0x0B |  |
|  |  | |  | Fail-Part2No Mismatch | 0x0C |  |
|  |  | |  | Fail-Invalid Apply Type Combo | 0x0D |  |
|  |  | |  | Fail-Access Denied | 0x0E |  |
|  |  | |  | Fail-Config Item Mismatch | 0x0F |  |
|  |  | |  | Fail-Already In Same State | 0x10 |  |
| O | ErrorCode | | Enum | - | - | To indicate a feature specific error code (see IVI-SOA-FUR-REQ-277456 for full list of errors) |
|  |  | |  | No Error | 0x000 |  |
|  |  | |  | Response  Time Error | 0x001 |  |
|  |  | |  | Cancel  Time Error | 0x002 |  |
|  |  | |  | … | … |  |
|  |  | |  |  | 0xFFF |  |

#### ECG广播认证状态

ECG收到中控主机对于设置主机认证状态消息的反馈后, 发送ECGProvisioningStateBroadcast消息

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |
| **Method Type** | | One-Shot | | | | |
| **QoS Level** | | Default | | | | |
| **Retained** | | Yes | | | | |
|  | | | | | | |
| **R/O** | **Name** | | **Type** | **Literals** | **Value** | **Description** |
| **Request (\_Rq)** | | | | | | |
| - | N/A | | - | - | - | N/A |
| **Response (\_Rsp)** | | | | | | |
| R | ECGProvisioningState | | Enum | - | - |  |
|  |  | |  | Factory Mode | 0x20 |  |
|  |  | |  | Unprovisioned | 0x21 |  |
|  |  | |  | Waiting for ECG Provisioning Response | 0x22 |  |
|  |  | |  | Waiting for TCU Provisioning Response | 0x23 |  |
|  |  | |  | Waiting for HomeURL | 0x24 |  |
|  |  | |  | Connecting to HomeURL | 0x25 |  |
|  |  | |  | Provisioned | 0x26 |  |

### 交互数据

中控主机认证使用的元数据条目如下

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **R/O (\*)** | **Name** | **Attribute** | **Datatype** | **Based64**  **encoded** | **Length** | **Sample** |
| R | FESN | 0xF17F | ASCII | No | 8 chars | 1EG004Q6 |
| R | SecurityKeyPackageID | 0xD03D | ASCII | Yes | 40 chars. | EF9FAD62EAD4DA9E635BAFCE8E6B7A50AD0D8B62 |
| R | Hardware/CoreAssembly Part Number | 0xF111 | ASCII | No | 24 chars. |  |
| R | Software Part Number | 0xF188 | ASCII | No | 24 chars. |  |
| R | Calibration Config Part number | 0xF10A | ASCII | No | 24 chars. |  |
| R | Delivery Assembly Number | 0xF113 | ASCII | No | 24 chars. |  |
| R | part2Partnumber | 0xF110 | ASCII | No | 20 chars. |  |
| R | ECUID | ECU ID is an unique and fixed value for each ECU | Hexadecimal | Yes | 8 chars. |  |
| R | ECU\_Provisioning State (ECUProvDID) | 0xD021 | Hexadecimal | Yes | Enum  24 chars. |  |
| O | Ethernet Mac Address | ECU internal data | ASCII | No | 17 chars. |  |
| O | Wi-Fi Mac Address | 0xFD26 | ASCII | No | 17 chars. |  |
| O | Bluetooth Mac Address | ECU internal data | ASCII | No | 24 chars. |  |
| O | Firmware Version | 0xFD12 and  0xFD15 | ASCII | No | 50 chars. |  |
| O | Primary Bootloader Part Number | CCPU: 0x8068  VMCU: 0xD027 | ASCII | No | 24 chars. |  |
| O | Recovery load part number | CCPU: 0xEEFF  VMCU: 0xEEFE | ASCII | No | 24 chars. |  |
| O | Global Configuration Version | Refer to ECU part II spec | ASCII | No | 50 chars. | [[1]](#footnote-1) |

### 电源管理相关

当车辆处于运输模式下, 点火开关一旦打开, 中控主机需保持唤醒, 以便ECG完成后续认证过程

### 网络通道功能

中控主机认证过程一般由ECG通过TCU提供的网络通道进行.在TCU不可用的情况下, 如中控主机具备WiFi连接广域网络, 应允许ECG使用此通道进行认证过程. 该部分功能详细描述参考WIR相关需求, 不在本文档详细描述.

-EOF-

1. 数据源于PMPR-REQ-354898/A-Payload Parameters Definition for ProvOnBoardClient 3 on Ethernet [↑](#footnote-ref-1)