Case Study:

Digital Key Implementation on Passenger Vehicles

1 Introduction

1.1 Overview

Digital Key is a common terminology for technologies that enable Locking/Unlocking and Starting Engine of a Vehicle without a Physical Key. The most appealing use case of Digital Key is to use the Phone as a Key, where in the Key of the Vehicle is imported into the Wallet app on the phone to do an access and engine start with a Security level on par with that used for Payments.

ThinkSeed is a leading provider of Digital Key for Automotive, providing end to end solution for integrating Digital Key technologies into the Car. This document explains a case study of a Digital Key integration experience of ThinkSeed for a leading Vehicle OEM.

1.2 Objectives

The Objective of this document is to examine a Case Study of integration of ThinkSeed Digital Key technology (also branded as THINKey) to a Vehicle of a leading OEM. The following aspects shall be covered

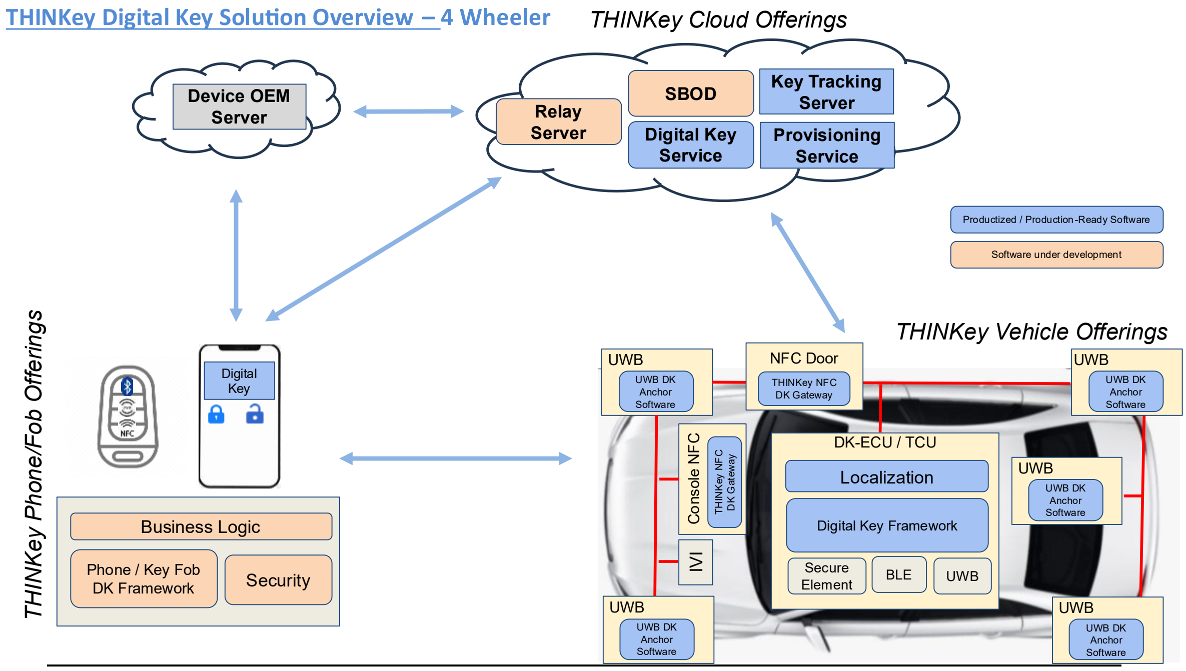
- What is THINKey Digital Key Solution Features and Offerings from ThinkSeed?
- What were the Digital Key solution Requirements of the OEM?
- What were the different ECUs and work components involved in integrating the Digital Key solution into a Vehicle?
- What were the different Performance and Certification requirements for the Digital Key solution
- What was the ThinkSeed's scope of work in integrating the Digital Key Solution to the OEM's Vehicle
- What were the Challenges for development and integration of this solution?
- What is OEMs future roadmap to upgrade the Digital Key Solution.

2 THINKey Digital Key Solution Offerings

2.1 THINKey Features

Serial No.	Feature	Sub Feature	Yes/No	Comments
1		BLE + UWB (CCC 3.0 WCC3)	Yes	
2		BLE + NFC (CCC 3.0 WCC2)	Yes	
3		NFC (CCC 3.0 WCC1)	Yes	
4	CCC Versions supported	CCC 4.0 Support	No	Under Development
5	Coarse Ranging	BLE	Yes	
6		BLE	No	
7	Fine Ranging	UWB	Yes	
8		Initiated from Phone	Yes	
9	Owner Pairing	Initiated from Vehicle	Yes	
10		Standard Authentication	Yes	
11	Authentication	Fast Authentication	Yes	
12		iPhone	Yes	
13	Phones Supported	Android phones	Yes	
14		Android -> Android	Yes	
15		iPhone -> iPhone	Yes	
16		Android -> iPhone	Yes	
17	Key Sharing	iPhone -> Android	Yes	
18		Delete Owner Key from Owner Phone	Yes	
19		Delete Friend Key from Owner Phone	Yes	
20		Delete Friend Key from Friend Phone	Yes	
21		Delete Owner Key from Vehicle	Yes	
22		Delete Friend Key from Vehicle	Yes	
23		Owner Re-pair initiated from Phone	Yes	
24		Owner Re-pair initiated from Vehicle	Yes	
25		Unpair (Factory Reset) from Phone	Yes	
26	Key Management	Unpair (Factory Reset) from Vehicle	Yes	
27	UWB Localization	UWB Localization Algorithm integrated	Yes	
28		Lock/Unlock	Yes	
29		Panic Alarm	Yes	
30	RKE Support	Ability to add Custom RKE commands	Yes	
31		Time Sync	Yes	
32		Multi Device Support	Yes	
33	Other System Features	Secure DK-ECU to UWB Anchor communication	Yes	
34		Digital Key Cloud Service Integrated	Yes	
35		Key Tracking support	Yes	
36		Key Management support	Yes	
37		SBOD Service	No	Under Development
38	Digital Key Cloud Service	Relay Server	No	
39	Vehicle Telematics	Integration with Vehicle Telematics	Yes	
40		Integrated with Apple Wallet	Yes	
41		Integrated with Google Wallet	Yes	
42	Wallet Integration	Integrated with Samsung Wallet	Yes	
43	NFC Card Support	Support for NFC Card	Yes	
44	Keyfob Support	Support for BLE+UWB, NFC Keyfob	No	Under Development
45		Kick-Sensing	No	Under Development
46		Intruder Detection	No	Under Development
47	UWB Sensing	Child Presence Detection	No	Under Development

THINKey Offerings Overview



2.1.1 Licensed Software (provided in binary)

- Vehicle
  - Digital Key Framework
  - Localization module
- Server
  - Digital Key Containerized Service
  - Key Tracking Server, Relay Server, SBOD
  - Provisioning Service
- Key Fob
  - Key Fob DK Framework
- UWB Radar
  - Child Presence Detection
  - Kick Sensing
- UWB PC Tool

2.1.2 Engineering Services

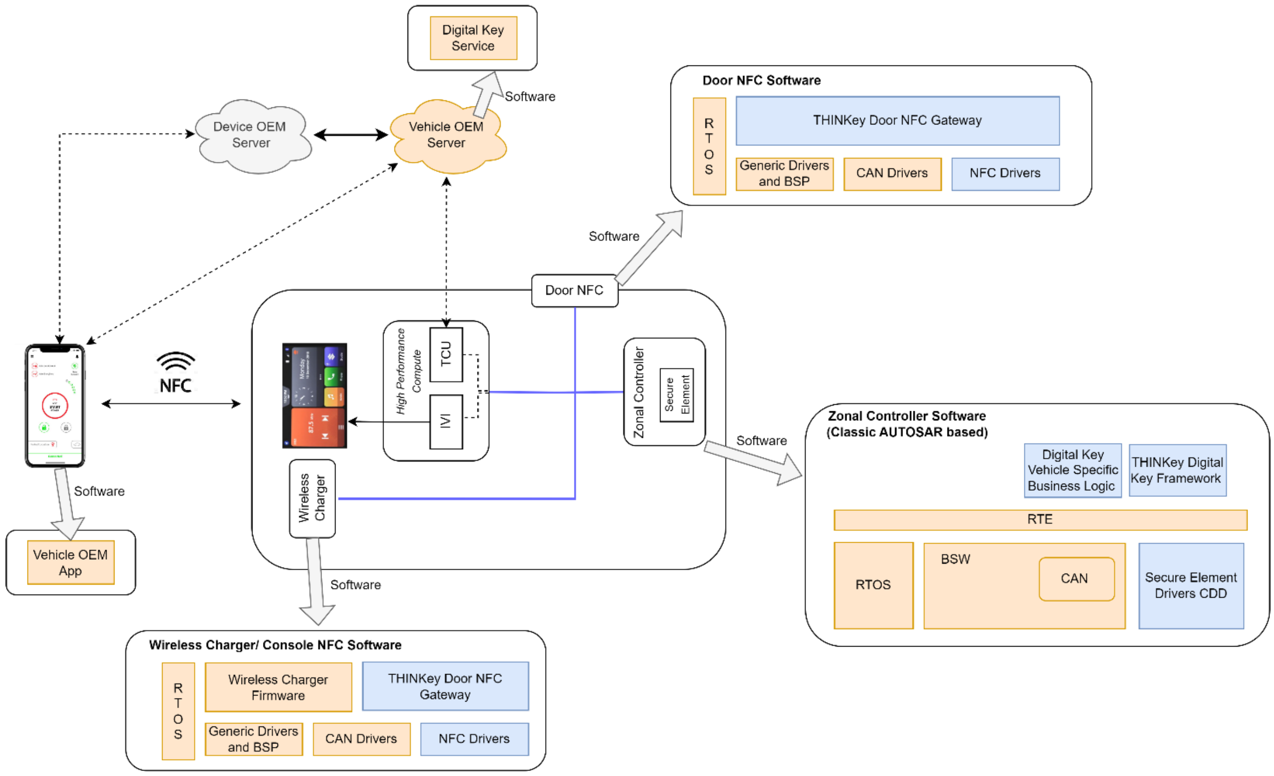
- Software (provided in source)
  - UWB Anchor Software, BLE+UWB Anchor Software
  - Door/Console NFC Software
  - Digital Key Business Logic
- System Integration & Validation
- Pre-Certification
  - Apple Car Keys,
  - Google, Samsung
  - CCC
- Certification
  - CCC (ThinkSeed is an ATL for CCC)

3 Case Study Overview

3.1 Company/Brand Overview

The Vehicle OEM for which the Digital Key was implemented is a leading Indian OEM for their newly launched EV portfolio. The Vehicle OEM introduced an advanced SDV architecture in this Vehicle. The goal was to integrate Digital Key into this Advanced Architecture Vehicle which the OEM planned to replicate into their other EV and ICE models as well.

3.2 Digital Key Solution System Requirements from Vehicle OEM



3.2.1 Feature Requirements

- Compliant to CCC Digital Key 3.0 (WCC1) – NFC Only
- Pairing of Owner Phone
  - Can be initiated from the Vehicle OEM App
  - Can be initiated from the Vehicle
  - Can be initiated from the Wallet App
- Authentication
  - Fast Authentication on the Door Handle for Door Lock/Unlock Authentication
  - Standard Authentication on the Console NFC for Engine Start Authentication
- Sharing
  - Ability to Share already Paired Owner Key with Friends from Wallet App
  - Support for Cross Platform Sharing (iPhone <-> Android Phone)
- Key Management
  - Ability to View and Manage keys from the Vehicle IVI
  - Ability to Manage keys from Owner or Friend Phone
  - Support Owner Change use cases (without the Friend getting removed)

  - Support Vehicle Unpair use cases (when a vehicle is sold)
- EOL and Field Requirements
  - Vehicle Specific Provisioning during EOL
  - Dynamic Provisioning in Field when Vehicle Owner Changes or for Certificate Revocation use cases

3.2.2 Platform Details

- Zonal Controller
  - Classic AUTOSAR based System
  - Digital Key Framework and Business Logic shall run as SWC
  - Secure Element with CCC applet is part of Zonal Controller. Special Provisioning needed during EOL and in field for the Secure Element.
  - Secure Element Drivers ported as Complex Device Drivers (CDD)
- Door NFC Reader / Wireless Charger(Console NFC)
  - RTOS based System
  - NFC Drivers supporting Polling requirements for Door/Console NFC as per CCC Reader Class
  - NFC Gateway needed to channel NFC data to CAN and vice-versa
- Vehicle OEM Server
  - Containerized Services Running on Cloud infrastructure to implement Digital Key Management and Key Tracking Services as per CCC
- Vehicle OEM App
  - OEM specific App running on iPhone or iOS to which Digital Key functions shall be integrated.
  - Vehicle OEM App shall interface to the Wallet App to give the user the Digital Key usage experience similar to what can be done with the Device OEM Wallet App.

3.2.3 Certification Requirements

- The Following Certifications/Approvals were needed
  - NFC Forum Certification
  - CCC Certification from the Car Connectivity Consortium (NFC Forum Certification is a pre-requisite for this)
  - Car Keys Certification
  - Google Approval
  - Samsung Audit

3.3 ThinkSeed Scope of Work in the Project

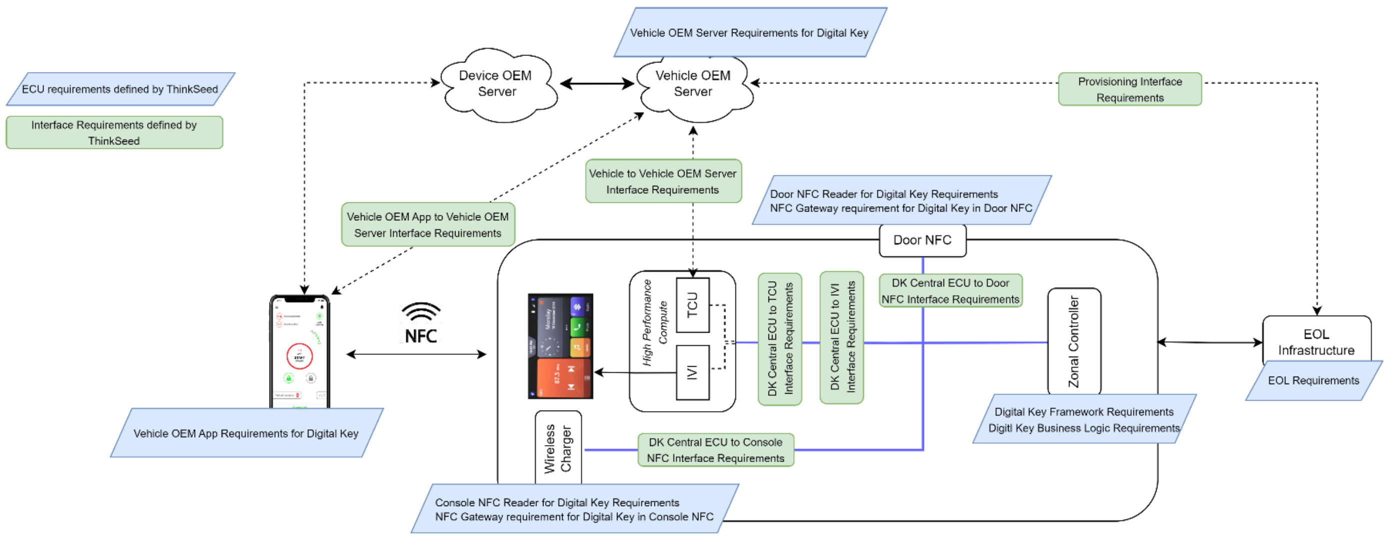
3.3.1 ThinkSeed Responsibilities Overview

The Following were the high-level Responsibilities for ThinkSeed in the project

  - Software IP (Licensed components)
    - Digital Key Stack (THINKey) on Vehicle ECU.
    - Secure Element Driver (CDD)

- Engineering Services
  - Define Full System and Component Level Requirements
  - System Integration and System Validation
  - CarKeys Pre-Certification, Google Pre-Certification
  - CCC Certification

3.3.2 System Requirements



- **ECU Requirements**
  - ThinkSeed was responsible for defining the requirements of the following ECUs/Components
    - Zonal Controller
    - Door NFC/ Console NFC
    - IVI Requirements
    - TCU Requirements
  - In each of these ECU component requirements ThinkSeed defined detailed State Machine, Flows and numbered requirements
  - One Key aspect taken care while authoring the requirements was to make sure all the certification requirements required at a System level is translated into component level requirements.

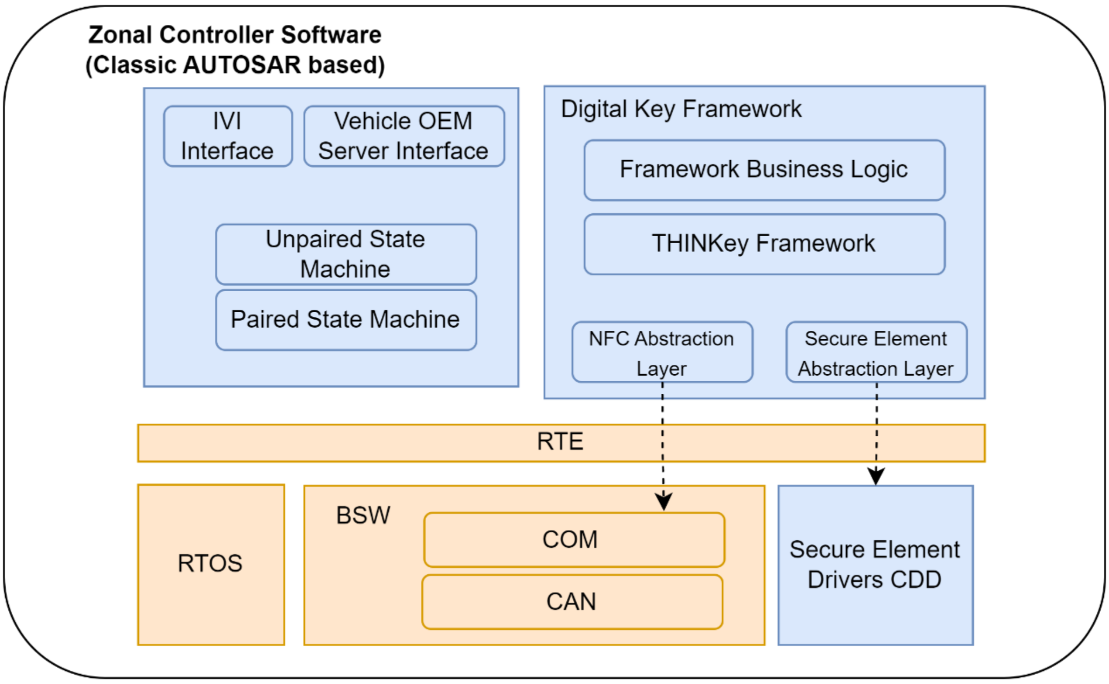
- **Vehicle OEM Server and App**
  - ThinkSeed was responsible for defining the Vehicle OEM Server requirements including functional requirements and SLAs (Service Level Agreements) for Availability, Response Time, Disaster management etc.
  - ThinkSeed was responsible for defining the Vehicle OEM App requirements including Owner Pairing, Key Management and User experience to align with Device OEM Certification requirements.

- **Interface Requirements**
  - ThinkSeed was responsible for defining the following Interface requirements
    - Between Zonal Controller and Door NFC
    - Between Zonal Controller and Wireless Charger (Console NFC)
    - Between Zonal Controller and IVI

- Between Zonal Controller and TCU
- Between Vehicle and Vehicle OEM Server
- Interface definitions were done by ThinkSeed and CAN DBC created by the OEM

- **EOL Provisioning and Field Provisioning requirements**
  - The Zonal controller has a secure element which has 100 odd provisioning parameters. There parameters are of 3 types
    - Certificates – ROOT CA, Intermediate CA certificates common to all Vehicles of the OEM
    - Static Parameters – Parameters which are configured as per the CCC implementation needs of the vehicle OEM. Common for all vehicles of the OEM
    - Vehicle Specific Parameters – Certificate and Parameters to be installed uniquely for every vehicle.
  - Owner Changing his phone scenario
  - Owner selling his Car Scenario
  - Certification Revocation scenario
  - Secure Element Re-provisioning scenario during Maintenance
    - Secure Element provisioning is usually locked in the EOL stage. Special procedures to be followed for re-provisioning

3.3.3 THINKey Digital Key Stack Integration

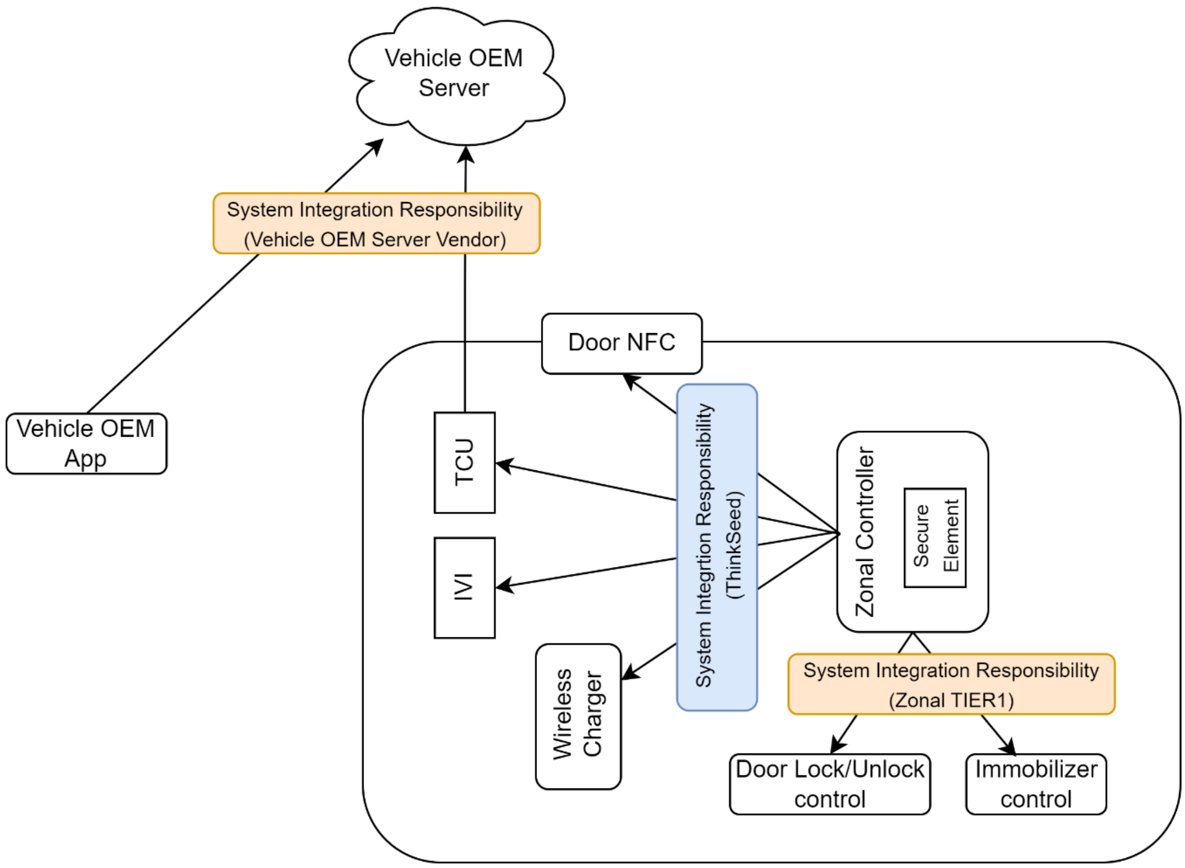


- Digital Key Framework is an IP already developed from ThinkSeed. This was integrated into Customer AUTOSAR platform as SWC. Integration included
  - Structuring the Digital Key Framework as an SWC to suit customer's AUTOSAR requirements

- Framework Business Logic layer implemented to take care of some custom requirements of Vehicle OEM
- Abstraction layers
  - NFC Abstraction Layer (NAL): Implemented to remotely access the NFC readers (Console and Door NFC) over CAN
  - Secure Element Abstraction Layer (SEAL): Implemented to access the Secure Element CDD over RTE

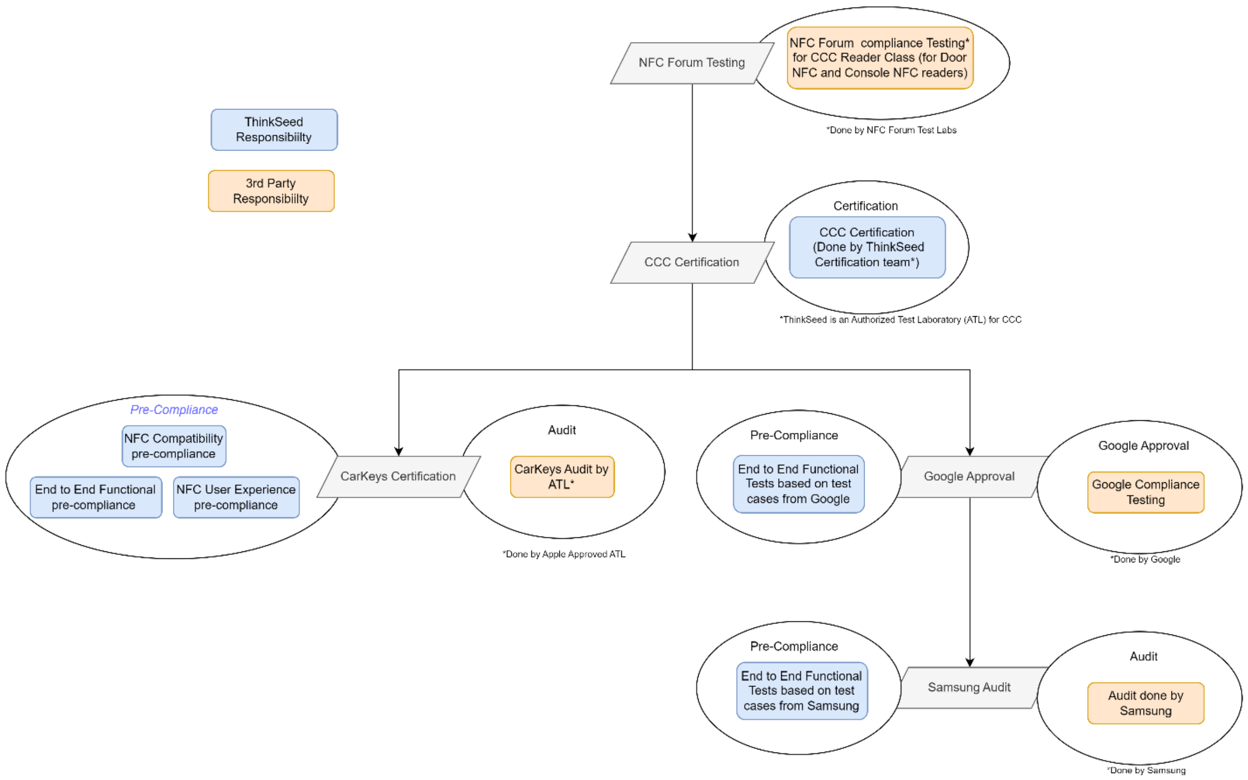
- Developed Secure Element Drivers as CDD (Complex Device Driver) needed for the Customer's AUTOSAR platform.
- Developed the Vehicle OEM specific business logic needed for Digital Key as a separate SWC

3.3.4 System Integration



- The System Integration Responsibilities were as shown in the Figure above.
- System Integration involves defining Integration test cases and individually testing each Integration link.
- System Integration also involved making sure performance parameters are met especially the Fast Authentication timing (700ms) and Standard Authentication timing (800ms). This involved splitting the full timing into different components and measuring the timing of each component and optimization.

3.3.5 Certification



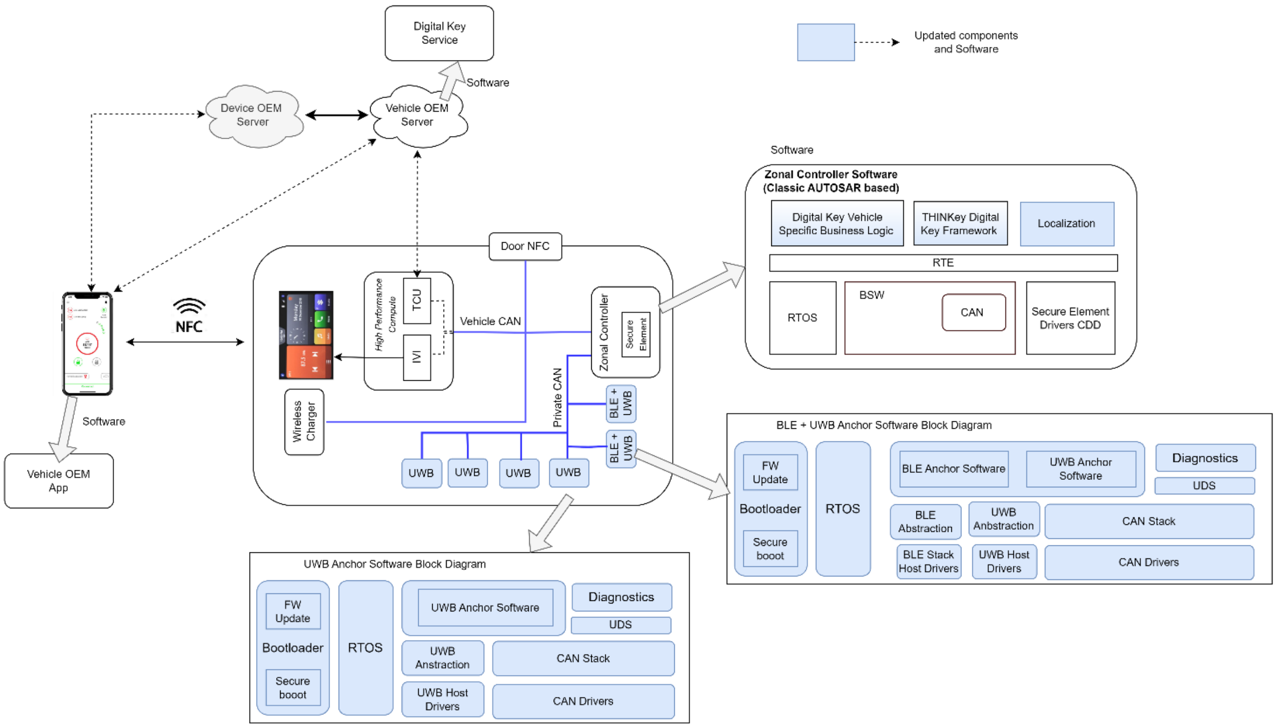
- The Figure above shows the certification flow to meet the Certification requirements
- The Certification and Pre-compliance done by ThinkSeed in the certification flow is colour coded in blue.

3.4 Challenges faced for Development and Integration

- Integrating Digital Key into a Vehicle involves integrating implementations in multiple ECUs. This is a big challenge especially when the vendors for each ECUs were different. ThinkSeed working as a Digital Key System integrator (working as an extended Systems team) helped defining and streamlining requirements and system integration Steps
- Meeting the Performance requirements was a big challenge because again performance requirements span over multiple ECUs. Splitting the overall Performance requirements as targets to different components (like latency of detection on NFC reader, NFC to CAN translation, CAN transit, THINKey framework latency, Secure Element processing) helped analysing and optimizing this.
- Figuring out the different EOL and Field Provisioning scenarios and creating flow was a big challenge because there were multiple stake holders for this including the EOL team. The flow needed to be optimized because any delays (or failures) here would directly affect the production line.

3.5 Future Roadmap (Upgrading to BLE+UWB based Digital Key)

The Vehicle OEM is planning upgrade of the above system to support CCC 3.0 WCC3 configuration. The system architecture update will be as shown in the figure below.



- ThinkSeed already has a reference implementation for CCC 3.0 WCC3 (Reference ECU software and reference Anchor software). This will be ported to Customer Platform Architecture
- Features like Passive Entry, Passive Engine start, Time Sync, Multi Device Support will be productized on the Vehicle OEM Platform
- ThinkSeed will be responsible for System Integration and will support TIER1 for Full System Validation
- ThinkSeed will also execute CarKeys, Google and CCC test cases as part of Self-Certification and triage issues.
- ThinkSeed will also be responsible for Certification Program Management
- Vehicle OEM is planning Launch of this feature in their Vehicle in Q1 2027